



HAL
open science

Vers un réseau Quantique de Communication

Sébastien Tanzilli

► **To cite this version:**

Sébastien Tanzilli. Vers un réseau Quantique de Communication. Physique Quantique [quant-ph].
Université Nice Sophia Antipolis, 2012. tel-00845762

HAL Id: tel-00845762

<https://theses.hal.science/tel-00845762>

Submitted on 17 Jul 2013

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

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

THÈSE D'HABILITATION À DIRIGER LES RECHERCHES

présentée à

L'UNIVERSITÉ DE NICE–SOPHIA ANTIPOLIS

École Doctorale : Sciences Fondamentales & Appliquées (ED-SFA n°364)

par

Sébastien TANZILLI

VERS UN RÉSEAU QUANTIQUE DE COMMUNICATION

Soutenue le 27 Septembre 2012 devant le jury composé de :

Alain Aspect	Directeur de recherche au CNRS, Laboratoire Charles Fabry de l'IOGS	
Fabien Bretenaker	Directeur de recherche au CNRS, Laboratoire Aimé Cotton	<i>Rapporteur</i>
Nicolas Gisin	Professeur, Group of Applied Physics, University of Geneva	
Ariel Levenson	Directeur de recherche au CNRS, Laboratoire de Photon. & Nanostructures	<i>Rapporteur</i>
Daniel B. Ostrowsky	Professeur émérite, Université de Nice – Sophia Antipolis	
John G. Rarity	Professor, Centre for Communications Research, University of Bristol	<i>Rapporteur</i>



**Laboratoire
Physique de la Matière Condensée**



UMR 7336 du CNRS & de l'Université de Nice – Sophia Antipolis (UNS)

THÈSE D'HABILITATION À DIRIGER LES RECHERCHES

présentée à

L'UNIVERSITÉ DE NICE–SOPHIA ANTIPOLIS

École Doctorale : Sciences Fondamentales & Appliquées (ED-SFA n°364)

par

Sébastien TANZILLI

VERS UN RÉSEAU QUANTIQUE DE COMMUNICATION

Soutenue le 27 Septembre 2012 devant le jury composé de :

Alain Aspect	Directeur de recherche au CNRS, Laboratoire Charles Fabry de l'IOGS	
Fabien Bretenaker	Directeur de recherche au CNRS, Laboratoire Aimé Cotton	<i>Rapporteur</i>
Nicolas Gisin	Professeur, Group of Applied Physics, University of Geneva	
Ariel Levenson	Directeur de recherche au CNRS, Laboratoire de Photon. & Nanostructures	<i>Rapporteur</i>
Daniel B. Ostrowsky	Professeur émérite, Université de Nice – Sophia Antipolis	
John G. Rarity	Professor, Centre for Communications Research, University of Bristol	<i>Rapporteur</i>



**Laboratoire
Physique de la Matière Condensée**



UMR 7336 du CNRS & de l'Université de Nice – Sophia Antipolis (UNS)

“Je connais la tendance de l’esprit humain à faire n’importe quoi plutôt que de penser. Certes, aucun d’entre nous n’espère réussir sans travail. Nous savons tous qu’acquérir un tant soit peu de science exige un effort intellectuel considérable, et je suis sûr que nous y sommes prêts pour avancer dans notre discipline. Mais effort intellectuel n’égale pas pensée. Et ceux qui, à grand’peine, ont acquis l’habitude de s’appliquer à leur tâche, souvent trouvent plus aisé d’apprendre une formule que de maîtriser un principe. [...] les principes sont fertiles en résultats, alors que les résultats seuls sont stériles. Celui qui a appris une formule est à la merci de sa mémoire, mais celui qui a maîtrisé un principe peut garder son esprit libre de formules, sachant qu’il peut en fabriquer autant que nécessaire, le moment venu. Dois-je ajouter que, malgré le recul naturel de l’esprit devant le dur processus de la pensée, pourtant, ce processus une fois accompli, l’esprit ressent une puissance et une jouissance qui l’amènent à mépriser désormais les peines et angoisses qui accompagnent son passage d’un stade de développement à un autre ?”

James C. Maxwell, Conférence inaugurale au King’s College de Londres (1860), texte original reproduit dans *Am. J. Phys.* **47**, 928 (1979).

Table des matières

1	Introduction Générale	13
1.1	La communication quantique	15
1.2	Contenu de ce manuscrit	16
2	La science de l'information quantique	19
2.1	La communication et le traitement de l'information classique	21
2.1.1	Concept sous-jacent : le bit	21
2.1.2	L'exemple des communications optiques standards	21
2.1.3	Les limitations de l'information classique	23
2.2	L'information quantique	23
2.2.1	Concept sous-jacent : la superposition cohérente d'états quantiques pour coder des qbits	23
2.2.2	Extension à deux systèmes quantiques : les paires de qbits intriqués	24
2.2.3	Deux propriétés quantiques fondamentales	26
2.2.3.1	Des résultats de mesure probabilistes	26
2.2.3.2	Le théorème de non-clonage	27
2.2.4	Les supports des qbits	28
2.3	Produire des qbits individuels	30
2.3.1	Isolation d'un système émetteur possédant 2 niveaux d'énergie distincts	30
2.3.2	Génération de photons uniques annoncés par conversion paramétrique	31
2.3.3	Pour aller plus loin	31
2.4	Produire des paires de qbits intriqués	32
2.4.1	Le paradoxe EPR et l'histoire (petite) des paires de photons intriqués	32
2.4.2	La conversion paramétrique au service de la production de paires de photons intriqués	35
2.4.2.1	L'observable polarisation des photons	35
2.4.2.2	L'observable énergie-temps ou 'time-bin'	35
2.4.3	Pour aller plus loin	37
2.4.4	Une remarque pour finir	38
2.5	La cryptographie quantique	38
2.5.1	Rappel sur les deux méthodes de chiffrement les plus pertinentes	39
2.5.1.1	Chiffrement à clé publique - protocole RSA	39
2.5.1.2	Chiffrement à clé privée - méthode du masque jetable	40
2.5.2	Résumé de la situation et conclusion	41
2.5.3	Le protocole Bennett et Brassard de 1984, ou BB84	41
2.5.3.1	Génération d'une clé privée	42
2.5.3.2	Transmission de la clé et espionnage	42
2.5.3.3	Réconciliation des bases	43
2.5.3.4	Ça marche vraiment ?	43
2.5.3.5	Où en est-on aujourd'hui ?	43
2.5.4	La cryptographie quantique à paires de photons, ou protocole d'Ekert	44
2.5.5	Les limitations des protocoles quantiques	44
2.5.6	Une remarque pour finir	45
2.6	La téléportation d'états	45
2.6.1	La téléportation d'états quantiques individuels : principe et théorie	45
2.6.2	Extension à la téléportation de l'intrication	47

