Solutions évolutives pour les réseaux de communication quantique

Bruno Fedrici

UNIVERSITÉ CÔTE D'AZUR

INPHYNI
INSTITUT DE PHYSIQUE DE NICE

École doctorale n°364 : Sciences Fondamentales et Appliquées
Unité de recherche : Institut de Physique de Nice, CNRS, UMR 7010

Thèse de doctorat

Présentée en vue de l'obtention du
grade de docteur en Sciences
de l'Université Côte d'Azur
dans la spécialité : Physique

par

Bruno Fedrici

Solutions évolutives pour les réseaux de communication quantique

Dirigée par Sébastien Tanzilli, DR CNRS, INPHYNI, UCA
et co-dirigée par Virginia D'Auria, Maître de conférence, INPHYNI, UCA

Soutenue le 13 décembre 2017
Devant le jury composé de :

Gerd	Leuchs	Professeur, MPL, Université d'Erlangen-Nuremberg	Président
Nicolas	Treps	Professeur, LKB, ENS-PSL et UPMC-Sorbonne Université	Rapporteur
Eleni	Diamanti	Chargée de recherche CNRS, LIP6, UPMC-Sorbonne Université	Rapporteur
Sébastien	Tanzilli	Directeur de recherche CNRS, INPHYNI, Université Côte d'Azur	Directeur de thèse
Virginia	D'Auria	Maître de conférence, INPHYNI, Université Côte d'Azur	Directeur de thèse
Alessandro	Zavatta	Chargé de recherche INO-CNR, LENS, Université de Florence	Invité

UNIVERSITÉ CÔTE D'AZUR

INPHYNI
INSTITUT DE PHYSIQUE DE NICE

École doctorale n°364 : Sciences Fondamentales et Appliquées
Unité de recherche : Institut de Physique de Nice, CNRS, UMR 7010

Thèse de doctorat

Présentée en vue de l'obtention du
grade de docteur en Sciences
de l'Université Côte d'Azur
dans la spécialité : Physique

par

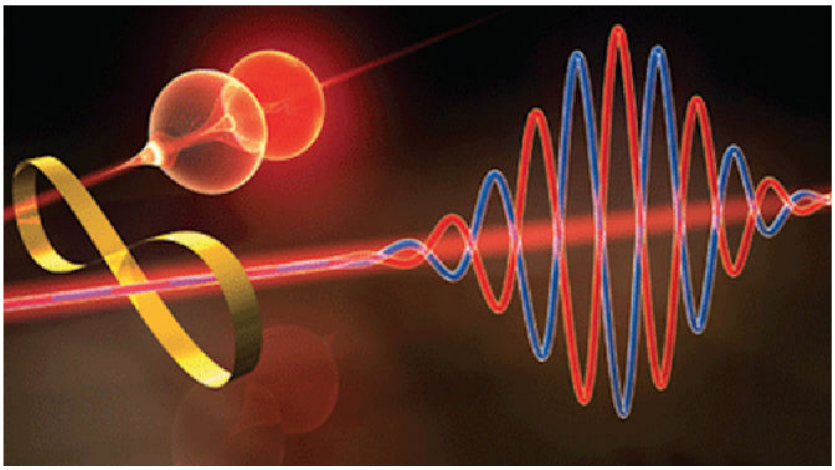
Bruno Fedrici

Solutions évolutives pour les réseaux de communication quantique

Dirigée par *Sébastien Tanzilli, DR CNRS, INPHYNI, UCA*
et co-dirigée par *Virginia D'Auria, Maître de conférence, INPHYNI, UCA*

Soutenue le 13 décembre 2017
Devant le jury composé de :

Gerd	Leuchs	Professeur, MPL, Université d'Erlangen-Nuremberg	Président
Nicolas	Treps	Professeur, LKB, ENS-PSL et UPMC-Sorbonne Université	Rapporteur
Eleni	Diamanti	Chargée de recherche CNRS, LIP6, UPMC-Sorbonne Université	Rapporteur
Sébastien	Tanzilli	Directeur de recherche CNRS, INPHYNI, Université Côte d'Azur	Directeur de thèse
Virginia	D'Auria	Maître de conférence, INPHYNI, Université Côte d'Azur	Directeur de thèse
Alessandro	Zavatta	Chargé de recherche INO-CNR, LENS, Université de Florence	Invité



"Information is physical", Rolf Landauer

Table des matières

Introduction générale **9**

1. Les technologies quantiques **15**
1.1. La deuxième révolution quantique 15
1.1.1. Le calcul quantique 15
1.1.2. La simulation quantique 21
1.1.3. La métrologie quantique 24
1.1.4. La cryptographie quantique 27
1.2. Internet des objets quantiques 33
1.2.1. Service cloud 35
1.2.2. Accès client longue distance 37
1.2.3. Mémoires quantiques et interfaces lumière-matière 42

2. Photons, modes et interferences **45**
2.1. Quantification du champ électromagnétique 45
2.2. Espace des phases 48
2.2.1. Quadratures 49
2.2.2. Opérateurs 50
2.3. Représentations 52
2.3.1. États de Fock 52
2.3.2. États cohérents 53
2.3.3. États comprimés 55
2.4. Interférences linéaires 56
2.4.1. Traitement quantique de la lame séparatrice 56
2.4.2. Lame séparatrice avec arrivée du champ sur un seul port d'entrée 58
2.4.3. Lame séparatrice avec arrivée du champ sur les deux ports d'entrée 60
2.4.4. Interféromètre de Mach-Zehnder avec un seul photon en entrée . . 63
2.4.5. Interféromètre de Mach-Zehnder avec n photons sur un port d'entrée 65
2.4.6. Détection par battement homodyne des quadratures du champ . . 66
2.5. Interférences non-linéaires 68
2.5.1. Conversion paramétrique non-dégénérée 68
2.5.2. Remarque sur le cas dégénéré 72

3. Synchronisation par horloge optique distribuée de sources de paires de photons intriqués **75**
3.1. Motivation . . . 75
3.2. Présentation générale du dispositif . . . 79
3.3. Caractérisation du dispositif . . . 82
3.3.1. Horloge optique . . . 82
3.3.2. Modules amplificateurs . . . 87
3.3.3. Étages de conversion en longueurs d'onde . . . 91
3.3.4. Filtrage spectrale . . . 96
3.3.5. Station relais . . . 100
3.3.6. Système de détection . . . 101
3.4. Étude de la visibilité en fonction de la statistique d'émission . . . 106
3.4.1. Nombre moyen de paires générées par impulsion . . . 106
3.4.2. Statistique d'émission . . . 106
3.4.3. Visibilité . . . 107
3.5. Position de la figure d'interférence . . . 109
3.6. Résultats . . . 110
3.6.1. Résultats préliminaires . . . 110
3.6.2. Synchronisation sur 100 km . . . 114
3.7. Conclusion . . . 118

4. Lumière comprimée à une longueur d'onde télécom : une approche entièrement guidée **121**
4.1. Motivation . . . 121
4.2. Présentation générale du dispositif . . . 123
4.3. Caractérisation du dispositif . . . 124
4.3.1. Étages de conversion en longueurs d'onde . . . 124
4.3.2. Système de détection homodyne . . . 128
4.3.3. Analyse spectrale . . . 133
4.4. Influence des pertes . . . 134
4.5. Résultats . . . 135
4.5.1. Mesure du niveau de compression . . . 135
4.5.2. Critère d'inséparabilité . . . 137
4.6. Conclusion . . . 138

5. Détecteurs de photons uniques en régime ON/OFF : traitement quantique des effets de gigue temporelle **139**
5.1. Motivation . . . 139
5.2. Rappel sur les règles de projection . . . 140
5.2.1. Cas d'une mesure idéale . . . 141
5.2.2. Cas d'une mesure générale . . . 142

5.3. Modélisation des effets de gigue temporelle 144
5.3.1. Notion de densité de POVM 144
5.3.2. État en entrée du détecteur 146
5.3.3. Statistiques et POVM 146
5.4. Applications 150
5.4.1. Détection directe 150
5.4.2. Mesure de coïncidences 151
5.4.3. Source de photons annoncés 155
5.5. Conclusion 157

6. Conclusion générale **159**

Annexes **161**
A. Établissement quantique de clés secrètes 161
A.1. Protocoles à variables discrètes 161
A.2. Protocoles à variables continues 170
A.3. Protocoles Device-Independent - DI-QKD 172
A.4. Protocoles Measurement-Device-Independent - MDI-QKD 173
A.5. Post-traitement classique 175
B. Caractérisation de photons uniques par interférence à deux photons . . . 177
B.1. Champ optique à un photon 177
B.2. Interférence à deux photons 180
B.3. Effets de gigue 188
C. Systèmes de détection 195
C.1. Détecteurs de photons uniques 195
C.2. Les compteurs de coïncidences 198

Bibliographie **200**

Introduction générale

Nous vivons actuellement au milieu d'une seconde révolution quantique [1]. En effet, la première révolution nous a permis d'établir et de vérifier les lois gouvernant l'interaction lumière-matière, lois ayant donné naissance à toute une myriade de dispositifs technologiques permettant de traiter et de communiquer de l'information au sens classique du terme. La seconde révolution va quant à elle nous permettre d'utiliser ces lois afin de développer de nouvelles technologies autorisant des opérations au niveau quantique !

La première révolution quantique pris place au début du siècle dernier, découlant de travaux visant à proposer un modèle théorique à même de reproduire les résultats obtenus lors d'expériences sur le rayonnement du corps noir [2]. De cette théorie surgit l'idée fondamentale de la complémentarité onde-corpuscule selon laquelle, pour reprendre les termes de Louis de Broglie, "deux conceptions apparemment incompatibles peuvent chacune représenter un aspect de la vérité" [3]. De cette simple idée découlent toutes les percées scientifiques et technologiques associées à cette première révolution quantique. Une fois réalisé comment un électron agit comme une onde, il est alors possible de comprendre la table périodique des éléments, les interactions chimiques et les fonctions d'onde électroniques qui sous-tendent la physique des semi-conducteurs. Ce dernier domaine d'étude nous a conduit à l'ère de l'information et à l'avènement de l'industrie de l'informatique. D'autre part, le fait qu'une onde lumineuse puisse aussi être traitée comme étant composée de particules, les fameux photons, nous a permis d'appréhender l'effet photoélectrique [4], à l'origine entre autres des cellules photovoltaïques. Enfin, le concept de photon est également à l'origine de notre compréhension de l'effet laser. Au cours du siècle dernier, cette première révolution quantique a permis l'émergence d'un grand nombre des technologies de base alimentant le quotidien de la société moderne.

Dans ce contexte, la deuxième révolution quantique devrait être responsable d'un nombre non négligeables d'avancées technologiques clés pour le vingt-et-unième siècle. Deux impératifs nous conduisent indubitablement vers les technologies quantiques. Le premier est d'ordre pratique. En effet la tendance dominante dans un siècle d'innovation technologique est la miniaturisation, à savoir construire des appareils de plus en plus petits, faciles à intégrer dans des systèmes plus complexes et plus fonctionnels. Ce premier impératif nous a d'ores et déjà mené à développer des nanotechnologies et devrait, à terme, nous mener à construire des dispositifs dont les quantités d'action s'approchent de la constante de Planck. À cette échelle, le fonctionnement des disposi-

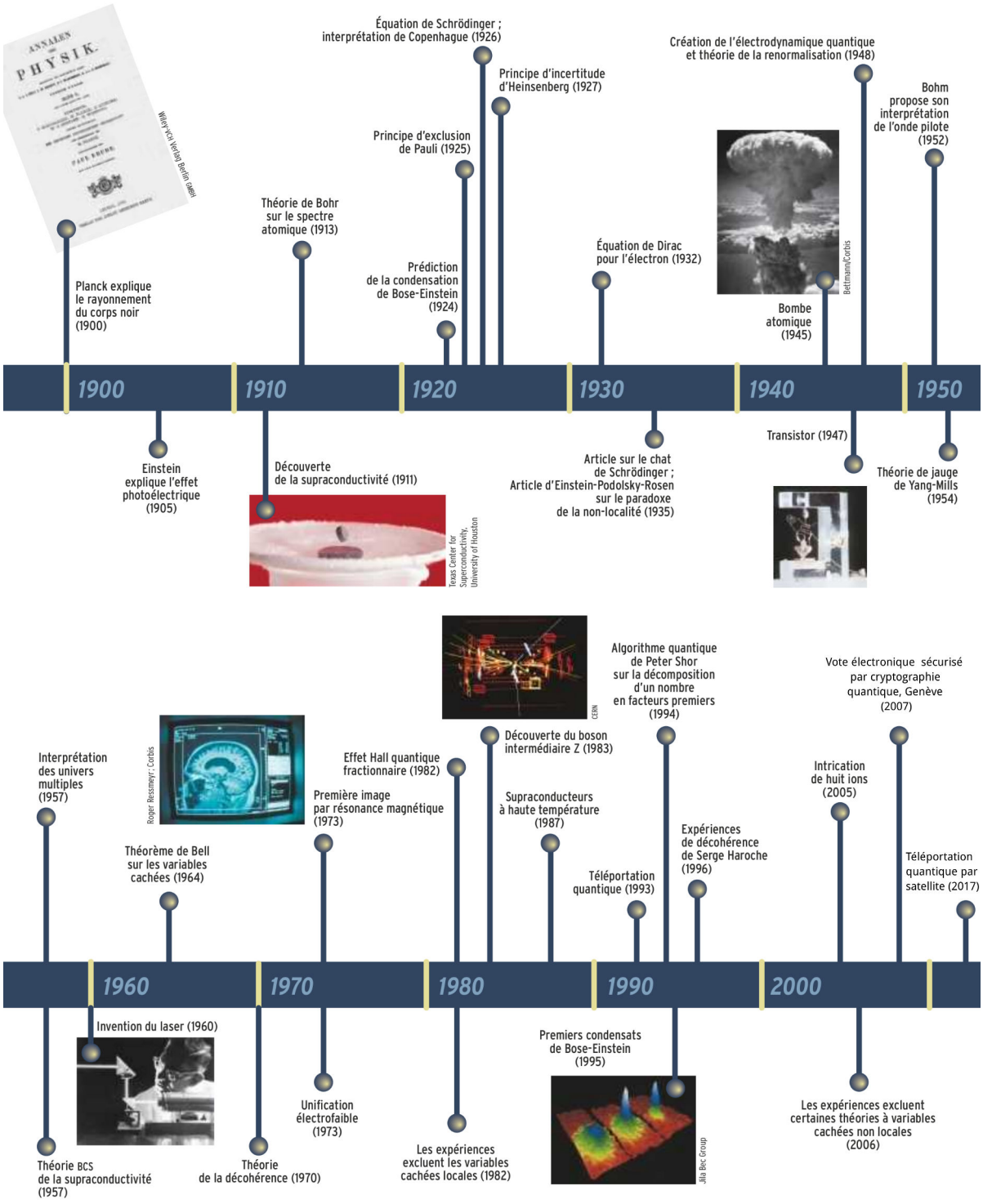


Figure 0.1. – Genèse et évolution de la physique quantique, des concepts fondamentaux à l'ingénierie.

tifs doit alors être basé sur des principes quantiques. Le second impératif est lui plus fondamental. Les principes de la physique quantique semblent offrir la promesse de performances considérablement améliorées par rapport à ce qui peut être réalisé dans un cadre classique.

La caractéristique de cette deuxième révolution quantique est la prise de conscience que les humains ne sont plus des observateurs passifs du monde quantique que la nature nous offre. Avec la première révolution quantique, dont la FIGURE 0.1 retrace la genèse et l'évolution, nous avons utilisé la physique quantique pour comprendre ce qui 'existait déjà'. Nous pouvons expliquer la table périodique, mais nous ne pouvons pas concevoir et construire nos propres atomes. Nous pouvons expliquer comment les métaux et les semi-conducteurs se comportent, mais nous ne pouvons pas vraiment manipuler ce comportement. La différence entre science et technologie tient dans le fait que la première est une entreprise de recherche visant à produire de la connaissance, tandis que la deuxième est son prolongement à des fins applicatives. Ainsi, nous nous attelons aujourd'hui à exploiter le monde quantique qui nous entoure. En d'autres termes, l'heure est à la manipulation des ressources pour concevoir nos propres états quantiques et développer de nouveaux dispositifs. Par exemple, en plus d'expliquer la table périodique, nous pouvons créer de nouveaux atomes artificiels - boites quantiques et excitons – auxquels nous pouvons attribuer les propriétés électroniques et optiques de notre choix. Nous pouvons créer des états en tant que superpositions cohérentes d'autres états ainsi que des états intriqués présentant des corrélations non-locales. Ces nouveaux états quantiques *man-made* ouvrent la voie au développement de processeurs [5], de simulateurs [6], de dispositifs métrologiques [7, 8] et de systèmes de cryptographie [9, 10] dits quantiques. Ainsi, bien que la physique quantique en tant que science a complètement mûri, l'ingénierie quantique en tant que technologie se dessine maintenant à part entière.

Les travaux présentés au sein de ce manuscrit s'inscrivent dans ce contexte. Plus spécifiquement, nous proposons des solutions tout-optiques dédiées au déploiement d'un réseaux quantique de communication aux longueurs d'ondes des télécommunications. Les divers facettes de ces travaux, qui se veulent complémentaires, répondent à des enjeux expérimentaux à la fois en régime de variables discrètes mais aussi continues, en vue d'associer, à terme, ces différentes approches dans des protocoles hybrides.

Plan du manuscrit

Chapitre 1 - Les technologies quantiques

Les technologies mettant en œuvre des superpositions quantiques d'états et/ou des états intriqués de divers systèmes physiques sont nombreuses. Dans ce premier chapitre, nous présentons un à un les principaux domaines applicatifs en lien avec ces technologies,

à savoir, le calcul, la simulation, la métrologie et la communication quantiques. Pour chaque domaine, nous discutons respectivement des avantages de l'approche quantique sur l'approche classique, puis nous dressons un état de l'art le plus exhaustif possible des différents supports physiques utilisés pour le codage et la manipulation de l'information quantique. Une fois la rétrospective des différents domaines applicatifs effectuée, nous discutons dans la seconde moitié du chapitre de leur interconnexion en vue de permettre, à terme, le déploiement d'un Internet quantique.

Chapitre 2 - Photons, modes et interférences

Dans ce second chapitre, nous introduisons les notions d'optique quantique utiles à la description des différents travaux expérimentaux présentés au sein de ce manuscrit. Nous traitons ainsi respectivement de la quantification du champ électromagnétique et de la représentation d'états quantiques dans l'espace des phases, d'un ensemble non-exhaustif d'effets d'interférence linéaire à un ou plusieurs photons en présence d'une ou deux lames séparatrices, et enfin du phénomène de conversion paramétrique en présence d'un milieu non-linéaire d'ordre 2.

Chapitre 3 - Synchronisation par horloge optique distribuée de sources de paires de photons intriqués

Nous démontrons dans ce troisième chapitre un schéma de synchronisation à très haute cadence et d'une précision inégalée pour des communications sécurisées sur très longue distance. Le dispositif présenté s'appuie sur une configuration de relais quantique pour laquelle les temps d'émission de sources indépendantes de paires de photons intriqués doivent être synchronisés. L'exigence d'un débit élevé exclut la possibilité d'utiliser un régime de pompage continu. De plus, toute conversion électro-optique associée à une configuration maître/esclave en régime impulsionnel induirait l'apparition d'une gigue temporelle limitant la précision recherchée et donc la distance de synchronisation. Dans cette réalisation, nous proposons de contourner ces différents problèmes par l'utilisation d'un système de synchronisation par horloge tout optique distribuée. L'idée principale s'appuie sur l'utilisation d'un unique laser telecom picoseconde cadencé à 2.5 GHz afin de générer l'horloge et de pouvoir la distribuer efficacement à deux sources indépendantes de paires de photons intriqués. Les résultats présentés au sein de ce chapitre démontrent la synchronisation de notre lien relais pour une distance effective séparant les sources de plus de 100 km.

Chapitre 4 - Lumière comprimée à une longueur d'onde télécom : une approche entièrement guidée

La lumière comprimée est une ressource fondamentale dans bon nombre de protocoles d'information quantique. En vue du déploiement de dispositifs de communication quantique en régime de variables continues, la réalisation de systèmes expérimentaux facilement reconfigurables et compatibles avec les réseaux télécoms fibrés existants représente une étape cruciale. En réponse à ce cahier des charges, nous démontrons dans ce chapitre la faisabilité d'une expérience de compression à une longueur d'onde de télécommunication réalisée, pour la première fois, de manière entièrement guidée. Le dispositif présenté repose uniquement sur la technologie de l'optique non-linéaire guidée ainsi que sur l'utilisation de composants optiques issus des télécoms standards.

Chapitre 5 - Détecteurs de photons uniques en régime ON/OFF : traitement quantique des effets de gigue temporelle

En complément de l'usage de larges alphabets pour l'encodage des données, la communication quantique haut débit nécessite d'avoir recours à des régimes de pompage ultra-rapide ($\geq$ GHz). Dans ce contexte, une limitation majeure nous est donnée par la gigue temporelle du système de détection. En effet, cette dernière peut conduire à l'introduction d'erreurs dans le marquage des temps d'arrivée, qui altèrent à leur tour le comptage d'événements de coïncidences ou l'ingénierie d'états quantiques spécifiques dans le cas d'un schéma de détection annoncée. Malgré l'importance des systèmes de détection dans les technologies quantiques photoniques émergentes, aucune modélisation quantique de leurs effets de gigue temporelle n'a été à notre connaissance développé jusqu'à présent. Nous proposons dans ce chapitre un modèle théorique, basé sur le formalisme de densité de POVM [1], capable de quantifier explicitement l'effet de la gigue temporelle pour une classe typique de détecteurs de photons uniques. Nous appliquons notre modèle à certaines situations expérimentales usuelles.

1. *Positive operator-valued measure.*

Chapitre 1.

Les technologies quantiques

La génération et la manipulation d'états non classiques de la lumière s'inscrivent au cœur de ce travail de thèse. La physique quantique, autrefois cantonnée à décrire les lois de la nature au sein d'instituts de recherche, permet aujourd'hui le développement de technologies nouvelles dont l'objectif est de servir la société civile. En particulier, l'émergence de l'information quantique, développement de la théorie de l'information de Claude Shannon [11] exploitant les propriétés de la physique quantique, a donné, entre autre, naissance à des dispositifs de communication permettant l'établissement à distance de clés de chiffrement avec une sécurité inconditionnelle, prémices d'une nouvelle génération de réseaux de communication, et faisant déjà pour certains l'objet de commercialisations [12, 13, 14, 15, 16, 17].

L'organisation de ce premier chapitre est la suivante : après une brève présentation des différents axes de recherche actuels relatifs au développement des technologies quantiques, l'accent est ensuite porté sur l'interfaçage de ces technologies en vue de permettre, à terme, le développement d'un Internet des objets quantiques.

1.1. La deuxième révolution quantique

Les technologies reposant sur le traitement quantique de l'information visent à résoudre de nombreux défis sociétaux d'aujourd'hui. Dans les sections qui suivent, nous présentons les différentes technologies quantiques faisant actuellement l'objet d'intenses recherches aussi bien fondamentales qu'appliquées, à savoir : le calcul, la simulation, la métrologie et la cryptographie quantique. Pour toutes ces applications, l'avantage de l'approche quantique sur l'approche classique ainsi que les différents supports physiques porteurs de l'information quantique sont à chaque fois discutés.

1.1.1. Le calcul quantique

Les taches de calcul sont généralement classées suivant le type de relation existant entre le volume des opérations à effectuer et la taille du problème [18]. Si le nombre d'opérations augmente comme une puissance entière de la taille N du problème, on dit

que ce dernier appartient à la classe de complexité polynomiale dénotée, de manière abrégée, par la lettre P. Si par contre le nombre d'opérations augmente plus rapidement qu'une fonction polynomiale, alors le problème est dit appartenir à une classe de complexité non-polynomiale (NP). Lorsque N croit, la valeur de la fonction non-polynomiale deviendra toujours supérieure à celle de la fonction polynomiale.

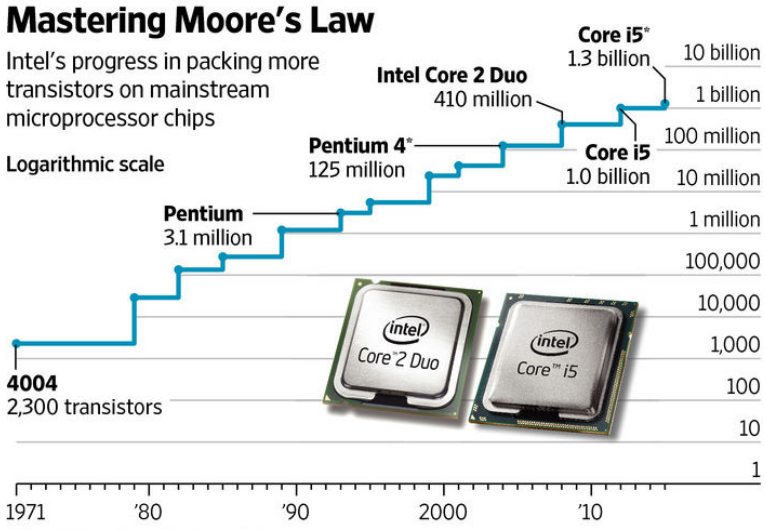


Figure 1.1. – La technologie actuelle des ordinateurs est fondée sur les microprocesseurs en silicium et a connu un essor extraordinaire depuis son introduction dans les années 60. La loi de Moore [19] affirme que le nombre de transistors dans un microprocesseur double tout les 18-24 mois. La croissance exponentielle que cette loi prédit est vérifiée depuis 40 ans. La figure montre la progression exponentielle du nombre de transistors dans une puce depuis le microprocesseur Intel 4004 introduit en 1971 et possédant 2300 transistors jusqu'au Core i5 introduit en 2009 et qui en possède 1 300 000 000 [20].

Les ordinateurs actuels sont capables de traiter des problèmes de la classe P sans trop de difficultés. Si le problème est pour l'instant trop difficile à résoudre, la loi de Moore nous montre, voir FIGURE 1.1, que nous devrions être capable de le résoudre dans un futur proche compte tenu de la croissance exponentielle de la puissance de calcul. En revanche, les problèmes de classe NP resteront quant à eux toujours difficiles voir impossible à traiter. Une légère augmentation de taille du problème se traduit dans ce cas par une forte augmentation de la puissance de calcul nécessaire. Un exemple important d'un problème de classe NP est la factorisation de grands entiers. Actuellement, la seule façon de trouver les facteurs premiers d'un grand nombre entier N est de diviser N par tous les entiers impaires jusqu'à $\sqrt{N}$ et de vérifier s'il y a un reste ou non. Cette procédure de division requiert environ N opérations supplémentaires chaque fois que nous augmentons N de un. En d'autres termes, le nombre d'opérations augmente exponentiellement avec N. De ce fait, en augmentant N, le temps de calcul nécessaire

pour trouver les facteurs premiers augmente également de manière exponentielle. C'est précisément ce qui rend sûr le protocole de cryptographie à clés publiques nommé RSA, d'après les initiales de ses trois inventeurs, utilisé sur Internet notamment pour le commerce électronique [21].

Les difficultés rencontrées en présence de problèmes de classe NP présupposent cependant que les ordinateurs en question sont des ordinateurs conventionnels fonctionnant selon les principes de la physique classique. Ces principes s'expriment mathématiquement en fonction des opérations des machines universelles de Church-Turing [22]. Une avancée significative a eu lieu en informatique lorsque l'on a réalisé qu'il peut exister d'autres types d'ordinateurs fonctionnant sur des principes différents de ceux des machines de Turing. Dans ce cas, la machine de Turing doit être considérée comme le cas limite d'une classe plus générale d'ordinateurs fonctionnant sur les principes de la physique quantique plutôt que de la physique classique. L'idée de faire fonctionner un ordinateur sur la base des lois de la physique quantique a été proposée initialement par Richard Feynman en 1982 [23]. Il a fait remarquer qu'il devient progressivement beaucoup plus difficile de simuler des systèmes quantiques avec des ordinateurs conventionnels vu l'augmentation exponentielle de la puissance de traitement nécessaire lorsque la taille de ces systèmes augmente. Il avança alors l'idée radicale d'introduire du hardware quantique dans l'ordinateur de manière à ce que la puissance de calcul de ce dernier puisse augmenter proportionnellement à la complexité du système considéré. Trois ans plus tard, David Deutsch écrivit un article théorique esquissant les principes de base de l'informatique quantique [24]. Par analogie avec la machine de Turing, il introduisit la notion d'ordinateur quantique universel et montra que ce dernier permettrait en principe de résoudre des problèmes qui ne sont pas solubles de manière efficace avec un ordinateur classique. Les idées à la base des ordinateurs quantiques impliquent de repenser en profondeur la manière dont fonctionnent les ordinateurs. Il est important de réaliser que l'information est de nature physique, comme l'expliqua Landauer [25], dans le sens où les ordinateurs classiques encodent les bits d'information par des procédés physiques variés tels que des voltages sur un transistor, la magnétisation d'un matériau ferromagnétique ou l'intensité d'une impulsion lumineuse. Bien que la physique des transistors, des aimants ferromagnétiques et des impulsions lumineuses est gouvernée par la physique quantique, la façon dont les données sont codées et exploitées par la suite est quant à elle purement classique. Cela signifie par exemple que la tension appliquée à un transistor a une valeur bien définie qui peut être déterminée de manière unique suivant les lois de l'électronique classique.

L'idée de Deutsch fut de faire un bond en avant en encodant l'information comme des états quantiques n'ayant aucun analogue classique, l'état le plus simple étant alors un qubit. Le qubit se compose d'une superposition de deux états de base, notés avec le formalisme de Dirac $|0\rangle$ et $|1\rangle$. Un bit classique se trouve toujours soit dans l'état $|0\rangle$, soit dans l'état $|1\rangle$. Dans le cas général, un qubit se trouve dans une superposition de ces deux

états, que l'on peut décrire par une combinaison linéaire des deux états : $\alpha\,|0\rangle + \beta\,|1\rangle$. Les coefficients α et β étant deux nombres complexes vérifiant la relation de normalisation $|\alpha|^2 + |\beta|^2 = 1$. De l'idée de Deutsch, il découle une augmentation exponentielle de la puissance de calcul lorsque le système devient plus grand. Ceci provient de l'exploitation avantageuse de la notion de superposition d'états. En conséquence, la superposition ouvre la porte au parallélisme quantique dans les algorithmes d'évaluation de fonctions. En effet, si un qubit est dans une quelconque superposition d'états $\alpha\,|0\rangle + \beta\,|1\rangle$, deux qubits réunis sont quant à eux dans une superposition d'états $\alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle$. Avec 10 qubits, on a 1024 états superposables, et avec n qubits, 2^n. Donc, quand un opérateur est appliqué à l'ensemble des qubits, il est, en quelque sorte, appliqué à 2^n états en même temps, ce qui équivaut à un calcul parallèle sur 2^n données. C'est pourquoi la puissance de calcul théorique d'un ordinateur quantique double à chaque fois qu'on lui adjoint un qubit. Une fonction $f(x)$ peut alors être évaluée simultanément pour plusieurs valeurs de x : c'est l'algorithme de Deutsch-Jozsa [26]. On peut également mentionner les avancées significatives qui eurent lieu en 1994 quand Peter Shor développa un algorithme reposant sur la manipulation d'états quantiques pour effectuer des opérations de factorisation [27], et en 1997 avec l'algorithme de Grover pour la recherche d'éléments dans une liste [28], deux problèmes passant ainsi de la classe NP à la classe P.

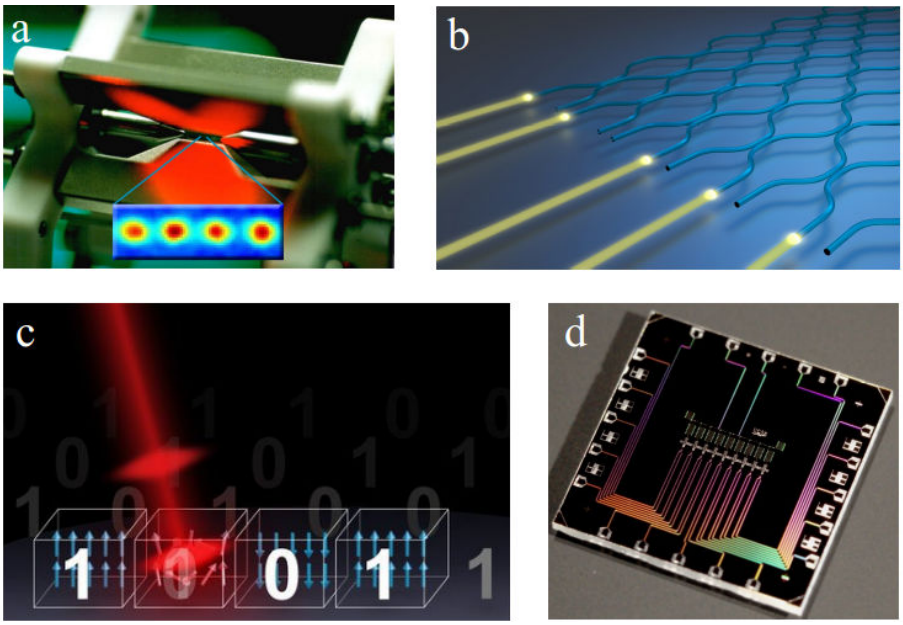


Figure 1.2. – **(a)** Intrication entre quatre ions piégés, R. Blatt et al., Université d'Innsbruck. **(b)** Photonique boson sampling, vue d'artiste, F. Scarrino et al., Université La Sapienza de Rome. **(c)** Manipulation de spin qubits par pulsations laser femtosecondes, vue d'artiste, B. Koopmans et al., Université Technologique d'Eindhoven. **(d)** Photographie d'un circuit supraconducteur avec neuf qubits, J. Martinis et al., Université de Californie.

Parmi les tentatives de réalisations expérimentales d'un processeur quantique, on peut citer différents supports, comme le propose la FIGURE 1.2 :

- **Les pièges à ions (Figure 1.2a)** - Les qubits correspondent aux états d'excitation d'une rangée d'ions se trouvant dans un piège. Les ions qui sont tous identiques, possèdent donc la même fréquence de résonance. Nous pouvons toutefois agir sur un seul ion en particulier à l'aide d'une impulsion laser car ces ions sont physiquement séparés les uns des autres. Les ions interagissent via des forces répulsives associées à des déplacements engendrés par les vibrations autour de leur position d'équilibre. La première réalisation d'une porte quantique CNOT (pour *Controlled-NOT*, bascule conditionnelle équivalent du OU exclusif classique) avec un système d'ions piégés fut proposée par Ignacio Cirac et Peter Zoller en 1995 [29], s'en suivit de nombreuses autres études [30, 31, 32] et réalisations expérimentales [33, 34, 35, 36, 37, 38, 39, 40, 41].

- **Les schémas tout optique (Figure 1.2b)** - L'implémentation pratique de portes logiques à un et deux qubits photoniques peut s'effectuer par encodage de l'information quantique sur les modes occupés par un photon unique et en manipulant ensuite ces modes par des composants d'optique linéaire (LOCQ - *Linear Optical Quantum Computing)* tels qu'une lame séparatrice, un rotateur de phase ou un miroir [42]. On peut citer le *boson sampling* [43, 44, 45, 46, 47, 48, 49] et le protocole KLM, du nom de ses inventeurs [50], comme deux approches du calcul quantique reposant sur l'optique linéaire, l'approche KLM bien que plus difficile à implémenter à l'avantage d'être universelle. Une approche reposant sur des états plus exotiques connus sous le nom d'états *clusters* (MBQC - *Measurement Based Quantum Computing*) a également été proposée [51] et fait actuellement l'objet d'intenses recherches expérimentales [52, 53, 54, 55, 56].

- **Les systèmes physiques exposés à la résonance magnétique (Figure 1.2c)** - Les qubits correspondent aux états de spin d'un noyau particulier à l'interieur d'une molécule ou d'un cristal, les opérations étant effectuées à l'aide d'impulsions radiofréquences [57, 58, 59]. Cette approche reste cependant limitée de part le faible rapport signal sur bruit intrinsèque à ce type de systèmes [60].

- **Les systèmes supraconducteurs (Figure 1.2d)** - On utilise la charge d'une petite région appelée "boîte" d'un matériau supraconducteur, plus couramment nommé 'transmon', pour stocker l'information quantique. La boîte est connectée à un réservoir de charges via une jonction Josephson. La charge est contrôlée par la tension à travers la jonction et les états 0 et 1 correspondent à des charges différant par une paire de Cooper avec $\Delta q = -2e$. Des boîtes adjacentes sont couplées électrostatiquement via leur répulsion coulombienne mutuelle, et les opérations effectuées par les portes logiques le sont via des séquences d'impul-

sions électriques. Des compagnies telles que Google [61], IBM [62] et Intel [63] investissent massivement sur cette technologie. Des résultats avec neuf qubits entièrement contrôlables à l'échelle 1D [64] et jusqu'à cinq dans une architecture 2D [62] ont jusqu'à maintenant été démontrés.

- **Les systèmes physiques liés à l'électrodynamique quantique en cavité** - Les qubits correspondent aux états de polarisation circulaire opposée de deux photons interagissant avec un atome dans une cavité résonante. Les photons interagissent l'un avec l'autre via leur couplage avec l'atome qui est fortement accrue par la cavité résonante [65, 66, 67].

- **Les points quantiques** - Les qubits consistent en excitons confinés dans un point quantique. Les excitons se comportent comme des atomes à deux niveaux, et les opérations sont effectuées à l'aide d'impulsions optiques résonantes. À l'intérieur d'une boite quantique, différents types d'excitons interagissent via l'interaction coulombienne [68, 69, 70, 71, 72].

Les opérations effectuées par un ordinateur quantique reposent sur la manipulation précise et le contrôle cohérent d'états quantiques de systèmes quantiques individuels. Notamment, il est requis que les qubits interagissent uniquement les uns avec les autres et ce, d'une manière contrôlée. Malheureusement, ce scénario idéal est difficile à réaliser en pratique, tous les systèmes quantiques étant fragilisés de part leur couplage à leur environnement. Il convient donc de quantifier la fragilité des qubits vis à vis du bruit généré par l'environnement en terme de taux de décohérence. Heureusement, la situation n'est pas aussi mauvaise qu'elle n'y parait. Dans le traitement des données classiques, des protocoles de vérification systématique des chaînes de bits sont utilisés à tout moment pour corriger les erreurs. De manière analogue, il est possible d'appliquer des codes correcteurs quantiques sur les qubits. Le principe de base est essentiellement le même que pour les correcteurs classiques d'erreurs, l'idée est d'utiliser des qubits supplémentaires pour vérifier la fidélité des données et ensuite appliquer les corrections adéquates afin de reconstruire les états d'origine [73, 74, 75, 76, 77]. De cette manière, nous pouvons réaliser des calculs quantiques tolérants aux fautes [78, 79, 80, 64, 81], le prix à payer se situe alors au niveau de la vitesse de traitement. De manière générale, le physicien David P. DiVincenzo proposa en l'an 2000, dans un papier intitulé "*l'implémentation physique du calcul quantique*", un ensemble de critères [82], parfois nommés commandements de DiVicenzo, qu'il est nécessaire de satisfaire en vue de construire un ordinateur quantique :

1. Posséder un système physique évolutif avec des qubits bien définis ;
2. Être capable d'initialiser le système dans un état fondamental de référence simple ;
3. Savoir générer des qubits avec des temps de décohérence beaucoup plus long que

les temps de fonctionnement des algorithmes à implémenter ;

4. Avoir un ensemble universel de portes quantiques ;
5. Permettre la projection rapide d'un état quantique spécifique ;

Ces cinq règles sont devenues un guide pour le développement du calcul quantique au cours de ces dernières années.

1.1.2. La simulation quantique

Figure 1.3. – Exemple de planétaire. Toutes les planètes sont parfaitement visibles, même si elles ne sont pas reproduites à l'échelle réelle de leur taille et des distances qui les séparent. Observatoire Richard Miller.

Les simulateurs et les ordinateurs sont des dispositifs physiques qui révèlent des informations sur une fonction mathématique. Que nous appelions un dispositif un simulateur ou un ordinateur dépend non seulement du dispositif, mais aussi de ce que l'on suppose de la fonction mathématique et de l'utilisation prévue de l'information obtenue. Ainsi, le terme d'ordinateur est plus souvent utilisé pour décrire des calculs liés à des fonctions mathématiques plus abstraites, non liées à un système physique et utilisées en dehors de la méthode scientifique, tandis que le terme de simulateur fait référence à des fonctions que l'on peut interpréter comme faisant partie d'un modèle physique, faisant ainsi de la simulation une composante à part entière de la méthode scientifique. Ce contexte explique pourquoi certains affirment que la simulation est l'utilisation d'un dispositif physique pour nous parler d'un autre système physique. En conséquence, la simulation a longtemps été au cœur de la science. Par exemple, des

planétaires ont été utilisés pendant des millénaires pour simuler des modèles de mouvements d'objets célestes, voir FIGURE 1.3. Plus récemment, des analyseurs différentiels ou des intégrateurs mécaniques ont été développés pour résoudre des modélisations d'équations différentielles, comme par exemple dans le cas des flux de chaleur [83] ou des lignes de transmission [84]. Malheureusement, ces développements ne sont pas toujours simples et il existe de nombreuses questions importantes auxquelles des simulations fourniraient des réponses mais où les difficultés de mise en œuvre dépassent les capacités technologiques actuelles. Les outils numériques classiques habituellement utilisés, qui ont tous leurs limites, comprennent les calculs exacts, le champ moyen et la théorie du champ moyen dynamique, la théorie des réseaux de tenseurs, la théorie de la fonctionnelle de la densité, ou les algorithmes de Monte Carlo.

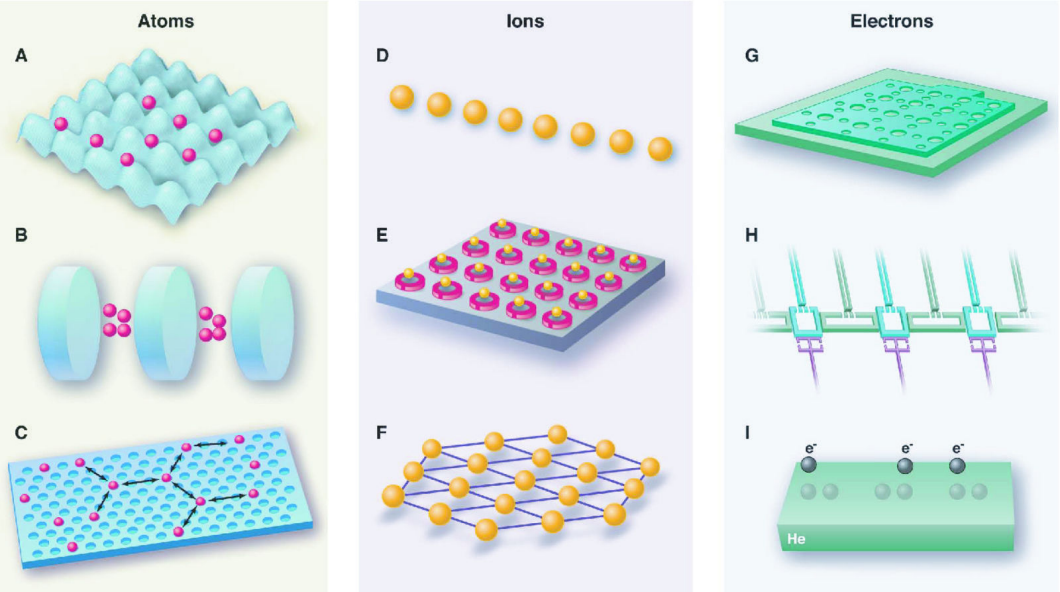


Figure 1.4. – Des structures quantiques à une ou deux dimensions peuvent être utilisées pour simuler divers modèles en physique de la matière condensée. Des exemples de tels simulateurs quantiques analogiques incluent les éléments suivants : **Les atomes** dans des réseaux optiques (A), les réseaux de cavités unidimensionnels (B) ou bidimensionnels (C) ; **Les ions** dans des chaînes linéaires (D), les réseaux bidimensionnels de pièges planaires (E), ou les cristaux de Coulomb bidimensionnels (F) ; **Les electrons** dans des tableaux de points quantiques créés par une maille (G), dans des réseaux de circuits supraconducteurs (H) ou piégés sur une surface d'hélium liquide (I).

Alors que l'idée de simulations est vieille de plusieurs siècles, la suggestion selon laquelle un dispositif quantique permettrait de mieux "imiter" certains modèles qu'un dispositif classique est généralement attribuée à Feynman [23]. Malgré le fort impact

de cette publication, Richard Feynman ne fut pas très précis sur la façon dont un ordinateur quantique devait fonctionner ou comment la simulation elle-même serait réalisée. Plus d'une décennie plus tard, Seth Lloyd a montré qu'un ordinateur quantique peut effectivement agir comme un simulateur quantique universel [85]. En principe tout système physique qui peut être utilisé comme ordinateur quantique serait également un simulateur quantique universel. La réciproque n'étant pas exacte, l'obtention d'un simulateur quantique universel devrait avoir lieu avant la réalisation d'un ordinateur quantique universel. Parmi les tentatives de réalisations expérimentales, on retrouve ainsi les mêmes systèmes que dans la section précédente à savoir les ions piégés, la résonance magnétique nucléaire solide et liquide, les photons, les points quantiques, les circuits supraconducteurs, ou encore les centres NV (*Nitrogen-Vacancy*, défauts ponctuels dans le diamant), les atomes froids et les superfluides atomiques, qui permettent de simuler une large variété de systèmes tels que :

- **Physique de la matière condensée** - La difficulté que représente la résolution de problèmes quantiques à N-corps [86] se reflète dans les questions encore laissées ouvertes de la physique de la matière condensée qui représente le plus vaste domaine d'application des simulateurs quantiques, voir FIGURE 1.4. Parmi les défis les plus connus dans ce domaine, on peut citer la supraconductivité à haute température [87, 88, 89, 90, 91], les systèmes frustrés [92, 93, 94] (cas où l'ordre local ne peut pas se propager librement dans tout l'espace), ou encore les systèmes désordonnés [95].

- **Physique des hautes énergies** - Une méthode pour simuler l'équation de Dirac en utilisant un ion piégé unique a été proposée [96]. Cette dernière offre la possibilité d'étudier l'effet Zitterbewegung [97] (phénomène physique de micro-oscillations d'un soliton, découvert par Erwin Schrödinger, censé expliquer le spin et le moment magnétique de l'électron) qui n'a encore jamais été observé dans sa forme orginelle, et le paradoxe de Klein qui en découle [98]. Le développement de théories de jauges présente également une grande complexité calculatoire qui peut être solutionnée par des simulateurs quantiques [99, 100, 101, 102].

- **Cosmologie** - La propagation d'ondes acoustiques dans un condensat de Bose-Einstein pour étudier les champs scalaires dans la structure spatio-temporelle courbée d'un univers en expansion [103], la simulation de la création de particules cosmologiques avec des ions piégés [104], ou encore l'utilisation d'hélium superfluide [105] ont été proposées comme simulateurs quantiques pour reproduire des observations cosmologiques en laboratoire. Avec les modèles analogiques il est également possible de tester des phénomènes prédits qui n'ont pas encore été observés par les cosmologistes, tel que l'effet Unruh (l'observation par un observateur accéléré d'un flux thermique de particules dans le vide) en utilisant l'excitation de phonons avec des ions piégés [106], l'effet Schwinger (la production

de paires électron-positron à partir du vide sous l'action d'un champ électrique fort) avec des atomes dans un réseau optique [107, 108], ou les radiations de Hawking ("l'évaporation des trous noirs" par annihilation de paires particule anti-particule) avec des atomes [109], des ions [110], des circuits supraconducteurs [111], ou même des impulsions de lumière ultra-courtes dans des fibres optiques micro-structurées [112].

- **Physique atomique** - Il existe une analogie profonde entre les atomes naturels et les atomes artificiels formés, par exemple, par des électrons dans de petits circuits supraconducteurs [113]. Les deux ont des niveaux d'énergie discrets et présentent, sans excitations contrôlées, des oscillations quantiques cohérentes entre ces niveaux. Les champs électriques et magnétiques qui résultent de l'application de tensions et de courant dans les atomes artificiels contrôlent l'effet tunnel des électrons à travers les jonctions Josephson. Les effets de ces champs sur les circuits sont les analogues des effets Stark et Zeeman dans les atomes. Contrairement aux atomes naturels, les atomes artificiels peuvent être conçus par lithographie pour avoir des caractéristiques spécifiques, comme un grand moment dipolaire ou des fréquences de transition particulières. Cette flexibilité est un avantage important par rapport aux atomes naturels.

- **Physique nucléaire** - En physique nucléaire, il faut résoudre des problèmes quantiques à N-corps [86]. Même si N n'est pas aussi large qu'en physique de la matière condensée, le calcul des forces nucléaires est difficile et, par conséquent, les simulations de physique nucléaire nécessitent une puissance de calcul importante. Plusieurs modèles phénoménologiques ont été développés, dont l'un est le modèle superfluide du noyau atomique. Ce modèle pourrait être simulé à l'aide d'un système contrôlable analogique, comme par exemple un gaz superfluide d'atomes fermioniques [114].

- **Interférométrie optique** - L'interféromètrie non linéaire, et plus récemment les interféromètres de Mach-Zehnder ou encore le *boson-sampling* ont entre autres été simulés dans des expériences d'ions piégés [115, 116, 117] et des circuits supraconducteurs [113].

Le lecteur intéressé pourra trouver plus de détails sur ces applications en référence [6].

1.1.3. La métrologie quantique

Dès les premières civilisations, il a été nécessaire d'effectuer des mesures (poids, longueurs), pour les échanges entre tiers. Pour éviter les contestations entre parties prenantes, sont très rapidement apparues des mesures de référence que nous appelons aujourd'hui étalons. Jusqu'au XVIIIe siècle, les grandeurs sont souvent évaluées en com-

paraison avec des références humaines, comme le pied ou le pouce pour les longueurs (souvent les organes des rois et empereurs), voir FIGURE 1.5, ou encore le journal pour la surface (grandeur d'un champ correspondant à la quantité de travail - moissonnage par exemple - que peut fournir une personne en une journée). Chaque pays, chaque province même, dispose de ses propres unités de mesure ; ainsi l'on dénombre plus de quatre-vingt mesures agraires employées au Moyen Âge. Ceci complique les échanges commerciaux et gêne la diffusion des connaissances. Les scientifiques français, inspirés par l'esprit des Lumières et la Révolution française, conçoivent alors un système de référence basé sur des références naturelles ayant la même valeur pour tous, sans rapport à une personne particulière, autrement dit un système universel. C'est ainsi que l'on prend la longueur du méridien terrestre comme référence de longueur pour bâtir le mètre. Au XXe siècle, la métrologie a su évoluer dans tous les domaines la concernant, notamment dans le changement de certaines définitions d'unités de base (longueur, temps, masse) ; elle a aussi favorisé les démarches normalisées pour étalonner les instruments de mesure. Au cours des dernières décennies elle a enfin proposé que la variabilité des valeurs mesurées soit considérée comme une dispersion et que cette incertitude métrologique soit traitée par des méthodes statistiques reconnues.

Figure 1.5. – Détermination d'un "pied étalon". Francfort, ca. 1575.

Tout procédé de mesure peut être divisé en trois étapes distinctes : la préparation d'une sonde, son interaction avec le système à mesurer et la lecture du résultat. Un tel procédé est généralement accompagné d'erreurs statistiques ou d'erreurs systématiques. Les sources d'erreurs statistiques peuvent être accidentelles, comme dans le cas d'un contrôle insuffisant de la sonde et du système que l'on cherche à mesurer, ou fondamentales comme nous allons le détailler. Quel que soit l'origine de ces erreurs statistiques, ces dernières peuvent être réduites en répétant la mesure et en moyennant les résultats. Ceci est en métrologie classique la conséquence du théorème de la limite cen-

trale qui établit que la moyenne des résultats obtenue sur un ensemble large de n mesures indépendantes, chacune ayant une déviation standard $\Delta\sigma$, converge vers une distribution gaussienne avec une distribution standard $\Delta\sigma/\sqrt{n}$, ce qui correspond par conséquent à une erreur en $n^{-1/2}$, voir section 2.4.5. On associe une erreur statistique en $n^{-1/2}$ à ce qu'il est coutume de nommer la limite quantique standard, ou *shot-noise* en optique quantique. Autrement dit, la présence d'une erreur statistique en $n^{-1/2}$ suppose que le procédé de mesure s'est effectué en présence de corrélations statistiques classiques entre les différentes sondes, qui ne sont généralement pas corrélées. On peut voir ici une analogie avec le procédé d'encodage de données en informatique conventionnelle où l'on avait vu que bien que le système permettant l'encodage et le système sur lequel on venait encoder étaient tous deux des systèmes quantiques, l'encodage en lui même restait quant à lui classique limitant ainsi la puissance de calcul. En métrologie, c'est l'absence de corrélations entre les différentes sondes qui empêche de descendre en dessous de la limite quantique standard, on échoue par conséquent une nouvelle fois à exploiter la nature quantique des sondes et du système étudié [8].

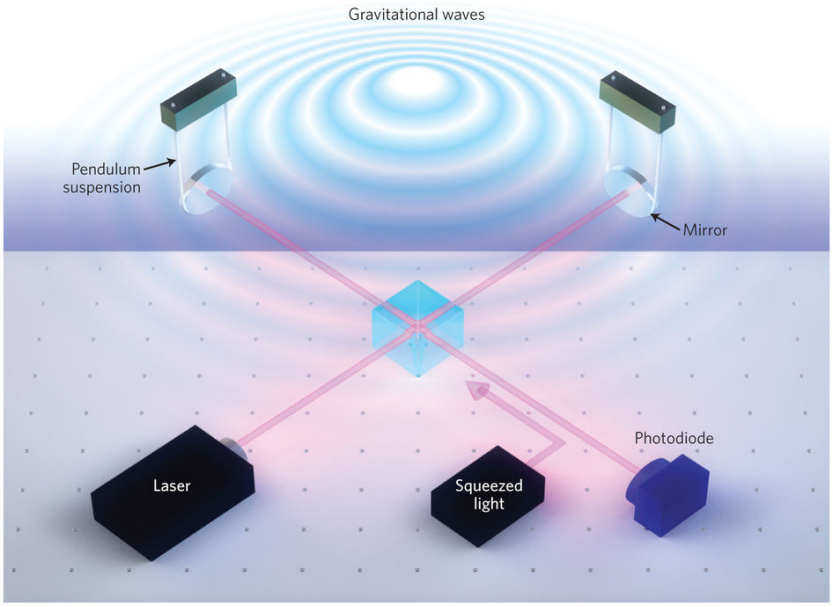


Figure 1.6. – Le Laser Interferometer Gravitational-Wave Observatory (Observatoire d'ondes gravitationnelles par interférométrie laser), en abrégé LIGO, est un interféromètre de Michelson à grande échelle dont le but est de détecter des ondes gravitationnelles. La sensibilité de l'interféromètre est rendue meilleure via l'injection de lumière dite comprimée, U. L. Andersen, Université Technique du Danemark [118].

Pour dépasser la limite quantique standard, on utilise en métrologie quantique des états non classiques tels que des états intriqués ou des états comprimés (nous reviendrons sur leurs définitions un peu plus tard au sein de ce manuscrit lorsque nous

traiterons de la quantification du champ électromagnétique au chapitre 2) afin de placer les sondes dans des états corrélés avant de les laisser interagir avec le système étudié. Pour un ensemble de N sondes corrélées, on obtient alors une erreur statistique en $1/(N\sqrt{n})$. Cependant la physique quantique impose toujours une limite ultime, connue sous le nom de limite de Heisenberg, qui ne permet pas de descendre en dessous d'une erreur statistique en n^{-1}. La métrologie quantique a donc pour but d'étudier cette limite et les stratégies quantiques qui permettent de l'atteindre. Parmi les exemples notables d'applications [7] on peut citer :

- **Ensembles atomiques** - Les horloges, les gyromètres, les magnétomètres, les électromètres et les gravimètres atomiques sont soumis au bruit de projection quantique qui constitue une limite fondamentale de tous les interféromètres atomiques étant donné le nombre fini d'atomes participant à l'expérience. Par ailleurs, des états intriqués à N atomes, dont le spin total est comprimé, peuvent permettre d'améliorer la sensibilité. Des premières expériences, qui utilisent les interactions entre atomes pour introduire de l'intrication, ont mis en évidence ce phénomène. On peut à ce titre citer deux récentes réalisations qui ont permis d'obtenir de l'intrication entre respectivement 3 000 et 500 000 atomes de rubidium 87 [119, 120]. De la lumière comprimée a aussi été utilisée dans des expériences de refroidissement d'atomes par laser afin d'abaisser la température au delà du minimum atteignable de manière conventionnelle [121], et des atomes de Rydberg ont également permis d'approcher la limite de Heisenberg lors de la mesure de champs électriques [122].

- **Interféromètres optiques** - L'utilisation d'états intriqués de type N00N (états obtenus en envoyant N photons indiscernables sur une lame séparatrice équilibrée) dans un interféromètre de Mach-Zehnder permet d'obtenir une précision sur le déphasage présent entre les deux bras de l'interféromètre dépassant la limite quantique standard [123, 124, 125, 126, 127, 128], voir calculs en section 2.4.5. On peut également citer l'utilisation d'états comprimés, voir 2.3.3, pour améliorer la sensitivité à la phase ou à l'amplitude. Il est notamment question dans les futures phases de développement des projets LIGO (Figure 1.6), VIRGO et GEO600, d'injecter de la lumière comprimée afin de permettre la détection d'ondes gravitationnelles [129] avec une sensibilité allant au delà du *shot-noise* pour ces trois interféromètres de Michelson géants [118, 130].

1.1.4. La cryptographie quantique

Avec le développement des emails et des applications de messagerie mobile, la demande du grand public pour des moyens de communication cryptés ne cesse de croître. Aussi, dans le contexte terroriste actuel, la cryptologie est devenue l'enjeu d'un bras de fer entre objectifs sécuritaires et protection de la vie privée. Le chiffrement des

données de communication, comme on l'appelle également, est un levier majeur de la confiance dans le numérique, un rempart contre l'espionnage et les cyberattaques. En effet, il se cache derrière des opérations aussi diverses que les transferts monétaires, la constitution de mots de passe, les dispositifs anti-piratage, la consultation de résultats médicaux en ligne, etc. C'est un élément crucial de notre sécurité en ligne et de la confidentialité sur Internet. Malheureusement, la sécurité de la cryptographie conventionnelle repose souvent sur de simples hypothèses de calcul. Par exemple, la sécurité du système RSA [21] - le système de cryptage à clé publique le plus répandu - est basée sur la difficulté présumée que représente la décomposition d'un grand nombre en ses facteurs premiers. Or nous l'avons vu, un processeur quantique pourrait permettre via l'algorithme de Shor [27] de factoriser des grands nombres en un temps polynomial à la taille de ces derniers, rendant ainsi la cryptographie conventionnelle vulnérable aux progrès technologiques. Sans même anticiper sur l'avènement de l'informatique quantique, un espion, que l'on appellera Eve, pourrait aussi simplement sauvegarder des communications cryptées datant de 2017 et attendre le développement d'un processeur classique contenant suffisamment de transistors pour permettre dans le futur de décrypter le message en un temps raisonnable, ce qui mettrait à mal la pérennité des données confidentielles du passé.

La physique quantique peut permettre de rendre obsolètes les techniques de cryptographie actuelles, mais elle peut également permettre de les dépasser. L'établissement quantique de clés secrètes (*Quantum Key distribution* - QKD), l'application la plus connue de la cryptographie quantique, promet d'atteindre le Saint Graal de la cryptographie, à savoir l'établissement de communication avec un niveau de sécurité inconditionnelle. On parle de sécurité inconditionnelle lorsque Eve n'est pas limitée par des hypothèses de calcul, mais seulement par les lois de la physique. La cryptographie quantique s'appuie sur le principe d'incertitude de Heisenberg formulé en 1927 [131] et le théorème de non-clonage décrit par Wootters et Zurek en 1982 [132]. Werner Heisenberg a formalisé l'un des principes fondamentaux de la physique quantique : "À l'instant où la position de l'électron est connue, sa dynamique ne peut être connue que jusqu'à des grandeurs qui correspondent à ce changement discontinu ; ainsi, plus la position est déterminée de manière précise, moins le moment est connu, et inversement". Par conséquent, nous ne pouvons pas mesurer les caractéristiques d'un système quantique sans l'altérer et nous ne pouvons pas avoir accès à toutes les propriétés d'un système quantique avant que ces propriétés ne soient mesurées. Le théorème de non-clonage démontre quant à lui qu'il est impossible de créer une copie parfaite d'un état quantique inconnu et arbitraire. L'impossibilité d'établir une copie parfaite oblige ainsi un espion à effectuer une mesure sur le système original. Or, lorsque la base choisie pour cette mesure ne correspond pas à celle utilisée pour préparer l'état, ce qui statistiquement arrive dans au moins 50% des cas puisque la QKD repose, pour les protocoles les plus simples, sur l'usage de manière aléatoire de deux bases incompatibles pour la préparation et l'analyse, cela laisse alors une signature rendant l'espion détectable. La

QKD est donc une solution remarquable pour répondre aux enjeux de sécurité sur le long terme puisque, en principe, elle offre une sécurité non péremptoire dans le temps.

Message originel m	Clé k	Message chiffré $m \oplus k$	Message déchiffré $(m \oplus k) \oplus k$
0	0	0	0
0	1	1	0
1	0	1	1
1	1	0	1

Table 1.1. – L'algorithme de chiffrement de Vernam repose sur l'opération la plus simple existante, une porte logique XOR ("ou exclusif", symbolisée mathématiquement par un $\oplus$). Le message original m est chiffré par une clé k via l'operation $m \oplus k$ et est envoyé via un canal public à un interlocuteur authentifié. Le message est décrypté en appliquant une nouvelle fois une porte logique XOR sur le message crypté, $(m \oplus k) \oplus k = m$. Bien qu'extrêmement simple à implémenter, ce protocole garantit un chiffrement avec une sécurité inconditionnelle à condition d'utiliser une nouvelle clé de même longueur que le message pour chaque nouveau message et que la clé soit connue uniquement par les deux utilisateurs authentifiés comme le permet la distribution quantique de clés secrètes.

Une fois la clé établie entre deux partenaires distants ayant pu s'assurer de la non-présence d'un espion sur la ligne, cette clé secrète peut ensuite être utilisée dans un algorithme classique de chiffrement symétrique, afin de chiffrer et déchiffrer des données confidentielles. Pour assurer une confidentialité maximale aux deux interlocuteurs, il faut que le niveau de sécurité de l'algorithme de chiffrement classique soit lui même, aussi élevé que le niveau de sécurité lors de l'établissement quantique de la clé, à savoir une sécurité inconditionnelle. Or, la sécurité de la majorité des algorithmes de chiffrement symétrique repose, comme les protocoles classiques de distribution de clés secrètes, sur des considérations calculatoires et non sur une sécurité inconditionnelle. Cependant, Claude Shanon en 1948 [11] a montré qu'il était malgré tout possible de démontrer formellement un niveau de sécurité inconditionnelle pour un algorithme de chiffrement en particulier, le codage à masque jetable, également nommé chiffrement de Vernam, voir Table 1.1. En combinant cet algorithme qui est le seul à présenter un tel niveau de sécurité avec les techniques de cryptographie quantique, il est ainsi possible de démontrer la sécurité globale de la transmission d'un message confidentiel.

Les réalisations expérimentales de dispositifs de QKD ont beaucoup progressé au cours des deux dernières décennies. Elles reposent sur la transmission de photons uniques ou de paires de photons intriqués, voir annexe A pour plus de détails. Dans la pratique, la transmission du signal peut se faire par espace libre (en utilisant des photons à une lon-

gueur d'onde d'environ 800 nm) ou par des fibres optiques (en utilisant la deuxième ou la troisième fenêtre des télécommunications optiques, c'est-à-dire des longueurs d'onde d'environ 1310 nm et 1550 nm, respectivement). Les configurations actuelles utilisent différents degrés de liberté pour coder les informations pertinentes dans les impulsions optiques. Un choix évident est d'utiliser l'état de polarisation des photons. Cette technique, connue sous le nom de codage en polarisation, est surtout utilisée dans les liens de QKD en espace libre. Cependant, la polarisation étant sujette aux perturbations résultant de la biréfringence dans les fibres, on choisit généralement pour les transmissions par fibre optique d'autres options de codage, par exemple, le codage via la phase, le codage en time-bin, le codage en énergie-temps, ou encore le codage en fréquence.

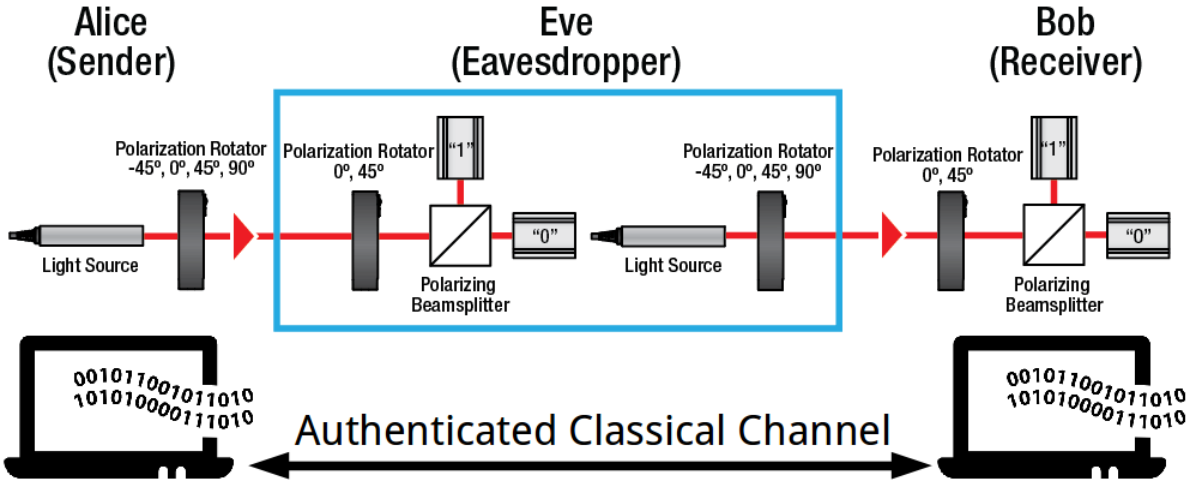


Figure 1.7. – Exemple d'implémentation d'un protocole d'établissement de clés secrètes entre deux protagonistes, Alice et Bob, en la présence d'un éventuel espion, Eve. L'observable choisie est la polarisation, la préparation s'effectue via un premier polariseur idéalement piloté par un générateur quantique de nombres aléatoires (QRNG), l'analyse s'effectue à l'aide d'un second polariseur, lui aussi idéalement piloté par un QRNG, suivi d'un séparateur de faisceau sensible à la polarisation pour lequel on a placé un détecteur sur chaque voie de sortie. Alice et Bob suivent ensuite diverses étapes de post-traitement de leurs données brutes en utilisant un canal de communication classique authentifié. Le protocole est décrit dans son intégralité au sein de l'annexe A.

Une fois le protocole, l'observable et le support de propagation choisi, on retrouve en général dans toute implémentation, comme illustré FIGURE 1.7, les éléments suivants :

- **Sources lumineuses** - Des sources lasers atténuées peuvent être utilisées en QKD pour simuler des sources de photons uniques idéales que l'on ne sait pas encore produire à ce jour à haut taux de répétition. En appliquant une phase globale aléatoire, il est possible de transformer l'état du signal lumineux en une

mixture classique d'états de Fock (états à nombre de photons déterminé) avec une distribution poissonienne.

- **Composants d'optiques linéaires standards** - Contrôleurs de polarisation, coupleurs directionnels, modulateurs de phase, modulateurs d'amplitude, etc, sont largement utilisés dans l'implémentation des protocoles de QKD.

- **Détecteurs de photons uniques** - La détection de photons uniques est la limite ultime de détection de lumière. Elle est importante non seulement dans les applications de type QKD, mais aussi dans toutes les expériences d'optique quantique reposant sur des observables discrètes. Traditionnellement, deux types de détecteurs semi-conducteurs sont utilisés : les détecteurs à base de silicium (Si), et les détecteurs de type indium gallium arsenide (InGaAs). Ces détecteurs reposent tous sur le phénomène d'avalanche électronique. Les détecteurs Si sont en général utilisés pour les longueurs d'ondes visibles (par exemple, 800 nm) et ont des efficacités de détection assez élevées d'environ 50%. Les détecteurs InGaAs sont quant à eux d'avantage utilisés en la présence de photons dans la plage des longueurs d'ondes des télécommunications, ils présentent des efficacités de détection de l'ordre de 20% et possèdent des temps de relaxation relativement longs limitant le taux de détection à seulement quelques centaines de kHz. Au cours des dernières années, cependant, de nouveaux circuits électroniques de gestion de la détection ont été développés pour les applications de type QKD afin de rendre ces détecteurs plus efficaces et plus rapides. On trouve notamment l'auto-différentiation (*self-differencing*) [133, 134], la synchronisation sinusoïdale (*sine-wave gating*) [135, 136, 137], ainsi qu'une approche hybride qui combine ces deux méthodes [138]. Enfin des détecteurs supra-conducteurs (SNSPD) ont été développés et ont révolutionnés le domaine [139]. En effet, ceux-ci permettent d'atteindre des standards allant, selon les dispositifs, de 50 à 90% d'efficacité [139, 140, 141], combinés à des temps de relaxation très courts. Pour plus de détails sur le fonctionnement des détecteurs de photons uniques, le lecteur pourra se référer à l'annexe C.

- **Générateurs de nombres aléatoires** - Les bits aléatoires sont nécessaires pour déterminer la séquence de bits à transmettre ainsi que pour choisir les bases lors des étapes d'encodage et d'analyse des clés secrètes. En informatique classique des nombres pseudo-aléatoires sont souvent utilisés et sont suffisants pour de nombreuses applications. Cependant ils ne peuvent pas en cryptographie être substitués à de vrais nombres aléatoires puisqu'il est toujours possible de remonter à une séquence produite de manière déterministe via sa redondance. Pour garantir un vrai aléa, il est possible de s'appuyer sur des processus physiques stochastiques. Les processus les plus fiables sont les processus quantiques, car la physique quantique est fondamentalement aléatoire [142].

Des réalisations s'appuyant sur l'envoi de photons sur une lame séparatrice équilibrée [143, 144, 145], sur les temps d'arrivées de photons [146, 147, 148], sur le comptage de photons [149, 150], sur la diffusion Raman spontanée [151, 152], sur le bruit de phase des lasers [153, 154, 155, 156, 157], sur l'émission spontanée amplifiée [158, 159, 160, 161, 162] ou encore sur l'exploitation des fluctuations quantiques du vide [163, 164, 165, 166] ont été démontrées avec des taux de génération allant jusqu'à plusieurs dizaines de GHz. Des nombres aléatoires ont même été extraits en utilisant la caméra d'un smartphone [167], tandis que certains générateurs sont déjà commercialisés [12, 13, 14, 15, 17].

- **Techniques de post-traitement classique** - Chaque transmission quantique est ensuite suivi d'une phase de post-traitement classique au cours de laquelle les partenaires du lien communiquent au travers d'un canal public authentifié. Le post-traitement se décompose en différentes étapes répondant chacune à une problématique [168], voir l'annexe A pour plus de détails.

- **Canal de communication classique authentifié** - Pour qu'un dispositif de QKD fonctionne, Alice et Bob doivent également partager un canal classique authentifié en plus du canal quantique afin de procéder aux étapes de post-traitement. Cela nécessite qu'une clé d'authentification, assez courte en général, soit initialement partagée entre Alice et Bob. Cette clé d'authentification peut être fournie lors de l'installation initiale du système de QKD dans un dispositif anti-intrusions. Une fois la distribution quantique de clés secrètes initiée, une nouvelle clé d'authentification peut être établie à partir de la clé générée par QKD.

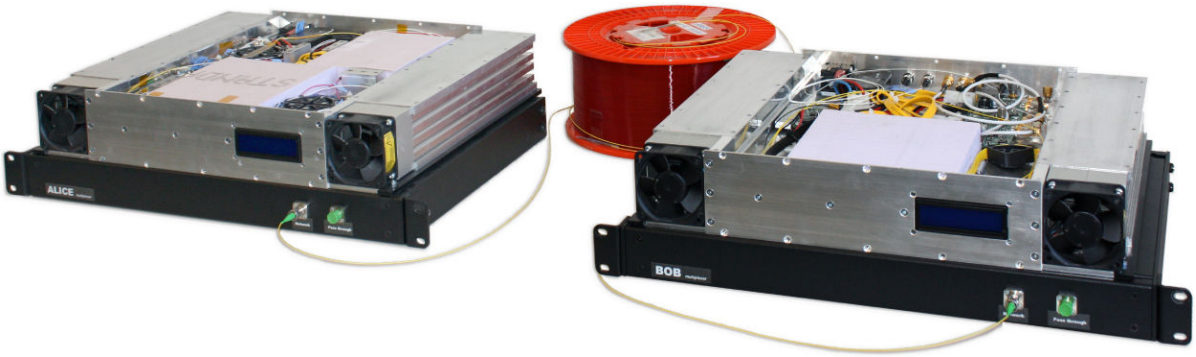


Figure 1.8. – **(a)** Un système de QKD compact et autonome capable d'établir des clés secrètes sur 307 km de fibre optique grâce au protocole Coherent One Way (COW) [169]. Voir annexe A pour une présentation du protocole.

En 2002, le record de distance pour la transmission quantique de clés secrètes sans

avoir recours à la distribution d'états intriqués était de 67 kilomètres, entre Genève et Lausanne [170]. Suite à plusieurs évolutions technologiques, ce record est passé en 2014 à 307 kilomètres, preuve de la croissance très rapide de ce champ d'application [169], voir FIGURE 1.8.

Outre l'établissement quantique de clé secrète, de nombreuses autres applications de la cryptographie quantique peuvent être citées, telles que : le calcul distribué sécurisé quantique (*secure quantum distributed computing*) [171, 172], le pile ou face quantique (*quantum coin flipping*) [173, 174, 175, 176], les preuves à divulgation nulle de connaissance (*quantum zero-knowledge proof*) [177, 178], le transfert quantique inconscient (*quantum oblivious transfer*) [179, 174, 175, 180], ou encore les gages quantiques (*quantum bit-commitment*) [174, 175, 181].

1.2. Internet des objets quantiques

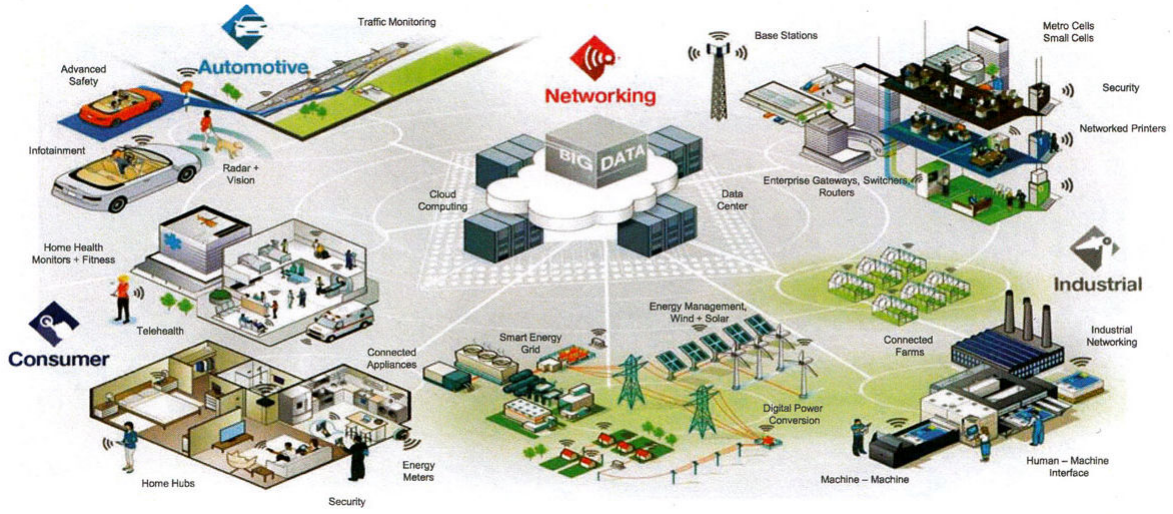


Figure 1.9. – Illustration de l'Internet des objets dans la vie quotidienne.

Internet est devenu en quelques années le vecteur principal de la diffusion de l'information. Il s'est imposé dans de nombreux domaines comme une infrastructure essentielle pour les individus, les entreprises et les institutions. Toutefois, ses capacités d'extension, au-delà des seuls ordinateurs et terminaux mobiles, sont encore considérables car il devrait permettre l'interaction d'un nombre croissant d'objets entre eux ou avec nous-mêmes. Internet se transforme progressivement en un réseau étendu, appelé Internet des objets ou *Internet of things* pour reprendre l'appellation anglaise, reliant plusieurs mil-

liards d'êtres humains mais aussi des dizaines de milliards d'objets [182]. Des domaines encore relativement peu affectés par Internet, comme la santé, l'habitat, l'automobile, ou encore l'assurance, seront bouleversés par cette mutation des réseaux, voir FIGURE 1.9.

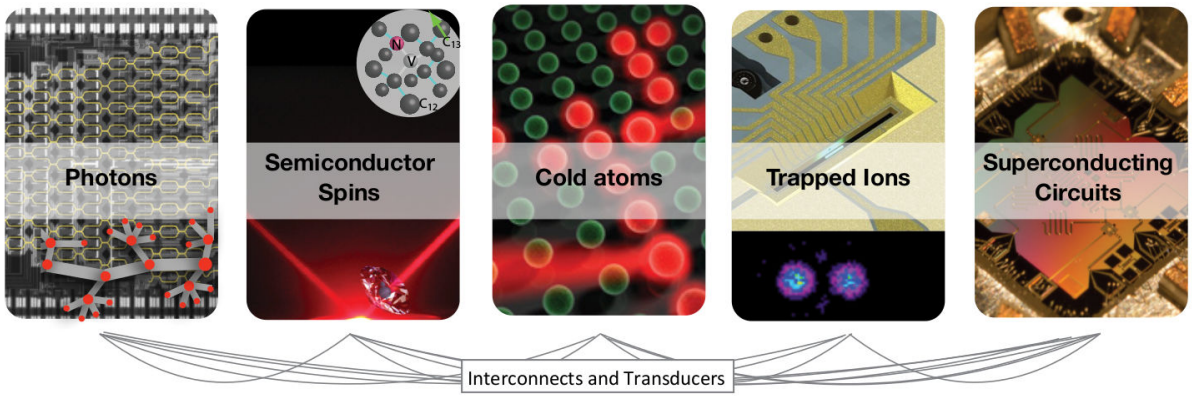


Figure 1.10. – Les plates-formes principales pour le traitement de l'information quantique comprennent les photons, les spins dans les semi-conducteurs, les atomes froids, les ions piégés et les circuits supraconducteurs. Un domaine de recherche majeur consiste à connecter ces différentes plates-formes, ce qui nécessite souvent le développement de transducteurs vers des états photoniques, qui peuvent alors parcourir au travers de fibres optiques ou de liaisons satellites des distances de plusieurs dizaines voir centaines de kilomètres avec peu de décohérence.

Dans la section précédente, nous avons présenté de manière indépendante les unes des autres, les différentes technologies au cœur de la seconde révolution quantique. Tout comme Internet a évolué vers l'Internet des objets, les différentes technologies quantiques seront amenées dans les années futures à être connectées les unes aux autres de sorte à construire un Internet des objets dans une version quantique, voir FIGURE 1.10. Ces futurs développements permettront à des utilisateurs désireux d'avoir accès à des capteurs, simulateurs et processeurs quantiques ou de vouloir tout simplement communiquer entre eux, de pouvoir le faire avec une sécurité inconditionnelle garantie par la cryptographie quantique. Outre les défis propres à chaque technologie, le déploiement d'un Internet des objets quantiques pose à son tour ses propres difficultés. Ces difficultés sont d'ordre topologique lorsqu'il est question de rendre accessible ces technologies au plus grand nombre, d'ordre fondamentale lorsqu'il s'agit d'établir des liens de communication sécurisés sur longue distance, et enfin d'ordre technologiques lorsqu'il est question de synchronisation et d'interfaçage. Dans cette section nous présentons les différents défis à relever et détaillons les solutions associées, à savoir la mise à disposition d'offres de *cloud computing* pour les applications quantiques, le déploiement de relais reposant sur le protocole de téléportation quantique, et enfin le développement de mémoires quantiques et de transducteurs vers des états photoniques.

1.2.1. Service cloud

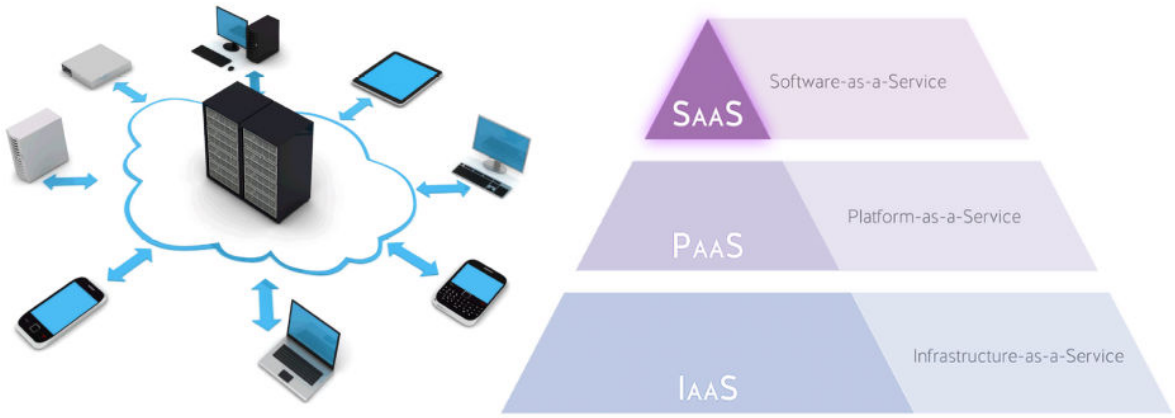


Figure 1.11. – Le terme de "*cloud*" ou "nuage" vient de la représentation métaphorique de ces services. Ces derniers sont présents sur les serveurs et non sur le disque dur du moyen technique de l'utilisateur. Celui-ci accède alors grâce à Internet au service en ligne, sans avoir besoin de stocker des données sur son appareil, qu'il s'agisse d'un ordinateur, d'une tablette ou même d'un smartphone. La multiplicité des services liés aux usages du *cloud computing* est telle que l'on distingue aujourd'hui trois principaux types de services, le SaaS : "*Software as a Service* ", c'est-à-dire la fourniture de logiciel en ligne ; le PaaS : "*Platform as a Service*", c'est-à-dire la fourniture d'une plateforme de développement d'applications en ligne ; le IaaS : "*Infrastructure as a Service*", c'est-à-dire la fourniture d'infrastructures de calcul et de stockage en ligne.