2.6.3	La téléportation au service de la cryptographie quantique	47
2.6.3.1	Le problème de la distance	47
2.6.3.2	Principe de la fonction relais quantique	48
2.6.3.3	L'augmentation des distance de communication quantique, oui mais à quel prix ?	51
2.6.4	Deux remarques pour finir	52
2.7	Le futur du domaine à court & moyen termes	52
2.7.1	Stocker les qbits	53
2.7.2	Les opérations de logique quantique pour le traitement et l'algorithmique quantiques . . .	53
2.8	Conclusion	54
3	Résumé des travaux de thèse et post-doctorat	57
3.1	Quelques bases d'optique non-linéaire	59
3.1.1	Le processus de conversion paramétrique optique	59
3.1.2	Le processus de génération de somme de fréquences	60
3.2	Sources de paires de photons intriqués à base d'optique non-linéaire intégrée	62
3.3	La génération de somme de fréquence au service de la communication quantique	63
3.3.1	Interface quantique pour qbits photoniques	63
3.3.2	Cryptosystèmes quantiques avec détection de photons par conversion de longueur d'onde	65
3.3.2.1	Cryptosystème quantique tout fibré à haut débit	66
3.3.2.2	Détection des photons à 4.6 μm pour la cryptographie quantique à l'air libre . . .	67
4	Sources photoniques pour la communication quantique	69
4.1	Source de photons uniques annoncés à 1550 nm	71
4.1.1	Interférométrie de Sagnac à photons uniques	72
4.1.2	Extension de la source	73
4.2	Sources de paires de photons intriqués en polarisation basée sur l'interaction non-linéaire de type-II	75
4.2.1	Contexte de l'étude	75
4.2.2	Principe de fonctionnement et détails de la source	75
4.2.3	Discussion et améliorations des résultats - mesures d'intrication	76
4.2.4	Améliorations potentielles	78
4.2.5	Finalisation pertinente de la source	79
4.2.6	Extension de la source à l'observable time-bin	79
4.3	Source de paires de photons intriqués en polarisation basée sur l'interaction non-linéaire de type-0	81
4.3.1	Contexte de l'étude	81
4.3.2	Principe de fonctionnement de la source	81
4.3.3	Résultats obtenus et versatilité d'emploi	82
4.3.4	Test quantique, à choix retardé, de la complémentarité des photons uniques	83
4.4	Étude d'un générateur paramétrique intégré sur semi-conducteur entouré d'un réseau de Bragg .	84
4.5	Analyse d'états intriqués en polarisation particuliers	85
5	Les relais quantiques	87
5.1	L'interférence quantique à deux photons	89
5.2	Relais quantique basé sur la téléportation de l'intrication en régime picoseconde - preuve de principe	89
5.3	Relais quantique intégré basé sur la téléportation - preuve de principe	92
6	Résumé des projets en cours de développement	97
6.1	Vers la réalisation d'un relais quantique indépendant des sources employées	99
6.2	Synchronisation de sources d'intrication par horloge optique distribuée	100
6.3	Photonique quantique intégrée	102
6.4	Réseau quantique de communication aux longueurs d'ondes des télécoms	103
6.5	Intrication à distance de deux mémoires quantiques à base d'atomes froids	105
7	Conclusion générale	109

8	Résumé de la carrière scientifique	113
8.1	Curriculum Vitæ court	115
8.2	Curriculum Vitæ étendu	117
8.2.1	Distinctions scientifiques	117
8.2.2	Encadrement, Animation et Management de la recherche	117
8.2.2.1	Responsabilités et activités de direction d'équipe	117
8.2.2.2	Responsabilités dans l'animation de programmes de recherche	117
8.2.2.3	Formation de (post-)doctorants et de stagiaires au métier de la recherche	118
8.3	Direction du GDR - IQFA et autres responsabilités collectives au sein du CNRS	121
8.3.1	Direction du GDR - IQFA	121
8.3.2	Membre du bureau du GDR - QMAP	122
8.4	Autres responsabilités ou activités collectives ailleurs qu'au CNRS	122
8.5	Transfert technologique, relations industrielles et valorisation	122
8.6	Enseignement	123
8.7	Participation à l'organisation de conférences, workshops, <i>etc.</i>	124
8.8	Diffusion de la culture scientifique	124
8.8.1	Interventions dans la presse écrite et audiovisuelle	125
8.9	Participation à des travaux d'expertise	125
9	Liste des productions scientifiques / Track records	127
9.1	Papiers publiés dans, soumis à, ou en préparation pour, des revues internationales	129
9.2	'Research Highlights' de certaines publications	130
9.3	Papiers publiés dans des proceedings internationaux avec comité de lecture	130
9.4	Thèse de doctorat & participation à des ouvrages scientifiques	130
9.5	Tutoriaux & cours	130
9.6	Talks invités dans des conférences internationales et nationales	131
10	Bibliographie générale	135

Chapitre 1

Introduction Générale

1.1 La communication quantique

Au début des années 1980, Alain Aspect réalisa ses célèbres “expériences de Bell” à l’aide d’une source plutôt complexe de paires de photons intriqués en polarisation basée sur la division de molécules diatomiques. Ces “photons jumeaux” présentent des corrélations si fortes que, même s’ils sont séparés spatialement, ils constituent un système quantique unique. A l’époque, il fut obtenu une preuve non ambiguë de cette intrigante prévision de la théorie quantique : les interactions dans le monde quantique sont régies par des lois non-locales que les théories classiques (à priori locales), à variables cachées ou non, ne peuvent pas décrire. Ceci fut mis en évidence par le viol des inégalités de Bell qui constituent une sorte de frontière entre les descriptions classiques (locales) et quantiques (non-locales). Depuis ces tests pionniers et fondamentaux, tout a été révolutionné, depuis les concepts théoriques aux outils expérimentaux. Même le vocabulaire a subi de profondes mutations...

D’une part, il y eut la rencontre, à la fin des années 1980, de l’optique quantique et de l’optique non-linéaire grâce à laquelle les physiciens ont mis au point de nouvelles sources de photons jumeaux et de photons uniques basées sur la conversion paramétrique dans les milieux quadratiques (χ^2). Les imposantes cascades atomiques ont donc avantageusement été remplacées par de simples cristaux de quelques mm de côté, plus efficaces et simples d’utilisation. Ces sources, au sein desquelles on trouve de plus en plus de développement (composants télécoms, optique intégrée, *etc.*), constituent aujourd’hui ce que j’appellerais les ressources technologiques.

D’autre part, les physiciens ont réalisé que les propriétés intrinsèques à la théorie quantique, telles que la superposition cohérente d’états et l’intrication, peuvent servir à encoder un nouveau type d’information, les bits quantiques, utile à plusieurs protocoles d’échange d’information regroupés sous le terme générique de *communication quantique* et parmi lesquels je citerais volontiers la cryptographie quantique et la téléportation d’états. On ne parle donc plus de superposition cohérente d’états ou de paires de photons intriqués mais volontiers de “qbit” (contraction des mots anglais quantum bit) et de paires de qbits par analogie avec les bits classiques usuels. En effet, à l’instar des bits classiques d’information, la physique quantique offre les possibilités d’encoder un état haut (noté $|1\rangle$) grâce, par exemple, à un photon polarisé verticalement, et un état bas (noté $|0\rangle$) à l’aide d’un photon polarisé horizontalement. Mais elle autorise surtout une infinité de possibilités grâce à toutes les combinaisons relatives à la superposition des deux états de base. Ceci se traduit en “langage information quantique” par l’obtention d’un qbit sous la forme $\alpha|0\rangle + \beta|1\rangle$, tant que la règle de normalisation $|\alpha|^2 + |\beta|^2 = 1$ est remplie. De là, si le nombre de systèmes de ce type devient grand, les possibilités de calcul s’avèrent extraordinaires si bien que l’on parle déjà de théorie quantique de l’information et que l’on spéculer sur l’énorme potentiel des protocoles de *calcul quantique* en termes de réduction des temps de calcul liés aux problèmes complexes (factorisation des grands entiers, *etc.*). Les qbits et états quantiques similaires constituent aujourd’hui ce que j’appellerais les ressources fondamentales.

La combinaison des ressources a permis de nombreux succès au cours des 20 dernières années, que ce soit d’un point de vue fondamental (théorie de l’information quantique, démonstrations d’états intriqués toujours plus probantes, états impliquant plusieurs particules, *etc.*) que du point de vue des applications (cryptographie quantique, relais quantiques destinés à augmenter les distances de communication, *etc.*). Mais au-delà des succès de la cryptographie quantique entre deux parties distantes, l’heure est à la construction de véritables réseaux de communication quantique mettant en jeu une distribution fibrée des qbits portés par des photons et des entités de stockage dans des ensembles ioniques ou atomiques permettant d’accroître à la fois la portée et le rendement des réseaux considérés. Pour aboutir, il faudra marier ces deux supports privilégiés des qbits que sont les photons télécoms à 1550 nm, répondant naturellement à la tâche de distribution, et les ensembles d’atomes isolés opérant entre de 600 et 1000 nm, bien adaptés aux tâches de stockage et de calcul. Si l’interaction lumière-matière peut permettre en théorie de passer d’un type de système à l’autre, un sérieux problème demeure en raison de désaccords majeurs entre les longueurs d’ondes et largeurs de raie associées aux deux types supports. L’avenir réside pourtant dans ce couplage afin de réaliser des réseaux quantiques efficaces et de longue portée, constitués de canaux fibrés interconnectés par des nœuds où le stockage et d’éventuelles tâches de calcul sont possibles.

Les réalisations expérimentales sont encore loin d’accomplir les prouesses escomptées par la théorie. Bien que l’on sache aujourd’hui téléporter l’état d’un qbit entre deux points séparés par quelques km de fibre optique, ou encore générer des états intriqués à plusieurs qbits, la communication quantique a grand besoin d’avancées majeures afin de sortir les expériences du laboratoire. C’est pourquoi les apports et le mariage pertinent de diverses techniques et technologies complémentaires, comme notamment l’optique non-linéaire intégrée et les ensembles atomiques froids, deux des spécificités du LPMC, sont des candidats de choix pour la réalisation des briques et fonctions élémentaires qui constitueront les futurs réseaux quantiques de communication. Plus précisément, c’est grâce à la technologie de l’optique intégrée, permettant la réalisation de guides d’ondes à la surface

de substrats de niobate de lithium polarisé périodiquement (on parle de guides PPLN), que j’ai pu démontrer, pendant ma thèse de doctorat, la source de paires de photons la plus efficace au monde, voir les Réfs. [1, 2] de la Sec. 9.1. C’est également grâce à cette technologie que j’ai pu réalisé, pendant mon stage post-doctoral, la première interface quantique à conversion cohérente de longueurs d’ondes afin de favoriser le couplage des qbits photoniques avec les ensembles atomiques, voir la Réf. [3] de la Sec. 9.1. Ce travail a par ailleurs été sélectionné par la revue *Optics & Photonics News* pour son numéro spécial “Optics in 2005”, voir la Réf. [1] de la Sec. 9.2. Le lecteur intéressé par la genèse et l’évolution de l’optique quantique intégrée pourra notamment se reporter à l’article de revue publié en 2012 par mon équipe, voir la Réf. [4] de la Sec. 9.1.

Désormais, à l’heure où les défis “réseaux quantiques de communication” et “calcul quantique” battent leur plein, couplant sources de qbits, canaux de distribution, interfaces à conversion cohérente de longueurs d’ondes, et entités de stockage des qbits basées sur des systèmes matériels, l’Information Quantique est devenue, au fil des années, un véritable champ disciplinaire, mais également complètement transverse. Pour s’en convaincre, le lecteur pourra consulter le site web du GDR - IQFA que je dirige (voir en ligne [IQFA](#)), afin de se figurer combien les équipes qui officient dans le domaine sont nombreuses et combien les axes de réflexion thématique mis en place par ce GDR sont effectivement transverses. En effet les expérimentateurs et les théoriciens du domaine font aujourd’hui appel à la fois à la physique (quantique, atomique, des matériaux, de la matière condensée, *etc.*), à l’optique (quantique, non-linéaire, guidée, intégrée, *etc.*), à la chimie (des matériaux (dopage de cristaux), *etc.*), et à l’informatique. C’est pourquoi, l’idée générale de la thématique “Information Quantique avec Lumière et Matière (QILM)” que je co-anime au sein du LPMC consiste à mettre l’ensemble de nos compétences et savoirs-faire expérimentaux au service de la création, de la manipulation, du traitement et du stockage des qbits. Nous couplons avantageusement, au sein d’expériences ambitieuses, optique non-linéaire intégrée, optique guidée au standard des télécoms et, dans un futur proche, ensembles d’atomes froids.