Le développement de processeurs reposant sur un traitement quantique de l'information est actuellement et sera certainement pour encore de nombreuses années de nature très coûteuse. Cet aspect, entre autres limitations, devrait empêcher dans un futur proche toute commercialisation grand public, du moins tant que cette technologie n'aura pas suffisamment gagné en maturité au point d'être exportable hors laboratoires. La question se pose alors de savoir si l'informatique quantique peut malgré tout être rendue accessible au plus grand nombre ? Afin de répondre à cette problématique, le développement d'architectures de type *cloud computing* avec du hardware non plus classique mais quantique est actuellement envisagée. Selon la définition du National Institute of Standards and Technology (NIST), le *cloud computing* - ou informatique en nuage, voir FIGURE 1.11 - est l'accès via un réseau de télécommunications, à la demande et en libre-service (généralement via Internet), à des ressources informatiques partagées configurables [183]. Né au début des années 2000, le *cloud computing* répond donc à une stratégie de migration de la puissance de traitement de l'ordinateur du client vers des serveurs Internet distants en accès partagé - public, privé ou hybride. Dans le cas d'un *cloud* quantique, cette puissance de traitement serait alors un processeur quantique.

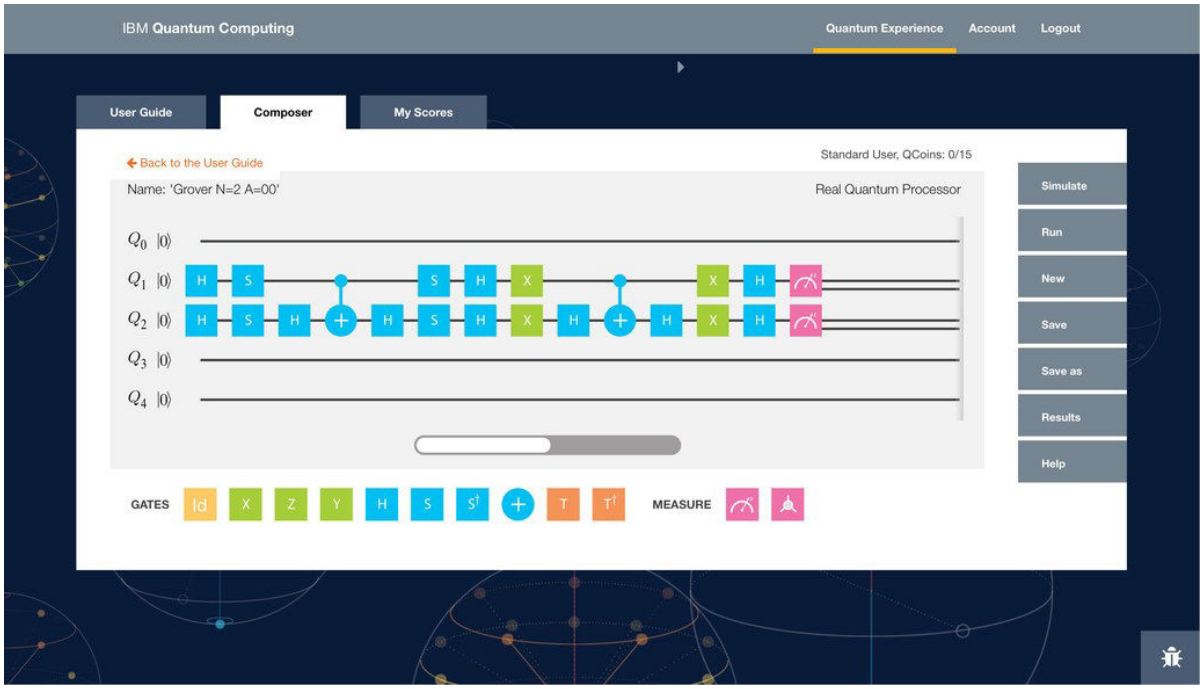


Figure 1.12. – Capture d'écran de la plateforme QX développée par IBM en mai 2016 [62]. Les utilisateurs interagissent avec le processeur quantique en construisant des algorithmes de calcul via une architecture de circuit quantique en appliquant des portes logiques sur les qubits à l'aide d'une interface graphique ou en écrivant le code de l'algorithme via une API Python mise à disposition par IBM en mars 2017 [184].

Le premier laboratoire à avoir développé une plate-forme de *cloud computing* avec du hardware quantique accessible via Internet a été le Centre de Photonique Quantique (CQP) de l'Université de Bristol qui a connecté en 2013 une puce permettant la manipulation à distance de deux qubits optiques au travers d'une porte CNOT [185, 186]. En 2016, IBM a ensuite donné accès à ses qubits supraconducteurs via un service accessible en mode *cloud* nommé *IBM Quantum Experience (QX)* [62], voir FIGURE 1.12. Cette approche est nettement plus avancée car elle permet d'accéder à un dispositif à 5 qubits reprogrammable qui autorise la conception, la simulation, le test et l'exécution réelle d'un algorithme sur un dispositif physique. La plate-forme QX est réservée avant tout aux chercheurs, voire aux développeurs, qui souhaitent s'essayer à cette nouvelle génération de solutions informatiques. IBM mentionne à ce titre qu'il y a eu plus de 40 000 utilisateurs, qui ont collectivement géré plus de 275 000 expériences dont une quinzaine ont pu faire l'objet de publications [187, 188, 189, 190, 191, 192]. On peut également mentionner que des professeurs d'université ont intégré des exemples et des expériences basés sur cette plate-forme dans leurs programmes d'enseignement, ouvrant ainsi la voie à une modernisation des techniques d'enseignement en science de l'informa-

tion quantique [193]. Bien qu'il ne s'agisse toutefois pas encore d'un ordinateur quantique universel capable de s'atteler à toutes les tâches informatiques, rendant la technologie actuelle limitée à des applications bien précises, l'initiative d'IBM marque sans aucun doute une avancée significative.

1.2.2. Accès client longue distance

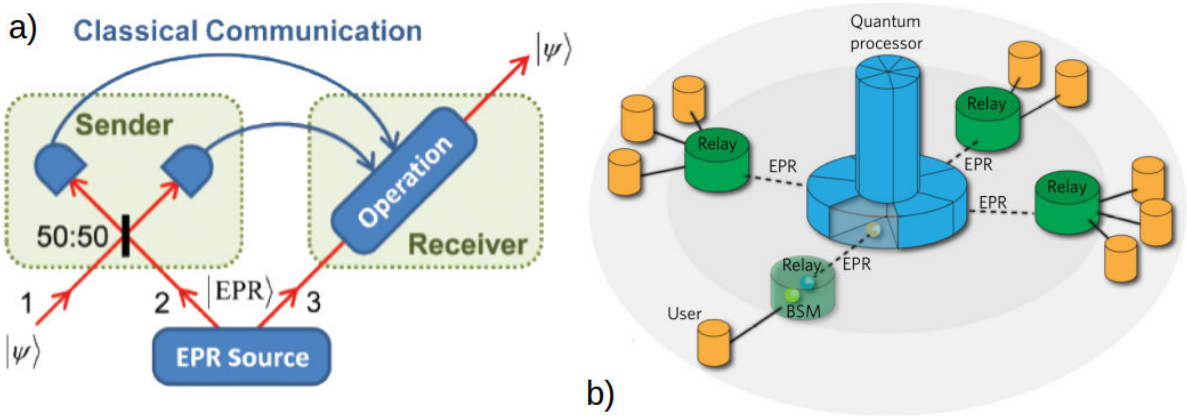


Figure 1.13. – **a)** Téléportation quantique : (1) Un émetteur souhaite transmettre à un receveur l'état inconnu du système 1, pour cela ils se partagent un système intriqué bipartite 2-3 ; (2) L'émetteur réalise une mesure jointe de 1 et 2 qui transforme alors l'état de 3, et transmet le résultat de sa mesure au receveur via un canal de communication classique ; (3) Grâce à cette information, le receveur effectue une opération unitaire sur le système 3 pour le placer dans le même état que le système 1 avant la mesure jointe. **b)** Schéma de principe d'un réseau quantique. Un processeur quantique est rendu accessible à des utilisateurs distants par l'intermédiaire de stations relais permettant d'effectuer des opérations de téléportation quantique.

Les offres de calcul quantique précédemment mentionnées s'appuient actuellement sur un accès via des canaux de communication classique, en l'occurrence Internet. À terme, l'accès à ces services devra lui aussi s'effectuer de manière quantique pour garantir la sécurité du lien d'accès, et ce, quelle que soit la distance séparant la plate-forme de calcul de l'utilisateur. Or, si les fibres optiques de télécommunication et les composants standards qui s'y rattachent représentent des canaux quasi-idéaux pour véhiculer les photons porteurs de l'information quantique, la tâche qui consiste à établir un lien de cryptographie quantique sur grande distance et à haut débit n'est pas simple. En effet, bien que les technologies des télécoms optiques soient mûres et éprouvées, les pertes dans les fibres optiques augmentent de façon exponentielle avec le nombre de kilomètres parcourus par les photons à raison de 0.2 dB de perte au kilomètre pour les fibres standard et de 0.16 dB pour les fibres les plus évoluées. Dans le monde classique ces pertes

ne sont pas un problème puisqu'il est toujours possible de venir amplifier à intervalles réguliers les impulsions lumineuses. En revanche, les opérations d'amplifications sont impossible à effectuer en présence d'états quantiques, ceci est une conséquence immédiate du théorème de non clonage que nous avions mentionné en section 1.1.4. En présence de protocoles de communication quantique reposant sur la manipulation de variables discrètes, l'établissement de lien de cryptographie quantique devient alors impossible lorsque le taux de transmission des photons uniques devient comparable au niveau de bruit des détecteurs au delà d'une certaine distance. Dans le cas de protocoles en variables continues, la sensibilité aux pertes est encore plus critique puisque le bruit au delà du *shot-noise* couramment appelé excès de bruit, qu'il est important de conserver à un niveau mesurable, est directement proportionnel aux pertes.

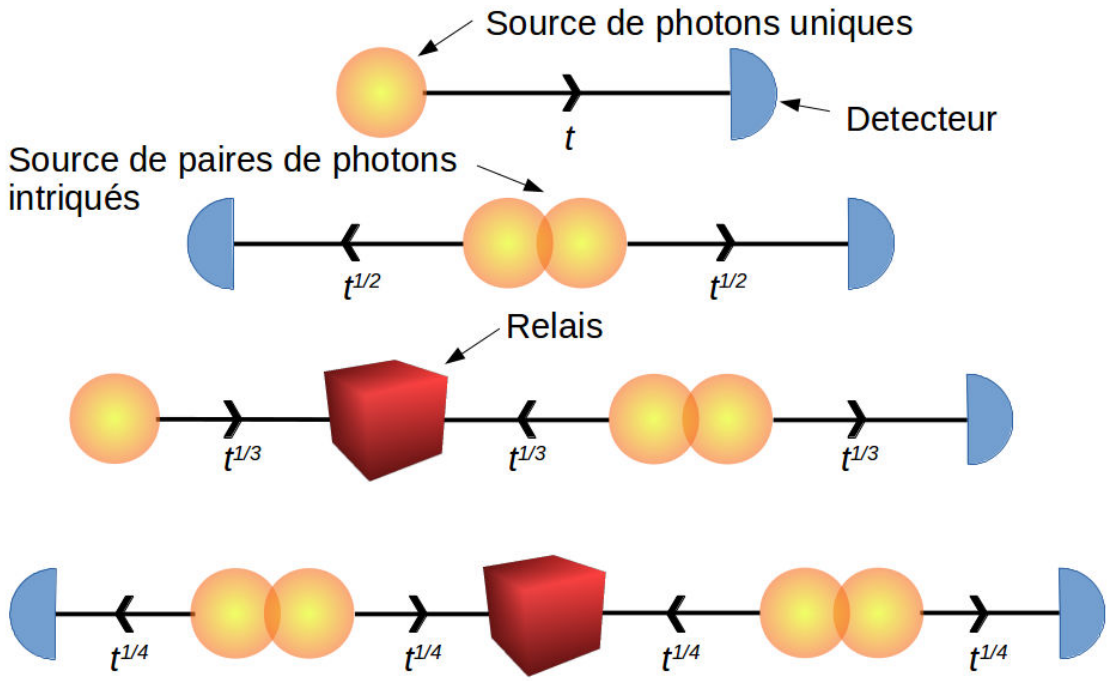


Figure 1.14. – Différentes techniques permettent d'augmenter la portée d'un lien de communication quantique. De haut en bas : un lien de communication direct reposant sur la distribution de qubits ; un lien impliquant des paires de photons intriqués ; téléportation quantique ; relais quantique.

Pour répondre au défi de la distance, et sachant que les pertes dans les fibres ne gagneront pas un ordre de grandeur au cours des dix prochaines années, les futurs réseaux devront reposer sur des liens de téléportation quantique [194]. La téléportation quantique est un protocole consistant à transférer l'état quantique d'un système vers un autre système similaire et séparé spatialement du premier en mettant à profit l'intrication quantique, voir FIGURE 1.13. Par extension, il est alors possible d'étendre

la téléportation de proche en proche, c'est la notion de relais quantiques, comme le montre la FIGURE 1.14.

L'utilisation d'un tel protocole pour gagner en distance est assez intuitif à comprendre : plus le nombre de ressources quantiques impliquées dans un réseau augmente, plus le nombre de nœuds où il est possible de tester la présence de l'information quantique devient grand. Ces nœuds sont soit des stations de génération soit des stations de mesure de l'information. Ainsi, le nombre global de détecteurs augmente lui aussi et le rapport entre la probabilité d'obtenir une détection de tous les photons impliqués et celle d'obtenir simultanément du bruit sur tous les détecteurs devient de plus en plus favorable. En d'autres termes, plus les ressources quantiques sont grandes, plus le rapport signal sur bruit du lien constitué est bon, voir FIGURE 1.15.

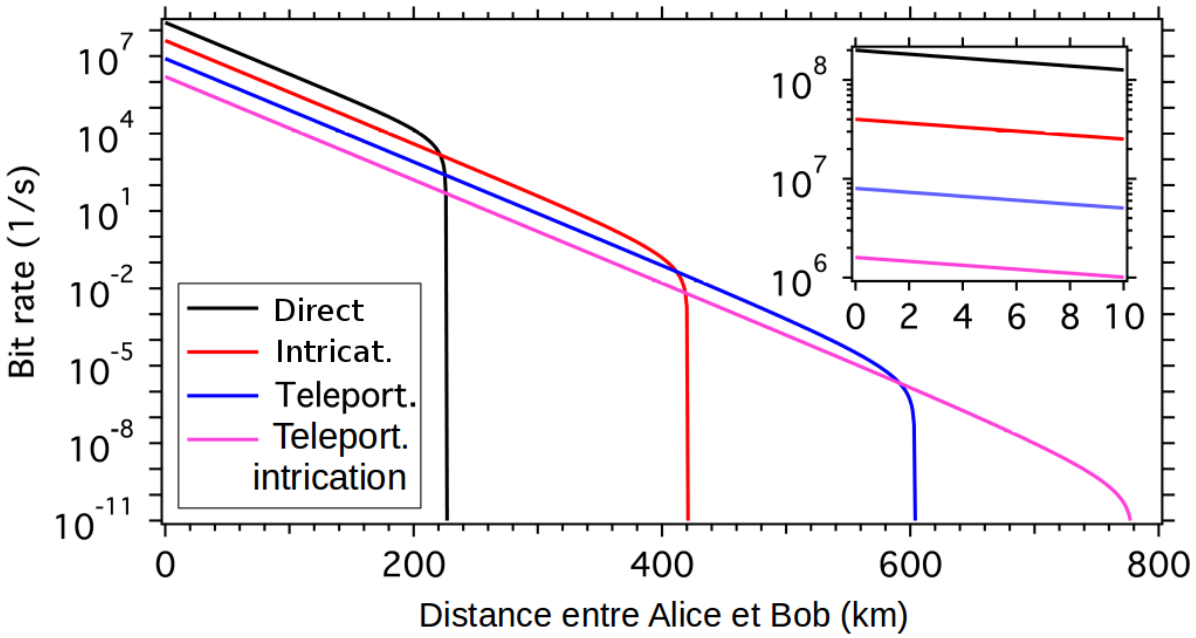


Figure 1.15. – Taux de clés secrètes en fonction de la distance entre Alice et Bob pour différents protocoles de transmission. Les paramètres utilisés sont un taux de génération de qubits de 10^9/s, une efficacité de détection de 20%, un taux de transmission de 0.2 dB/km, et un taux maximum d'erreur tolérable de 15%. Le lien direct (un détecteur requis) offre le meilleur débit à courte distance, mais le lien reposant sur la distribution de paires de photons intriqués (deux détecteurs) permet d'atteindre des distances plus grandes au prix d'un débit réduit. Des protocoles plus complexes comme la téléportation quantique (3 détecteurs) ou la téléportation d'intrication (4 détecteurs) permettent d'atteindre des distances encore plus importantes, mais une nouvelle fois au prix de débits réduits.

À ce jour de nombreuses implémentations du protocole de téléportation

quantique ont déjà été réalisé avec des photons, que ce se soit en variables discrètes [195, 196, 197, 198, 199, 200, 201, 202], en variables continues [203, 204, 205], ou en combinant les deux dans une approche hybride [206, 207]. Pour un état de l'art complet incluant d'autres supports que la lumière voir la référence [208]. Idéalement, les nœuds du réseau devraient être intriqués soit par paires, soit en créant des états intriqués multi-partite de grande échelle appelés états *cluster* que l'on viendrait diffuser à tous les nœuds. Des états *cluster* reliant des milliers de nœuds ont déjà été créés en laboratoire [56], le défis est désormais de démontrer la façon dont ils peuvent être déployés sur de longues distances.

Outre la téléportation quantique et le développement de relais quantiques qui restent la méthode la plus efficace, une solution naturelle pour augmenter la distance mais aussi le débit consiste à améliorer hardware et software que sont respectivement systèmes de détections et protocoles d'encodage. Pour la partie hardware, cela passe par de meilleures efficacités, de plus courts temps de réponse et de plus faibles niveau de bruit lorsqu'il est question de détections de photons uniques, tandis que dans le cas de systèmes de détections homodynes et hétérodynes cela passe par de plus large bandes passantes à niveau de bruit électronique équivalent. Pour la partie software, certains protocoles récemment développés permettent au travers d'alphabets plus larges d'encoder plus d'un bit par porteur d'information augmentant ainsi les débits pour une distance donnée tout en offrant la possibilité de procéder à du multiplexage pour router le signal vers un plus grand nombre d'utilisateurs [209, 210, 211, 212, 213, 214, 215], tandis que d'autres protocoles autorisent désormais des seuils d'erreurs tolérables plus élevés qu'auparavant ce qui à pour effet d'accroître la distance d'échange maximale autorisée [216, 217, 218, 219].

Enfin, une solution plus coûteuse mais qui tend à démontrer la faisabilité de la cryptographie quantique à l'échelle planétaire consiste à s'affranchir de distributions par fibre optique au profit de distributions par satellite [220], seuls les 10 km de traversé de la basse atmosphère occasionnant des pertes. En 2015, une équipe italienne a transmis des impulsions optiques jusqu'à un satellite permettant la réflexion de ces derniers à l'échelle du photon unique jusqu'à la station d'émission [221]. Enfin en embarquant en 2016 une source de paires de photons intriqués, l'administration spatiale nationale chinoise (CNSA) plaçait sur orbite le premier satellite de communication quantique jamais fabriqué. Récemment, des corrélations quantiques entre photons jumeaux ont pu être mesurées entre deux sites terrestres séparés de plus de 1000 km, voir Figure 1.16, pour une altitude de transmission moyenne de 1200 km, un record absolu [222, 223, 224]. Bien que les débits soient encore faibles, quelques hertz, et que les fenêtres d'alignement soient très courtes à ces altitudes (quelques minutes), la perspective d'un réseau de satellites synchronisés à plus haute altitude pourrait, en complément de réseaux fibrés métropolitains, venir permettre d'établir des liens de cryptographie quantique entre réseaux métropolitains distants.

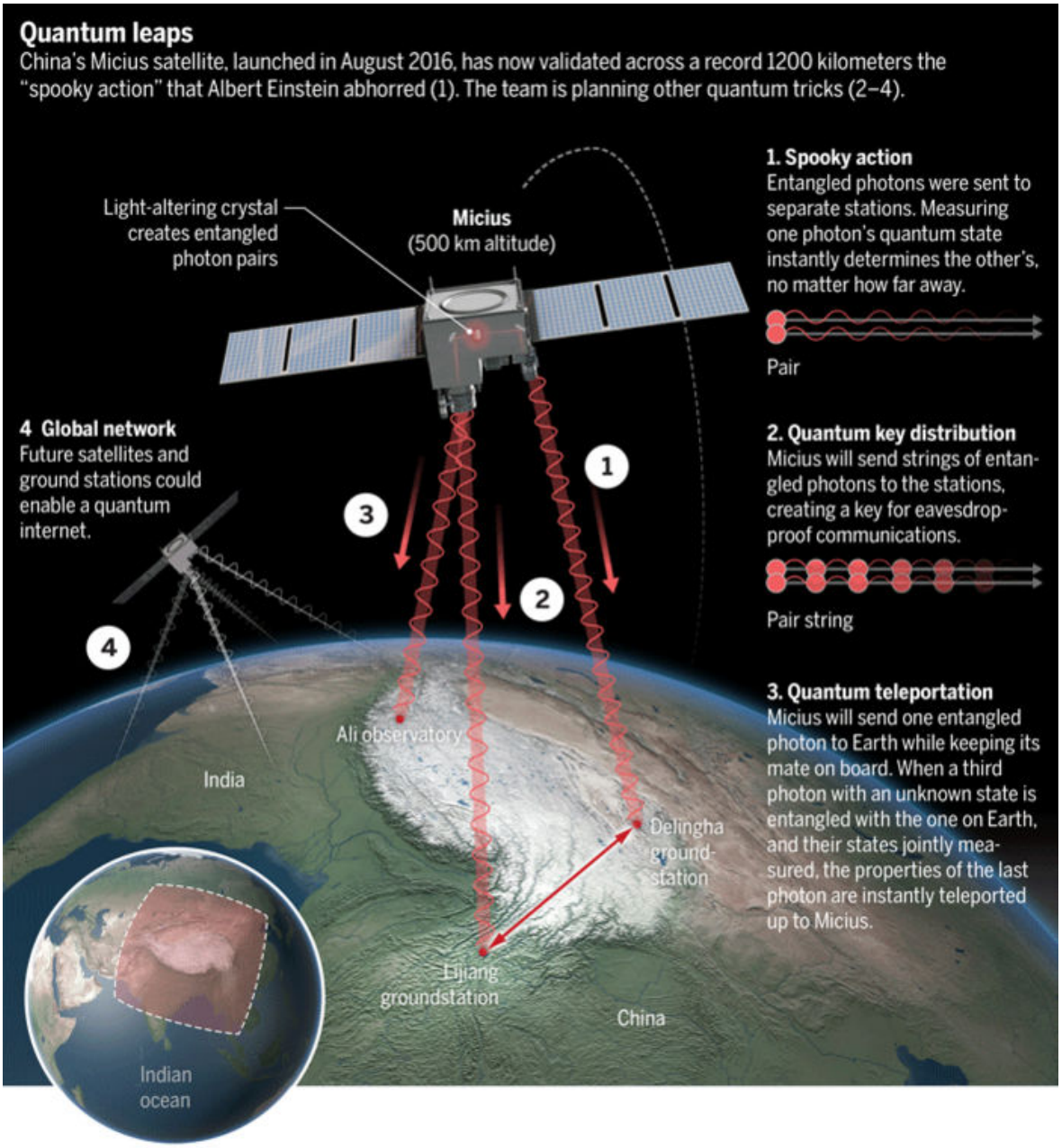


Figure 1.16. – Illustration du programme spatial chinois en vue du déploiement d'un réseau de communication quantique sur grandes distances, les étapes (1) et (3) ayant respectivement été franchies en juin [222] et août 2017 [223], tandis que l'étape (2) est en cours de réalisation [224].

1.2.3. Mémoires quantiques et interfaces lumière-matière

Les futurs réseaux quantiques nécessiteront également des mémoires pour stocker l'information quantique, idéalement pendant des durées arbitraires, en protégeant ces dernières de toutes interactions indésirables avec l'environnement. De telles mémoires sont nécessaires au niveau des processeurs quantiques ainsi qu'au niveau des nœuds relais pour synchroniser les différents signaux optiques [225], une condition *sine qua non* pour le bon fonctionnement d'un répéteur quantique. Le rôle d'une mémoire quantique est de stocker temporairement un état quantique avec une certaine probabilité p_{in} et, idéalement, sans que celui-ci ne soit dégradé. Le système physique qui constitue le support du stockage doit donc être capable de préserver la cohérence de l'état, puis de le transférer sur demande sur un autre état photonique, avec une certaine probabilité p_{out}. Suivant les applications visées, il existe deux types de mémoires quantiques : absorbantes et émissives, voir la référence [226] pour des protocoles détaillés.

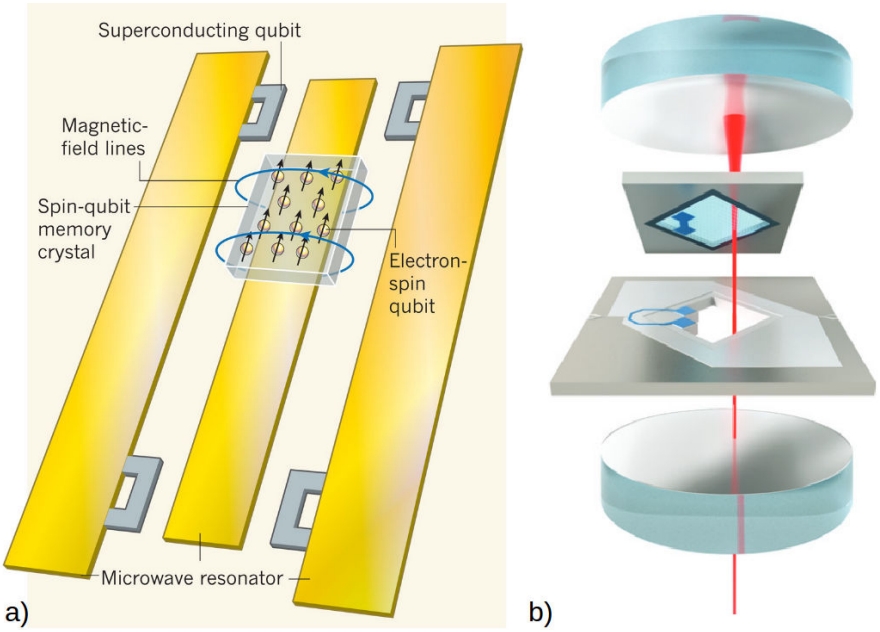


Figure 1.17. – **a)** Architecture d'un processeur quantique hybride selon la proposition de [227, 228, 229], combinant des qubits supraconducteurs et des spin qubits servant de cristal mémoire. Les états des qubits supraconducteurs peuvent être transférés à la mémoire par l'intermédiaire de photons à résonances micro-ondes. **b)** Conversion optomécanique selon la proposition [230]. Une cavité optique et une cavité micro-onde sont couplées à une membrane nanomécanique. La pression de rayonnement à partir de la lumière infrarouge piégée met en vibration la membrane, ce qui modifie la capacité du circuit micro-onde.

Les ensembles de spins représentent un premier exemple de mémoires quantiques. Des gaz d'atomes froids constitués d'environ un million d'atomes de rubidium peuvent

convertir un photon unique en une excitation atomique collective connue sous le nom d'onde de spin [231, 232, 233, 234, 235, 236, 237, 238, 239, 239]. Les temps de stockage dépassent les 100 millisecondes requis pour transmettre un signal optique à n'importe quel endroit à travers le monde. Des mémoires quantiques à l'état solide font également l'objet de développement [240, 241, 242, 243, 244, 245]. Des ensembles de spins dans des cristaux solides, créés en insérant des défauts dans des diamants ou en utilisant des cristaux dopés de terre rare, peuvent garder une cohérence pendant des secondes, des minutes, voir des heures à des températures cryogéniques.

Au niveau des futurs nœuds de calcul, les qubits supraconducteurs, qui sont définis par des quantités physiques telles que la charge d'un condensateur ou le flux d'une inductance, interagissent dans un processeur quantique en libérant et en absorbant des photons aux longueurs d'ondes micro-ondes. Par conséquent, si l'on veut pouvoir stocker et récupérer de manière réversible dans une mémoire quantique attachée au processeur les résultats des calculs de ce dernier, des interfaces efficaces entre photons micro-ondes et des ensembles de spins à l'état atomique ou à l'état solide devront également être développés comme cela a déjà pu être fait [227, 228, 229, 246], voir FIGURE 1.17a. Cette technologie hybride constituerait un élément prometteur en vue d'obtenir un ordinateur quantique distribué.

Enfin, l'incorporation de processeurs supraconducteurs dans un Internet quantique nécessitera que les photons micro-ondes stockés puissent être interfacées aux signaux optiques entrant en provenance des utilisateurs. Une solution hybride, appelée transducteur quantique optomécanique est actuellement en train d'émerger afin de répondre à cette problématique, tel qu'illustré en FIGURE 1.17b. Ces appareils exploitent des oscillateurs nanomécaniques, tels que des miroirs vibrants microscopiques, pour transformer des photons optiques en photons micro-ondes et vice versa. Leur efficacité reste à améliorée afin de s'assurer que les qubits ne sont pas perdus pendant le processus de conversion et que toutes les propriétés quantiques sont bien préservées durant la conversion dont l'efficacité est actuellement d'environ 10% [230].

Chapitre 2.

Photons, modes et interferences

Dans ce second chapitre, les notions d'optique quantique utiles à la description des travaux expérimentaux présentés au sein de ce manuscrit sont introduites. Sont respectivement présentés la quantification du champ électromagnétique et sa représentation sous forme de phaseur, les bases de représentation usuelles, ainsi que différents effets d'interférences linéaires et non-linéaires. Le lecteur désireux de plus de détails pourra se référer aux ouvrages sur lesquels nous nous sommes appuyés pour la rédaction de ce chapitre [247, 248, 249, 250, 251, 252].

2.1. Quantification du champ électromagnétique

Avec $\vec{E}(\vec{r},t)$ et $\vec{B}(\vec{r},t)$ désignant respectivement , en toute généralité, le champ électrique et le champ magnétique, un point de départ usuel pour la quantification du champ électromagnétique sont les équations de Maxwell en l'absence de sources :

$$\begin{cases} \vec{\nabla}\times\vec{H} = \dfrac{\partial\vec{D}}{\partial t}, \\ \vec{\nabla}\times\vec{E} = -\dfrac{\partial\vec{B}}{\partial t}, \\ \vec{\nabla}\cdot\vec{B} = 0, \\ \vec{\nabla}\cdot\vec{D} = 0, \end{cases} \tag{2.1}$$

où $\vec{B} = \mu_0\vec{H}$ et $\vec{D} = \varepsilon_0\vec{E}$, μ_0 et ε_0 correspondent respectivement à la permittivité diélectrique et à la perméabilité magnétique du vide, de sorte que $\mu_0\varepsilon_0 = c^{-2}$. Les équations de Maxwell sont invariantes de jauge en l'absence de sources. Nous faisons ici le choix de nous placer dans la jauge de Coulomb qui permet de remonter directement aux vecteurs $\vec{E}$ et $\vec{B}$ à partir du potentiel vecteur $\vec{A}(\vec{r},t)$ via les relations :

$$\vec{B} = \vec{\nabla}\times\vec{A}, \tag{2.2}$$

$$\vec{E} = -\frac{\partial\vec{A}}{\partial t}, \tag{2.3}$$

avec la condition de jauge de Coulomb :

$$\vec{\nabla} \cdot \vec{A} = 0. \tag{2.4}$$

En substituant (2.2) dans (2.1) on trouve alors que le potentiel vecteur satisfait l'équation d'onde :

$$\vec{\nabla}^2 \vec{A}(\vec{r}, t) = \frac{1}{c^2} \frac{\partial^2 \vec{A}(\vec{r}, t)}{\partial t^2}. \tag{2.5}$$

Nous séparons ensuite le potentiel vecteur en deux termes complexes :

$$\vec{A}(\vec{r}, t) = \vec{A}^{(+)}(\vec{r}, t) + \vec{A}^{(-)}(\vec{r}, t), \tag{2.6}$$

avec un terme $\vec{A}^{(+)}(\vec{r}, t)$ qui contient les amplitudes variant en $e^{-i\omega t}$ pour $\omega > 0$ et un terme $\vec{A}^{(-)}(\vec{r}, t)$ qui contient les amplitudes variant en $e^{i\omega t}$ telles que $\vec{A}^{(-)} = (\vec{A}^{(+)})^*$.

Il est d'ordinaire plus aisé de travailler avec un ensemble discret de variables plutôt qu'avec un continuum, nous décrivons par conséquent le champ restreint à un certain volume de l'espace et exprimons le potentiel vecteur sur la base d'un ensemble discret de modes orthogonaux :

$$\vec{A}^{(+)}(\vec{r}, t) = \sum_k c_k \vec{u}_k(\vec{r}) e^{-i\omega_k t}, \tag{2.7}$$

où les coefficients de Fourier sont constants pour un champ en espace libre. Les modes $\vec{u}_k(\vec{r})$ correspondant aux fréquences ω_k obéissent à l'équation d'onde :

$$\left(\vec{\nabla}^2 + \frac{\omega_k^2}{c^2}\right) \vec{u}_k(\vec{r}) = 0, \tag{2.8}$$

à condition que le volume d'espace considéré ne contienne pas de matériaux réfractif. Les différents modes doivent aussi satisfaire la condition de transversalité :

$$\vec{\nabla} \cdot \vec{u}_k(\vec{r}) = 0. \tag{2.9}$$

Enfin les différentes fonctions $\vec{u}_k(\vec{r})$ forment un ensemble complet de modes orthogonaux :

$$\int_V \vec{u}_k^*(\vec{r}) \vec{u}_{k'}(\vec{r}) \, \mathrm{d}\vec{r} = \delta_{k,k'}. \tag{2.10}$$

Les différents modes dépendent des conditions aux limites du volume physique considéré. Des conditions aux limites périodiques correspondant aux modes de propagation d'ondes dites 'ondes planes', tandis que des conditions appropriées à des parois réfléchissantes conduisent à des ondes stationnaires. Par exemple, les modes associés à des ondes planes dans un volume cubique de côté L s'écrivent comme :

$$\vec{u}_k(\vec{r}) = \frac{1}{L^{2/3}} \hat{e}^{(j)} e^{i\vec{k}\cdot\vec{r}}, \tag{2.11}$$

où $\hat{e}^{(j)}$ est le vecteur polarisation unitaire. L'indice k d'un mode décrit différentes variables, à savoir l'indice de polarisation ($j = 1, 2$) et les trois coordonnées cartésiennes associées à la propagation du vecteur $\vec{k}$. Les composantes du vecteur d'onde $\vec{k}$ prennent alors les valeurs :

$$k_x = \frac{2\pi n_x}{L}, \quad k_y = \frac{2\pi n_y}{L}, \quad k_z = \frac{2\pi n_z}{L}. \qquad n_x, n_y, n_z = 0, \pm 1, \pm 2, ... \tag{2.12}$$

Le vecteur polarisation $\hat{e}^{(\lambda)}$ doit être perpendiculaire à $\vec{k}$ de part la condition de transversalité (2.9).

Le potentiel vecteur peut désormais s'écrire sous la forme suivante :

$$\vec{A}(\vec{r}, t) = \sum_k \left(\frac{\hbar}{2\omega_k \varepsilon_0} \right)^{1/2} \left[a_k \vec{u}_k e^{-i\omega_k t} + a_k^\dagger \vec{u}_k^* e^{i\omega_k t} \right]. \tag{2.13}$$

Où les a_k sont les coefficients de Fourier de la décomposition. Le champ électrique correspondant est alors :

$$\vec{E}(\vec{r}, t) = i \sum_k \left(\frac{\hbar\omega_k}{2\varepsilon_0} \right)^{1/2} \left[a_k \vec{u}_k e^{-i\omega_k t} - a_k^\dagger \vec{u}_k^* e^{i\omega_k t} \right]. \tag{2.14}$$

Les facteurs de normalisation on été choisis de sorte à ce que les amplitudes a_k et $a_k^\dagger$ soient sans dimension.

Selon une approche classique de l'électromagnétisme, ces amplitudes de Fourier sont des nombres complexes. La quantification du champ électromagnétique est accomplie en considérant a_k et $a_k^\dagger$ comme des opérateurs adjoints mutuels que nous noterons $\hat{a}_k$ et $\hat{a}_k^\dagger$. Étant donné que les photons, les quanta d'énergie associés aux ondes électromagnétiques, sont des bosons, les opérateurs $\hat{a}_k$ et $\hat{a}_k^\dagger$ obéissent aux relations de commutations suivantes :

$$[\hat{a}_k, \hat{a}_{k'}] = \left[\hat{a}_k^\dagger, \hat{a}_{k'}^\dagger \right] = 0, \quad \left[\hat{a}_k, \hat{a}_{k'}^\dagger \right] = \delta_{k,k'}. \tag{2.15}$$

Le comportement dynamique des amplitudes du champ électrique peut désormais ainsi être décrit par un ensemble d'oscillateurs harmoniques indépendants obéissants aux relations de commutation mentionnées ci-dessus. Les états quantiques associés à chaque mode peuvent maintenant être discutés de manière indépendante les uns des autres. L'état pour chaque mode peut être décrit par un vecteur d'état $|\psi\rangle_k$ de l'espace de

Hilbert associé à ce mode. Les états du champ pris dans son intégralité sont alors définis comme un produit tensoriel des espaces de Hilbert associés à chacun des modes.

Le Hamiltonien du champ électromagnétique est donné par :

$$\hat{\mathcal{H}}_{EM} = \frac{1}{2}\int (\varepsilon_0 \hat{\vec{E}}^2 + \mu_0 \hat{\vec{H}}^2)\,\mathrm{d}\vec{r}. \tag{2.16}$$

En substituant (2.14) pour $\hat{\vec{E}}$ ainsi que l'expression équivalente pour $\hat{\vec{H}}$ et en utilisant les conditions (2.9) et (2.10), on obtient alors pour le Hamiltonien l'expression traditionnelle :

$$\hat{\mathcal{H}}_{EM} = \sum_k \hbar\omega_k \left(\hat{a}_k^\dagger \hat{a}_k + \frac{\hat{\mathbb{1}}}{2}\right). \tag{2.17}$$

Cette expression représente la somme du nombre de photons dans chaque mode multiplié par l'énergie d'un photon pris dans ce mode, plus $\frac{1}{2}\hbar\omega_k$ qui représente les fluctuations quantiques du vide présentes pour chaque mode. Nous allons dans la suite désormais considérer trois bases de représentation pour le champ électromagnétique quantifié.

2.2. Espace des phases

Une des bases de la physique statistique classique est la notion de distribution de probabilité dans l'espace des phases, généralement représenté dans le plan position/impulsion (x, p). Pour une particule classique, impulsion et position peuvent être simultanément et parfaitement déterminées. La distribution correspondante est donc un pic de Dirac dans le plan (x, p). Afin de décrire l'incertitude statistique sur ces deux variables, on introduit une densité de probabilité $f(x, p)$ positive et normalisée décrivant la probabilité de trouver la particule dans une région de l'espace des phases. Ainsi, le calcul de toute grandeur statistique O sur l'état de la particule est donc une moyenne classique :

$$\langle O \rangle = \int f(x,p) O(x,p)\,\mathrm{d}x\mathrm{d}p. \tag{2.18}$$

Les physiciens se sont heurtés très tôt au problème d'étendre cette représentation à la description des systèmes quantiques. Dans ce cas, même lorsque la particule est préparée dans un état pur, position et impulsion ne sont pas parfaitement déterminées simultanément. Et dans le cas d'un mélange statistique, encore une fois, incertitude quantique et incertitude classique s'ajoutent.

Nous introduisons dans cette section les opérateurs de quadrature qui sont définis par analogie aux opérateurs de position et d'impulsion d'un oscillateur harmonique régi par

les opérateurs de création et annihilation introduits précédemment. Ils seront définis de manière générale, en tenant compte d'une éventuelle rotation d'angle dans le plan de Fresnel. Nous présenterons ensuite des classes générales d'états quantiques ainsi que leurs représentations et opérations de transformations associées dans l'espace des phases.

2.2.1. Quadratures

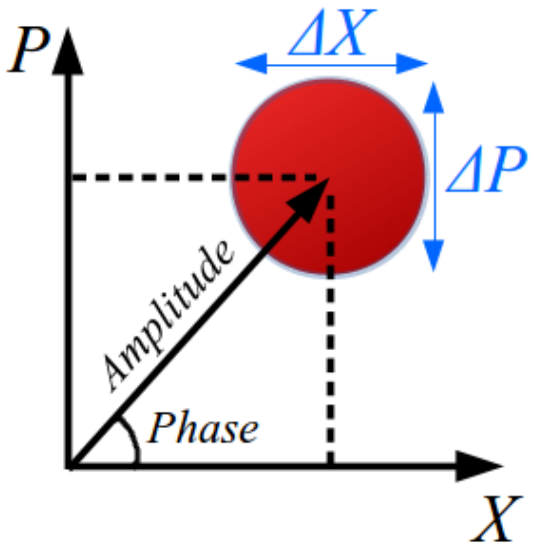


Figure 2.1. – Représentation du champ électromagnétique quantifié dans l'espace des phases de Fresnel. La zone rouge représente les fluctuations du champ.

Bien que le champ électromagnétique contienne un nombre infini de modes, chaque mode est décrit par un espace indépendant de Hilbert. Nous pouvons donc, sans perte de généralité, restreindre notre attention à un mode en particulier. Aussi par analogie à l'optique classique, chaque mode du champ électrique peut également être écrit dans l'espace des phases de Fresnel en termes de ses parties réelles et imaginaires, voir Figure 2.1. En ne considérant qu'un seul mode l'opérateur champ électrique peut alors être réécrit comme suit :

$$\hat{E}(\vec{r},t) = \left(\frac{\hbar\omega}{2V\varepsilon_0}\right)^{1/2}\left[\hat{X}\sin\left(\vec{k}\cdot\vec{r}-\omega t\right) - \hat{P}\cos\left(\vec{k}\cdot\vec{r}-\omega t\right)\right], \tag{2.19}$$

où $\hat{X}$ et $\hat{P}$ sont connus sous le nom d'opérateurs de quadratures du champ. Leur expression en fonction des opérateurs $\hat{a}$ et $\hat{a}^\dagger$ est donnée par :

$$\hat{X} = \frac{\hat{a}^\dagger + \hat{a}}{2} \qquad \text{et} \qquad \hat{P} = \frac{\hat{a}^\dagger - \hat{a}}{2i}. \tag{2.20}$$

Ces deux opérateurs obéissent à la relation de commutation suivante :

$$\left[\hat{X}, \hat{P}\right] = 2i\mathbb{1}. \tag{2.21}$$

Et puisque ces deux opérateurs sont des variables conjuguées, ils obéissent également à la relation d'indétermination de Heisenberg :

$$\Delta\hat{X}\Delta\hat{P} \geq 1. \tag{2.22}$$

Les opérateurs de quadratures sont également des observables et par conséquent des opérateurs Hermitiens. Ils sont associés à des vecteurs propres orthogonaux, $\hat{X}\,|x\rangle = x\,|x\rangle$, qui forment un ensemble complet $\int |x\rangle\langle x|\,\mathrm{d}x = \mathbb{1}$. Enfin, les opérateurs de quadratures peuvent être généralisés à tout angle θ dans la représentation de Fresnel :

$$\hat{X}_\theta = \frac{\hat{a}^\dagger e^{i\theta} + \hat{a}e^{-i\theta}}{2}. \tag{2.23}$$

2.2.2. Opérateurs

Dans cette section sont déclinés les principaux opérateurs qui seront mis en œuvre expérimentalement dans la suite du manuscrit lors de la manipulation et de l'ingénierie d'états quantiques.

Opérateur déplacement

Cet opérateur permet de déplacer l'état dans l'espace de phase. Son expression est la suivante :

$$\hat{D}(\alpha) = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}, \tag{2.24}$$

avec α un nombre complexe qui peut être représenté à l'aide d'une exponentielle complexe : $\alpha = |\alpha|e^{i\phi}$, où $|\alpha|$ et ϕ sont respectivement l'amplitude et la phase de l'état. Il en résulte les propriétés suivantes où nous avons fait appel au théorème de Baker-Hausdorff pour démontrer la deuxième :

$$\hat{D}^\dagger(\alpha) = \hat{D}^{-1}(\alpha) = \hat{D}(-\alpha), \qquad \hat{D}(\alpha+\beta) = \hat{D}(\alpha)\hat{D}(\beta)e^{-i\mathrm{Im}\{\alpha\beta^*\}}. \tag{2.25}$$

Enfin, son action sur un mode correspond aux relations :

$$\hat{D}^\dagger(\alpha)\hat{a}\hat{D}(\alpha) = \hat{a} + \alpha, \tag{2.26}$$
$$\hat{D}^\dagger(\alpha)\hat{a}^\dagger\hat{D}(\alpha) = \hat{a}^\dagger + \alpha^*, \tag{2.27}$$

ce qui dans l'espace des phases se traduit par une simple opération de translation :

$$\begin{cases} \{x,p\} \to \{x + \mathrm{Re}\,[\alpha]\,, p + \mathrm{Im}\,[\alpha]\}\,, \\ \{\Delta x, \Delta p\} \to \{\Delta x, \Delta p\}\,. \end{cases} \tag{2.28}$$

Expérimentalement, cet opérateur est implémenté en mélangeant l'état avec un champ cohérent via un séparateur de faisceau asymétrique

Opérateur compression

La relation de Heisenberg qui contraint les quadratures conjuguées montre que le produit des indéterminations ne peut pas dépasser une certaine limite fondamentale. Cependant, il est possible d'accroître le niveau de détermination d'une des deux quadratures au prix d'une plus grande indétermination sur l'autre. Un tel phénomène est connu sous le nom de compression (ou *squeezing* en anglais), où les fluctuations d'une quadrature diminuent tandis que l'autre quadrature fait l'objet d'une 'anti-compression'. L'opérateur de compression peut s'écrire comme suit :

$$\hat{S}(\xi) = e^{\frac{1}{2}\left(\xi^* \hat{a}^2 - \xi \hat{a}^{\dagger 2}\right)}, \tag{2.29}$$

où $\xi = re^{2i\varphi}$. $r = |\xi|$ et φ sont respectivement le facteur et l'angle de compression. L'action de cet opérateur sur un mode est la suivante :

$$\begin{cases} \hat{S}^\dagger(\xi)\hat{a}\hat{S}(\xi) = \hat{a}\cosh r - \hat{a}^\dagger e^{-2i\varphi}\sinh r, \\ \hat{S}^\dagger(\xi)\hat{a}^\dagger\hat{S}(\xi) = \hat{a}^\dagger\cosh r - \hat{a}e^{2i\varphi}\sinh r, \end{cases} \tag{2.30}$$

ce qui dans l'espace des phases se traduit comme suit :

$$\begin{cases} \{x,p\} \to \left\{e^{-r}x, e^{r}p\right\}, \\ \{\Delta x, \Delta p\} \to \left\{e^{-2r}\Delta x, e^{2r}\Delta p\right\}. \end{cases} \tag{2.31}$$

Expérimentalement, cet opérateur peut être implémenté en utilisant des processus non linéaires tel que le processus de conversion paramétrique spontanée, voir section 2.5.2.

Opérateur rotation

Cet opérateur permet d'effectuer un décalage de phase sur un état quantique :

$$\hat{U}(\gamma) = e^{i\hat{a}^\dagger\hat{a}\gamma}. \tag{2.32}$$

Ce qui dans l'espace des phase se traduit par une simple opération de rotation :

$$\begin{cases} \{x,p\} \to \{x\cos\gamma - p\sin\gamma, x\sin\gamma + p\cos\gamma\}\,, \\ \{\Delta x, \Delta p\} \to \{\Delta x, \Delta p\}\,. \end{cases} \tag{2.33}$$

2.3. Représentations

Dans cette section sont listés les principales bases des états qui seront utilisés dans le reste du manuscrit lors de la manipulation et de l'ingénierie d'états quantiques.

2.3.1. États de Fock

Le Hamiltonien (2.17) restreint à un mode a pour valeurs propres $\hbar\omega\left(n+\frac{1}{2}\right)$, où n est un entier positif ou nul ($n = 0, 1, 2, ..., \infty$). Les vecteurs propres associés s'écrivent $|n_k\rangle$. De tels états sont appelés états de Fock, ils sont états propres de l'opérateur nombre de photons $\hat{n} = \hat{a}^\dagger\hat{a}$

$$\hat{a}^\dagger\hat{a}\,|n\rangle = n_k\,|n\rangle\,. \tag{2.34}$$

$\hat{a}^\dagger$ et $\hat{a}$ sont respectivement les opérateurs création et annihilation d'un photon dans le mode considéré :

$$\hat{a}\,|n\rangle = \sqrt{n}\,|n-1\rangle\,, \qquad \hat{a}^\dagger\,|n\rangle = \sqrt{n+1}\,|n+1\rangle\,. \tag{2.35}$$

L'état fondamental de l'oscillateur (ou état de vide quantique) est défini par :

$$\hat{a}\,|0\rangle = 0. \tag{2.36}$$

De là, à partir des équations (2.17) et (2.36), nous voyons que l'énergie de cet état vaut :

$$\langle 0|\,\hat{\mathcal{H}}_{EM}\,|0\rangle = \frac{1}{2}\hbar\omega. \tag{2.37}$$

Enfin, le vecteur d'état pour un état excité quelconque peut être obtenu à partir de l'application successive d'opérateurs créations sur le vide :

$$|n\rangle = \frac{\left(\hat{a}^\dagger\right)^n}{\sqrt{n!}}\,|0\rangle\,, \qquad n = 0, 1, 2, ... \tag{2.38}$$

Notons également que les états de Fock sont orthogonaux :

$$\langle n|m\rangle = \delta_{mn}, \tag{2.39}$$

et forment une base complète :

$$\sum_{n=0}^{\infty} |n\rangle\langle n| = \mathbb{1}. \tag{2.40}$$

À titre de remarque, si l'on considère désormais tous les modes, étant donné qu'il n'y a pas de limite supérieure aux fréquences dans la somme sur les modes du champ électromagnétique, l'énergie de l'état fondamental est censée être infinie, une difficulté

conceptuelle de la théorie quantique des champs. Toutefois, sachant qu'en pratique les expériences mesurent une variation de l'énergie totale du champ électromagnétique, l'énergie infinie du vide n'entraîne aucune divergence dans la pratique. Aussi, bien que les états de Fock représentent une base idéale pour décrire des sources parfaites de photons uniques, en pratique de telles sources restent aujourd'hui encore difficiles à développer. Il est alors courant de simuler de telles sources avec des impulsions lasers très largement atténuées, dans quel cas une description en terme d'états cohérents devient plus appropriée. Une autre alternative réside également dans la réalisation de sources de photons annoncés [253, 254].

2.3.2. États cohérents

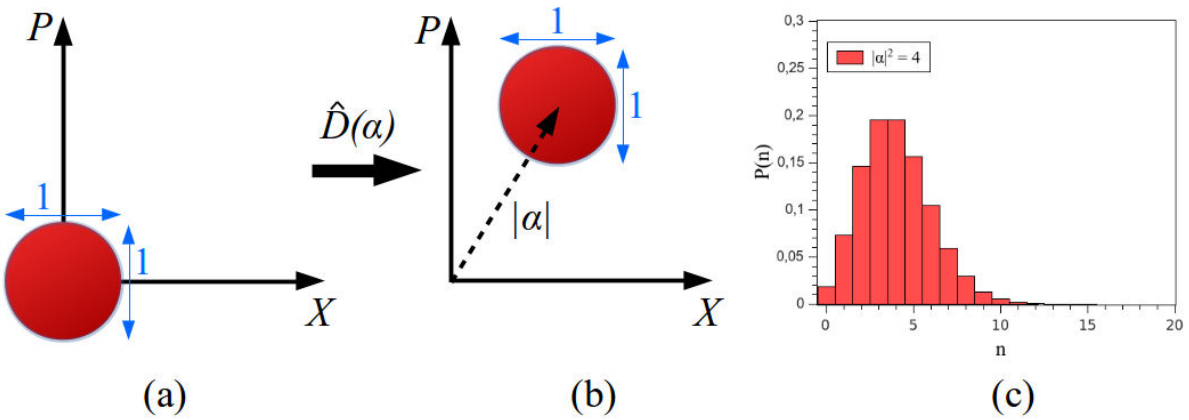


Figure 2.2. – **a,b)** Représentation dans l'espace des phases de l'évolution d'un état de vide quantique (a), $|0\rangle$, en un état cohérent (b), $|\alpha\rangle$, par application de l'opérateur déplacement. **c)** Distribution du nombre de photons pour un état cohérent avec $\bar{n} = 4$.

Les états cohérents contiennent un nombre indéfini de photons, ce qui permet à ces derniers d'avoir une phase plus précisément définie que celle des états des Fock, qui est elle complètement indéfinie. Le produit des indéterminations en amplitude et en phase pour les états cohérents correspond au minimum autorisé par le principe d'indétermination. En ce sens, les états cohérents sont les états quantiques les plus proches d'une description classique du champ électromagnétique. Nous allons exposer ci-après les propriétés de bases de ces états. Ces états s'obtiennent en appliquant l'opérateur unitaire déplacement sur le vide, voir FIGURE 2.2 :

$$|\alpha\rangle = \hat{D}(\alpha)\,|0\rangle\,. \tag{2.41}$$

Les états cohérents sont des vecteurs propres de l'opérateur annihilation $\hat{a}$:

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle\,. \tag{2.42}$$

Les états cohérents contiennent un nombre indéfini de photons comme dit en introduction de cette section. Une façon de le montrer consiste à développer l'expression d'un état cohérent sur la base des états de Fock. En prenant le produit scalaire entre les deux membres de (2.42) et $\langle n|$ on obtient la relation de récursion :

$$\sqrt{n+1}\,\langle n+1|\alpha\rangle = \alpha\,\langle n|\alpha\rangle\,. \tag{2.43}$$

Il s'ensuit que :

$$\langle n|\alpha\rangle = \frac{\alpha^n}{\sqrt{n!}}\,\langle 0|\alpha\rangle\,. \tag{2.44}$$

De là, il vient :

$$|\alpha\rangle = \sum_n |n\rangle\,\langle n|\alpha\rangle = \langle 0|\alpha\rangle \sum_n \frac{\alpha^n}{\sqrt{n!}}\,|n\rangle\,. \tag{2.45}$$

La norme au carré du vecteur $|\alpha\rangle$ est ainsi égale à :

$$|\langle\alpha|\alpha\rangle|^2 = |\langle 0|\alpha\rangle|^2 \sum_n \frac{|\alpha|^{2n}}{n!} = |\langle 0|\alpha\rangle|^2\, e^{|\alpha|^2}. \tag{2.46}$$

De plus il est également facile de voir que :

$$\langle 0|\alpha\rangle = \langle 0|\,\hat{D}(\alpha)\,|0\rangle = e^{-\frac{|\alpha|^2}{2}}. \tag{2.47}$$

Les états cohérents sont par conséquent normalisés $|\langle\alpha|\alpha\rangle|^2 = 1$, et on obtient finalement la décomposition suivante :

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_n \frac{\alpha^n}{\sqrt{n!}}\,|n\rangle\,. \tag{2.48}$$

On reconnaît ici une distribution de Poisson :

$$P(n) = |\langle n|\alpha\rangle|^2 = \frac{|\alpha|^{2n}\, e^{-|\alpha|^2}}{n!}, \tag{2.49}$$

où $|\alpha|^2$ est le nombre moyen de photons ($\bar{n} = \langle\alpha|\,\hat{a}^\dagger\hat{a}\,|\alpha\rangle = |\alpha|^2$), voir FIGURE 2.2.

Enfin en utilisant à nouveau le théorème de Baker-Hausdorff il est également possible de montrer que les états cohérents ne sont pas orthogonaux deux à deux :

$$|\langle\beta|\alpha\rangle| = e^{|\alpha-\beta|^2}. \tag{2.50}$$

En revanche ils forment une base complète de l'espace des états :

$$\frac{1}{\pi}\int |\alpha\rangle\langle\alpha|\ \mathrm{d}^2\alpha\ = \mathbb{1}. \tag{2.51}$$

Pour conclure avec les états cohérents, ces derniers sont souvent appelés états quasi-classiques car les indéterminations associées aux deux quadratures sont égales tandis que leur produit est le minimum autorisé par la relation d'Heisenberg (2.22), c'est-à-dire :

$$\Delta\hat{X} = \Delta\hat{P} = 1. \tag{2.52}$$

2.3.3. États comprimés

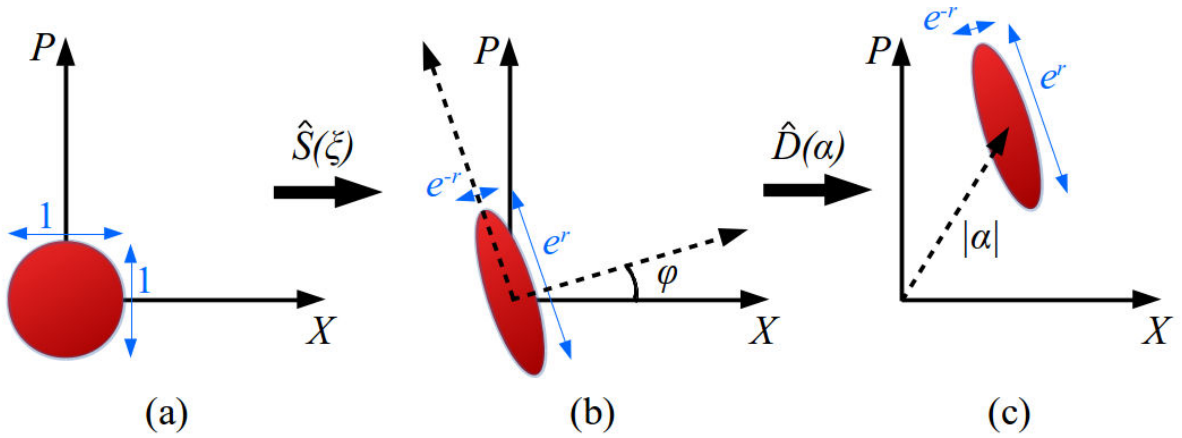


Figure 2.3. – Représentation dans l'espace des phases de l'évolution d'un état de vide quantique (a), $|0,0\rangle$, en un état de vide comprimé (b), $|0,\xi\rangle$, puis en un état comprimé arbitraire (c), $|\alpha,\xi\rangle$, par application successive des opérateurs compression et déplacement.

Comme nous l'avons vu, les états cohérents sont des états d'indétermination minimale avec un niveau d'indétermination identique sur les deux quadratures. Cependant, on peut facilement définir une famille d'états d'indétermination minimale avec des indéterminations déséquilibrées sur les deux quadratures. Les états correspondants sont appelés états comprimés et jouent un rôle important dans le traitement quantique de l'information en variables continues. En particulier, ils fournissent une approximation des états propres non physiques des opérateurs de quadratures, respectivement $|x\rangle$ et $|p\rangle$. Par action de l'opérateur $\hat{S}(\xi)$ précédemment défini sur un état de vide quantique, il est possible de générer des états de vide comprimé :

$$|\xi\rangle = \hat{S}(\xi)\,|0\rangle\,, \tag{2.53}$$

ou, comme illustré FIGURE 2.3, des états comprimés arbitraires, en comprimant d'abord le vide avant de le déplacer via les applications successives des opérateur compression et déplacement :

$$|\alpha, \xi\rangle = \hat{D}(\alpha)\hat{S}(\xi)\,|0\rangle\,. \tag{2.54}$$

En développant l'expression d'un état de vide comprimé sur la base des états de Fock comme nous l'avions fait avec les états cohérents, nous obtenons la statistique suivante :

$$\hat{S}(\xi)\,|0\rangle = (1-\lambda^2)^{1/4} \sum_{n=0}^{\infty} \binom{2n}{n} \left(\frac{\lambda}{2}\right) |2n\rangle\,, \tag{2.55}$$

où nous avons posé $\lambda = \tanh r$.

2.4. Interférences linéaires

Les phénomènes d'interférence entre états quantiques sont au cœur de ce travail de thèse. Nous analysons dans cette section des expériences d'interférence et de mesure de champs qui vont nous permettre de décrire des méthodes essentielles pour la préparation et l'étude de superpositions d'états, donnant notamment naissance à des corrélations. Dans les précédentes sections nous avons décrit des états monomodes du champ. L'analyse des expériences d'interférence nous conduit à envisager à présent des champs à plusieurs modes, et à décrire le couplage entre ces modes.

Le couplage le plus simple entre deux modes est réalisé à l'aide d'une lame séparatrice linéaire. Après avoir donné un modèle simple de la lame séparatrice, nous montrerons à partir de ce modèle comment on peut, à l'aide de telles lames, réaliser des expériences d'interférence à un ou deux photons, dont nous analyserons brièvement les caractéristiques. Nous montrerons également qu'une lame séparatrice est l'élément essentiel pour réaliser une détection homodyne d'une quadrature du champ électromagnétique dans le cadre d'une expérience mettant en jeu de la lumière comprimée.

2.4.1. Traitement quantique de la lame séparatrice

Utilisé pour modéliser des pertes, séparer ou mélanger des modes optiques, mais aussi dans les schémas de détection conditionnelle, une lame séparatrice est un dispositif optique à quatre ports avec deux ports d'entrée (a et b) et deux ports de sorties (c et d). Le principe de la lame séparatrice est illustré en FIGURE 2.4. Chaque port est défini par ses propres opérateurs création et annihilation, et les opérateurs associés aux ports de sortie peuvent s'exprimer en fonction des opérateurs associés aux ports d'entrée à l'aide de la matrice de transformation unitaire $\mathbf{B}$, de sorte que :

$$\begin{pmatrix} \hat{c} \\ \hat{d} \end{pmatrix} = \mathbf{B} \begin{pmatrix} \hat{a} \\ \hat{b} \end{pmatrix} \qquad \text{et} \qquad \left(\hat{c}^\dagger, \hat{d}^\dagger\right) = \left(\hat{a}^\dagger, \hat{b}^\dagger\right) \mathbf{B}^*. \tag{2.56}$$

Dans ce qui suit, nous considérons le cas d'une lame séparatrice idéale sans pertes, insensible à la polarisation des champs optiques incidents, et de coefficient de transmission $t = \cos(\theta)$. La matrice de transformation unitaire associée est alors donnée par :

$$\mathbf{B} = \begin{pmatrix} \cos(\theta) & i\sin(\theta) \\ -i\sin(\theta) & \cos(\theta) \end{pmatrix}. \tag{2.57}$$

Les signes opposés des éléments non-diagonaux traduisent le saut de phase de π entre les deux faces d'un matériau diélectrique.

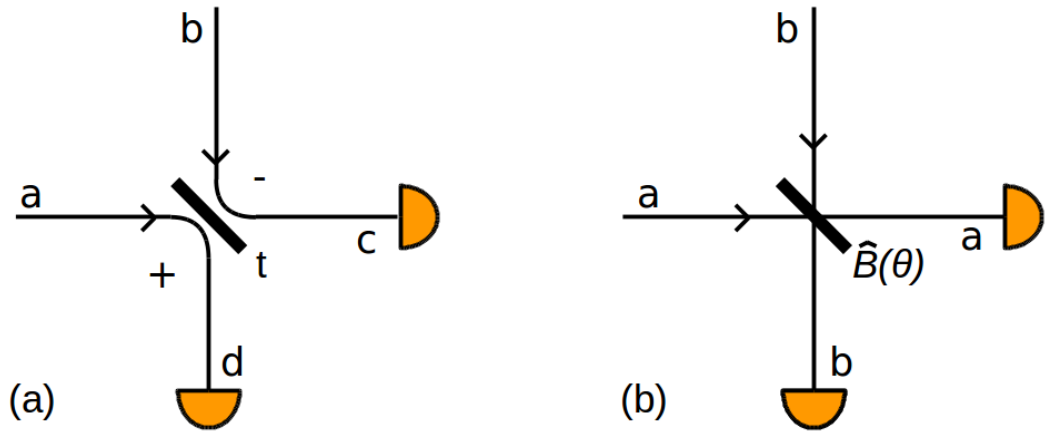


Figure 2.4. – La lame séparatrice idéale (sans pertes) est entièrement caractérisée par son coefficient de transmission $t = \cos(\theta)$. Le coefficient de réflexion est alors donné par $\sqrt{1-t}$. La lumière traversant la lame peut provenir de deux ports d'entrée distincts, labellisés a et b. Les deux ports de sortie portent quant à eux les labels c et d. Pour l'une des réflexions, la lumière est assujettie à un saut de phase de π représenté ici par un signe moins. Dans le point de vue de Heisenberg **a)**, le procédé est décrit au travers de l'évolution des opérateurs création et annihilation associés aux modes a et b en opérateurs correspondants aux modes c et d. Tandis que dans le point de vue de Schrödinger **b)**, l'action de la lame séparatrice est décrite par l'opérateur d'évolution unitaire $\hat{B}(\theta)$ agissant sur les vecteurs d'onde et couplant les deux modes de propagation a et b.

Dans une expérience réelle, les champs ont une enveloppe dépendant du temps et ils 'passent' sur la lame durant un temps fini τ correspondant au temps de cohérence des champs optiques. On peut voir le processus comme une collision de deux paquets d'onde (dont l'un peut être le vide), mélangés par la lame. Pour décrire ce processus, il convient, en toute rigueur, de considérer que chaque paquet est une superposition de modes $\vec{k}$ (opérateurs $\hat{a}_k$) répartis en fréquence sur un intervalle $c\Delta k = 1/\tau$. Une telle

approche est mathématiquement lourde, c'est pourquoi nous en proposons le traitement en annexe B.

Un modèle équivalent, et beaucoup plus simple à mettre en œuvre, consiste à décrire les champs par des ondes planes stationnaires et à 'brancher' et 'débrancher' le couplage de la lame pendant le même intervalle de temps τ autour de 0. Ceci revient à considérer que le couplage est de la forme :

$$\hat{\mathcal{H}}_{BS}(t) = -\hbar g(t) \left(\hat{a}^\dagger \hat{b} + \hat{a} \hat{b}^\dagger \right), \tag{2.58}$$

avec :

$$\int g(t)\, \mathrm{d}t = \theta, \tag{2.59}$$

où $g(t)$ est une fonction du temps de largeur de l'ordre de τ dont la forme précise n'importe pas.

Pour décrire l'évolution des champs sous l'effet du couplage avec la lame, on peut adopter deux points de vue équivalents : le point de vue de Heisenberg et le point de vue de Schrödinger. Dans le point de vue de Heisenberg, on considère que le champ reste dans un état $|\psi\rangle$ indépendant du temps, alors que les opérateurs champ évoluent, passant de leur état initial à leur état final en un temps τ. En utilisant les opérateurs unitaires $\hat{B}(\theta) = e^{i\theta\left(\hat{a}^\dagger \hat{b} + \hat{a}\hat{b}^\dagger\right)}$ et $\hat{B}^\dagger(\theta)$, l'évolution peut ainsi être exprimée comme :

$$\begin{pmatrix} \hat{c} \\ \hat{d} \end{pmatrix} = \mathbf{B} \begin{pmatrix} \hat{a} \\ \hat{b} \end{pmatrix} = \hat{B} \begin{pmatrix} \hat{a} \\ \hat{b} \end{pmatrix} \hat{B}^\dagger \qquad \text{et} \qquad \mathbf{B}^* \begin{pmatrix} \hat{a} \\ \hat{b} \end{pmatrix} = \hat{B}^\dagger \begin{pmatrix} \hat{a} \\ \hat{b} \end{pmatrix} \hat{B}, \tag{2.60}$$

ou plus simplement :

$$\begin{cases} \hat{B}(\theta) \hat{a} \hat{B}^\dagger(\theta) = \hat{a} \cos\theta + i\hat{b} \sin\theta, \\ \hat{B}(\theta) \hat{b} \hat{B}^\dagger(\theta) = \hat{b} \cos\theta + i\hat{a} \sin\theta. \end{cases} \tag{2.61}$$

De manière alternative, le point de vue de Schrödinger considère au contraire que les opérateurs sont indépendants du temps et que c'est l'état du système qui évolue sous l'effet de l'opérateur d'évolution : $|\psi_{out}\rangle = \hat{B} |\psi_{in}\rangle$. Nous adopterons dans ce qui suit le point de vue de Schrödinger, sauf lorsqu'il sera question de traiter le cas de l'interférence à deux photons où nous aurons alors recourt aux deux représentations. Notons enfin que les deux points de vue sont parfaitement équivalents quant aux prévisions physiques.

2.4.2. Lame séparatrice avec arrivée du champ sur un seul port d'entrée

Commençons par considérer que seul le mode (a) est initialement excité, le mode (b) étant vide, et ce pour différentes situation illustrées en FIGURE 2.5.

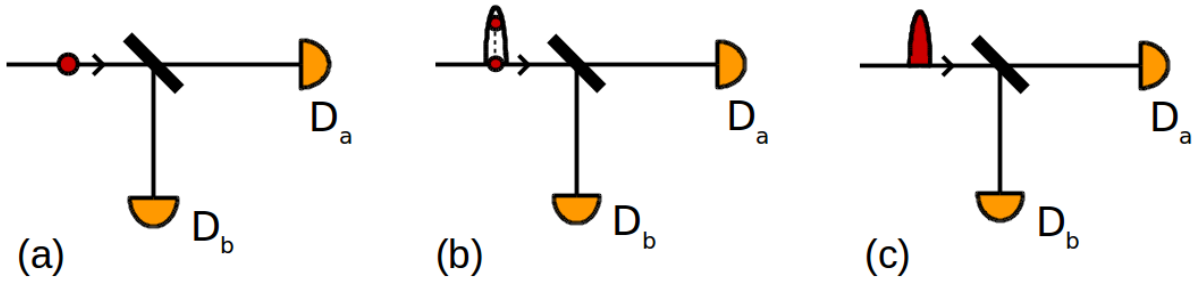


Figure 2.5. – Lame séparatrice avec arrivée du champ sur un seul port d'entrée. **a)** Cas où le champ entrant est un état de Fock à un photon ; **b)** Cas où le champ entrant est un état de Fock à n photons ; **c)** Cas où le champ entrant est un état cohérent.

État initial : état de Fock à un photon sur un mode d'entrée

$$
\begin{aligned}
|1_a, 0_b\rangle \to |\psi\rangle &= \hat{B}(\theta)\,|1_a, 0_b\rangle && (2.62)\\
&= \hat{B}(\theta)\hat{a}^\dagger\,|0_a, 0_b\rangle && (2.63)\\
&= \hat{B}(\theta)\hat{a}^\dagger\hat{B}^\dagger(\theta)\,|0_a, 0_b\rangle && (2.64)\\
&= \left(\hat{a}^\dagger\cos\theta + i\hat{b}^\dagger\sin\theta\right)|0_a, 0_b\rangle && (2.65)\\
&= \cos\theta\,|1_a, 0_b\rangle + i\sin\theta\,|0_a, 1_b\rangle\,. && (2.66)
\end{aligned}
$$

La lame place le photon dans une superposition d'états en sortie : il est 'suspendu' de façon cohérente entre les deux modes (a) et (b), voir FIGURE 2.5a.

État initial : état de Fock à n photons sur un mode d'entrée

$$
\begin{aligned}
|n_a, 0_b\rangle \to |\psi\rangle &= \hat{B}(\theta)\,|n_a, 0_b\rangle && (2.67)\\
&= \hat{B}(\theta)\frac{\left(\hat{a}^\dagger\right)^n}{\sqrt{n!}}\,|0_a, 0_b\rangle && (2.68)\\
&= \frac{1}{\sqrt{n!}}\hat{B}(\theta)\left(\hat{a}^\dagger\right)^n\hat{B}^\dagger(\theta)\,|0_a, 0_b\rangle && (2.69)\\
&= \frac{1}{\sqrt{n!}}\left(\hat{a}^\dagger\cos\theta + i\hat{b}^\dagger\sin\theta\right)^n|0_a, 0_b\rangle && (2.70)\\
&= \sum_{p=0}^{n}\binom{n}{p}^{1/2}(\cos\theta)^{n-p}\,(\sin\theta)^p\,|(n-p)_a, p_b\rangle\,. && (2.71)
\end{aligned}
$$

Il y a une répartition binomiale des photons dans les deux modes en sortie de la lame. Si $\theta = \pi/4$ (lame semi-réfléchissante), il y a alors en moyenne $n/2$ photons dans chaque mode, avec une fluctuation Poissonnienne en $\sqrt{n/2}$, voir FIGURE 2.5b.

État initial : état cohérent sur un mode d'entrée

$$|\alpha_a, 0_b\rangle \to |\psi\rangle = \hat{B}(\theta)\,|\alpha_a, 0_b\rangle \tag{2.72}$$
$$= \hat{B}(\theta) e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}} \hat{B}^\dagger(\theta)\,|0_a, 0_b\rangle \tag{2.73}$$
$$= e^{\alpha\left(\hat{a}^\dagger \cos\theta + i\hat{b}^\dagger \sin\theta\right) - \alpha^*\left(\hat{a}\cos\theta - i\hat{b}\sin\theta\right)}\,|0_a, 0_b\rangle \tag{2.74}$$
$$= |\alpha\cos\theta\rangle_a\,|i\alpha\sin\theta\rangle_b\,. \tag{2.75}$$

Il y a répartition des amplitudes, sans intrication, sur les deux modes. Si $\theta = \pi/4$, on a encore en moyenne $n/2$ photons dans chaque mode, avec une fluctuation Poissonnienne en $\sqrt{n/2}$, voir FIGURE 2.5c.

2.4.3. Lame séparatrice avec arrivée du champ sur les deux ports d'entrée

Point de vue de Schrödinger

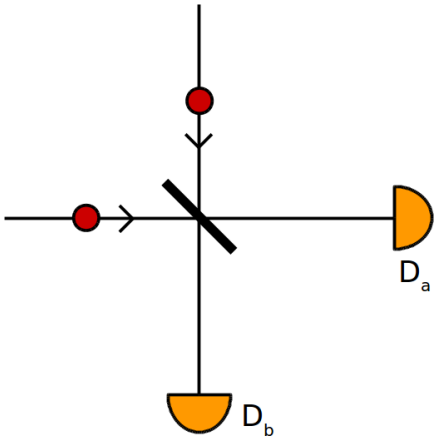


Figure 2.6. – Lame séparatrice avec un photon sur chaque port d'entrée.

Comme le montre la FIGURE 2.6, envisageons maintenant le cas simple ou chacun des modes (a) et (b) contient un photon. Nous avons :

$$|1_a, 1_b\rangle \rightarrow |\psi\rangle = \hat{B}(\theta)\,|1_a, 1_b\rangle \tag{2.76}$$
$$= \hat{B}(\theta)\hat{a}^\dagger\hat{b}^\dagger\hat{B}^\dagger(\theta)\,|0_a, 0_b\rangle \tag{2.77}$$
$$= \left(\hat{a}^\dagger\cos\theta + i\hat{b}^\dagger\sin\theta\right)\left(i\hat{a}^\dagger\sin\theta + \hat{b}^\dagger\cos\theta\right)|0_a, 0_b\rangle \tag{2.78}$$
$$= i\sin 2\theta\left(\frac{|2_a, 0_b\rangle + |0_a, 2_b\rangle}{\sqrt{2}}\right) + \cos 2\theta\,|1_a, 1_b\rangle\,. \tag{2.79}$$

Dans le cas particulier où la lame séparatrice est semi réfléchissante ($\theta = \pi/4$), nous obtenons :

$$|1_a, 1_a\rangle \rightarrow |\psi\rangle = \frac{|2_a, 0_b\rangle + |0_a, 2_b\rangle}{\sqrt{2}}. \tag{2.80}$$

Les deux photons sont suspendus, on est en présence d'une superposition de deux photons dans une voie et dans l'autre. La probabilité de répartir un photon dans chaque voie est nulle dans ce cas. Nous montrons plus loin comment tester expérimentalement un tel état par le biais d'un dispositif d'interférence à deux photons.

Point de vue de Heisenberg

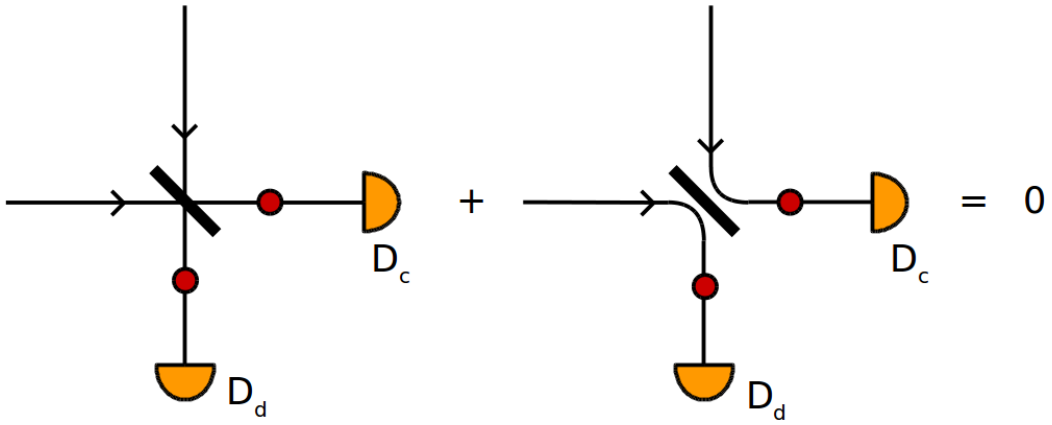


Figure 2.7. – Phénomène d'interférence à deux photons.

L'analyse dans le point de vue de Schrödinger nous a montré que le taux de détection double est nul, puisque le système évolue vers l'état $|\psi\rangle = (|2_a, 0_b\rangle + |0_a, 2_b\rangle)/\sqrt{2}$ (pas de composante $|1_a, 1_b\rangle$). Il est instructif de reprendre la question avec le point de vue de Heisenberg. En appelant $\hat{c}$ et $\hat{d}$ les expressions finales des opérateurs $\hat{a}$ et $\hat{b}$ qui dépendent dans ce point de vue du temps, le taux de coïncidences C_{cd} entre les détecteurs D_c et D_d s'écrit alors :

$$C_{cd} \propto \langle 1_a, 1_b | \hat{c}^\dagger \hat{d}^\dagger \hat{d}\hat{c} | 1_a, 1_b \rangle = | \langle 0_a, 0_b | \hat{d}\hat{c} | 1_a, 1_b \rangle |^2 \tag{2.81}$$

$$= \frac{1}{2} | \langle 0_a, 0_b | (i\hat{a} + \hat{b})(\hat{a} + i\hat{b}) | 1_a, 1_b \rangle |^2 \tag{2.82}$$

$$= \frac{1}{2} | \langle 0_a, 0_b | (i\hat{a})(i\hat{b}) + \hat{b}\hat{a} | 1_a, 1_b \rangle |^2 \tag{2.83}$$

$$= 0. \tag{2.84}$$

Il y a interférence destructive de l'amplitude du chemin où le photon (a) est détecté par D_c et le photon (b) par D_d avec le processus croisé, c'est le phénomène d'interférence à deux photons, encore appelé effet de coalescence à la Hong-Ou-Mandel [255], voir FIGURE 2.7.

Franges d'interférence spatiale à deux photons

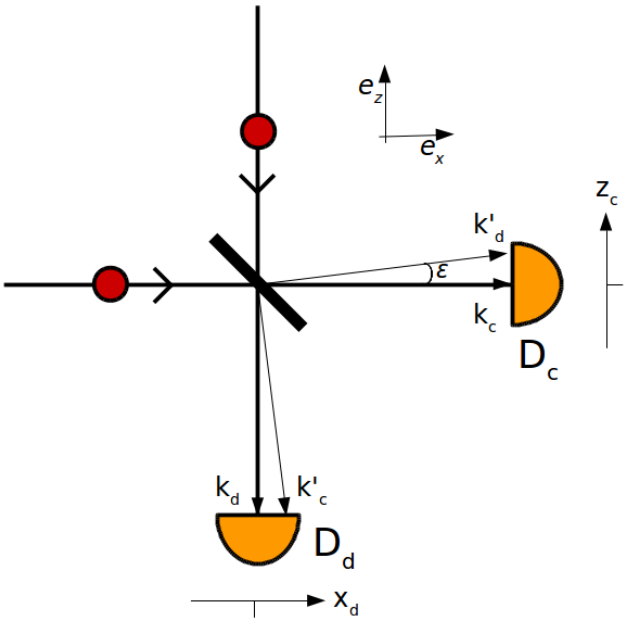


Figure 2.8. – Franges d'interférences spatiales à deux photons [255].

On suppose la lame tournée d'un angle $\varepsilon/2$ par rapport à la direction de 45° comme dans la proposition originelle de Hong-Ou-Mandel [255]. Le faisceau réfléchi de (b) a un vecteur d'onde $\vec{k'}_d = \vec{k}_c + \varepsilon k \vec{e}_z$ et et le faisceau réfléchi de (a) un vecteur d'onde $\vec{k'}_c = \vec{k}_d + \varepsilon k \vec{e}_x$, voir FIGURE 2.8 où les vecteurs sont notés en gras et où k désigne le module du vecteur d'onde. L'expression du taux de coïncidences s'exprime à partir de (2.82) comme :

$$C_{cd} \propto \left| \langle 0_a, 0_b | \left(i\hat{a}e^{i\vec{k}'_c\cdot\vec{r}_d} + \hat{b}e^{i\vec{k}_d\cdot\vec{r}_d} \right) \left(\hat{a}e^{i\vec{k}_c\cdot\vec{r}_c} + i\hat{b}e^{i\vec{k}'_d\cdot\vec{r}_c} \right) | 1_a, 1_b \rangle \right|^2 \tag{2.85}$$

$$= \left| \langle 0_a, 0_b | \left(\hat{b}\hat{a}e^{i(\vec{k}_d\cdot\vec{r}_d + \vec{k}_c\cdot\vec{r}_c)} - \hat{a}\hat{b}e^{i(\vec{k}'_c\cdot\vec{r}_d + \vec{k}'_d\cdot\vec{r}_c)} \right) | 1_a, 1_b \rangle \right|^2 \tag{2.86}$$

$$= \left| e^{i(\vec{k}_d\cdot\vec{r}_d + \vec{k}_c\cdot\vec{r}_c)} - e^{i(\vec{k}'_c\cdot\vec{r}_d + \vec{k}'_d\cdot\vec{r}_c)} \right|^2 \tag{2.87}$$

$$= \left| 1 - e^{i\left[(\vec{k}'_c - \vec{k}_d)\cdot\vec{r}_d + (\vec{k}'_d - \vec{k}_c)\cdot\vec{r}_c\right]} \right|^2 \tag{2.88}$$

$$= \frac{1 - \cos\left[\varepsilon k(z_c + x_d)\right]}{2}. \tag{2.89}$$

On a bien $C_{cd} = 0$ pour $\varepsilon = 0$. Les coordonnées x_d et z_c décrivent des translations horizontales et verticales respectivement des détecteurs D_d et D_c, voir FIGURE 2.8. On observe dans le courant de photo-détection double des interférences de contraste 100% lorsqu'on déplace D_d (D_c restant fixe) ou D_c (D_d restant fixe). L'interfrange $\delta = 2\pi/\varepsilon k$ devient infini pour $\varepsilon = 0$. Cette interférence implique que si un photon est détecté à la position z_c alors il existe des positions x_d où l'autre photon ne peut être trouvé. Cette impossibilité résulte de l'interférence destructrice entre deux amplitudes impliquant chacune les deux photons. Il n'y a pas d'interférence dans le courant de photo-détection simple.