1.2 Contenu de ce manuscrit

Les activités de l’équipe QILM, telles qu’elles le sont aujourd’hui, ont débuté avec mon recrutement en 2005 en tant que Chargé de recherche au CNRS. Le pari était quelque peu risqué, ou le projet audacieux, dans le sens où le LPMC n’était que très peu doté en équipements susceptibles de servir ne serait-ce que de point de départ à des expériences d’optique et de communication quantiques. En effet, le laboratoire était plutôt (et est toujours par ailleurs) spécialisé dans l’optique non-linéaire intégrée, cependant en régime classique. Si les composants optiques non-linéaires intégrés sont au cœur de la plupart des développements de mon équipe, les éléments qui les entourent sur une table optique sont d’une nature complètement différente lorsque l’on s’intéresse aux propriétés classiques ou quantiques de la lumière qu’ils émettent. Il a donc fallu trouver un peu d’argent (les expériences quantiques coûtent cher), négocier (tous !) les achats (on n’a jamais assez d’argent pour monter des expériences de haut niveau), trouver (merci Messieurs les directeurs) et équiper des salles d’expérience (cela prend du temps lorsque l’on part quasiment ‘from scratch’), recruter d’excellents collaborateurs, convaincre de “bons” étudiants de venir s’éclater en thèse à compter des photons dans le noir à longueur de journées (alors qu’à Nice il fait beau toute l’année) pour violer Bell (le pauvre !), faire les bons choix (dans la vie il faut faire des choix, mais les bons), et enfin avancer le plus efficacement possible tant la concurrence est rude... en bref, il a fallu monter rapidement une équipe compétitive.

J’espère que le lecteur pourra s’apercevoir, tout au long de ce manuscrit, que la partie n’est pas trop mal engagée. Et je me permettrais d’ajouter que les collaborateurs et les doctorants que j’ai eu le plaisir et l’honneur d’encadrer au cours de ces années n’y sont pas pour rien.

Ainsi, je discuterai dans ce qui suit l’ensemble des réalisations que j’ai pu effectuer au cours de ma carrière, au LPMC ou par le biais de collaborations fortes, en ayant à l’esprit le développement des briques élémentaires en vue de la construction des futurs réseaux quantiques de communication. Pour ce qui concerne la partie scientifique, le manuscrit est organisé de la façon suivante :

- Le Chapitre 2 est consacré à la déclinaison des concepts de physique fondamentale et appliquée sous-jacents à la communication et au traitement de l’information quantique. Il y est question du théorème de non-clonage, de cryptographie, de téléportation, de relais et de mémoires quantiques. Nombres de ces concepts se situent au cœur de mes propres travaux de recherche, si bien qu’ils sont mis en exergue à divers endroits dans ce manuscrit. Ce chapitre permet également de dresser un état de l’art, certes non

exhaustif tant la communauté est vaste et les réalisations nombreuses, du domaine.

- Le Chapitre 3 joue de rôle de mise en contexte et de point de départ de mes propres travaux de recherche. Après quelques rappels de base en optique non-linéaire (voir Sec. 3.1), notamment en configuration de type guide d’ondes, je propose un résumé (très) succinct des mes travaux de thèse ainsi que de post-doctorat. Nous verrons que mes travaux de thèse ont concerné le développement de sources de paires de photons intriqués en ‘énergie-temps’ et en ‘time-bin’ à l’aide d’un générateur non-linéaire fait en optique intégrée sur niobate de lithium émettant aux longueurs d’ondes des télécommunications (voir Sec. 3.2). Par ailleurs, la Sec 3.3 est dédiée au processus non-linéaire de génération de somme de fréquences (SFG) pour la réalisation d’interfaces photoniques à conversion cohérente de longueurs d’ondes (voir Sec. 3.3.1) ou de détecteurs de photons uniques hybrides (voir Sec. 3.3.2). Nous verrons donc que l’intérêt du processus SFG est double. D’une part, lorsque celui-ci est rendu cohérent, les interfaces photoniques correspondantes permettent de transférer l’information quantique portée par un photon, par exemple télécom, vers un photon de longueur d’onde plus basse bien adaptée au stockage quantique dans les mémoires développées aujourd’hui. D’autre part, lorsque le processus SFG sert de simple convertisseur, celui-ci permet de détecter des photons initialement télécoms à l’aide de bien meilleurs détecteurs : c’est le principe de la détection hybride qui trouve notamment des applications en cryptographie quantique comme nous le discuterons brièvement.
- Le Chapitre 4 est consacré aux diverses sources photoniques que j’ai pu développer au cours des années qui ont suivi ma thèse de doctorat. C’est donc le début du cœur de ce manuscrit. Sont déclinées sources de photons uniques annoncés (voir Sec. 4.1) et une expérience d’interférométrie Sagnac à photons uniques, sources de paires de photons intriqués en polarisation (voir Sec. 4.2 et 4.3) et en time-bin (voir Sec. 4.2.6), le tout à base de générateurs non-linéaires fait en optique intégrée sur niobate de lithium émettant aux longueurs d’ondes des télécommunications. Sont également présentées une étude théorique pour l’implémentation d’une source de paires de photons intriqués à base d’un générateur de type semi-conducteur entouré d’un réseau de Bragg (voir Sec. 4.4) et des études théoriques et expérimentales qui concernent l’analyse d’états intriqués en polarisation voir (Sec. 4.5).
- Le Chapitre 5 relate pour sa part des “expériences amont en vue d’applications” associées à des configurations de type relais quantiques, briques élémentaires des futurs réseaux de communication quantique. Je discute notamment l’observation d’interférences quantiques à deux photons issus de sources séparés spatialement opérant en régime picoseconde (voir Sec. 5.2) et une réalisation originale d’une puce optique intégrant toutes les fonctions optiques de base pour la réalisation de la fonction relais (voir Sec. 5.3).
- J’introduirai enfin au Chapitre 6 les projets en cours, ou qui viennent de démarrer, et ceux que je compte développer dans le futur. Nous verrons que ceux-ci s’orientent naturellement vers les défis de la communication quantique d’aujourd’hui et de demain, mariant de façon pertinente entités de génération, d’ingénierie, de manipulation et de stockage de l’information quantique.

Pour ce qui concerne la partie “moins scientifique”, le lecteur pourra trouver un résumé de ma carrière scientifique au Chapitre 8 et la liste de mes productions au Chapitre 9. La bibliographie générale est, quant à elle, déclinée au Chapitre 10.

Chapitre 2

La science de l'information quantique

Note préliminaire

Ce chapitre, plutôt long, propose une revue, non exhaustive, des concepts sous-jacents à la communication et au traitement quantiques de l'information, tout en donnant les références séminales ainsi que l'état de l'art du domaine. Ce choix a été fait dans le sens où la plupart des notions qui sont introduites dans ce chapitre seront utilisées dans les chapitres qui suivent et qui traitent des travaux de recherche réalisés par l'auteur au cours de sa carrière.