On a ici décrit le cas idéal et non réaliste d'un signal indépendant du temps (modes monochromatiques), en pratique les deux photons utilisés dans ce type d'expérience sont en général produits par conversion paramétrique spontanée dans un cristal non-linéaire, et possèdent dès lors un spectre polychromatique, voir section 2.5.1.

Dès lors, plutôt que de venir jouer sur la position des détecteurs, il est possible de manière totalement analogue d'obtenir la signature de l'interférence à deux photons en appliquant un délai variable sur le trajet de l'un des deux photons de sorte à jouer sur le recouvrement des modes, non plus spatial mais cette fois-ci temporel, au niveau de la lame séparatrice. Ceci représente une méthode beaucoup plus pratique à mettre en œuvre expérimentalement et que nous détaillons en annexe B.

2.4.4. Interféromètre de Mach-Zehnder avec un seul photon en entrée

On s'intéresse désormais au cas d'un interféromètre de Mach-Zehnder, dispositif avec deux lames séparatrices semi-réfléchissantes ($\theta_1 = \theta_2 = \pi/4$) et deux miroirs pour séparer le faisceau (a) en deux parties (a) et (b) et les recombiner ensuite, voir FIGURE 2.9. Une lame retardatrice déphase la voie (b) d'un angle φ variable. On peut détecter le champ dans les deux voies finales avec deux détecteurs compteurs de photons.

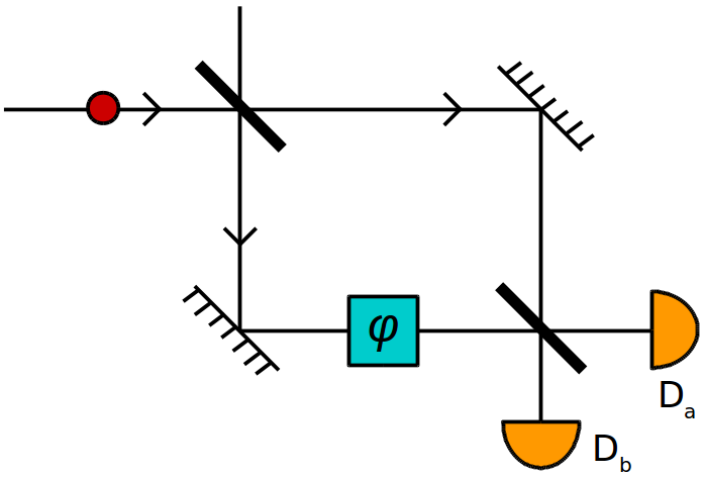


Figure 2.9. – Interféromètre de Mach-Zehnder avec un photon incident sur un port d'entrée.

Dans le cas où un seul photon se présente à la première lame séparatrice, disons dans le mode (a), l'état initial subit tout d'abord l'action de la première lame séparatrice :

$$|1_a, 0_b\rangle \to \frac{|1_a, 0_b\rangle + i\,|0_a, 1_b\rangle}{\sqrt{2}}, \tag{2.90}$$

suivi de l'action de la lame à retard de phase dans la voie du bas :

$$\frac{|1_a, 0_b\rangle + i\,|0_a, 1_b\rangle}{\sqrt{2}} \to \frac{|1_a, 0_b\rangle + ie^{i\varphi}\,|0_a, 1_b\rangle}{\sqrt{2}}, \tag{2.91}$$

et enfin de la seconde lame séparatrice :

$$\begin{aligned}\frac{|1_a, 0_b\rangle + ie^{i\varphi}\,|0_a, 1_b\rangle}{\sqrt{2}} \to \frac{|1_a, 0_b\rangle + i\,|0_a, 1_b\rangle}{2} + ie^{i\varphi}\frac{|0_a, 1_b\rangle + i\,|1_a, 0_b\rangle}{2} \\ = \frac{1 - e^{i\varphi}}{2}\,|1_a, 0_b\rangle + \frac{1 + e^{i\varphi}}{2}\,|0_a, 1_b\rangle\,.\end{aligned} \tag{2.92}$$

Si l'on s'intéresse désormais au comptage de photons sur les différentes sorties de l'interféromètre en notant respectivement S_a et S_b le taux de photons détectés sur les sorties (a) et (b), on a :

$$S_a \propto \langle\psi|\,\hat{a}^\dagger\hat{a}\,|\psi\rangle = \langle\psi|\,\hat{a}^\dagger\,|0_a, 0_b\rangle\,\langle 0_a, 0_b|\,\hat{a}\,|\psi\rangle = |\langle 0_a, 0_b|\,\hat{a}\,|\psi\rangle|^2 = \frac{1 - \cos\varphi}{2}, \tag{2.93}$$

et

$$S_b \propto \frac{1+\cos\varphi}{2}. \tag{2.94}$$

Le taux de comptage est indépendant du temps pour ce problème stationnaire. Le photon est détecté dans la voie (a) avec la probabilité $(1-\cos\varphi)/2$ et il peut arriver n'importe quand. En fait dans l'intervalle τ correspondant à la largeur de son paquet d'onde. Pour citer Paul Dirac, le photon ne peut 'interférer qu'avec lui-même'. En d'autres termes, les deux chemins qu'il suit ont des amplitudes de probabilité qui interfèrent.

2.4.5. Interféromètre de Mach-Zehnder avec n photons sur un port d'entrée

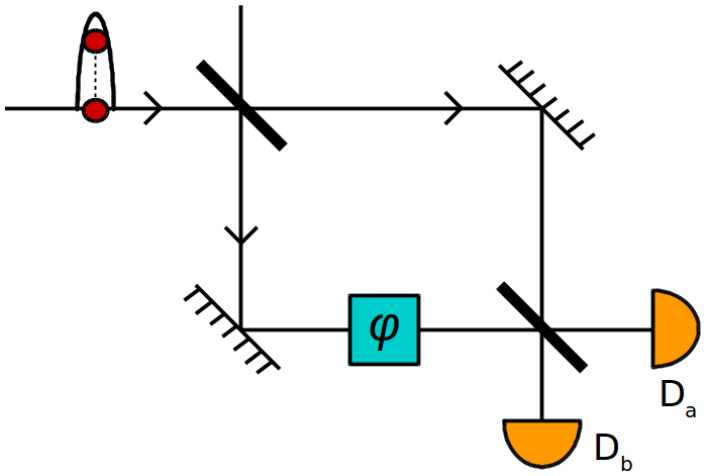


Figure 2.10. – Interféromètre de Mach-Zehnder avec n photons incident sur le même port d'entrée.

Si l'état initial est un état de Fock à n photons incident sur un seul port, voir Figure 2.10, un calcul très semblable donne pour l'état final du champ :

$$|n_a, 0_b\rangle \to \frac{1}{\sqrt{n!}}\left[\left(\frac{1-e^{i\varphi}}{2}\right)\hat{a}^\dagger + \left(\frac{1+e^{i\varphi}}{2}\right)\hat{b}^\dagger\right]^n |0_a, 0_b\rangle\,. \tag{2.95}$$

Cela revient à reproduire n fois l'expérience avec un photon. À la sortie de l'interféromètre, les photons se répartissent sur les detecteurs (a) et (b) selon les probabilités respectives $p = (1-\cos\varphi)/2$ et $q = 1-p$. Le signal détecté par comptage est proportionnel au nombre moyen de photons, soit $(n/2)(1-\cos\varphi)$ dans (a) et $(n/2)(1+\cos\varphi)$ dans (b). Le signal a la même forme que dans le cas à un seul photon.

La fluctuation de S_a est donnée par l'expression habituelle de la variance $\Delta\hat{n}_a = \sqrt{\langle n_a^2\rangle - \langle n_a\rangle^2}$, avec $\hat{n}_a = \hat{a}^\dagger\hat{a}$. Elle est immédiate à évaluer par la loi binomiale :

$$\Delta\hat{n}_a = \sqrt{npq} = \frac{\sqrt{n(1-(\cos\varphi)^2)}}{2} = \frac{\sqrt{n}\sin\varphi}{2}. \tag{2.96}$$

La sensibilité η de l'interféromètre est définie comme l'inverse du plus petit déphasage $(\delta\varphi)_{min}$ détectable. Elle dépend de la 'pente' des franges $\delta S_a/\delta\varphi$ ainsi que de la variation minimale de signal observable $(\delta S_a)_{min} = \Delta\hat{n}_a$:

$$\frac{\delta S_a}{\delta\varphi} = \frac{n\sin\varphi}{2}, \qquad \eta = \frac{1}{(\delta\varphi)_{min}} = \frac{\delta S_a/\delta\varphi}{(\delta S_a)_{min}} = \frac{\delta S_a/\delta\varphi}{\Delta\hat{n}_a} = \sqrt{n}. \tag{2.97}$$

On voit que la sensibilité η est égale à la racine du nombre de photons traversant l'appareil pendant le temps de mesure. On retrouverait essentiellement le même résultat avec un champ cohérent. L'interféromètre se comporte de la même façon avec un état de Fock (pas de phase) ou avec un champ cohérent (de phase définie).

2.4.6. Détection par battement homodyne des quadratures du champ

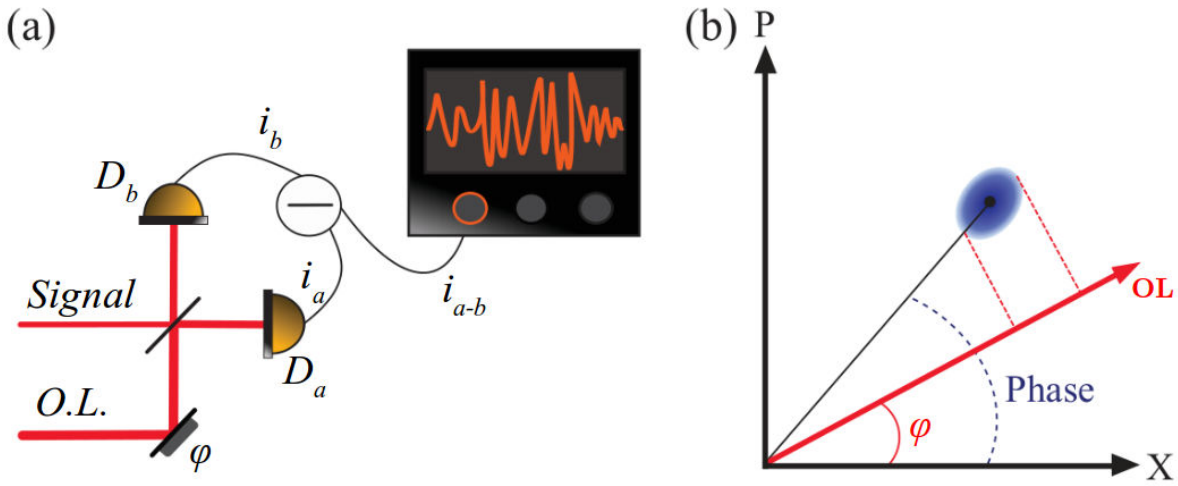


Figure 2.11. – **a)** Schéma expérimental de la détection homodyne. **b)** Détection homodyne dans l'espace des phases : l'état signal est projeté sur l'oscillateur local (OL). En scannant continûment la phase de l'OL, il est possible de reconstruire l'ensemble des quadratures du champ signal.

Traitons maintenant le cas du couplage par une lame de transmission $T = |t|^2$ d'un champ 'signal' avec un champ de référence dans un état cohérent $|\alpha\rangle = |\alpha_0 e^{i\varphi}\rangle$ que l'on

nomme traditionnellement oscillateur local (OL), voir FIGURE 2.11. En toute généralité, le champ 'signal' que l'on cherche à mesurer étant inconnu, on le décrira à l'aide d'un opérateur densité $\hat{\rho}_s$. La mesure du courant de photo-détection transmis dans le mode (a) se calcule de la manière suivante :

$$\begin{aligned} i_a \propto \mathrm{Tr}\left\{\hat{\rho}_s\,|\alpha\rangle\langle\alpha|\left(\hat{a}^\dagger\cos\theta - i\hat{b}^\dagger\sin\theta\right)\left(\hat{a}\cos\theta + i\hat{b}\sin\theta\right)\right\} \\ = (\sin\theta)^2\,\langle\alpha|\,\hat{b}^\dagger\hat{b}\,|\alpha\rangle + (\cos\theta)^2\,\mathrm{Tr}\left\{\hat{\rho}_s\hat{a}^\dagger\hat{a}\right\} \\ + i\,(\sin\theta\cos\theta)\,\mathrm{Tr}\left\{\hat{\rho}_s\,|\alpha\rangle\langle\alpha|\left(\hat{a}^\dagger\hat{b} - \hat{a}\hat{b}^\dagger\right)\right\}. \quad (2.98) \end{aligned}$$

Ce qui, en utilisant la relation $t = \cos\theta$, voir 2.4.1, se réécrit :

$$i_a \propto (1-T)\alpha_0^2 + T\langle\hat{a}^\dagger\hat{a}\rangle_s + i\sqrt{1-T}\alpha_0\left(\langle\hat{a}^\dagger\rangle_s e^{i\varphi} - \langle\hat{a}\rangle_s e^{-i\varphi}\right). \quad (2.99)$$

Le premier terme s'interprète comme étant l'intensité réflechie de l'oscillateur local (fond fixe), le second terme comme l'intensité transmise du signal, et le dernier terme comme le battement entre l'oscillateur local et le signal. Le même calcul sur la voie (b) conduit à :

$$i_b \propto T\alpha_0^2 + (1-T)\langle\hat{b}^\dagger\hat{b}\rangle_s - i\sqrt{1-T}\alpha_0\left(\langle\hat{b}^\dagger\rangle_s e^{i\varphi} - \langle\hat{b}\rangle_s e^{-i\varphi}\right), \quad (2.100)$$

où le changement de signe sur le dernier terme provient du déphasage introduit par la lame séparatrice.

Dans le cas d'une lame semi-réfléchissante ($T = 1/2 \Leftrightarrow \theta = \pi/4$), la soustraction des deux photo-courants i_a et i_b permet de conserver uniquement le terme de battement :

$$i_{a-b} = i_a - i_b = 2i\sqrt{1-T}\alpha_0\left(\langle\hat{a}^\dagger\rangle_s e^{i\varphi} - \langle\hat{a}\rangle_s e^{-i\varphi}\right), \quad (2.101)$$

où l'on a utilisé le fait que $\langle\hat{a}^\dagger\hat{a}\rangle_s = \langle\hat{b}^\dagger\hat{b}\rangle_s$. Enfin, en retravaillant quelque peu l'équation précédente, on s'aperçoit qu'il est possible de faire apparaître l'opérateur quadrature :

$$i_{a-b} \propto \alpha_0\frac{\langle\hat{a}^\dagger e^{i\varphi} - \hat{a}e^{-i\varphi}\rangle_s}{2i} = \alpha_0\langle\hat{X}_{\varphi+\pi/2}\rangle_s. \quad (2.102)$$

On mesure ainsi la quadrature du champ en avance de $\pi/2$ sur la phase du champ cohérent de référence, voir FIGURE 2.11. En variant cette phase, on peut alors mesurer n'importe quelle quadrature. Finalement, on voit au travers de l'expression obtenue que plus le champ cohérent est intense, plus la mesure de la quadrature devient simple. Nous avons en effet traité ici un cas idéal, mais en pratique il faut être capable d'extraire le signal du bruit électronique associés aux appareils de mesures (photodiodes, analyseurs de spectre, amplificateurs, etc.).

2.5. Interférences non-linéaires

2.5.1. Conversion paramétrique non-dégénérée

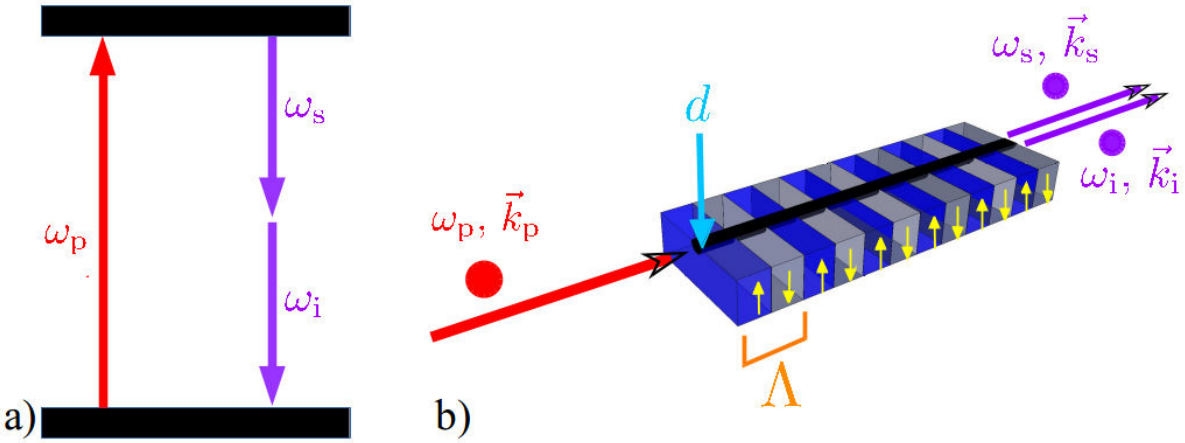


Figure 2.12. – **a)** Principe du processus de conversion paramétrique spontanée. Un photon de pompe de fréquence ω_p et de vecteur d'onde $\vec{k}_p$ est converti en deux photons de fréquences ω_s et ω_i et de vecteurs d'ondes $\vec{k}_s$ et $\vec{k}_i$. Le cas spécifique de longueurs d'onde dégénérées est ici représenté : $\omega_p := 2\omega$ et $\omega_s = \omega_i = \omega$. **b)** Schéma d'un guide d'ondes inscrit sur un matériau non linéaire d'ordre 2 périodiquement polarisé fonctionnant dans le régime de SPDC. Un photon de pompe entrant, caractérisé par une fréquence ω_p et un moment $\vec{k}_p$ est converti en une paire de photons (ω_s, $\vec{k}_s$; ω_i, $\vec{k}_i$). Afin d'augmenter l'efficacité de ce procédé, il est d'usage d'avoir recours à un guide d'ondes qui maintient des densités d'énergie de champ lumineux élevées sur quelques cm de longueur. Afin de permettre de trouver la condition d'accord de phase pour le processus à trois photons en question, la polarisation ferroélectrique du cristal est inversée de manière répétée (période d'inversion Λ) le long de l'axe de propagation de la lumière. Cette technique porte le nom de quasi accord de phase (QPM). Le QPM est principalement influencé par la période d'inversion tandis que le diamètre du guide d'onde (d) et la température du cristal permettent de faire des ajustements fins.

L'une des interactions les plus communes en optique non-linéaire consiste à convertir un photon de pompe (p) de fréquence 2ω en deux photons de fréquence ω communément appelés photon *signal* (s) et photon *idler* (i). Ce processus se produit en présence d'un milieu présentant une susceptibilité non-linéaire d'ordre deux $\bar{\bar{\chi}}^{(2)}$ et lorsque sont simultanément satisfaites les conditions de conservation de l'énergie et d'accord de phase :

$$\begin{cases} \omega_p = \omega_s + \omega_i \\ \vec{k}_p = \vec{k}_s + \vec{k}_i \end{cases} \Leftrightarrow \begin{cases} \omega_p = \omega_s + \omega_i \\ n(\omega_p) \cdot \omega_p = n(\omega_s) \cdot \omega_s + n(\omega_i) \cdot \omega_i \end{cases} \tag{2.103}$$

En pratique, l'indice de propagation du milieu, $n(\omega_j)$ $(j = i, s, p)$, dépend de la fréquence du champ optique. Satisfaire ces deux relations à la fois n'est donc possible qu'en présence de milieux biréfringents et/ou en inversant, à intervalles réguliers lors de la fabrication du cristal, la polarisation non-linéaire du matériau, une technique connue sous le nom de quasi-accord de phase, voir FIGURE 2.12b.

Le procédé de conversion paramétrique spontanée (*Spontaneous Parametric Down Conversion* - SPDC) permet en optique quantique de décrire un amplificateur paramétrique. Afin de décrire l'évolution du nombre de photons dans les modes de pompe (p), signal (s) et idler (i), nous considérons ici un modèle simple où le champ de pompe à la fréquence ω_p est traité classiquement par un champ complexe $v_p e^{-i\omega_p t}$ d'amplitude v_p, tandis que les champs signal et idler sont traités au travers des opérateurs création et annihilation $\hat{a}^\dagger_{s,i}$ et $\hat{a}_{s,i}$. L'expression du Hamiltonien décrivant l'interaction est ainsi donnée par :

$$\hat{\mathcal{H}}_{SPDC}(t) = \sum_{j=s,i} \hbar\omega_j \left(\hat{a}^\dagger_j \hat{a}_j + \frac{1}{2}\right) + i\hbar g \left(\hat{a}^\dagger_s \hat{a}^\dagger_i e^{-i\omega_p t} - \hat{a}_s \hat{a}_i e^{+i\omega_p t}\right), \tag{2.104}$$

où g est un terme de couplage proportionnel à la susceptibilité non-linéaire d'ordre 2 et à l'amplitude v_p de la pompe. Si l'on se place dans le point de vue de Dirac (représentation d'interaction), un point de vue intermédiaire entre le point de vue de Schrödinger et celui de Heisenberg, on peut alors travailler avec un Hamiltonien indépendant du temps :

$$\hat{\mathcal{H}}^I_{SPDC} = i\hbar g \left(\hat{a}^\dagger_s \hat{a}^\dagger_i - \hat{a}_s \hat{a}_i\right). \tag{2.105}$$

Se placer dans la représentation d'interaction peut s'interpréter comme de travailler dans un référentiel tournant à la fréquence $\omega_p/2$. Les équations de Heisenberg pour les observables s'écrivent alors :

$$\begin{cases} \dfrac{\mathrm{d}\hat{a}_s}{\mathrm{d}t} = \dfrac{1}{i\hbar}\left[\hat{a}_s, \hat{\mathcal{H}}^I_{SPDC}\right] = g\hat{a}^\dagger_i, \\ \dfrac{\mathrm{d}\hat{a}^\dagger_i}{\mathrm{d}t} = \dfrac{1}{i\hbar}\left[\hat{a}^\dagger_i, \hat{\mathcal{H}}^I_{SPDC}\right] = g\hat{a}_s. \end{cases} \tag{2.106}$$

Elles admettent pour solutions :

$$\begin{cases} \hat{a}_s(t) = \hat{a}_s(0)\cosh(gt) + \hat{a}^\dagger_i(0)\sinh(gt), \\ \hat{a}_i(t) = \hat{a}_i(0)\cosh(gt) + \hat{a}^\dagger_s(0)\sinh(gt). \end{cases} \tag{2.107}$$

À partir de ces expressions et sachant que seul le champ de pompe est injecté, et donc que les modes signal et idler sont initialement inoccupés, il est alors facile de calculer le nombre moyen de photons contenus dans les modes signal et idler à un instant t :

$$\left\langle \hat{N}_j(t) \right\rangle_{j=s,i} = \langle 0,0|\, \hat{a}^\dagger_j \hat{a}_j \,|0,0\rangle = \sinh^2(gt). \tag{2.108}$$

Nous constatons que $\left\langle \hat{N}_j(t) \right\rangle$ est non nul, ainsi, bien que les modes signal et idler soient initialement non peuplés, il est toujours possible d'initier le processus. Cela traduit le fait que les fluctuations quantiques du vide fournissent un champ effectif en entrée d'une intensité suffisante pour initier la conversion paramétrique de la pompe vers les modes signal et idler.

Afin d'étudier la statistique d'émission des photons, nous nous plaçons désormais dans la représentation de Schrödinger afin de décrire l'évolution temporelle des fonctions d'ondes :

$$|\psi(t)\rangle = e^{-\frac{i}{\hbar}\hat{\mathcal{H}}^I_{SPDC}t} |\psi(0)\rangle \,, \tag{2.109}$$

avec $\hat{\mathcal{H}}^I_{SPDC}$ le Hamiltonien d'interaction de l'équation (2.105) pour un processus monochromatique. L'état du système après un temps t s'érit alors :

$$|\psi(t)\rangle = e^{g\left(\hat{a}_s^\dagger \hat{a}_i^\dagger - \hat{a}_s \hat{a}_i\right)t} |\psi(0)\rangle \,, \tag{2.110}$$

À l'aide du théorème suivant :

$$e^{\alpha\left(\hat{a}_1^\dagger \hat{a}_2^\dagger - \hat{a}_1 \hat{a}_2\right)} = e^{\Gamma \hat{a}_1^\dagger \hat{a}_2^\dagger} e^{-\Omega\left(\hat{a}_1^\dagger \hat{a}_2^\dagger - \hat{a}_1 \hat{a}_2\right)} e^{-\Gamma \hat{a}_1 \hat{a}_2}, \tag{2.111}$$

où α est une constante, $\Gamma = \tanh(\alpha)$ et $\Omega = \ln(\cosh(\alpha))$, et du développement en série de Taylor de la fonction exponentielle, nous aboutissons à :

$$|\psi(t)\rangle = \frac{1}{\cosh(gt)} \sum_{n=0}^{\infty} \tanh^n(gt) \, |n, n\rangle \,. \tag{2.112}$$

Calculons à présent la matrice densité associée au mode signal (ou au mode idler) :

$$\hat{\rho}_{s(i)}(t) = \mathrm{Tr}_{i(s)} \left\{ |\psi(t)\rangle\langle\psi(t)| \right\} = \frac{1}{\cosh^2(gt)} \sum_{n=0}^{\infty} \tanh^{2n}(gt) \, |n\rangle\langle n| \,. \tag{2.113}$$

Ainsi, la probabilité de créer n photons dans un mode suit une loi géométrique :

$$P_n = \frac{\tanh^{2n}(gt)}{\cosh^2(gt)}, \tag{2.114}$$

ce qui est caractéristique des distributions de type Bose-Einstein. Ainsi, une source paramétrique n'ayant qu'un mode d'émission présentera une statistique d'émission de type Bose-Einstein.

Nous avons jusqu'à présent considéré que le processus de conversion paramétrique spontanée donnait naissance à deux photons signal et idler parfaitement monochromatiques. Nous levons désormais cette restriction afin d'étudier la statistique d'émission

en fonction de la largeur spectrale des photons. Supposons maintenant que notre source possède un grand nombre N de modes possibles pour le signal et l'idler, notés s_m et i_m. Le Hamiltonien d'interaction s'écrit alors :

$$\hat{\mathcal{H}}^I_{SPDC} = i\hbar\, g \sum_{m=1}^{N} \left(\hat{a}^\dagger_{s_m} \hat{a}^\dagger_{i_m} - \hat{a}_{s_m} \hat{a}_{i_m} \right).$$

Il faut noter que les opérateurs d'indices m différents commutent, $\left[\hat{a}_{s_m}, \hat{a}^\dagger_{s_n}\right] = \left[\hat{a}_{i_m}, \hat{a}^\dagger_{i_n}\right] = \delta_{m,n}$ ce qui nous permet d'écrire l'état du système comme le produit tensoriel de N états identiques à celui que l'on vient de considérer :

$$|\psi(t)\rangle = \prod_{m=1}^{N} \left[\frac{1}{\cosh(gt)} \sum_{n_m=0}^{\infty} \tanh^{n_m}(gt) |n_m, n_m\rangle \right].$$

Pour voir simplement ce qu'il se passe, restreignons nous aux états à 0, 1 et 2 photons répartis dans m modes. Il vient :

$$|\psi(t)\rangle = \prod_{m=1}^{N} \left[\frac{1}{\cosh(b)} \left(|0_m, 0_m\rangle + \tanh(gt)|1_m, 1_m\rangle + \tanh^2(gt)|2_m, 2_m\rangle + \ldots \right) \right].$$

$$\begin{aligned}
|\psi(t)\rangle \;=\; & \frac{1}{\cosh^N(gt)} \Big[|0_1, 0_1\rangle \ldots |0_N, 0_N\rangle \\
& + \sum_{m=1}^{N} \tanh(gt) |0_1, 0_1\rangle \ldots |0_{m-1}, 0_{m-1}\rangle |1_m, 1_m\rangle |0_{m+1}, 0_{m+1}\rangle \ldots |0_N, 0_N\rangle \\
& + \sum_{m=1}^{N} \tanh^2(gt) |0_1, 0_1\rangle \ldots |0_{m-1}, 0_{m-1}\rangle |2_m, 2_m\rangle |0_{m+1}, 0_{m+1}\rangle \ldots |0_N, 0_N\rangle \\
& + \sum_{m=1}^{N} \sum_{j>m}^{N} \tanh^2(gt) |0_1, 0_1\rangle \ldots |1_m, 1_m\rangle \ldots |1_j, 1_j\rangle \ldots |0_N, 0_N\rangle \Big].
\end{aligned} \tag{2.115}$$

Nous pouvons donc écrire pour un nombre de modes N grand et une efficacité totale d'interaction petite :

$$P_1 = \frac{N \tanh^2(gt)}{\cosh^{2N}(gt)} \sim N(gt)^2,$$

et :

$$P_2 = \frac{N \tanh^4(gt) + \frac{N(N-1)}{2} \tanh^4(gt)}{\cosh^{2N}(gt)} \sim \frac{N^2 (gt)^4}{2}.$$

Il vient alors simplement la relation :

$$P_2 = \frac{P_1^2}{2},$$

qui est caractéristique des sources ayant une statistique poissonnienne.

Ainsi, si nous ne pouvons pas sélectionner qu'un seul mode d'émission du guide d'onde nous obtenons des paires de photons avec une distribution de type poissonnienne, dans le cas contraire la distribution est de type Bose-Einstein. Plus précisément cela signifie, que si le temps de mesure est plus grand que le temps de cohérence des photons, nous pouvons venir sélectionner qu'un seul temps démissions. Il faut donc suffisamment filtrer les photons en sortie du cristal pour augmenter leur temps de cohérence pour qu'il soit plus grand que le jitter des détecteur, ou bien utiliser un laser en régime impulsionnel et faire en sorte que le temps de cohérence des photons soit plus grand que l'étalement temporel des impulsions.

2.5.2. Remarque sur le cas dégénéré

Dans le cas dégénéré ($\omega_s = \omega_i \equiv \omega$), le Hamiltonien d'interaction se simplifie est se réécrit comme :

$$\hat{\mathcal{H}}^I_{SPDC} = i\hbar\frac{g}{2}\left(\hat{a}^{\dagger 2} - \hat{a}^2\right). \tag{2.116}$$

Les équation de Heisenberg pour les observables s'écrivent alors :

$$\begin{cases} \dfrac{\mathrm{d}\hat{a}}{\mathrm{d}t} = \dfrac{1}{i\hbar}\left[\hat{a}, \hat{\mathcal{H}}^I_{SPDC}\right] = g\hat{a}^\dagger, \\ \dfrac{\mathrm{d}\hat{a}^\dagger}{\mathrm{d}t} = \dfrac{1}{i\hbar}\left[\hat{a}^\dagger, \hat{\mathcal{H}}^I_{SPDC}\right] = g\hat{a}, \end{cases} \tag{2.117}$$

et ont pour solution :

$$\hat{a}(t) = \hat{a}(0)\cosh(gt) + \hat{a}^\dagger(0)\sinh(gt). \tag{2.118}$$

On reconnaît ici la forme d'un générateur pour l'opération de compression avec un facteur de compression $r = gt$, voir équation (2.29).

Par conséquent, il résulte du procédé d'amplification paramétrique dégénérée un faisceau de lumière dans un état comprimé. Ceci peut immédiatement être vu en utilisant les opérateurs quadratures $\hat{X}$ et $\hat{P}$, voir expression (2.20), qui permettent de diagonaliser les équations (2.117) :

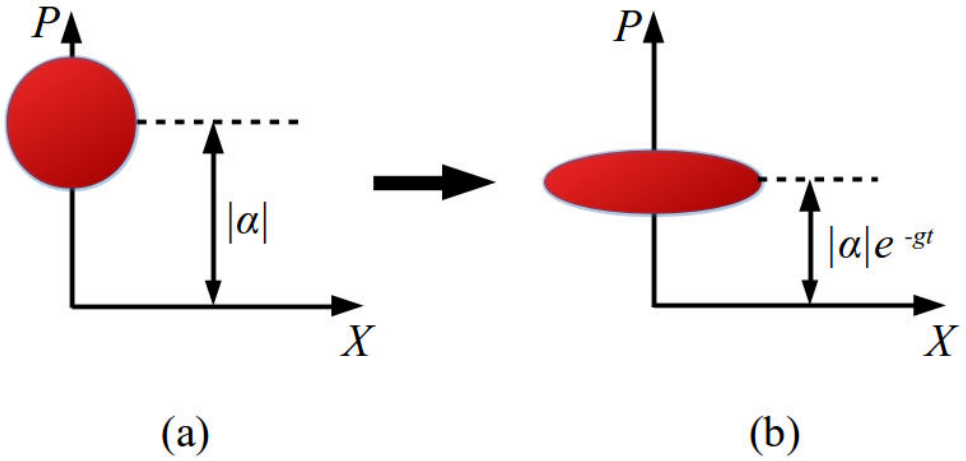


Figure 2.13. – Évolution dans l'espace des phase d'un état cohérent (a), en un état comprimé (b), par amplification paramétrique.

$$\begin{cases} \dfrac{\mathrm{d}\hat{X}}{\mathrm{d}t} = g\hat{X}, \\ \dfrac{\mathrm{d}\hat{P}}{\mathrm{d}t} = -g\hat{P}. \end{cases} \tag{2.119}$$

Ces deux dernières équations démontrent qu'un amplificateur paramétrique est un amplificateur sensible à la phase qui amplifie une quadrature et atténue la seconde :

$$\begin{cases} \hat{X}(t) = \hat{X}(0)e^{gt}, \\ \hat{P}(t) = \hat{P}(0)e^{-gt}. \end{cases} \tag{2.120}$$

Un amplificateur paramétrique réduit aussi le niveau de bruit sur $\hat{P}$ tout en augmentant celui sur $\hat{X}$. L'évolution des variances est donnée par :

$$\begin{cases} \Delta\hat{X}(t) = \Delta\hat{X}(0)e^{2gt}, \\ \Delta\hat{P}(t) = \Delta\hat{P}(t)e^{-2gt}, \end{cases} \tag{2.121}$$

Dans le cas où le champ initial est un état de vide quantique ou un état cohérent, ce qui est le cas dans la quasi-totalité des expériences, on a alors $\Delta\hat{X}(0) = \Delta\hat{P}(0) = 1$:

$$\begin{cases} \Delta\hat{X}(t) = e^{2gt}, \\ \Delta\hat{P}(t) = e^{-2gt}, \end{cases} \tag{2.122}$$

où l'on voit que le produit des variances satisfait bien au principe d'indétermination de Heisenberg puisque quel que soit t, on a toujours $\Delta\hat{X}(t)\Delta\hat{P}(t) = 1$. Par conséquent,

la quadrature non amplifiée présente un niveau de bruit plus faible que celui du bruit quantique standard, voir FIGURE 2.13. Le niveau de compression ou réduction de bruit est comme nous l'avons vu proportionnel aux coefficients non-linéaires du cristal, à l'amplitude de la pompe et enfin au temps d'interaction au sein du matériaux.

Chapitre 3.

Synchronisation par horloge optique distribuée de sources de paires de photons intriqués

Dans ce troisième chapitre, nous introduisons et présentons un schéma de synchronisation tout optique, à très haute vitesse, et d'une précision inégalée, en vue de permettre le déploiement sur longues distances de communications sécurisées par cryptographie quantique. Le dispositif présenté exploite des sources indépendantes et distantes de paires de photons intriqués dans une configuration déjà brièvement présentée en section 1.2.2 du chapitre 1, à savoir celle d'un relais quantique. La synchronisation est alors validée par l'observation d'une interférence à deux photons dans le taux de coïncidences quadruples de l'expérience.

Afin de motiver ce travail, nous revenons tout d'abord sur les limitations associées au déploiement d'un relais quantique en fonction du régime de pompage choisi. Une vue générale de notre dispositif est ensuite donnée et ses différents éléments constitutifs sont détaillés. Des résultats préliminaires obtenus sur courte distance sans stabilisation active sont reportés. Enfin, nous nous intéressons aux résultats finaux obtenus pour une distance effective de 100 km entre les sources et en présence d'une correction active des différents effets de gigue temporelle liés aux fluctuations thermiques de l'environnement en présence.

3.1. Motivation

Le schéma de communication quantique étudié ici est basé sur une configuration de type relais quantique, voir Figure 3.1, où deux photons ('2' et '3') issus de deux sources de paires de photons intriqués indépendantes (SPDC) interfèrent au niveau d'une station relais, de sorte à étendre le lien d'intrication à leurs jumeaux respectifs (photons '1' et '4'). Expérimentalement, la coalescence des photons s'obtient en assurant l'indiscernabilité des deux photons interférant vis-à-vis de leurs différents degrés de liberté (polarisation, longueur d'onde, profil spectral et mode temporel). L'influence de

chacun de ces degrés de liberté sur la figure d'interférence à deux photons est discutée, du point de vue théorique, en détails au sein de l'annexe B. Nous nous contenterons donc ici de relever que c'est l'indiscernabilité des modes temporels qui constitue à ce jour la principale difficulté expérimentale. Très concrètement, les incertitudes temporelles liées aux temps d'émission et de détection des photons doivent être négligeables devant le temps de cohérence des photons uniques que l'on souhaite faire interférer. En d'autres termes, dans le cas d'un régime de pompage impulsionnel, le temps de cohérence des photons doit être supérieur à la durée des impulsions de pompe ayant permis de les créer. Ou alors, dans le cas d'un régime de pompage continu, ce même temps de cohérence doit être grand devant les gigues temporelles des détecteurs utilisés. Pour satisfaire à ces différentes conditions, il est courant d'avoir recours à une étape de filtrage en sortie du processus de conversion paramétrique spontanée, de sorte à venir augmenter le temps de cohérence des photons, le prix à payer étant alors une réduction du débit. Dans ce contexte, le régime opérationnel de pompage des deux sources de paires de photons joue un rôle central puisque c'est essentiellement ce dernier qui conditionne le filtrage spectral à appliquer.

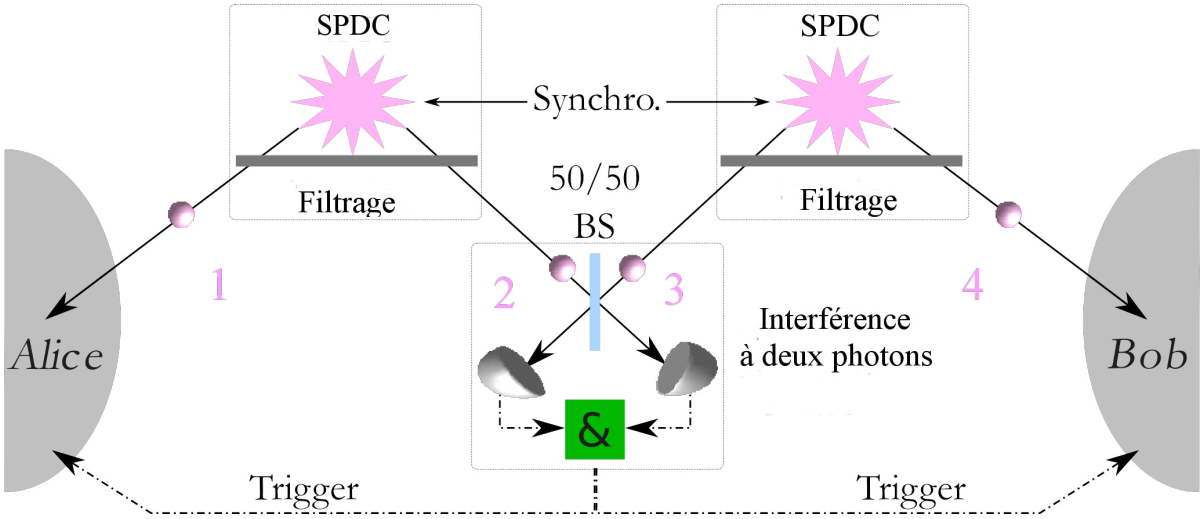


Figure 3.1. – Schéma de principe d'un relais quantique exploitant des sources indépendantes de paires de photons intriqués. Pour assurer un recouvrement parfait des paquets d'ondes des deux photons se présentant à la lame séparatrice équilibrée (50/50), leurs temps de cohérence doivent être plus grands que l'incertitude temporelle avec laquelle ils ont tout deux été créés (régime impulsionnel) ou détectés (régime continu).

Une première approche possible consiste à synchroniser les temps d'émission des paires en utilisant deux lasers femtosecondes (fs) dans une configuration maître/esclave. Dans cette configuration, les dérives de la cavité du laser esclave sont asservies sur celle de la

cavité du laser maître. Cette approche présente le double avantage de réduire l'incertitude sur les temps de création des photons vis-à-vis de la durée des impulsions de pompe, de sorte que le filtrage requis ne soit dans ce cas que de l'ordre du nanomètre, voir Figure 3.2a, et d'introduire dans le même temps une horloge intrinsèque induite par le taux de répétition. Cependant, lorsqu'on commence à séparer les deux lasers, il devient vite pratiquement impossible, au bout d'une dizaine de kilomètres de distance, de maintenir la même dynamique pour les cavités des lasers maître et esclave [256, 257]. Ceci s'explique tout simplement par la vitesse finie du signal électro-optique se propageant dans la boucle de rétroaction. De plus, tous les travaux effectués jusqu'à maintenant dans cette configuration ont été limités à des taux de répétitions de l'ordre de la centaine de mégahertz de par la conception même des lasers utilisés qui sont souvent des lasers à l'état solide.

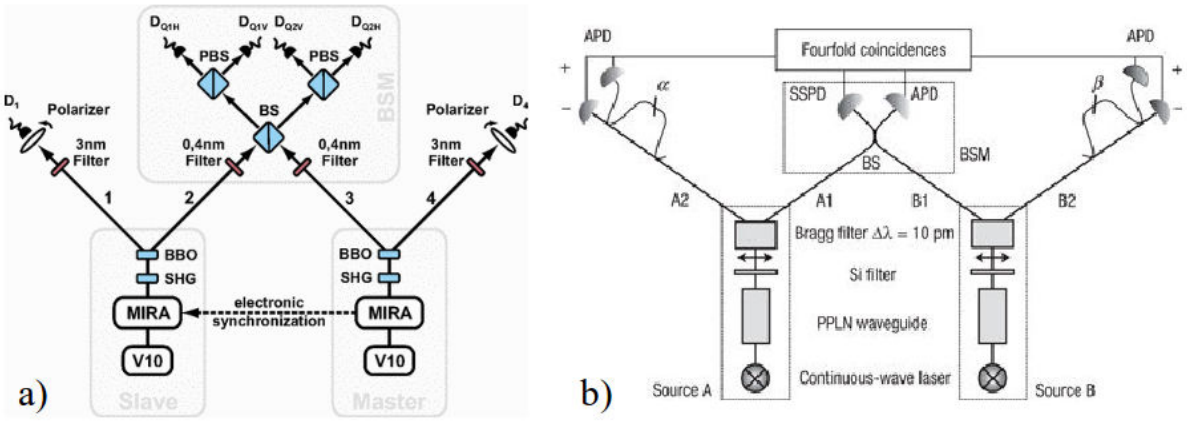


Figure 3.2. – **a)** Relais quantique en régime de pompage impulsionnel femtoseconde selon la proposition de la référence [257]. Les photons *signal* et *idler* aux longueurs d'ondes des télécommunications passent respectivement dans des filtres de bandes passantes de 0,4 et 3 nm. **b)** Relais quantique en régime de pompage continu selon la proposition de la référence [258]. Les photons *signal* et *idler* aux longueurs d'ondes des télécommunications passent tous deux dans des filtres de bandes passantes de 10 pm.

Une seconde approche consiste à travailler dans un régime de fonctionnement continu [258], voir Figure 3.2b. Dans ce cas, les contraintes liées à la dynamique des lasers de pompe sont complètement relaxées. Cependant, étant donné qu'aucune référence de temps n'est fournie par les lasers continus, les gigues temporelles des détecteurs deviennent alors la principale source d'incertitude. Le prix à payer se situe dès lors non plus en termes de distance comme en régime impulsionnel, mais sur le débit, puisque des filtres de bandes passantes très étroites, de l'ordre de la dizaine de picomètres, doivent alors être employés de sorte à ce que le temps de cohérence des photons uniques devienne bien supérieur à la gigue temporelle des détecteurs (dans le

meilleur des cas, de l'ordre de quelques dizaines de ps). Avec un tel temps de cohérence, le taux de répétition 'effectif' maximum de ces sources serait limité à 100 MHz, mais le taux d'émission subséquent est en pratique réduit à 1 MHz en raison du filtrage très fin. En outre, si le contrôle de la longueur du trajet n'est plus nécessaire, l'indiscernabilité en termes de longueur d'onde centrale est sensible à tout décalage des filtres.

En vue de répondre aux difficultés liées aux deux régimes précédemment mentionnés, le régime picoseconde a été identifié comme un compromis vis à vis de la stabilisation de la longueur des canaux de communication (de l'ordre de quelques mm) et de la stabilisation de la longueur d'onde centrale des filtres (de l'ordre de la centaine de pm). Deux réalisations en régime ps d'un lien de téléportation quantique métropolitain reposant sur une approche hybride opto-électrique ont ainsi récemment pu être démontrées à Calgary [201] et à Hefei [202]. Dans les deux cas, des modulateurs électro-optiques (EOM) associés à des lasers continus sont utilisés pour simuler un régime impulsionnel ps. Ce système ingénieux permet, grâce à la modulation électro-optique et à une boucle de rétroaction, d'ajuster en temps réel le taux de répétition de l'une des deux sources pour corriger les dérives temporelles engendrées par les fluctuations thermiques liées à l'environnement. Toutefois, cette idée intéressante repose de nouveau sur une séquence de conversion d'un signal optique vers un signal électrique, ce qui limite fortement les performances du système. En effet, les EOM introduisent, de par leurs propriétés intrinsèques, une gigue temporelle à l'émission. Il devient alors impossible de travailler avec des impulsions de durée inférieure à la centaine de ps, et donc à des taux de répétition supérieurs à la centaine de MHz.

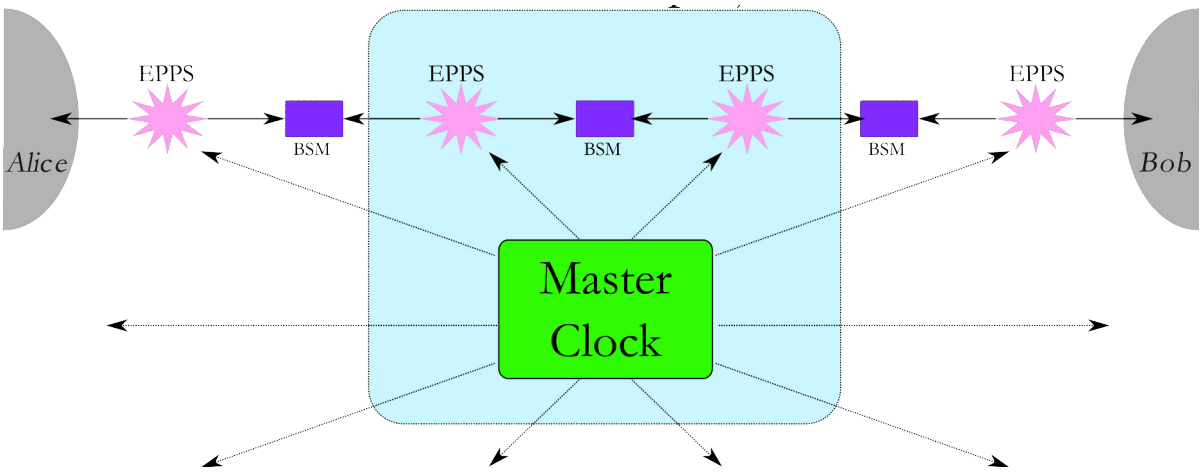


Figure 3.3. – Synchronisation par horloge optique distribuée de sources indépendantes de paires de photons intriquées dans une configuration de relais quantique. EPPS : *Entangled Photon Pair Source* ; BSM : *Bell State Measurement*.

Ainsi, bien que des résultats encourageants aient été obtenus, les stratégies utilisées jusqu'à maintenant en régimes impulsionnel et continu présentent des contraintes techniques non triviales, rendant difficiles les déploiements sur grandes distances ($\geq$100 km) d'opérations de relais quantiques. La réalisation présentée au sein de ce chapitre s'inscrit dans ce contexte délicat. Nous présentons ici une approche originale inspirée du principe de synchronisation par horloge distribuée' des télécoms standard, reposant sur la distribution tout optique d'une horloge maîtresse émettant des impulsions de l'ordre de la ps jusqu'aux différentes sources de paires de photons utilisées comme illustré en FIGURE 3.3. Aucune gigue temporelle liée à une quelconque conversion électro-optique n'est ainsi présente dans cette configuration puisque le dispositif repose sur un laser unique, et les photons générés par les sources ne sont pas soumis à des conditions drastiques de filtrage puisque nous travaillons en régime impulsionnel. En d'autres termes, l'idée de partager un seul laser de pompe permet de contourner, de manière simple, les principaux problèmes liés à la synchronisation des sources pompées par des lasers indépendants.

3.2. Présentation générale du dispositif

Notre dispositif présente de fait l'avantage de reposer uniquement sur des composants au standard des télécommunications optiques, ainsi que sur des cristaux aux propriétés non linéaires facilement disponibles dans le commerce.

Concrètement, nous proposons de synchroniser les temps d'arrivée des photons uniques au niveau du nœud relais en distribuant, à travers le réseau, des impulsions de durée de l'ordre de la ps au moyen d'un laser à fibre (Pritel, UOC [1] 100) opérant à la longueur d'onde télécom λ_p = 1540,0 nm. Ce laser agit comme une horloge commune alimentant, à un taux de répétition de 2,5 GHz, des sources indépendantes de paires de photons corrélés, voir FIGURE 3.4.

À chaque station, l'horloge maîtresse est tout d'abord amplifiée à l'aide d'amplificateurs à fibre dopée à l'erbium (Pritel, LNHPFA 30) avant d'être convertie par génération de seconde harmonique au sein de cristaux massifs de niobate de lithium périodiquement polarisé (Covesion, MgO:PPLN) à la longueur d'onde visible de λ_{shg} = 770,0 nm. Enfin, les faisceaux convertis sont utilisés pour pomper en parallèle deux étages de conversion paramétrique spontanée (processus décrit en section 2.5.1) au sein de guides d'ondes inscrits sur niobate de lithium. Ces deux sources de paires de photons sont alors automatiquement synchronisées à distance.

Les sources émettent des paires de photons dans la bande des télécommunications, plus précisément autour de la longueur d'onde centrale de 1540,0 nm. Un étage de

1. UOC : *Ultrafast Optical Clock*

filtrage (DWDM) permet alors la distribution de photons centrés à 1543,6 nm (ITU [2] 42), dans une fenêtre de 800 pm, au sein des canaux externes. Par ailleurs, un filtre de Bragg situé au sein de la station relais permet, à partir des signaux réfléchis par les deux DWDM, de sélectionner les photons jumeaux à 1537,4 nm (ITU 50) dans une fenêtre de 200 pm.

Les coïncidences quadruples entre photons à 1543,6 et 1537,4 nm sont enfin enregistrées, et la qualité de la synchronisation est alors analysée au travers de la mesure d'une figure d'interférence à deux photons que l'on vient balayer à l'aide d'un rétroréflecteur dont on fait varier la position. L'indiscernabilité des modes de polarisation des photons interférant est assurée par un ensemble de contrôleurs de polarisation [3] (PC) et de coupleurs à fibre qui maintiennent les états de polarisations incidents.

2. ITU : *International Telecommunication Union.*
3. Ensemble composé de deux lames quart-d'onde et d'une lame demie-onde.

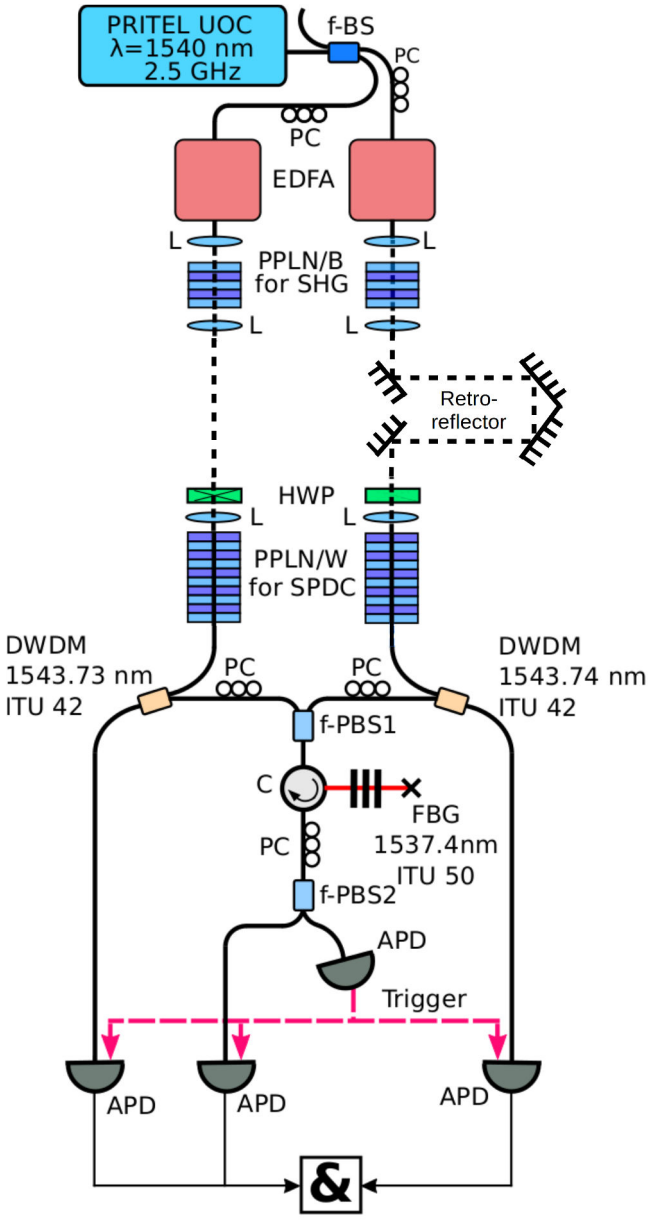


Figure 3.4. – Synchronisation par horloge optique distribuée de deux sources 'indépendantes' de paires de photons intriqués : vue d'ensemble du dispositif expérimental. BS : coupleur 50/50 ; PC : contrôleur de polarisation ; EDFA : amplificateur à fibre dopée à l'erbium ; L : lentille, PPLN/B : cristal massif de PPLN ; PPLN/W : guide d'onde PPLN ; HWP : lame demie onde ; f-PBS : PBS à fibre, DWDM : dense wavelength division multiplexer, C : circulateur ; FBG : filtre de Bragg à fibre ; APD : photodiode à avalanches ; & : compteur de coïncidences quadruples.

3.3. Caractérisation du dispositif

Dans cette section, nous présentons de manière plus détaillée les différents blocs constitutifs de notre système de synchronisation.

3.3.1. Horloge optique

Nous commençons par expliciter le principe de fonctionnement de l'horloge optique utilisée, avant de présenter une étude du temps de cohérence du signal émis par cette cavité laser.

Principe de fonctionnement

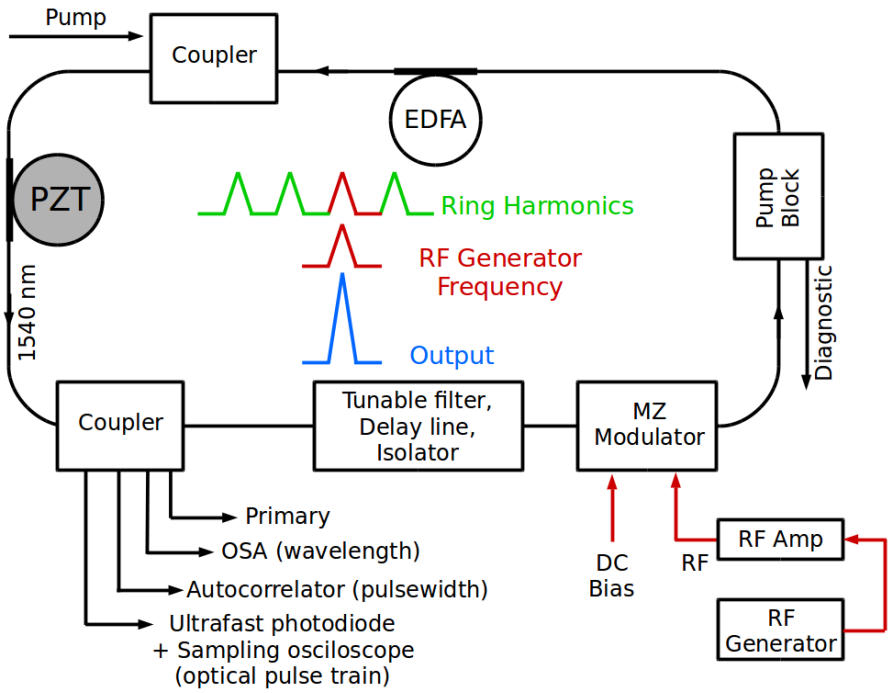


Figure 3.5. – **a)** Description schématique de l'horloge optique. EDFA : Amplificateur à fibre dopée à l'erbium ; MZ : Mach-Zehnder ; PZT : dispositif piézoélectrique ; OSA : analyseur de spectre optique ; RF : radiofréquence.

La génération d'impulsions à des taux de répétition élevés (>GHz) est aujourd'hui communément assurée par des cavités laser en anneaux, à verrouillage actif de modes, et où l'effet laser prend place au sein d'un milieu à gain de type fibre monomode dopée

aux ions de terres-rares [4] [259]. Pour atteindre un tel régime de fonctionnement, notre cavité laser intègre, tel qu'illustré en FIGURE 3.5, un modulateur d'intensité électro-optique de type Mach-Zehnder. Cette modulation introduit des pertes périodiques à un taux de répétition qu'il nous est alors possible de choisir au moyen d'un générateur radiofréquence externe. Ce taux doit correspondre précisément à l'intervalle spectral libre (*free spectral range* - FSR) de la cavité, c'est-à-dire à l'écart séparant deux modes longitudinaux successifs (FIGURE 3.6a), ou à un harmonique de ce dernier.

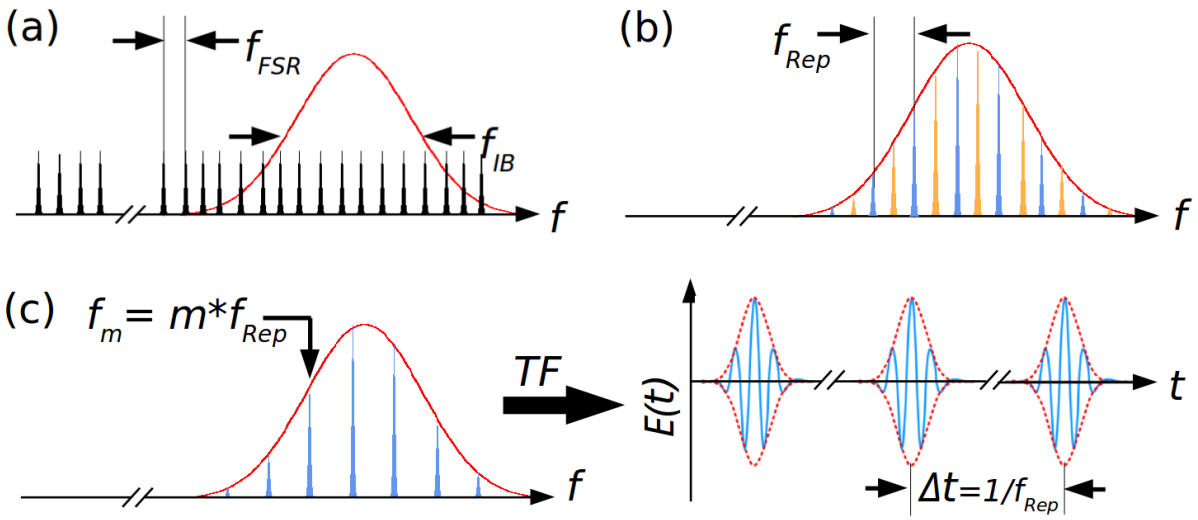


Figure 3.6. – **a)** Le spectre d'une cavité optique passive (sans milieu à gain) forme un peigne de modes longitudinaux. La distance séparant deux modes adjacents, f_{FSR}, correspond à l'intervalle spectral libre (FSR) de la cavité. La courbe rouge représente la courbe de gain du milieu amplificateur, de largeur f_{IB}, d'une cavité active. **b)** Apparition de super-modes après modulation active des pertes de la cavité à un taux de répétition, f_{Rep}, que l'on a ici pris égal, dans un souci de représentation, à seulement deux fois l'intervalle spectral libre. Dans ce cas particulier, seuls sont disponibles deux super-modes respectivement représentés en bleu et en orange. **c)** Pour garantir la stabilité en amplitude du signal, il est alors nécessaire de ne conserver qu'un seul super-mode, ce qui en pratique se fait à l'aide d'un filtre étalon ajustable inséré dans le circuit de la cavité.

Cette configuration laser admet des 'super-modes', constitués chacun d'un sous-ensemble de modes longitudinaux synchronisés, l'écart entre deux modes adjacents d'un même super-mode correspondant à la fréquence de modulation, voir FIGURE 3.6b. Concrètement, plus la largeur de la courbe de gain est grande, plus le nombre de modes au sein de chaque super-mode devient important. Dans le domaine temporel, une augmentation de bande passante se traduit par une diminution de la durée des impulsions

4. La longueur d'onde obtenue dépend de l'ion choisi : Ytterbium 1050 nm ; Erbium 1540 nm ; Thulium 1940 nm ; Holmium 2100 nm.

en sortie de cavité. En principe, chaque super-mode est susceptible de 'laser'. Or, si plusieurs super-modes sont en concurrence vis à vis du gain de la cavité, le signal en sortie de la cavité risque de présenter alors des instabilités, comme des battements entre super-modes. Pour garantir une stabilité en amplitude et en fréquence satisfaisante au cours du temps, il est crucial de supprimer tous les super-modes à l'exception du super-mode d'intérêt, voir FIGURE 3.6c. À cette fin, on intègre au sein de la cavité un filtre étalon à angle accordable (labellisé 'filtre accordable' sur la FIGURE 3.5) permettant de discriminer les différents super-modes présents au sein de la cavité. Dans cette configuration, seul le super-mode de plus fort gain peut 'laser', du moment que la largeur de la cavité demeure constante au cours du temps. À un taux de répétition de 2.5 GHz l'analyseur de spectre en notre possession ne permet pas de résoudre ce super mode, ainsi seule l'enveloppe de ce dernier apparaît sur le spectre de la FIGURE 3.7 mesuré en sortie de la cavité laser.

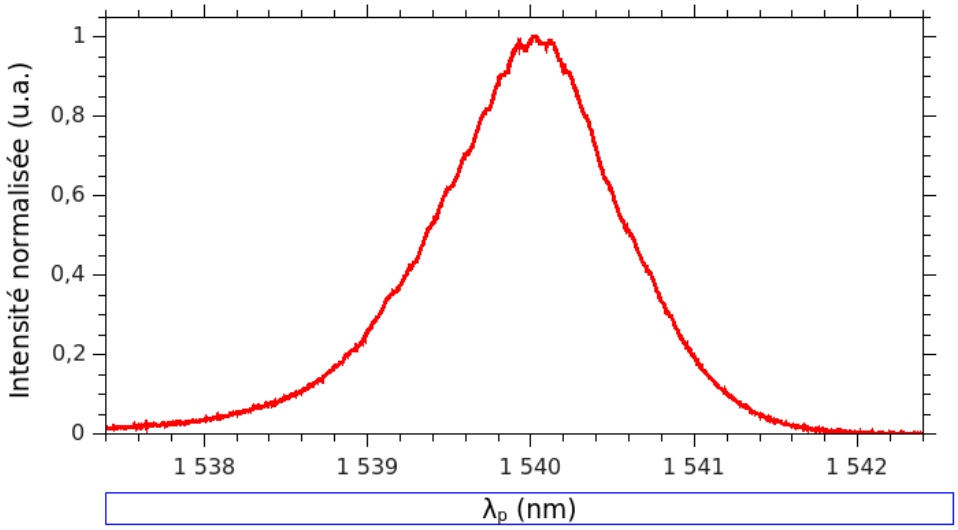


Figure 3.7. – Spectre d'émission typique de l'horloge optique.

Les principaux paramètres de la cavité laser utilisée sont résumés au sein du tableau 3.1.

λ	$\Delta\lambda$	δt	f_{FSR}	f_{Rep}
1540,0 nm	1,1 nm	2,2 ps	4,67 MHz	2,49648 GHz

Table 3.1. – Principales caractéristiques de la cavité laser utilisée. λ : longueur d'onde centrale du spectre d'émission ; $\Delta\lambda$: largeur à mi-hauteur du spectre d'émission ; δt : durée des impulsions ; f_{FSR} : intervalle spectrale libre de la cavité ; f_{Rep} : taux de répétition.

Estimation de la cohérence temporelle du train d'impulsion

En pratique, des fluctuations de la température et des vibrations acoustiques au sein du montage engendrent inévitablement au cours du temps de légères fluctuations de longueur de la cavité laser, qui occasionnent à leur tour un décalage des fréquences contenues au sein du super-mode. Si le décalage provoque un espacement symétrique de deux super-modes adjacents autour de la fréquence du filtre, aucun des deux super-modes n'est plus dominant et on observe de nouveau des fluctuations du signal de sortie. Pour contrer ces effets, la cavité laser est montée au sein d'une chambre isolante équipée d'une boucle à verrouillage de phase, ce qui limite les fluctuations thermiques à $\pm 0{,}1\,^{\circ}$C.

Malgré ces efforts, il est impossible de supprimer totalement le bruit technique au sein de la cavité. En conséquence, les différentes contributions au bruit sont responsables, au sein du super-mode, d'un élargissement des différentes composantes spectrales. Le profil de ces modes longitudinaux est dicté par la géométrie de la cavité et par la forme de la modulation. Leur largeur à mi-hauteur, lorsque leur profil est connu, permet de remonter au temps de cohérence τ_c du train d'impulsions [5]. Idéalement, le temps de cohérence τ_c du train d'impulsions correspond dans le vide, à une constante près qui dépend du profil des modes longitudinaux de la cavité, à l'inverse de la bande passante de ces derniers. On associe à ce temps de cohérence une longueur de cohérence $L_c = c\tau_c/n$, où n représente l'inde de réfraction du matériaux. Lorsque le signal de sortie de la cavité est injecté au sein d'un dispositif interférométrique présentant un déséquilibre $\Delta L > L_c$, aucune interférence entre les deux trains d'impulsions ne peut plus être observée en sortie de l'interféromètre.

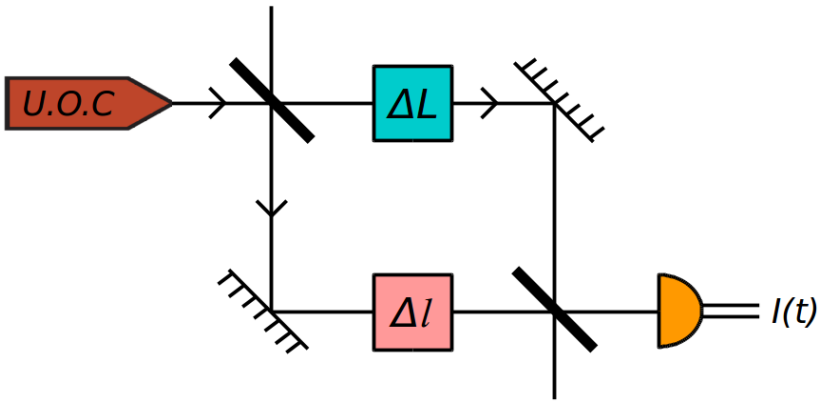


Figure 3.8. – Dispositif interférométrique utilisé pour mesurer la longueur de cohérence temporelle de la lumière issue de notre cavité laser. Δl représente un délai ajustable contrôlé au moyen d'un dispositif motorisé.

5. Il est important de ne pas confondre le temps de cohérence τ_c du train d'impulsion avec la durée δt des impulsions.

Pour mesurer la longueur de cohérence associée au train d'impulsions, nous avons ainsi injecté le signal sortant de la cavité laser dans l'une des entrées d'un interféromètre de Mach-Zehnder déséquilibré tel qu'illustré en FIGURE 3.8. Sur le bras du haut nous avons décalé les deux trains d'impulsions à l'aide de différents délais optiques $\Delta L \geq c/f_{Rep}$, tandis que sur le bras du bas, une ligne à retard motorisée de résolution 10^{-2} ps nous a permis l'ajustement d'un délai $\Delta l < c/f_{Rep}$ afin de replacer, pour chaque ΔL testé, les deux trains d'impulsions en parfait vis-à-vis lors de leur recombinaison au niveau de la seconde lame séparatrice. Pour un ΔL donné, on enregistre alors à l'aide d'une photodiode le profil $I(t)$ des interférences en fonction du temps, qui pour des impulsions gaussiennes nous est donné par [249] :

$$I(t) \propto \frac{1}{2}\left\{1 + e^{-\frac{4\ln(2)(c\Delta l)^2}{(\delta t)^2}} \cos^2\left(\varphi(t)\right)\right\}. \tag{3.1}$$

Aucune stabilisation de l'interféromètre n'est ici nécessaire puisque les fluctuations aléatoires de la phase relative $\varphi(t)$ induites par l'environnement entre les deux bras sont suffisamment lentes pour être résolues à l'aide d'un détecteur de puissance optique standard.

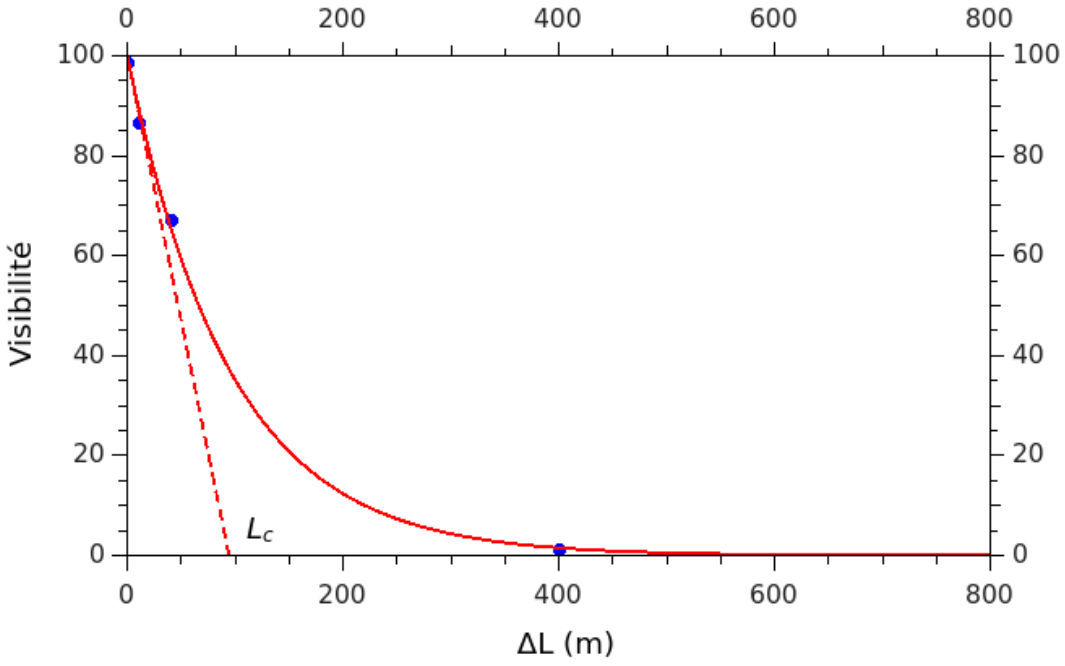


Figure 3.9. – Visibilité de la figure d'interférence en sortie de l'interféromètre de Mach-Zenhder pour différent ΔL dans le cas de trains d'impulsions synchronisés. L'ajustement des données avec un profil exponentiel décroissant nous permet d'estimer un temps de cohérence de 0,5 μs associé à une longueur de cohérence L_c, dans la silice, d'environ 100 m.

La FIGURE 3.9 présente les différents pourcentages de visibilité :

$$V = \frac{I_{Max} - I_{Min}}{I_{Max} + I_{Min}}, \tag{3.2}$$

obtenus une fois les trains d'impulsions synchronisés pour les différents délais optiques ΔL testés. Nous observons une perte quasi totale de cohérence pour un déséquilibre de 400 m entre les trains d'impulsions. Le cas ΔL nul est illustré en FIGURE 3.10. Les résultats obtenus nous permettent d'estimer, le temps de cohérence du train d'impulsions : $\tau_c = 0{,}5\,\mu$s.

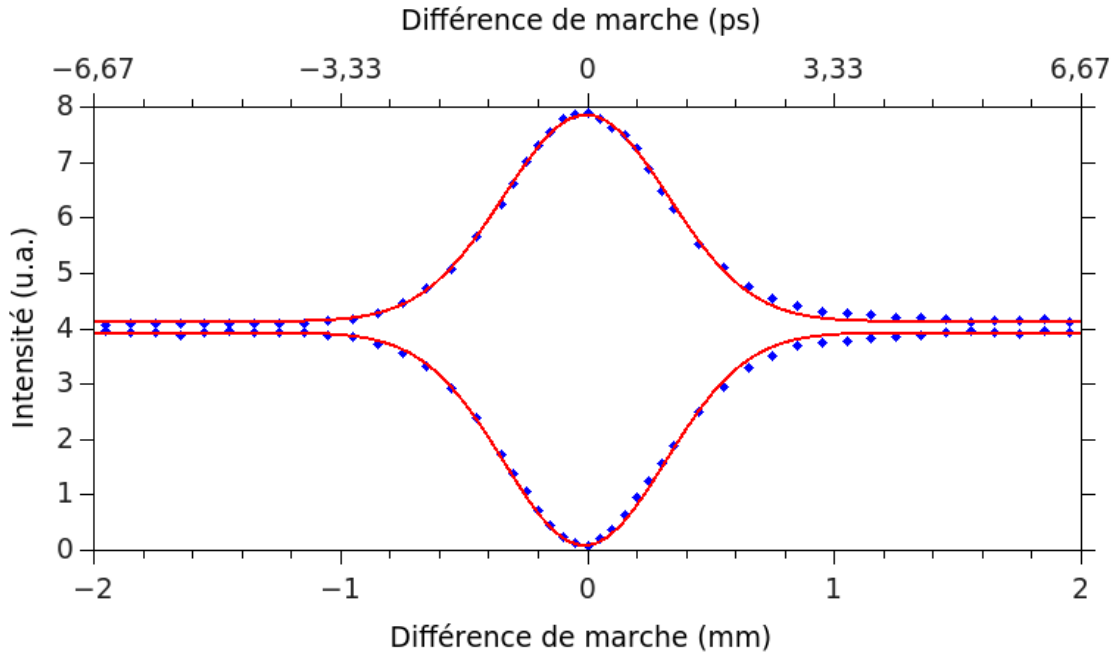


Figure 3.10. – Mesure de synchronisation des trains d'impulsions en sortie de l'interféromètre de Mach-Zehnder. Les données expérimentales en bleu représentent les maxima et minima d'interférence observés dans le profil d'intensité en fonction du délai Δl appliqué au moyen de la ligne à retard motorisée présente dans le bras inférieur de l'interféromètre, et ce en l'absence de délai optique ΔL dans le bras supérieur (séparation puis recombinaison de la même impulsion). Les courbes rouges correspondent à un ajustement gaussien dont la largeur à mi-hauteur nous donne directement accès à la durée des impulsions, à savoir ici δt = 2.2 ps.

3.3.2. Modules amplificateurs

En sortie de la cavité laser, le signal est routé à l'aide d'un coupleur 50/50 en direction de deux modules comprenant chacun un pré-amplificateur et un amplificateur à

fibre [260]. Dans cette section, nous nous intéressons à la réponse de ces modules à la puissance du signal entrant avant de discuter des effets d'auto-modulation de phase du mode guidé en sortie du dispositif.

Seuil d'amplification

Le seuil de fonctionnement des pré-amplificateurs utilisés est, d'après les données fabriquant, de -20 dBm. Cette valeur est à mettre en relation avec la puissance moyenne du signal optique en sortie de la cavité laser et les pertes à la propagation jusqu'à ces différents modules. La puissance moyenne du signal optique en sortie de la cavité est ajustable à un niveau compris entre 0 et 10 dBm (1 et 10 mW). Ce niveau, bien supérieur au seuil de pré-amplification précédemment mentionné, nous permettra de nous affranchir de toutes considérations liées à la puissance en amont des modules d'amplification lors de nos tentatives de synchronisation du lien relais sur de courtes distances (pertes à la propagation négligeables).

Toutefois, en prévision de la situation où la synchronisation sera réalisée sur de longues distances, ce qui ne manquera pas d'occasionner des pertes importantes (voir section 3.6.2, nous avons étudié la réponse des modules amplificateurs à des pertes simulées au moyen d'un atténuateur variable.

Signal d'entrée :	Pas de signal	-10 dBm	-3 dBm	0 dBm
Signal de sortie :	8 mW	42 mW	65 mW	72 mW

Table 3.2. – Puissance en sortie des pré-amplificateurs en fonction de la puissance entrante.

Notre premier test a simplement consisté à mesurer la puissance en sortie des pré-amplificateurs en fonction du niveau de puissance incident ; les résultats obtenus sont reportés dans le tableau 3.2.

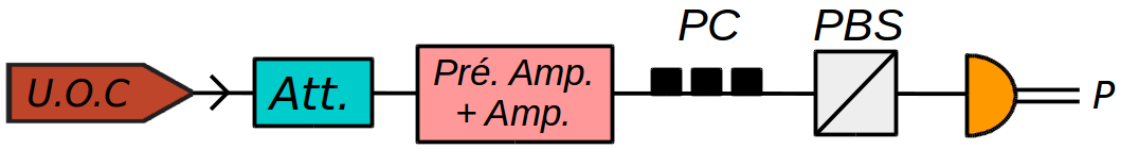


Figure 3.11. – Dispositif expérimental permettant la mesure du taux d'extinction de la polarisation en sortie du module d'amplification en fonction de la puissance incidente. Att. : atténuateur variable ; PC : contrôleur de polarisation ; PBS : cube polarisant.

En complément de ces résultats, nous avons également mesuré le pourcentage d'émission spontanée amplifiée contribuant au signal de sortie des modules d'amplifi-

cation (pré-amp. + amp.). L'émission spontanée étant un mélange statistique homogène au regard des modes de polarisation (faisceau dépolarisé), un moyen simple d'estimer sa contribution au signal de sortie consiste à analyser la polarisation de ce dernier [260]. Afin de mesurer le taux d'extinction de la polarisation, nous avons, tel qu'illustré en FIGURE 3.11, transmis les signaux sortants des amplificateurs à travers la combinaison d'un contrôleur de polarisation suivi d'un cube polariseur. La FIGURE 3.12 présente le rapport d'extinction observé en sortie du cube en fonction des pertes introduites en amont des modules amplificateurs.

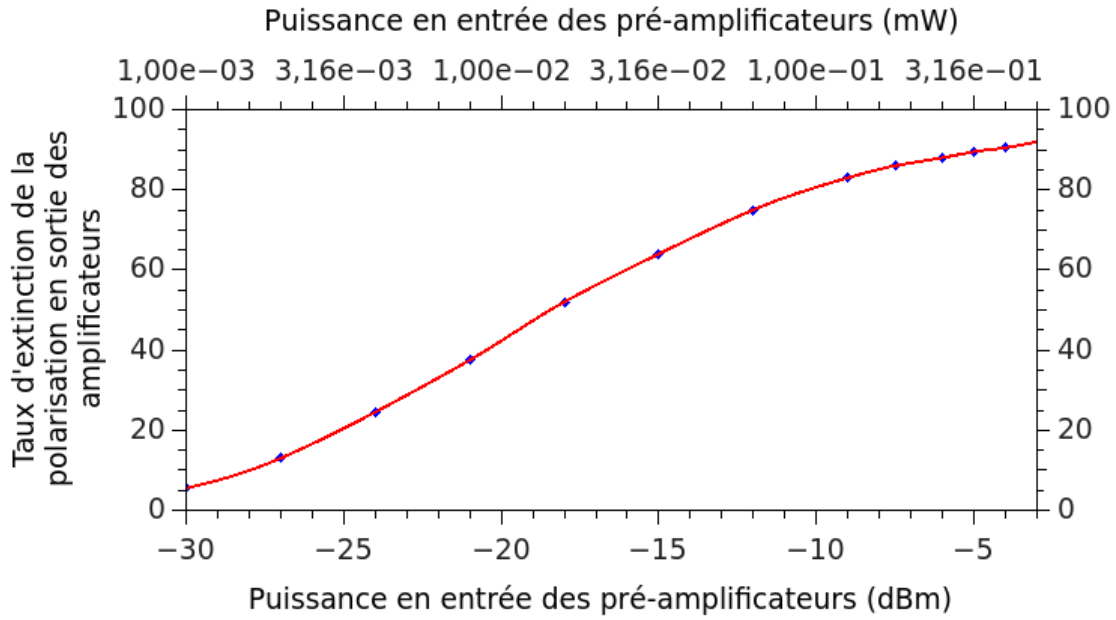


Figure 3.12. – Mesure du taux d'extinction de la polarisation en sortie des amplificateurs en fonction de la puissance en entrée des pré-amplificateurs. Le point correspondant à un rapport d'extinction de 50% nous permet d'avoir directement accès au seuil amplificateur du système, situation où émission spontanée et émission stimulée contribuent de manière égale au signal émis, à savoir -18 dBm.

Auto-modulation de phase

Un dernier paramètre critique à prendre en compte lorsqu'on travaille dans un milieu guidant en régime d'impulsions ultra-courtes est la puissance crête du signal optique. Pour des impulsions de forme réguilière, la puissance crête peut être estimée à partir de la puissance moyenne en multipliant cette dernière par la durée séparant deux impulsions successives et en divisant le tout par la durée d'une impulsion.

Comme nous pouvons le voir sur la FIGURE 3.13, le spectre mesuré après environ 5 m de fibre optique en sortie des amplificateurs s'élargit et se déforme en fonction de la puissance crête des impulsions. Ce phénomène bien connu d'auto-modulation de phase (SPM) est une conséquence de l'effet Kerr optique. Concrètement, une impulsion ultra-courte voyageant dans un milieu matériel induit une variation de l'indice de réfraction de ce milieu par effet Kerr :

$$n(I) = n_L + I\Delta n_{NL}, \tag{3.3}$$

où n_L, Δn_{NL} et I représentent respectivement l'indice de réfraction linéaire, la variation d'indice due au processus non-linéaire d'ordre 3 ($\Delta n_{NL} \propto \chi^{(3)}$) et l'intensité du signal. Ainsi, les impulsions se propageant au sein des fibres de sortie de nos amplificateurs voient une variation d'indice entre le passage de leur crête et celui de leurs flancs. Cette variation induit alors un décalage de la phase instantanée de l'impulsion, qui provoque à son tour un élargissement du spectre en fréquence des impulsions. Le profil temporel de nos impulsions étant symétrique, l'auto-modulation de phase élargit également le spectre en fréquence selon un profil symétrique.