Ainsi, le lecteur aguerri à tout cela pourra avantageusement sauter ce chapitre, alors que le lecteur désirent obtenir un état de l'art plus complet, cependant toujours non exhaustif, pourra se référer aux publications de l'auteur (voir Sec.9.1) et, bien entendu, à toutes les références qu'elles contiennent.

Une vue d'ensemble du chapitre

Les modes de communication et de traitement de l'information classique ont révolutionné la société depuis quelques décennies : les cinq continents sont reliés par des câbles optiques, l'information est manipulée sans perte à très haut débit sur des distances quasi illimitées.

Toutefois, une limitation forte existe s'il s'agit de communiquer l'information d'une façon sécurisée. Le domaine de la cryptographie a un long passé qui remonte à l'antiquité. Aujourd'hui elle intervient à chaque instant dans de très nombreux domaines de la vie privée ou publique et devient un vrai problème de société. Les protocoles utilisés pour le chiffrement et déchiffrement des messages utilisent des codes de plus en plus complexes à mesure qu'augmente la puissance des ordinateurs capables de les briser. Le chiffrement des messages ne peut jamais être considéré comme inviolable pour toujours. Il faut donc se tourner vers une autre stratégie et c'est là que la physique quantique intervient, susceptible d'apporter des solutions à la distribution de clés parfaitement sécurisées et à distance. L'information quantique est un domaine très vaste, loin des performances de la communication classique mais en plein développement. Il fait l'objet de recherches dans de très nombreux laboratoires dans le monde, réunis en France par le Groupe de Recherche **IQFA** (Information Quantique, Fondements et Applications), que je dirige.

L'encodage binaire de l'information quantique se fait via une entité nommée qbit¹ qui peut être préparée dans deux états de base distincts. L'idée est qu'en physique quantique un qbit peut être créé dans les deux états à la fois, dans une superposition dite cohérente de ces deux états. Il existe de nombreux supports possibles pour la communication et le calcul quantiques. Toutefois, pour envoyer des qbits sur de grandes distances, il est approprié d'utiliser des photons comme support, en encodant l'information sur des observables telles que la polarisation de la lumière, le chemin optique, ou encore le temps d'émission ('time-bin'). Les protocoles de cryptographie quantique peuvent être considérés comme inviolables en résultat de deux théorèmes très fondamentaux qui régissent les lois suivies par les états quantiques et empêchent leurs utilisateurs de prédire, connaître, ou manipuler le système à leur guise. Le chapitre explicite clairement ces deux 'no-go' théorèmes, piliers de la méthode : le premier prédit que le résultat est aléatoire pour une mesure unique sur un support préparé dans une superposition de deux états ; le second, dit théorème de non-clonage, démontre qu'il n'est pas

1. Contraction anglaise de 'quantum bit'.

possible de cloner parfaitement un état quantique inconnu au préalable. Ceci signifie que toute personne qui tenterait d'espionner une ligne de communication sur une clé secrète avec une stratégie de clonage ne pourrait pas le faire à la perfection.

Après le rappel de ces notions théoriques fondamentales pour l'information quantique, ce chapitre décrit diverses méthodes expérimentales actuellement développées pour réaliser des qbits en optique, codés sur des photons uniques. Les sources de photons uniques sont aujourd'hui diverses, fondées soit sur un pompage optique afin d'isoler des systèmes à deux niveaux d'énergie (centres colorés dans le diamant, boîtes quantiques semi-conductrices), soit sur la fluorescence paramétrique dans un cristal non-linéaire. Dans ce second cas, les photons sont générés par paires, et l'un des photons peut servir d'annonceur pour le second. Quelle que soit la configuration choisie, le codage en polarisation s'effectue avec un polariseur linéaire, suivi d'une lame demi-onde tournante qui permet de superposer à volonté les deux états du qbit. Pour un codage dit en 'time-bin', les deux états correspondent au passage soit dans un bras court soit dans un bras long dans un dispositif de type interférométrique. Le record actuel de distribution de qbit unique à distance est de 200 km. Il a été obtenu via l'utilisation de l'observable 'time-bin', avec des photons émis aux longueurs d'onde des télécommunications au travers de fibres optiques standards. Ce chapitre décrit également des systèmes fondés sur les mêmes principes, mais destinés cette fois à générer des paires de qbits intriqués qui sont nécessaires à certains protocoles de cryptographie quantique ainsi qu'à la téléportation d'état.

La situation de la cryptographie est ensuite détaillée. Les méthodes de chiffrement classique les plus pertinentes sont décrites assez complètement et leurs limitations quant à l'inviolabilité bien mises en évidence; celles-ci sont liées au fait qu'il faut générer une clé parfaitement aléatoire aussi longue que le message à chiffrer. Les mêmes limitations n'apparaissent pas en cryptographie quantique qui permet l'établissement de clés privées entre deux partenaires distants. Le protocole le plus utilisé en cryptographie quantique (appelé BB84 du nom de ses inventeurs en 1984) est explicité en détail. Une variante de la méthode BB84, utilisant des paires de photons intriqués est également discutée (protocole d'Ekert). Tous ces protocoles quantiques sont en principe totalement sécurisés. En pratique, les imperfections des composants du système peuvent fragiliser la sécurité des clés établies.

Les protocoles de téléportation de qbits uniques, ainsi que leur extension à la téléportation de l'intrication, sont également présentés, à la fois du point de vue théorique et en indiquant l'état de l'art expérimental. En configuration relais quantiques, ils sont destinés à accroître les distances de communication quantique. Ils reposent sur les mêmes principes que ceux qui sous-tendent la cryptographie quantique. Ils utilisent en particulier des paires de qbits intriqués. La distance record obtenue pour une transmission d'information secrète avec téléportation est aujourd'hui de l'ordre de quelques km en raison des défis technologiques, notamment liés à la détection peu efficaces et bruitée des photons télécoms, qui sont ceux d'aujourd'hui.

Enfin, le devenir du domaine est discuté au travers des applications potentielles liées à la réalisation d'une brique de base supplémentaire : la mémoire quantique, envisagée généralement à base de systèmes matériels tels que des ions ou des atomes. Avec de telles briques, la réalisation de véritables réseaux quantiques de communication, et également la mise en œuvre d'algorithmes quantiques plus efficaces que leurs correspondants classiques (factorisation de grands entiers, recherche dans une base de données), pourront un jour devenir possibles. Les recherches en cryptographie avec téléportation quantique se développent extrêmement rapidement dans tous les grands pays du monde, en France dans une quarantaine de laboratoires. Si les performances sont encore très loin de celles obtenues en communication classique, la sécurisation de la transmission des informations par voie quantique semble remarquable et fait déjà l'objet d'applications pratiques, comme pour le système bancaire dans le périmètre d'un petit pays comme la Suisse. Les générateurs de photons uniques sont des appareils qu'on trouve facilement dans le commerce. De petites entreprises de cryptographie quantique commencent à se monter dans plusieurs pays et notamment en France. Le domaine est d'une grande richesse et n'en est encore qu'à ses débuts.