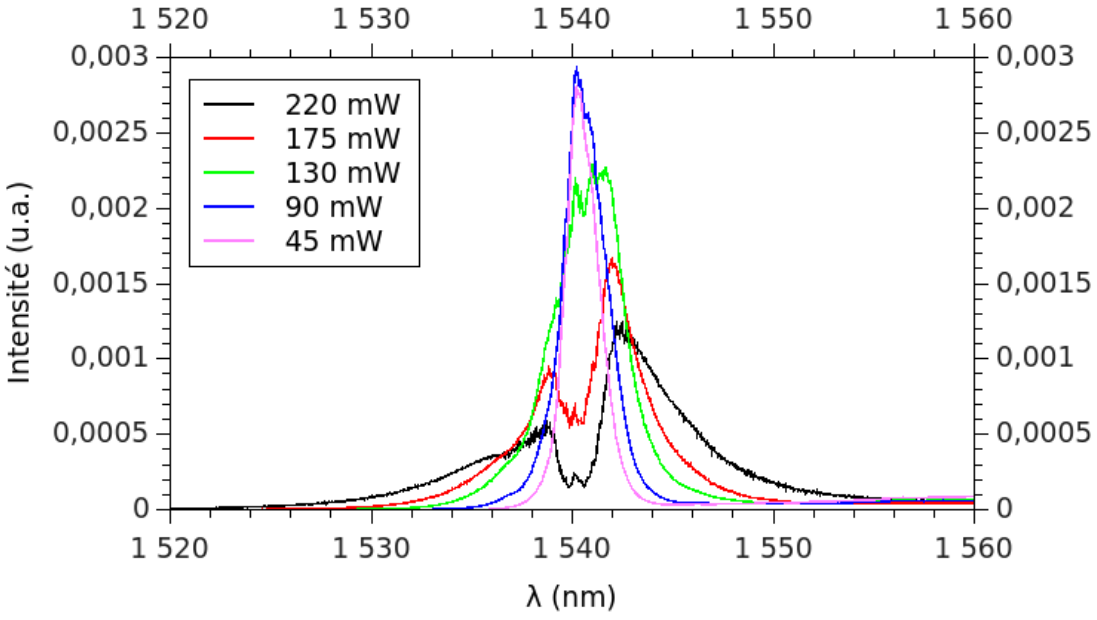


Figure 3.13. – Spectre en sortie de 5 m de fibre optique après amplification pour différentes puissances crêtes mesurées en sortie de la fibre optique.

Pour réduire cet effet, qui est d'autant plus présent que la longueur de l'interaction non-linéaire au sein de notre dispositif est grande, il faut donc, à puissance constante, diminuer la longueur des fibres optiques amenant le signal de sortie des amplificateurs jusqu'au cristaux de SHG.

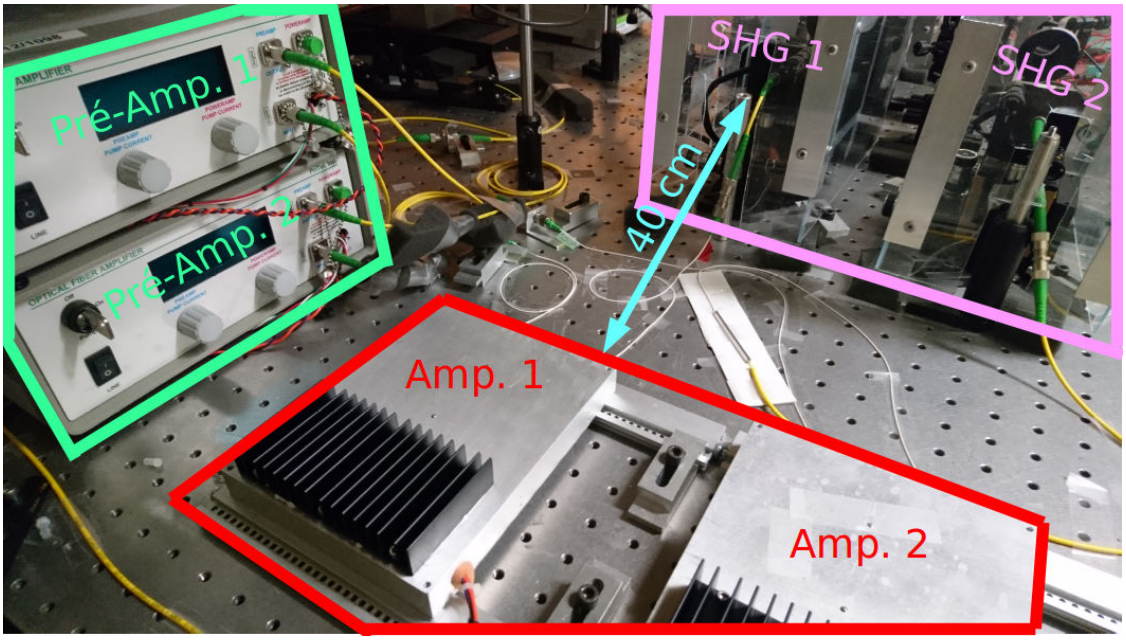


Figure 3.14. – Photographie du dispositif expérimental. Les amplificateurs (cadre rouge) ont été sortis de leurs boîtiers d'origine (cadre vert) au sein desquels on a uniquement laissé les pré-amplificateurs. Dans cette configuration, la longueur de fibre optique entre les amplificateurs et les cristaux de doublage en fréquence (cadre rose) n'est plus que de 40 cm, rendant ainsi l'effet d'auto-modulation de phase pratiquement négligeable.

De sorte à ramener cette longueur à environ 40 cm, nous avons tout d'abord placé les contrôleurs de polarisation, qui permettent d'optimiser l'efficacité des étages de doublage en fréquence (SHG), en amont des modules amplificateurs, ce qui représente un premier gain de 3 m. Enfin, voir FIGURE 3.14, nous avons sorti les amplificateurs de leurs boîtiers d'origine de sorte à directement pouvoir les connecter aux lentilles d'injection en entrée des cristaux, ce qui représente un second gain d'environ 1 m. Avec ces modifications, seul un faible résidu de SPM apparaît encore pour des puissances moyennes supérieures au watt. Toutefois, au regard des taux de saturation des détecteurs de photons uniques utilisés et de l'efficacité des différents étages de conversion du dispositif, nous n'avons jamais dépassé un tel seuil de puissance au cours de nos différentes expériences de synchronisation du lien relais.

3.3.3. Étages de conversion en longueurs d'onde

Dans cette section, nous présentons les différentes caractérisations des cristaux PPLN qui permettent, par étapes de conversion successives, de générer des paires de photons corrélés aux longueurs d'onde des télécommunications.

Génération de seconde harmonique (SHG)

À l'aide de lentilles traitées anti-reflets directement connectorisées en sortie des fibres, les signaux amplifiés sont injectés dans des cristaux massifs périodiquement polarisés de niobate de lithium dopés à l'oxyde de magnésium. Ces cristaux, de 5 mm de longueur, permettent la conversion, par génération de seconde harmonique, de la longueur d'onde télécom à 1540,0 nm vers la longueur d'onde du visible à 770,0 nm. Le dopage améliore la résistance du matériaux aux hautes puissances de pompe et limite l'effet photoréfractif[6] pouvant apparaître au sein des cristaux à ces régimes de puissance. Les deux cristaux ayant démontré des performances quasi identiques, seules les caractéristiques de l'un des deux sont représentées en FIGURE 3.15.

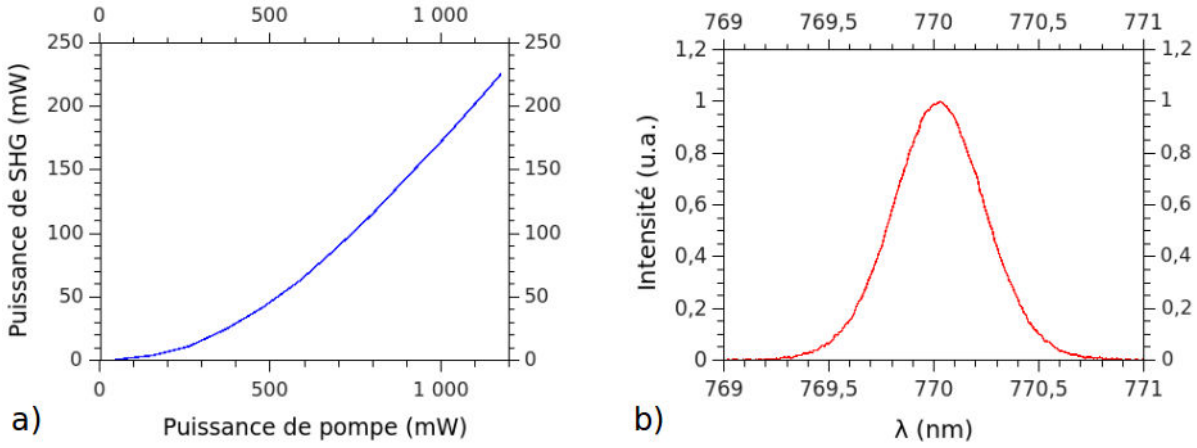


Figure 3.15. – **a)** Puissance de SHG en fonction de la puissance de pompe. **b)** Spectre de SHG typique en sortie des cristaux.

La réponse du cristal à la puissance de la pompe incidente est donnée en FIGURE 3.15a. On observe un profil quadratique caractéristique des effets non-linéaires du deuxième ordre. La FIGURE 3.15b correspond quant à elle au spectre du signal converti pour lequel nous pouvons, à l'aide d'un contrôle en température, ajuster la longueur d'onde centrale. Ce degré de liberté joue un rôle important puisqu'il nous permet de venir superposer les deux spectres de SHG, une condition *sine qua non* si l'on veut par la suite travailler avec des photons parfaitement indiscernables. Le résidu de pompe à 1540 nm est éliminé à l'aide de filtres coupe-bande placés directement en sortie des étages de doublage de fréquence. Le signal converti est quant à lui collimaté jusqu'à l'étage de conversion paramétrique spontanée où l'on vient, à l'aide d'une lentille d'injection, le focaliser dans un guide d'onde inscrit sur niobate de lithium.

6. L'effet photoréfractif, ou photoréfractivité, consiste en une modification locale de l'indice d'un milieu par l'onde optique incidente qui le traverse. En conséquence, le faisceau lumineux modifie lui-même les conditions de sa propagation.

Conversion paramétrique spontanée (SPDC)

Comme dans le cas de la SHG, le choix de la longueur des cristaux utilisés pour ce second étage de conversion nous est dicté par un compromis entre efficacité de conversion et *walk-off* temporel entre impulsions de pompe et paires de photons. L'efficacité de conversion est, comme nous l'avions vu à la section 2.5.1, d'autant plus importante que la durée de l'interaction est grande. Le *walk-off* temporel, qui provient du fait que les signaux à 770 et à 1540 nm ne présentent pas la même vitesse de groupe au sein du niobate, nous impose quant à lui des restrictions sur le filtrage à appliquer en sortie des étages de SPDC. Concrètement, plus le temps de propagation des impulsions de pompe dans le cristal est grand devant leur durée, plus la largeur des filtres à placer en sortie des cristaux de SPDC doit être étroite, et donc plus les pertes sont importantes. L'idéal est alors de travailler avec des temps de propagation pour les impulsions de pompe de l'ordre de leur durée.

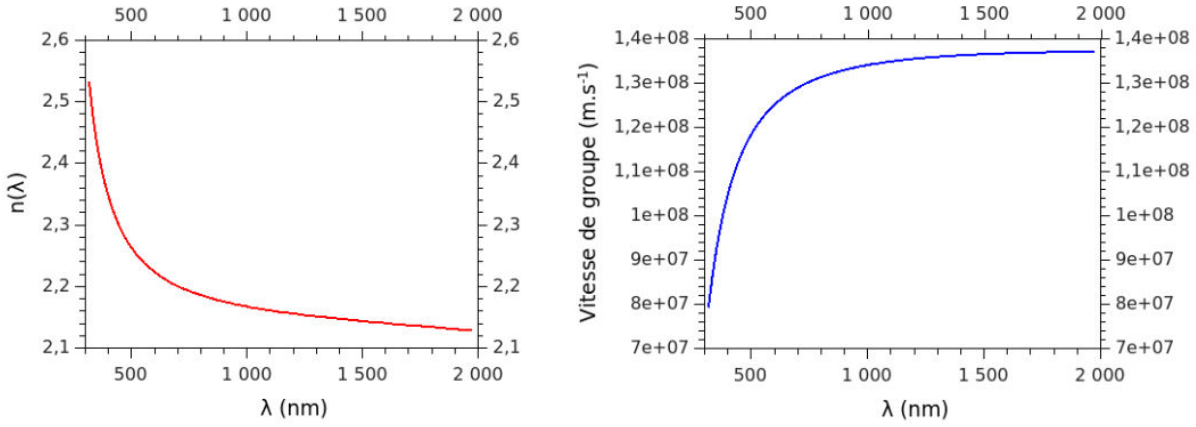


Figure 3.16. – **a)** Similulation de l'évolution de l'indice de réfraction du niobate de lithium en fonction de la longueur d'onde du signal optique à partir de l'équation de Sellmeier du matériau. **b)** Simulation de l'évolution de la vitesse de groupe au sein du niobate de lithium en fonction de la longueur d'onde du signal optique.

À partir de la simulation de la vitesse de groupe du signal au sein du niobate de lithium présentée en FIGURE 3.16, et sachant que la durée des impulsions de pompe vaut environ 2.2 ps, nous avons décidé de travailler avec des échantillons de longueur L= 21 mm, voir FIGURE 3.17. Ces échantillons, fabriqués au sein de l'équipe Optique Non-Linéaire Intégrée de notre institut de recherche, contiennent la reproduction en quatre exemplaires (I à IV) de séries de guides correspondant à différentes périodes d'inversion Λ allant de 15,7 à 16,3 μm. Chaque série contient un ensemble de guides correspondant à des diamètres allant de 4 à 8 μm. La reproduction en plusieurs exemplaires de chaque série de guides nous permet d'anticiper d'éventuels défauts de fabrication et de conserver plusieurs guides de secours en cas de d'éventuels dommages lors de l'utilisation. Pour trouver les guides nous permettant de générer des paires de photons autour de 1540,0 nm

et de ne garder que le plus efficace d'entre eux, nous avons caractérisé leur accord de phase par génération de seconde harmonique.

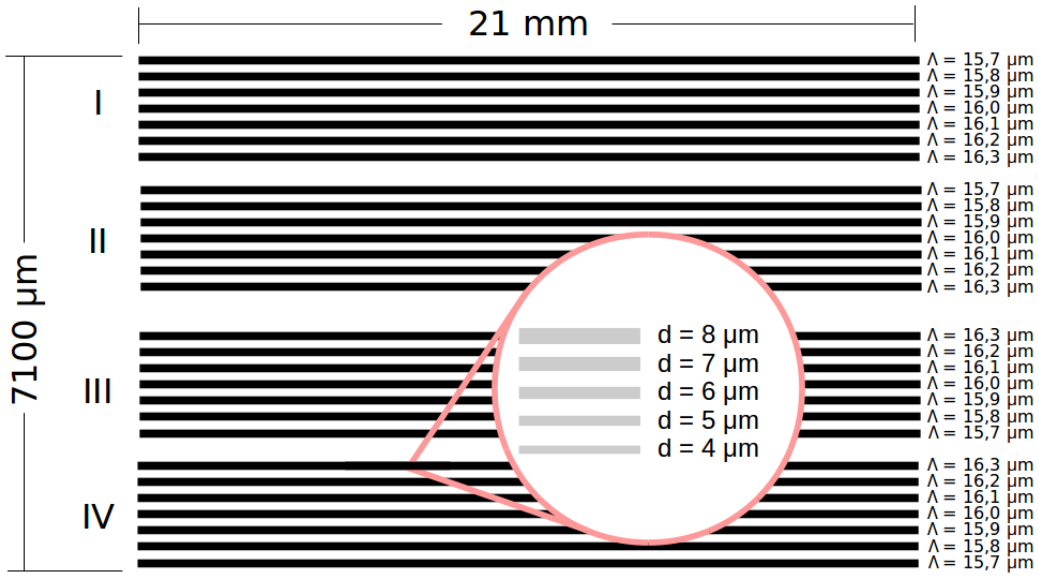


Figure 3.17. – Cartographie des guides d'ondes inscrits sur niobate de lithium. Différentes longueurs de guides et de pas d'inversion sont disponibles afin de trouver l'interaction non-linéaire désirée.

Afin de réaliser cette mesure, nous nous sommes servi d'un laser accordable émettant aux longueurs d'onde des télécommunications (Yenista Optics, Tunics 100). Le dispositif d'injection contra-propagée que nous avons utilisé est illustré en FIGURE 3.18. De sorte à optimiser l'efficacité de conversion de la SHG, nous avons tout d'abord connecté la fibre de sortie du laser à un contrôleur de polarisation. L'injection du signal télécom dans les différents guides se fait ensuite à l'aide de la fibre de récolte placée en sortie d'échantillon. L'acquisition du signal de SHG, effectuée au moyen d'un puissance-mètre optique opérant dans le domaine du visible, nous a permis, pour chacun des deux échantillons, de trouver les bonnes conditions d'accord de phase, à savoir $\lambda_{shg} = 770{,}0\,\text{nm}$, au sein de guides de largeur d=7 μm et de période d'inversion Λ=16,2 μm.

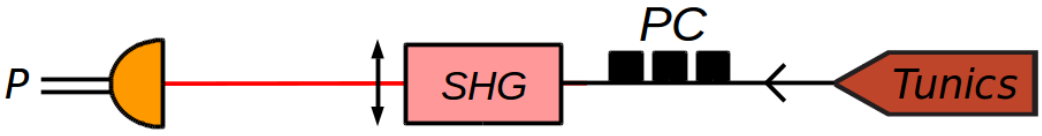


Figure 3.18. – Dispositif expérimental de caractérisation des différents guides par génération de seconde harmonique. PC : contrôleur de polarisation.

Une fois les caractérisations classiques effectuées et un guide d'onde choisi pour les deux échantillons, il nous reste, après optimisation de l'accord de phase au moyen du

contrôle en température des cristaux, à mesurer le spectre de SPDC pour chacune des sources. Comme dans le cas des spectres de SHG discutés dans le section précédente, il est important de s'assurer que les spectres des deux sources de paires de photons soient une nouvelle fois bien superposés.

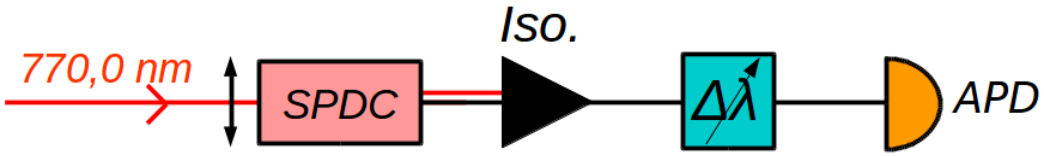


Figure 3.19. – Dispositif expérimental permettant de mesurer le spectre de SPDC en sortie des échantillons. Iso : isolateur optique.

Pour mesurer ces spectres nous avons placé en sortie des fibres de récolte, tel qu'illustré en FIGURE 3.19, un isolateur permettant de supprimer le résidu de pompe à 770 nm, suivi d'un filtre passe-bande accordable (Yenista Optics, XTM-50) de largeur à mi-hauteur 200 pm. Les photons sont détectés au moyen d'un détecteur de type photodiode à avalanche fonctionnement en régime de détection continue (ID Quantique, ID220). Le spectre associé à chaque source s'obtient alors en déplaçant la longueur d'onde centrale du filtre accordable, à longueur d'onde de pompe et température d'échantillon fixées.

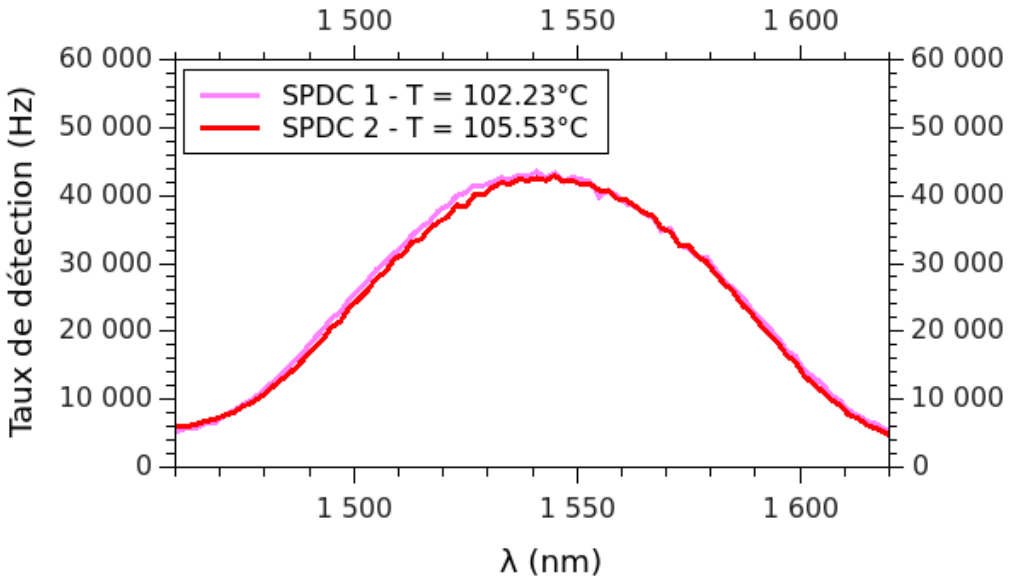


Figure 3.20. – Spectres de SPDC mesurés en sorties de nos deux échantillons pour des longueurs d'onde de pompe de 770,0 nm. Le niveau de bruit du détecteur utilisé est d'environ 2.5 kHz et les températures des deux échantillons ont été choisies de sorte à maximiser l'efficacité de conversion des processus non-linéaires.

Les spectres mesurés sont représentés en FIGURE 3.20. La largeur à mi-hauteur de 80 nm permet d'estimer un temps de cohérence $\tau_{s,i}$ du signal généré de 0.1 ps.

3.3.4. Filtrage spectrale

Pour garantir la synchronisation du lien relais, le temps de cohérence des photons générés par conversion paramétrique spontanée doit être au moins égal à la durée des impulsions de pompe afin de garantir, pour ces photons, des modes temporels uniques (limite de transformée de Fourier). Ceci implique de venir réaliser une étape de filtrage en sortie des étages de SPDC. Nous revenons ici sur cette notion et introduisons les différents filtres utilisés au sein de notre dispositif expérimental.

Intensité spectrale jointe

En négligeant les contributions des doubles paires et en notant η l'efficacité du processus de conversion, l'état en sortie d'un cristal de SPDC s'écrit :

$$|\psi(\omega_s,\omega_i)\rangle = |0\rangle + \eta \int_0^\infty \mathrm{d}\,\omega_s \int_0^\infty \mathrm{d}\,\omega_i\; \alpha(\omega_s+\omega_i)\phi(\omega_s,\omega_i)\hat{a}_s^\dagger(\omega_s)\hat{a}_s^\dagger(\omega_i)\,|0\rangle\,, \tag{3.4}$$

où $\phi(\omega_s+\omega_i)$ et $\alpha(\omega_s+\omega_i)$ représentent l'accord de phase colinéaire :

$$\phi(\omega_s,\omega_i) = \mathrm{sinc}\left(\frac{\Delta kL}{2}\right) \quad e^{\dfrac{i\Delta kL}{2}}, \tag{3.5}$$

et où $\alpha(\omega_s+\omega_i)$ représente l'enveloppe de la pompe. D'après le profil spectral du faisceau à 770 nm donné en FIGURE 3.15b, nous avons décrit l'enveloppe de la pompe comme une gaussienne centrée à deux fois la fréquence centrale du spectre de SPDC, ω_0, et définie comme :

$$\alpha(\omega_s+\omega_i) = e^{-\left(\dfrac{\omega_s+\omega_i-2\omega_0}{\sigma}\right)^2}. \tag{3.6}$$

σ est défini à partir de la largeur à mi-hauteur de l'intensité spectrale de la pompe comme :

$$\sigma = \frac{\Delta\omega_p}{\sqrt{2\ln 2}} = \frac{2\pi c}{\lambda_{0p}^2}\frac{\Delta\lambda_p}{\sqrt{2\ln 2}}, \tag{3.7}$$

où $\Delta\omega_p$ et $\Delta\lambda_p$ sont les largeurs à mi-hauteur de l'intensité spectrale de la pompe, respectivement mesurées dans les domaines des fréquences et des longueurs d'onde. D'après la FIGURE 3.15b, cette largeur spectrale est ici égale à 0,5 nm.

Il est possible de regrouper ces deux fonctions en une seule, $f(\omega_s, \omega_i) = \alpha(\omega_s + \omega_i)\phi(\omega_s, \omega_i)$, communément appelée amplitude spectrale jointe du signal, et d'utiliser cette nouvelle fonction pour décrire l'intensité spectrale jointe des paires de photons générées :

$$F(\omega_s, \omega_i) = |f(\omega_s, \omega_i)|^2. \tag{3.8}$$

Pour une paire de photons donnée, cette dernière s'interprète comme la probabilité jointe de détecter le photon signal à ω_s et le photon idler à ω_i.

Factorisation et pureté

En ignorant la composante de vide, qui sera de toute manière éliminée avec notre schéma de détection annoncée (voir section 3.3.6, et en s'affranchissant de la constante représentant l'efficacité de conversion du processus, l'état bi-photon s'écrit alors :

$$|\Psi(\omega_s, \omega_i)\rangle = \int_0^\infty \mathrm{d}\,\omega_s \int_0^\infty \mathrm{d}\,\omega_i \; f(\omega_s, \omega_i)\hat{a}_s^\dagger(\omega_s)\hat{a}_s^\dagger(\omega_i)\,|0\rangle\,. \tag{3.9}$$

On est en présence d'un état pur, dont l'amplitude spectrale jointe peut contenir des corrélations entre les degrés de liberté spatiaux-temporels des photons. Cette description de $|\Psi(\omega_s, \omega_i)\rangle$ est celle, dans le cas général, d'un état intriqué. En présence d'un tel état, lorsque l'un des photons de la paire est détecté, le second se retrouve alors dans un mélange statistique des différents modes spectraux.

Toutefois, une condition indispensable à la synchronisation du lien relais est que les photons prenant part à l'interférence soient dans des états à la fois purs spectralement et indiscernables. Plus spécifiquement, la visibilité $V = \mathrm{Tr}\,\{\hat{\rho}_1\hat{\rho}_2\}$ d'une figure d'interférence à deux photons (1 et 2) peut s'écrire, de sorte à faire apparaître pureté et discernabilité, comme :

$$V = \frac{\mathrm{Tr}\,\{(\hat{\rho}_1)^2\} + \mathrm{Tr}\,\{(\hat{\rho}_2)^2\} - ||\hat{\rho}_1 - \hat{\rho}_2||^2}{2}, \tag{3.10}$$

où :

$$||\hat{\rho}_1 - \hat{\rho}_2||^2 = \mathrm{Tr}\left\{(\hat{\rho}_1)^2\right\} + \mathrm{Tr}\left\{(\hat{\rho}_2)^2\right\} - 2\mathrm{Tr}\,\{\hat{\rho}_1\hat{\rho}_2\}\,. \tag{3.11}$$

La seule façon de projeter un photon annoncé dans un état pur est de travailler avec des paires de photons non-intriquées, autrement dit, de travailler avec des amplitudes spectrales jointes factorisables : $f(\omega_s, \omega_i) = g_s(\omega_s)g_i(\omega_i)$. Une façon d'y parvenir consiste à fabriquer des cristaux présentant des accords de phase très particuliers permettant d'éliminer directement les corrélations à la source, toutefois, dans la majorités des expériences, et ce sera également notre cas, ces corrélations sont éliminés en aval au moyen d'une ou plusieurs opérations de filtrage.

Décomposition de Schmidt

Si l'on considère, en sortie des étages de SPDC des états bi-partites initiaux non factorisables, il est essentiel de disposer d'une méthode précise permettant de quantifier les corrélations et d'estimer le degré de pureté attendu pour les photons annoncés. La méthode la plus intuitive consiste à effectué la décomposition de Schmidt des états bi-partites.

En algèbre linéaire, la décomposition de Schmidt se réfère à une manière particulière de décomposer, sur une base complète, un vecteur d'état comme une superposition linéaire. Par exemple, la décomposition de Schmidt de l'état $|\Psi(\omega_s, \omega_i)\rangle$ peut être trouvé en décomposant ce vecteur comme [5] :

$$|\Psi(\omega_s, \omega_i)\rangle = \sum_j \sqrt{\lambda_j} \, |\zeta_j(\omega_s)\rangle \, |\xi_j(\omega_i)\rangle \,, \tag{3.12}$$

où les coefficients de Schmidt λ_j sont réels, non-négatifs, et normalisés, de sorte que $\sum_j \lambda_j = 1$. Les vecteurs $|\zeta_j(\omega_s)\rangle$ et $|\xi_j(\omega_i)\rangle$ de la base orthonormée sont généralement appelés modes de Schmidt. Le nombre d'éléments requis dans la somme pour décomposer $|\Psi(\omega_s, \omega_i)\rangle$ sur les modes de Schmidt indique alors le degré de factorisation de l'état bi-partite. Ceci est quantifié au moyen du nombre de Schmidt, K, défini comme :

$$K = \frac{1}{\sum_j (\lambda_j)^2} = \frac{1}{\mathrm{Tr}\left\{(\hat{\rho}_s)^2\right\}} = \frac{1}{\mathrm{Tr}\left\{(\hat{\rho}_i)^2\right\}}. \tag{3.13}$$

K est une mesure du nombre de modes fréquentiels actifs dans l'état bi-photon, c'est par conséquent un témoin d'intrication.

À partir de nos mesures, un moyen d'estimer le nombre de Schmidt associés aux états produits consiste à comparer le temps de cohérence $\tau_{s,i}$ des photons générés avec la durée δt des impulsions du laser de pompe. Le rapport de ces deux grandeurs nous permet ainsi d'estimer le nombre de modes actifs à $K = 22$.

Paires de photons corrélées et filtrage

Comme le montre la FIGURE 3.21a, la largeur du spectre d'émission en sortie de SPDC est de 80 nm et contient une vingtaine de modes actifs. Pour ne conserver plus qu'un seul mode spectral, nous avons recours à deux types de filtres qui nous permettent d'effectuer une séparation déterministe des photons *signal* et *idler*, voir FIGURE 3.21b :

- Un DWDM de bande passante 100 GHz (800 pm) centré à la longueur d'onde de 1543,73 nm (ITU 42) est directement connectorisé à la fibre de récolte de chaque cristal de SPDC. La transmission de ces filtres est dirigée sur les canaux externes de notre dispositif, tandis que la réjection est envoyée en direction de la station

relais.

- Un unique filtre de Bragg (FBG) de bande passante 25 GHz (200 pm) placé au sein de la station relais vient ensuite sélectionner les photons jumeaux, destinés à interférer, à la longueur d'onde de 1536,27 nm. La réjection du FBG, pour éviter toute réflexion, est dirigée vers une fiole contenant du liquide d'indice.

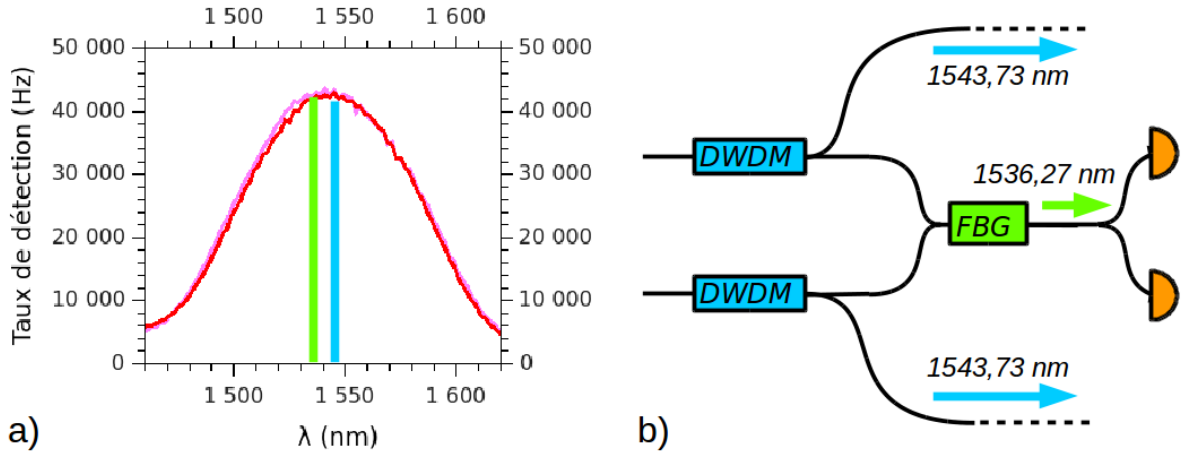


Figure 3.21. – **a)** Position des longueurs d'ondes centrales des filtres. **b)** Représentation schématique de la disposition des filtres au sein de notre dispositif.

Les DWDM utilisés présentent un taux de réjection de 30 dB (99,9%) combiné à un taux de transmission de l'ordre de 95%. De plus, ce type de filtre présente un profil de transmission (quasi) rectangulaire qui est avantageux pour l'optimisation des pertes en matière de transmission des paires de photons. Par ailleurs, ces DWDM présentent une longueur d'onde centrale intrinsèquement stable au cours du temps, et ne montrent qu'une très faible dépendance en transmission à la polarisation incidente. De plus, ce type de composants issus des télécoms optiques, sont relativement bon marché.

Un filtre de Bragg fibre alterne des couches de deux matériaux d'indices de réfraction différents, ce qui provoque une variation périodique de l'indice de réfraction effectif de la fibre optique, voir FIGURE 3.22a. Un choix de modulation adéquat permet d'atteindre des bandes passantes de 10 GHz [7].

7. Insérer un défaut de phase au sein de la fibre peut même permettre de d'atteindre des bandes passantes de l'ordre de quelques MHz. C'est en quelque sorte l'équivalent à fibre d'une cavité optique en espace libre, puisque l'insertion d'un défaut de phase de π au milieu d'un FBG ordinaire forme en effet l'équivalent d'un système de deux miroirs

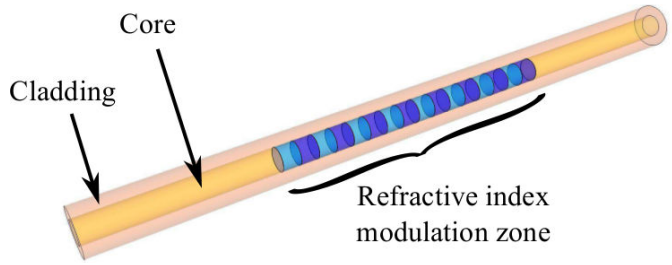


Figure 3.22. – Représentation schématique d'un filtre de Bragg à fibre standard (FBG).

3.3.5. Station relais

Pour assurer l'indiscernabilité en polarisation des photons se présentant au niveau du nœud relais, nous avons reproduit pour la station relais le dispostif expérimental schématisé en FIGURE 3.23.

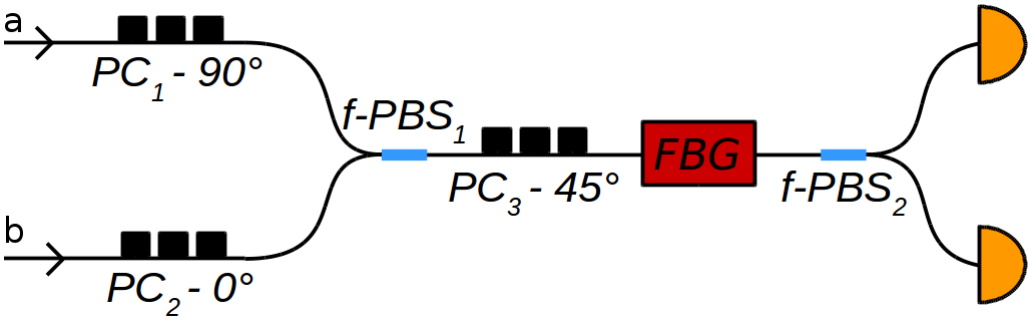


Figure 3.23. – Station relais : schéma du dispositif expérimental.

Étant donné que les modes de polarisation sont associés aux différents modes spatiaux, l'état quantique en entrée du dispositif s'écrit :

$$\begin{aligned} |\psi\rangle_{in} &= \left(\alpha_a |H_a\rangle + \beta_a e^{i\phi_a} |V_a\rangle\right)\left(\alpha_b |H_b\rangle + \beta_b e^{i\phi_b} |V_b\rangle\right), \\ &= \alpha_a\alpha_b |H_a, H_b\rangle + \beta_a\beta_b e^{i(\phi_a+\phi_b)} |V_a, V_b\rangle + \alpha_a\beta_b e^{i\phi_b} |H_a, V_b\rangle + \beta_a\alpha_b e^{i\phi_a} |V_a, H_b\rangle, \end{aligned} \tag{3.14}$$

où a et b correspondent respectivement aux modes spatiaux du haut et du bas. On est en présence de deux photons indépendants dans des états de superposition arbitraire de $|H\rangle$ et de $|V\rangle$. De sorte à optimiser le taux de transmission du premier PBS fibré (f-PBS$_1$), les polarisations des deux photons sont respectivement orientées de manière horizontale et verticale à l'aide de deux contrôleurs de polarisation (PC$_1$ et PC$_2$) :

$$|\psi\rangle_{PC_{1,2}} = e^{i\phi_b} |H_a, V_b\rangle \,, \tag{3.15}$$

Immédiatement après le franchissement du f-PBS$_1$, on est alors en présence de l'état :

$$|\psi\rangle_{PBS_1} = |H, V\rangle \,. \tag{3.16}$$

Ici, nous avons volontairement omis la phase globale qui n'apporte rien à notre discussion. Un troisième contrôleur de polarisation (PC$_3$) tourne alors la polarisation des photons de 45° :

$$|\psi\rangle_{PC_3} = \left(\frac{-|H\rangle + |V\rangle}{\sqrt{2}}\right)\left(\frac{|H\rangle + |V\rangle}{\sqrt{2}}\right), \tag{3.17}$$

$$= \frac{1}{2}\left(-|H, H\rangle + |V, V\rangle + |H, V\rangle - |V, H\rangle\right), \tag{3.18}$$

avant que ces derniers, après passage au sein du filtre de Bragg (FBG), ne franchissent le PBS fibré de sortie (f-PBS$_2$) :

$$|\psi\rangle_{PBS_2} = \frac{1}{2}\left(-|H_a, H_a\rangle + |V_b, V_b\rangle + |H_a, V_b\rangle - |V_b, H_a\rangle\right). \tag{3.19}$$

Finalement, en post-sélectionnant uniquement les événements correspondants à des coïncidences, on obtient alors l'état :

$$|\psi\rangle = \frac{|H_a, V_b\rangle - |V_b, H_a\rangle}{\sqrt{2}}. \tag{3.20}$$

Dès lors, on s'aperçoit qu'il impossible, à partir du mode de polarisation, de dire si un photon détecté sur le détecteur du bras supérieur provenait initialement de ce même bras ou du bras inférieur. De plus, si jamais une rotation de la polarisation des photons avait lieu de manière incontrôlée en amont de la station relais, un PBS agissant comme un filtre, aucune perte de visibilité au sein de la figure d'interférence à deux photons ne serait observée, seul le débit serait affecté.

Notons enfin que la présence d'un unique filtre de Bragg au sein de la station relais permet d'assurer un parfait recouvrement des modes fréquentiels, que ce soit en terme de longueur d'onde centrale ou de largeur spectrale. L'accordabilité du filtre nous permet également, si jamais un décalage de la longueur d'onde centrale de l'horloge optique advenait au cours du temps, de pouvoir le rattraper facilement.

3.3.6. Système de détection

Pour conclure cette présentation des différents bloques constitutifs de notre dispositif expérimental, nous présentons ici le schéma de détection utilisé.

Schéma du circuit électronique

Traditionnellement, on a recours dans ce type d'expériences à deux détecteurs à haute cadence et à bas niveau de bruit que l'on dispose sur les voies externes du dispositif, typiquement des détecteurs supraconducteurs (voir annexe C pour le principe de fonctionnement), de sorte à annoncer l'arrivée des photons en sortie de la station relais où deux APD en régime de fonctionnement déclenché sont positionnées. Les détections quadruples sont alors comptabilisées à l'aide de deux modules de coïncidences (*Time to Amplitude Converter* ou *Time to Digital Converter*, voir annexe C pour le principe de fonctionnement) et d'une porte logique 'ET' à laquelle sont envoyés les signaux de sorties des convertisseurs. Ne disposant pas de détecteurs supraconducteurs au moment de réaliser cette expérience, un schéma alternatif a du être imaginé, ce dernier est illustré en FIGURE 3.24.

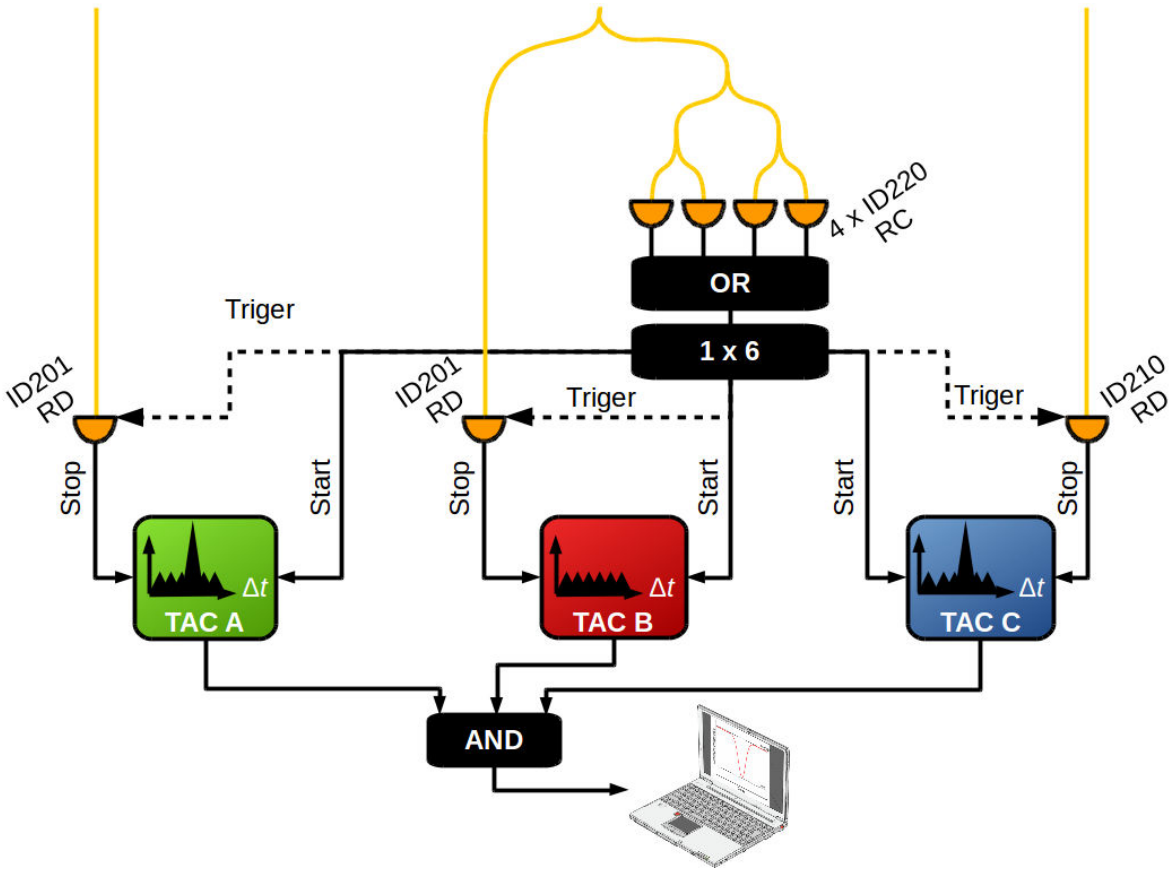


Figure 3.24. – Schéma de l'électronique de détection. RC : Régime Continu ; RD : Régime Déclenché.

Trois APD en régime déclenché (2x ID201, 1x ID210, voir annexe C) sont respectivement placées sur les deux voies externes et l'une des deux voies de sortie de la station relais, tandis que nous avons simulé un 'super-détecteur' en régime de fonctionnement continu sur la dernière voie vacante (deuxième sortie de la station relais). Ce super-détecteur repose sur le multiplexage spatial de quatre APD (4x ID220, performances détaillées en annexe C) dont les signaux de sorties sont envoyés jusqu'à une porte logique 'OU', de sorte à ne former plus qu'un unique signal. Ce 'super-détecteur', bien qu'il présente des performances très en deçà de celle d'un détecteur supraconducteur, nous permet toutefois de réaliser nos mesures en des temps raisonnables (quelques heures) grâce à un taux de détection avant saturation de l'ordre de 200 kHz. Trois convertisseurs temps/amplitude (TAC), nous permettent ensuite de dresser un histogramme des coïncidences pour chaque APD déclenchée. Enfin, après post-sélection pour chaque TAC du 'bon pic de coïncidence' (nous allons revenir sur le sens de cette formulation par la suite) à l'aide d'un *single channel analyzer* (SCA), les signaux de sortie des TAC sont envoyés à une porte 'ET' qui génère alors un nouveau signal de sortie pour chaque nouveau cas de coïncidence quadruple.

Post-sélection

Bien que conceptuellement très simple, ce schéma de détection nous impose de prendre certaines précautions vis-à-vis de la post-sélection.

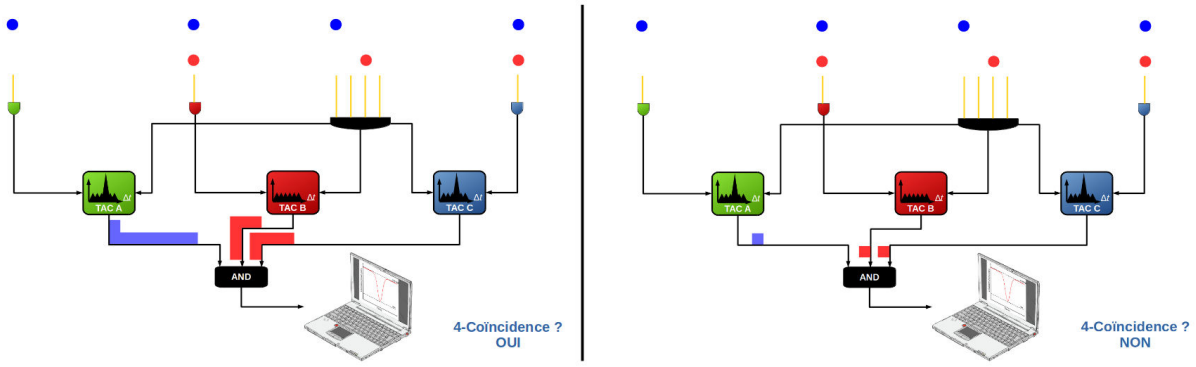


Figure 3.25. – **a)** Cas de signaux électroniques mal ajustés en sortie des TAC. Les signaux électroniques se recouvrent alors qu'optiquement les photons à l'origines de ces signaux ne correspondent pas tous au même *time tag*. **b)** Cas de signaux électroniques bien ajustés, les fausses coïncidences quadruples sont discriminées des bons événements en raccourcissant la durée des signaux de sortie des TAC. Aucun recouvrement de signaux électroniques associés à des photons avec différents *time tags* n'a alors lieu.

La première difficulté provient du multiplexage spatial des quatre détecteurs continus. Le fait de multiplexer spatialement ces quatre détecteurs est équivalent à travailler avec

un unique détecteur dont le temps de relaxation serait négligeable. En effet, lorsqu'un photon contenu dans une première impulsion est détecté, l'un des quatre détecteurs devient temporairement indisponible (temps de relaxation) mais les trois autres restent quant à eux ouverts et peuvent ainsi immédiatement détecter à leur tour un photon contenu dans l'une des impulsions successives à la première. Dès lors, il est possible dans la suite du circuit électronique, si la durée des signaux électroniques en sortie des SCA est plus grande que l'intervalle temporel entre deux impulsions optiques successives, d'enregistrer de fausses détections quadruples, voir FIGURE 3.25a. Pour s'affranchir de ce problème, nous avons réduit la durée des signaux de sorties des SCA avant d'envoyer ces derniers en direction de la porte 'ET', voir FIGURE 3.25b.

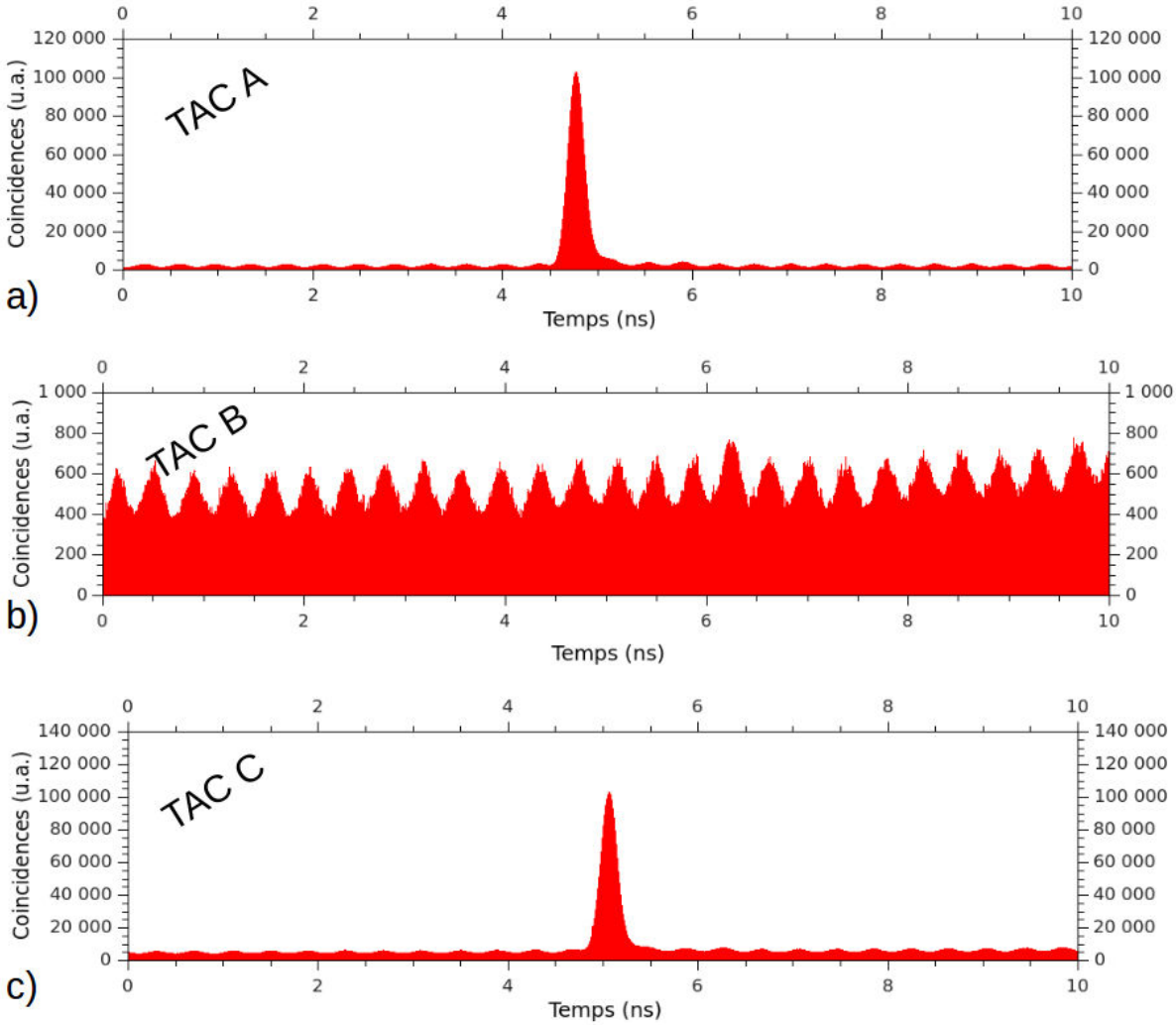


Figure 3.26. – Histogrammes typiques des coïncidences relevés sur les différents TAC.

La deuxième difficulté provient quant à elle du signal à post-sélectionner au niveau du TAC central (TAC B sur l'illustration). Lorsqu'on s'intéresse aux trois histogrammes de coïncidences, voir FIGURE 3.26, on observe à chaque fois une succession de pics. La largeur des pics correspond à la convolution des *jitters* des détecteurs, et l'intervalle entre pics successifs correspond à l'inverse du taux de répétition de l'horloge optique, à savoir 0.4 ns. Parmi tous ces pics, l'un d'eux correspond au cas de coïncidences entres photons générés par une même impulsion de pompe, alors que les deux pics qui lui sont adjacents correspondent aux cas de coïncidences entre photons décalés d'une impulsion, et ainsi de suite de proche en proche. Ces différentes situations s'expliquent physiquement par les pertes (propagation et détection) qui introduisent des multiples du taux de répétition dans les temps des détections. Dans le cas plus spécifique de coïncidences entre photons générés au sein d'un même cristal, les photons étant émis par paires, la contribution au pic correspondant à une même impulsion de pompe devient prépondérante. C'est ainsi que l'on voit clairement un pic de coïncidence émerger du bruit dans le cas des TAC A et C, pic que l'on vient ensuite post-sélectionner à l'aide de SCA. En revanche, dans les cas du TAC B, seules sont enregistrées des coïncidences entre photons provenant de sources indépendantes. Dans ce cas précis, aucun pic n'émerge à un niveau supérieur à celui des autres et ils nous est dès lors impossible de savoir quel pic post-sélectionner pour enregistrer ces coïncidences quadruples.

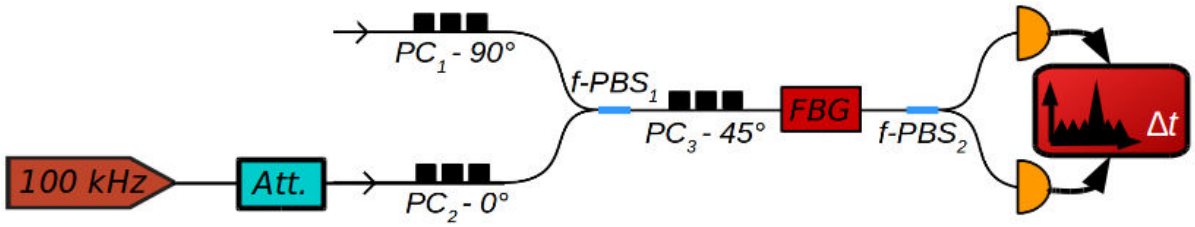


Figure 3.27. – Sélection du pic de coïncidence en sortie de la station relaie par injection dans l'une des deux voies d'entrée de la station d'un signal atténué issu d'un laser impulsionnel présentant un taux de répétition bien inférieur à celui de notre horloge optique. Dans ces conditions seul un pic apparaît dans la fenêtre du TAC, les autres étant situés hors fenêtre. Il nous reste alors plus qu'à marquer la position de ce pic avant de réinjecter notre horloge optique. Att : atténuateur.

Pour lever cette difficulté, l'idée consiste alors à momentanément injecter dans l'une des deux voies d'entrée de la station relais, voir FIGURE 3.27, un signal atténué issu d'un laser impulsionnel présentant un taux de répétition bien inférieur à celui de notre horloge optique. Dans ces conditions seul un pic apparaît dans la fenêtre du TAC, les autres étant situés hors fenêtre. Il nous reste alors plus qu'à marquer la position de ce pic avant de réinjecter notre horloge optique. Aucune longueur n'ayant été modifiée au cours de cette manipulation, le bon pic à post-sélectionner est ainsi celui qui coïncide

avec la position que nous venons de marquer. Pour effectuer cette opération nous avons eu recours à un laser émettant des impulsions ayant une durée de 300 ps à un taux de répétition ajustable que nous avons pris égal à 100 kHz. À titre de comparaison, les fenêtres de nos TAC sont elles de 10 ns.

3.4. Étude de la visibilité en fonction de la statistique d'émission

Depuis le début de ce chapitre nous avons supposé que seul deux photons se présentent à la station relais. Toutefois, un paramètre critique dans les expériences de synchronisation est la statistique d'émission, et en particulier la contribution des multi-paires. Cette dernière, si elle n'est pas négligeable, altère la visibilité de la figure d'interférence. Nous revenons dans cette section sur ces différents aspects.

3.4.1. Nombre moyen de paires générées par impulsion

À partir du taux de détection dans le canal associé au signal d'annonce (R_H, taux de détection du 'super-détecteur'), il est possible, connaissant le taux de répétition de l'horloge (f_{Rep}), le couplage dans la fibre de récolte en sortie de guide (γ), les pertes à la propagation (α) et l'efficacité du système de détection (η_H), d'estimer le nombre moyen ($\bar{n}$) de paires générées par impulsion. La relation, assez intuitive, reliant ces différentes grandeurs est la suivante [254] :

$$\frac{R_H}{2} = f_{Rep} \cdot \bar{n} \cdot \gamma \cdot \alpha \cdot \eta_H, \tag{3.21}$$

où un facteur 1/2 a été introduit du fait que les photons détectés proviennent ici de deux sources indépendantes présentant, à puissances incidentes de pompe identiques, des statistiques d'émission similaires.

Sachant que le taux maximum de photons qu'il nous est possible de détecter avant saturation des détecteurs est d'environs 200 kHz, que leur efficacité est de 20%, que le couplage dans les fibres de récolte est de 60% et que les pertes dans les canaux centraux sont d'environs 7 dB, on estime le nombre moyen de paires émises par impulsion de pompe à : $\bar{n} = 1,6 \cdot 10^{-2}$.

3.4.2. Statistique d'émission

Comme nous l'avions démontré en section 2.5.1, la statistique d'émission des paires dépend du caractère monomode ou multimode en fréquence du signal généré. À une émission monomode est associée une statistique de type Bose-Einstein :

$$P_{B-E}(n,\bar{n}) = \frac{1}{(1+\bar{n})}\left(\frac{\bar{n}}{1+\bar{n}}\right)^{n}, \tag{3.22}$$

tandis qu'à une émission multi-mode est associée une statistique de Poisson :

$$P_{P}(n,\bar{n}) = \frac{\bar{n}^{n}e^{-\bar{n}}}{n!}. \tag{3.23}$$

Dans notre cas, les filtres nous permettent, comme nous l'avons vu, de ne conserver qu'un unique mode actif au niveau de la station relais. Dès lors, nous devons considérer pour l'estimation de la visibilité le cas d'une statistique d'émission de type Bose-Einstein.

3.4.3. Visibilité

Dans ce qui suit, nous dénoterons par 'in' les deux canaux internes du dispositif (stations relais), et par 'ext' les deux canaux externes.

Commençons par définir les états quantiques entrant par la voie $i \in (a,b)$ de la station relais, que nous pouvons écrire à l'aide du formalisme des états de Fock sous la forme :

$$|\Psi_i\rangle_{in} = p_{0,i}\,|0_i\rangle_{in} + p_{1,i}\,|1_i\rangle_{in} + p_{2,i}\,|2_i\rangle_{in} + O^3, \tag{3.24}$$

avec $|p_{0,i}|^2 = P_{0,i}$, $|p_{1,i}|^2 = P_{1,i}$ et $|p_{2,i}|^2 = P_{2,i}$ représentant respectivement les probabilités d'avoir 0, 1 où 2 photons. Nous considérons, pour cette étude, la probabilité d'avoir 3 photons comme négligeable. En tenant compte des notations que l'on vient d'introduire, la visibilité est, en première approximation, donnée par :

$$V \approx \frac{1}{1 + \dfrac{P_{2,a}P_{0,b}}{P_{1,a}P_{1,b}} + \dfrac{P_{0,a}P_{2,b}}{P_{1,a}P_{1,b}}}. \tag{3.25}$$

En ne considérant dans le calcul des différentes probabilités uniquement la propagation de photons au sein de la station relais, il est possible de montrer que la visibilité ne peut excéder 33%. Afin d'atteindre une visibilité maximale, il est alors obligatoire de conditionner la détection en sortie de la station relais à la détection de photons sur les voies externes, voir explications détaillées au chapitre 2 du manuscrit de thèse [261].

Dans le cas où une unique paire a été générée, un photon sera détecté sur un canal externe si il est à la fois couplé dans la fibre, si il se propage jusqu'au détecteur, et s'il est vu par ce dernier. La probabilité associée est ainsi simplement :

$$\gamma \cdot \alpha_{ext} \cdot \eta_{ext}, \tag{3.26}$$

où nous avons repris les notations précédemment introduites. Dans le cas d'une double paire la situation devient plus complexe, il faut considérer le cas où le premier photon est détecté mais aussi le cas où le second photon est détecté sachant que le premier ne l'a pas été. La probabilité d'obtenir une détection s'écrit alors :

$$\gamma \cdot \alpha_{ext} \cdot \eta_{ext} + \gamma \cdot \alpha_{ext} \cdot \eta_{ext} \cdot (1 - \gamma \cdot \alpha_{ext} \cdot \eta_{ext}) = \gamma \cdot \alpha_{ext} \cdot \eta_{ext} \cdot (2 - \gamma \cdot \alpha_{ext} \cdot \eta_{ext}). \quad (3.27)$$

Sachant cela, il est maintenant possible de calculer $P_{0,i}$, $P_{1,i}$ et $P_{2,i}$ pour les deux canaux internes. Notre dispositif étant parfaitement symétrique du point de vue des pertes, nous omettrons l'indice i dans ce qui suit. Le cas le plus simple à traiter est celui du P_2, il correspond à la situation de deux photons collectés ayant réussi à se propager à travers les canaux centraux :

$$P_2 = \gamma \cdot \alpha_{ext} \cdot \eta_{ext} \cdot (2 - \gamma \cdot \alpha_{ext} \cdot \eta_{ext}) \cdot (\gamma \cdot \alpha_{int})^2 \cdot P_{B-E}(2, \bar{n}). \quad (3.28)$$

Pour calculer P_1 il faut considérer les contributions respectives d'une double paire et d'une simple paire. Dans le premier scenario, la contribution correspond au cas où un photon a été perdu tandis que le second continue à se propager [8], alors que dans le second scenario seul un unique photon se propage. Nous avons ainsi :

$$\begin{aligned} P_1 =& \gamma \cdot \alpha_{ext} \cdot \eta_{ext} \cdot (2 - \gamma \cdot \alpha_{ext} \cdot \eta_{ext}) \cdot 2\gamma \cdot \alpha_{int}(1 - \gamma \cdot \alpha_{int}) \cdot P_{B-E}(2, \bar{n}) \\ &+ \gamma \cdot \alpha_{ext} \cdot \eta_{ext} \cdot \gamma \cdot \alpha_{int} \cdot P_{B-E}(1, \bar{n}). \end{aligned} \quad (3.29)$$

Enfin, dans le cas de P_0, soit une double paire a été émise et il faut considérer que les deux photons ont été perdus, soit une simple paire a été émise et donc qu'un seul photon est perdu :

$$\begin{aligned} P_0 =& \gamma \cdot \alpha_{ext} \cdot \eta_{ext} \cdot (2 - \gamma \cdot \alpha_{ext} \cdot \eta_{ext}) \cdot (1 - \gamma \cdot \alpha_{int})^2 \cdot P_{B-E}(2, \bar{n}) \\ &+ \gamma \cdot \alpha_{ext} \cdot \eta_{ext} \cdot (1 - \gamma \cdot \alpha_{int}) \cdot P_{B-E}(1, \bar{n}). \end{aligned} \quad (3.30)$$

La FIGURE 3.28 représente la visibilité attendue en fonction de $\bar{n}$ dans les conditions de notre dispositif, à savoir respectivement 3 et 7 dB de pertes à la propagation sur les canaux externes et internes, 60% de couplage dans les fibres de récolte en sortie des cristaux, et 20% d'efficacité de détection. Dans cette configuration, nous pouvons espérer obtenir plus de 90% de visibilité lorsque $\bar{n}$ est inférieure à 0,04 paires générées par impulsion.

8. Comme les rôles des deux photons sont interchangeables, la contribution est à comptabiliser deux fois.

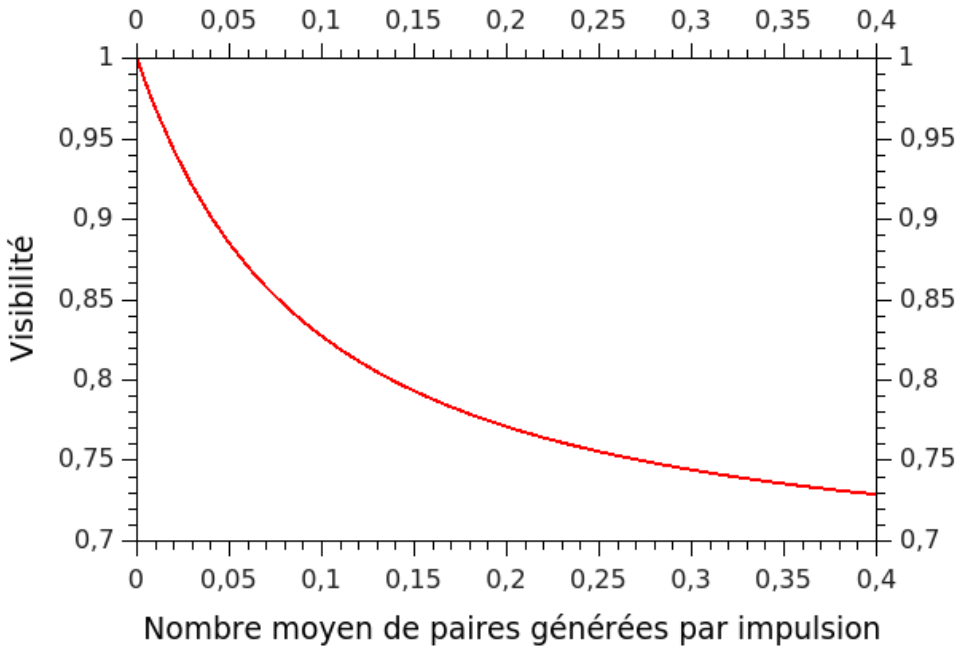


Figure 3.28. – Visibilité en fonction du nombre moyen de paires émises par les sources pour des distributions de Bose-Einstein et pour les pertes de notre dispositif. Au sein de notre dispositif expérimental, cette distribution est garantie par l'étage de filtrage qui permet de sélectionner, pour les photons qui interfèrent à la station relais, un seul mode fréquentiel.

3.5. Position de la figure d'interférence

L'intervalle spatial entre impulsions de pompe successives est de 12 cm dans le vide, tandis que la largeur à mi-hauteur attendue du *dip* est elle d'environs 6 mm avec le système de filtrage décrit à la section 3.3.4. Avec de telles valeurs, évaluer l'emplacement du *dip* en scannant la position du retroréflecteur jusqu'à observer une chute du taux de coïncidences quadruples pourrait nous prendre, à raison d'une heure par point, jusqu'à plus d'un jour. Pour éviter ce désagrément, nous avons eu recourt à une mesure d'interférence classique pour estimer la position attendue de la figure d'interférence quantique.

En retirant les filtres coupe-bande en sortie des étages de doublage de fréquence et en ôtant le FBG de la station relais, nous avons laissé se propager librement les impulsions à 1540,0 nm émisent par l'horloge à travers tout le dispositif (à l'exception des canaux externes du fait de la présence des DWDM), voir FIGURE 3.29. Dès lors, en déconnectant les détecteurs de photons uniques et en positionnant un puissance-mètre en sortie de l'une des deux voies de la station relais, il devient possible, comme nous

l'avions déjà fait à la section 3.3.1, de superposer les trains d'impulsions en vis-à-vis. Pour cela il nous suffit de déplacer, avec un pas inférieur au mm, la position du retroréflecteur jusqu'à observer des franges d'interférences. La position du *dip* doit alors correspondre à celle du maximum de visibilité observé classiquement. Une fois la position trouvée, il ne reste alors plus qu'à replacer tous les filtres et commencer la mesure du *dip*. Notons que déconnecter et reconnecter le FBG, qui empêche le signal à 1540,0 nm de passer, n'a aucune incidence sur la position attendu du *dip* puisque le FBG se trouve au sein de la station relais, il n'influe donc pas sur la longueur des deux bras.

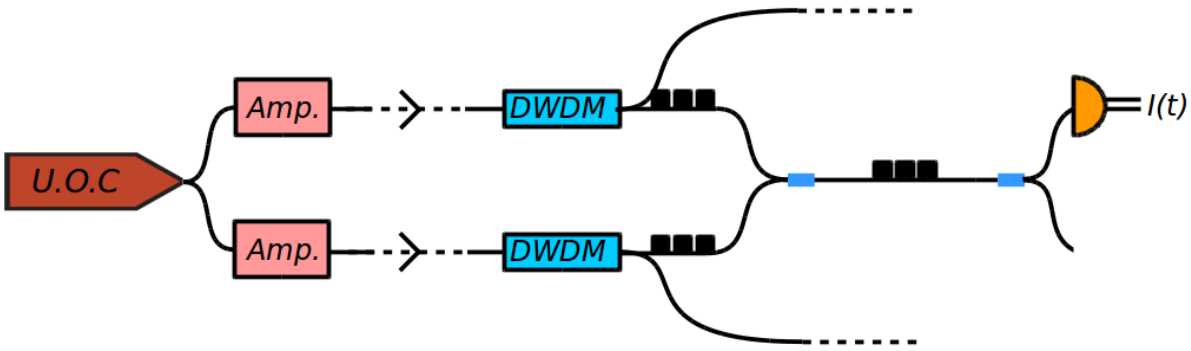


Figure 3.29. – Montage expérimental permettant d'estimer la position à laquelle se trouver le creux du *dip* au moyen d'une interférence classique.

3.6. Résultats

Nous présentons dans cette section les différents résultats obtenus validant la synchronisation du lien relais.

3.6.1. Résultats préliminaires

Avant de présenter les résultats finaux obtenus en présence de 100 km de distance effective entre les sources de paires de photons intriqués, nous revenons tout d'abord sur différents résultats préliminaires obtenus sur de courtes distances de transmission.

Mesures dans le temps de cohérence de l'horloge

La première mesure que nous avons souhaité réaliser à été de synchroniser des paires de photons générées dans les deux cristaux à partir d'une même impulsion de pompe. Ce choix permet de s'affranchir, dans un premier temps, de toute phase intempestive

qui pourrait éventuellement introduire un décalage des trains d'impulsions entre les deux bras. Cette mesure demande ainsi d'égaliser les deux trajets optiques séparant l'horloge optique de la station relais au mm près. À un taux de répétition de 2,5 GHz, la distance dans le vide séparant deux impulsions successives est de 12 cm. Compte tenus des nombreux composants optiques présents de part et d'autres du dispositif, il nous est impossible de de manière simple de nous assurer qu'il y a bien moins de 12 cm d'écart entre les deux bras.

Pour dans un premier temps égaliser les longueurs de manière grossière, à savoir dans la limite des *jitters* des détecteurs, nous avons momentanément remplacé notre horloge optique par un laser fs de taux de répétition 80 MHz émettant lui aussi à la longueur d'onde centrale de 1540 nm. Afin de permettre la libre propagation de ces impulsions à travers l'intégralité de notre dispositif, nous avons retiré les filtres coupe bande en sortie des cristaux de SHG. De plus, le régime fs garantissant un spectre large bande, il n'est pas nécessaire ici de retirer le FBG de la station relais comme nous l'avions fait en 3.5. Avec ce montage, nous monitorons à l'aide d'un TAC les coïncidences en sortie de la station relais [9], voir FIGURE 3.30, ce qui nous permet de venir égaliser les longueurs des deux bras via la fusion des pics de coïncidences correspondant aux différents chemins optiques que peut emprunter la lumière.

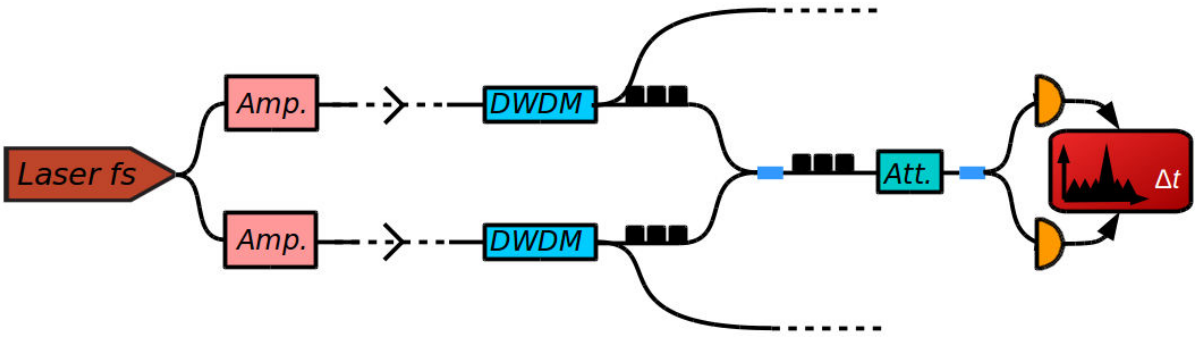


Figure 3.30. – Montage expérimental permettant d'égaliser, à l'impulsion près, la longueur des deux bras de notre dispositif.

Plus concrètement, l'histogramme de la fenêtre du TAC révèle des séries de trois pics. Ces trois pics correspondent respectivement aux cas de coïncidences : entre photons ayant uniquement empruntés le trajet court ou le trajet long (deux contributions, pic de hauteur double), entre un photon *start* ayant emprunté le trajet court et un photon *stop* ayant emprunté le trajet long, et inversement. L'écart entre pics d'une même série correspond ainsi au déséquilibre de l'interféromètre, à savoir 1 ns d'après la mesure re-

9. Une dernière précaution avant de lancer la mesure consiste à ne pas oublier de placer un atténuateur au sein de la station relais au risque d'endommager les détecteurs de photons uniques.

portée en FIGURE 3.31a où une seule série de trois pics est représentée, tandis que l'écart de 12,5 ns entre séries adjacentes correspond à l'inverse du taux de répétition. Dans le domaine spatial, ces 1 et 12,5 ns (inverse de 80 MHz) correspondent respectivement à 30 cm et à environ 4 m. Sachant que le déséquilibre que nous devons compenser est bien inférieur à 4 m, il nous reste ainsi plus qu'à égaliser les trajets en fusionnant les trois pics en un via l'ajout de 30 cm de fibre sur le bras le plus court, voir FIGURE 3.31b.

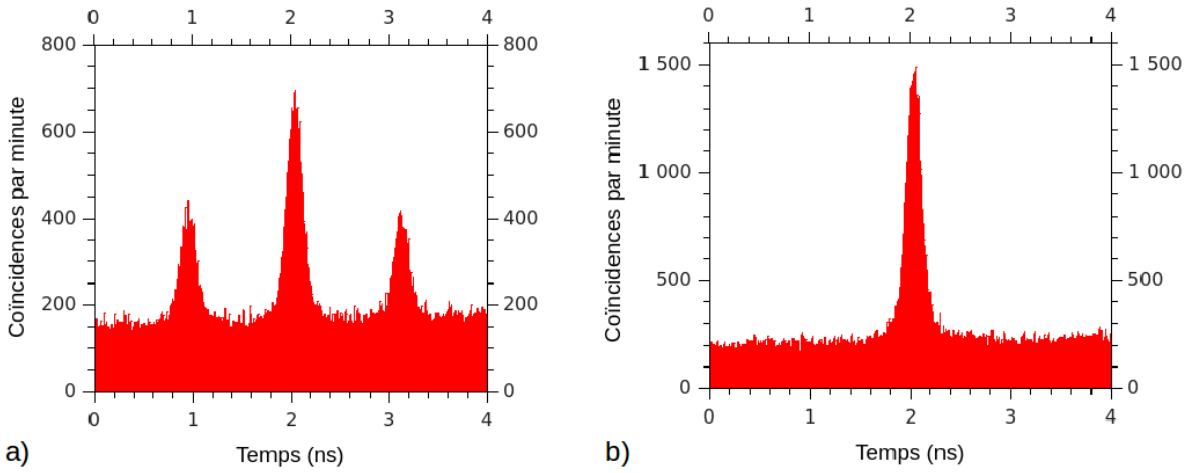


Figure 3.31. – **a)** Histogramme des coïncidences mesuré à l'aide d'un laser impulsionnel fs (80 MHz) atténué en présence d'une asymétrie d'environs 30 cm de fibre ($\sim$ 1 ns) entre les deux bras du dispositif. Les trois pics correspondent respectivement à la configuration long-court, long-long + court-court, court-long. **b)** Fusion des trois pics après avoir ajouté environs 30 cm de fibre sur le bras le plus court.

Une fois l'estimation précise de la position du *dip* effectuée via la technique présentée en section 3.5, nous avons finalement pu procéder à la mesure de ce dernier. En jouant sur la position du rétro-réflecteur situé entre les étages de SHG et de SPDC du bras supérieur, nous compensons la seule discernabilité restante entre les deux photons, à savoir celle de leur temps d'arrivée au niveau de la station relais.

Ainsi, lorsque le délai entre les deux photons est nul, nous observons une chute du taux de coïncidences quadruples comme le montre la figure FIGURE 3.32. La figure d'interférence présente une visibilité supérieure à 99%. Cette valeur est à la fois une visibilité brute et une visibilité net puisque aucun événement de bruit n'a été enregistré lors de la mesure annexe de ce dernier. De plus, la largeur à mi-hauteur du *dip*, qui est d'environ 6 mm, est en parfait accord avec le temps de cohérence de 17 ps de nos photons calculé à partir de la largeur du filtre de Bragg.

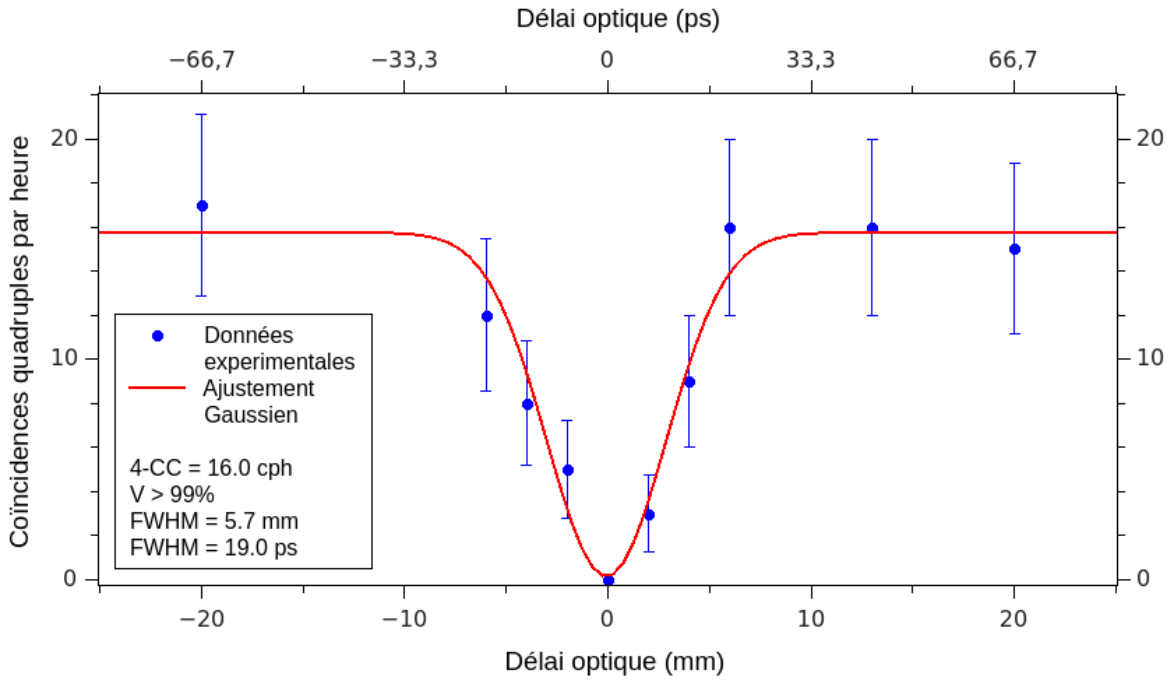


Figure 3.32. – Taux de coïncidences quadruples en fonction du délai optique. Cette mesure est effectuée dans une configuration où les longueurs des chemins optiques allant de l'horloge optique à la station relais sont ajustés, à l'impulsion près, de manière parfaitement symétrique.

Mesures hors du temps de cohérence de l'horloge

Dans une configuration hors laboratoire, notre dispositif sera nécessairement sujet à une asymétrie des longueur des deux bras. On peut par exemple imaginer une situation où un bras du dispositif aurait une longueur de 30 km tandis que la longueur du second serait elle de 50 km. En anticipation d'une telle situation, nous nous sommes posé la question de savoir si une telle asymétrie pouvait être responsable de l'introduction d'une phase non globale pouvant altérer la visibilité de la figure d'interférence à deux photons. Bien qu'il semble intuitif que seule une phase globale soit introduite dans un tel cas, nous avons tout de même souhaité vérifier cette affirmation par une nouvelle mesure.

Pour réaliser cette mesure, nous avons introduitune bobine de 400 m de fibre optique en amont du module amplificateur de l'un des deux bras. Cette longueur n'a pas été choisie au hasard puisqu'elle correspond, d'après la caractérisation présentée en section 3.3.1, à la longueur pour laquelle on observe une perte quasi-totale de cohérence entre les deux trains d'impulsions.

Le profil du *dip* que l'on obtient avec cette nouvelle configuration, voir FIGURE 3.33, est parfaitement similaire à celui obtenu dans le scenario symétrique (largeur à mi-hauteur et visibilité). Ce nouveau résultat confirme donc que seule une phase globale est introduite en présence d'un déséquilibre entre les distances de propagation de l'horloge.

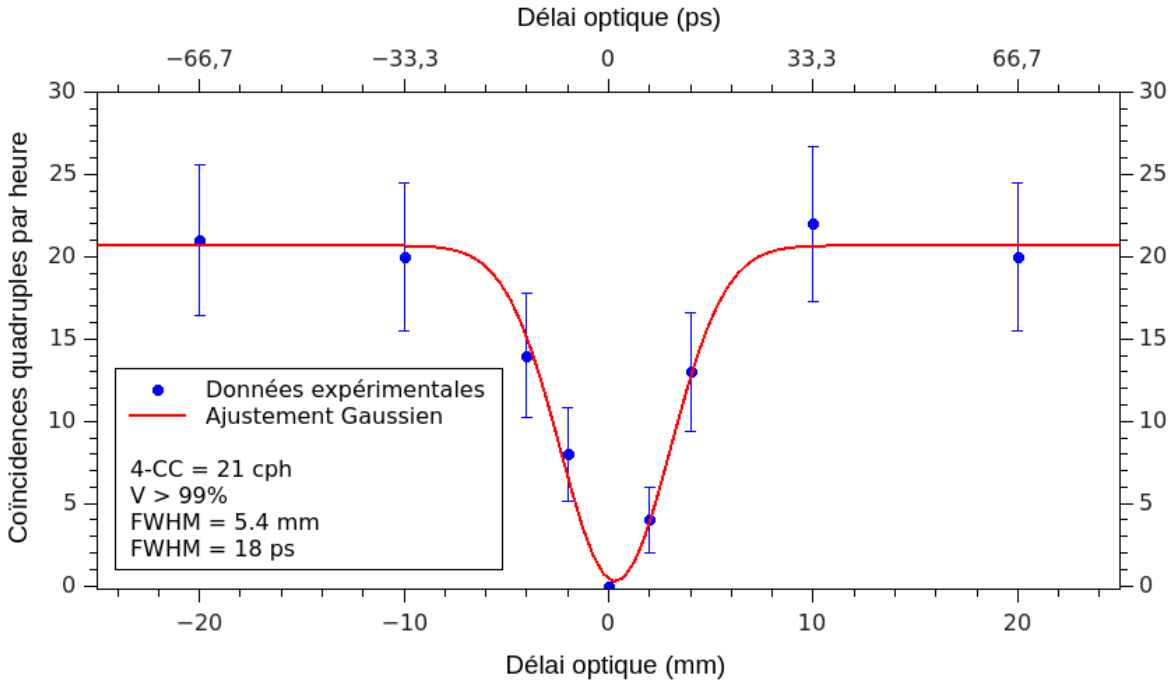


Figure 3.33. – Taux de coïncidences quadruples en fonction du délai optique. Cette mesure a été effectuée dans une configuration où les longueurs des chemins optiques allant de l'horloge optique à la station relais présentent une asymétrie de 400 m.