Chapitre 3

Résumé des travaux de thèse et post-doctorat

Mon travail de thèse s'est déroulé à l'Université de Nice, plus précisément au Laboratoire de Physique de la Matière Condensée (LPMC), sous la direction du Prof. Daniel B. Ostrowsky [166]. Ce travail a été consacré à l'un des éléments clés de nombreux protocoles de communication quantique : la source de paires de photons intriqués. Compte tenu des limitations des sources de l'époque, il fallait opérer un véritable changement de paradigme à la fois en termes d'efficacité, de compacité, de compatibilité avec les réseaux de fibres optiques standards, et simplicité dans leur utilisation. L'optique intégrée non-linéaire, développée notamment par le LPMC via une "technologie propriétaire" mûre, offre, entre autres, l'ensemble de ces atouts. Mon travail de thèse a donc englobé la conception, la fabrication et l'utilisation de guides d'ondes intégrés sur substrats de niobate de lithium polarisés périodiquement (PPLN) en tant que nouveaux générateurs d'états intriqués basés sur le processus optique non-linéaire de fluorescence paramétrique (voir la Sec. 3.2 pour plus de détails). C'est grâce à une collaboration avec le 'Group of Applied Physics' (GAP) de l'Université de Genève dirigé par le Prof. Nicolas Gisin, que j'ai pu, à cette époque, mettre en exergue les qualités de ce type de générateurs. Nous verrons tout au long de ce rapport à quel point ce choix fut judicieux puisque les générateurs intégrés de paires de photons intriqués sont au cœur de (presque) toutes les expériences d'optique et de communication quantiques que j'ai pu développer en post-doctorat au GAP, et que je développe actuellement au LPMC à Nice en tant que Chargé de recherche au CNRS.

Avant de décliner ce petit résumé de mon travail de thèse et de post-doctorat, je m'autorise tout d'abord à effectuer quelques rappels de base (vraiment) en optique non-linéaire, que ce soit en régime de conversion paramétrique ou de génération de somme de fréquences.

3.1 Quelques bases d'optique non-linéaire

L'optique non-linéaire est aujourd'hui l'une des ressources clés de la communication quantique. D'une part, en régime de conversion paramétrique (SPDC¹), elle au cœur de 95% des sources de paires de photons intriqués qui ont été réalisées au cours des 20 dernières années. D'autre part, en régime de génération de somme de fréquences (SFG²), processus inverse de la conversion paramétrique, elle permet de changer la longueur d'onde d'un photon unique afin de bénéficier de détecteurs de photons plus performants : c'est le principe des détecteurs hybrides, ou 'up-conversion detectors' qui couplent optique non-linéaire et détecteurs de photons standards. Aussi, lorsque le processus SFG est rendu cohérent, les propriétés quantiques portées par le photon unique considéré peuvent être transférée d'une longueur d'onde à une autre : on parle alors de conversion cohérente de longueurs d'ondes, ou encore de 'photonic quantum interfaces'.

Nous rappelons dans ce qui suit les principes de base qui régissent les processus SPDC et SFG. Le lecteur spécialiste de l'optique non-linéaire, pourra avantageusement sauter ce chapitre.

3.1.1 Le processus de conversion paramétrique optique

Aujourd'hui, la méthode la plus utilisée pour générer des paires de photons intriqués repose sur le processus optique non-linéaire de conversion, ou fluorescence, paramétrique (SPDC). Ce processus spontané peut prendre place, sous certaines conditions d'accord de phase (voir la seconde Eq. du système 3.1), au sein de cristaux non centro-symétriques, autrement dit possédant une non-linéarité d'ordre 2. Comme le montre le schéma de principe de la FIGURE 3.1, cette non-linéarité est alors rendue effective lorsqu'un champ dit "de pompe" excite le cristal considéré au travers de son tenseur susceptibilité d'ordre 2 ($[\chi^{(2)}]$).

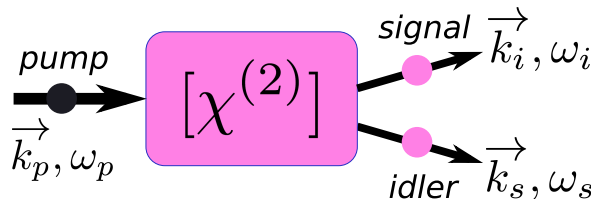


FIGURE 3.1: Schéma de principe du processus SPDC au sein d'un cristal non-linéaire d'ordre 2, c'est-à-dire possédant un tenseur susceptibilité de type $[\chi^{(2)}]$. Un photon issu d'un laser de pompe donne naissance à une paire de photons corrélés en énergie, en impulsion (voir le système d'Eqs. 3.1), et émis en même temps.

D'une manière générale, ce processus de conversion paramétrique met donc en jeu trois ondes, la pompe (p , incidente) et les photons générés, toujours appariés, communément appelés signal (s) et idler (i). Cette interaction est régie par les lois de conservation de l'énergie et de l'impulsion des photons, telles que :

$$\begin{cases} \omega_p &= \omega_s + \omega_i \\ \vec{k}_p &= \vec{k}_s + \vec{k}_i, \end{cases} \quad (3.1)$$

où ω_j et \vec{k}_j représentent respectivement l'énergie et l'impulsion de chaque photon, avec $j = \{p, s, i\}$. Notons que la seconde équation porte aussi le nom de condition d'accord de phase qui doit être satisfaite afin de rendre l'interaction efficace. L'accord de phase dépend alors des indices n_j du matériaux pris aux longueurs d'onde p , s , et i , ainsi que de la température à laquelle est porté le cristal utilisé. Dans le cas de cristaux massifs, l'accord de phase est généralement obtenu via l'exploitation de la biréfringence du cristal qui, lorsque la condition $n_p = n_{s,i}$ est remplie, simplifie considérablement la seconde équation du système 3.1. On parle alors d'accord de phase par biréfringence.