3.6.2. Synchronisation sur 100 km

Nous présentons les résultats finaux obtenus en présence d'un système de stabilisation active pour une distance effective entre sources de paires de photons de l'ordre 100 km. Ces résultats viennent valider notre schéma de synchronisation dans sa configuration finale.

Effets de dispersion chromatique

Un premier effet que nous avons négligé jusqu'à maintenant est celui de la dispersion chromatique dans les fibres. Compte tenu des distances dont il est question au sein de cette section, il nous faut désormais le prendre en compte également. Pour des photons appartenant à la bande-C des télécoms (1530-1565 nm), la dispersion engendre un

élargissement des impulsions de pompe d'environ 18 ps par nm de largeur spectrale et par km de fibre optique. Les impulsions de pompe ne sont dès lors plus limitées par transformée de Fourier transformes.

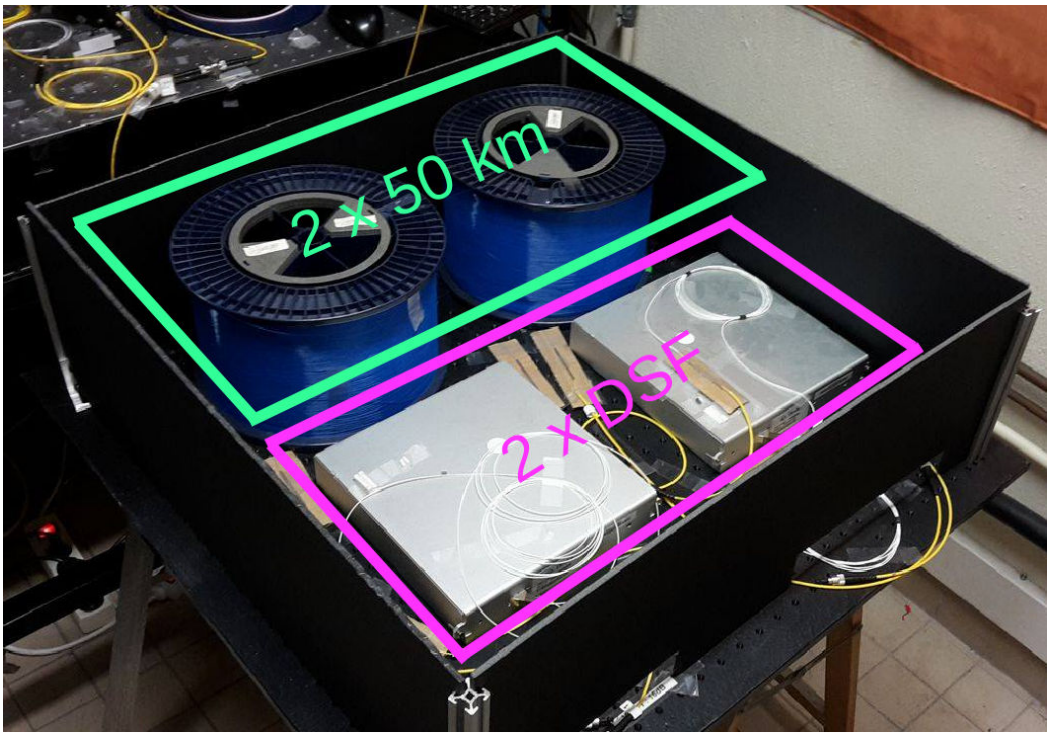


Figure 3.34. – Photographie des bobines de 50 km et des modules de compensation de dispersion (DSF). Les bobines et les modules sont placés au sein d'une boite fermée que l'on a ensuite rempli de billes de polystyrène de sorte à garantir une meilleure isolation thermique.

Si l'on compare cet élargissement à la durée de nos impulsions, à savoir 2,2 ps, on s'aperçoit immédiatement qu'il nous est impossible de le négliger. L'étirement des impulsions diminue la puissance crête disponible, ce qui à son tour diminue l'efficacité de conversion des différents processus non linéaires sur lesquels s'appuie notre dispositif. Mais pire encore, le caractère monomode fréquentiel des photons qui interfèrent n'est plus garanti, et ce malgré la présence du système de filtrage. Pour compenser cet effet, nous avons dû souder, comme de coutume en pareille situation, des fibres à dispersion décalée (*dispersion shifted fibers* - DSF) en sortie de nos bobines de 50 km de fibre standard [262, 263], voir Figure 3.34.

Système de stabilisation active

Deux effets à prendre en considération dans un scénario sur longue distance sont l'expansion thermique des fibres et la dépendance à la température de l'indice de

réfraction de la silice. L'évolution thermale non-homogène au sein du laboratoire peut ainsi occasionner un décalage de la position de la figure d'interférence à deux photons.

On trouve dans la littérature pour l'expansion thermique des fibres standards à 1550 nm (SMF-28) la relation [264] :

$$\frac{\Delta L}{L} \approx 0,55.10^{-6}\mathrm{K}^{-1} \cdot \Delta T, \tag{3.31}$$

où ΔT représente la variation de température, ΔL le décalage relatif engendré par cette variation et L la longueur de fibre.

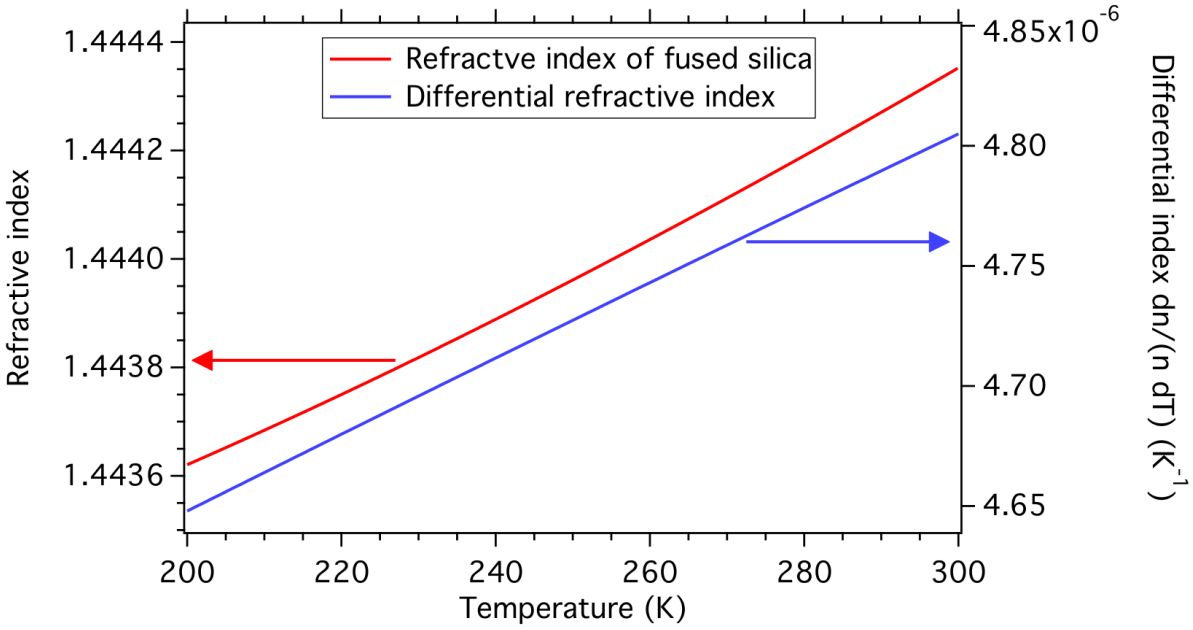


Figure 3.35. – Dépendance à la température de l'indice de réfraction de la silice. L'axe des ordonnées de gauche donne la valeur absolue de l'indice et celui de droite la valeur des variations $\frac{dn}{ndt}$.

La dépendance en température de l'indice de réfraction de la silice à 1550 nm est donnée Figure 3.35. À partir du graphe, on voit que la dépendance à température ambiante (300 K) nous est donnée par :

$$\frac{\Delta n}{n} \approx 4,8.10^{-6}\mathrm{K}^{-1} \cdot \Delta T. \tag{3.32}$$

Cette dépendance à la température est ainsi dix fois plus importante que celle de l'expansion thermique et domine donc au sein de notre dispositif.

Dans notre cas, on estime les fluctuations de températures entre bobines sur une dizaine d'heures (temps que nous prend la mesure de la figure d'interférence) à environ un dixième degré, ce qui, pour une longueur de fibre de 50 km, nous amène à considérer un décalage de l'ordre de 30 mm. Si l'on compare ce décalage à la largeur à mi-hauteur du *dip*, qui est d'environs 6 mm, on s'aperçoit dès lors qu'il devient obligatoire de corriger cette dérive.

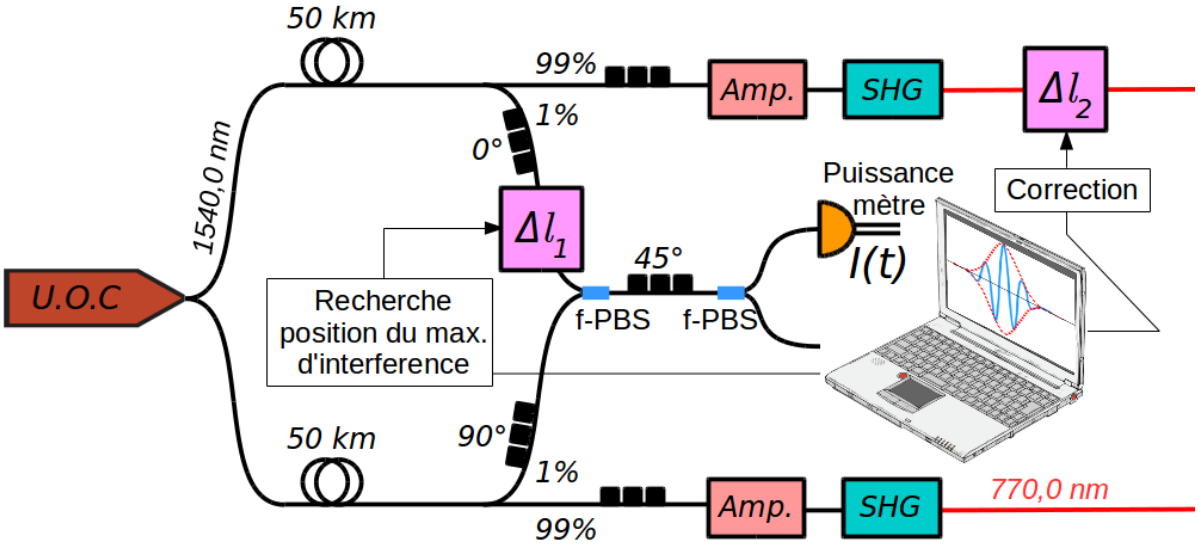


Figure 3.36. – Système de stabilisation active permettant de corriger la dérive induite par les fluctuations thermiques de l'environnement.

Le système de stabilisation mis en place est illustré en FIGURE 3.36. 1% du signal en amont des amplificateurs est prélevé sur chaque voie en sortie des bobines de 50 km et est envoyé dans une combinaison semblable à celle de la station relais (voir section 3.3.5), à savoir un contrôleur de polarisation orienté à 45 degrés placé entre deux PBS à fibre, de sorte à pouvoir observer une interférence entre faisceaux indiscernables en polarisation à l'aide d'un puissance mètre placé sur l'une des deux sorties. Une ligne à retard motorisée (Δl_1) de 15 cm de long et de résolution 10^{-2} ps permet de mettre en vis-à-vis les trains d'impulsions. À l'aide d'une interface Labview que nous avons développée, il nous est alors possible de suivre de manière automatisée le déplacement du maximum d'interférence. Le déplacement mesuré permet ensuite de corriger la position du rétro-réflecteur (Δl_2) nous servant à mesurer le *dip*.

La precision sur la position du maximum d'interférence, et donc du *dip*, est estimée à +/- 0,4 mm. L'évolution de la dérive est illustrée en FIGURE 3.37 où chaque point de l'enregistrement correspond à un scan de 10 min. On voit que cette mesure corrobore notre hypothèse d'un gradient de température de l'ordre d'un dixième de degré puisque

la dérive est en effet de l'ordre de 15 mm sur une durée de dix heures.

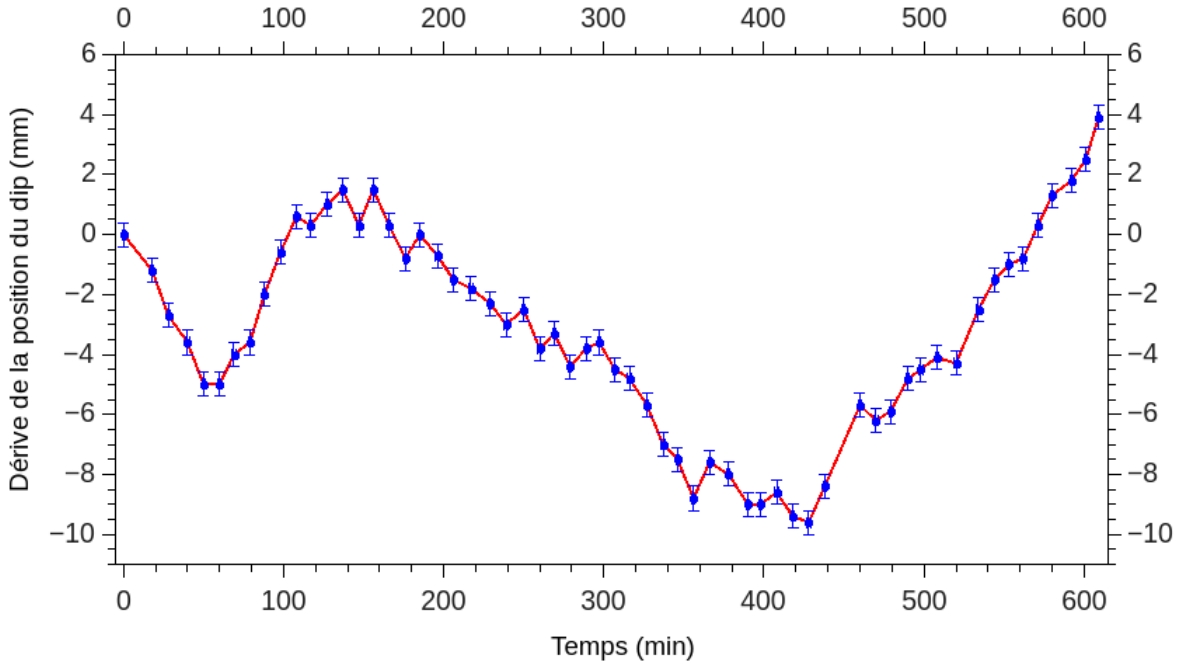


Figure 3.37. – Dérive au cours du temps de la position du *dip* mesurée à l'aide de notre système de stabilisation active.

Résultats

La figure d'interférence obtenue alors que le système de stabilisation est en marche est illustrée en FIGURE 3.38. De nouveau, la largeur à mi-hauteur du *dip* est en accord avec la largeur des filtres utilisés. La visibilité obtenue est de 90,5%, les quelques pourcents manquant s'expliquant par la résolution de notre système de stabilisation, une imprécision de l'ordre du mm résultant en un lissage du fond du *dip*. Ce dernier résultat vient définitivement valider la pertinence de notre approche.

3.7. Conclusion

Nous avons présenté un schéma original de synchronisation par horloge optique distribuée de sources de paires de photons intriqués permettant de s'affranchir de toute conversion électro-optique en vue d'établir un relais quantique sur grande distance. L'opération de synchronisation est alors validée, comme de coutume pour ce type de réalisations, par l'observation d'une figure d'interférence à deux photons dans le taux

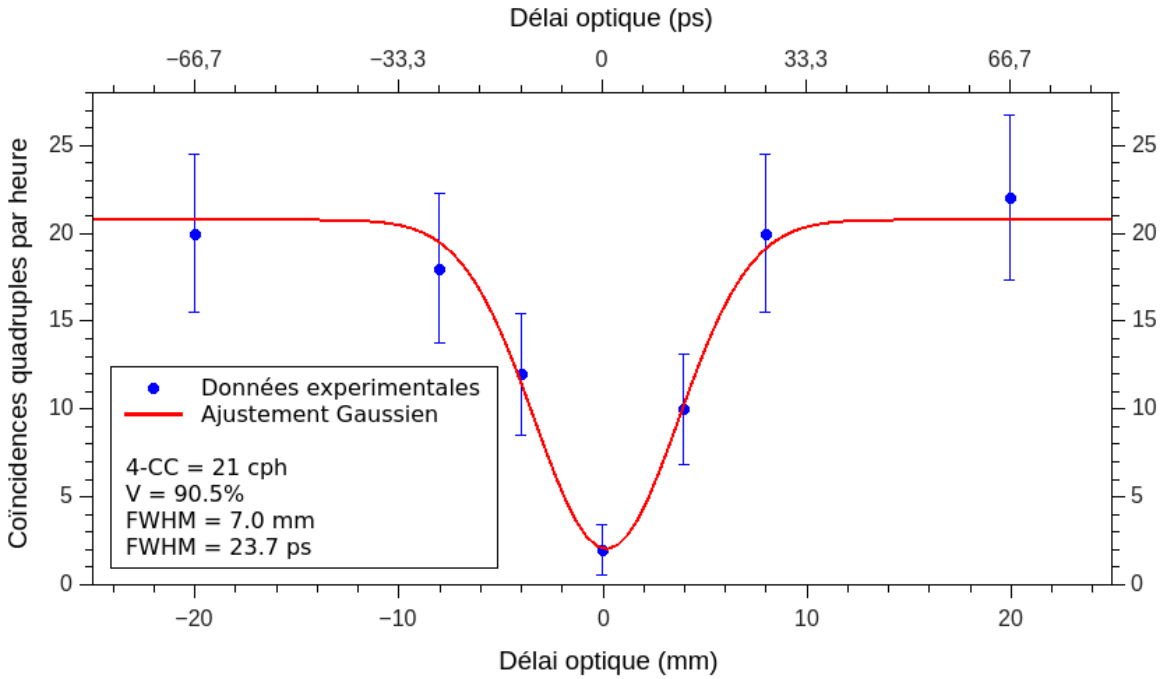


Figure 3.38. – Taux de coïncidences quadruples en fonction du délai optique. Cette mesure a été effectuée dans une configuration où 50 km de fibre optique ont été insérés en amont de chaque module amplificateur.

de coïncidences quadruples de l'expérience. Suite à de nombreux travaux préliminaires qui nous ont permis de gagner en expertise, les résultats obtenus pour une séparation effective de 100 km entre sources valident notre approche puisqu'une visibilité quasi parfaite a pu être observée pour une telle distance. Ces résultats constituent, à notre connaissance, un record de synchronisation en terme de distance entre sources au sein d'un lien à fibre optique. Notre dispositif ouvre ainsi la porte au développement sur longue distance d'un large éventail d'applications liées au traitement quantique de l'information. En particulier, un codage de l'information au moyen de l'observable *time-bin* serait particulièrement approprié en vue de permettre l'établissement quantique de clés secrètes entre deux clients distants. Cette étape supplémentaire est en cours d'étude au laboratoire. Bien entendu, des améliorations du dispositif sont toujours envisageables, en particulier le débit pourrait gagner un à deux ordres de grandeur via le remplacement de nos détecteurs par d'autres à base de technologie supraconductrice. Des détecteurs avec des *jitters* plus petits pourraient également nous permettre d'accroître la cadence de notre horloge optique, et ce jusqu'à un le taux de répétition de 10 GHz.

Le travail présenté au sein de ce chapitre a récemment été soumis pour publication

dans une revue internationale avec comité de lecture.

Chapitre 4.

Lumière comprimée à une longueur d'onde télécom : une approche entièrement guidée

La lumière comprimée est une ressource fondamentale pour la communication quantique. En vue du déploiement efficace des protocoles qui s'y rapportent, la réalisation de systèmes expérimentaux faciles à utiliser et compatibles avec les réseaux télécoms fibrés existants est une étape cruciale. En réponse à ce cahier des charges, nous démontrons dans ce chapitre la faisabilité d'une expérience de compression à une longueur d'onde de télécommunication réalisée, pour la première fois, de manière entièrement guidée.

Pour motiver ce travail, nous revenons tout d'abord sur les avantages et les limitations liées à la génération, à la propagation et à la détection de lumière comprimée en optique massive. Une vue générale de notre dispositif est ensuite donnée et les caractéristiques de ses différents éléments constitutifs sont détaillées. Après estimation du gain paramétrique, nous présentons enfin nos résultats correspondant à un niveau de compression de 1,83 dB en dessous de la limite quantique standard à la longueur d'onde de 1542,0 nm en régime de pompage continu.

4.1. Motivation

La première expérience de génération de lumière comprimée remonte à 1985 quand des atomes de sodium placés au sein d'une cavité optique ont permis de générer de la lumière comprimée par mélange à quatre ondes [265]. Peu de temps après, de la lumière comprimée a également été générée par mélange à quatre ondes dans une fibre optique (1986) [266] et par conversion paramétrique (PDC) dans un cristal présentant une non-linéarité du d'ordre 2 placé au sein d'une cavité optique (*optical parametric amplifier* - OPA, 1986) [267]. Ces expériences pionnières ont permis d'atteindre des facteurs de compression allant de quelques pourcents jusqu'à environ 3 dB. De nos jours, il est désormais courant avec des montages de type OPA d'observer des facteurs de compression dépassant les 10 dB [268, 269, 270] obtenus par amplification paramétrique.

La FIGURE 4.1 correspond au schéma typique d'un dispositif expérimental permettant de générer des états de vide comprimé monomode par conversion paramétrique dégénérée à l'aide d'un cristal non-linéaire du second ordre et d'une source laser.

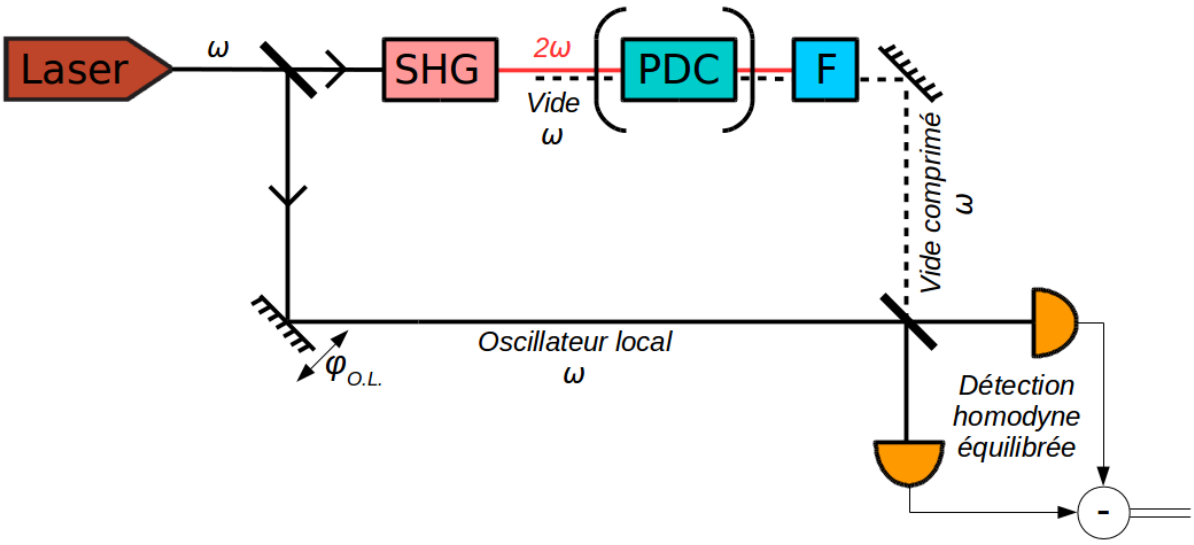


Figure 4.1. – Montage expérimental typique permettant la génération, par amplification paramétrique dégénérée, la propagation et la détection de lumière comprimée. Le faisceau issu d'un laser émettant à la fréquence ω est divisé en deux faisceaux de forte intensité à l'aide d'une lame séparatrice. L'un des deux faisceaux est utilisé pour donner naissance à un signal de pompe à la fréquence 2ω par génération de seconde harmonique (SHG), tandis que le second faisceau sert d'oscillateur local pour la détection homodyne (voir section 2.4.6 pour une description détaillée de cette technique de détection). Le signal à 2ω est utilisé pour pomper un étage de conversion paramétrique (PDC) constitué d'un cristal non-linéaire placé au sein d'une cavité optique. Ceci donne alors naissance à un faisceau dans un état de vide comprimé à la fréquence angulaire ω. Le faisceau de pompe qui est transmis est ensuite éliminé au moyen d'un filtre (F) à la sortie de l'amplificateur paramétrique. En plaçant l'un des miroirs sur un transducteur piézoélectrique, nous pouvons faire varier la phase de l'oscillateur local.

La grande majorité des réalisations qui viennent d'être citées reposent pour la génération du *squeezing* sur des cavités optiques et plus généralement sur de l'optique massive. De tels dispositifs rendent de fait très difficile toute implémentation d'un protocole de communication quantique en régime de variables continues hors laboratoire. En effet, de tels montages, en plus d'être très difficilement reconfigurables, ne sont absolument pas compact et demandent des systèmes de rétroaction contre les bruits acoustiques. De plus, la présence d'une cavité optique réduit drastiquement la bande spectrale d'émission empêchant ainsi tout multiplexage éventuel du lien de communication.

Dans ce contexte, nous proposons un montage original où la génération, la propagation, et la détection de lumière comprimée ont lieu, pour la première fois, de manière entièrement guidée. Dans notre schéma, de la lumière comprimée à la longueur d'onde de dégénérescence 1542 nm est générée par SPDC dans un guide d'onde *ridge* inscrit sur substrat de niobate de lithium périodiquement polarisé (PPLN/RW). À la sortie du PPLN/RW, les fluctuations non-classiques sont mesurées à l'aide d'un système de détection homodyne fibré. Ces différents éléments permettent de mettre en place un dispositif extrêmement simple basé entièrement sur des composants disponibles dans le commerce et entièrement compatible avec les réseaux de fibres optiques existants. D'une part, l'optique non linéaire basée sur la technologie des guides d'ondes offre, en comparaison avec les implémentations en optique de volume, une meilleure compacité et une meilleure stabilité, ainsi que la garantie d'avoir une conversion paramétrique plus efficace pour un passage unique de la pompe. D'autre part, l'utilisation de composants fibrés issus des télécoms optiques permet de réaliser une configuration simple et *plug-and-play* qui ne requiert aucun effort d'alignement pour le recouvrement des différents modes spatiaux au niveaux de la détection homodyne. De plus, notre dispositif peut très simplement être reconfiguré en connectant d'autres composants fibrés ou en adaptant les longueurs d'onde.

4.2. Présentation générale du dispositif

Le schéma de notre dispositif expérimental est présenté en FIGURE 4.2. Un laser en régime de fonctionnement continu couplé à une fibre (Toptica, DL Pro), et émettant à la longueur d'onde des télécommunications de 1542 nm, est amplifié au moyen d'un amplificateur à fibre dopée à l'erbium (Keopsys, CEFA-C-HG) et dirigé à l'entrée d'un coupleur à fibre déséquilibré (70/30 f-BS).

Le faisceau de plus faible intensité est utilisé comme oscillateur local pour la détection homodyne, tandis que le faisceau de plus forte intensité est doublé en fréquence à 771 nm par génération de seconde harmonique (SHG) dans un guide d'onde inscrit sur niobate de lithium (PPLN/W, HC-Photonics). Le faisceau doublé sert alors de pompe pour la génération de lumière comprimée par conversion paramétrique spontanée (SPDC) au sein d'un PPLN/RW *ridge* (NEL, WH-0770-000-F-B-C).

Afin de détecter la lumière, nous la dirigeons enfin vers un système de détection homodyne composé d'un coupleur fibré équilibré (50/50 f-BS) dont les sorties sont connectées à deux photodiodes InGaAs (Thorlabs, FGA10). L'indiscernabilité en polarisation entre faisceaux entrants est simplement obtenue en insérant un contrôleur de polarisation (PC) sur le trajet de l'oscillateur local. Un élongateur (*phase controller*) de notre conception permet enfin de scanner la phase de l'oscillateur local tandis que le niveau de compression

est mesuré à l'aide d'un analyseur de spectre électronique (HP, ESA-L1500A).

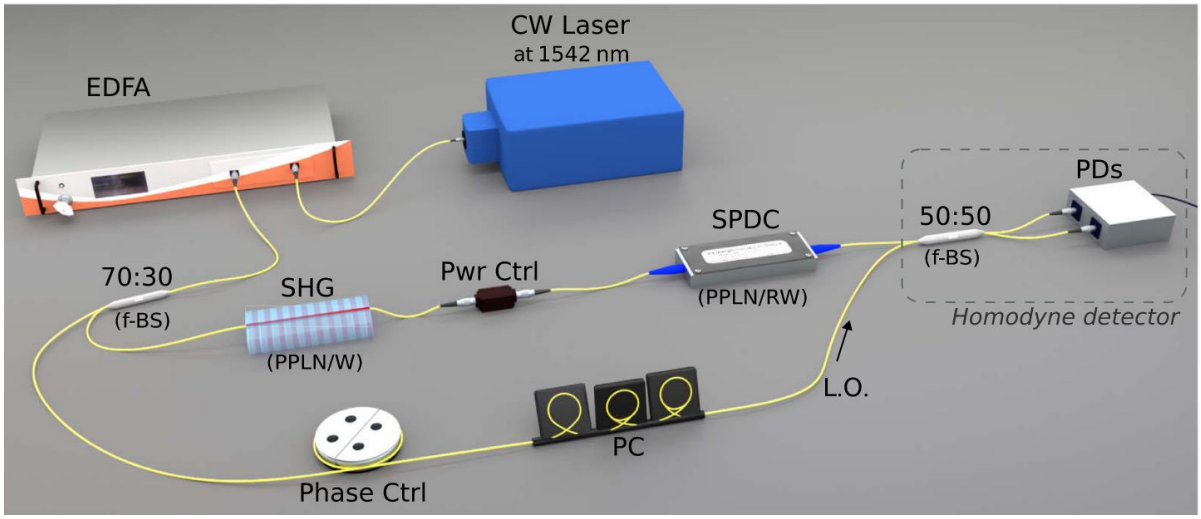


Figure 4.2. – Vue d'ensemble du dispositif expérimental. EDFA : amplificateur à fibres dopées à l'erbium ; f-BS : coupleur fibré ; Phase Ctrl : stretcheur ; Pwr Ctrl : atténuateur fibré ; L.O. : oscillateur local ; PPLN/W : PPLN *waveguide* ; PPLN/RW : PPLN *ridge waveguide* ; PC : contrôleur de polarisation ; PDs : photodiodes.

4.3. Caractérisation du dispositif

Au sein de cette section, nous revenons de manière plus détaillée sur les différents éléments constitutifs de notre dispositif expérimental.

4.3.1. Étages de conversion en longueurs d'onde

Nous commençons par présenter les caractéristiques des différents guides d'ondes non-linéaires qui permettent, par conversion successives, de générer un faisceau dans un état de vide comprimé aux longueurs d'onde des télécommunications.

Génération de seconde harmonique (SHG)

En sortie du cristal de SHG, la puissance du signal à 771 nm, P_{shg}, évolue avec la puissance du signal incident à 1542 nm, P_{in}, selon la relation :

$$P_{shg} = P_{in} \cdot \tanh^2\left(\sqrt{\eta_{shg} P_{in}}\right), \tag{4.1}$$

avec une efficacité de conversion mesurée $\eta_{shg} \sim 2000\%/\mathrm{W}$. La lumière doublée en fréquence est directement collectée à l'aide d'une fibre monomode standard à 780 nm qui agit également comme un filtre quasi parfait pour la lumière résiduelle non convertie à 1542 nm. Le faisceau à 771 nm passe alors à travers un atténuateur variable fibré qui nous permet de contrôler la puissance de pompe incidente en entrée de l'étage de SPDC.

Le couplage mesuré dans la fibre de récolte monomode est de 60%, alors que la puissance maximum disponible mesurée directement en sortie de la fibre de récolte est de 28 mW.

Conversion paramétrique spontanée (SPDC)

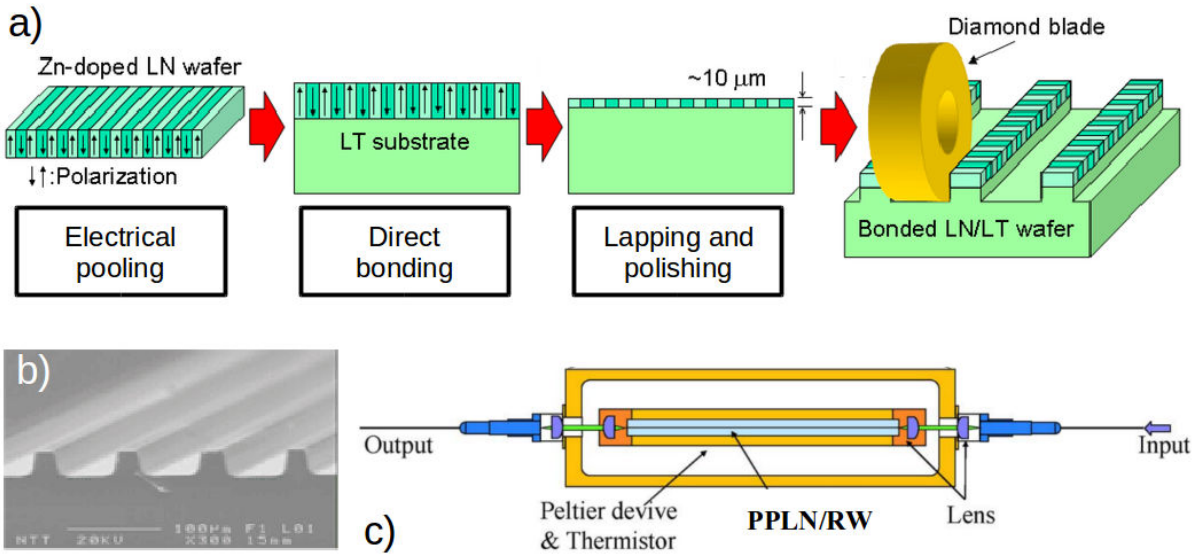


Figure 4.3. – **a)** Illustration des étapes de fabrication du PPLN/RW. **b)** Photographie des structures guidantes. **c)** Schéma du module connectorisé.

Le processus de SPDC (de type-0 [1]), a lieu au sein d'un guide d'onde *ridge* inscrit sur niobate de lithium périodiquement polarisé (PPLN/RW) de 4 cm de long et de longueur d'onde de dégénérescence 1542 nm. La conception du guide d'onde *ridge* offre un fort confinement de la lumière et garantit une efficacité de conversion élevée sur une large bande passante de fonctionnement. De plus, par rapport à d'autres structures PPLN/W montrant des efficacité de conversion similaires, les structures *ridges* résistent mieux en terme de dommages à des régimes de gain paramétrique élevés ou les puissances en jeux peuvent être particulièrement importantes. Les facettes d'entrée et de sortie

1. Cas où photon *signal* et photon *idler* ont même polarisation que le faisceau de pompe incident.

du PPLN/RW sont connectées à des fibres à maintien de polarisation (PMF), dont le couplage avec le guide d'onde *ridge* est optimisé grâce à des micro-lentilles.

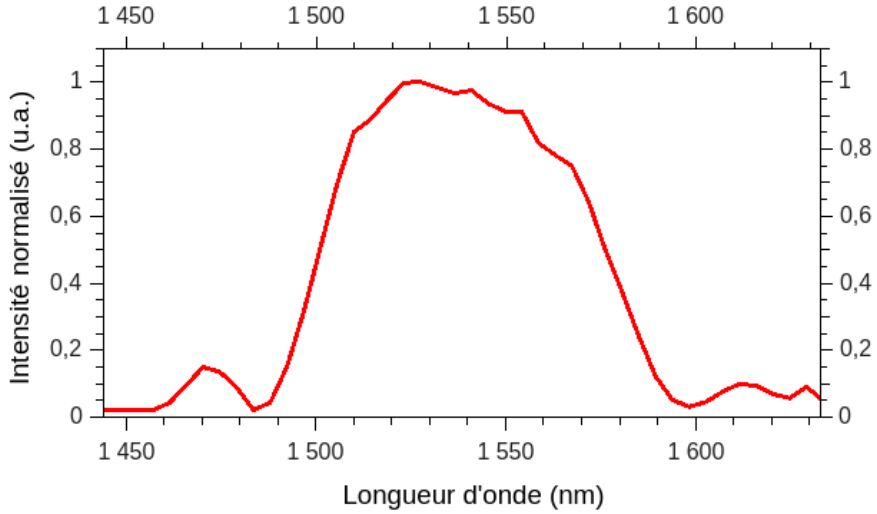


Figure 4.4. – Spectre de SPDC mesuré en sortie du PPLN/RW.

Le spectre d'émission mesuré, reporté en FIGURE 4.2, présente une largeur à mi-hauteur de 80 nm. Cette largeur correspond, dans le domaine fréquentiel, à une bande passante de 10 THz. Étant donné qu'aucune cavité optique n'est utilisée pour amplifier le processus, cette bande passante est directement celle de notre faisceau comprimé. Aussi, afin de caractériser notre source, nous avons mesurée sa brillance B, définie comme :

$$B = \frac{\text{Nombre de paires générées}}{(\text{mW de pompe}) \cdot (\text{seconde}) \cdot (\text{GHz de bande passante spectrale})}. \tag{4.2}$$

Bien que les trois quantités au dénominateur soient facilement accessibles, le nombre de paires générées est parfois difficile à estimer. Pour remonter à ce dernier, nous avons procédé en sortie du guide à une mesure du taux de coïncidences. Pour cela, nous avons connecté l'une des deux voies d'entrée d'un coupleur 50/50 à la sortie du PPLN/RW et placé un détecteur de photons unique sur chacune des sorties du coupleur. Les coïncidences sont ensuite enregistrées au moyen d'un TAC (*Time to Amplitude Converter*). Les taux de détection de photons uniques sur chaque détecteur, respectivement notés S_1 et S_2, nous sont donnés après soustraction du bruit par :

$$\begin{cases} S_1 = \mu_1 \eta_1 N_{paires}, \\ S_2 = \mu_2 \eta_2 N_{paires}, \end{cases} \tag{4.3}$$

où $\mu_{1,2}$ et $\eta_{1,2}$ désignent respectivement les pertes à la propagation et à la détection dans chaque bras du dispositif. Le taux de coïncidence net, noté C, a quant à lui pour expression :

$$C = \frac{1}{2}\mu_1\mu_2\eta_1\eta_2 N_{paires}. \tag{4.4}$$

où le facteur 1/2 correspond aux pertes introduites par le coupleur directionnel (dans 50% des cas les deux photons sortent du même côté du coupleur et les coïncidences ne sont pas enregistrées). Finalement, à partir des expressions de S_1, S_2 et C, nous obtenons un nombre de paires générées par seconde égal à :

$$N_{paires} = \frac{S_1 S_2}{2C}. \tag{4.5}$$

Cette mesure nous a permis d'estimer la brillance de notre source à $1,2 \cdot 10^6$ paires de photons/mW/GHz/s.

Une fois N_{paires} connu, il est également possible à partir de l'expression (4.3) de S_i de remonter au couplage dans le fibre de récolte en sortie du PPLN/RW que l'on notera η_c. Le coefficient μ_i tenant compte de l'intégralité des pertes depuis le centre du PPLN/RW jusqu'à l'entrée du détecteur correspondant, la soustraction des différentes pertes à la propagation nous permet de remonter à un couplage à la récolte de $\eta_c = 80\%$.

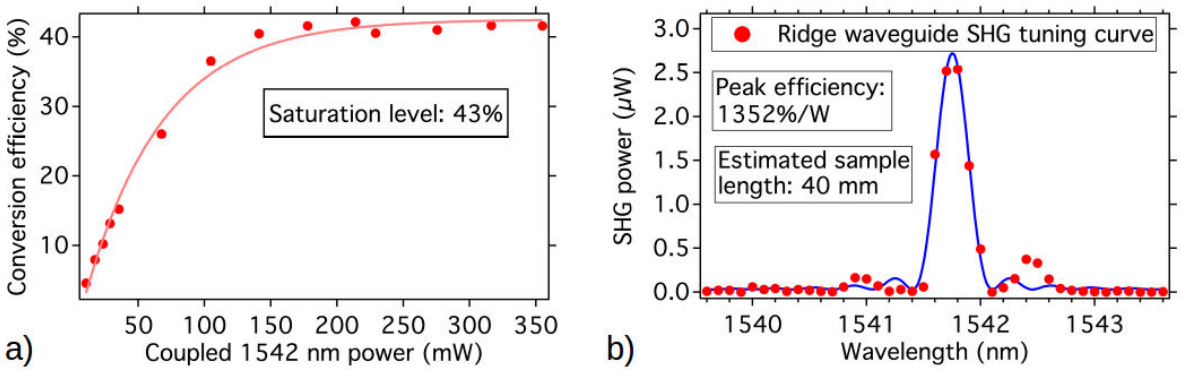


Figure 4.5. – **a)** Efficacité du processus de SHG en fonction de la puissance de pompe à 1542 nm injectée de manière contra-propagé au sein du PPLN/RW. **b)** Spectre de SHG typique mesuré.

Finalement, la connaissance du couplage de sortie permet d'estimer le couplage d'entrée. Pour cela nous avons injecté de manière contra-propagé un faisceau amplifié à la longueur d'onde de pompe de 1542 nm et mesuré en sortie la puissance du signal de SHG alors généré. À saturation, et sachant que 80% du signal de pompe est injecté dans le guide, le rapport entre puissance de SHG en sortie et puissance de pompe injectée

dans le guide nous indique une transmission $\sim 43\%$, voir FIGURE 4.5. La pente de la courbe avant saturation permet également, voir équation (4.1), d'estimer une efficacité de conversion pour la SHG de 1352 %/W.

À notre connaissance, il s'agit de la première fois qu'un guide d'onde *ridge* est utilisé pour une expérience en régime de variables continues.

4.3.2. Système de détection homodyne

Le procédé de détection homodyne a été présenté à la section 2.4.6, ainsi nous ne réintroduirons pas dans cette section le principe de ce schéma de détection. Toutefois, nous souhaitons mentionner ici qu'outre la compacité et la stabilité du dispositif dans son ensemble, un avantage majeur de notre approche au regard de la détection homodyne est qu'aucun ajustement n'a besoin d'être effectué pour garantir un haut degré de recouvrement des modes spatiaux au niveau du f-BS [271], ce qui représente un avantage important vis-à-vis des réalisations en optique massive. De plus, le fait de travailler en régime continu nous permet d'éviter toute considération liée à la synchronisation temporelle d'impulsions au niveau du coupleur [272]. Enfin, de sorte à minimiser les pertes liées aux réflexions de Fresnel en sortie du coupleurs 50/50, les sorties de ce derniers ont été soudées à des fibres soumises à un traitement anti-reflets (Thorlabs, AR-Coated Single Mode Fiber Optic Patch Cables), et les faisceaux lumineux en sortie de ces fibres sont directement envoyés aux photodiodes (pas de lentilles avant les éléments sensibles des détecteurs). Les pertes depuis la sortie de la fibre PM jusqu'à l'entrée des photodiodes sont ainsi d'environs 5%, soit une transmission η_T de 95%.

Caractérisation des photodiodes

De sorte à avoir une estimation de l'ensemble des pertes de notre dispositif, nous avons caractérisé l'efficacité quantique de détection, η_{det}, des photodiodes utilisées en fonction de la puissance incidente envoyée sur ces dernières. Concrètement, si l'on appelle Φ le flux de photons incident sur une des photodiodes, le photo-courant $i_{opt}(t)$ généré dans le circuit extérieur a alors pour expression :

$$i_{opt}(t) = \eta_{det} \cdot e \cdot \Phi(t) \cdot \equiv \eta_{det} \cdot e \cdot \frac{P(t)}{\hbar\omega}, \tag{4.6}$$

où e est le module de la charge de l'électron, P la puissance moyenne du faisceau incident et ω sa fréquence. La mesure de la responsivité $i_{opt}/P = \eta_{det}e/\hbar\omega$ des photodiodes permet ainsi, connaissant la longueur d'onde de la lumière, de remonter à l'efficacité de détection. Cette mesure, effectuée après avoir décapsulé nos deux photodiodes, nous a permis d'estimer l'efficacité de détection de ces dernières à environ 88% , voir FIGURE 4.2.

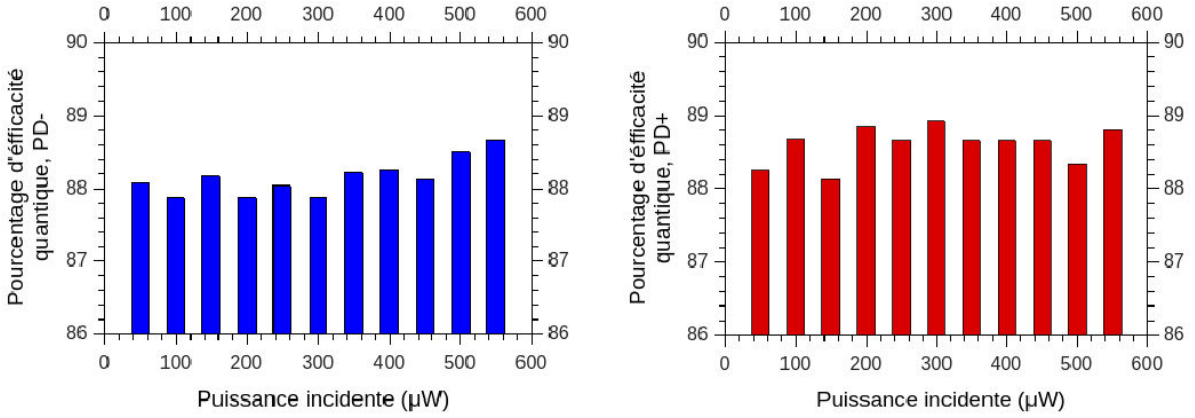


Figure 4.6. – Efficacité de détection des deux photodiodes décapsulées en fonction de la puissance moyenne incidente à la longueur d'onde de 1542 nm.

Afin de réaliser une mesure quantitative des fluctuations du champ quantique généré, nous devons également nous intéresser à la variance, $\sigma[i_{opt}(t)]$, du photo-courant. En tenant directement compte du flux de photo-électrons plutôt que du flux de photons incidents, l'intensité nous est donnée par $i_{opt}(t) = n_e(t)e/\Delta t$, où Δt représente la durée de la mesure et $n_e(t)$ le nombre de photo-électrons générés durant cet intervalle. À partir de cette expression, on obtient pour la variance du photo-courant :

$$\sigma[i_{opt}(t)] = \sigma\left[\frac{n_e(t)e^2}{\Delta t^2}\right] = \frac{\sigma[n_e(t)]e^2}{\Delta t^2}. \tag{4.7}$$

En considérant la génération de chaque photo-électron comme un processus indépendant, la statistique de génération est alors une statistique de Poisson, et donc $\sigma[n_e(t)] = \langle n_e\rangle = \langle i_{opt}\rangle\Delta t/e$. Ainsi, pour un nombre important d'électrons au sein de chaque intervalle temporel, nous avons :

$$\sigma[i_{opt}(t)] = \frac{\langle i_{opt}\rangle e}{\Delta t}, \tag{4.8}$$

ce qui, en fonction de la bande-passante $B = 1/(2\Delta t)$ du système de détection nous conduit à considérer l'expression :

$$\sigma[i_{opt}(t)] = 2\langle i_{opt}\rangle eB, \tag{4.9}$$

où nous avons considéré $\langle i_{opt}\rangle$ comme une quantité constante tout au long de la mesure, ce qui en pratique est bien le cas.

Sources de bruit

Théoriquement, si la lumière comprimée est générée par un processus non-linéaire continu, on peut, comme expliqué à la section 2.4.6, révéler son niveau de compression à travers la mesure de la variance du photo-courant soustrait en sortie du détecteur homodyne équilibré en fonction de la phase de l'oscillateur local. En pratique, cependant, cette mesure est polluée par divers bruits parasites, à savoir le bruit de l'électronique de détection et le bruit technique (classique) du dispositif optique.

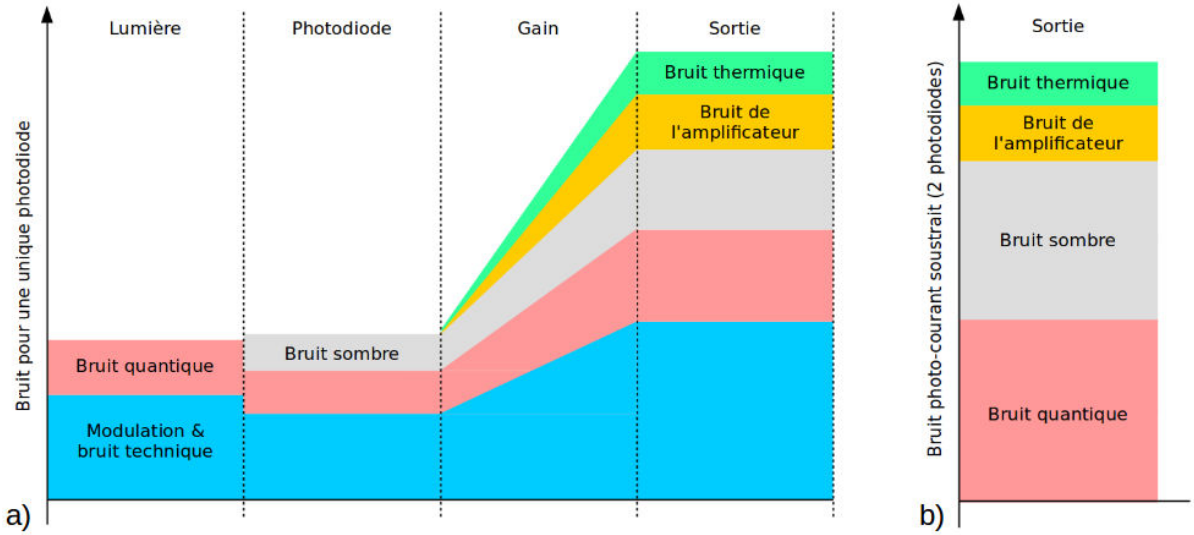


Figure 4.7. – **a)** Évolution du bruit dans la situation où le signal optique serait détecté par une unique photodiode. Dans un soucis de lisibilité, les différentes contributions ne sont ici pas représentées à leurs échelles respectives. **b)** Bruit du photo-courant soustrait en sortie du circuit de détection homodyne. Dans le cas de photodiodes parfaitement identiques, le bruit technique (bleu) est entièrement supprimé lors de la soustraction. Les bruits sombres associés aux deux photodiodes (gris) étant décorrélés, ces derniers s'additionnent, de même que les contributions de bruit quantique (rouge). L'amplification ayant directement lieu sur le photo-courant soustrait, le bruit de l'amplificateur (jaune) et le bruit thermique (vert) sont quant à eux à comptabiliser qu'une fois.

Le photo-courant en sortie d'une photodiode contient une composante continue (DC) et une composante alternative (AC). La contribution de la composante AC est typiquement de l'ordre de 10^{-7} en comparaison de la composante continue, d'où la nécessité d'une étape d'amplification. La solution la plus courante consiste à placer une résistance de $50\,\Omega$ en terminaison de la photodiode et d'utiliser un amplificateur RF qui va amplifier à la fois le bruit et le signal entrant. La FIGURE 4.7a présente l'évolution du bruit. Les différentes contributions du bruit sont respectivement :

- **Bruit sombre** - $\sigma[i_{dark}(t)]$. Ce bruit correspond aux faux événements de détection (*dark noise*). Pour nos mesures qui impliquent des puissances optiques de quelques mW, cette contribution peut être négligée.

- **Bruit thermique** - Le bruit thermique du circuit est donné par $\sigma[i_{th}(t)] \approx 4k_BTB/R$ où T est la température, B est la bande-passante du circuit définie comme la bande passante de l'amplificateur, et R l'impédance d'entrée du circuit.

- **Bruit de l'amplificateur** - $\sigma[i_{amp}(t)] \approx 2eGBF$. Ici G est le gain en tension de l'amplificateur, B sa bande passante, et F le facteur de bruit excédentaire [2].

Toutes ces contributions au bruit électronique sont indépendantes, par conséquent les variances doivent être sommées. Ainsi, si l'on veut avoir une chance de pouvoir remonter à la variance du photo-courant associé au champ optique, $\sigma[i_{opt}(t)]$, on doit par conséquent avoir :

$$\sigma[i_{el}(t)] = \sigma[i_{dark}(t)] + \sigma[i_{amp}(t)] + \sigma[i_{th}(t)] \ll \sigma[i_{opt}(t)]. \tag{4.10}$$

À température ambiante, la contribution prédominante est celle du bruit thermique. En tenant compte de nos paramètres, à savoir une longueur d'onde de 1542 nm et une efficacité de détection de 88%, le bruit thermique à température ambiante pour une impédance de 50 Ω, une puissance optique incidente de 1 mW (soit un courant de ∼1 mA d'après l'équation 4.6) et une bande passante de détection B donnée, est $\sigma[i_{th}(t)]/\langle i\rangle^2 = 4k_BTB/R\langle i\rangle^2 = 4 \cdot 1,38 \cdot 10^{-23} \cdot 300 \cdot B/(50 \cdot 10^{-6}) \backsimeq 3,3 \cdot 10^{-16} \cdot B$. Ce bruit thermique relatif est à comparer avec le bruit quantique standard à même puissance optique et même bande passante de détection : $\sigma[i_{opt}(t)]/\langle i\rangle^2 = 2eB/\langle i\rangle = 2 \cdot 1,6 \cdot 10^{-19} \cdot B/10^{-3} = 3,3 \cdot 10^{-16} \cdot B$. Ce résultat indique que le bruit thermique est comparable au bruit quantique standard à cette puissance optique et que les deux contributions ne peuvent être dissociées qu'en travaillant avec des puissances optiques plus élevées. Afin de s'affranchir de cette difficulté, notre circuit électronique est équipé d'un amplificateur transimpédance de bande passante 5 MHz, voir Figure 4.10b. Ce dernier permet de convertir un photo-courant AC en une tension AC au moyen d'une résistance (R1) de 1 kΩ, le bruit thermique étant inversement proportionnel à la résistance du circuit, ceci a pour conséquence de grandement diminuer la contribution de cette source de bruit.

Un schéma de notre circuit de détection est donné en Figure 4.8. Sont représéntés

2. Le facteur de bruit d'un dispositif électronique (*noise figure* ou *noise factor* en anglais) est défini comme le quotient des rapports signal sur bruit en entrée et en sortie de ce même dispositif quand le bruit en entrée est un bruit thermique à la température normalisée T_0=290 K.

sur ce schéma les deux photodiodes (D1 et D2), l'amplificateur transimpédance (IC2 + R1 + C9), ainsi que les différents filtres requis pour obtenir un circuit avec un faible niveau de bruit.

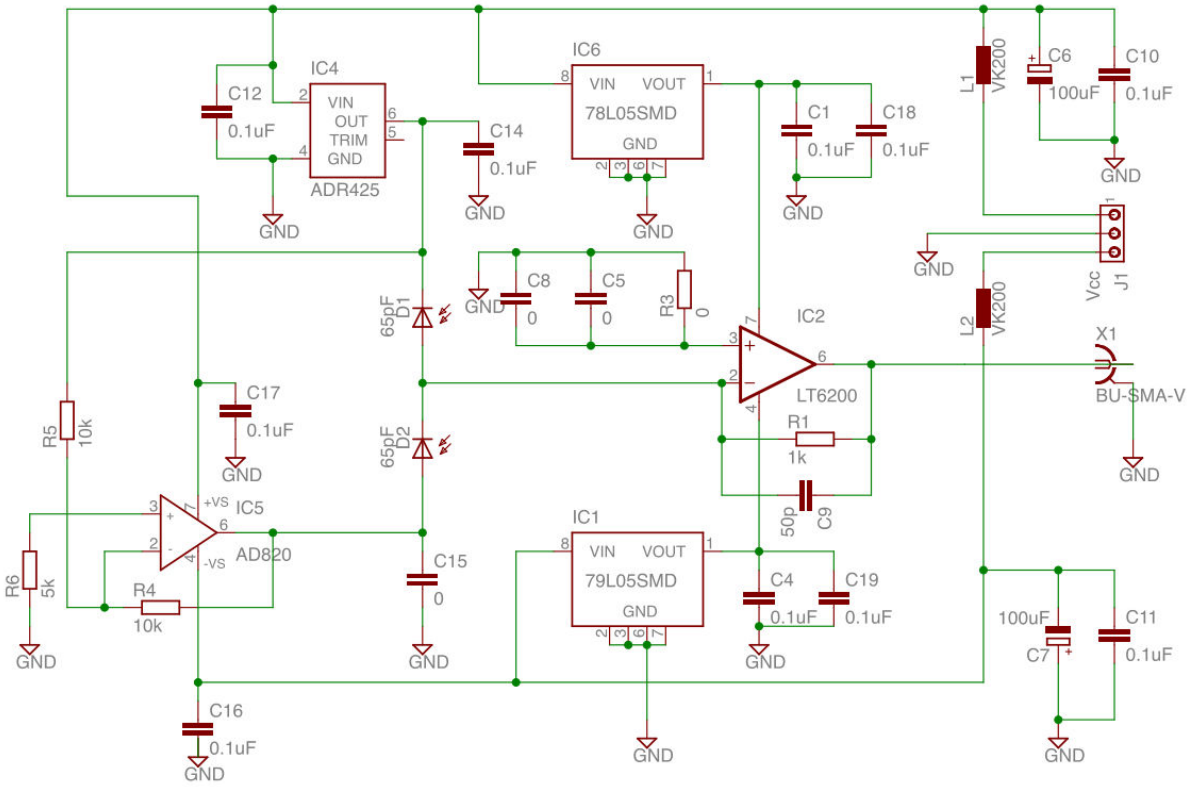


Figure 4.8. – Schéma du circuit électronique de notre détecteur homodyne. Le circuit a été conçu au sein du groupe d'optique quantique de l'université de Florence (It), tandis que les photodiodes ont été ajoutées à Nice où l'expérience ici décrite a été conduite.

Outre le bruit de l'électronique, le bruit technique du dispositif optique constitue une seconde source de bruit parasite. Par exemple, des battements entre modes de la cavité laser peuvent engendrer des modulations à des fréquences de détection spécifiques, ou encore des vibrations acoustiques de la table optique peuvent avoir lieu, ce qui peut complètement noyer le bruit quantique au sein du bruit technique au delà d'une certaine amplitude de modulation. Cependant, ces modulations étant généralement basses fréquences, le bruit technique peut être distingué du bruit quantique au moyen d'une analyse spectrale.

4.3.3. Analyse spectrale

Afin mesurer la puissance de bruit pour chaque quadrature nous avons recours à un analyseur de spectre électronique. Avant d'analyser le faisceau de lumière comprimé, nous nous intéressons tout d'abord au spectre du bruit pour différentes puissance incidente de l'oscillateur local sur les photodiodes.

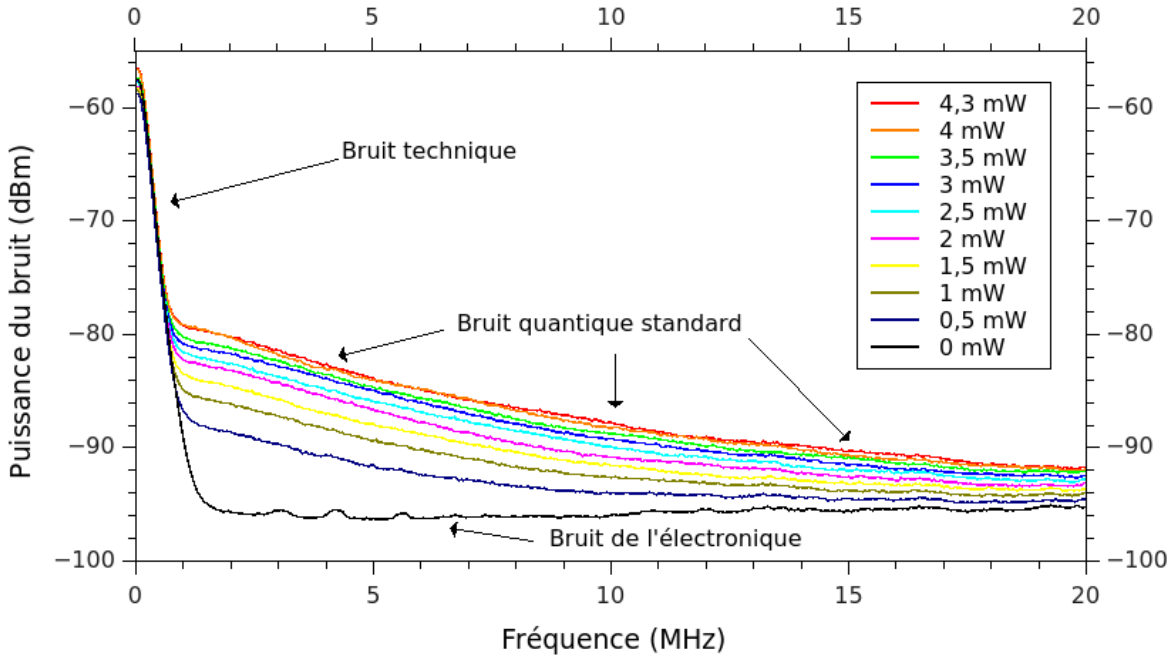


Figure 4.9. – Spectre du bruit pour différents niveaux de puissance incidente à 1542 nm en entrée des photodiodes.

La Figure 4.9 présente les résultats obtenus. Comme attendu, les données indiquent que le bruit thermique domine aux basses fréquences. Ce dernier atteint la limite du bruit quantique un peu avant la fréquence de 2 MHz, autrement dit il devient alors négligeable. La linéarité de la puissance de bruit avec la puissance optique incidente tel que prédit par l'équation 4.9 est démontrée par le graphique de la Figure 4.10a.

La Figure 4.10b, qui correspond au spectre du bruit pour une puissance incidente sur chaque photodiode de 4,3 mW auquel on a retiré la contribution du bruit électronique, nous permet de trouver la fréquence d'analyse associée au meilleur rapport signal sur bruit (SNR) possible. Ainsi, à 2 MHz le rapport signal sur bruit atteint un maximum de 15,6 dB. Le bruit électronique résiduel se traite comme une contribution additionnelle, η_{el}, aux pertes de l'ensemble de notre dispositif [273] :

$$\eta_{el} = \frac{SNR - 1}{SNR} = \frac{10^{\frac{15,6}{10}} - 1}{10^{\frac{15,6}{10}}} \approx 0,97. \tag{4.11}$$

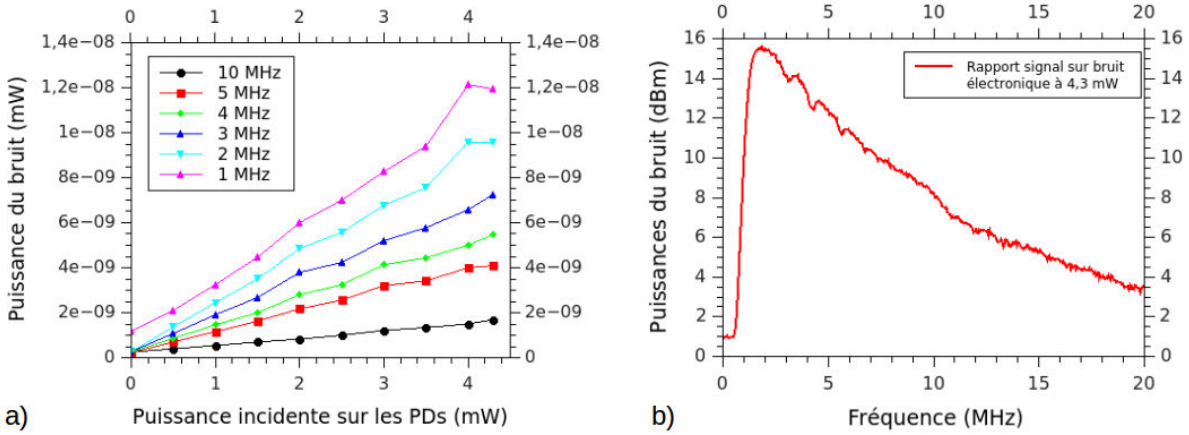


Figure 4.10. – **a)** Mesure de la puissance du bruit en fonction de la puissance optique. **b)** Spectre du bruit pour une puissance incidente de 4,3 mW en entrée des photodiodes auquel on a soustrait la contribution du bruit électronique. La fréquence de 2 MHz correspond au meilleur rapport signal sur bruit possible.

Enfin, nous souhaitons souligner que la lumière comprimée que nous avons générée pourrait être détectée sur des largeurs de bande supérieures à 2 GHz, au moyen de détecteurs dans la bande-C des télécoms et d'une électronique ultra-rapides [274]. Exploiter de larges bande-passantes est, comme nous l'avions déjà mentionné au chapitre 1, un élément clé pour la réalisation d'opérations de multiplexage ainsi que pour la communication quantique à haut débit [274, 275].

4.4. Influence des pertes

En présence de pertes, la variance des fluctuations associées à la quadrature mesurée nous est donnée par [276] :

$$\Delta\hat{X}^2_{\theta,mes} = \eta_{tot}\left[e^{2\cdot r}\cos(\theta) + e^{-2\cdot r}\sin(\theta)\right] + 1 - \eta_{tot}, \tag{4.12}$$

où η_{tot} représente l'efficacité de détection totale du dispositif. Les valeurs $\theta = 0$ et $\theta = \pi/2$ correspondent ici respectivement à la mesure du grand axe et du petit axe de l'ellipse associée à la représentation de notre état de vide comprimé dans l'espace des phases. Le facteur de compression dépend de la puissance de pompe P_{shg} en entrée de l'étage de SPDC via la relation $r = \mu \cdot \sqrt{P_{shg}}$, où μ est une constante dépendant de la

longueur du PPLN/RW et des propriétés non-linéaires de ce dernier.

Dans le cas de notre dispositif, nous devons donc respectivement ternir compte des pertes liées à la propagation dans le PPLN/RW, η_{wg}, des pertes liées au couplage dans la fibre de récolte, η_c, des pertes liées à la propagation dans la fibre et au passage dans les différents composants optiques, η_T, des pertes à la détection, η_{det}, ainsi que des pertes liées au bruit de l'électronique, η_{el}. L'expression de l'efficacité totale est ainsi donnée par :

$$\eta_{tot} = \eta_{wg} \cdot \eta_c \cdot \eta_T \cdot \eta_{det} \cdot \eta_{el}. \tag{4.13}$$

4.5. Résultats

4.5.1. Mesure du niveau de compression

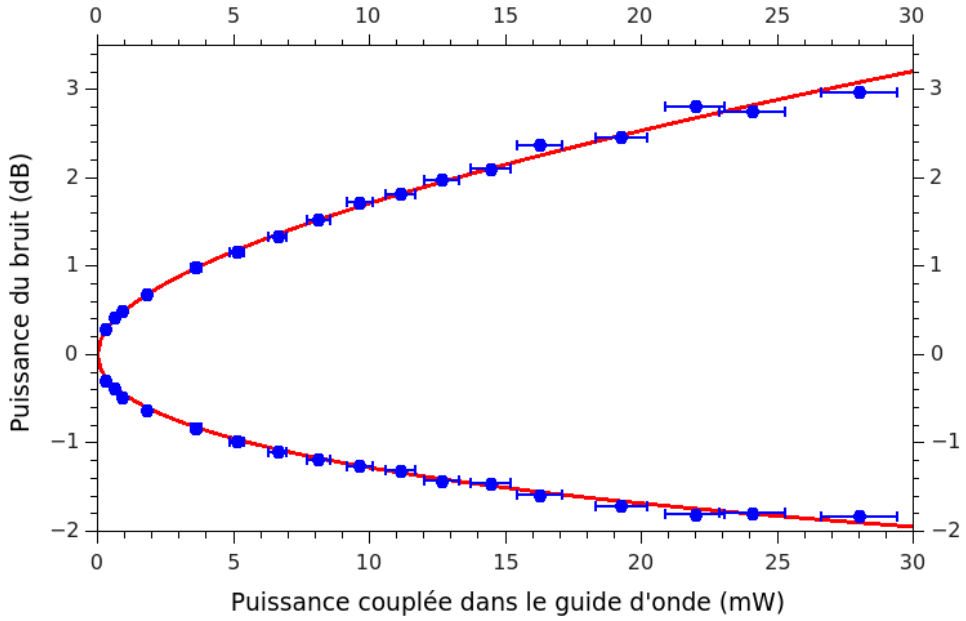


Figure 4.11. – Niveau de compression et d'anti-compression en fonction de la puissance de pompe en entrée du PPLN/RW. L'erreur est de $\pm 0,05\,\mathrm{dB}$ sur la puissance de bruit mesurée et de 5% sur la puissance de pompe incidente. L'ajustement des données permet d'estimer l'efficacité totale à $\eta_{tot,fit} = 0,54 \pm 0,01$ et un paramètre de compression de $\mu_{fit} = (0,101 \pm 0,002)\,\mathrm{mW}$, voir équation 4.12.

La FIGURE 4.11 représente les niveaux de compression et d'anti-compression mesurés en fonction de la puissance de pompe à 771 nm. Chaque point correspond à une moyenne

effectuée suite à plusieurs acquisitions avec une erreur sur la mesure de $\pm 0,05\,\mathrm{dB}$. Les différentes puissances de pompes, obtenus à l'aide de l'atténuateur variable fibré placé en sortie de l'étage de SHG, correspondent aux valeurs en entrée du PPLN/RW en tenant compte du couplage et des pertes à la propagation à 771 nm. L'erreur associée à ces estimations est de 5%. Comme on peut le voir, les données expérimentales pour la compression et l'anti-compression suivent correctement le comportement quadratique prédit par la théorie. Ceci montre, en particulier, l'absence d'excès de bruit classique sur l'anti-compression.

Un ajustement de l'ensemble des données à l'aide de l'expression 4.12 nous fournit comme paramètres $\mu_{fit} = (0,101 \pm 0,002)\mathrm{mW}^{1/2}$ et une efficacité totale $\eta_{tot,fit} = 0,54 \pm 0,01$. Une comparaison entre $\eta_{tot,fit}$ et notre connaissance des différents paramètres : $\eta_{est} = \eta_c \cdot \eta_T \cdot \eta_{det} \cdot \eta_{el} \approx 0,65$ nous permet d'estimer [3] les pertes à la propagation dans le *ridge* à $\eta_{wg} \backsimeq 0{,}4\,\mathrm{dB/cm}$, une valeur standard pour ce type de composants [277].

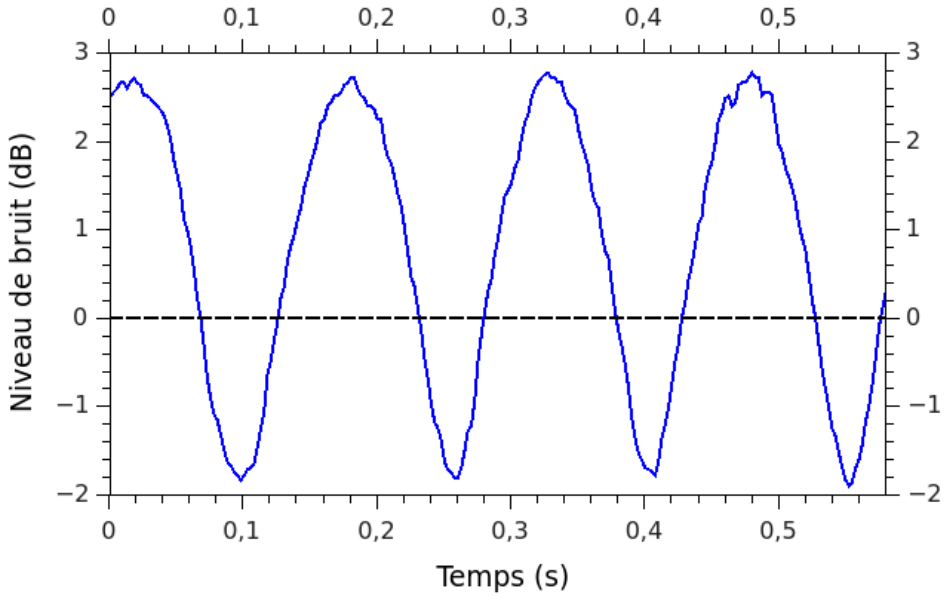


Figure 4.12. – Variance du bruit en fonction de la phase de l'oscillateur local pour une puissance de pompe de 28 mW en entrée du PPLN/RW. Les résultats ont été normalisés au niveau du bruit quantique standard. La fréquence du bruit est de 2 MHz, tandis que la résolution (*resolution bandwidth* - RBW) et la bande vidéo (*video bandwidth* - VBW) de l'analyseur de spectre sont respectivement de 300 kHz et de 30 Hz.

La FIGURE 4.12 correspond à un enregistrement de la puissance du bruit en fonction de le phase de l'oscillateur local dans le cas limite où 28 mW sont injectés en entrée du

3. Pour cette estimation nous avons tenus compte de $L_{ridge}/2$, c'est-à-dire 2 cm.

PPLN/RW. Les niveaux de compression et d'anti-compression mesurés correspondent respectivement à $-1,83 \pm 0,05$ dB et $2,79 \pm 0,05$ dB. En corrigeant ces valeurs par les pertes, cela correspond à un niveau de compression d'environ -3,3 dB obtenu directement à la sortie du guide d'onde, l'une des toutes meilleurs valeurs à ce jour en régime de passage unique et de pompage continu [278]. Une valeur plus élevée pourrait être obtenue en réduisant les pertes de propagation à l'intérieur du PPLN/RW et en employant des photodiodes avec des efficacités de détection plus élevées. L'état de l'art sur la fabrication de PPLN/RW montre des composants présentant moins de 0,2 dB/cm de pertes à la propagation [279]. Parallèlement, des efficacités de détection de 99% à 1550 nm ont déjà été démontrées pour des photodiodes actuellement non-commercialisées [280]. Enfin, une dernière amélioration possible pourrait être de réaliser également l'étage de SHG au sein d'un PPLN/RW de sorte à injecter plus de 28 mW en entrée de l'étage de SPDC.

4.5.2. Critère d'inséparabilité

Nous souhaitons également souligner que notre dispositif peut facilement être reconfiguré de sorte à générer des états intriqués reposant sur de la compression bi-modale. Pour cela, il suffit de mélanger les signaux de sortie de deux PPLN/RW au sein d'un coupleur à fibre 50/50 en amont du système de détection homodyne. L'utilisation d'un tel composant à fibre garantit, de manière automatique, le recouvrement parfait des modes spatiaux associés aux deux faisceaux de lumière comprimée entrants, tout en n'insérant que 0,05 dB de pertes additionnelles.

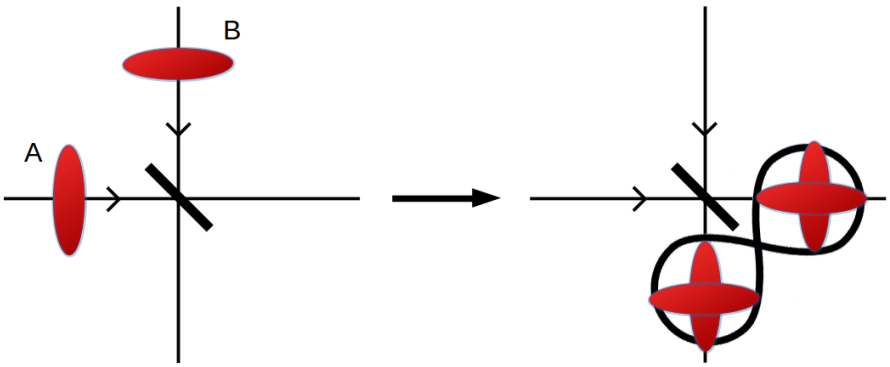


Figure 4.13. – Génération d'intrication par injection de deux états comprimés orthogonaux en entrée d'un coupleur 50/50.

Le critère de Duan [281] nous permet d'estimer le degré d'intrication auquel on peut s'attendre. Concrètement, pour deux états comprimés labellisés A et B, un témoin d'intrication nous est donné par la quantité :

$$\Delta^2_{A,B} = \left\langle [\Delta(\hat{x}_A - \hat{x}_B)]^2 \right\rangle + \left\langle [\Delta(\hat{p}_A + \hat{p}_B)]^2 \right\rangle , \tag{4.14}$$

où une variance des corrélations $\Delta^2_{A,B} < 1$ atteste de la présence d'intrication en sortie du coupleur. En considérant le niveau de compression le plus élevé que nous ayons obtenu, à savoir -1,83 dB, nous obtenons une variance des corrélations de l'ordre de 0,68, soit une valeur bien en dessous de la limite classique.

4.6. Conclusion

Nous avons développé, et ce pour la première fois, un dispositif permettant la génération, la propagation et la détection de lumière comprimé de manière entièrement guidée. Avec un niveau de compression de 3,3 dB directement en sortie du cristal, notre dispositif affiche à ce jour l'une des toutes meilleures valeurs en régime de passage unique jamais mesurée. Notre montage repose uniquement sur les avancées de l'optique non-linéaire guidée et l'utilisation de composants *plug-and-play* issus des télécoms optiques standards. Ces avantages rendent notre approche entièrement compatible avec les réseaux fibrés télécoms en vue de réaliser des protocoles de communication quantique en régime de variables continues en dehors du simple cadre des laboratoires. Le niveau de compression mesuré de 1,83±0,05 dB pourrait être amélioré par l'usage de photodiodes présentant des efficacités de détection proche de l'unité, un guide d'onde avec moins de pertes à la propagation et un étage de SHG présentant une meilleure stabilité ainsi qu'une meilleure efficacité.

Le travail présenté au sein de ce chapitre a fait l'objet d'une publication dans une revue internationale avec comité de lecture, voir la référence [282].

Chapitre 5.

Détecteurs de photons uniques en régime ON/OFF : traitement quantique des effets de gigue temporelle

En complément de l'usage de large alphabets pour l'encodage des données, la communication quantique haut débit nécessite d'avoir recours à des régimes de pompage ultra-rapide ($\geq$ GHz). Dans ce contexte, une limitation majeurd nous est donnée par la gigue temporelle du système de détection. Malgré leur importance dans les technologies quantiques photoniques émergentes, aucun modèle de détecteur incluant de tels effets n'a été développé jusqu'à présent. Nous proposons dans ce chapitre un modèle théorique, basé sur le formalisme de densité de POVM (*Positive Operatore-Valued Measure*), capable de quantifier explicitement l'effet de la gigue temporelle pour la classe de détecteurs de photons uniques la plus couramment utilisée, à savoir celle des détecteurs ON/OFF.

Afin de motiver ce travail, nous revenons tout d'abord sur les limitations associées aux effets de gigue temporelle des détecteurs de photons uniques. Nous présentons ensuite un traitement quantique de ces effets au travers du modèle que nous avons développé. Enfin, nous appliquons notre modèle à différentes situations expérimentales usuelles telles que la détection directe, la détection d'événements en coïncidence ou au cas d'une source de photons annoncés.

5.1. Motivation

La communication quantique est indéniablement la technologie quantique la plus mature dont nous disposons actuellement. Néanmoins, les taux de détection des différents dispositifs en cours d'étude ou d'ors et déjà commercialisés, constituent encore à ce jour une importante limitation. Des techniques de multiplexage temporel permettent en principe de pomper des sources photoniques à des taux de l'ordre du

GHz [283, 284, 285, 254], comme nous l'avons par exemple fait avec le dispositif présenté au chapitre 3. Cependant, les temps de relaxation après chaque événement de détection limitent le débit auquel les signaux de sortie peuvent être délivrés [286]. Et plus critique encore, la résolution temporelle du détecteur introduit un délai aléatoire que nous nommerons τ, entre le temps t auquel le photon arrive effectivement au détecteur, et le temps T auquel le signal électronique associé à l'événement de détection est émis. Dans le cas de régimes de pompage ultra-rapides où les cycles de l'horloge ne sont pas suffisamment espacés temporellement, cet effet empêche la différenciation des différentes contributions [286, 287]. Une illustration de ce phénomène pour un taux de répétition de 2,5 GHz nous est donnée en FIGURE 3.26, où l'on voit clairement les différents pics de coïncidences élargis par l'effet de gigue temporelle se chevaucher à leurs bases.

L'identification rapide et précise des temps de détection des photons joue un rôle crucial dans de nombreuses opérations telles que l'ingénierie d'états quantiques, la génération quantique de nombres aléatoires ou encore l'établissement quantique de clés secrètes. Il est donc de la plus haute importance de pouvoir correctement décrire les performances du système de détection. Malgré de nombreuses études des effets de gigue temporelle à la détection [286, 288, 289], ces derniers n'ont jamais été, à notre connaissance, inclus dans un modèle reposant entièrement sur un traitement quantique de la photodétection.

Dans notre étude, nous abordons explicitement ce point en fournissant une théorie capable de tenir compte du comportement temporel des détecteurs standard de photons individuels affectés par une instabilité temporelle non négligeable et en présence de temps mort. Nous adoptons le formalisme des mesures positives évaluées par l'opérateur (POVM). Cette approche a été largement exploitée pour décrire différents types d'appareils de mesure [290], y compris les effets de temps mort [291], ainsi que pour caractériser expérimentalement les paramètres de détecteurs inconnus [292, 293, 294, 295, 296]. Dans notre travail, nous nous concentrerons sur les dispositifs ON/OFF tels que les photodiodes à avalanches (APD), c'est-à-dire les détecteurs de photons uniques sans capacités de résolution du nombre de photons. Notre étude peut être facilement généralisée à tout schéma de multiplexage spatial où plusieurs détecteurs ON/OFF sont utilisés en parallèle [290, 297]. Aussi, pour des raisons de simplicité mais sans perte de généralité, nous avons choisi dans notre traitement de négliger la contribution des coups sombres qui pourraient toutefois facilement être pris en compte, comme nous le préciserons par la suite.

5.2. Rappel sur les règles de projection

Avant d'introduire notre modélisation des effets de gigue temporelle, nous revenons dans cette section sur la mesure quantique et la règle de projection qui lui est associée.

Après un rappel sur le cas d'une mesure idéale (projective), nous introduisons la notion de POVM dans le cadre d'une mesure générale.

5.2.1. Cas d'une mesure idéale

Dans l'expérience dite du 'chat de Schrödinger', le chat joue à merveille le rôle d'appareil de mesure. C'est un système macroscopique dont l'état - mort ou vivant - permet de réaliser une mesure de l'état du noyau atomique. Ainsi, un chat mort indique que le noyau est dans son état fondamental $|f\rangle$ alors qu'un chat vivant indique que le noyau est dans son état excité $|e\rangle$. Les mesures sur le noyau sont en fait caractérisées par ces états et peuvent être représentées par des projecteurs $\hat{P}_{mort} = |f\rangle\langle f|$ et $\hat{P}_{vivant} = |e\rangle\langle e|$. Ces derniers agissent sur l'espace de Hilbert du système mesuré et constituent une résolution de son identité $\hat{P}_{mort} + \hat{P}_{vivant} = \hat{\mathbb{1}}$.

De manière générale, l'état du système mesuré $|\psi\rangle$ à la lecture du résultat n est projeté sur l'état correspondant à ce résultat :

$$|\psi\rangle \longrightarrow |\psi_n\rangle = \frac{\hat{P}_n |\psi\rangle}{\sqrt{\langle\psi| \hat{P}_n |\psi\rangle}}, \tag{5.1}$$

où les projecteurs $\hat{P}_n$ constituent un ensemble complet de projecteurs orthogonaux tels que $\hat{P}_m \hat{P}_n |\psi\rangle = \delta_{m,n} \hat{P}_n$ et $\sum_n \hat{P}_n = \hat{\mathbb{1}}$. La projection décrite par l'équation 5.1 se généralise sans grande difficulté à un système décrit par un opérateur densité $\hat{\rho}$:

$$\hat{\rho} \longrightarrow \hat{\rho}_n = \frac{\hat{P}_n \hat{\rho} \hat{P}_n}{\mathrm{Tr}\left\{\hat{P}_n \hat{\rho} \hat{P}_n\right\}}. \tag{5.2}$$

Il s'agit de l'énoncé habituel du postulat de projection introduit par John Von Neumann en 1932 [298]. Il donne l'état conditionné sur le résultat de la mesure n, obtenu avec une probabilité donnée par la règle de Born :

$$\Pr(n) = \mathrm{Tr}\left\{\hat{\rho} \hat{P}_n\right\}. \tag{5.3}$$

On parle également de mesures projectives. Ces dernières sont très intéressantes puisque l'état conditionné est alors simplement donné par $\hat{\rho} = \hat{P}_n$. Si l'on effectue une autre mesure immédiatement après la première, le résultat de cette dernière devient même certain, c'est encore le résultat n puisque $\hat{P}_n^2 = \hat{P}_n = \hat{P}_n^\dagger$. Ce comportement est à l'origine par exemple de l'effet Zénon quantique où l'évolution d'un système peut être 'gelée' par la répétition de mesures appropriées.

Enfin, lorsque le résultat de la mesure n'est pas utilisé pour conditionner l'évolution future du système (mesure 'non-lue'), l'évolution du système est alors décrite par :

$$\hat{\rho} \longrightarrow \sum_n \Pr(n)\hat{\rho}_n = \sum_n \hat{P}_n \hat{\rho} \hat{P}_n. \tag{5.4}$$

L'opérateur densité se réduit à sa partie diagonale (par blocs) dans la base des états propres associés aux $\hat{P}_n$, il y a décohérence induite par la mesure.

5.2.2. Cas d'une mesure générale

Généralité

Les mesures projectives obéissants aux postulats de von Neumann ne sont pas le mode le plus fréquent d'acquisition d'information sur un système quantique. Souvent, de l'information est obtenue par une mesure qui détruit le système mesuré (c'est le cas général du comptage de photons). En pratique, l'état de l'appareil de mesure est un paramètre important à prendre en compte, en particulier parce que la dimension de l'espace des états de l'ensemble système mesuré + appareil de mesure est plus grande que celle du sous-espace du système seul. Cela implique de revoir la notion de projecteur et de mesure projective.

Pour décrire l'évolution du système mesuré dans le cas d'une mesure généralisée, commençons par remplacer les projecteurs $\hat{P}_n$ d'une mesure idéale par un ensemble d'opérateurs $\hat{M}_n$ (non nécessairement hermitiques) satisfaisant la relation :

$$\sum_n \hat{M}_n^\dagger \hat{M}_n = \hat{\mathbb{1}}. \tag{5.5}$$

Une mesure généralisée associée à cet ensemble d'opérateurs effectuée sur un état $|\psi\rangle$, donne le résultat n avec la probabilité $\Pr(n) = \langle\psi| \hat{M}_n^\dagger \hat{M}_n |\psi\rangle$, et projette dans ce cas le système dans l'état après mesure :

$$|\psi\rangle \longrightarrow |\psi_n\rangle = \frac{\hat{M}_n |\psi\rangle}{\sqrt{\langle\psi| \hat{M}_n^\dagger \hat{M}_n |\psi\rangle}}. \tag{5.6}$$

Pour un système dans un mélange statistique (décrit par $\hat{\rho}$), le résultat n est donné avec la probabilité :

$$\Pr(n) = \mathrm{Tr}\left\{\hat{\rho}\hat{M}_n^\dagger \hat{M}_n\right\}, \tag{5.7}$$

et l'évolution est alors décrite par :

$$\hat{\rho} \longrightarrow \hat{\rho}_n = \frac{\hat{M}_n \hat{\rho} \hat{M}_n^\dagger}{\mathrm{Tr}\left\{\hat{\rho}\hat{M}_n^\dagger \hat{M}_n\right\}}. \tag{5.8}$$

De façon générale, les $\hat{\Pi}_n = \hat{M}_n^\dagger \hat{M}_n$ sont des opérateurs hermitiques positifs (à valeurs propres positives ou nulles). L'ensemble des $\hat{\Pi}_n$ constitue un POVM. Il est facile de vérifier que ces éléments POVM sont également une résolution de l'identité :

$$\sum_n \hat{\Pi}_n = \hat{\mathbb{1}}. \tag{5.9}$$

Contrairement aux mesures projectives décrites précédemment, ces opérateurs ne sont pas des projecteurs puisqu'en général $\hat{\Pi}_m \hat{\Pi}_n \neq \delta_{m,n} \hat{\Pi}_n$. Une mesure POVM mélange les états et ne préserve pas la pureté. On parle alors de mesures généralisées qui sont le cadre dans lequel nous nous plaçons dans ce chapitre.

Exemple du comptage de photons

Un compteur de photons absorbe les quanta de lumière en ionisant les atomes d'une photo-cathode, les électrons résultant étant détectés après une amplification par avalanche. Certains photodétecteurs fournissent un courant proportionnel au nombre de photons absorbés et sont ainsi capable de résoudre des nombres de photons différents. Si l'on néglige les effets de gigue temporelle, cette mesure destructive peut être décrite par les opérateurs du champ :

$$\hat{M}_n = |0\rangle\langle n| \quad (n = 0, 1, 2, ...), \tag{5.10}$$

où $|0\rangle$ est l'état du vide dans le mode du champ mesuré et $|n\rangle$ un état de Fock à n photons. La relation de fermeture est ici bien vérifiée :

$$\sum_n \hat{M}_n^\dagger \hat{M}_n = \sum_n |n\rangle\langle n| = \hat{\mathbb{1}}. \tag{5.11}$$

La probabilité de trouver n photons dans l'état $|\psi\rangle$ du mode du champ est donnée par :

$$\Pr(n) = |\langle n|\psi\rangle|^2. \tag{5.12}$$

L'état qui subsiste après la mesure étant celui du vide, les photons sont détruits lorsqu'ils sont 'comptés'.

Exemple d'une APD en l'absence de gigue temporelle

Une APD, la classe de détecteur à laquelle nous nous intéressons dans ce chapitre, ne permet pas de résoudre le nombre de photons. Un tel détecteur possède uniquement deux réponses traditionnellement appelées ON, c'est-à-dire au moins un photon a été détecté, et OFF, c'est-à-dire aucun photon n'a été détecté. Dans le cas d'une efficacité parfaite, les deux éléments POVM sont donnés par $\hat{\Pi}_{\text{off}} = |0\rangle\langle 0|$ et $\hat{\Pi}_{\text{on}} = \hat{\mathbb{1}} - \hat{\Pi}_{\text{off}}$. En tenant compte de l'efficacité η du détecteur, ces expressions deviennent :

$$\begin{cases} \hat{\Pi}_{\text{off}} = \sum_k (1-\eta)^n \left|n\right\rangle\!\left\langle n\right|, \\ \hat{\Pi}_{\text{on}} = \hat{\mathbb{1}} - \hat{\Pi}_{\text{off}}, \end{cases} \tag{5.13}$$

5.3. Modélisation des effets de gigue temporelle

Nous venons de voir comment décrire une APD au moyen d'éléments POVM en l'absence de gigue temporelle. Lorsque les propriétés temporelles du détecteurs sont prises en compte, nous sommes alors en présence d'un panel continu d'événements 'ON' qu'il nous faut modéliser.

5.3.1. Notion de densité de POVM

Cette structure plus riche nous amène à composer avec la notion de densité de POVM que nous introduisons au sein de cette section.

Définitions

En considérant les propriétés temporelles du détecteur, chaque événement de détection correspond désormais à un signal électronique délivré au temps $T = t + \tau$ et à l'information 'au moins un photon s'est présenté au détecteur à un temps inférieur à T', voir FIGURE 5.1.

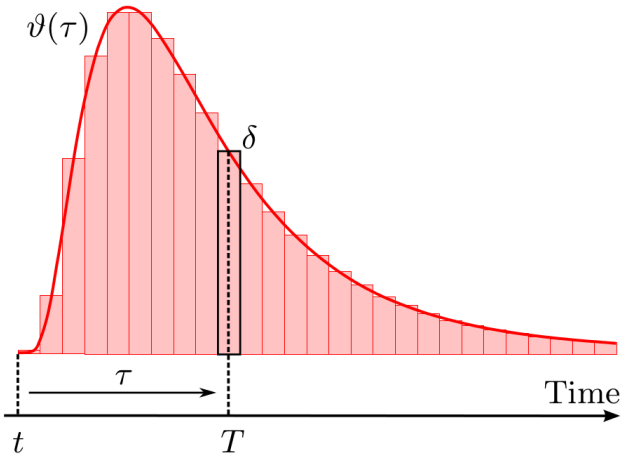


Figure 5.1. – Temps caractéristiques et fonction de réponse $\vartheta(\tau)$ d'un détecteur ON/OFF. La résolution temporelle du détecteur introduit un délai aléatoire τ, entre le temps t auquel le photon arrive effectivement au détecteur, et le temps T auquel le signal électronique associé à l'événement de détection est émis.

Pour décrire l'effet de gigue temporelle, nous introduisons pour une variable aléatoire τ, une densité de probabilité $\vartheta(\tau)$. Le principe de causalité nous impose $\vartheta(\tau < 0) = 0$, tandis que le profil de la fonction dépend du détecteur utilisé et peut en principe être reconstruit expérimentalement. Il existe une infinité de valeurs possibles de τ - et donc également de valeurs possibles de T - infiniment proches les unes des autres. Par conséquent, les résultats de mesure sont infinis et distribués de manière continue. De fait, la probabilité pour un état entrant $\hat{\rho}$ donné que le détecteur délivre un signal de sortie entre T et $T + \mathrm{d}T$ ($\mathrm{d}T$ étant infinitésimale) peut, en toute généralité, être exprimée comme $p_{\mathrm{on}}(T, \hat{\rho})\,\mathrm{d}T$, avec $p_{on}(T, \hat{\rho})$ une densité de probabilité dont le profil dépend explicitement de $\vartheta(\tau)$ [1] et de l'efficacité de détection η.

Par analogie avec la raisonnement qui vient d'être fait, nous introduisons la densité de POVM, $\hat{\pi}_{\mathrm{on}}(T)$ [299], telle que :

$$p_{on}(T, \hat{\rho}) = \mathrm{Tr}\left\{\hat{\rho}\hat{\pi}_{on}(T)\right\}. \tag{5.14}$$

À titre de remarque, le cas d'un détecteur ON/OFF standard (cas où l'on ne tient pas compte des effets temporels) s'obtient facilement à travers l'opération d'intégration : $\hat{\Pi}_{\mathrm{on}} = \int \hat{\pi}_{\mathrm{on}}(T)\,\mathrm{d}T$ (et donc $\hat{\Pi}_{\mathrm{off}} = \hat{\mathbb{1}} - \int \hat{\pi}_{\mathrm{on}}(T)\,\mathrm{d}T$). Aussi, afin de décrire plus facilement le cas de situations expérimentales, il est possible de discrétiser l'ensemble continu en introduisant une partition des valeurs de T sur des intervalles δ (voir Figure 5.1) correspondant à la résolution temporelle de l'électronique de détection. Par l'intermédiaire de cette simplification, il est dès lors possible de travailler avec un ensemble fini de résultats de mesure, et donc de se placer dans la situation d'un ensemble fini de POVMs, $\left\{\hat{\Pi}_{\mathrm{on}}(T \in \delta), \hat{\Pi}_{\mathrm{off}}(T \in \delta)\right\}$, où, $\forall\delta$, $\hat{\Pi}_{\mathrm{on}}(T \in \delta) = \int_{\delta} \hat{\pi}_{\mathrm{on}}(T)\,\mathrm{d}T$, et $\hat{\Pi}_{\mathrm{off}}(T \in \delta) = \hat{\mathbb{1}} - \hat{\Pi}_{\mathrm{on}}(T \in \delta)$.

Normalisation

Avant d'expliciter l'expression de $\hat{\pi}_{on}(T)$, nous souhaitons également insister sur le fait que nous avons défini les éléments POVM ON et OFF uniquement au moyen de $\hat{\pi}_{on}(T)$. Il est en effet impossible de définir de densité de probabilité et de densité de POVM associés au résultat de mesure 'le capteur ne se déclenche pas'. La raison pour cela est que l'absence de déclenchement à un moment donné n'est pas spécifique d'un événement, mais commun à plusieurs. Sur un intervalle infinitésimal, $\hat{\Pi}_{\mathrm{off}}(T)$ est en effet proche de l'opérateur identité, donc loin d'être proportionnel à la taille de cet intervalle. Sommer sur les $\hat{\Pi}_{\mathrm{off}}(T)$ n'aurait ainsi aucun sens, de même que de définir une densité de probabilité $p_{\mathrm{off}}(T, \hat{\rho})$, ou une densité de POVM $\hat{\pi}_{\mathrm{off}}(T)$. Dans le cadre de notre étude, ces considérations n'ont aucune incidence puisque la densité de POVM $\hat{\pi}_{on}(T)$ est suffisante pour décrire différentes situations expérimentales usuelles englobant la détection directe,

1. Le cas d'un détecteur sans effet de gigue correspond à la limite où $\vartheta(\tau)$ tend vers une distribution de Dirac.

la mesure de coïncidences, ainsi que les sources de photons annoncés, puisque toutes ces opérations reposent uniquement sur les résultats de la détection ON.

5.3.2. État en entrée du détecteur

Notre étude se voulant la plus exhaustive possible, ceci nous amène à considérer le cas général de photons non simultanés en entrée du détecteur, et donc à nous placer dans le cadre d'un formalisme multimode. Concrètement, dans le cas de k photons se présentant au détecteur à des temps t_j, $j \in [1, k]$, ceci revient à travailler avec des opérateurs $\hat{\rho} = \hat{\rho}_k$ de la forme :

$$\hat{\rho}_k = |1_{t_1}\rangle\langle 1_{t_1}| \otimes |1_{t_2}\rangle\langle 1_{t_2}| \otimes \cdots \otimes |1_{t_k}\rangle\langle 1_{t_k}|\,, \tag{5.15}$$

où les $|1_{t_j}\rangle$ sont définis à partir de l'action des opérateurs création : $\hat{a}^\dagger(t_j)\,|0\rangle$. Différents '$t_j$' correspondent à différents modes temporels [300] :

$$[\hat{a}\,(t_i)\,, \hat{a}\,(t_j)] = 0 \quad \text{et} \quad [\hat{a}\,(t_i)\,, a^\dagger\,(t_j)] = \delta\,(t_i - t_j)\,. \tag{5.16}$$

Dans le cas particulier de k photons parfaitement simultanés ($t_j = t$, pour tout j), $\hat{\rho}_k$ se réduit, à un facteur de normalisation près, à $|k\rangle\langle k|$, c'est-à-dire à un projecteur sur un état de Fock à k photons dans le même mode temporel.

5.3.3. Statistiques et POVM

Expression générique de la densité de POVM

L'expression de $\hat{\pi}_{\text{on}}(T)$ est bien entendu indépendante de l'état entrant sur le détecteur, toutefois dans un soucis de pédagogie visant à ne pas trop alourdir les notations, nous commençons, en suivant une approche similaire à celle de la référence [290], par dériver son expression dans le cas particulier d'un état de Fock monomode, c'est-à-dire $\hat{\rho}_k = |k\rangle\langle k|$. Une photodiode étant insensible à la phase et faisant l'hypothèse que la densité de POVM est diagonale dans la base des états que l'on vient de définir en 5.3.2, nous pouvons alors écrire pour un état de Fock monomode :

$$\hat{\pi}_{\text{on}}(T) = \sum_k c_k(T)\,|k\rangle\langle k|\,. \tag{5.17}$$

Et à partir de l'expression de la densité de probabilité,

$$
\begin{aligned}
p_{\mathrm{on},k}(T) &= \mathrm{Tr}\left\{\hat{\pi}_{\mathrm{on}}(T)\,|k\rangle\langle k|\right\}, && (5.18)\\
&= \sum_m \langle m|\,\hat{\pi}_{\mathrm{on}}(T)\,|k\rangle\,\langle k|m\rangle\,, && (5.19)\\
&= \langle k|\,\hat{\pi}_{\mathrm{on}}(T)\,|k\rangle\,, && (5.20)\\
&= \langle k|\left[\sum_l c_l(T)\,|l\rangle\langle l|\right]|k\rangle\,, && (5.21)\\
&= \sum_l c_l(T)\,\langle k|l\rangle\,\langle l|k\rangle\,, && (5.22)\\
&= c_k(T), && (5.23)
\end{aligned}
$$

on obtient comme expression de la densité de POVM :

$$\hat{\pi}_{\mathrm{on}}(T) = \sum_k p_{\mathrm{on},k}(T)\,|k\rangle\langle k|\,. \tag{5.24}$$

La démarche que l'on vient de suivre est facilement généralisable à un état $\hat{\rho}_k$ quelconque, au quel cas on arrive, après quelques lignes de calcul que nous ne détaillerons pas ici, à l'expression standard de la densité de POVM :

$$\hat{\pi}_{\mathrm{on}}(T) = \sum_k p_{\mathrm{on},k}(T)\hat{\rho}_k. \tag{5.25}$$

Construction de la loi de probabilité

Nous allons maintenant déterminer la loi de probabilité pour l'instant de détection du premier photon vu par le capteur. Étant donné un état $\hat{\rho}_k$, chacun des k photons peut engendrer la génération d'un signal de détection au temps $T_j = t_j + \tau_j$, où les τ_j sont distribués selon la densité de probabilité $\vartheta(\tau)$. Cependant, lorsqu'un premier signal est émis, le détecteur devient aveugle à tout signal optique durant son temps de relaxation (temps mort). Ainsi, un détecteur éclairé par de multiples photons émettra un unique signal 'ON' à un temps $T = \min(T_j)$. En d'autres termes, tous les photons conduisant à des événements de détection associés à des temps supérieurs à T et inférieur au temps de relaxation ne contribuent pas au signal de sortie du détecteur. Après relaxation, le détecteur est réinitialisé et un nouveau cycle de détection peut commencer. En tenant compte des effets combinés du temps de relaxation et de la gigue temporelle à la détection, $p_{\mathrm{on},k}(T)$ peut alors être exprimée de la façon suivante :

$$p_{\mathrm{on},k}(T) = \sum_{i=1}^{k} p_i(T) \prod_{j\neq i} P\left(t_j + \tau_j > T\right). \tag{5.26}$$

Nous allons désormais expliciter chaque terme de (5.26) afin d'obtenir une expression complète de la densité de probabilité. Ainsi :

- La somme provient du fait que chacun des photons peut être détecté en premier. Plus on envoie de photons, plus le capteur a de chance d'en voir un à un instant donné (ici on ne prend pas en compte la primauté à la détection).
- $p_i(T)$ représente la densité de probabilité pour le photon i d'être détecté au temps T. Il ne faut pas oublier de prendre en compte l'efficacité finie η du détecteur. Comme vu en première partie, $p_i(T) = \eta\vartheta_i\left(T-t\right)$, où $T-t$ est le délai écoulé depuis l'arrivée du photon sur le capteur.
- Le produit apparaît parce qu'il faut que tous les photons autres que i arrivent après celui-ci. Détaillons l'obtention de la valeur de $P\left(t+\tau_j > T\right)$:

  — $P\left(t+\tau_j > T\right)$ est la probabilité que le photon j soit détecté après le temps T, ou jamais. C'est aussi la probabilité que le délai τ_j soit supérieur à $T-t$: $P\left(t+\tau_j > T\right) = P\left(\tau_j > T-t\right)$.

  — $\eta \int_{-\infty}^{T} \vartheta_j(T'-t_j)\,\mathrm{d}T'$ est la probabilité pour le photon j d'être détecté avant que le délai depuis son arrivée ne soit de $T-t$, c'est-à-dire la probabilité d'être détecté avant le temps T. Ici, l'efficacité η a été prise en compte. L'intégrale part de $-\infty$ mais on rappelle que la causalité implique que $\vartheta(\tau) = 0$ pour τ négatif ; on pourrait donc aussi démarrer de 0.

  — $1-\eta \int_{-\infty}^{T} \vartheta_j(T'-t_j)\,\mathrm{d}T'$ est donc la probabilité pour le photon j de ne pas être détecté avant T, celle que l'on cherchait à déterminer. Il vient alors :

$$P\left(t+\tau_j > T\right) = 1-\eta\int_{-\infty}^{T}\vartheta_j(T'-t_j)\,\mathrm{d}T' \tag{5.27}$$

En combinant les équations (5.25), (5.26) et (5.27), nous arrivons finalement à l'expression générale de $\hat{\pi}_{\mathrm{on}}(T)$:

$$\hat{\pi}_{\mathrm{on}}(T) = \sum_{k\in\mathbb{N}}\sum_{i=1}^{k}\eta\hat{\vartheta}_i(T)\bigotimes_{j\neq i}\left[\hat{\mathbb{1}}-\eta\int_{-\infty}^{T}\hat{\vartheta}_j(T')\,\mathrm{d}T'\right], \tag{5.28}$$

avec $\hat{\vartheta}_j(T)$ prenant désormais la forme d'un opérateur :

$$\hat{\vartheta}_j(T) = \int \vartheta(T-t_j)\,|1_{t_j}\rangle\langle 1_{t_j}|\,\mathrm{d}t_j. \tag{5.29}$$

Dans cette dernière expression nous avons conservé un label sur $\hat{\vartheta}_j(T)$ afin d'expliciter le sous espace sur lequel nous travaillons. En pratique cependant, l'expression de $\hat{\pi}_{\mathrm{on}}(T)$

est indépendante des temps d'arrivée des photons, 't_j' étant seulement une variable d'intégration.

Les coups sombres (*dark counts*) étant indépendant du signal optique et constant dans le temps, le bruit à la détection pourrait facilement être pris en compte dans notre modèle en ajoutant à la densité de POVM un terme correspondant à l'opérateur identité $\hat{\mathbb{1}}$, pondéré par le taux de coups sombres du détecteur.

Remarque sur le cas de photons simultanés

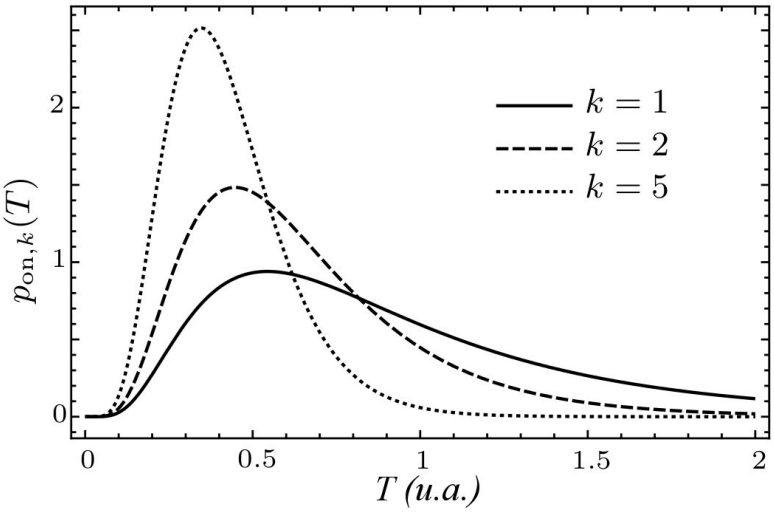


Figure 5.2. – Densité de probabilité associée au temps de détection pour $k = 1, 2, 5$ photons arrivant simultanément au niveau du détecteur à l'instant $t = 0$. Le profil choisi est celui d'une distribution log-normale avec une moyenne de 1 et une déviation standard de 1/2. Pour mieux différencier les effets, nous avons considéré un détecteur sans perte ($\eta = 1$).

L'opérateur densité de l'équation (5.28) correspond au cas général de photons non simultanés. Le cas particulier où tout les photons, ou juste une partie d'entre eux, sont simultanés peut être obtenu en prenant $t_j = t$ pour $j = 1, \ldots, k'$ avec $k' \leq k$. Remarquons qu'en pareille situation, les effets de gigue dépendent du nombre de photons simultanés k'. La FIGURE 5.2 présente l'évolution de $p_{\mathrm{on},k}(T)$ dans le cas limite où $k' = k$, et ce pour différentes valeurs de k. À titre d'exemple, nous avons choisi pour $\vartheta(\tau)$ un profil en log-normal, avec une moyenne de 1 et une déviation standard de 1/2. Aussi, pour mieux différencier les effets, nous avons considéré un détecteur sans perte, c'est-à-dire $\eta = 1$. Le cas $k = 1$ correspond à $p_{\mathrm{on},k}(T) = \vartheta(T - t)$. Comme on peut le voir, plus le nombre de photons arrivant simultanément est important, plus le profil de $p_{\mathrm{on},k}(T)$ est modifié, la gigue devient alors moins large et son maximum est translaté en direction des

T inférieurs. Ceci confirme un comportement intuitif : plus un grand nombre de photons arrivent simultanément, plus la proabilité que le détecteur se déclenche tôt augmente. En conséquence de quoi le profil de la gigue dépend du signal entrant. Dans un contexte experimental, cet effet est rarement observé puisque le nombre moyen de photons par impulsion est souvent inférieur voir bien inférieur à 1.

5.4. Applications

Nous appliquons dans cette section le modèle qui vient d'être introduit à différentes situations expérimentales courantes telles que la détection directe, la détection d'événements de coïncidences ou encore le cas d'une source de photons annoncés.

5.4.1. Détection directe

À l'aide de l'expression de la densité de POVM $\hat{\pi}_{\text{on}}(T)$ que nous venons d'établir, il nous est désormais possible d'étudier le cas d'une détection directe où le temps de cohérence des photons est non négligeable devant l'amplitude de la gigue temporelle du détecteur. Dans ces conditions, les incertitudes temporelles liées au temps de cohérence du signal entrant et à la gigue du détecteur deviennent corrélées.

Photon gun

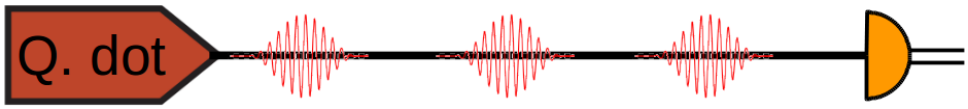


Figure 5.3. – Une source de type *photon gun* à base d'une boîte quantique. La photodiode à avalanche mesure directement la lumière provenant de la source.

Ces corrélations peuvent être visualisées, de manière triviale, en considérant le cas d'un état de Fock à un photon $\hat{\rho} = |\psi\rangle\langle\psi|$ avec $|\psi\rangle = \int \psi(t)\,|1_t\rangle\,\mathrm{d}t$. Cette situation correspond au cas d'un 'pistolet à photons' (*photon gun*) comme ceux réalisés à partir de boîtes quantiques en cavité idéales [301]. Un tel scénario est illustré Figure 5.3. À partir de l'équation (5.28) avec $k = 1$, on a pour la densité de POVM l'expression simple :

$$\hat{\pi}_{\text{on}}(T) = \eta \int \vartheta(T-t)\,|1_t\rangle\langle 1_t|\,\mathrm{d}t, \tag{5.30}$$

et par application de la relation (5.14), on obtient pour la densité de probabilité de détection :

$$p_{\text{on}}(T, |\psi\rangle\langle\psi|) = \eta \int \vartheta(T-t)|\psi(t)|^2 \mathrm{d}t. \tag{5.31}$$

La densité de probabilité de détecter un photon est ainsi donnée par la convolution de la réponse du détecteur avec la densité de probabilité d'arrivée du photon sur le détecteur.

Cas de N photons séparables

Ce résultat se généralise facilement au cas de N photons en l'absence d'intrication. Les états des photons étant séparables, on peut écrire l'opérateur densité de l'état sous la forme $\hat{\rho}_N = \bigotimes_{i=1}^{N} |\psi_i\rangle\langle\psi_i|$, avec $|\psi_i\rangle = \int \psi_i(t_i)\,|1_{t_i}\rangle\,\mathrm{d}t_i$. À titre d'exemple, on obtient pour $N = 2$:

$$\begin{aligned} p_{\text{on}}(T, \hat{\rho}_2) = p_{\text{on}}(T, |\psi_1\rangle\langle\psi_1|) \left[1 - \eta \int_{-\infty}^{T} \mathrm{d}T' \int \vartheta(T'-t_2)|\psi_2(t_2)|^2\,\mathrm{d}t_2\right] \\ + p_{\text{on}}(T, |\psi_2\rangle\langle\psi_2|) \left[1 - \eta \int_{-\infty}^{T} \mathrm{d}T' \int \vartheta(T'-t_1)|\psi_1(t_1)|^2\,\mathrm{d}t_1\right], \end{aligned} \tag{5.32}$$

où le premier terme représente à la situation où le signal de sortie émis au temps T est associé à la détection du photon '1' et à la non-détection du photon '2', tandis que le second terme correspond à la situation inverse. Des résultats analogues peuvent être obtenus dans le cas d'un nombre de photons N quelconque.

5.4.2. Mesure de coïncidences

On étudie maintenant le cas d'une mesure de coïncidences entre photons d'une même paire. Nous labellisons dans ce qui suit par A et B les modes spatiaux respectifs des deux photons.

Photons intriqués

L'état joint est, en absence d'information sur la séparabilité des photons, un état intriqué de la forme :

$$|\varphi_{A,B}\rangle = \int \varphi(t_A, t_B)\,|t_A\rangle_A \otimes |t_B\rangle_B\,\mathrm{d}t_A\mathrm{d}t_B, \tag{5.33}$$

auquel on associe l'opérateur densité $\hat{\rho}_{A,B} = |\varphi_{A,B}\rangle\langle\varphi_{A,B}|$. Par analogie avec la quantité nommée amplitude spectrale jointe que nous avions introduit en section 3.3.4, $\varphi(t_A, t_B)$ est ici l'amplitude temporelle jointe du système. Un tel état correspond, par exemple,

au signal émis par un convertisseur paramétrique spontané non dégénéré (SPDC), voir FIGURE 5.4. Afin de simplifier l'étude, nous considérons ici uniquement la présence d'un unique photon dans chaque mode spatial. Le cas de multi-paires peut être facilement obtenus en appliquant, pour chaque mode, la densité de POVM décrite par l'équation (5.28).

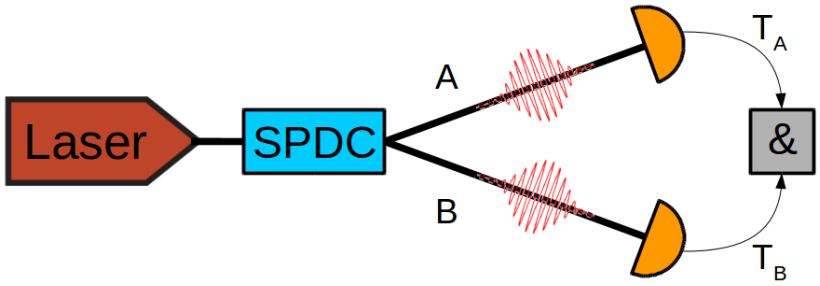


Figure 5.4. – Génération de paires de photon par conversion paramétrique spontanée (SPDC) et mesure de coïncidences.

Les corrélations temporelles peuvent alors êtres évaluées au moyen de la densité de probabilité jointe :

$$p_{\text{on}}(T_A, T_B) = \langle \varphi_{A,B} | \, \hat{\pi}_{\text{on}}(T_A, T_B) \, | \varphi_{A,B} \rangle \, , \tag{5.34}$$

où $\hat{\pi}_{\text{on}}(T_A, T_B) = \hat{\pi}_A(T_A) \otimes \hat{\pi}_B(T_B)$ est la densité de POVM étendue au cas de deux photons spatialement non-dégénérés. Dans la limite d'un unique photon par mode spatial, $\hat{\pi}_A(T_A)$ et $\hat{\pi}_B(T_B)$ sont décrits par l'équation (5.30). En accord avec l'état (5.33) :

$$p_{\text{on}}(T_A, T_B) = \eta^2 \iint \vartheta_A(T_A - t_A)\vartheta_B(T_B - t_B)|\varphi(t_A, t_B)|^2 \, \mathrm{d}t_A \mathrm{d}t_B. \tag{5.35}$$

Ici nous gardons le résultat le plus général possible en considérant deux détecteurs ON/OFF avec, à priori, deux gigues temporelles décrites par des fonctions différentes. La densité de probabilité exprimé en 5.35 est une convolution double entre les fonctions de réponse des deux détecteurs et l'intensité temporelle jointe de la paire de photons.

Expérimentalement, la densité de probabilité de détection peut être reconstruite à l'aide d'une électronique de coïncidence permettant le *time-tag* des événements de détection tel qu'un TDC (*Time to Digital Converter*, voir annexe C). Cependant, il est également courant dans les experiences d'optique quantique d'enregistrer les évenements de coïncidences au moyen d'un TAC (*Time to Amplitude Converter*, voir annexe C), où seul le délai Δ_d entre la détection du photon *start* et la détection du photon *stop* est mesuré. La densité de probabilité associée à ce type de mesure est donné par :

$$p_{B-A}(\Delta_d) = \int p_{\text{on}}(T, T+\Delta_d)\,\mathrm{d}T. \tag{5.36}$$

Cette dernière peut être obtenue par l'application de la densité de POVM $\hat{\pi}_{B-A}(\Delta_d)$ associée à la mesure du délai et définie comme :

$$\hat{\pi}_{B-A}(\Delta_d) = \int \hat{\pi}_{A,B}(T, T+\Delta_d)\,\mathrm{d}T. \tag{5.37}$$

Notons également que par le changement de variables suivant, $T_A = t_A + \tau$ et $t_B = t_A + bart$, $\hat{\pi}_{B-A}(\Delta_d)$ peut être exprimée comme la convolution de deux fonctions de corrélation, la première dépendant uniquement des propriétés des détecteurs utilisés, et la seconde uniquement des états entrants :

$$\hat{\pi}_{B-A}(\Delta_d) = \eta^2 \int\int \vartheta_A(\tau)\vartheta_B(\tau+\Delta_d\bar{t}\,\mathrm{d}\tau \int |t_A\rangle\langle t_A| \otimes |t_A+\bar{t}\rangle\langle t_A+\bar{t}|\;\mathrm{d}t_A\,\mathrm{d}\bar{t}. \tag{5.38}$$

Photons quasi-simultanés

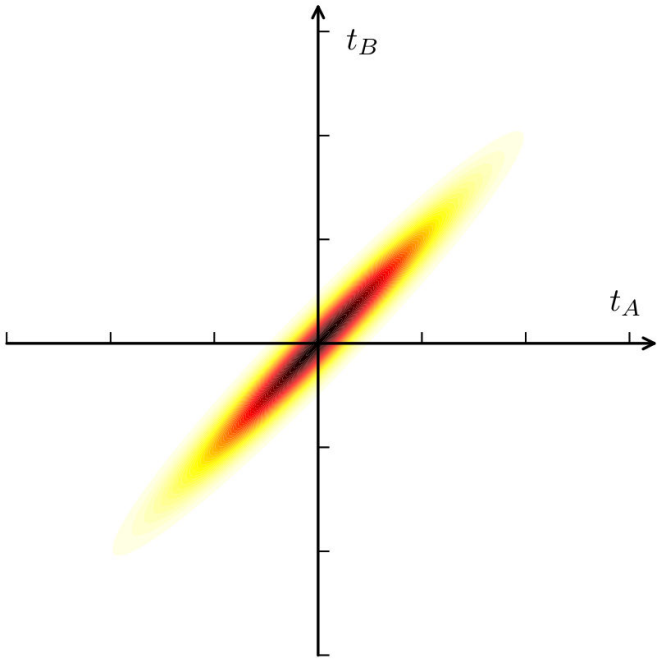


Figure 5.5. – Exemple d'intensité temporelle jointe $|\varphi(t_A, t_B)|^2$ pour une paire de photons quasi-simultanés émis par SPDC.

Dans le cas particulier de photons quasi-simultanés, comme ceux produits par SPDC, l'amplitude temporelle jointe prend la forme $\varphi(t_A, t_B) = \psi(t_A)\chi(t_B - t_A)$, où ψ correspond à la distribution des temps d'émissions associés aux paires de photons, tandis que χ représente la distribution des délais entre photons d'une même paire [302]. Un exemple d'intensité temporelle jointe est donné en FIGURE 5.5. Les deux fonctions étant normalisées, le résultat de l'intégration de leurs normes au carré est égal à l'unité. À l'aide des équations (5.35), (5.36) et (5.37), on obtient :

$$p_{B-A}(\Delta_d) = \eta^2 \int |\chi(\bar{t})|^2 \int \vartheta_A(\tau)\vartheta_B(\tau + \Delta_d - \bar{t})\,\mathrm{d}\tau\,\mathrm{d}\bar{t}. \tag{5.39}$$

Comme on pouvait s'y attendre, la distribution sur les temps d'émission des paires a complètement disparu, seule compte ici la différence entre les temps d'émission des photons d'une même paire.

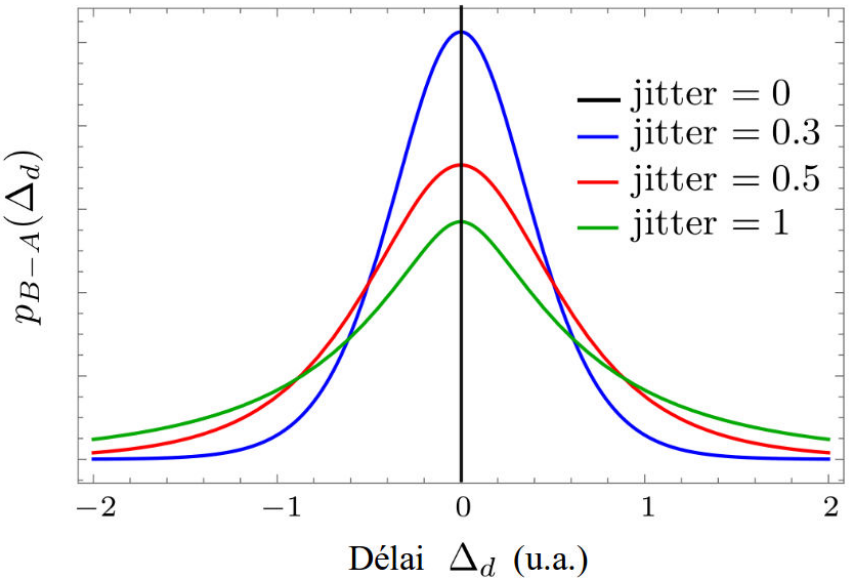


Figure 5.6. – Densité de probabilité du délai dans le cas d'une paire de photons simultanés (c'est-à-dire $|\chi(\bar{t})|^2 = \delta(\bar{t})$) pour différentes gigues temporelles à la détection. Les différentes gigues correspondent à différentes déviations standards de la loi log-normale $\vartheta(\tau)$.

Pour des photons parfaitement simultanés, la distribution temporelle sur la différence des temps d'émission tend vers une distribution de Dirac $|\chi(\bar{t})|^2 = \delta(\bar{t})$ et le délai pour un événement de coïncidence ne dépend alors plus que des propriétés des détecteurs :

$$p_{B-A}(\Delta_d) = \eta^2 \int \vartheta_A(\tau)\vartheta_B(\tau + \Delta_d)\,\mathrm{d}\tau. \tag{5.40}$$

Ce comportement est communément observé dans les expériences où le profil de tout pic de coïncidences (obtenu pour $\Delta_d = 0$) dépend de la gigue temporelle du système

de détection. Ceci est parfaitement illustré en FIGURE 5.6 où la densité de probabilité du délai pour une paire de photons simultanés est calculée pour différentes déviations standards de la gigue temporelle du système de détection dans le cas de deux détecteurs identiques présentant des efficacités parfaites.

5.4.3. Source de photons annoncés

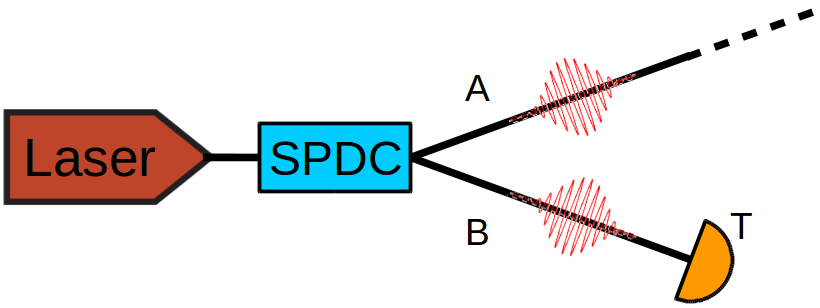


Figure 5.7. – Schéma typique d'une source de photons annoncés. Après génération d'une paire de photons par conversion paramétrique spontanée (SPDC), la présence d'un photon sur la voie A est annoncée au moyen d'un événement de détection au temps T sur la voie B.

En présence d'un état intriqué $\hat{\rho}_{A,B}$ généré par SPDC, où A et B réfèrent toujours aux différents modes spatiaux des photons, on se place désormais dans la configuration où un détecteur placé sur la voie B permet d'annoncer la présence d'un photon sur la voie A. Un tel schéma de détection annoncée est illustré en FIGURE 5.7. L'opérateur densité associé au photon A nous est donné par [293] :

$$\hat{\rho}_A(T) = \frac{\mathrm{Tr}_B\left\{\left[\hat{\mathbb{1}}_A \otimes \hat{\pi}_B(T)\right]\hat{\rho}_{A,B}\right\}}{\mathrm{Tr}\left\{\left[\hat{\mathbb{1}}_A \otimes \hat{\pi}_B(T)\right]\hat{\rho}_{A,B}\right\}}, \tag{5.41}$$

où Tr_B correspond à l'opération de trace partielle sur le sous-système B. À partir des équations (5.30) et (5.33), nous obtenons dans le cas de photons simultanés ($|\chi(\bar{t})|^2 = \delta(\bar{t})$) :

$$\hat{\rho}_A(T) = \frac{\int \vartheta(T-t)|\psi(t)|^2 \,|1_t\rangle\langle 1_t|\,\mathrm{d}t}{\int \vartheta(T-t)|\psi(t)|^2\,\mathrm{d}t}, \tag{5.42}$$

où, comme précédemment, $\psi(t)$ correspond à la distribution temporelle sur le temps d'émission de la paire. Comme le montre l'équation (5.42), l'état annoncé est un mélange statistique représenté par un opérateur densité diagonal. Il n'y a ainsi pas de cohérence entre les différents temps d'arrivée possibles. La dispersion dans le temps du photon est purement statistique. Les différents éléments diagonaux représente la densité

de probabilité associée au temps d'émission du photon annoncé.

La FIGURE 5.8 représente la densité des éléments diagonaux de l'état annoncé en fonction du temps t dans le cas de paires de photons simultanés, et ce pour différentes gigues temporelles. Nous considérons ici que le détecteur émet un signal électronique au temps $T = 0 + \tau$ (c'est-à-dire que le photon se présente au détecteur à l'instant $t = 0$). Dans le cas idéal d'un détecteur sans gigue, on a $\vartheta(\tau) \to \delta(\tau - \tau_m)$, avec τ_m un délai constant à la détection. Comme attendu, l'état annoncé dans ce cas est parfaitement défini et correspond à l'état pur $|1_0\rangle\langle 1_0|$, la matrice densité possède un unique élément non-nul. À l'opposé, dans le cas d'une gigue infinie, c'est-à-dire pour un $\vartheta(\tau)$ infiniment large, aucune information ne peut être extraite de la détection du photon d'annonce et l'état annoncé se trouve alors dans une mixture où les différents états sont tous équiprobables (opérateur identité).

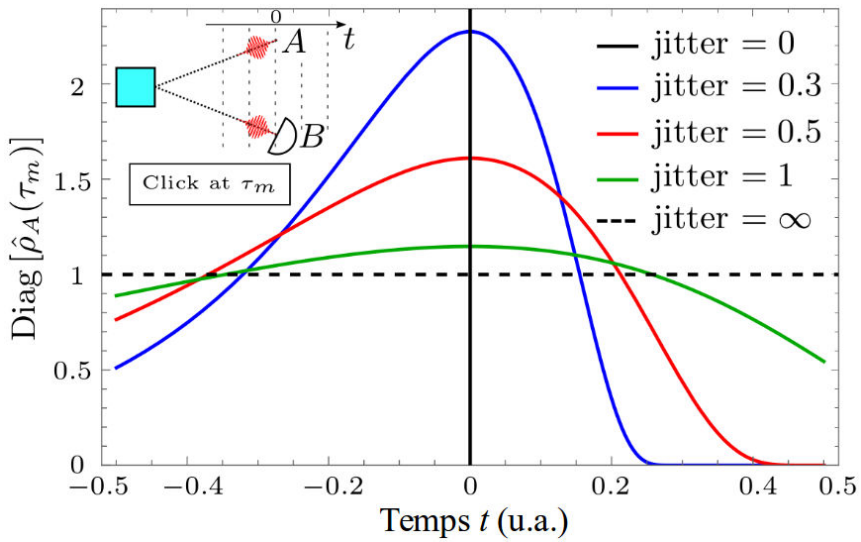


Figure 5.8. – Poids des différents éléments diagonaux de l'opérateur densité $\hat{\rho}_A$ de l'état annoncé. La source considérée ici émet des paires de photons simultanés avec une distribution des différents temps d'émission, $\psi(t)$, équiprobable, centrée en $t = 0$, et de largeur égale à 1. Nous considérons également ici que le détecteur émet un signal électronique au temps $T = 0+\tau_m$, τ_m étant l'instant d'émission du signal électronique le plus probable. La normalisation est telle que l'aire sous chaque courbe est égale à l'unité.

Aussi, dans le cas d'émission multi-paires que nous avions ignoré jusque-là, la pureté de l'état annoncé se retrouve encore davantage dégradé du fait que les détecteurs ON/OFF ne sont pas en capacité de résoudre le nombre de photons se présentant à ces derniers.

5.5. Conclusion

Nous avons présenté un modèle original, reposant sur le formalisme des POVMs, permettant de décrire les caractéristiques d'un détecteur ON/OFF sans négliger les effets de gigue temporelle qui lui sont associés. Bien que nous nous soyons contenté de décrire des situations proposant seulement un ou deux photon(s) en entrée du détecteur, notre approche permet également de décrire sans difficulté majeure des situations impliquant un plus grand nombre de photons. Nous espérons en conséquent que ce travail puisse constituer un outil utile dans le cadre de futurs protocoles de communication quantique ou de génération quantique de nombres aléatoires en régime d'émission ultra-rapide.

Le travail présenté au sein de ce chapitre a récemment été soumis pour publication dans une revue internationale avec comité de lecture.

Chapitre 6.

Conclusion générale

Dans un monde où le paysage technologique est en train d'être révolutionné par les tendances digitales émergentes que sont le big data et l'intelligence artificielle, la demande en matière de puissance de calcul n'a jamais été aussi forte. Pour répondre à ces nouveaux défis, des géants de l'informatique tels que Google, Amazon et Netflix ont mis au point des systèmes de calculs parallèles répondant aux noms de MapReduce, Hadoop, ou encore Spark. Toutefois, le hardware des ordinateurs actuels ne favorise pas le traitement massif d'opérations en parallèle. Pour effectivement dépasser le paradigme de la programmation séquentielle, l'informatique quantique apparaît comme une solution prometteuse. Un calculateur quantique permet de faire des calculs en parallèle grâce, notamment, à la superposition d'états et à l'intrication de systèmes quantiques. Toutefois, en plus d'être très coûteux à fabriquer, les processeurs quantiques restent, dans leur stade de développement actuel, particulièrement sensibles aux effets de décohérence. L'idée serait de pouvoir bénéficier dans le monde de quelques ordinateurs quantiques uniquement, fonctionnant dans des conditions particulières, accessibles en mode hébergé, ou en mode *cloud*, et conçus dans le but de décharger les ordinateurs classiques de la partie la plus difficile de la *data science*, à savoir les algorithmes d'optimisation combinatoire [1].

Les méthodes de chiffrement actuelles reposant sur des problèmes de classe de complexité NP, l'avènement de l'informatique quantique suppose également de repenser intégralement la cybersécurité des systèmes d'information. Dans ce contexte, la cryptographie quantique, qui repose sur le principe d'indétermination de Heisenberg et sur le théorème de non-clonage, pourrait offrir la garantie d'une sécurité inconditionnelle. Bien que certains dispositifs d'établissement quantique de clés secrètes fassent déjà l'objet de commercialisations, de nombreux défis restent encore à relever en vue d'obtenir un réseau quantique de communication reposant sur l'implémentation, hors laboratoire, de liens de cryptographie quantique à haut débit et synchronisés sur de longues distances.

Le travail qui a été présenté au sein de ce manuscrit de thèse s'inscrit dans cette stratégie d'arriver, à terme, à un Internet quantique. Nous avons en effet démontré

1. Problèmes NP-complets

une approche originale au problème de la synchronisation d'un lien relais en régime de variables discrètes, prouvé la faisabilité d'une expérience de génération et de manipulation de lumière comprimée à une longueur d'onde télécom de manière entièrement guidée, et développé un modèle simple pour la description quantique des effets de gigue temporelle dans les systèmes de détection de photons uniques les plus courants.

En écho avec le titre de ce manuscrit, ces travaux représentent des solutions évolutives dans le sens où l'approche suivie est à chaque fois, soit généralisable, soit reconfigurable à la demande. En effet, dans le cas de notre schéma de synchronisation par horloge optique distribuée nous pourrions, sans difficulté conceptuelle supplémentaire, venir synchroniser un plus grand nombre de stations d'émission que celui de deux retenu ici pour fournir une preuve de principe. Les promesses de nouvelles générations de détecteurs de photons uniques avec des gigues temporelles plus faibles nous laissent également entrevoir la perspective de débrider la cadence de l'horloge à un taux de répétition bien supérieur à 2,5 GHz retenu ici. Aussi, dans le cas de notre dispositif entièrement guidé pour le régime de variables continues, on a vu que ce dernier pouvait facilement être reconfiguré de par l'utilisation quasi-exclusive de composants *plug-and-play* issus des télécoms optiques. Enfin, dans le cadre de l'étude faite sur les détecteurs, les expressions obtenues ne pré-supposent aucune restriction sur les états quantiques entrants, ce qui fait de notre approche un outil adaptable à tout type d'expériences reposant sur l'usage de détecteurs ON/OFF.

Annexes

A. Établissement quantique de clés secrètes

Nous avons discuté à la section 1.1.4 que l'établissement de communications sécurisées reposent sur deux fondamentaux de la physique quantique : le principe d'indétermination de Heisenberg et l'impossibilité de cloner des états quantiques inconnus. Ces deux notions sont à l'origine de la faisabilité des protocoles de QKD mais également des preuves de sécurité qui leur sont associées. Dans cette annexe, les principaux protocoles d'établissement quantique de clés secrètes sont décrits en détail. La plupart des protocoles suivent la même structure générale. Nous allons uniquement décrire ici le cas des scénarios bipartites, où deux protagonistes, Alice et Bob, essayent de construire une séquence partagée de bits secrets avec une distribution aléatoire. Cependant, il est important de garder à l'esprit qu'il existe également des schémas de type multi-utilisateurs [303, 304].

A.1. Protocoles à variables discrètes

Les protocoles contiennent au moins une mesure dont les résultats proviennent d'un ensemble discret, ils sont modélisés par le codage de bits classiques dans des états quantiques à dimension finie. Les premiers protocoles présentés ici s'appuient sur la transmission de qubits photoniques (Bennett & Brassard 1984 - BB84, Ekert 1991 - E91, Six-State-Protocol 1998 - SSP, Scarani-Acin-Tibordy-Gisin 2004 - SARG, et Bennett 1992 - B92), tandis que les suivants sont qualifiés de protocoles à référence de phase distribuée (Differential Phase Shift - DPS, et Coherent One Way 2004 - COW).

Bennett & Brassard 1984 - BB84

Proposé en 1984 par Bennett et Brassard, le protocole BB84 fait figure de tout premier protocole d'établissement quantique de clés secrètes [173]. C'est probablement le protocole le plus analysé, non seulement car il a été le premier protocole développé, mais aussi du fait de sa simplicité et de sa symétrie. BB84 a été prouvé comme étant robuste contre tous les types d'attaques autorisées par la physique quantique, à la fois pour des implémentations reposant sur des sources de photons uniques parfaites [305], mais aussi pour des sources de photons émettant des impulsions avec des statistiques dégradées [306].

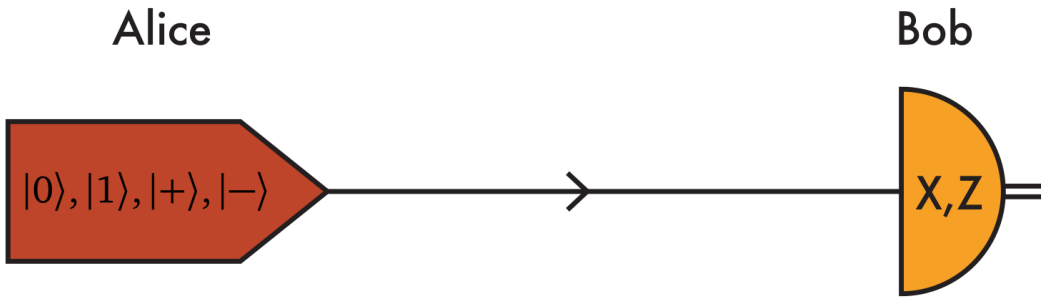


Figure A.1. – Le protocole BB84. Alice prépare l'un des quatre états $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ de manière équiprobable avant d'envoyer l'état à Bob qui éffectue alors une mesure dans la base X ($\{|+\rangle, |-\rangle\}$) ou dans la base Z ($\{|0\rangle, |1\rangle\}$) de manière aléatoire.

Le protocole suit la procédure suivante. Tout d'abord, Alice prépare des qubits en choisissant, de manière aléatoire pour chacun d'entre eux, l'un des quatre états suivant :

$$|0\rangle, \qquad |1\rangle, \qquad |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}, \tag{A.1}$$

et envoie ces qubits à Bob au travers d'un canal quantique non sécurisé, voir FIGURE A.1. Bob sélectionne ensuite, de manière aléatoire, pour chaque qubit qu'il reçoit, l'une des deux bases d'analyse ($\{|0\rangle, |1\rangle\}$) ou $\{|+\rangle, |-\rangle\}$) et analyse chaque qubit en fonction de la base choisie. Ces deux bases sont couramment et respectivement appelées base Z et base X puisqu'elles correspondent respectivement aux vecteurs propres des matrices de Pauli :

$$\hat{\sigma}_Z = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \hat{\sigma}_X = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{A.2}$$

À chaque fois qu'Alice/Bob envoie/mesure l'un des états $|0\rangle$ ou $|+\rangle$ elle/il enregistre un 1 dans une base de données, tandis qu'elle/il enregistre un 0 à chaque fois qu'elle/il envoie/mesure l'un des états $|1\rangle$ ou $|-\rangle$. Ils obtiennent ainsi chacun une séquence de bits que l'on nomme clé brute.

Alice transmet ensuite à Bob via un canal classique authentifié les bases d'encodage qu'elle a utilisées, et Bob fait de même en transmettant à Alice par ce même canal ses choix de bases d'analyses. Alice et Bob éliminent ensuite les bits de leurs clés brutes correspondant à des choix de bases différents. Cette étape, qui consiste à éliminer les bits qui ne peuvent présenter de corrélations puisque associés à des bases incompatibles, se nomme le tamissage (ou plus couramment *sifting* en anglais). Alice et Bob poursuivent ensuite avec les étapes de post-traitement classique présentées en section A.5 à la toute fin de cette annexe.

Ekert 1991 - E91

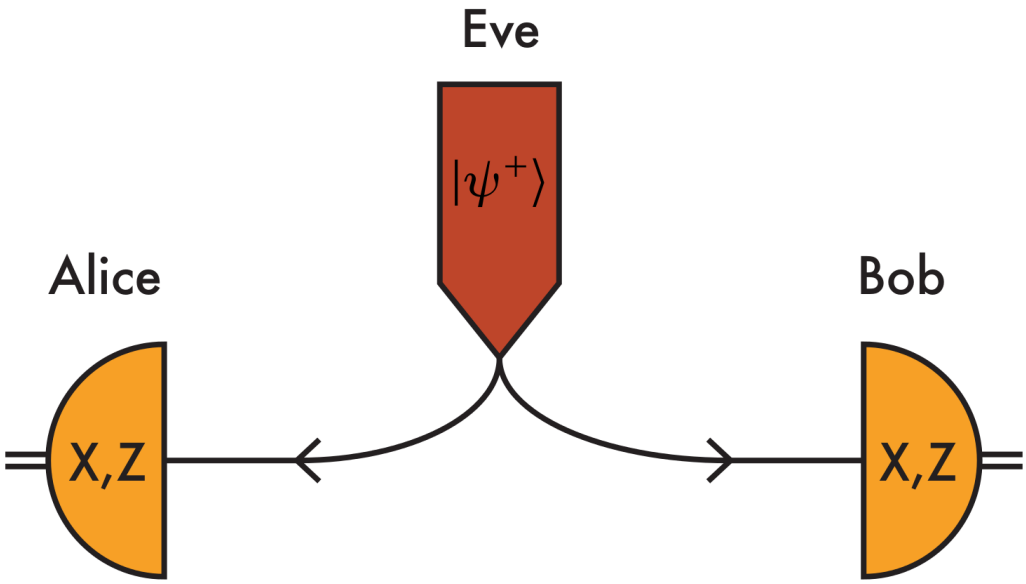


Figure A.2. – Le protocole E91. Eve prépare un état bipartite, idéalement un état maximalement intriqué $|\psi^+\rangle$. Alice et Bob effectuent chacun une mesure sur la partie qui leur a été transmise en choisissant de manière aléatoire la base X ou la base Z.

Le protocole E91 [307] est très similaire au protocole BB84 et lui est même complètement équivalent dans le cas d'un dispositif idéal [308]. Ici nous présentons ce protocole dans une version légèrement différente de celle présentée originellement par Ekert de sorte à faire ressortir l'analogie existant entre ce protocole et le protocole BB84 vu précédemment. Une source non certifiée que l'on nommera Eve prépare des paires de photons dans l'état idéalement maximalement intriqué [5] :

$$|\psi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{A.3}$$

Alice reçoit l'une des deux parties et Bob reçoit la seconde via deux canaux quantiques non sécurisés, voir FIGURE A.2. De manière aléatoire ils choisissent chacun une base d'analyse afin d'effectuer une mesure sur le qubit qu'ils reçoivent, à l'instar de ce que fait Bob dans le protocole BB84 (base Z : $\{|0\rangle, |1\rangle\}$, ou base X : $\{|+\rangle, |-\rangle\}$).

Alice et Bob procèdent ensuite au tamissage, de manière similaire à ce qui a été présenté avec le protocole BB84, suivi des étapes de post-traitement classique, voir section A.5 de cette annexe.

Pour comprendre l'équivalence entre les protocoles BB84 et E91, notons que la génération d'un état $|\psi^+\rangle$ suivit d'une mesure sur l'une des deux parties dans l'une des deux bases $\{|0\rangle, |1\rangle\}$ ou $\{|+\rangle, |-\rangle\}$ projète la deuxième partie dans l'un des quatre états présentés en équation (A.1). Dans le protocole BB84 tel que nous l'avons décrit, Alice choisit directement l'un des quatre états à envoyer, mais elle pourrait tout aussi bien le sélectionner en effectuant une mesure sur un système auxiliaire à quatre dimensions reposant sur des états $|0\rangle, |1\rangle, |2\rangle, |3\rangle$. Écrivons l'état du système auxiliaire d'Alice dans le protocole BB84 comme :

$$\begin{aligned}
&\frac{1}{2}(|0\rangle|0\rangle + |1\rangle|1\rangle + |2\rangle|+\rangle + |3\rangle|-\rangle) \\
&= \frac{1}{2}\left(|0\rangle|0\rangle + |1\rangle|1\rangle + |2\rangle\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) + |3\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\right) \\
&= \frac{1}{2}\left(\left(|0\rangle + \frac{|2\rangle + |3\rangle}{\sqrt{2}}\right)|0\rangle + \left(|1\rangle + \frac{|2\rangle - |3\rangle}{\sqrt{2}}\right)|1\rangle\right) \\
&= \frac{1}{\sqrt{2}}\left(|\tilde{0}\rangle|0\rangle + |\tilde{1}\rangle|0\rangle\right), \qquad \text{(A.4)}
\end{aligned}$$

où $|\tilde{0}\rangle$ et $|\tilde{1}\rangle$ sont des états orthonormaux combinaisons linéaires des vecteurs de la base des états à quatre dimensions d'Alice. Par conséquent, si Alice prépare un état intriqué et effectue une mesure sur une sous-partie de ce dernier, cela revient alors au même que d'avoir une source qui fournie simplement l'un des quatre états de (A.1). Ainsi les protocoles BB84 et E91 sont équivalent si Alice ou Bob reçoivent conjointement l'état maximalement intriqué $|\psi^+\rangle$ et en mesure une sous-partie.

Si Eve prépare l'état bipartite dans le protocole E91, elle aura plus de pouvoir que dans le protocole BB84 étant donné qu'elle peut dans ce dernier modifier uniquement l'état qu'Alice a envoyé à Bob. Le protocole E91 peut donc être vue comme un protocole BB84 où l'on aurait donné plus de pouvoir à Eve. Cette logique se retrouve dans la plupart des protocoles que l'on qualifie de *prepare-and-measure* (PM), tel que le protocole BB84, lorsqu'ils sont transformés en protocoles reposant sur la distribution d'états intriqués tel que le protocole E91, que l'on qualifie habituellement de protocoles de type *entanglement based* (EB).

Le protocole dans sa présentation originelle [307] avait été introduit avec une approche *device-independant*, limitant ainsi considérablement le potentiel d'action d'un espion éventuel, voir section A.3 de cette annexe.

Les variantes du protocole BB84

Il existe de nombreuses variantes du protocole BB84. Deux variantes notables sont le protocole SSP [309] et le protocole SARG [310].

Le protocole SSP est une généralisation directe du protocole BB84 en passant de quatre ($\{|0\rangle, |0\rangle, |+\rangle, |-\rangle\}$) à six états en ajoutant les états :

$$|i\rangle = \frac{(|0\rangle + i\,|1\rangle)}{\sqrt{2}}, \qquad |-i\rangle = \frac{(|0\rangle - i\,|1\rangle)}{\sqrt{2}}, \tag{A.5}$$

qui composent la base Y, puisqu'ils sont les vecteurs propres de la matrice de Pauli :

$$\hat{\sigma}_Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \tag{A.6}$$

L'intérêt du protocole vient du fait qu'il permet plus facilement de détecter un espion puisque ce dernier a désormais plus qu'une chance sur trois de mesurer un qubit dans la bonne base d'analyse, à savoir la même que celle choisie par Alice lors de la préparation du qubit. De manière générale, plus la dimension de l'espace de Hilbert est élevée, plus la sécurité tend à être améliorée [311].

Le protocole SARG a quant à lui été introduit pour parer à une attaque spécifique qu'il est possible d'intenter avec le protocole BB84 dans le cas d'une source imparfaite de photons uniques [312, 313]. Le principe du protocole SARG est essentiellement le même que celui du protocole BB84, excepté le fait que l'on vient ici inverser le rôle des bases et des états. Si Alice envoie un état appartenant à la base Z elle note un 0, et si elle envoie un état appartenant à la base X elle note un 1. Pour Bob les choses sont en revanche moins triviales comme nous l'expliquons ci-après.

Après la phase de transmission des qubits, Alice communique à Bob via un canal classique authentifié l'un des quatre ensemble suivant : $\{|0\rangle, |+\rangle\}$, $\{|0\rangle, |-\rangle\}$, $\{|1\rangle, |+\rangle\}$ et $\{|1\rangle, |-\rangle\}$, en prenant soin parmi ces quatre ensembles de choisir l'un des deux ensembles contenant l'état effectivement transmis. Chaque ensemble étant composé de deux états, Bob peut alors connaître l'état qu'Alice lui avait transmis avec une probabilité de 1/2. Par exemple, si Alice annonce à Bob l'ensemble $\{|0\rangle, |+\rangle\}$ et qu'elle avait transmis l'état $|+\rangle$, alors Bob sait avec certitude, s'il a analysé le qubit dans la base Z et obtenu l'état $|1\rangle$, qu'Alice lui a effectivement transmis l'état $|+\rangle$; il note alors un 1 dans son registre. Alice ayant choisi l'état $|+\rangle$, elle a donc utilisé la base X et avait donc elle aussi noté un 1 dans son registre.

Alice et Bob procèdent ensuite au tamissage comme dans le protocole BB84. Si Bob obtient un résultat de mesure qui n'appartient pas à l'ensemble à deux états annoncé par Alice ou qu'il n'est pas possible de conclure (par exemple si la mesure de Bob a pour résultat $|0\rangle$ dans l'exemple ci-dessus, et que l'ensemble annoncé est l'ensemble $\{|0\rangle, |+\rangle\}$, Bob le fait savoir à Alice et le bit correspondant est éliminé.

Enfin, Alice et Bob effectuent les étapes de post-traitement classique habituelles, voir section A.5 de cette annexe.

Bennett 1992 - B92

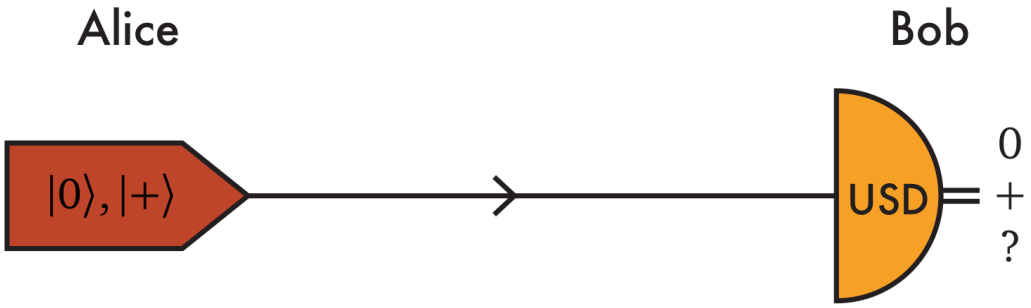


Figure A.3. – Le protocole B92. Alice prépare de manière aléatoire soit l'état $|0\rangle$ soit l'état $|1\rangle$ et Bob procède ensuite à une discrimination non ambiguë entre ces états (*Unambiguous State Discrimination* - USD), voir equation (A.7). Bob obtient comme résultat 0, ou +, ou '?' quand la mesure ne permet pas de conclure.

Le protocole B92 [314] est une autre variante du protocole BB84, il diffère de ce dernier du fait qu'il repose sur la préparation de deux états uniquement : $|0\rangle$ et $|+\rangle$, voir FIGURE A.3. Parfois, d'autres paires d'états non-orthogonaux sont utilisés, mais nous utiliserons ici les deux états que nous venons de mentionner par simplicité. Aussi, dans ce protocole, Bob effectue toujours la même mesure, il n'a donc pas à choisir une base de manière aléatoire. Par conséquent, la phase quantique de transmission n'est ici pas suivie d'un tamissage des résultats.

Bob procède ensuite à une mesure permettant une discrimination non ambiguë, pour cela il a recourt à trois POVM (voir définition d'un élément POVM au chapitre 5) :

$$\hat{F}_0 = \frac{\sqrt{2}}{1+\sqrt{2}} |-\rangle \langle -|, \qquad \hat{F}_1 = \frac{\sqrt{2}}{1+\sqrt{2}} |1\rangle \langle 1|, \qquad \hat{F}_? = \hat{\mathbb{1}} - \hat{F}_0 - \hat{F}_1. \tag{A.7}$$

Avec cette mesure, Bob sait que quand il obtient le résultat 0 Alice n'a alors pas pu lui envoyer l'état $|+\rangle$ étant donné que les états $|+\rangle$ et $|-\rangle$ sont orthogonaux. De manière similaire, quand Bob obtient le résultat 1, Alice n'a alors pas pu lui envoyer l'état $|0\rangle$. Et s'il obtient comme résultat '?', il ne peut tout simplement pas conclure. Les résultats '?' sont importants puisqu'un espion potentiel peut reproduire le même type de mesures que Bob et par conséquent avoir accès aux résultats des mesures de

ce dernier. Cependant, si l'espion effectue les mêmes mesures que Bob, Bob verra alors une augmentation du nombre de '?' dans sa liste de résultats. Alice et Bob mettent alors fin au protocole si le nombre de '?' dépasse alors un certain seuil définit par la preuve de sécurité à laquelle on se réfère pour ce protocole.

Si le taux de '?' reste en dessous d'un certain seuil, Bob révèle ensuite à Alice les emplacements dans son registre correspondants à des '?' de sorte à ce qu'Alice supprime les bits correspondants de sa propre liste. Enfin, Alice et Bob procèdent aux étapes de post-traitement classique, voir section A.5 de cette annexe.

Le protocole B92 a fait l'objet de preuves de sécurité avec un niveau inconditionnel en la présence de photons uniques [315, 316] mais aussi dans le cas de l'utilisation d'impulsions optiques adaptée à la compensation d'une faille de sécurité lié aux pertes à la propagation que pouvait alors exploiter un espion [317, 318].

Differential Phase Shift (2003) - DPS

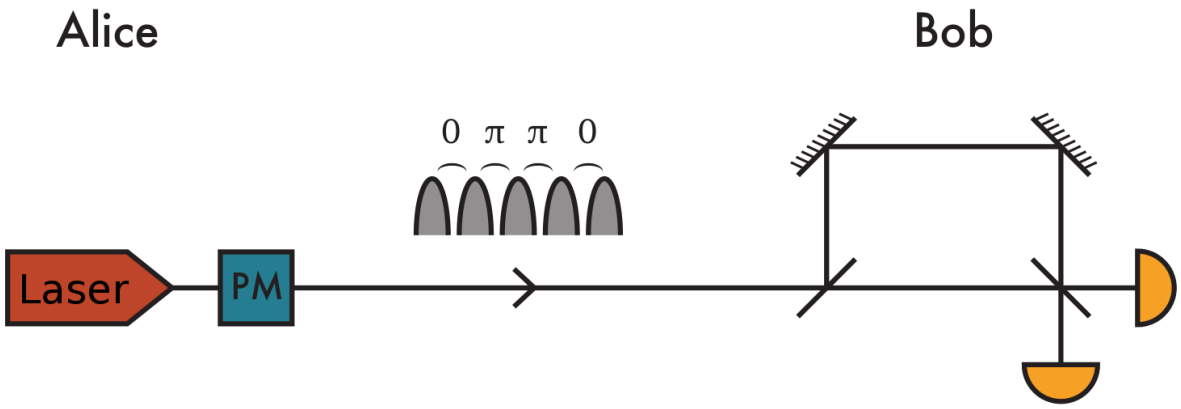


Figure A.4. – Le protocole DPS. Alice produit des états cohérents dont elle module la phase relative à l'aide d'un modulateur de phase (PM). Elle applique une différence de phase entre deux impulsions successives, soit de 0 soit de π. Bob mesure cette différence par le biais d'un interféromètre de Mach-Zehnder déséquilibré, dont le déséquilibre temporel correspond l'écart entre deux impulsions.

Le désavantage majeur des protocoles basés sur la préparation et la mesure de qubits que nous avons précédemment mentionnés réside dans le fait que ces derniers requièrent le choix d'une base de préparation et d'une base d'analyse, soit de manière active comme au travers d'une action opto-électronique (ou mécanique) pilotée par un générateur quantique de nombre aléatoire, soit de manière passive. Le protocole DPS permet de s'affranchir de cette contrainte puisqu'il ne nécessite pas le choix d'une base [319, 320],

c'est donc un protocole qui s'implémente de manière totalement passive de ce point de vue.

Nous présentons ici le protocole dans sa version simplifiée telle que proposée par Inoue et ses collaborateurs [320]. Alice envoie un train d'impulsions cohérentes très atténuées qui sont modulées de manière aléatoire par une phase relative de 0 ou π entre deux impulsions successives. Bob reçoit le signal transmis et fait interférer une impulsion avec la suivante par l'intermédiaire d'un interféromètre de Mach-Zehnder déséquilibré dont le déséquilibre correspond à l'intervalle séparant deux impulsions successives, voir FIGURE A.4. Les photons sont ensuite détectés en fonction de la différence de phase de sorte que le détecteur du haut (ou du bas) clique pour une différence de phase nulle (ou de π). Après la transmission du signal, Bob indique à Alice le temps de détection des photons dans via canal classique. Avec cette information de temps et ses données de modulation de phase, Alice sait quel détecteur a cliqué chez Bob. Alice et Bob obtiennent ainsi des chaînes de bits identiques, un 0 correspondant à une détection sur le détecteur du haut, et un 1 correspondant à une détection sur le détecteur du bas.

La sécurité du protocole DPS est basée sur le fait que des séquences d'impulsions cohérentes de faible intensité avec différentes phases relatives entre impulsions sont utilisées, ces différentes impulsions ne sont pas dans des états orthogonaux et ne peuvent donc pas être parfaitement distinguées par un tiers. Ce protocole ne présente pas une sécurité inconditionnelle, mais de nombreuses attaques ont toutefois été étudiées et contrées [321, 322, 323].

Coherent One-Way (2004) - COW

Un autre protocole qui ne repose pas sur la distribution de qubits mais qui reste malgré tout un protocole en variables discrètes est le coherent one way protocole (COW) [324, 325]. Les états qu'Alice souhaite transmettre sont les suivants :

$$|0_L\rangle_i = |\alpha\rangle_{2i-1} |0\rangle_{2i}, |1_L\rangle_i = |0\rangle_{2i-1} |\alpha\rangle_{2i}, \tag{A.8}$$

où $|0\rangle$ désigne un état de vide quantique, $|\alpha\rangle$ un état cohérent, et où $|0_L\rangle_i$ et $|1_L\rangle_i$ représentent les bits logiques qu'Alice souhaite transmettre, 0 et 1, pour le signal numéro i. Alice envoie donc deux impulsions par bit, voir FIGURE A.5. Notons également que les états $|0_L\rangle_i$ et $|1_L\rangle_i$ ne sont pas orthogonaux étant donné qu'un état cohérent contient une composante de vide.

De manière à pouvoir contrer un espion, Alice a également recourt à un autre type d'états, états qui ne seront pas utilisés par Alice et Bob pour former leurs clés mais qui auront pour seul usage de permettre la détection d'un espion potentiel. Alice prépare ainsi, avec une probabilité q, des états leurres (*decoy states*) qui occupent eux aussi deux intervalles temporels :

$$|\text{decoy}\rangle_i = |\alpha\rangle_{2i-1} |\alpha\rangle_{2i} , \tag{A.9}$$

tandis-qu'elle prépare avec une probabilité 1-q des états $|0_L\rangle_i$ et $|1_L\rangle_i$ de manière aléatoire.

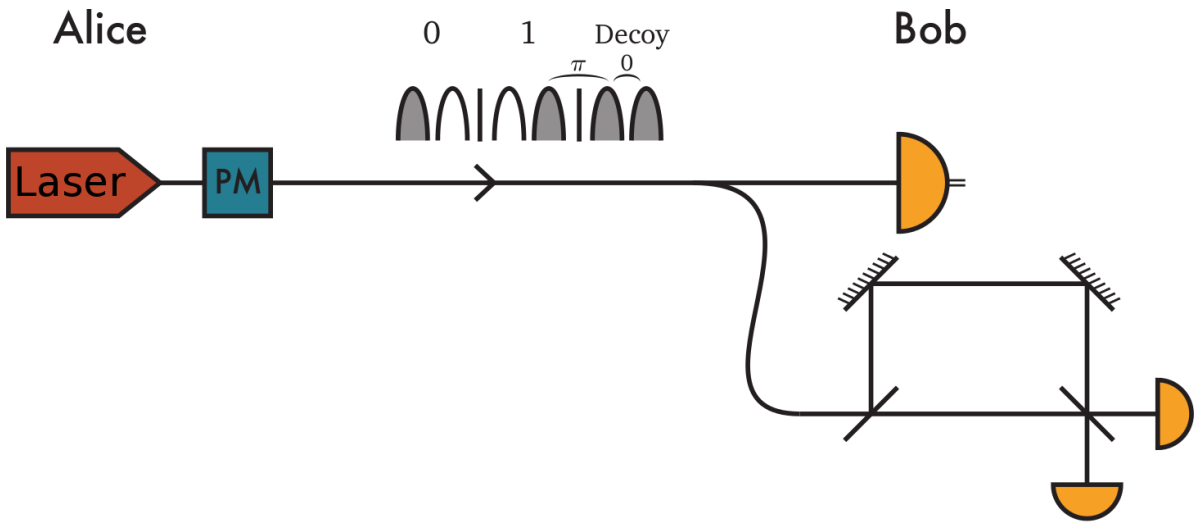


Figure A.5. – Le protocole COW. Alice prépare l'un des trois états suivant : un état cohérent suivi d'une composante de vide (0), une composante de vide suivie d'un état cohérent (1), ou un état leurre, à savoir deux états cohérents placés de manière successive. Alice module la phase relative entre les différents états cohérents à l'aide d'un modulateur de phase (PM). Bob choisit, de manière aléatoire, soit de mesurer le temps d'arrivée, soit de mesurer par l'intermédiaire d'un interféromètre de Mach-Zehnder déséquilibré la phase relative entre impulsions successives. Il peut mesurer une phase relative entre les deux impulsions d'un état leurres, entre un 1 suivi d'un état leurre, entre un état leurre suivi d'un 0, ou entre un 1 suivi d'un 0.

La mesure de Bob se décompose en deux parties. Avec un probabilité p il mesure la présence de photons dans chaque impulsion. Cette mesure lui permet de savoir si Alice a essayé de lui transmettre un 0 ou un 1. Avec une probabilité 1-p il effectue une mesure d'interférence entre impulsions successives à l'aide d'un interféromètre de Mach-Zehnder déséquilibré comme dans le protocole DPS. Cet interféromètre permet de mesurer la phase relative entre impulsions successives. En d'autres termes, Bob peut mesurer la phase relative entre les deux impulsions d'un état leurre, entre un état $|1\rangle_L$ suivi d'un état leurre, entre un état leurre suivi d'un $|0\rangle_L$, ou entre un état $|1\rangle_L$ suivi d'un état $|0\rangle_L$. Or, un espion potentiel ne peut pas mesurer de manière cohérente à la fois un état $|0\rangle_L$ et un état $|1\rangle_L$ sans perturber un état leurre [324]. Par conséquent, l'interféromètre est utilisé pour estimer de manière continue le taux d'erreurs lors de la

transmission afin de détecter la présence d'un potentiel espion.

Alice et Bob procèdent à un tamissage de leurs séquences de bits durant lequel Alice communique via un canal public authentifié l'emplacement des états leurres afin que Bob retire de son registre les bits correspondants. Bob communique également à Alice quel détecteur a détecté un signal en sortie du Mach-Zehnder pour chaque intervalle temporel afin de pouvoir estimer le taux d'erreurs. Alice et Bob poursuivent ensuite avec les étapes de post-traitement classique habituelles, voir A.5.

A.2. Protocoles à variables continues

Bien que les protocoles en variables discrètes soient les plus couramment utilisés de part leur simplicité, ces derniers nécessitent l'usage de détecteurs dédiés au régime de photons uniques pour les phases de détection. Or, de tels détecteurs présentent en général des efficacités aux longueurs d'onde des télécommunications, des niveaux de bruits, ou encore des temps de réponse qui limitent fortement les taux d'établissement de clés secrètes. Il existe cependant une classe de protocoles différents, dans laquelle les informations sont véhiculées par des degrés de libertés cette fois-ci continus, tels que les valeurs des composantes en quadrature d'un état cohérent. L'utilisation de telles observables aux spectres continus comme porteur de l'information quantique constitue une alternative aux limitations des protocoles en variables discrètes. D'un point de vue pratique, par exemple, les protocoles d'établissement quantique de clés secrètes en régime de variables continues présentent l'avantage majeur de reposer uniquement sur des composants issus de la technologie des télécommunications optiques standard. Notamment, plutôt que d'utiliser des détecteurs de photons uniques, on a ici recours à des photodiodes standards pour permettre la détection homodyne ou hétérodyne des signaux lumineux.

Un certain nombre de protocoles reposant sur des variables continues ont été proposés dans la littérature et dépendent du choix des états qui sont préparés : états cohérents [326, 327, 328] ou comprimés [329, 330, 331] ; du choix de la modulation : gaussienne [326, 327, 328, 329, 330, 331] ou non gaussienne [332, 333] ; du choix de la détection : homodyne [326, 328, 329, 331] ou hétérodyne [327, 330]. Bien sûr, certains de ces protocoles sont plus faciles à mettre en œuvre et certains ont de meilleures preuves de sécurité que d'autres. Dans cette annexe, nous décrirons uniquement les plus simples, qui sont aussi les mieux compris, à savoir les protocoles utilisant une modulation gaussienne. D'autres protocoles avec une modulation non gaussienne existent, comme nous l'avons mentionné, mais nous ne les présenterons pas ici car leur analyse de sécurité est moins avancée.

Comme en variables discrètes, un protocole donné peut être mis en œuvre selon deux méthodes possibles, à savoir *prepare-and-measure* (PM) ou *entanglement-based*

(EB). Ces deux méthodes sont équivalentes dans le cas des protocoles gaussiens. Plus précisément, la sécurité de la version PM se réduit à celle du protocole EB. Pour cette raison, il suffit donc d'analyser la sécurité des protocoles EB. Par ailleurs, les mises en oeuvre experimentales, sont généralement plus simples pour les protocoles PM. Le protocole d'établissement quantique de clé secrète en variables continues le plus simple est certainement le protocol GG02 introduit par Grosshans et Grangier en 2002 [326], ou sa variante reposant sur un schéma de détection hétérodyne [327]. Le protocole se compose des étapes habituelles : distribution, mesure de l'état et étapes de post-traitement classique.