Dans le cas d'une interaction non-linéaire guidée, par exemple au sein d'un guide d'ondes intégré à la surface d'un matériau $[\chi^{(2)}]$, l'accord de phase par biréfringence est très difficile, voire impossible, à obtenir. En effet, les trois ondes en jeu dans l'interaction étant colinéaires, il faudrait, pour satisfaire ce type d'accord de phase, porter la température de l'échantillon à des valeurs proches du point de fusion. La stratégie communément employée pour satisfaire l'accord de phase est alors d'appliquer une micro-structuration au substrat qui consiste à renverser périodiquement le signe du coefficient non-linéaire mis en jeu dans l'interaction. C'est la cas par

1. Acronyme anglais pour spontaneous parametric down-conversion.

2. Acronyme anglais pour sum frequency generation.

exemple pour les guides d'ondes intégrés sur des substrats de niobate de lithium polarisés périodiquement, spécialité du LPMC, et plus connus sous l'appellation anglaise de 'periodically poled lithium niobate (PPLN) waveguides' [167]. La schéma de principe du processus de conversion paramétrique au sein d'un guide d'ondes PPLN est décrit en FIGURE 3.2.

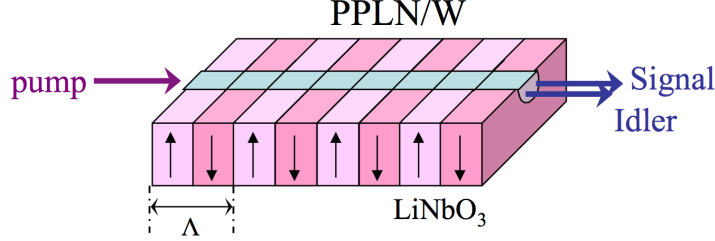


FIGURE 3.2: Schéma de principe du processus SPDC au sein d'un guide d'ondes PPLN. Les trois ondes, pompe, signal ; et idler, mises en jeu sont colinéaires. L'accord de phase est satisfait grâce à la micro-structuration du substrat de niobate de lithium, identifiée par le pas d'inversion Λ associé.

Dans ce cas, l'énergie et l'impulsion des photons doivent toujours être conservées, mais il apparaît pour la seconde équation un terme qui dépend de la micro-structuration du cristal et qui permet de compenser, selon la valeur qu'on lui donne à la fabrication, la dispersion du matériau pour les trois ondes mises en jeu. Il vient donc :

$$\begin{cases} \omega_p &= \omega_s + \omega_i \\ \vec{k}_p &= \vec{k}_s + \vec{k}_i + \frac{2\pi}{\Lambda} \vec{z}, \end{cases} \quad (3.2)$$

où Λ représente le pas d'inversion du signe du coefficient non-linéaire d'ordre 2 sélectionné par l'interaction. Notons cette fois que la seconde équation porte aussi le nom de condition de "quasi accord de phase" (QPM³). De là, en choisissant la valeur de Λ de manière appropriée, il est possible de générer tous les couples de longueurs d'ondes s et i dans la bande de transparence du matériau considéré. Dans le cas du niobate de lithium, cette bande s'étend de 350 nm à $\sim 5 \mu\text{m}$, ce qui est considérable.

L'intérêt d'utiliser des guides d'ondes PPLN pour la génération de paires de photons intriqués est triple :

- (i) D'une part, le confinement des ondes en interaction au sein du guide d'ondes permet d'améliorer grandement le rendement de cette interaction, comme nous le verrons aux Secs. 3.2 et 4.3.
- (ii) D'autre part, la collection des photons est rendue plus aisée qu'avec des cristaux massifs, puisqu'un simple 'pigtail' en sortie des composants doit suffire, du moins dans le cas idéal, à limiter les pertes associées au couplage dans les fibres optiques au standard des télécoms.
- (iii) Enfin, l'optique intégrée, comme l'indique l'article de revue porté en Réf. [4] de la Sec. 9.1, favorise, en général, la miniaturisation des briques de base utilisés pour la communication quantique. Outre la compacité, il en résulte une meilleure fiabilité pour les composants que nous qualifions aujourd'hui de type "photonique quantique intégrée" (voir aussi les Secs. 5.3 et 6.3).

Notons par ailleurs que, selon l'état de polarisation de la pompe et le coefficient non-linéaire mis en jeu au sein du tenseur $[\chi^{(2)}]$, plusieurs types d'interaction paramétrique peuvent être exploités, comme le résume le Tableau 3.1.

Nous verrons dans tout ce qui suit que les guides d'ondes intégrés sur substrats PPLN constitue le cœur de la plupart des expériences d'optique et de communication quantiques que j'ai développées au cours de ma carrière. Ces guides PPLN ont notamment été avantageusement utilisés pour générer des états intriqués en énergie-temps ou en time-bin (voir les Secs. 3.2 et 3.3.1), des états intriqués en polarisation (voir les Secs. 4.2, 4.2.5, et 4.3), ou encore des photons uniques annoncés (voir la Sec. 4.1).

3.1.2 Le processus de génération de somme de fréquences

Le processus de génération de somme de fréquences (SFG) correspond au processus inverse de la conversion paramétrique. Ainsi, comme le montre la FIGURE 3.3 pour un cristal non-linéaire d'ordre 2 ($[\chi^{(2)}]$), ce sont cette

3. Acronyme anglais pour quasi phase matching.

Type d'inter.	Polar. p	Polar. $\{s, i\}$	Coeff. NL	Intrication	Voir Section(s)
0	$ V\rangle$	$ V\rangle V\rangle$	d_{33}	ET/TB + Transfert TB \mapsto polar.	3.2, 3.3.1 4.3 et 4.4 [†]
I	$ H\rangle$	$ V\rangle V\rangle$	d_{31}	ET/TB	N/A [‡]
II	$ H\rangle$	$ H\rangle V\rangle$	d_{23}	Polar. + Transfert polar. \mapsto TB	4.2

TABLE 3.1: Tableau comparatif des différents types de conversion paramétrique pouvant être exploités au sein d'un cristal non-linéaire d'ordre 2, qu'il soit massif ou optique intégré. Dans le cas d'un guide d'ondes PPLN, et selon le type d'interaction, la mention 'Coeff. NL' correspond au coefficient non-linéaire du tenseur $[\chi^{(2)}]$ qui est sélectionné, alors que 'ET', 'TB' et 'Polar.' sont mis respectivement pour l'intrication établie sur les observables énergie-temps, time-bin, et polarisation. La dernière colonne du tableau indique dans quelle(s) section(s) sont discutés ces types d'interaction et les états intriqués correspondants. Notons que l'exploitation d'un type d'interaction, 0, I, ou II, n'est pas limité à une seule observable pour l'intrication. En effet, il est possible de transférer l'intrication d'une observable à une autre. [†] Cette étude est basée sur un générateur paramétrique de type semi-conducteur. [‡] Processus non utilisé dans mes travaux de recherche. Le lecteur pourra se reporter à l'article de revue porté en Réf. [106] pour trouver des réalisations qui mettent en jeu le processus de type-I.

fois deux champs en entrée du cristal, la pompe et le signal, qui donne naissance à un troisième champ dont la fréquence correspond à la somme des celles des deux premiers.