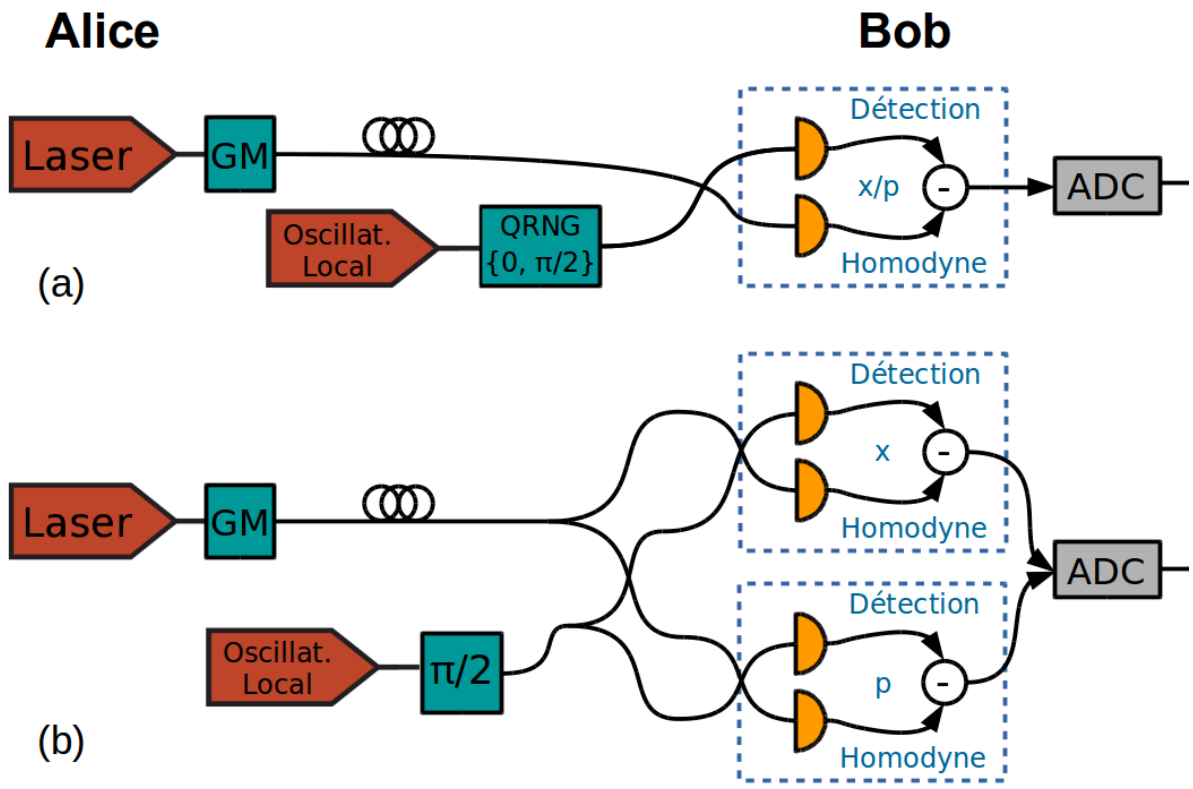


Figure A.6. – Distinctions entre le protocole GG02 lorsqu'il est mis en œuvre avec un système de détection homodyne (a), ou un système de détection hétérodyne (b). Dans le premier cas, un générateur quantique de nombres aléatoires (*Quantum Random Number Generator* - QRNG) est utilisé pour sélectionner la phase de l'oscillateur local : 0 ou $\pi/2$, pour mesurer respectivement x ou p. Dans le cas de la détection hétérodyne, le signal est divisé en utilisant un coupleur 50 :50. Un bras est utilisé pour mesurer x, l'autre - après un changement de phase de $\pi/2$ sur l'oscillateur local- pour mesurer p. La clé est ensuite obtenue dans les deux cas en utilisant un convertisseur analogique-numérique (*Analog to Digital Converter* - ADC).

Dans un scénario de modulation gaussienne (*Gaussian Modulation* - GM), Alice prépare des états cohérents déplacés, voir 2.3.2, avec des composantes en quadrature x et p qui sont les réalisations de deux variables gaussiennes complexes aléatoires X et P, indépendantes et identiquement distribués. Les variables aléatoires X et P obéissent à la même répartition normale centrée en zéro :

$$X \backsim P \backsim \mathcal{N}(0, V_{mod}) \tag{A.10}$$

où V_{mod} est la variance de la modulation. Alice prépare une séquence $|\alpha_1\rangle, ..., |\alpha_j\rangle, ..., |\alpha_N\rangle$ d'états cohérents déplacés :

$$|\alpha_j\rangle = |x_j + ip_j\rangle, \tag{A.11}$$

obéissant à l'équation aux valeurs propres habituelle :

$$\hat{a}\,|\alpha_j\rangle = \alpha_j\,|\alpha_j\rangle, \tag{A.12}$$

$$\frac{1}{2}(\hat{x} + i\hat{p})\,|\alpha_j\rangle = (x_j + ip_j)\,|\alpha_j\rangle. \tag{A.13}$$

Selon le protocole (homodyne ou hétérodyne), voir FIGURE A.6, Bob mesure soit une quadrature aléatoire (x ou p) pour chaque état et informe Alice de ses choix, soit les deux quadratures. Bob obtient alors une liste de N ou $2N$ nombres réels correspondant à ses résultats de mesure. Alice dispose également de sa propre liste de données (elle conserve uniquement les valeurs de la quadrature pertinente si Bob a effectué une détection homodyne). Alice et Bob procèdent ensuite aux étapes de post-traitement classique, voir A.5.

A.3. Protocoles Device-Independent - DI-QKD

Les protocoles d'établissement quantique de clés secrètes que nous avons présentés, ainsi que les preuves de sécurité qui leurs sont associées, semblent offrir la garantie d'une sécurité inconditionnelle. Cependant, les mises en œuvre pratiques de ces protocoles impliquent nécessairement des dispositifs imparfaits, et il a vite été compris que ces imperfections pourraient être exploitées par un tiers malveillant afin de briser la sécurité inconditionnelle garantie par les lois de la physique quantique [334].

Mayers et Yao ont présenté en 1998 [335] une évolution pour restaurer la sécurité inconditionnelle en présence de dispositifs imparfaits ou même 'malveillants' en cherchant à établir la sécurité d'un protocole d'établissement quantique de clés secrètes en se basant uniquement sur la validité de la physique quantique, à savoir l'isolement physique des dispositifs et le passage de certains tests statistiques. Ce nouveau champ de recherche porte le nom de *Device Independent Quantum Key Distribution* (DI-QKD). L'idée que la sécurité d'un protocole doit être indépendante du dispostif était déjà présente dans

la proposition originelle du protocole E91 [307] qui préconisait des tests basés sur la violation des inégalités de Bell, et a été plus explicitement discutée en 2005 par Barrett, Hardy et Kent dans une publication présentant comment générer des bits aléatoires avec un tel niveau de sécurité [336]. De nombreux autres travaux ont suivi, le lecteur intéressé pourra consulter la référence [337]. Tous ces développements, cependant, ne peuvent être transcrits expérimentalement que sous des hypothèses d'indépendance très restrictive rendant une telle approche inexploitable à ce jour.

A.4. Protocoles Measurement-Device-Independent - MDI-QKD

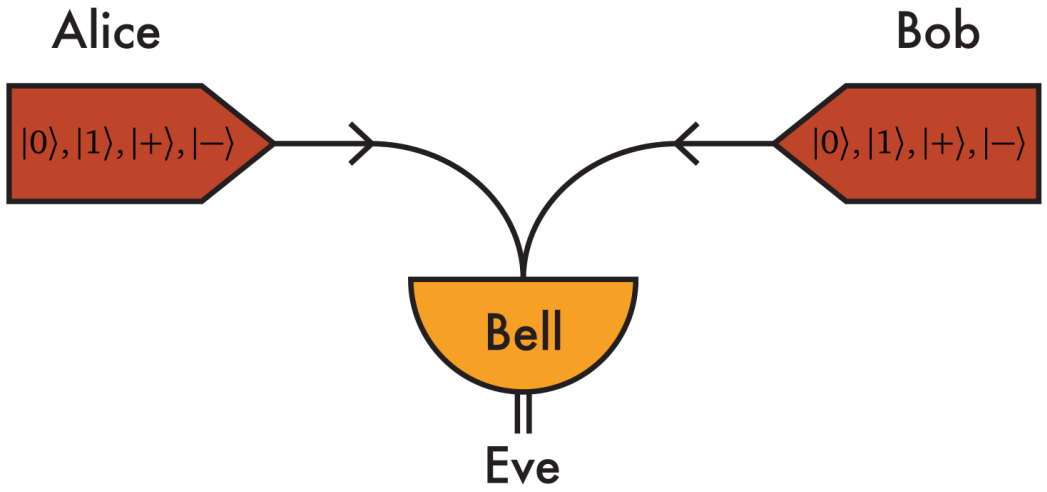


Figure A.7. – Alice et Bob préparent de manière aléatoire l'un des quatres états du protocole BB84 ($\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$). Eve mesure ces états en effectuant une mesure dans la base de Bell. Eve communique ensuite le résultat de la mesure à Alice et Bob.

L'établissement quantique de clés secrètes indépendante du dispositif de mesure (MDI-QKD) représente une alternative hybride des scenarii dépendant et indépendant du dispositif. L'avantage de l'utilisation de ces protocoles est qu'ils sont indépendants du système de détection, ce qui évite de nombreuses hypothèses qui sont généralement nécessaires pour prouver la sécurité. Le scénario MDI présente un autre avantage par rapport aux protocoles traditionnels puisqu'il permet également d'accroître les distances qui séparent les partenaires d'un lien de cryptographie quantique.

Il existe deux protocoles MDI en variables discrètes [338, 339], le second étant la version avec intrication du premier, de la même manière que le protocole BB84 est

équivalent au protocole E91 dans le cas d'un dispositif idéal.

Dans le protocole de type PM [338], Alice et Bob prépare chacun de manière aléatoire l'un des quatre états du protocole BB84, voir FIGURE A.7. Ils envoient ensuite chacun leur état à Eve, un tiers auquel ils ne font pas confiance. Eve effectue alors une mesure jointe des états d'Alice et de Bob dans la base de Bell $\{|\psi^+\rangle, |\psi^-\rangle, |\phi^+\rangle, |\phi^-\rangle\}$ [5], définie comme :

$$|\psi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \quad |\psi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \quad |\phi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \quad |\phi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \tag{A.14}$$

Eve annonce alors à Alice et à Bob le résultat de sa mesure. Alice et Bob annoncent à leur tour les bases qu'ils ont utilisé, et procèdent alors à un tamissage afin d'écarter les résultats pour lesquels ils n'ont pas choisi des bases identiques. De la même manière que dans BB84, Alice et Bob associent des valeurs binaires aux différents états lors de la préparation. Selon le résultat annoncée par Eve, Alice (ou Bob de manière équivalente) doit alors éventuellement modifier dans son registre la valeur du bit correspondant à son état préparé. Par exemple, si Eve annonce le résultat $|\phi^+\rangle$ et qu'Alice et Bob ont préparé leurs états dans la base Z, Alice (ou Bob de manière équivalente) doit alors modifier la valeur de son bit. Un autre exemple, si Alice et Bob ont préparé leurs états dans la base Z et que Eve annonce l'état $|\psi^+\rangle$ alors aucune opération sur le bit d'Alice (ou Bob de manière équivalente) n'est nécessaire.

Notons également qu'Eve ne peut pas déterminer la valeur des bits d'Alice et Bob. En effet, bien qu'elle connaisse la base de préparation des états d'Alice et Bob et le résultat de la mesure de Bell, elle sait uniquement qu'Alice et Bob possèdent le même bit sans pour autant connaître sa valeur.

Le protocole MDI de type EB est similaire à ce qui vient d'être présenté excepté qu'Alice et Bob préparent cette fois-ci une copie de l'état $|\psi^+\rangle$ [339]. Alice et Bob effectuent une mesure identique à celle du protocole BB84 sur une composante de l'état et envoient la seconde composante à Eve pour qu'elle effectue une mesure de Bell. Le reste du protocole suit alors les mêmes étapes que dans la version PM.

Les deux protocoles discutés font l'objet de preuves de sécurité [338, 339]. Des protocoles similaires existent également avec des variables continues [340, 341, 342, 343], ainsi que des variantes avec respectivement une source de qubits non caractérisée [344, 345], des états leurres [346], des sources laser à taux de répétition allant jusqu'au GHz [347], un schéma de répéteur quantique pour étendre la distance d'échange [348, 349], ou encore une version reposant sur la violation d'inégalités Bell [350, 346]. De nombreux développements expérimentaux ont également vu le jour [351, 352, 353, 354].

A.5. Post-traitement classique

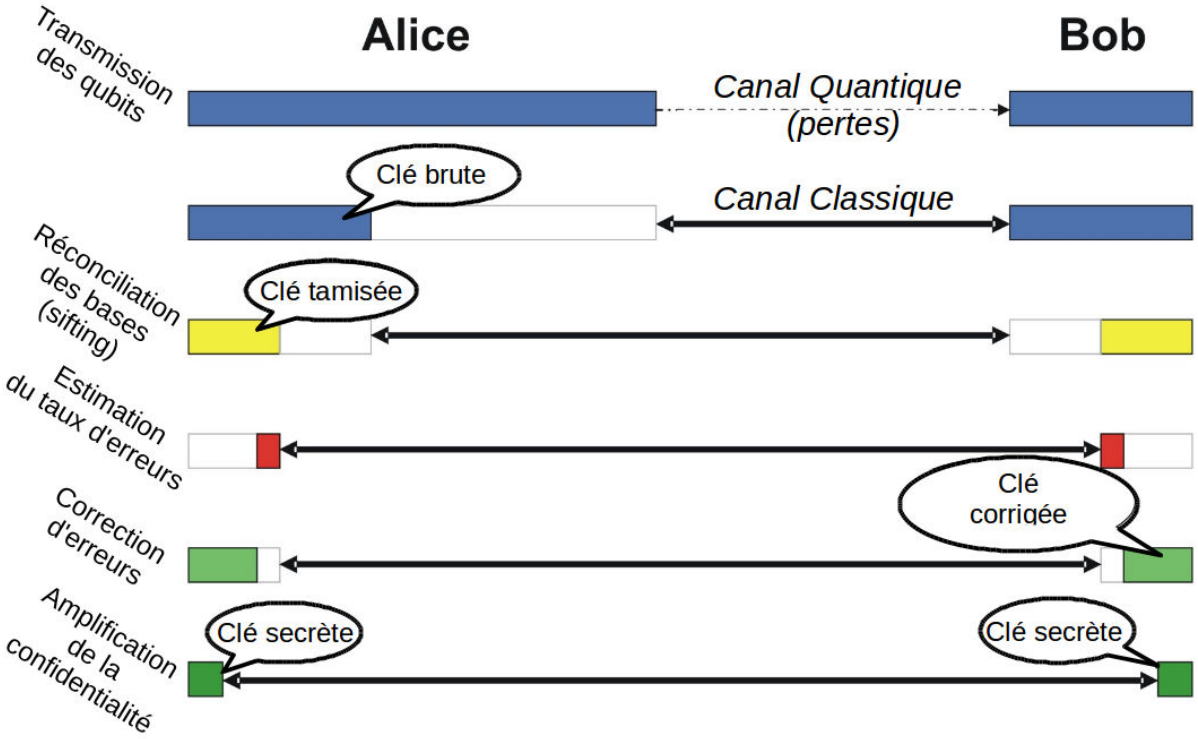


Figure A.8. – Schéma du processus de transmission quantique et de distillation d'une clé secrète.

La phase de post-traitement classique aussi nommée phase de distillation [168], au cours de laquelle Alice et Bob communiquent au travers d'un canal de communication publique authentifié, se décompose généralement en trois étapes successives, voir FIGURE A.8, à savoir : l'estimation des paramètres, la réconciliation de l'information, et l'amplification de la confidentialité :

- **Estimation des paramètres** - Alice et Bob évaluent tout d'abord le niveau d'erreurs et de bruit séparant leurs deux ensembles de données. Pour cela, Alice et Bob comparent un échantillon statistiques de leur résultats pour estimer le taux d'erreur global en supposant l'erreur uniformément répartie. Si ce taux d'erreur ne dépasse pas la limite autorisée par la preuve de sécurité, on conserve alors uniquement les bits n'ayant pas servi à l'estimation des erreurs (les autres ayant désormais été rendu publiques) en vue de la phase de réconciliation.

- **Réconciliation de l'information** - Durant la phase de réconciliation, Alice

et Bob procèdent à la correction des erreurs entre leurs deux séquences de bits aléatoires. De nombreux codes correcteurs d'erreurs ont été développés pour les communications classiques et peuvent ici être utilisés. Le protocole Casade couramment utilisé permet de remonter à l'emplacement d'une erreur en comparant tout d'abord la parité d'une séquence de bits successifs, avant de reproduire ensuite l'opération sur un sous-échantillon et ainsi de suite jusqu'à remonter à l'emplacement exact de l'erreur qui peut alors être éliminée. Un nombre pair d'erreurs pouvant appartenir à la même séquence, il est important de reproduire l'algorithme quelques fois en redistribuant la séquence de bits afin d'être certain de ne louper aucune erreur.

- **Amplification de la confidentialité** - Cette dernière étape a pour objectif de réduire au maximum l'information qu'un espion aurait pu glaner durant la phase de transmission quantique et l'étape classique de réconciliation. Un exemple simple d'amplification de la confidentialité consiste pour Alice et Bob à choisir de manière concertée deux bits successifs de leur clé et de les remplacer par leur somme modulo deux, ce qui n'introduit aucune erreur supplémentaire mais qui pour l'espion, s'il ne connaissait que l'un des deux bits initiaux, correspond à une perte d'information.

B. Caractérisation de photons uniques par interférence à deux photons

Nous avons traité à la section 2.4.3 l'interference à deux photons selon une approche mathématique consistant à décrire les champs par des ondes planes stationnaires et à 'brancher' et 'débrancher' le couplage de la lame pendant un intervalle de temps correspondant à la durée réelle des impulsions. Bien que cette approche permette d'arriver très simplement à une expression du taux de coïncidences, elle ne permet en revanche pas d'appréhender pleinement l'influence des différentes propriétés spatio-temporelles des photons dont il nous faut tenir compte dans une expérience réelle. Dans cette annexe, nous représentons le processus comme une collision de deux paquets d'onde mélangés par la lame en traitant rigoureusement chaque paquet d'onde comme une superposition de modes.

B.1. Champ optique à un photon

Le traitement quantique d'un champ optique au sein d'une cavité cubique de côté L et de volume V a été largement détaillé à la section 2.1. Le champ électromagnétique à l'intérieur de la cavité est soumis à des conditions aux limites conduisant à une distribution discrète des modes du champ. Chaque mode peut être labellisé par un indice k et est caractérisé par sa fréquence ω. Les fréquences propres sont séparées d'un intervalle $\Delta\omega = 2\pi c/L$. Il résulte de la quantification du champ un ensemble discret de niveaux d'énergie, $E_n = \hbar\omega(n + 1/2)$, auxquels sont associés les opérateurs création et annihilation $\hat{a}_k^\dagger$ et $\hat{a}_k$. Rappelons également que les vecteurs propres sont donnés par :

$$|n\rangle = \frac{\left(\hat{a}_k^\dagger\right)^n}{\sqrt{n!}} |0\rangle \,. \tag{B.1}$$

À la limite $L \to \infty$ et $\Delta\omega \to 0$, les modes constitutifs du spectre tendent vers un ensemble continu. Pour décrire cette situation, nous introduisons des opérateurs $\hat{a}^\dagger(\omega)$ et $\hat{a}(\omega)$ intégrant cette notion :

$$\hat{a}_k^\dagger \to \hat{a}^\dagger(\omega). \tag{B.2}$$

Ces opérateurs créent et annihilent des photons correspondant à des ondes monochromatiques dans l'espace libre à la fréquence ω. Ces ondes d'extension spatiale infinie n'ont ni 'commencement' ni 'fin', ce sont des ondes planes. Cependant, les photons générés en laboratoire sont caractérisés par une certaine largeur spectrale et par une extension spatiale finie. Par conséquent, il nous faut définir des opérateurs qui permettent de créer ou d'annihiler des photons avec une certaine largeur spectrale, ou en d'autres termes, avec une extension spatio-temporelle bien déterminée.

Modes fréquentiels

Nous décrivons ici des modes correspondant à une distribution fréquentielle donnée. Ces modes représentent des paquets d'ondes se propageant à la vitesse de la lumière c à travers le vide, avec une largeur spectrale κ permettant de remonter à la durée temporelle du paquet d'onde δt. Une distribution fréquentielle se caractérise par une fonction complexe normalisée $\chi(\omega)$. Les opérateurs $\hat{a}^\dagger(\omega)$ et $\hat{a}(\omega)$ peuvent alors être utilisés pour définir un nouvel ensemble d'opérateurs création et annihilation de photons dans ces nouveaux modes :

$$\hat{b}_\chi^\dagger = \int \chi(\omega)\hat{a}^\dagger(\omega)\,\mathrm{d}\omega. \tag{B.3}$$

La fonction $\chi(\omega)$ se décompose comme le produit d'une amplitude réelle, $\varepsilon(\omega)$, et d'un terme de phase complexe $e^{-i\Phi(\omega)}$. Le terme de phase tient compte de l'instant d'émission τ_0 du paquet d'onde et de sa propagation. Nous nous limiterons dans la suite au cas de paquets d'ondes gaussiens centrés en ω_0. La distribution s'écrit alors :

$$\chi(\omega) = \sqrt[4]{\frac{2}{\pi\kappa^2}}\; e^{-\dfrac{(\omega-\omega_0)^2}{\kappa^2}}\; e^{-i\omega\left(\tau_0+\dfrac{z}{c}\right)}, \tag{B.4}$$

où z représente la position du paquet d'onde et c la vitesse de la lumière. Pour une source idéale de photons uniques produisant toujours des photons identiques le champ optique généré est alors décrit par l'application de $\hat{b}_\chi^\dagger$ sur le vide :

$$|1_\chi\rangle = \hat{b}_\chi^\dagger\,|0\rangle\,. \tag{B.5}$$

En pratique cependant de telles sources sont difficiles à fabriquer. En général le procédé de génération ne peut pas être parfaitement contrôlé et la fonction $\chi(\omega)$ est par conséquent soumis à de faibles variations. Pour prendre en compte ces variations, le champ optique doit alors être décrit par un opérateur densité :

$$\hat{\rho} = \int f(\vartheta)\,|1_{\chi(\vartheta)}\rangle\,\langle 1_{\chi(\vartheta)}|\,\mathrm{d}\vartheta. \tag{B.6}$$

Ici, nous faisons l'hypothèse que la source produit des photons uniques avec une distribution de fréquence gaussienne et que le paramètre de cette distribution est soumis à de petites variations décrites par la fonction de distribution $f(\vartheta)$. Le paramètre ϑ correspond soit à la fréquence centrale ω_0, à la largeur spectrale κ ou au temps d'émission τ_0 des photons, soit à une combinaison de ces différents paramètres.

Modes spatio-temporels

En utilisant le théorème de Fourier, il est possible d'assigner à chaque mode avec une certaine distribution de fréquence $\chi(\omega)$ un paquet d'onde temporel se propageant à

travers l'espace. À chaque mode de distribution en fréquence gaussienne donnée par (B.4) correspond par conséquent un mode spatio-temporel $\xi(t - z/c)$ au profil gaussien. En définissant $q := t - z/c$, ce mode est donné par la fonction :

$$\xi(q) = \sqrt[4]{\frac{2}{\pi(\delta t)^2}}\; e^{-\frac{q^2}{(\delta t)^2}}\; e^{i\omega_0(\tau_0 - q)} \equiv \epsilon(q)\; e^{i\omega_0(\tau_0 - q)}. \tag{B.7}$$

La durée δt de ce paquet d'onde gaussien est donnée par l'inverse de la largeur spectrale, $\delta t = 2/\kappa$. Il est également possible de construire par transformée de Fourier des opérateurs création et annihilation associés à ces modes spatio-temporels :

$$\hat{a}^\dagger(q) = \frac{1}{\sqrt{2\pi}} \int \hat{a}^\dagger(\omega)\; e^{-i\omega q}\, \mathrm{d}\omega, \qquad \hat{a}(q) = \frac{1}{\sqrt{2\pi}} \int \hat{a}(\omega)\; e^{i\omega q}\, \mathrm{d}\omega. \tag{B.8}$$

On associe à ces nouveaux opérateurs création et annihilation l'opérateur nombre de photons par unité de temps (taux de photons) $\hat{a}^\dagger(q)\hat{a}(q)$ qui nous sera utile pour évaluer la détection des photons uniques dans un mode donné.

Par analogie avec l'équation (B.3), les opérateurs obtenus par transformée de Fourier peuvent être utilisés pour définir la création et l'annihilation de photons dans le mode spatio-temporel $\xi(q)$:

$$\hat{c}_\xi^\dagger = \int \xi(q)\hat{a}^\dagger(q)\, \mathrm{d}q. \tag{B.9}$$

Pour prendre en compte les fluctuations, on peut à nouveau écrire l'opérateur densité du champ optique comme on l'a fait en (B.6) mais en utilisant désormais des modes spatio-temporels. Dans ce cas ϑ correspond à ω_0, δt and τ_0.

Détection

On se place ici dans la base des modes spatio-temporels afin de décrire la détection de photons uniques au travers d'un détecteur d'efficacité η placé en $z = 0$. La réponse du détecteur sur un intervalle temporel $\mathrm{d}t_0$ centré en t_0 est donnée par la valeur moyenne de l'opérateur taux de photons :

$$P^{(1)}(t_0) = \eta \int_{t_0 - \mathrm{d}t_0/2}^{t_0 + \mathrm{d}t_0/2} \mathrm{Tr}\left\{\hat{\rho}\hat{a}^\dagger(t)\hat{a}(t)\right\}\, \mathrm{d}t, \tag{B.10}$$

où $\hat{\rho}$ représente l'opérateur densité de l'état entrant. Dans le cas de paquets d'ondes associés à des photons uniques, la fonction $P^{(1)}(t_0)$ correspond à la probabilité de détecter un photon durant l'intervalle temporel considéré. En pratique, la valeur minimale que peut prendre $\mathrm{d}t_0$ est donné par la résolution temporelle du détecteur T, soit $\mathrm{d}t_0 \geq T$. Si la durée du paquet d'onde est bien supérieure à la résolution du détecteur, $\delta t \gg T$ et $\mathrm{d}t_0 = T$, l'équation (B.10) se simplifie et on a alors :

$$P^{(1)}(t_0) = \eta T \,\mathrm{Tr}\left\{\hat{\rho}\hat{a}^\dagger(t_0)\hat{a}(t_0)\right\}. \tag{B.11}$$

La mesure de la probabilité de détection requiert un large ensemble de photons uniques. Dans la suite nous considérons un flux périodique de photons uniques émis les uns après les autres, de sorte à ce que les photons soient bien détectés un à un. Si tous les photons sont identiques, le champ lumineux est simplement décrit par le vecteur $|1_\xi\rangle$ et l'opérateur densité $\hat{\rho} = |1_\xi\rangle\langle 1_\xi|$ avec $|1_\xi\rangle = \hat{c}_\xi^\dagger|0\rangle$. Dans ce cas particulier, la probabilité moyenne de détection de l'ensemble des photons est donnée par la norme au carré de la fonction $\xi(q)$, qui est identique pour chaque paquet d'onde :

$$P^{(1)}(t_0) = \eta T \,|\xi(t_0)|^2 = \eta T \epsilon^2(t_0), \tag{B.12}$$

avec $\epsilon(t_0)$ défini comme en (B.7). Comme discuté précédemment, les propriétés des photons peuvent différer de l'un à l'autre, auquel cas l'opérateur densité est alors donné par (B.6). La probabilité moyenne de détection est alors donnée par :

$$P^{(1)}(t_0) = \eta T \int f(\vartheta)\epsilon^2(t_0,\vartheta)\,\mathrm{d}\vartheta. \tag{B.13}$$

Pour obtenir cette équation, nous avons tenus compte du fait, que dans nos conditions, trace et intégration sont des opérations interchangeables. De manière évidente, la probabilité de détection pour l'ensemble des photons diffère de celle associée à un photon unique. La probabilité de détection moyenne est en général affectée par la variation, décrite par $f(\vartheta)$, des paramètres de la fonction $\xi(t)$. Par conséquent, on observe ici uniquement l'enveloppe temporelle de l'ensemble de des photons. Cependant, l'effet de chaque paramètre sur $P^{(1)}(t_0)$ peut être très différent. Une variation de la fréquence centrale, par exemple, n'affecte pas l'amplitude réelle de $\xi(t)$. Pour un tel cas, $P^{(1)}(t_0)$ peut simplement être décrite par (B.12), ce qui n'est pas le cas pour une variation des autres paramètres.

B.2. Interférence à deux photons

On considère désormais le cas de l'interférence à deux photons introduit à la section 2.4.3, avec dans chaque port d'entrée de la lame séparatrice équilibrée des impulsions gaussienne à un photon, on s'intéresse de nouveau au taux de coïncidences en sortie de la lame. Comme nous l'avions montré, dans le cas de photons parfaitement identiques, la probabilité de détection jointe est alors nulle. Pour illustrer cet effet de coalescence avec le formalisme introduit dans cette annexe, nous considérons que l'état de chaque photon dans chacun des modes d'entrée de la lame séparatrice peut être décrit par le même vecteur d'état $|1_\xi\rangle$, cependant ce vecteur d'état n'est pas nécessairement le même dans chacune des deux voies. Dans la section B.3 nous généraliserons ensuite la discussion à des flux de photons présentant des variations de paramètres au sein de la fonction

décrivant le mode optique, telles que des variations dans la fréquence centrale du paquet d'onde.

Aspects temporels de l'interférence à deux photons

Nous ne reviendrons pas ici sur le traitement quantique d'une lame séparatrice ni sur le principe de base de l'interférence à deux photons que le lecteur pourra respectivement retrouver aux sections 2.4.1 et 2.4.3 où nous avions négligé les aspects temporels des champs optiques. Dans la présente section, l'interférence à deux photons est uniquement discutée vis-à-vis de la durée des impulsions et de de la résolution des détecteurs.

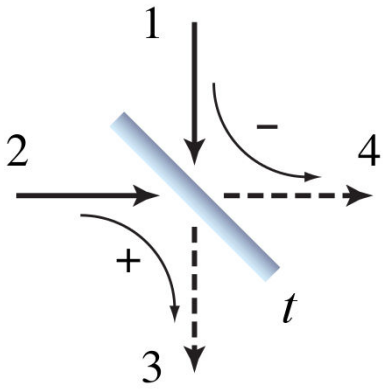


Figure B.1. – Une lame séparatrice idéale est entièrement caractérisée par son coefficient de transmission t. Dans le point de vue de Heisenberg, les opérateurs $\hat{a}_1^\dagger$ et $\hat{a}_2^\dagger$ associées aux deux modes d'entrée (1) et (2) évoluent en opérateurs $\hat{a}_3^\dagger$ et $\hat{a}_4^\dagger$ associés aux modes de sorties (3) et (4).

En notant t_3 et t_4 les temps correspondants à la photodétection d'un photon dans les deux sorties respectives de la lame, nous nous plaçons dans le point de vue de Heisenberg (voir FIGURE B.1 pour les labels des différents modes spatiaux) afin de calculer la probabilité jointe d'une photodétection à partir de la fonction de corrélation du second ordre :

$$G^{(2)}(t_3,t_4) = \sum_{s,s'} \mathrm{Tr}\left\{\hat{\rho}_{1,2}\hat{A}_{3s,4s'}(t_3,t_4)\right\}, \tag{B.14}$$

où $\hat{\rho}_{1,2}$ décrit l'état entrant à deux photons et $s,s' \in \{H,V\}$. L'opérateur $\hat{A}_{3s,4s'}(t_3,t_4)$ est donné par :

$$\hat{A}_{3s,4s'}(t_3,t_4) = \hat{a}_{3s}^\dagger(t_3)\hat{a}_{4s'}^\dagger(t_4)\hat{a}_{4s'}(t_4)\hat{a}_{3s}(t_3). \tag{B.15}$$

La probabilité jointe d'obtenir à la fois une photodétection au niveau du premier détecteur au cours de l'intervalle temporel $[t_0 - \mathrm{d}t_0/2, t_0 + \mathrm{d}t_0/2]$ et au niveau du second durant le même intervalle translaté de τ, $[t_0 + \tau - \mathrm{d}\tau/2, t_0 + \tau + \mathrm{d}\tau/2]$ est alors donnée de manière analogue à l'équation (B.10) par :

$$P^{(2)}(t_0, \tau) = \eta_3 \eta_4 \int_{t_0 - \mathrm{d}t_0/2}^{t_0 + \mathrm{d}t_0/2} \int_{t_0 + \tau - \mathrm{d}\tau/2}^{t_0 + \tau + \mathrm{d}\tau/2} G^{(2)}(t_3, t_4)\, \mathrm{d}t_3 \mathrm{d}t_4. \tag{B.16}$$

où η_3 et η_4 correspondent aux efficacités respectives des détecteurs placés aux sorties (3) et (4). Par analogie avec B.1, la durée la plus courte pour l'intervalle d'intégration est donnée par la résolution temporelle T des détecteurs, de sorte que $\mathrm{d}t_0/2 \geq T$ et $\mathrm{d}\tau/2 \geq T$. Nous allons dans la suite établir l'expression de la probabilité jointe de photodétection dans les cas limites de paquets d'onde avec une durée très courte et très longue vis-à-vis de T.

Si la durée des impulsions est très courte devant la résolution des détecteurs, $\delta t \ll T$, les bornes des deux intégrales dans l'expression (B.16) peuvent être étendues à l'infini et la probabilité d'obtenir une coïncidence devient alors :

$$P^{(2)} = \eta_3 \eta_4 \int \int G^{(2)}(t_3, t_4)\, \mathrm{d}t_3 \mathrm{d}t_4. \tag{B.17}$$

Dans le cas opposé de paquets d'onde avec une durée bien supérieure à la résolution des détecteurs, $\delta t \gg T$, l'intégration dans (B.16) conduit à :

$$P^{(2)}(t_0, \tau) = \eta_3 \eta_4\, G^{(2)}(t_0, t_0 + \tau)\, \mathrm{d}t_0 \mathrm{d}\tau. \tag{B.18}$$

Par conséquent, la probabilité d'obtenir une photodétection jointe peut être étudiée comme un fonction des seuls paramètres t_0 et $t_0 + \tau$. En pratique, seul la différence de temps τ entre les deux photodétections est un paramètre d'intérêt. Ainsi, nous intégrons $P^{(2)}(t_0, \tau)$ sur le temps t_0 de la première photodétection, ce qui nous donne :

$$P^{(2)}(\tau) = \eta_3 \eta_4 T \int G^{(2)}(t_0, t_0 + \tau)\, \mathrm{d}t_0, \tag{B.19}$$

où $\mathrm{d}\tau$ a été substitué par la résolution temporelle T du détecteur. La fonction de corrélation du second ordre, $G^{(2)}$, joue ainsi un rôle centrale dans le calcul de la probabilité d'obtenir une photodétection jointe. Nous allons maintenant détailler son expression en tenant compte de la polarisation et de la structure spatio-temporelle des photons en entrée de la lame séparatrice.

Fonction de corrélation

Nous calculons ici la fonction de corrélation $G^{(2)}$ pour deux photons caractérisés par deux modes respectivement décrits par les fonctions ξ_1 et ξ_2. Sans aucune perte de

généralité nous considérons que les deux photons sont ici linéairement polarisés avec un angle φ entre les directions de polarisation. En prenant pour référence horizontale la polarisation du premier photon, l'état de chaque photon est respectivement donné par $|1_{\xi_1}\rangle_{1H}$ et $\cos(\varphi)\,|1_{\xi_2}\rangle_{2H} + \sin(\varphi)\,|1_{\xi_2}\rangle_{2V}$. L'opérateur densité $\hat{\rho}_{1,2} = |\psi_{in}\rangle\langle\psi_{in}|$ de la paire entrante est ainsi donné par :

$$|\psi_{in}\rangle = \cos(\varphi)\,|1_{\xi_1}\rangle_{1H}\,|1_{\xi_2}\rangle_{2H} + \sin(\varphi)\,|1_{\xi_1}\rangle_{1H}\,|1_{\xi_2}\rangle_{2V}\,, \tag{B.20}$$

où l'on observe la superposition d'un terme où les photons sont dans le même état de polarisation avec un second terme où ils sont dans des états de polarisation orthogonaux. La fonction de corrélation peut ainsi être décomposée en deux contributions $G^{(2)}_{HH}$ et $G^{(2)}_{HV}$:

$$G^{(2)} = \cos^2(\varphi)\; G^{(2)}_{HH} + \sin^2(\varphi)\; G^{(2)}_{HV}. \tag{B.21}$$

En prenant en compte les fonctions associées aux modes on arrive aux expressions suivantes pour $G^{(2)}_{HH}$ et $G^{(2)}_{HV}$:

$$G^{(2)}_{HH}(t_3,t_4) = \frac{\left|\xi_1(t_3)\xi_2(t_4) - \xi_2(t_3)\xi_1(t_4)\right|^2}{4}, \tag{B.22}$$

$$G^{(2)}_{HV}(t_3,t_4) = \frac{\left|\xi_1(t_3)\xi_2(t_4)\right|^2 + \left|\xi_1(t_4)\xi_2(t_3)\right|^2}{4}. \tag{B.23}$$

Un premier enseignement est que la fonction de corrélation pour des photons avec des polarisations parallèles est toujours nulle lorsqu'elle est évaluée en $t_3 = t_4$, et ce même si les fonctions $\xi_1(t)$ et $\xi_2(t)$ ne sont pas identiques. En conséquence, la probabilité d'obtenir une coïncidence est toujours nulle pour $\tau = t_4 - t_3 = 0$; autrement dit, aucune photodétection simultanée n'est attendue même si les photons sont discernables de par leurs modes spatio-temporels.

Comme déjà mentionné en B.1, la fonction associée à un mode peut se décomposer en une amplitude réelle et une phase complexe, $\xi_j(t) = \epsilon_j(t)e^{i\Phi_j(t)}$, avec $j \in \{1,2\}$. Étant donné que la fonction de corrélation $G^{(2)}_{HV}$ pour des photons avec des polarisations perpendiculaires est indépendante de la phase, elle peut être réécrite sous la forme :

$$G^{(2)}_{HV}(t_3,t_4) = \frac{\left(\epsilon_1(t_3)\epsilon_2(t_4)\right)^2 + \left(\epsilon_1(t_4)\epsilon_2(t_3)\right)^2}{4}. \tag{B.24}$$

Une telle écriture n'est pas possible dans le cas des polarisations parallèles puisqu'un terme supplémentaire de recouvrement conduisant à des interférences dépendantes de la phase est également présent. Une façon de le voir est de développer le carré de la norme dans (B.22), ce qui conduit à $G^{(2)}_{HH}(t_3,t_4) = G^{(2)}_{HV}(t_3,t_4) - F(t_3,t_4)$, avec :

$$F(t_3, t_4) = \frac{\epsilon_1(t_3)\epsilon_2(t_4)\epsilon_1(t_4)\epsilon_2(t_3)}{2} \cos\left(\Phi_1(t_3) - \Phi_1(t_4) + \Phi_2(t_4) - \Phi_2(t_3)\right). \tag{B.25}$$

Cependant, cette dépendance de phase n'est effective que si $\Phi_1(t)$ et $\Phi_2(t)$ présentent des évolutions temporelles différentes. Dans le cas contraire la somme des termes de phase est toujours égale à zéro. Une différence dans les évolutions temporelles de $\Phi_1(t)$ et $\Phi_2(t)$ peut être obtenue si par exemple les fréquences des deux photons ne sont pas identiques. Dans ce cas, le terme d'interférence oscille avec la différence des fréquences, donnant alors naissance à des oscillations au sein de la probabilité de photodétection jointe $P^{(2)}(\tau)$, que nous discuterons davantage dans la suite de cette annexe.

En tenant compte du terme d'interférence, l'expression complète de la fonction de corrélation se résume à :

$$G^{(2)}(t_3, t_4) = G^{(2)}_{HV}(t_3, t_4) - \cos^2(\varphi)\ F(t_3, t_4), \tag{B.26}$$

où l'effet d'interférence dépend de l'angle φ entre les polarisations des deux photons.

Dans les deux sections suivantes, la probabilité (B.16) d'obtenir une photodétection jointe est explicitée dans le cas de photons ayant des temps de cohérence respectivement bien inférieurs et bien supérieurs à la résolution temporelle des détecteurs.

Interférence à deux photons sans résolution temporelle

Nous considérons dans un premier temps le cas de paquets d'ondes gaussiens de durée très courte devant la résolution temporelle des détecteurs, c'est-à-dire $\delta t \ll T$. Dans ce cas, il nous est seulement possible de dire si une coïncidence a eu lieu ou non à l'intérieur de l'intervalle temporel T, et l'expression de la probabilité d'obtenir une coïncidence nous est donnée par (B.17). En définissant $\Delta := \omega_{02} - \omega_{01}$, le décalage éventuel entre les fréquences centrales des deux photons, et $\delta\tau := \tau_{02} - \tau_{01}$, le délai éventuel entre les temps d'arrivée des deux photons, la probabilité d'obtenir une coïncidence est alors donnée par :

$$P^{(2)}(\delta\tau) = \frac{1}{2} - \frac{1}{2}\cos^2(\varphi)\ e^{-\frac{\delta t^2}{4/\Delta^2}}\ e^{-\frac{\delta\tau^2}{\delta t^2}}, \tag{B.27}$$

où nous avons considéré le cas de photodétecteurs présentant des efficacités parfaites $\eta_3 = \eta_4 = 1$ et une lame sans pertes. Nous discutons maintenant la probabilité d'obtenir une coïncidence en fonction du délai $\delta\tau$ pour différents angles et différents écarts entre respectivement les polarisations et les fréquences centrales des deux photons, voir Figure B.2.

Comme attendu, aucune interférence ne se produit pour des états de polarisation perpendiculaires puisque pour $\varphi = \pi/2$, on a alors $P^{(2)} = 1/2$, et ce quel que soit $\delta\tau$.

Si les photons ont même polarisation et même fréquence centrale, $\varphi = 0$ et $\Delta = 0$, la probabilité d'obtenir une coïncidence a alors le profil d'un *dip* gaussien centré en $\delta\tau = 0$.

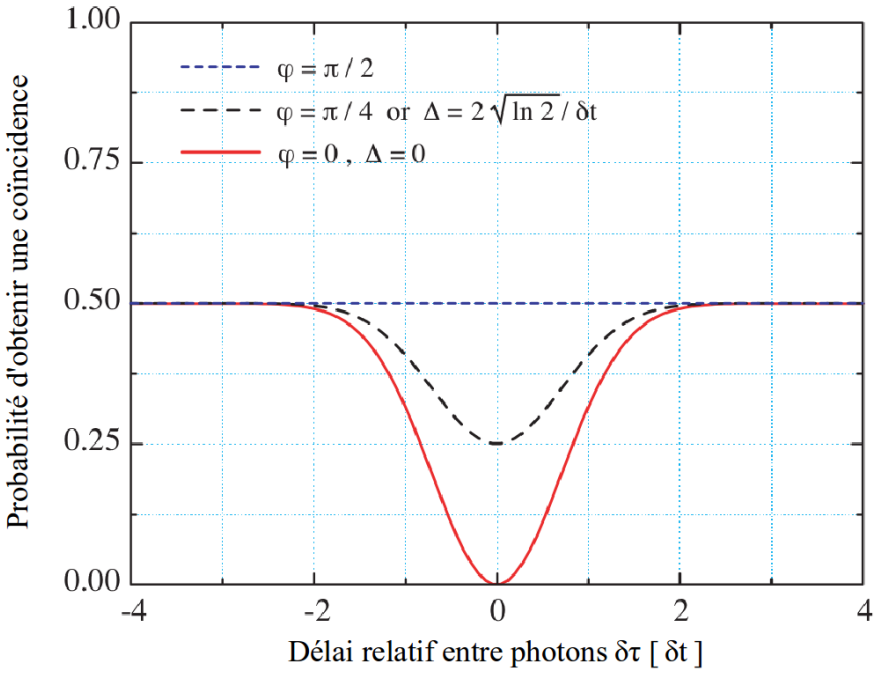


Figure B.2. – Probabilité de photodétection jointe $P^{(2)}$ en fonction du délai relatif $\delta\tau$ entre photons. Dans le cas de photons perpendiculairement polarisés ($\varphi = \pi/2$) aucune interférence n'a lieu et la probabilité d'obtenir une coïncidence a pour valeur constante 1/2. Si les photons ont des polarisations parallèles ($\varphi = 0$) et des fréquences centrales identiques ($\Delta = 0$) on observe un dip ayant un profil Gaussien atteignant zéro en $\delta\tau = 0$, dont la visibilité vaut 100%. Toute perturbation sur l'un des paramètres se traduit par une réduction de la visibilité.

Le minimum du dip atteint zéro, indiquant que les deux photons ne quittent jamais la lame séparatrice séparément. On associe en général à cette figure d'interférence une visibilité V, qui se calcule par définition de la manière suivante :

$$V = \frac{P^{(2)}(\delta\tau \to \pm\infty) - P^{(2)}(\delta\tau = 0)}{P^{(2)}(\delta\tau \to \pm\infty)}. \tag{B.28}$$

Dans le cas de photons de même polarisation, de fréquences centrales et de profils spatio-temporels identiques, la visibilité sera ainsi de 100%. Si les photons de la paire présentent en revanche des différences de polarisation, de fréquences, ou de profils

spatio-temporels, l'interférence n'est alors plus parfaite ce qui se traduit par un dip qui ne descend plus jusqu'à zéro et donc par une visibilité réduite ($V < 100\%$). Par conséquent, l'interférence à deux photons peut être utilisée pour évaluer sans distinction le degré d'indiscernabilité en polarisation et en fréquence entre deux photons.

La première mesure du taux de coïncidences en fonction du délai relatif entre photons a été effectuée par Hong, Ou et Mandel en utilisant des paires de photons générés par conversion paramétrique [255]. Le délai relatif entre photons d'une même paire était contrôlé en décalant la position de la lame séparatrice, comme nous l'avons vu à la section 2.4.3. Les fréquences centrales et les largeurs spectrales des photons étaient ajustées en utilisant deux filtres optiques identiques, de sorte que le taux de coïncidences tende vers zéro pour des photons arrivant simultanément sur la lame. Comme on peut le voir sur la FIGURE B.2, la largeur du dip est identique au temps de cohérence δt des photons. Cette expérience a ainsi été utilisée pour mesurer la durée et la largeur spectrale des photons.

Jusqu'à maintenant, la plupart des expériences d'interférence à deux photons ont été réalisées dans les conditions décrite ici, à savoir $\delta t \ll T$, où pour rappel T est la résolution des détecteurs et δt la durée des photons. La probabilité d'obtenir une détection jointe a par conséquent souvent été uniquement traitée comme une fonction de la seule variable $\delta\tau$. Cependant, si l'on se place maintenant dans le cas où $\delta t \gg T$, le temps τ qui sépare la détection du premier photon de celle du second peut alors être mesuré et la probabilité d'obtenir une photodétection jointe peut alors également être étudiée au travers de ce paramètre.

Interférence à deux photons résolue temporellement

On se place donc désormais dans la situation $\delta t \gg T$, où la probabilité d'obtenir une photodétection jointe peut être étudiée en fonction de l'intervalle temporel τ qui sépare les détections respectives des deux photons. En utilisant l'équation (B.19) et en considérant des paquets d'ondes gaussiens de durées identiques δt, la probabilité d'obtenir une photodétection jointe est donnée par :

$$P^{(2)}(\tau, \delta\tau) = \frac{T}{\delta t\sqrt{\pi}} \left[\frac{1 - \cos^2(\varphi)\ \cos(\tau\ \Delta)}{2} + \sinh^2\left(\frac{\tau\ \delta\tau}{\delta t^2}\right) \right]\ e^{-\frac{\delta\tau^2 + \tau^2}{\delta t^2}}. \qquad \text{(B.29)}$$

La FIGURE B.3 représente la probabilité d'obtenir une photodétection jointe en fonction du délai variable $\delta\tau$ et de la différence dans les temps de détection τ, et ce pour différents états de polarisation et écarts entre fréquences centrales. Le signe de τ indique quel détecteur a cliqué en premier. De manière similaire, le signe de $\delta\tau$ indique quel paquet d'onde s'est présenté à la lame séparatrice en premier. Il est important de

souligner que la probabilité de détection jointe ne peut être différente de zéro que si $|\tau| \approx |\delta\tau|$, ce qui conduit à des profils d'interférence en forme de 'croix' dans l'espace à trois dimensions.

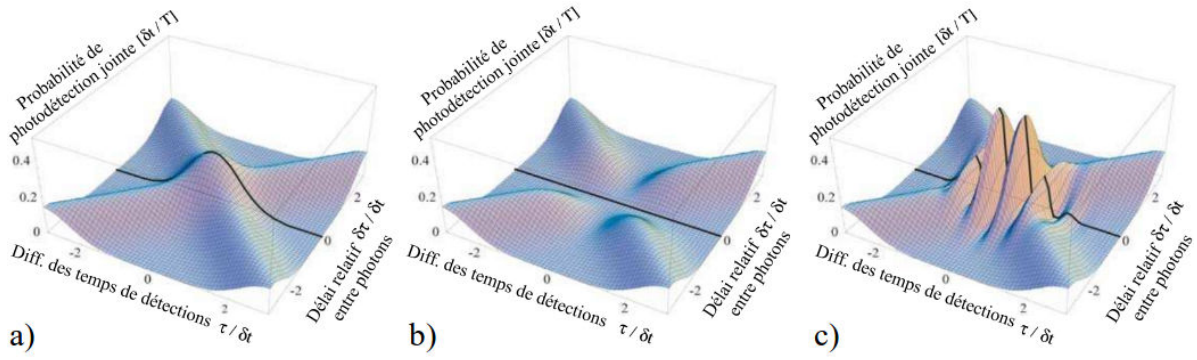


Figure B.3. – Probabilité de photodétection jointe $P^{(2)}$ en fonction du délai relatif $\delta\tau$ entre photons, et de l'intervalle de temps τ entre les deux photodétections. **a)** Cas de photons avec des fréquences centrales identiques ($\Delta = 0$) et des polarisations perpendiculaires ($\varphi = \pi/2$). **b)** Cas de photons avec des fréquences centrales identiques ($\Delta = 0$) et des polarisations parallèles ($\varphi = 0$). **c)** Cas de photons avec des fréquences centrales différentes ($\Delta \neq 0$) et des polarisations parallèles ($\varphi = 0$). Tout les temps et fréquences ont ici été normalisés par la durée δt des paquets d'onde.

En présence de polarisations perpendiculaires, comme nous nous y attendions aucune interférence ne se produit, ceci est illustré Figure B.3(a). La probabilité de photodétection jointe présente par conséquent dans ce cas un pic de profil gaussien, illustré sur la Figure B.3(a) par la ligne noire à $\delta\tau = 0$. L'équation (B.29) nous permet d'affirmer que la largeur à mi-hauteur de ce pic est identique à la durée δt des photons. Étant donné que les photons sont ici discernables en terme de polarisation, une éventuelle différence Δ de leurs fréquences centrales n'aurait ici aucune influence. En se plaçant dans le cas de profils spatio-temporels identiques, la probabilité d'obtenir une photodétection jointe pour des photons perpendiculairement polarisés peut alors être utilisée pour déterminer la durée des paquets d'onde.

La Figure B.3(b) montre la probabilité de photodétection jointe dans le cas de photons ayant des états de polarisation et des fréquences centrales identiques ($\Delta = 0$). Dans le cas de photons arrivant simultanément sur la lame, la probabilité d'obtenir une coïncidence est toujours nulle, ce qui est la signature de la coalescence des photons.

Toujours dans le cas de photons de polarisations identiques, si leurs fréquences centrales sont désormais décalées l'une de l'autre ($\Delta \neq 0$), la probabilité de pho-

todétection jointe oscille en fonction de la différence dans les temps de détection τ. Ceci est illustré par la FIGURE B.3(c). Comme on peut le voir à travers l'équation (B.29), la différence de fréquences Δ détermine la période de ces oscillations. Notons que les oscillations présentent toujours un minimum à $\tau = 0$, et ce quelle que soit la valeur de Δ. Ainsi, même des photons de fréquences centrales différentes ne peuvent dans cette configuration conduire à la détection de coïncidences. De plus, la largueur à mi-hauteur de la figure d'interférence (voir la ligne noire de la FIGURE B.3c) est ici plus large que celle que l'on obtient dans le cas de photons perpendiculairement polarisés.

Sans résolution temporelle, la différence dans les temps de détection ne peut pas être mesurée et la probabilité $P^{(2)}(\tau, \delta\tau)$ d'obtenir une photodétection jointe doit alors être intégrée sur τ. Ceci relie ainsi les différents résultats obtenus au cours de notre traitement du phénomène d'interférence à deux photons. Dans le cas de photons perpendiculairement polarisés, la fonction intégrée $P^{(2)}(\delta\tau)$ a pour valeur constante 1/2. Si les photons sont indiscernables, l'intégration conduit à un *dip* au profil gaussien comme nous l'avions vu précédemment. En revanche, les oscillations présentent dans le cas $\Delta \neq 0$ ne sont plus visibles une fois intégrées. L'intégration conduit dans ce cas, en accord avec l'équation (B.27), à un *dip* gaussien de visibilité réduite.

B.3. Effets de gigue

Nous avons jusqu'à maintenant considéré que tous les photons du flux entrant sur une voie de la lame séparatrice pouvaient être décrits par le même vecteur d'état $|1_\xi\rangle$. Cependant, cela requiert en pratique une source parfaite de photons uniques capable de générer un flux de photons sans aucune variation des différents paramètres de la fonction associée au mode spatio-temporel. Nous considérons ici un scénario plus réaliste pour lequel le flux de photons possède une gigue ϑ pour ses différents paramètres. La description de l'état en sortie de la source est alors donnée par l'opérateur densité de l'équation (B.6).

Une telle gigue sur les paramètres du mode spatio-temporel a d'importantes conséquen- ces sur les résultats des mesures pouvant être réalisées sur le flux de photons uniques. Comme nous l'avons discuté à la section B.1, cela affecte d'une part la probabilité de détection d'un photon de sorte que la mesure ne révèle en général aucune information sur la durée ou sur le profil du paquet d'onde. D'autre part, si l'on considère cette fois-ci la paire de photons, la gigue altère également la qualité de la mesure ; c'est ce que nous allons discuter en détails dans cette section.

Pour analyser l'effet de la gigue sur l'interférence à deux photons, nous considérons deux flux de photons aux profils gaussiens présentant des variations de leurs paramètres. Par analogie avec l'expression (B.6), l'opérateur densité pour la paire de photon est donné par :

$$\hat{\rho}_{1,2} = \int\int f_1(\vartheta_1) f_2(\vartheta_2) \left|1_{\xi_1}\right\rangle \left|1_{\xi_2}\right\rangle \left\langle 1_{\xi_1}\right| \left\langle 1_{\xi_2}\right| \mathrm{d}\vartheta_1 \mathrm{d}\vartheta_2, \tag{B.30}$$

et donc, en utilisant (B.14) et en définissant $\hat{\rho}(\xi_1, \xi_2) \equiv \left|1_{\xi_1}\right\rangle \left|1_{\xi_2}\right\rangle \left\langle 1_{\xi_1}\right| \left\langle 1_{\xi_2}\right|$, la fonction de corrélation s'écrit :

$$G^{(2)}(t_0, t_0+\tau) = \int\int f_1(\vartheta_1) f_2(\vartheta_2)\ \mathrm{Tr}\left\{\hat{\rho}(\xi_1, \xi_2)\hat{A}(t_0, t_0+\tau)\right\}\ \mathrm{d}\vartheta_1 \mathrm{d}\vartheta_2. \tag{B.31}$$

Pour écrire l'équation (B.30), nous avons considéré que tous les photons sont complètement indépendants les uns des autres et tous définis dans le même état de polarisation. En conséquence, seul les termes diagonaux de l'opérateur densité sont non nuls. Les différents paramètres des fonctions ξ_1 et ξ_2 associées aux modes sont respectivement encapsulés par ϑ_1 et ϑ_2. En général, tous les paramètres d'un mode peuvent faire l'objet de variations, et toutes les variations peuvent en principe dépendre les unes des autres. Cependant, nous allons dans la suite focaliser notre attention sur deux paramètres uniquement et analyser dans chaque cas les expressions de $P^{(1)}$ et $P^{(2)}$.

Nous allons dans un premier temps étudier le cas de flux de photons avec une gigue sur leurs fréquences centrales ω_{0j} de sorte à ce que pour chaque paire on ait une variation de la différence de fréquences centrales $\Delta = \omega_{02} - \omega_{01}$ entre les photons. Tout les autres paramètres sont alors considérés comme identiques. Dans un second temps nous nous intéresserons uniquement au cas d'une gigue sur le temps d'émission des photons, de sorte à ce que pour chaque paire on ait une variation du délai relatif $\delta\tau = \tau_{02} - \tau_{01}$ entre les photons.

Gigue fréquentielle

Nous démarrons notre discussion de la gigue fréquentielle en analysant ses effets sur la probabilité moyenne de détection, $P^{(1)}(t_0)$, dans le cas d'un détecteur avec une efficacité parfaite, $\eta = 1$. Si la variation de fréquence dans le flux de photons uniques est décrit par une fonction de distribution normalisée, $f(\omega)$, la probabilité moyenne de détection est donnée, d'après l'équation (B.13), par l'intégrale suivante :

$$P^{(1)}(t_0) = T \int f(\omega)\ |\xi(t_0, \omega)|^2\ \mathrm{d}\omega. \tag{B.32}$$

Étant donné que seul la phase des modes gaussiens dépend de la fréquence, la valeur absolue, $|\xi(t_0, \omega)|^2 = \epsilon^2(t_0)$, est en réalité indépendante de ω. Par conséquent, la probabilité moyenne d'obtenir une photodétection est nullement affectée par la présence de la gigue fréquentielle, la probabilité est entièrement déterminée par la seule fonction associée au mode spatio-temporel considéré.

Si une gigue fréquentielle n'a aucun impact sur $P^{(1)}$, dans le cas d'une interférence à deux photons cette dernière affecte en revanche la probabilité d'obtenir une photodétection jointe. Pour illustrer ceci, nous nous plaçons dans le cas de deux flux de photons uniques indépendants, chacun fluctuant autour d'une fréquence centrale commune, ω_0. Les fluctuations sur chaque voie sont décrites par deux fonctions de distribution normalisées et de profils Gaussiens, $f_1(\omega_{01})$ et $f_2(\omega_{02})$. En conséquence, la différence de fréquences de la paire de photons, $\Delta = \omega_{02} - \omega_{01}$, présente elle aussi des variations suivant un profil gaussien normalisé :

$$f(\Delta) = \frac{1}{\sqrt{\pi}\ \delta\omega} e^{-\dfrac{\Delta^2}{\delta\omega^2}}, \tag{B.33}$$

avec $\delta\omega$ une largeur dépendant des largeurs à mi hauteur des distributions fréquentielles respectives des deux flux :

$$\delta\omega = \sqrt{\delta\omega_{01}^2 + \delta\omega_{02}^2}. \tag{B.34}$$

L'opérateur densité de la paire de photons peut désormais être exprimé en fonction de la fonction de distribution de la différence des fréquences :

$$\hat{\rho}_{1,2} = \int f(\Delta)\ \hat{\rho}(\xi_1, \xi_2)\ \mathrm{d}\Delta. \tag{B.35}$$

La trace et l'intégration étant interchangeable, la fonction de corrélation, d'après l'équation (B.31), peut alors s'écrire :

$$G^{(2)}(t_0, \tau) = \int f(\Delta)\ \mathrm{Tr}\left\{\hat{\rho}(\xi_1, \xi_2)\hat{A}(t_0, t_0 + \tau)\right\}\ \mathrm{d}\Delta. \tag{B.36}$$

Dans le cas de photons avec une durée très grande devant la résolution temporelle des détecteurs, la probabilité moyenne associée à l'obtention d'une photodétection jointe est donnée par (B.19). Pour des photons simultanés ($\delta\tau = 0$), ceci conduit à :

$$P^{(2)}(\tau) = \frac{T}{2\sqrt{\pi}\ \delta t}\left[1 - \cos^2(\varphi)\ e^{-\dfrac{\tau^2}{4/\delta\omega^2}}\right]\ e^{-\dfrac{\tau^2}{\delta t^2}}. \tag{B.37}$$

Pour des photons de polarisations identiques, $P^{(2)}(\tau)$ est représenté en FIGURE B.4. Dans la limite $\delta\omega \to \infty$ la probabilité d'obtenir une photodétection jointe à la forme d'un pic suivant un profil gaussien avec comme largeur $\Gamma_1 = \delta t$. Lorsque $\delta\omega$ est une quantité finie, l'équation (B.37) nous montre que la probabilité d'obtenir une photodétection jointe est toujours nulle en $\tau = 0$. En fait, on est alors en présence d'un *dip* centré en $\tau = 0$ et de largeur $\Gamma_2 = 2/\delta\omega$. $Gamma_2$ représente ici un temps de cohérence qu'il est important de ne pas confondre avec la durée δt des paquets d'onde.

Pour déterminer la gigue fréquentielle en présence à partir d'une interférence à deux photons résolue temporellement ($\delta t \gg T$), deux mesures doivent être effectuées. Tout d'abord, la mesure de la probabilité moyenne d'une photodétection jointe dans le cas de photons perpendiculairement polarisés ($\varphi = \pi/2$) nous permet de d'accéder à la durée δt des paquets d'onde. Une mesure similaire avec des photons cette fois-ci parallèlement polarisés permet ensuite denmesurer Γ_2 et d'estimer la gigue fréquentielle, $\delta\omega$.

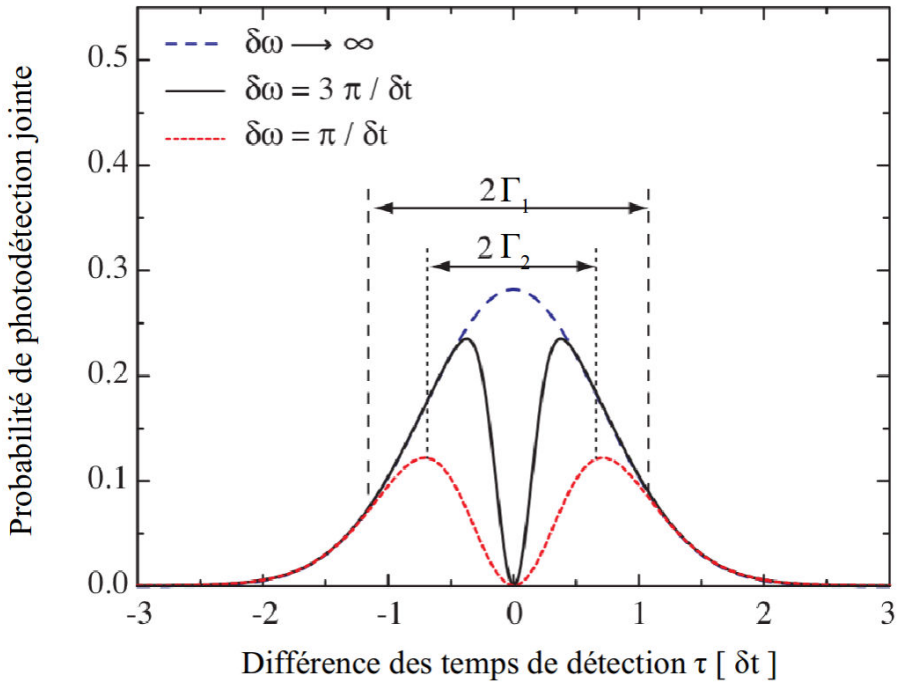


Figure B.4. – Probabilité de photodétection jointe, $P^{(2)}$, en fonction du temps, τ, séparant les détections des deux photons, et ce, dans le cas où le délai relatif $\delta\tau$ entre photons est nul. Les polarisations des photons sont ici parallèles, et on est de plus en présence d'une gigue fréquentielle, $\delta\omega$.

Si les photons sont de courtes durées devant la résolution des détecteurs, la probabilité d'obtenir une coïncidence doit alors être calculée à partir de l'équation (B.17). La probabilité moyenne d'une photodétection jointe est alors une fonction dépendant du délai relatif entre photons, $\delta\tau$, d'expression :

$$P^{(2)}(\delta\tau) = \frac{1}{2} - \frac{\cos^2(\varphi)}{\sqrt{4+\delta t^2\delta\omega^2}}\, e^{-\frac{\delta\tau^2}{\delta t^2}}. \tag{B.38}$$

Par comparaison avec les résultats obtenus précédemment sans gigue, on voit ici qu'une gigue fréquentielle $\delta\omega$ conduit à un *dip* de profondeur réduite, tandis que sa largeur à

mi-hauteur reste inchangée.

En principe, il est également possible d'estimer la gigue fréquentielle à partir d'une interférence à deux photons non résolue temporellement ($\delta t \ll T$), mais cela présente des désavantages. Tout d'abord, la profondeur du *dip* dépend non seulement de la gigue fréquentielle, mais aussi du degré de recouvrement des modes transverses des deux faisceaux. Un recouvrement imparfait conduit à un facteur comparable au $\cos^2(\varphi)$ de l'équation (B.38). Par conséquent, à la différence du cas résolu temporellement, on ne peut plus distinguer les deux contributions l'une de l'autre. Deuxièmement, dans le cas de deux flux de photons indépendants, il est impossible de dire si la perte de visibilité est due à des fréquences centrales décalées ou à un effet de gigue. Et troisièmement, si la gigue est trop grande, le *dip* devient très peu profond dans le cas $\delta t \ll T$, comme nous l'avions illustré en FIGURE B.2, alors qu'il reste de profondeur inchangée dans le cas $\delta t \gg T$. Il est en effet plus simple de déterminer une faible largeur plutôt qu'une faible profondeur.

Gigue temporelle à l'émission

On considère maintenant des flux de photons uniques soumis à un effet de gigue temporelle lors de l'émissions des photons. De nouveau on se place dans le cas d'une gigue ayant un profil gaussien décrit par la fonction de distribution normalisée, $f(\tau_0)$. La probabilité moyenne de détection d'un photon pour un détecteur idéal d'efficacité $\eta = 1$ est de nouveau donnée par (B.13) :

$$P^{(1)}(t_0) = T \int f(\tau)\ |\xi(\tau - t_0)|^2\ \mathrm{d}\omega. \tag{B.39}$$

On est en présence d'une corrélation croisée (*cross-correlation*) entre la probabilité de détection, $|\xi(t_0)|^2$, de chaque photon unique, et la distribution du temps d'émission, $f(\tau_0)$, du flux de photons. Par conséquent, la probabilité moyenne de détection est toujours plus grade que dans le cas d'un flux de photons sans gigue temporelle lors de l'émission de ces derniers. Ceci traduit le fait qu'une variation dans les paramètres d'un mode spatio-temporel peut altérer la probabilité de détection des photons. En général, le probabilité moyenne de détection n'est pas identique à la probabilité de détection des photons individuels.

Pour étudier l'influence d'une gigue temporelle à l'émission des photons lors de la réalisation d'une expérience d'interférence à deux photons, on considère que les deux flux de photons ont des distributions gaussiennes de leurs temps d'émission de largeurs identiques, $\Delta\tau$. Dans ce cas, les paires de photons sont caractérisées par une gigue du délai relatif entre photons, qui est de nouveau donnée par une distribution gaussienne :

$$f(\delta\tau) = \frac{1}{\sqrt{\pi}\ \Delta\tau}\ e^{-\frac{\delta\tau^2}{\Delta\tau^2}}. \tag{B.40}$$

La fonction de correlation $G^{(2)}(t_0, t_0+\tau)$ peut s'écrire, par analogie avec (B.36), en utilisant la seule variation du délai relatif entre photons :

$$G^{(2)}(t_0,\tau) = \int f(\delta\tau)\ \mathrm{Tr}\left\{\hat{\rho}(\xi_1,\xi_2)\hat{A}(t_0,t_0+\tau)\right\}\ \mathrm{d}(\delta\tau), \tag{B.41}$$

et la probabilité d'obtenir une photodétection jointe doit être calculée à partir de (B.19). Dans le cas de photons se présentant simultanément en entrée de la lame séparatrice, cela conduit à l'expression :

$$P^{(2)}(\tau) = \frac{T}{2\sqrt{\pi}\sqrt{\delta t^2+\Delta\tau^2}}\ \left[1-\cos^2(\varphi)\ e^{-\frac{\tau^2}{\delta t^2+\delta t^4/\Delta\tau^2}}\right]\ e^{-\frac{\tau^2}{\delta t^2+\Delta\tau^2}}. \tag{B.42}$$

Par contraste avec le cas précédent, la largeur du pic de profil gaussien au sein de la probabilité d'obtenir une photodétection jointe dans le cas de photons perpendiculairement polarisé ne correspond ici plus à la durée des paquets d'onde. La variation dans le temps d'émission affecte également l'amplitude de la fonction associée au mode spatio-temporel et affecte la probabilité d'obtenir une photodétection jointe même sans interférence. Ceci est illustré en FIGURE B.5 où est représentée la probabilité d'obtenir une photodétection jointe avec des paires de photons caractérisées par une distribution du délai relatif.
La largeur, Γ_1, du pic gaussien n'est ici plus identique à la durée, δt, des paquets d'onde. On voit à partir de l'équation (B.42) que Γ_1 est agrandie du fait des variations dans le délai relatif des photons, $\Delta\tau$:

$$\Gamma_1 = \sqrt{\delta t^2+\Delta\tau^2}. \tag{B.43}$$

De plus, la largeur du dip dans le cas de photons parallèlement polarisés n'est pas indépendante de Γ_1, son expression est donnée par :

$$\Gamma_2 = \sqrt{\delta t^2+\delta t^4/\Delta\tau^2} = \frac{\delta t}{\Delta\tau}\Gamma_1. \tag{B.44}$$

Une expérience d'interférence à deux photons résolue temporellement peut à nouveau être utilisée pour déterminer les variations introduites lors de l'émission des photons. Toutefois, étant donné que les profils des variations dans le cas d'une gigue fréquentielle et d'une gigue temporelle à l'émission sont les mêmes, il est en général impossible de les discerner expérimentalement.

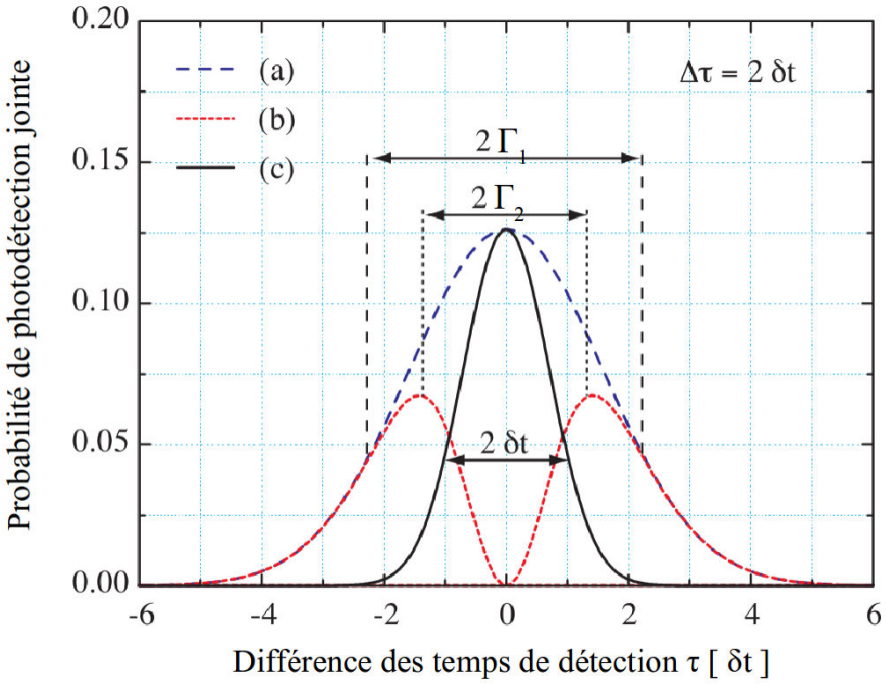


Figure B.5. – Probabilité de photodétection jointe, $P^{(2)}$, en fonction du temps, τ, séparant les détections des deux photons, et ce pour le cas où le délai relatif entre photons, $\delta\tau$, est soumis à des variations. **a)** Cas de photons polarisés identiquement. **b)** Cas de photons parallèlement polarisés. **c)** Gaussienne de largeur δt. La largeur Γ_1 du pic gaussien en (a) est élargie par la variation du délai relatif, $\Delta\tau$, que l'on considère ici égale à $2\delta t$.

Dans le cas de photons avec des durées courtes devant la résolution des détecteurs, la probabilité d'obtenir une coïncidence se calcule une nouvelle fois à partir de (B.17) :

$$P^{(2)}(\delta\tau) = \frac{1}{2} - \frac{\cos^2(\varphi)}{2\sqrt{1+\Delta\tau^2/\delta t^2}}\, e^{-\dfrac{\delta\tau^2}{\delta t^2+\Delta\tau^2}}. \tag{B.45}$$

La largeur du *dip* gaussien est agrandie par la gigue de largeur $\Delta\tau$, et sa profondeur est également réduite. À nouveau il est possible de déterminer la gigue à partir de ce type de mesure ; cependant les désavantages restent les mêmes que ceux discutés précédemment en comparaison d'une mesure résolue temporellement.

C. Systèmes de détection

La détection est un élément crucial dans les expériences de communications quantiques. Dans cette annexe, nous allons présenter les différents détecteurs dont nous disposons, basés sur deux technologies. Après une brève description du principe de fonctionnement des photodiodes à avalanche et des détecteurs supraconducteurs, nous présenterons les caractéristiques importantes de nos détecteurs. Puis nous finirons par un autre élément clef de la détection que sont les compteurs de coïncidences.

C.1. Détecteurs de photons uniques

Photodiode à avalanche

Une photodiode à avalanche (APD) consiste généralement en une jonction semiconductrice de type P-N [2] susceptible de supporter des tensions de polarisation inverse. La caractéristique tension-courant inverse dans ce type de jonction présente un front très raide au-dessus d'une certaine tension de claquage, ce qui confère un véritable gain au système, comme le montre la FIGURE C.1. L'idée est d'appliquer à la jonction une tension légèrement inférieure à la tension de claquage, pour que l'absorption d'un seul photon apporte l'énergie suffisante pour déclencher l'avalanche.

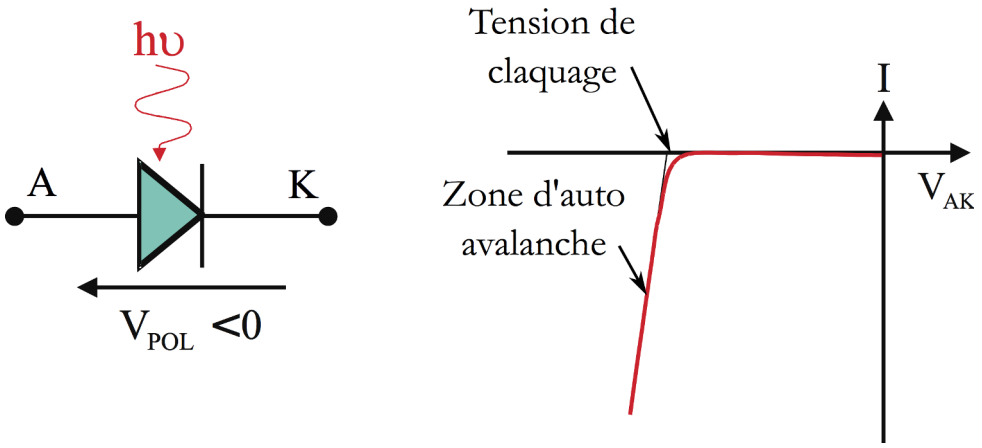


Figure C.1. – Courbe schématique de la réponse en courant I d'une jonction de type P-N polarisée en inverse V_{POL}. Le phénomène d'avalanche apparaît pour des tensions supérieures à la tension de claquage. Note : par convention A est l'anode de la diode et est reliée à la zone dopée P et K est la cathode reliée à la zone dopée N.

En effet, l'absorption d'un photon par un défaut du réseau cristallin va générer un paire électron-trou (e^-/h^+) qui va être accélérée sous l'effet du champ électrique présent dans

2. Une jonction P-N est un cristal avec une zone dopée en électrons (P) collée à une zone dopée en trous (N).

la zone active. Comme le montre la FIGURE C.3, l'électron (resp. trou) va se diriger vers la zone dopée P (resp. N). Les porteurs traversant la zone de déplétion peuvent alors atteindre une énergie suffisante pour créer d'autres porteurs par ionisation due aux collisions avec les atomes du cristal. Ainsi l'avalanche se déclenche et permet de générer un courant suffisant pour être mesuré.

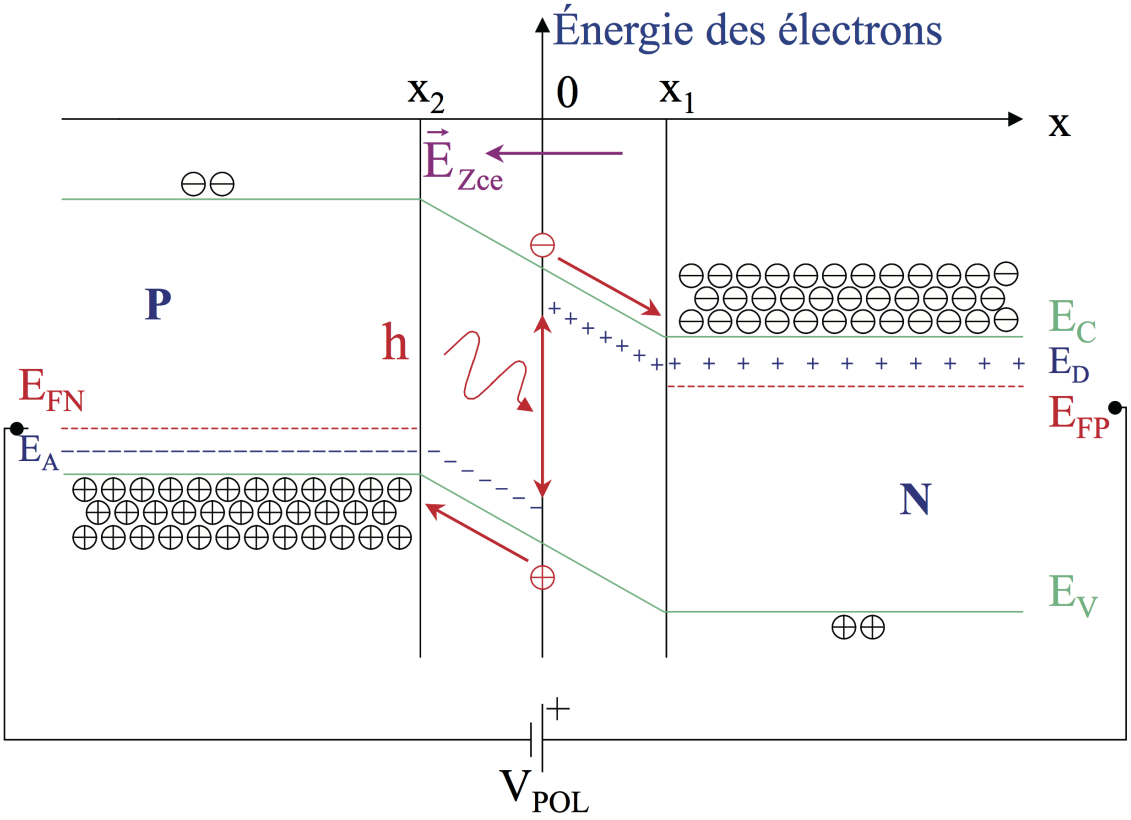


Figure C.2. – Diagramme de bande en énergie simplifié représentant l'amorçage de l'avalanche au sein de la zone de déplétion d'une APD. Les deux parties du semi-conducteur dopée P (à gauche) et N (à droite) sous l'effet de la polarisation inverse V_{POL} laisse apparaitre une zone sans porteur de charge délimitée par les bornes x_1 et x_2 (zone de déplétion). Les niveaux d'énergie E_C, E_V, E_A, E_D, E_{FP} et E_{FN} représentent respectivement l'énergie de la bande de Conduction, de la bande de Valence, des ions accepteurs (P), des ions donneurs (N), du niveau de Fermi en zone P et du niveau de Fermi en zone N.

Détecteur supraconducteur

Les détecteurs de photon unique supraconducteur (SSPD) consistent en un film ultra-fin supraconducteur, généralement du nitrure de niobium refroidi à des températures

comprises entre 1.5 K et 4 K à l'aide d'hélium liquide. Ce film supraconducteur doit avoir la capacité de conduire l'électricité sans perte d'énergie pour une densité de courant $J < J_C$, avec J_C la densité de courant critique, voir FIGURE C.3. Dans le cas d'un détecteur de photon unique, une intensité de biais proche de l'intensité critique est appliquée, de sorte qu'un photon crée un échauffement local sur le film de supraconducteur suffisant pour que l'intensité critique devienne plus faible que l'intensité de biais. Ainsi, une tension se crée aux bornes du film, qui annonce l'absorption du photon.

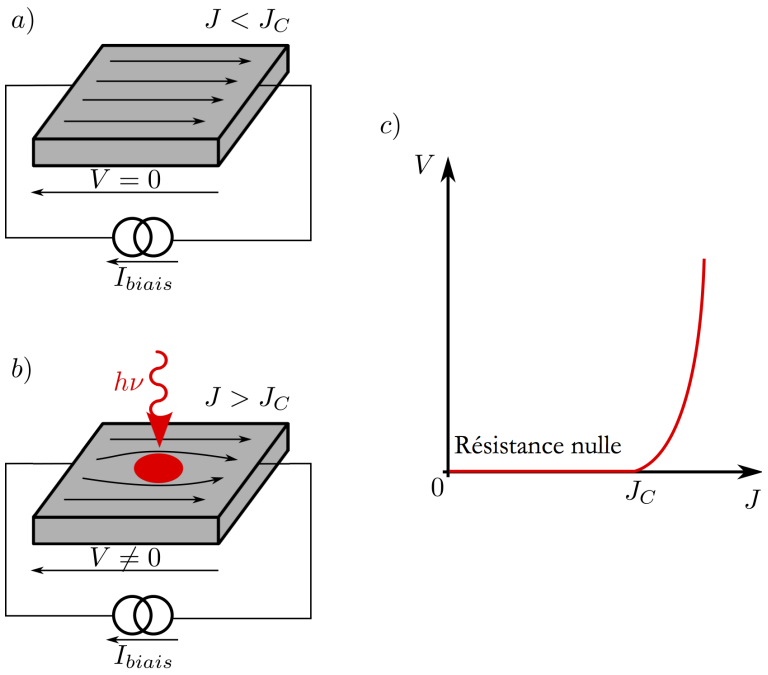


Figure C.3. – Schéma de principe d'un détecteur supraconducteur. **a)** Le film supraconducteur a l'équilibre thermodynamique présente une résistance nulle pour une densité de courant J inférieure à la densité de courant critique J_C. **b)** Lorsqu'un photon arrive sur le film supraconducteur, il crée un point chaud qui a pour effet de réduire la densité de courant critique J_C. Ainsi en appliquant une intensité de biais proche de l'intensité critique, nous pouvons observer une augmentation de la tension aux bornes du supraconducteur annonçant l'arrivé d'un photon. **c)** Courbe intensité-tension aux bornes du film supraconducteur, qui montre que pour une densité de courant inférieure à J_C, la tension est nulle.

Caractéristiques importantes des détecteurs

Les caractéristiques importantes pour les détecteurs de photons uniques sont :

- L'efficacité quantique de détection (P_d) qui détermine le pourcentage de photons détectés. Elle est généralement donnée en fonction de la longueur d'onde des pho-

tons. Dans le cas d'une APD, elle dépend essentiellement de la tension de biais et pour un SSPD de l'intensité de biais.
- Le taux de coups sombres (R_{dc}) qui correspond au nombre de détection sans apport d'énergie par un photon.
- Le mode opératoire, continu ou déclenché qui dépend généralement du niveau de bruit intrinsèque au détecteur [3].
- Le jitter ou gigue temporelle (τ_j) qui représente l'incertitude sur le temps de détection.
- Le taux de saturation (R_S) qui représente le taux maximum de comptage pour lequel le détecteur présente une réponse linéaire.
- Le temps mort (τ_d), qui est la durée après une détection durant lequel le détecteur est aveugle.

	APD InGaAs ID201	APD InGaAs/InP ID210	APD InGaAs/InP ID220	SSPD ID281
λ	900-1700 nm	900-1700 nm	900-1700 nm	400-2500 nm
Mode	déclenché	déclenché	continu	continu
P_d	10-25% (@ 1550 nm)	5-25% (@ 1550 nm)	10-20% (@ 1550 nm)	50%
R_{dc}	$< 10^4$ Hz	$< 10^4$ Hz	$< 10^4$ Hz	< 100 Hz
τ_j	200 ps (@ 25% d'efficacité)	200 ps (@ 25% d'efficacité)	250 ps (@ 20% d'efficacité)	50 ps
R_S	200 kHz	200 kHz	100 kHz	15 MHz
τ_d	0-100 μs	0-100 μs	0-25 μs	

Table C.1. – Tableau des caractéristiques des différents détecteurs disponibles au sein du laboratoire.

C.2. Les compteurs de coïncidences

La mesure de coïncidences est très importante en communication quantique, aussi bien pour la mesure d'intrication que pour la réalisation de relais. Pour cela, nous disposons de deux outils, des convertisseurs temps-amplitude (TAC) [4] et une porte logique 'ET' [5], formant un ensemble d'appareils complémentaires.

Le TAC permet de mesurer le temps ΔT entre un signal *start* et un signal *stop* en le convertissant en amplitude. L'utilisation d'un ordinateur avec une carte d'acquisition

3. En effet, certains semi-conducteurs comme l'InGaAs possèdent beaucoup de défauts susceptibles de piéger des porteurs de charges lors de l'avalanche. Une repolarisation trop rapide de la jonction libère ces porteurs de charges qui déclenchent une avalanche, nous parlons alors d'*after-pulse*.

4. Produit de la gamme ORTEC model 567

5. Produit de la gamme ORTEC model CO4020

permet alors de reconstruire l'histogramme temporel des temps relatifs d'arrivées. Dans le cas de photons appairés, nous voyons apparaître un pic de coïncidence. Ainsi il est facile d'ajuster les délais optiques et électroniques dans nos expériences. En post-sélectionnant différents pics de coïncidence et en envoyant les différents signaux post-sélectionnés (sorties *Single Channel Analyser* des TAC) à une porte logique 'ET', il devient alors possible de comptabiliser des coïncidences triples, quadruples, etc. dans une fenêtre temporelle ajustable.

Bibliographie

[1] A. Aspect, "Du débat Bohr-Einstein à l'information quantique : la seconde révolution quantique ?", in *Séances publiques*. Institut de France, Académie des sciences, 2014.

[2] M. Planck, "On the law of distribution of energy in the normal spectrum", *Annalen der Physik*, vol. 4, pp. 553, 1901.

[3] L. de Broglie, "Sur la complémentarité des idées d'individu et de système", *Dialectica*, vol. 2, no. 3/4, pp. 325–330, 1948.

[4] A. Einstein, "Über einen die Erzeugung und Verwandlung des Lichtes betreffenden heuristischen Gesichtspunkt", *Annalen der Physik*, vol. 322, pp. 132–148, 1905.

[5] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.

[6] I. M. Georgescu, S. Ashhab, and F. Nori, "Quantum simulation", *Rev. Mod. Phys.*, vol. 86, pp. 153–185, Mar 2014.

[7] C. L. Degen, F. Reinhard, and P. Cappellaro, "Quantum sensing", *Rev. Mod. Phys.*, vol. 89, pp. 035002, Jul 2017.

[8] V. Giovannetti, S. Lloyd, and L. Maccone, "Advances in quantum metrology", *Nat. Photonics*, vol. 5, pp. 222–229, 2011.

[9] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography", *Rev. Mod. Phys.*, vol. 74, pp. 145–195, Mar 2002.

[10] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution", *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, Sep 2009.

[11] C. A. Shannon, "A mathematical theory of communication", *Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948.

[12] "ID Quantique (Switzerland)", `http://idquantique.com/`.

[13] "MagiQ Technology (USA)", `http://www.magiqtech.com/`.

[14] "SeQureNet (France)", `http://www.sequrenet.fr/`.

[15] "NuCrypt (USA)", `http://www.nucrypt.net/`.

[16] "QuTools (Germany)", `http://www.qutools.com/`.

[17] "QuintessenceLabs (Australia)", `http://qlabsusa.com/`.

[18] S. Perifel, *Complexité algorithmique*, Ellipses, 2014.

[19] G. E. Moore, "Cramming more components onto integrated circuits", *Electronics*, vol. 38, pp. 33 – 35, 1965.

[20] Intel Corporation (USA), "Intel timeline : A history of innovation", `www.intel.com/content/www/us/en/history/historic-timeline.html`.

[21] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[22] A. M. Turing, "On computable numbers, with an application to the Entscheidungs problem", *Proceedings of the London Mathematical Society*, vol. 42, pp. 230–265, 1937.

[23] R. Feynman, "Simulating physics with computers", *International Journal of Theoretical Physics*, vol. 21, no. 6, pp. 467–488, 1982.

[24] D. Deutsch, "Quantum theory, the Church-Turing principle and the universal quantum computer", *Proc. R. Soc. A*, vol. 400, no. 1818, pp. 97–117, 1985.

[25] R. Landauer, "The physical nature of information", *Phys. Lett. A*, vol. 217, pp. 188–193, 1996.

[26] D. Deutsch and R. Jozsa, "Rapid solutions of problems by quantum computation", *Proc. R. Soc. A*, vol. 439, pp. 553–558, 1992.

[27] P. Shor, "Algorithms for quantum computation : Discrete logarithms and factoring", *IEEE Symposium on Foundations of Computer Science*, pp. 124–134, 1994.

[28] L. K. Grover, "A fast quantum mechanical algorithm for database search", *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, pp. 212–219, 1996.

[29] J. I. Cirac and P. Zoller, "Quantum computations with cold trapped ions", *Phys. Rev. Lett.*, vol. 74, pp. 4091–4094, May 1995.

[30] J. I. Cirac and P. Zoller, "A scalable quantum computer with ions in an array of microtraps", *Nature*, vol. 404, pp. 579, 2000.

[31] D. Kielpinski, C. Monroe, and D. J. Wineland, "Architecture for a large-scale ion-trap quantum computer", *Nature*, vol. 417, pp. 709–711, 2002.

[32] C. Monroe and J. Kim, "Scaling the ion trap quantum processor", *Science*, vol. 339, no. 6124, pp. 1164–1169, 2013.

[33] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland, "Demonstration of a fundamental quantum logic gate", *Phys. Rev. Lett.*, vol. 75, pp. 4714–4717, Dec 1995.

[34] A. Sorensen and K. Molmer, "Quantum computation with ions in thermal motion", *Phys. Rev. Lett.*, vol. 82, pp. 1971–1974, Mar 1999.

[35] S. Gulde, M. Riebe, G. P. T. Lancaster, C. Becher, J. Eschner, H. Häffner, F. Schmidt-Kaler, I. L. Chuang, and R. Blatt, "Implementation of the Deutsch–Jozsa algorithm on an ion-trap quantum computer", *Nature*, vol. 421, pp. 48–50, 2003.

[36] J. Chiaverini, J. Britton, D. Leibfried, E. Knill, M. D. Barrett, R. B. Blakestad, W. M. Itano, J. D. Jost, C. Langer, R. Ozeri, T. Schaetz, and D. J. Wineland, "Implementation of the semiclassical quantum fourier transform in a scalable system", *Science*, vol. 308, no. 5724, pp. 997–1000, 2005.

[37] H. Häffner, W. Hänsel, C.F. Roos, J. Benhelm, D. Chek-al ka, M. Chwalla, T. Körber, U. D. Rapol, M. Riebe1, P. O. Schmidt, C. Becher, O. Gühne, W. Dür, and R. R. Blatt, "Scalable multiparticle entanglement of trapped ions", *Nature*, vol. 438, pp. 643–646, 2005.

[38] C. Ospelkaus, U. Warring, Y. Colombe, K.R. Brown, J. M. Amini, D. Leibfried, and D. J. Wineland, "Microwave quantum logic gates for trapped ions", *Nature*, vol. 476, pp. 181–184, 2011.

[39] T. R. Tan, J. P. Gaebler, Y Lin, Y. Wan, R. Bowler, D. Leibfried, and D. J. Wineland, "Multi-element logic gates for trapped-ion qubits", *Nature*, vol. 528, pp. 380–383, 2015.

[40] T. Monz, D. Nigg, E. A. Martinez, M. F. Brandl, P. Schindler, R. Rines, S. X. Wang, I. L. Chuang, and R. Blatt, "Realization of a scalable Shor algorithm", *Science*, vol. 351, no. 6277, pp. 1068–1070, 2016.

[41] E. A. Martinez, C. A. Muschik, P. Schindler, D. Nigg, A. Erhard, M. Heyl, P. Hauke, M. Dalmonte, P. Monz, T.and Zoller, and R. Blatt, "Real-time dynamics of lattice gauge theories with a few-qubit quantum computer", *Nature*, vol. 534, pp. 516–519, 2016.

[42] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, "Linear optical quantum computing with photonic qubits", *Rev. Mod. Phys.*, vol. 79, pp. 135–174, Jan 2007.

[43] S. Aaronson and A. Arkhipov, "The computational complexity of linear optics", *Theory of Computing*, vol. 9, pp. 143–252, 2013.

[44] M. A. Broome, A. Fedrizzi, S. Rahimi-Keshari, J. Dove, S. Aaronson, T. C. Ralph, and A. G. White, "Photonic boson sampling in a tunable circuit", *Science*, vol. 339, no. 6121, pp. 794–798, 2013.

[45] J. Spring, B. Metcalf, P. Humphreys, S. Kolthammer, X. Jin, M. Barbieri, A. Datta, N. Thomas-Peter, N. Langford, D. Kundys, J. Gates, B. Smith, P. Smith, and I Walmsley, "Boson sampling on a photonic chip", *Science*, vol. 339, no. 6121, pp. 798–801, 2013.

[46] M. Tillmann, B. Dakic, R. Heilmann, S. Nolte, A. Szameit, and P. Walther, "Experimental boson sampling", *Nat. Photonics*, vol. 7, pp. 540–544, 2013.

[47] A ; Crespi, R. Osellame, R. Ramponi, D. Brod, E. Galvao, N. Spagnolo, C. Vitelli, E. Maiorino, P. Mataloni, and F. Sciarrino, "Integrated multimode interferometers with arbitrary designs for photonic boson sampling", *Nat. Photonics*, vol. 7, pp. 545–549, 2013.

[48] J. Carolan, C. Harrold, C. Sparrow, E. Martín-López, N. J. Russell, J. W. Silverstone, P. J. Shadbolt, N. Matsuda, M. Oguma, M. Itoh, G. D. Marshall, M. G. Thompson, J. C . F. Matthews, T. Hashimoto, J. L. O'Brien, and A Laing, "Universal linear optics", *Science*, vol. 349, no. 6249, pp. 711–716, 2015.

[49] M. Bentivegna, N. Spagnolo, C. Vitelli, F. Flamini, N. Viggianiello, L. Latmiral, P. Mataloni, E. Brod, D. and ; Galvão, A. Crespi, R. Ramponi, R. Osellame, and F. Sciarrino, "Experimental scattershot boson sampling", *Sci. Adv., Year = 2015, Number = 3, Volume = 1, Owner = bfedrici, Timestamp = 2017.05.27.*

[50] E. Knill, R. Laflamme, and G. J. Milburn, "A scheme for efficient quantum computation with linear optics", *Nature*, vol. 409, no. 6816, pp. 46–52, 2001.

[51] R. Raussendorf and H. J. Briegel, "A one-way quantum computer", *Phys. Rev. Lett.*, vol. 86, pp. 5188–5191, May 2001.

[52] P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, and A. Zeilinger, "Experimental one-way quantum computing", *Nature*, vol. 434, no. 7030, pp. 169–176, 2005.

[53] D. E. Browne and T. Rudolph, "Resource-efficient linear optical quantum computation", *Phys. Rev. Lett.*, vol. 95, pp. 010501, Jun 2005.

[54] N. C. Menicucci, P. van Loock, M. Gu, C. Weedbrook, T. C. Ralph, and M. A. Nielsen, "Universal quantum computation with continuous-variable cluster states", *Phys. Rev. Lett.*, vol. 97, pp. 110501, Sep 2006.

[55] N. C. Menicucci, S. T. Flammia, and O. Pfister, "One-way quantum computing in the optical frequency comb", *Phys. Rev. Lett.*, vol. 101, pp. 130501, Sep 2008.

[56] S. Yokoyama, R. Ukai, S. C. Armstrong, C. Sornphiphatphong, T. Kaji, S. Suzuki, J. Yoshikawa, H. Yonezawa, N. C. Menicucci, and A. Furusawa, "Ultra-large-scale continuous-variable cluster states multiplexed in the time domain", *Nat. Photonics*, vol. 7, pp. 982–986, 2013.

[57] D. G. Cory, A. F. Fahmy, and T. F. Havel, "Ensemble quantum computing by NMR spectroscopy", *Proc. Natl. Acad. Sci.*, vol. 94, no. 5, pp. 1634–1639, 1997.

[58] N. A. Gershenfeld and I. L. Chuang, "Bulk spin-resonance quantum computation", *Science*, vol. 275, no. 5298, pp. 350–356, 1997.

[59] L. M. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance", *Nature*, vol. 414, pp. 883–887, 2001.

[60] S. W. Warren, "The usefulness of NMR quantum computing", *Science*, vol. 277, no. 5332, pp. 1688–1690, 1997.

[61] M. Mohseni, P. Read, H. Neven, S. Boixo, V. Denchev, R. Babbush, A. Fowler, V. Smelyanskiy, and J. M. Martinis, "Commercialize quantum technologies in five years", *Nature*, vol. 543, pp. 171–174, 2017.

[62] International Business Machines Corporation (USA), "IBM makes quantum computing available on IBM cloud", `www.research.ibm.com/ibm-q/`.

[63] Intel Corporation (USA), "Intel invests 50 million dollars to advance quantum computing", `https://newsroom.intel.com/news-releases/intel-invests-us50-million-to-advance-quantum-computing/`.

[64] J. Kelly, R. Barends, A. G. Fowler, A. Megrant, E. Jeffrey, T. C. White, D. Sank, J. Y. Mutus, B. Campbell, Y. Chen, Z. Chen, B. Chiaro, A. Dunsworth, I.-C. Hoi, C. Neill, P. J. J. O'Malley, C. Quintana, P. Roushan, A. Vainsencher, J. Wenner, A. N. Cleland, and J. M. Martinis, "State preservation by repetitive error detection in a superconducting quantum circuit", *Nature*, vol. 519, no. 7541, pp. 66–69, 2015.

[65] T. Pellizzari, S. A. Gardiner, J. I. Cirac, and P. Zoller, "Decoherence, continuous observation, and quantum computing : A cavity QED model", *Phys. Rev. Lett.*, vol. 75, pp. 3788–3791, Nov 1995.

[66] Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi, and H. J. Kimble, "Measurement of conditional phase shifts for quantum logic", *Phys. Rev. Lett.*, vol. 75, pp. 4710–4713, Dec 1995.

[67] A. Rauschenbeutel, G. Nogues, S. Osnaghi, M. Raimond J. M. Bertet, P.and Brune, and S. Haroche, "Coherent operation of a tunable quantum phase gate in cavity QED", *Phys. Rev. Lett.*, vol. 83, pp. 5166–5169, Dec 1999.

[68] D. Loss and D. P. DiVIcenzo, "Quantum computation with quantum dots", *Phys. Rev. A*, vol. 57, pp. 120–126, Jan 1998.

[69] H. Kamada, "Quantum computing with QD excitons", *NTT Tech. Rev.*, vol. 1, no. 3, pp. 31–40, 2003.

[70] X. Li, Y. Wu, D. Steel, D. Gammon, T. H. Stievater, D. S. Katzer, D. Park, C. Piermarocchi, and L. J. Sham, "An all-optical quantum gate in a semiconductor quantum dot", *Science*, vol. 301, no. 5634, pp. 809–811, 2003.

[71] T. Calarco, A. Datta, E. Pazy, and P. Zoller, "Spin-based all-optical quantum computation with quantum dots : Understanding and suppressing decoherence", *Phys. Rev. A*, vol. 68, pp. 012310, Jul 2003.

[72] D. Press, T. D. Ladd, B. Zhang, and Y. Yamamoto, "Complete quantum control of a single quantum dot spin using ultrafast optical pulses", *Nature*, vol. 456, pp. 218–221, 2008.

[73] P. Shor, "Scheme for reducing decoherence in quantum computer memory", *Phys. Rev. A*, vol. 52, pp. R2493–R2496, Oct 1995.

[74] A. M. Steane, "Error correcting codes in quantum theory", *Phys. Rev. Lett.*, vol. 77, pp. 793–797, Jul 1996.

[75] E. Knill and R. Laflamme, "Theory of quantum error-correcting codes", *Phys. Rev. A*, vol. 55, pp. 900–911, Feb 1997.

[76] E. Knill, R. Laflamme, and W.H. Zurek, "Resilient quantum computation", *Science*, vol. 279, no. 5249, pp. 342–345, 1998.

[77] A. M. Steane, "Efficient fault-tolerant quantum computing", *Nature*, vol. 399, pp. 124–126, 1999.

[78] J. Chiaverini, D. Leibfried, T. Schaetz1, M. D. Barrett, R. B. Blakestad, J. Britton, W. M. Itano, J. D. Jost, E. Knill, C. Langer, R. Ozeri, and D. J. Wineland, "Realization of quantum error correction", *Nature*, vol. 432, pp. 602–605, 2004.

[79] E. Knill, "Quantum computing with realistically noisy devices", *Nature*, vol. 434, pp. 39–44, 2005.

[80] P. Schindler, J. T. Barreiro, T. Monz, V. Nebendahl, D. Nigg, M. Chwalla, M. Hennrich, and R. Blatt, "Experimental repetitive quantum error correction", *Science*, vol. 332, no. 6033, pp. 1059–1061, 2011.

[81] N. Ofek, A. Petrenko, R. Heeres, P. Reinhold, Z. Leghtas, B. Vlastakis, Y. Liu, L. Frunzio, S. M. Girvin, L. Jiang, M. Mirrahimi, M. H. Devoret, and R. J. Schoelkopf, "Extending the lifetime of a quantum bit with error correction in superconducting circuits", *Nature*, vol. 536, no. 7617, pp. 441–445, 2016.

[82] D. P. DiVicenzo, "The physical implementation of quantum computation", *Fortschritte der Physik*, vol. 48, pp. 771–783, 2000.

[83] J. Thomson, "An integrating machine having a new kinematic principle", *Proc. R. Soc. Lond.*, vol. 24, pp. 262–265, 1875.

[84] W. J. Cairns, J. Crank, and E.C. Lloyd, "Some improvements in the construction of a small scale differential analyser and a review of recent applications", *Techical report*, vol. 27/44, Armament Research Department Theoretical Research ; 1944. UK National Archives reference DEFE 15/751 C20779.

[85] S. Lloyd, "Universal quantum simulators", *Science*, vol. 273, no. 5278, pp. 1073–1078, 1996.

[86] T. Schweigler, V. Kasper, S. Erne, I. Mazets, B. Rauer, F. Cataldini, T. Langen, T. Gasenzer, J. Berges, and J. Schmiedmayer, "Experimental characterization of a quantum many-body system via higher-order correlations", *Nature*, vol. 545, no. 7654, pp. 323–326, 2017.

[87] E. Manousakis, "A quantum-dot array as model for copper-oxide superconductors : a dedicated quantum simulator for the many-fermion problem", *J. Low. Temp.*, vol. 126, pp. 1501–1513, 2002.

[88] L. A. Wu, M. S. Byrd, and D. A. Lidar, "Polynomial-time simulation of pairing models on a quantum computer", *Phys. Rev. Lett.*, vol. 89, pp. 057904, Jul 2002.

[89] C. A. Regal, M. Greiner, and D. S. Jin, "Observation of resonance condensation of fermionic atom pairs", *Phys. Rev. Lett.*, vol. 92, pp. 040403, Jan 2004.

[90] M. W. Zwierlein, J. B. Abo-Shaeer, A. Schirotzek, C. H. Schunck, and W. Ketterle, "Vortices and superfluidity in a strongly interacting Fermi gas", *Nature*, vol. 435, pp. 1047–1051, 2005.

[91] T. Hensgens, T. Fujita, L. Janssen, X. Li, C. J. Van Diepen, C. Reichl, W. Wegscheider, S. D. Sarma, and L. M. K. Vandersypen, "Quantum simulation of a fermi–hubbard model using a semiconductor quantum dot array", *Nature*, vol. 548, pp. 70–73, 2017.

[92] K. Kim, M. S. Chang, S. Korenblit, R. Islam, E. E. Edwards, J. K. Freericks, G. D. Lin, L. M. Duan, and C. Monroe, "Quantum simulation of frustrated Ising spins with trapped ions", *Nature*, vol. 465, pp. 590–593, 2010.

[93] J. Struck, C. Ölschläger, R. L. Targat, P. Soltan-Panahi, A. Eckardt, M. Lewenstein, P. Windpassinger, and K. Sengstock, "Quantum simulation of frustrated classical magnetism in triangular optical lattices", *Science*, vol. 333, no. 6045, pp. 996–999, 2011.

[94] J. Zhang, M. Man-Hong Yung, R. Laflamme, A. Aspuru-Guzik, and J. Baugh, "Digital quantum simulation of the statistical mechanics of a frustrated magnet", *Nat. Commun.*, vol. 3, no. 880, 2012.

[95] C. Negrevergne, R. Somma, G. Ortiz, E. Knill, and R. Laflamme, "Liquid-state NMR simulations of quantum many-body problems", *Phys. Rev. A*, vol. 71, pp. 032344, Mar 2005.

[96] L. Lamata, J. León, T. Schätz, and E. Solano, "Dirac equation and quantum relativistic effects in a single trapped ion.", *Phys. Rev. Lett.*, vol. 98, pp. 253005, Jun 2007.

[97] R. Gerritsma, G. Kirchmair, F. Zähringer, E. Solano, R. Blatt, and C. F. Roos, "Quantum simulation of the Dirac equation", *Nature*, vol. 463, pp. 68–71, 2010.

[98] R. Gerritsma, B. P. Lanyon, G. Kirchmair, F ; Zähringer, C. Hempel, J. Casanova, J. J. García-Ripoll, E. Solano, R. Blatt, and C. F. Roos, "Quantum simulation of the Klein paradox with trapped ions", *Phys. Rev. Lett.*, vol. 106, pp. 060503, Feb 2011.

[99] J. Dalibard, F. Gerbier, G. Juzeliunas, and P. Öhberg, "Colloquium : artificial gauge potentials for neutral atoms", *Rev. Mod. Phys.*, vol. 83, pp. 1523–1543, Nov 2011.

[100] U. J. Wiese, "Ultracold quantum gases and lattice systems : quantum simulation of lattice gauge theories", *Annalen der Physik*, vol. 525, no. 10/11, pp. 776–796, 2013.

[101] S. Barrett, K. Hammerer, S. Harrison, T. E. Northup, and T. J. Osborne, "Simulating quantum fields with cavity QED", *Phys. Rev. Lett.*, vol. 110, pp. 090501, Feb 2013.

[102] D. Marcos, P. Rabl, E. Rico, and P. Zoller, "Superconducting circuits for quantum simulation of dynamical gauge fields", *Phys. Rev. Lett.*, vol. 111, pp. 110504, Sep 2013.

[103] U. R. Fischer and R. Schützhold, "Quantum simulation of cosmic inflation in two-component Bose-Einstein condensates", *Phys. Rev. A*, vol. 70, pp. 063615, Dec 2004.

[104] R. Schützhold, M. Uhlmann, L. Petersen, H. Schmitz, A. Friedenauer, and T. Schätz, "Analogue of cosmological particle creation in an ion trap", *Phys. Rev. Lett.*, vol. 99, pp. 201301, Nov 2007.

[105] G. E. Volovik, *The Universe in a Helium Droplet*, Oxford University Press, 2009.

[106] P. M. Alsing, J. P. Dowling, and G. J. Milburn, "Ion trap simulations of quantum fields in an expanding universe", *Phys. Rev. Lett.*, vol. 94, pp. 220401, Jun 2005.

[107] N. Szpak and R. Ralf Schützhold, "Quantum simulator for the Schwinger effect with atoms in bichromatic optical lattices", *Phys. Rev. A*, vol. 84, pp. 050101, Nov 2011.

[108] N. Szpak and R. Ralf Schützhold, "Optical lattice quantum simulator for quantum electrodynamics in strong external fields : spontaneous pair creation and the Sauter–Schwinger effect", *New J. Phys.*, vol. 14, no. 035001, 2012.

[109] S. Giovanazzi, "Hawking radiation in sonic black holes", *Phys. Rev. Lett.*, vol. 94, pp. 061302, Feb 2005.

[110] B. Horstmann, S. Reznik, B. Fagnocchi, and J. I. Cirac, "Hawking radiation from an acoustic black hole on an ion ring", *Phys. Rev. Lett.*, vol. 104, pp. 250403, Jun 2010.

[111] P. D. Nation, M. P. Blencowe, A. J. Rimberg, and E. Buks, "Analogue Hawking radiation in a dc-SQUID array transmission line", *Phys. Rev. Lett.*, vol. 103, pp. 087004, Aug 2009.

[112] T. G. Philbin, C. Kuklewicz, S. Robertson, S. Hill, F. Konig, and U. Leonhardt, "Fiber-optical analog of the event horizon", *Science*, vol. 319, no. 5868, pp. 1367–1370, 2008.

[113] J. Q. You and F. Nori, "Atomic physics and quantum optics using superconducting circuits", *Nature*, vol. 474, pp. 589–597, 2011.

[114] I. M. Georgescu, S. Ashhab, T. Nakatsukasa, and F. Nori, "Analog quantum simulation of the atomic nucleus with a fermionic condensat", 2011, Non publié actuellement.

[115] D. D. Leibfried, B. DeMarco, V. Meyer, M. Rowe, A. Ben-Kish, J. Britton, W. M. Itano, C. Jelenković, B. and. Langer, T. Rosenband, and Wineland D. J., "Trapped-ion quantum simulator : Experimental application to nonlinear interferometers", *Phys. Rev. Lett.*, vol. 89, pp. 247901, Nov 2002.

[116] Y. M. Hu, M. Feng, and C. Lee, "Adiabatic Mach-Zehnder interferometer via an array of trapped ions", *Phys. Rev. A*, vol. 85, pp. 043604, Apr 2012.

[117] H. K. Lau and D. F. V. James, "Proposal for a scalable universal bosonic simulator using individually trapped ions", *Phy*, vol. 85, no. 062329, 2012.

[118] U. L. Andersen, "Quantum optics : Squeezing more out of ligo", *Nat. Photonics*, vol. 7, pp. 589–590, 2013.

[119] R. McConnell, H. Zhang, J. Hu, S. Ćuk, and V. Vuletić, "Entanglement with negative Wigner function of almost 3,000 atoms heralded by one photon", *Nature*, vol. 519, no. 7544, pp. 439–442, 2014.

[120] N. J. Engelsen, R. Krishnakumar, O. Hosten, and M. A. Kasevich, "Bell correlations in spin-squeezed states of 500 000 atoms", *Phys. Rev. Lett.*, vol. 118, pp. 140401, Apr 2017.

[121] J. B. Clark, F. Lecocq, R. W. Simmonds, J. Aumentado, and J. D. Teufel, "Sideband cooling beyond the quantum backaction limit with squeezed light", *Nature*, vol. 541, pp. 191–195, 2017.

[122] A. Facon, E. V. Dietsche, D. Grosso, S. Haroche, J. M. Raimond, and S. Gleyzes, "A sensitive electrometer based on a Rydberg atom in a Schrödinger-cat state", *Nature*, vol. 535, no. 7611, pp. 262–265, 2016.

[123] P. Walther, J.-W. Pan, M. Aspelmeyer, R. Ursin, S. Gasparoni, and A. Zeilinger, "De Broglie wavelength of a non-local four-photon state", *Nature*, vol. 429, pp. 158–161, 2004.

[124] M. W. Mitchell, J. S. Lundeen, and A. M. Steinberg, "Super-resolving phase measurements with a multiphoton entangled state", *Nature*, vol. 429, pp. 161–164, 2004.

[125] Higgins, D. W. B. L. Berry, S. D. Bartlett, H. M. Wiseman, and G. J. Pryde, "Entanglement-free Heisenberg-limited phase estimation", *Nature*, vol. 450, pp. 393–396, 2007.

[126] T. Nagata, R. Okamoto, J. L. O'Brien, K. Sasaki, and S. Takeuchi, "Beating the standard quantum limit with four-entangled photons", *Science*, vol. 316, no. 5825, pp. 726–729, 2007.

[127] I. Afek, O. AMbar, and Y. Silberberg, "High-N00N states by mixing quantum and classical light", *Science*, vol. 328, no. 5980, pp. 879–881, 2010.

[128] Y. Israel, S. Rosen, and Y. Silberberg, "Supersensitive polarization microscopy using N00N states of light", *Phys. Rev. Lett.*, vol. 112, pp. 103604, Mar 2014.

[129] LIGO Scientific Collaboration and Virgo Collaboration, "Observation of gravitational waves from a binary black hole merger", *Phys. Rev. Lett.*, vol. 116, pp. 061102, Feb 2016.

[130] Y. Ma, H. Miao, B. Heyun, H. Pang, P. Matthew, M. Evans, C. Zhao, J. Harms, R. Schnabel, and Y. Chen, "Proposal for gravitational-wave detection beyond the standard quantum limit through EPR entanglement", *Nat. Phys.*, , no. 4118, 2017.

[131] W. Heisenberg, "Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik", *Zeitschrift für Physik*, vol. 43, no. 3/4, pp. 172–198, 1927.

[132] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned", *Nature*, vol. 299, pp. 802–803, 1982.

[133] Z. L. Yuan, B. E. Kardynal, A. W. Sharpe, and A. J. Shields, "High speed single photon detection in the near infrared", *Appl. Phys. Lett.*, vol. 91, 2007.

[134] A. R. Dixon, J. F. Dynes, A. W. Sharpe, A. J. Bennett, and A. J. Shields, "Ultrashort dead time of photon-counting InGaAs avalanche photodiodes", *Appl. Phys. Lett.*, vol. 94, 2009.

[135] N. Namekata, S. Sasamori, and S. Inoue, "800 MHz single photon detection at 1550-nm using InGaAs/InP avalanche photodiode operated with a sine wave gating", *Opt. Express*, vol. 14, 2006.

[136] X. L. Liang, Liu J. H., Q. Wang, D. B. Du, J. Ma, G. Jin, Cen Z. B., J. Zhang, and J. W. Pan, "Fully integrated InGaAs/InP single-photon detector module with gigahertz sine wave gating.", *Rev. Sci. Instrum.*, vol. 83, 83.

[137] Q.-L. Wu, N. Namekata, and S. Inoue, "Sinusoidally gated InGaAs avalanche photodiode with direct hold-off function for efficient and low-noise single-photon detection", *Appl. Phys. Express*, vol. 6, 2013.

[138] J. Zhang, R. Thew, C. Barreiro, and H. Zbinden, "Practical fast gate rateInGaAs/InP single-photon avalanche photodiodes", *Appl. Phys. Lett.*, vol. 95, 2009.

[139] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam, "Detecting single infrared photons with 93% system efficiency", *Nat. Photonics*, vol. 7, pp. 210–214, 2013.

[140] D. Rosenberg, A. J. Kerman, R. J. Molnar, and E. A. Dauler, "High-speed and high-efficiency superconducting nanowire single photon detector array", *Opt. Express*, vol. 21, 2013.

[141] S. Miki, T. Yamashita, H. Terai, and Z. Wang, "High performance fiber-coupled NbTiN superconducting nanowire single photon detectors with Gifford-McMahon cryocooler", *Opt. Express*, vol. 21, 2013.

[142] M. Herrero-Collantes, "Quantum randomnumber generators", *Rev. Mod. Phys.*, vol. 89, pp. 015004, Feb 2017.

[143] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, "A fast and compact quantum random number generator", *Rev. Sci. Instrum.*, vol. 71, pp. 1675–1680, 2000.

[144] P. X. Wang, "Scheme for a quantum random number generator", *J. Appl. Phys.*, vol. 100, no. 056107, 2006.

[145] M. Naruse, M. Berthel, A. Drezet, S. Huant, M. Aono, H. Hori, and S. J. Kim, "Single-photon decision maker", *Sci. Rep.*, vol. 5, no. 13253, 2015.

[146] M. Stipcevic and M. Rogina, "Quantum random number generator based on photonic emission in semiconductors", *Rev. Sci. Instrum.*, vol. 78, no. 045104, 2007.

[147] M. A. Wayne, E. R. Jeffrey, G. M. Arkselrod, and P. Kwiat, "Photon arrival time quantum random number generation", *J. Mod. Opt.*, vol. 56, pp. 516–522, 2009.

[148] M. Wahl, M. Leifgen, M. Berlin, T. Röhlicke, H. J. Rahn, and O. Benson, "An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements", *Appl. Phys. Lett.*, vol. 98, no. 171105, 2011.

[149] M. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, "High speed optical quantum random number generation", *Opt. Express*, vol. 18, pp. 13029–13037, 2010.

[150] M. Ren, E. Wu, Y. Liang, Y. Jian, G. Wu, and H. Zeng, "Quantum random-number generator based on a photon-number-resolving detector", *Phys. Rev. A*, vol. 83, pp. 023820, Feb 2011.

[151] P. J. Bustard, D. Moffatt, R. Lausten, G. Wu, I. A. Walmsley, and B. J. Sussman, "Quantum random bit generation using stimulated Raman scattering", *Opt. Express*, vol. 19, pp. 25173–25180, 2011.

[152] M. J. Collins, A. S. Clark, Xiong C., E. Mägi, M. J. Steel, and B. J. Eggleton, "Random number generation from spontaneous Raman scattering", *Appl. Phys. Lett.*, vol. 107, no. 141112, 2015.

[153] B. Qi, Y. M. Chi, H. K Lo, and L. Qian, "High-speed quantum random number generation by measuring phase noise of a single-mode laser", *Opt. Lett.*, vol. 35, no. 3, pp. 312–314, 2010.

[154] F. Xu, B. Qi, X. Ma, H. Zheng, and H. K. Lo, "Ultrafast quantum random number generation based on quantum phase fluctuations", *Opt. Express*, vol. 20, no. 12366, 2012.

[155] C. Abellan, W. Amaya, M. Jofre, M Curty, A. Acín, J. Capmany, V. Pruneri, and M. W. Mitchell, "Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode", *Opt. Express*, vol. 22, no. 1645, 2014.

[156] H. Zhou, W. Yan, and X. Ma, "Randomness generation based on spontaneous emissions of lasers", *Phys. Rev. A*, vol. 91, pp. 062316, Jun 2015.

[157] Y. Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J. W. Pan, "The generation of 68 Gbps quantum random number by measuring laser phase fluctuations,", *Rev. Sci. Instrum.*, vol. 86, no. 063105, 2015.

[158] R. Caitlin, S. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, "Fast physical random number generator using amplified spontaneous emission", *Opt. Express*, vol. 18, pp. 23584–23597, 2010.

[159] X. Li, A. B. Cohen, T. E. Murphy, and R. Roy, "Scalable parallel physical random number generator based on a super-luminescent led", *Opt. Lett.*, vol. 36, no. 1020, 2011.

[160] Y. Liu, M. Y. Zhu, B. Luo, J. W. Zhang, and H. Guo, "Implementation of 1.6 tb s^{-1} truly random number generation based on a super-luminescent emitting diode", *Laser Phys. Lett.*, vol. 10, no. 4, 2013.

[161] L. Li, A. Wang, P. Li, H. Xu, L. Wang, and Y. Wang, "Random bit generator using delayed self-difference of filtered amplified spontaneous emission", *IEEE Photonics J.*, vol. 6, pp. 1–9, 2014.

[162] A. Martin, B. Sanguinetti, C. C. W. Lim, R. Houlmann, and H. Zbinden, "Quantum random number generation for 1.25-GHz quantum key distribution systems", *J. Lightwave Technol.*, vol. 33, no. 13, pp. 2855–2859, 2015.

[163] C. Gabriel, C ; Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, "A generator for unique quantum random numbers based on vacuum states,", *Nat. Photonics*, vol. 4, pp. 711–715, 2010.

[164] Y. Shen, L. Tian, and H. Zou, "Practical quantum random number generator based on measuring the shot noise of vacuum state", *Phys. Rev. A*, vol. 81, pp. 063814, Jun 2010.

[165] T. Symul, S. M. Assad, and P. K. Lam, "Real time demonstration of high bitrate quantum random number generation with coherent laser light", *Appl. Phys. Lett.*, vol. 98, no. 231103, 2011.

[166] Y. G. Zhu and G. Zeng, "Unbiased quantum random number generation based on squeezed vacuum state", *Int. J. Quantum Inf.*, vol. 10, no. 1250012, 2010.

[167] B. Sanguinetti, A. Martin, H. Zbinden, and Gisin. N., "Quantum random number generation on a mobile phone", *Phys. Rev. X*, vol. 4, pp. 031056, Sep 2014.

[168] C. Kollmitzer and M. Pivk, *Applied Quantum Cryptography*, vol. 797 of *Lecture notes in Physics*, Springer, 2010.

[169] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, "Provably secure and practical quantum key distribution over 307 km of optical fibre", *Nat. Photonics*, vol. 9, pp. 163–168, 2015.

[170] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a plug and play system", *New J. Phys.*, vol. 4, pp. 1–8, 2002.

[171] P. P. Rohde, J. F. Fitzsimons, and A. Gilchrist, "Quantum walks with encrypted data", *Phys. Rev. Lett.*, vol. 109, pp. 150501, Oct 2012.

[172] A. M. Childs, "Secure assisted quantum computation", *Quant. Inf. Comp.*, vol. 5, no. 6, pp. 456–466, 2005.

[173] C. H. Bennett and G. Brassard, "Quantum cryptography : Public key distribution and coin tossing", *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175–179, 10-12 December, 1984.

[174] H. K Lo and H. Chau, "Why quantum bit commitment and ideal quantum coin tossing are impossible", *Phys. D Nonlinear Phenom.*, vol. 120, no. 1-2, pp. 177–187, 1998.

[175] D. Mayers, "Unconditionally secure quantum bit commitment is impossible", *Phys. Rev. Lett.*, vol. 78, pp. 3414–3417, Apr 1997.

[176] A. Chailloux and I. Kerenidis, "Optimal quantum strong coin flipping", *2009 50th Annu. IEEE Symp. Found. Comput. Sci.*, pp. 527–533, 2009, IEEE.

[177] D. Unruh, "Quantum proof of knowledge", *Eurocrypt 2012*, vol. 7237, pp. 135–152, 2012, Springer.

[178] A. Ambainis, A. Rosmanis, and D. Unruh, "Quantum attacks on classical proof system : The hardness of quantum rewinding"", *IEEE 55th Annual Symposium on Foundations of Computer Science*, pp. 474–483, 2014.

[179] S. Wiesner, "Conjugate coding", *ACM SIGACT News*, vol. 15, no. 1, pp. 78–88, 1983.

[180] A. Chailloux, G. Gutoski, and J. Sikora, "Optimal bounds for quantum weak oblivious transfer", *arXiv :1310.3262*, 2013.

[181] G. Brassard, C. Crépeau, D. Mayers, and L. Salvail, "A brief review on the impossibility of quantum bit commitment", *arXiv : quant-ph/9712023*, 1997.

[182] France Stratégie, "Demain, l'internet des objets", `www.strategie.gouv.fr/publications/demain-linternet-objets`.

[183] National Institute of Standards and Technology (USA), "The NIST definition of cloud computing", `http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf`.

[184] International Business Machines Corporation (USA), "A Python library for the Quantum Experience API", `https://github.com/IBM/qiskit-api-py`.

[185] Bristol University Center for Quantum Photonic (UK), "Quantum in the Cloud", `https://cnotmz.appspot.com/`.

[186] J. L. O'Brien, G. J. Pryde, A. G. White, T. C. Ralph, and D. Branning, "Demonstration of an all-optical quantum controlled-NOT gate", *Nature*, vol. 426, pp. 264–267, 2013.

[187] S. J. Devitt, "Performing quantum computing experiments in the cloud", *Phys. Rev. A*, vol. 94, pp. 032329, Sep 2016.

[188] D. Alsina and J. I. Latorre, "Experimental test of Mermin inequalities on a five-qubit quantum computer", *Phys. Rev. A*, vol. 94, pp. 012314, Jul 2016.

[189] M. Berta, S. Wehner, and M. M. Wilde, "Entropic uncertainty and measurement reversibility", *New J. Phys.*, vol. 18, 2016.

[190] M. Hebenstreit, D. Alsina, J. I. Latorre, and B. B. Kraus, "Compressed quantum computation using a remote five-qubit quantum computer", *Phys. Rev. A*, vol. 95, pp. 052339, May 2017.

[191] E. Huffman and A. Mizel, "Violation of noninvasive macrorealism by a superconducting qubit : Implementation of a Leggett-Garg test that addresses the clumsiness loophole", *Phys. Rev. A*, vol. 95, pp. 032131, Mar 2017.

[192] N. M. Linke, D. Maslov, M. Roetteler, S. Debnath, C. Figgatt, K. Landsman, K. Wright, and C. Monroe, "Experimental comparison of two quantum computing architectures", *Proc. Natl. Acad. Sci.*, vol. 114, no. 13, pp. 3305–3310, 2017.

[193] International Business Machines Corporation (USA), "Students try hand at cracking quantum code", `https://www.ibm.com/blogs/research/2016/06/students-try-hand-cracking-quantum-code/`.

[194] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolosky-Rosen channels", *Phys. Rev. Lett.*, vol. 70, pp. 1895–1899, Mar 1993.

[195] D. Bouwmeester, J. W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, "Experimental quantum teleportation", *Nature*, vol. 390, pp. 575–579, 1997.

[196] I. Marcikic, H. de Riedmatten, W. Tittel, and N. Zbinden, H. ad Gisin, "Long-distance teleportation of qubits at telecommunication wavelengths.", *Nature*, vol. 421, pp. 509–513, 2003.

[197] R. Ursin, T. Jennewein, M. Aspelmeyer, R. Kaltenbaek, M. Lidenthal, P. Walther, and A. Zeilinger, "Quantum teleportation across the danube", *Nature*, vol. 430, pp. 849, 2004.

[198] J. Yin, J. G. Re, H. Lu, Y. Cao, H. L. Yong, Y. P. Wu, C. Liu, S. K. Liao, F. Zhou, Y. Jiang, X. D. Cai, G. S. Pan, J. J. Jia, Y. M. Huanf, H. Yin, J.-Y. WWang, Y. A. Chen, C. Z. Peng, and J. W. Pan, "Quantum teleportation and entanglement distribution over 100-kilometre free-space channels", *Nature*, vol. 488, pp. 185–188, 2012.

[199] X. S. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, J. Kofler, E. Anisimova, V. Makarov, T. Jennewein, R. Ursin, and A. Zeilinger, "Quantum teleportation over 143 kilometres using active feed-forward", *Nature*, vol. 489, pp. 269–273, 2012.

[200] X. L. Wang, X. D. Cai, Z. E. Su, M. C. Chen, D. Wu, L. Li, N. L. Liu, C. Y. Lu, and J. W. Pan, "Quantum teleportation of multiple degrees of freedom of a single photon", *Nature*, vol. 518, pp. 516–519, 2015.

[201] R. Valivarthi, M. G. Puigibert, Q. Zhou, G. H. Aguilar, V. B. Verma, F. Marsili, M. D. Shaw, S. W. Nam, D. Oblak, and W. Tittel, "Quantum teleportation across a metropolitan fibre network", *Nat. Photonics*, vol. 10, pp. 676–680, 2016.

[202] Q. C. Sun, Y. L Mao, S. J. Chen, W. Zhang, Y. F. Jiang, Y. B. Zhang, W. J. Zhang, S. Miki, T. Yamashita, H. Terai, X. Jiang, T. Y. Chen, L. X. You, H.X. F. Chen, Z. Wang, J. Y. Fan, Q. Zhang, and J. W. Pan, "Quantum teleportation with independent sources and prior entanglement distribution over a network", *Nat. Photonics*, vol. 10, pp. 671–675, 2016.

[203] A. Furusawa, A. Sorensen, and S. L. Braunstein, "Unconditional quantum teleportation", *Science*, vol. 282, no. 5389, pp. 706–709, 1998.

[204] H. Yonezawa, T. Aoki, and A. Furusawa, "Demonstration of a quantum teleportation network for continuous variables", *Nature*, vol. 431, pp. 430–433, 2004.

[205] H. Yonezawa, S. L. Braunstein, and A. Furusawa, "Experimental demonstration of quantum teleportation of broadband squeezing", *Phys. Rev. Lett.*, vol. 99, pp. 110503, Sep 2007.

[206] N. Lee, H. Benichi, Y. Takeno, S. Takeda, J. Webb, E. Huntington, and A. Furusawa, "Teleportation of nonclassical wave packets of light", *Science*, vol. 332, no. 6027, pp. 330–333, 2011.

[207] S. Takeda, T. Mizuta, M. Fuwa, P. van Loock, and A. Furusawa, "Deterministic quantum teleportation of photonic quantum bits by a hybrid technique", *Nature*, vol. 500, pp. 315–318, 2013.

[208] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein, "Advances in quantum teleportation", *Nat. Photonics*, vol. 9, pp. 641–652, 2015.

[209] J. Nunn, L. Wright, C. Soller, L. Zhang, I. A. Walmsley, and B. J. Smith, "Large-alphabet time-frequency entangled quantum key distribution by means of time-to-frequency conversion", *Opt. Express*, vol. 21, no. 13, pp. 15959–15973, 2013.

[210] Z. Zhang, J. Mower, D. Englund, F. N. C. Wong, and J. Shapiro, "Unconditional security of time-energy entanglement quantum key distribution using dual-basis interferometry", *Phys. Rev. Lett.*, vol. 112, pp. 120506, Mar 2014.

[211] D. Bunandar, Z. Zhang, J. Shapiro, and D. Englund, "Practical high-dimensional quantum key distribution with decoy states", *Phys. Rev. A*, vol. 91, pp. 022336, Feb 2015.

[212] T. Zhong, H. Zhou, R. D. Horansky, C. Lee, V. B. Verma, A. E. Lita, A. Restelli, J. C. Bienfant, R. P. Mirin, and T. Gerrits, "Photon-efficient quantum key distribution using time–energy entanglement with high-dimensional encoding", *New J. Phys.*, vol. 17, 2015.

[213] D. Aktas, B. Fedrici, F. Kaiser, T. Lunghi, L. Labonté, and S. Tanzilli, "Entanglement distribution over 150 km in wavelength division multiplexed channels for quantum cryptography", *Laser and Photon. Rev.*, vol. 10, no. 3, pp. 451–457, 2016.

[214] Z. Zhang, Q. Zhuang, F. N. C. Wong, and J. Shapiro, "Floodlight quantum key distribution : Demonstrating a framework for high-rate secure communication", *Phys. Rev. A*, vol. 95, pp. 012332, Jan 2017.

[215] M. Kues, C. Reimer, P. Roztocki, L. M. Cortés, S. Sciara, B. Wetzel, Y. Zhang, A. Cino, S. T. Chu, B. E. Little, D. J. Moss, L. Caspani, J. Azana, and R. Morandotti, "On-chip generation of high-dimensional entangled quantum states and their coherent control", *Nature*, vol. 546, pp. 622–626, 2017.

[216] T. Sasaki, Y. Yamamoto, and M. Koashi, "Practical quantum key distribution protocol whitout monitoring signal distrurbance", *Nature*, vol. 509, pp. 475–478, 2014.

[217] H. Takesue, H. Sasaki, K. Tamaki, and M. Koashi, "Experimental quantum key distribution without monitoring signal distrurbance", *Nat. Photonics*, vol. 9, pp. 827–831, 2015.

[218] S. Wang, Z. Q. Yin, W. Chen, D. Y. He, X. T. Song, H. W. Li, L. J. Zhang, Z. Zhou, G. C. Guo, and Z. F. Han, "Experimental demonstration of a quantum key distribution without signal disturbance monitoring", *Nat. Photonics*, vol. 9, pp. 827–831, 2015.

[219] J. Y. Guan, Y. Liu, G. L. Shen-Tu, J. S. Pelc, M. M. Fejer, C. Z. peng, X. Ma, zhang Q., and J. W. Pan, "Experimental passive round-robin differential phase-shift quantum key distribution", *Phys. Rev. Lett.*, vol. 114, pp. 180502, May 2015.

[220] R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution", *npj Quantum Information*, vol. 3, no. 30, 2017.

[221] G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, "Experimental satellite quantum communications", *Phys. Rev. Lett.*, vol. 115, pp. 040502, Jul 2015.

[222] J. Yin, Y. Cao, Y. H. Li, S. K. Liao, L. Zhang, J. G. Ren, W. Q. Cai, W. Y. Liu, B. Li, H. Dai, G. B. Li, Q. M Lu, Y. H. Gong, Y. Xu, S. L. Li, F. Z. Li, Y. Y. Yin, Z. Q. Jiang, M. Li, J. J. Jia, G. Ren, D. He, Y. L. Zhou, X. X. Zhang, N. Wang, X. Chang, Z. C. Zhu, N. L. Liu, Z. P. Chen, J. Y. Wang, and J. W. Pan, "Satellite-based entanglement distribution over 1200 kilometers", *Science*, vol. 356, no. 6343, pp. 1140–1444, 2017.

[223] J. G. Ren, P. Xu, H. L. Yong, L. Zhang, S. K. Liao, J. Yin, W. Y. Liu, W. Q. Cai, M. Yang, L. Li, K. X. Yang, X. Han, Y. Q. Yao, J. Li, H. Y. Wu, S. Wan, L. Liu, D. Q. Liu, Y. W. Kuang, Z. P. He, P. Shang, C. Guo, R. H. Zheng, K. Tian, Z. C. Zhu, N. L. Liu, C. H. Lu, R. Shu, Y. A. Chen, C. Z. Peng, J. Y. Wang, and J. W. Pan, "Ground-to-satellite quantum teleportation", *Nature*, 2017, Published online 09 August 2017.

[224] S. K. Liao, W. Q. Cai, W. L. Liu, L. Zhang, Y. Li, J. G. Ren, J. Yin, Q. Shen, Y. Cao, Z. P. Li, F. Z. Li, X. W. Chen, L. H. Sun, J. J. Jia, J. C. Wu, X. J. Jiang, J. F. Wang, Y. M. Huang, Q. Wang, Y. L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y-A. Chen, N. L. Liu, X. B. Wang, Z. C. Zhu, C. Y. Lu, R. Shu, C. Z. Peng, J. Y. Wang, and J. W. Pan, "Satellite-to-ground quantum key distribution", *Nature*, 2017, Published online 09 August 2017.

[225] N. Sanguard, C. Simon, H. de Riedmatten, and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics", *Rev. Mod. Phys.*, vol. 83, pp. 33–80, Mar 2011.

[226] K. Hammerer, A. Sorensen, and E. S. Polzik, "Quantum interface between light and atomic ensembles", *Rev. Mod. Phys.*, vol. 82, pp. 1041–1093, Apr 2010.

[227] D. I. Schuster, A. P. Sears, E. Ginossar, L. DiCarlo, L. Frunzio, J. J. L. Morton, H. Wu, G. A. D. Briggs, B. B. Buckley, D. D. Awschalom, and R. J. Schoelkopf, "High-cooperativity coupling of electron-spin ensembles to superconducting cavities", *Phys. Rev. Lett.*, vol. 105, pp. 140501, Sep 2010.

[228] Y. Kubo, F. R. Ong, P. Bertet, D. Vion, V. Jacques, D. Zheng, A. Dréau, J. F. Roch, A. Auffeves, F. Jelezko, J. Wrachtrup, M. F. Barthe, P. Bergonzo, and D. Esteve, "Strong coupling of a spin ensemble to a superconducting resonator", *Phys. Rev. Lett.*, vol. 105, pp. 140502, Sep 2010.

[229] H. Wu, R. E. George, J. H. Wesenberg, K. Molmer, D. I. Schuster, R. J. Schoelkopf, K. H. Itoh, A. Ardavan, J. J. L. Morton, and G. A. D. Briggs, "Storage of multiple coherent microwave excitations in an electron spin ensemble", *Phys. Rev. Lett.*, vol. 105, pp. 140503–140507, 2010.

[230] R. W. Andrews, R. W. Peterson, T. P. Purdy, K. Cicak, R. W. Simmonds, C. A. Regal, and K. W. Lehnert, "Bidirectional and efficient conversion between microwave and optical light", *Nat. Phys.*, vol. 10, pp. 321–326, 2014.

[231] B. Dyan, A. S. Parkins, T. Aoki, K. J. Vahala, and H. J. Kimble, "A photon turnstile dynamically regulated by one atom", *Science*, vol. 319, no. 5866, pp. 1062–1065, 2008.

[232] Z. S. Yan, Y. A. Chen, B. Zhao, S. Chen, J. Schmiedmayer, and J. W. Pan, "Experimental demonstration of a BDCZ quantum repeater node", *Nature*, vol. 454, pp. 1098–1101, 2008.

[233] H. P. Specht, C. Nolleke, G. lleke, A. Reiserer, M. Uphoff, E. Figueroa, S. Ritter, and G. Rempe, "A single-atom quantum memory", *Nature*, vol. 473, pp. 190–193, 2011.

[234] A. Reiserer, S. Ritter, and G. Rempe, "Nondestructive detection of an optical photon", *Science*, vol. 342, no. 6164, pp. 1349–1351, 2013.

[235] L. Li, Y. O. Dudin, and A. Kuzmich, "Entanglement between light and an optical atomic excitation", *Nature*, vol. 498, pp. 466–469, 2013.

[236] A. Reiserer, N. Kalb, G. Rempe, and S. Ritter, "A quantum gate between a flying optical photon and a single trapped atom", *Nature*, vol. 508, pp. 237–240, 2014.

[237] T. G. Tiecke, J. D. Thompson, N. P. de Leon, L. R. Liu, V. Vuletic, and M. D. Lukin, "Nanophotonic quantum phase switch with a single atom", *Nature*, vol. 508, pp. 241–244, 2014.

[238] I. Shomroni, S. Rosenblum, Y. Lovsky, O. Bechler, G. Guendelman, and B. Dayan, "All-optical routing of single photons by a one-atom switch controlled by a single photon", *Science*, vol. 345, no. 6199, pp. 903–906, 2014.

[239] E. Distante, P. Farrera, A. Padron-Bitro, D. Paredes-Barato, G. Heinze, and de Riedmatten H., "Storing single photons emitted by a quantum memory on a highly excited rydberg state", *Nat. Commun.*, vol. 8, no. 14072, 2017.

[240] E. Togan, Y. Chu, A. S. Trifonov, J. Jiang, J. Maze, L. Childress, M. V. G. Dutt, A. S. Sorensen, P. R. Hemmer, A. S. Zibrov, and M. D. Lukin, "Quantum entanglement between an optical photon and a solid-state spin qubit", *Nature*, vol. 466, pp. 730–734, 2010.

[241] C. Clausen, I. Usmani, F. Bussières, N. Sangouard, M. Afzelius, de Riedmatten H., and N. Gisin, "Quantum storage of photonic entanglement in a crystal", *Nature*, vol. 469, pp. 508–511, 2011.

[242] H. Bernien, B. Hensen, W. Pfaff, G. Koolstra, M. S. Blok, L. Robledo, T. H. Taminiau, M. Markham, D. J. Twitchen, L. Childress, and R. Hanson, "Heralded entanglement between solid-state qubits separated by three metres", *Nature*, vol. 497, pp. 86–90, 2013.

[243] W. Pfaff, B. J. Hensen, H. Bernien, S. B. van Dam, M. S. Blok, T. H. Taminiau, M. J. Tiggelman, R. N. Schouten, M. Markham, D. J. Twitchen, and R Hanson, "Unconditional quantum teleportation between distant solid-state quantum bits", *Science*, vol. 345, pp. 532–535, 2014.

[244] N. Kosaka, H.and Niikura, "Entangled absorption of a single photon with a single spin in diamond", *Phys. Rev. Lett.*, vol. 114, pp. 053603, Feb 2015.

[245] S. Yang, Y. Wang, D. D. B. Rao, T. H. Tran, A. S. Momenzadeh, M. Markham, D. J. Twitchen, P. Wang, W. Yang, R. Stöhr, P. Neumann, H. Kosaka, and J. Wrachtrup, "High-fidelity transfer and storage of photon states in a single nuclear spin", *Nat. Photonics*, vol. 10, pp. 507–511, 2016.

[246] Z. L. Xiang, S. Ashhab, J. Q. You, and F. Nori, "Hybrid quantum circuits : Superconducting circuits interacting with other quantum systems", *Rev. Mod. Phys.*, vol. 85, pp. 623–653, Apr 2013.

[247] U. Leonhardt, *Measureing the Quantum State of Light*, Cambridge Studies in Modern Optics. Cambridge University Press, 1997.

[248] M. O. Scully and M. S. Zubairy, *Quantum Optcs*, Cambridge University Press, 1997.

[249] R. Loudon, *The Quantum Theory of Light*, Oxford University Press, third edition, 2000.

[250] D. F. Walls and G. J. Milburn, *Quantum Optics*, Springer, second edition, 2008.

[251] R. Boyd, *Nonlinear Optics*, Academic Press, third edition, 2008.

[252] G. Grynberg, A. Aspect, and C. Fabre, *Introduction to Quantum Optics : From the Semi-classical Approach to Quantized Light*, Cambridge University Press, 2010.

[253] S. Fasel, O. Alibart, S. Tanzilli, H. Zbinden, P. Baldi, and N. Gisin, "High quality asynchronous heralded single photon source at telecom wavelength", *New J. Phys.*, vol. 6, pp. 163, 2004.

[254] L. A. Ngah, O. Alibart, L. Labonté, V. D'Auria, and S. Tanzilli, "Ultra-fast heralded single photon source based on telecom technology", *Laser and Photon. Rev.*, vol. 9, no. 2, pp. 1–5, 2015.

[255] C. K. Hong, Z. Y. Ou, and L. Mandel, "Measurement of subpicosecond time intervals between two photons by interference", *Phys. Rev. Lett.*, vol. 59, pp. 2044–2046, Nov 1987.

[256] R. Kaltenbaek, B. Blauensteiner, M. Zukowski, M. Aspelmeyer, and A. Zeilinger, "Experimental interference of independent photons", *Phys. Rev. Lett.*, vol. 96, pp. 240502, Jun 2006.

[257] R. Kaltenbaek, R. Prevedel, M. Aspelmeyer, and A. Zeilinger, "High-fidelity entanglement swapping with fully independent sources", *Phys. Rev. A*, vol. 79, pp. 040302, Apr 2009.

[258] M. Halder, A. Beveratos, N. Gisin, V. Scarani, C. Simon, and H. Zbinden, "Entangling independent photons by time measurement", *Nat. Phys.*, vol. 3, pp. 692–695, 2007.

[259] G. Sobon and K. Abramski, "Fiber-based laser frequency combs", *Bulletin of the Polish Academy of Sciences, Technical Sciences*, vol. 60, pp. 697–706, 02 2013.

[260] E. Desurvire, *Erbium-Doped Fiber Amplifiers : Principles and Applications*, Wiley, 1994.

[261] A. Martin, *Puces photoniques pour la communication quantique longue distance*, PhD thesis, Université Nice Sophia Antipolis, 2011.

[262] L. G. Cohen, C. Lin, and W. G. French, "Tailoring zero chromatic dispersion into the 1.5 μm-1.6 μm low-loss spectral region of single-mode fibres", *Electron. Lett.*, vol. 15, no. 12, pp. 334, 1979.

[263] S. Fasel, N. Gisin, G. Ribordy, and 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", *Euro. Phys. J. D.*, vol. 30, no. 1, pp. 143–148, 2004.

[264] J. W. Berthold and S. F. Jacobs, "Ultraprecise thermal expension measurements of seven low expension materials", *Appl. Opt.*, vol. 15, pp. 2344–2347, 1976.

[265] R. E. Slusher, L. W. Hollberg, B. Yurke, J. C. Mertz, and J. F. Valley, "Observation of squeezed states generated by four-wave mixing in an optical cavity", *Phys. Rev. Lett.*, vol. 55, no. 22, pp. 2409–2412, 1986.

[266] R. M. Shelby, M. D. Levenson, S. H. Perlmutter, R. G. DeVoe, and D. F. Walls, "Broad-band parametric deamplification of quantum noise in an optical fiber", *Phys.Rev. Lett.*, vol. 57, no. 6, pp. 691–694, 1986.

[267] L. A. Wu, H. J. Kimble, and H. Wu, "Generation of squeezed states by parametric down conversion", *Phys. Rev. Lett.*, vol. 57, no. 20, pp. 2520–2523, 1986.

[268] T. Eberle, S. Steinlechner, J. Bauchrowitz, V. Handchen, H. Vahlbruch, M. Mehmet, H. Muller-Ebhardt, and R. Schnabel, "Quantum enhancement of the zero-area sagnac interferometer topology for gravitational wave detection", *Phys. Rev. Lett.*, vol. 104, no. 25, pp. 251102–251106, 2010.

[269] T. Eberle, V. Handchen, and R. Schnabel, "Stable control of 10 db two-mode squeezed vacuum states of light", *Opt. Express*, vol. 21, no. 9, pp. 11546–11553, 2013.

[270] H. Vahlbruch, M. Mehmet, K. Danzmann, and R. Schnabel, "Detection of 15 db squeezed states of light and their application for the absolute calibration of photoelectric quantum efficiency", *Phys. Rev. Lett.*, vol. 117, no. 11, pp. 110801–110806, 2016.

[271] G. Masada, K. Miyata, A. Politi, T. Hashimoto, J. L. O'Brien, and A. Furusawa, "Continuous-variable entanglement on a chip", *Nat. Photonics*, vol. 9, pp. 316–319, 2015.

[272] Y. Eto, T. Tajima, Y. Zhang, and T. Hirano, "Observation of squeezed light at 1.535 μm using a pulsed homodyne detector", *Opt. Express*, vol. 32, no. 12, pp. 1698–1700, 2007.

[273] J. Appel, D. Hoffman, E. Figueroa, and A. I. Lvovsky, "Electronic noise in optical homodyne tomography", *Phys. Rev. A*, vol. 75, no. 3, pp. 035802, 2007.

[274] S. Ast, A. Samblowski, M. Mehmet, S. Steinlechner, T. Eberle, and R. Schnabel, "Continuous-wave nonclassical light with gigahertz squeezing bandwidth", *Opt. Lett.*, vol. 37, no. 12, pp. 2367–2369, 2012.

[275] J. Roslund, R. M. Araujo, S. Jiang, C. Fabre, and N. N. Treps, "Wavelength-multiplexed quantum networks with ultrafast frequency combs", *Nat. Photonics*, vol. 8, pp. 109–112, 2013.

[276] T. Hirano, K. Kotani, T. Ishibashi, S. Okude, and T. Kuwamoto, "3 db squeezing by single-pass parametric amplification in a periodically poled $ktiopo_4$", *Opt. Lett.*, vol. 30, no. 13, pp. 1722–1724, 2005.

[277] T. Umeki, O. Tadanaga, and M. Asobe, "Highly efficient wavelength converter using direct-bonded PPZnLN ridge waveguide", *IEEE J. Quantum Electron.*, vol. 46, no. 8, pp. 1206–1213, 2010.

[278] K. Yoshino, T. Aoki, and A. Furusawa, "Generation of continuous-wave broadband entangled beams using periodically poled lithium niobate waveguides", *App. Phys. Lett.*, vol. 90, pp. 041111–041113, 2007.

[279] A. Gerthoffer, C. Guyot, W. Qiu, A. Ndao, M. P. Bernal, and N. Courjal, "Strong reduction of propagation losses in $linbo_3$ ridge waveguides", *Opt. Matter.*, vol. 38, pp. 37–41, 2014.

[280] M. Mehmet, S. Ast, T. Eberle, S. Steinlechner, H. Vahlbruch, and R. Schnabel, "Squeezed light at 1550 nm with a quantum noise reduction of 12.3 dB", *Opt. Express*, vol. 19, no. 25, pp. 25763–25772, 2011.

[281] L. M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, "Inseparability criterion for continuous variable systems", *Phys. Rev. Lett.*, vol. 84, no. 12, pp. 2722–2725, 2000.

[282] F. Kaiser, B. Fedrici, A. Zavatta, V. D'Auria, and S. Tanzilli, "A fully guided-wave squeezing experiment for fiber quantum networks", *Optica*, vol. 3, no. 4, pp. 362–366, 2016.

[283] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, and Y. Tamaki K. andYamamoto, "Quantum key distribution over a 40-db channel loss using superconducting single-photon detectors", *Nat. Photonics*, vol. 1, pp. 343–348, 2007.

[284] C. Y. Lu, T. Yang, and J. W. Pan, "Experimental multiparticle entanglement swapping for quantum networking", *Phys. Rev. Lett.*, vol. 103, no. 2, pp. 020501–020505, 2009.

[285] R. B. Jin, M. Takeoka, U. Takagi, R. Shimizu, and M. Sasaki, "Highly efficient entanglement swapping and teleportation at telecom wavelength", *Sci. Rep.*, vol. 5, no. 9333, 2015.

[286] R. H Hadfield, "Single-photon detectors for optical quantum information applications", *Nat. Photonics*, vol. 3, pp. 696–705, 2009.

[287] B. Baek, K. S. McKay, M. J. Stevens, J. Kim, H. H. Hogue, and S. W. Nam, "Single-photon detection timing jitter in a visible light photon counter", *IEEE J. Quantum Electron.*, vol. 46, no. 6, pp. 991–995, 2010.

[288] A. Tosi, N. Calandri, M. Sanzaro, and F. Acerbi, "Low-noise, low-jitter, high detection efficiency InGaAs/InP single-photon avalanche diode", *IEEE J. Sel. Top. Quantum Electron.*, vol. 20, no. 6, 2014.

[289] N. Calandri, Q. Y. Zhao, D. Zhu, A. Dane, and K. K. Berggren, "Superconducting nanowire detector jitter limited by detector geometry", *Appl. Phys. Lett.*, vol. 109, no. 152601, 2016.

[290] H. B. Coldenstrodt-Ronge, J. S. Lundeen, K. L. Pregnell, A. Feito, B. J. Smith, W Mauerer, C. Silberhorn, J. Eisert, M. B. Plenio, and I. A. Walmsley, "A proposed testbed for detector tomography", *J. Mod. Opt.*, vol. 56, no. 2-3, pp. 432–441, 2010.

[291] J. Fiurasek, C. Baune, A. Schonbeck, and R. Schnabel, "Analysis of counting measurements on narrowband frequency up-converted single photons and the influence of heralding detector dead time", *Phys. Rev. A*, vol. 91, no. 1, pp. 013829–013839, 2015.

[292] L. Zhang, H. B. Coldenstrodt-Ronge, A. D. Datta, G. Puentes, J. S. Lundeen, X. S. Jin, B. J. Smith, M. B. Plenio, and I. A. Walmsley, "Mapping coherence in measurement via full quantum tomography of a hybrid optical detector", *Nat. Photonics*, vol. 6, pp. 364–368, 2012.

[293] V. D'Auria, N. Lee, T. Amri, C. Fabre, and J. Laurat, "Quantum decoherence of single-photon counters", *Phys. Rev. Lett.*, vol. 107, no. 5, pp. 050504–050508, 2011.

[294] G. Brida, L. Ciavarella, I. P. Degiovanni, M. Genovese, L. Lolli, M. G. Mingolla, F. Piacentini, M. Rajteri, E. Taralli, and M. G. A. Paris, "Quantum characterization of superconducting photon counters", *New J. Phys.*, vol. 14, pp. 085001–085010, 2012.

[295] J. Ma, X. Chen, H. Hu, H. Pan, E Wu, and H. Zeng, "Quantum detector tomography of a single-photon frequency upconversion detection system", *Opt. Express*, vol. 24, no. 18, pp. 20973–20981, 2016.

[296] S. Grandi, A. Zavatta, M. Bellini, and M. G. A. Paris, "Experimental quantum tomography of a homodyne detector", *New J. Phys.*, vol. 19, pp. 053015–053027, 2017.

[297] J. Sperling, W. Vogel, and G. S. Agarwal, "Correlation measurements with on-off detectors", *Phys. Rev. A*, vol. 88, no. 4, pp. 043821–043829, 2013.

[298] J. Von Neumann, *Mathematische Grundlagen der Quantenmechanik*, Springer, 1932.

[299] G. Chiribella, G. M. D'Ariano, and D. Schlingemann, "How continuous quantum measurements in finite dimensions are actually discrete", *Phys. Rev. Lett.*, vol. 98, no. 19, pp. 190403–190407, 2007.

[300] P. P. Rohde, W. Mauerer, and C. Silberhorn, ", *New J. Phys.*, vol. 9, pp. 91–114, 2007.

[301] N. Somaschi, V. Giesz, L. De Santis, J. C. Loredo, M. P. Almeida, G. Hornecker, S. L. Portalupi, T. Grange, C. Anton, J. Demory, C. Gomez, I. Sagnes, N. D. Lanzillotti-Kimura, A. Lemaítre, A. Auffeves, A. G. White, L. Lanco, and P. Senellart, "Near-optimal single-photon sources in the solid state", *Nat. Photonics*, vol. 10, pp. 340–345, 2016.

[302] G. F. Sinclair and J. D. Thompson, "Effect of self- and cross-phase modulation on photon pairs generated by spontaneous four-wave mixing in integrated optical waveguides", *Phys. Rev. A*, vol. 94, no. 6, pp. 063855–063865, 2016.

[303] A. Cabello, "Multiparty key distribution and secret sharing based on entanglement swapping", *arXiv :quant-ph/0009025*, 2000.

[304] J. Lee, S. Lee, J. Kim, and S. Oh, "Entanglement swapping secures multiparty quantum communication.", *Phys. Rev. A*, vol. 70, pp. 032305, Sep 2004.

[305] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol", *Phys. Rev. Lett.*, vol. 85, pp. 441–444, Jul 2000.

[306] D. Gottesman, H. K Lo, N. Lutkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect divices", *Quant. Inf. Comp.*, vol. 4, no. 325, 2004.

[307] A. K. Ekert, "Quantum cryptography based on Bell's theorem", *Phys. Rev. Lett.*, vol. 67, pp. 661–663, Aug 1991.

[308] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem", *Phys. Rev. Lett.*, vol. 68, pp. 557–559, Feb 1992.

[309] D. Brush, "Optimal eavesdropping in quantum cryptography with six states", *Phys. Rev. Lett.*, vol. 81, pp. 3018–3021, Oct 1998.

[310] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations", *Phys. Rev. Lett.*, vol. 92, pp. 057901, Feb 2004.

[311] D. Brush and C. Macchiavello, "Optimal eavesdropping in cryptography with three-dimensional quantum states", *Phys. Rev. Lett.*, vol. 88, pp. 127901, Mar 2002.

[312] B. Huttner, H. Imoto, N. Gisin, and T. Mor, "Quantum cryptography with coherent states", *Phys. Rev. A*, vol. 51, pp. 1863–1869, Mar 1995.

[313] G. Brassard, N. Lütkenhaus, T. Mor, and B. Sanders, "Limitations on practical quantum cryptography", *Phys. Rev. Lett.*, vol. 85, pp. 1330–1333, Aug 2000.

[314] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states", *Phys. Rev. Lett.*, vol. 68, pp. 3121–3124, May 1992.

[315] K. Tamaki, M. Koashi, and N. Imoto, "Unconditionally secure key distribution based on two nonorthogonal states", *Phys. Rev. Lett.*, vol. 90, pp. 167904, Apr 2003.

[316] K. Tamaki and N. Lutkenhaus, "Unconditional security of the Bennett 1992 quantum key-distribution protocol over a lossy and noisy channel.", *Phys. Rev. A*, vol. 69, pp. 032316, Mar 2004.

[317] M. Koashi, "Unconditional security of coherent-state quantum key distribution with a strong phase-reference pulse", *Phys. Rev. Lett.*, vol. 93, pp. 120501, Sep 2004.

[318] K. Tamaki, N. Lutkenhaus, M. Koashi, and J. Batuwantudawe, "Unconditional security of the Bennett 1992 quantum-key-distribution scheme with a strong reference pulse.", *Phys. Rev. A*, vol. 80, pp. 032302, Sep 2009.

[319] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution", *Phys. Rev. Lett.*, vol. 89, pp. 037902, Jun 2002.

[320] K. Inoue, E. Waks, and Y. Yamamoto, "Differential-phase-shift quantum key distribution using coherent light", *Phys. Rev. A*, vol. 68, pp. 022317, Aug 2003.

[321] M. Curty, K. Tamaki, and T. Moroder, "Effect of detector dead times on the security evaluation of differential-phase-shift quantum key distribution against sequential attacks", *Phys. Rev. A*, vol. 77, pp. 052321, May 2008.

[322] L. Gyongyosi and S. Imre, "Information geometric security analysis of differential phase-shift quantum key distribution protocol", *Secur. Commun. Networks*, vol. 6, no. 2, pp. 129–150, 2012.

[323] T. Moroder, M. Curty, C. C. W. Lim, P. Thinh, H. Zbinden, and N. Gisin, "Security of distributed-phase-reference quantum key distribution", *Phys. Rev. Lett.*, vol. 109, pp. 260501, Dec 2012.

[324] N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, and V. Scarani, "Towards practical and fast quantum cryptography", *arXiv :quant-ph/0411022*, 2004.

[325] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution.", *Appl. Phys. Lett.*, vol. 87, no. 19, 2005.

[326] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states", *Phys. Rev. Lett.*, vol. 88, pp. 057902, Jan 2002.

[327] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, "Quantum cryptography without switching", *Phys. Rev. Lett.*, vol. 93, pp. 170504, Oct 2004.

[328] V. C. Usenko and F. Grosshans, "Unidimensional continuous-variable quantum key distribution", *Phys. Rev. A*, vol. 92, pp. 062337, Dec 2015.

[329] N. J. Cerf, M. Lévy, and G. Van Assche, "Quantum distribution of gaussian keys using squeezed states", *Phys. Rev. A*, vol. 63, pp. 052311, Apr 2001.

[330] R. Garcia-Patron and N. J. Cerf, "Continuous-variable quantum key distribution protocols over noisy channels", *Phys. Rev. Lett.*, vol. 102, pp. 130501, Mar 2009.

[331] L. S. Madsen, V. C. Usenko, M. Lassen, R. Filip, and U. L. Andersen, "Continuous variable quantum key distribution with modulated entangled states", *Nat. Commun.*, vol. 3, pp. 1083–1088, 2012.

[332] A. Leverrier and P. Grangier, "Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation", *Phys. Rev. Lett.*, vol. 102, pp. 180504, May 2009.

[333] A. Leverrier and P. Grangier, "Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation", *Phys. Rev. A*, vol. 83, pp. 042312, Apr 2011.

[334] V. Scarani and C. Kurtsiefer, "The black paper of quantum cryptography : real implementation problems", *TCS*, vol. 560, pp. 27–32, 2014.

[335] D. Mayers and A. Yao, "Quantum cryptography with imperfect apparatus", *Proceedings of the 39th Annual Symposium on Foundations of Computer Science*, 1998.

[336] J. Barrett, L. Hardy, and A. Kent, "No signaling and quantum key distribution", *Phys. Rev. Lett.*, vol. 95, pp. 010503, Jun 2005.

[337] U. Vazirani and T. Vidick, "Fully device-independent quantum key distribution", *Phys. Rev. Lett.*, vol. 113, pp. 140501, Sep 2014.

[338] H. K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution", *Phys. Rev. Lett.*, vol. 108, pp. 130503, Mar 2012.

[339] C. C. W. Lim, C. Portmann, M. Tomamichel, R. Renner, and N. Gisin, "Device-independent quantum key distribution with local Bell test", *Phys. Rev. X*, vol. 3, pp. 031006, Jul 2013.

[340] Y. C. Zhang, Z. Li, S. Yu, W. Gu, X. Peng, and H. Guo, "Continuous-variable measurement-device-independent quantum key distribution using squeezed states", *Phys. Rev. A*, vol. 90, pp. 052325, Nov 2014.

[341] Z. Li, Y. C. Zhan, F. Xu, X. Peng, and H. Guo, "Continuous-variable measurement-device-independent quantum key distribution", *Phys. Rev. A*, vol. 89, pp. 052301, May 2014.

[342] X. C. MMa, S. H. Sun, M. S. Jian, M. Gui, and L. M. Liang, "Gaussian-modulated coherent-state measurement-device-independent quantum key distribution", *Phys. Rev. A*, vol. 89, pp. 042335, Apr 2014.

[343] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, "High-rate measurement-device-independent quantum cryptography", *Nat. Photonics*, vol. 9, pp. 397–402, 2015.

[344] Z. Q. Yin, C. H. F. Fung, X. Ma, C. M. Zhang, H. W. Li, W. Chen, S. Wang, G. C. Guo, and Z. F. Han, "Measurement-device-independent quantum key distribution with uncharacterized qubit sources", *Phys. Rev. A*, vol. 88, pp. 062322, Dec 2013.

[345] Z. Q. Yin, C. H. F. Fung, X. Ma, C. M. Zhang, H. W. Li, W. Chen, S. Wang, G. C. Guo, and Z. F. Han, "Mismatched-basis statistics enable quantum key distribution with uncharacterized qubit sources", *Phys. Rev. A*, vol. 90, pp. 052319, Nov 2014.

[346] C H. Zhang, M. Li, H. W. Li, Z. Q. Yin, D. Wang, J. Z. Huang, Y. G. Han, M. L. Xu, W. Chen, S. Wang, P. Treeviriyanupab, G. C. Guo, and Z. F. Han, "Decoy-state measurement-device-independent quantum key distribution based on the Clauser-Horne-Shimony-Holt inequality", *Phys. Rev. A*, vol. 90, pp. 034302, Sep 2014.

[347] L. C. Comandar, M. Lucamarini, B. Frohlich, J. F. Dynes, A. W. Sharpe, S. W. B. Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Quantum key distribution without detector vulnerabilities using optically seeded lasers", *Nat. Photonics*, vol. 10, pp. 312–315, 2016.

[348] N. L. Piparo, M. Razavi, and C. Panayi, "Measurement-device-independent quantum key distribution with ensemble-based memories", *IEEE Journal of Selected Topics in Quantum Electronics,*, vol. 21, no. 3, 2014.

[349] N. L. Piparo and M. Razavi, "Long-distance trust-free quantum key distribution", *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, 2015.

[350] H. L. Yin, Y. L. Tang, Chen T. Y., and Chen Z. B., "Measurement-device-independent quantum key distribution based on Bell's inequality", *arXiv :1407.7375*, 2014.

[351] Z ; Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H. K. Lo, "Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution", *Phys. Rev. Lett.*, vol. 112, pp. 190503, May 2014.

[352] Y. L. Tang, H. L. Yin, S. J. Chen, Y. Liu, W. J. Zhang, X. Jiang, L. Zhang, J. Wang, L. X. You, J. Y. Guan, D. X. Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T. Y. Chen, Q. Zhang, and J. W. Pan, "Field test of measurement-device-independent quantum key distribution", *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, 2015.

[353] H. L. Yin, T. Y. Chen, Z. W. Yu, H. Liu, L. X. You, Y. H. Zhou, S. J. Chen, Y. Mao, M. Q. Huang, W. J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X. B. Wang, and J. W. Pan, "Measurement-device-independent quantum key distribution over a 404 km optical fiber", *Phys. Rev. Lett.*, vol. 117, pp. 190501, Nov 2016.

[354] Y. L. Tang, H. L. Yin, Q. Zhao, H. Liu, X. X. Sun, M. Q. Huang, W. Z. Zhang, S. J. Chen, L. Zhang, L. X. You, Z. Wang, Y. Liu, C. L. Lu, X. Jiang, X. Ma, Q. Zhang, T. Y. Chen, and J. W. Pan, "Measurement-device-independent quantum key distribution over untrustful metropolitan network", *Phys. Rev. X*, vol. 6, pp. 011024, Mar 2016.

Abstract

This thesis presents solutions to the challenges of developing quantum communication networks. Two powerful experimental devices have been set up relying only on standard telecom and integrated optical components. The first device corresponds to an all-optical synchronization scheme allowing, with an unprecedented accuracy, quantum key distribution at a high rate over long distances. The experimental scheme relies on two independent entangled photon pair sources that have to be synchronized in their emission time. Our approach is based on using a 2.5 GHz picosecond telecom laser as a master clock to efficiently synchronize the different sources. We demonstrate the synchronization for an effective distance of 100 km between sources. With our second device, we perform a squeezing experiment at telecom wavelengths and this for the first time in a fully guided-wave approach. Squeezed light being a fundamental resource for several quantum information protocols, developing plug-and-play experimental devices that are compatible with already existing telecom fiber networks is of first interest in the perspective of future quantum networks. Finally, we propose a quantum description of timing jitter effects in 0N/0FF detectors. Despite the importance of detection systems in emerging photonic quantum technologies, no quantum description of their timing jitter effects has been proposed so far.

Résumé

Le déploiement de réseaux de communication quantique représente un défi auquel cette thèse apporte des solutions originales. Deux dispositifs très performants sont construits uniquement autour de composants standards de l'optique intégrée et des télécommunications optiques. Le premier correspond à un schéma de synchronisation tout optique sur longue distance à très haute cadence et de précision inégalée pour la communication sécurisée par cryptographie quantique. Le montage expérimental repose sur une configuration de relais quantique mettant en œuvre deux sources indépendantes de paires de photons intriqués dont il faut synchroniser les temps d'émissions. L'idée principale s'appuie sur l'utilisation d'un unique laser telecom picoseconde cadencé à 2.5 GHz afin de générer l'horloge et de pouvoir la distribuer efficacement aux deux sources. Nous démontrons la synchronisation de notre lien relais pour une distance effective séparant les sources de plus de 100 km. Le second dispositif correspond quant à lui à la réalisation d'une expérience de compression à une longueur d'onde des télécommunications réalisée, pour la première fois, de manière entièrement guidée. La lumière comprimée étant une ressource fondamentale dans bon nombre de protocoles d'information quantique, la réalisation de systèmes expérimentaux facilement reconfigurables et compatibles avec les réseaux télécoms fibrés existants représente une étape cruciale en vue du déploiement de dispositifs de communication quantique en régime de variables continues. Enfin, un traitement quantique des effets de gigue temporelle dans les détecteurs de photons 0N/0FF est proposé. Malgré l'importance des systèmes de détection dans les technologies quantiques photoniques émergentes, aucune modélisation quantique de leurs effets de gigue temporelle n'avait été, à notre connaissance, développé jusqu'à présent.