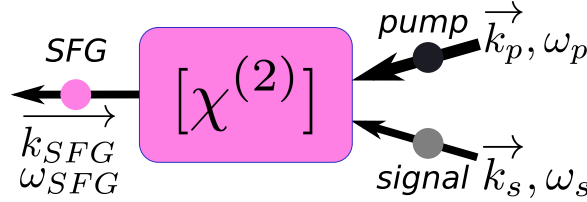


FIGURE 3.3: Schéma de principe du processus SFG au sein d'un cristal non-linéaire d'ordre 2, c'est-à-dire possédant un tenseur susceptibilité de type $[\chi^{(2)}]$. Un photon signal à la fréquence ω_s et un laser de pompe à la fréquence ω_p peuvent donner naissance à un photon à la fréquence ω_{SFG} qui correspond à la somme des fréquences d'entrée. Les lois de conservation de l'énergie et de l'impulsion des photons sont bien entendu toujours de mises (voir le système d'Eqs. 3.3).

Les Eqs. du système 3.1 sont bien entendu toujours valables, seules les notations changent. On a donc :

$$\begin{cases} \omega_p + \omega_s &= \omega_{SFG} \\ \vec{k}_p + \vec{k}_s &= \vec{k}_{SFG}, \end{cases} \quad (3.3)$$

où ω_j et \vec{k}_j représentent (toujours) respectivement l'énergie et l'impulsion de chaque photon, avec $j = \{p, s, SFG\}$. Notons que la seconde équation porte encore le nom de condition d'accord de phase qui doit être satisfaite afin de rendre l'interaction efficace, et ce selon les mêmes principes qui ce qui est discuté à la Sec. 3.1.1.

Dans le cas d'une interaction SFG non-linéaire guidée (figure non représentée mais identique à celle de la FIGURE 3.2 en prenant les sens des flèches et les notations de la FIGURE 3.3), par exemple au sein d'un guide d'ondes intégré à la surface d'un matériau $[\chi^{(2)}]$, l'accord de phase est e nouveau obtenue via le renversement périodique du signe du coefficient non-linéaire mis en jeu dans l'interaction. Dans ce cas, l'énergie et l'impulsion des photons doivent toujours être conservées, mais il apparaît de nouveau dans la seconde équation un terme qui dépend de la micro-structuration du cristal et qui permet de compenser, selon la valeur qu'on lui donne à la fabrication, la dispersion du matériau pour les trois ondes mises en jeu. Il vient donc :

$$\begin{cases} \omega_p + \omega_s &= \omega_{SFG} \\ \vec{k}_p + \vec{k}_s + \frac{2\pi}{\Lambda} \vec{z} &= \vec{k}_{SFG}, \end{cases} \quad (3.4)$$

où Λ représente toujours le pas d'inversion du signe du coefficient non-linéaire d'ordre 2 sélectionné par l'interaction, et la seconde équation porte encore le nom de "quasi accord de phase" (QPM). De là, en choisissant la valeur de Λ de manière appropriée, il est possible de générer toutes les fréquences *SFG* possibles, à partir du moment où les fréquences des trois champs en interaction appartiennent à la bande de transparence du matériau considéré.

De nouveau, l'intérêt d'utiliser des guides d'ondes PPLN pour mettre en œuvre le processus SFG est triple :

- (i) D'une part, le confinement des ondes en interaction au sein du guide d'ondes permet d'améliorer grandement le rendement de cette interaction, comme nous le verrons à la Sec. 3.3.
- (ii) D'autre part, la couplage des photons de pompe et signal est rendue plus aisée qu'avec des cristaux massifs, puisqu'un simple 'pigtail' en entrée des composants doit suffire, du moins dans le cas idéal, à limiter les pertes associées au couplage entre une fibre au standard des télécoms et le guide optique intégrée. Ceci marche d'autant mieux que les longueurs d'ondes pompe et signal sont proches en raison d'un problème de recouvrement spatial des modes excités au sein du guide intégré.
- (iii) Enfin, l'optique intégrée, comme l'indique l'article de revue porté en Réf. [4] de la Sec. 9.1, favorise, en général, la miniaturisation des briques de base utilisés pour la communication quantique. Outre la compacité, il en résulte une meilleure fiabilité pour les composants que nous qualifions aujourd'hui de type "photonique quantique intégrée" (voir aussi les Secs. 5.3 et 6.3).

Notons que le processus SFG est couramment utilisé comme outil de première caractérisation du processus SPDC. En effet, il est facile, pour une température de cristal donnée, de balayer, par exemple, en laser télécom accordable sur une très large plage afin d'observer à quelle longueur d'onde se situe l'accord de phase.

Enfin, il faut savoir que les règles de sélection de l'interaction SFG en fonction de la polarisation des trois champs sont les mêmes que celles présentées à la Sec. 3.1.1 pour le processus SPDC. Au cours de mes travaux concernant l'utilisation de la SFG au sein d'expériences de communication quantique, l'interaction qui a toujours été utilisée est celle de type-0 au sein de guides d'ondes PPLN, qui met en jeu trois champs de polarisation verticale (voir Sec. 3.3).

3.2 Sources de paires de photons intriqués à base d'optique non-linéaire intégrée

*Période concernée : 1^{er} octobre 1998 \mapsto 22 février 2002 (date de soutenance de thèse)
Université de Nice – Sophia Antipolis, LPMC.*

En résumé de ce travail, j'ai étudié et conçu expérimentalement deux nouvelles sources de paires de photons, intriqués en énergie-temps et en time-bin, basées sur un guide d'ondes intégré sur un substrat PPLN. Dans les deux cas, les photons appairés ont été créés, au sein du guide, par génération de fluorescence paramétrique via l'interaction d'un laser de pompe à 655 nm et la non-linéarité de type χ^2 présente dans le cristal de PPLN. En choisissant correctement la condition d'accord de phase (température du cristal et micro-structuration du substrat PPLN), il fut possible d'émettre les deux photons à la longueur d'onde dégénérée de 1310 nm (bande O des télécoms optiques), autorisant leur transport par fibre optique standard.

Les guides PPLN étudiés ont montré des efficacités de conversion, à savoir la probabilité de créer une paire de photons par photon issu du laser de pompe, supérieures à 10^{-6} . Ceci constitua une amélioration de 4 ordres de grandeur par rapport à l'état de l'art de l'époque essentiellement alimenté par des générateurs basés sur des cristaux non-linéaires massifs. L'efficacité de ces nouveaux générateurs a été caractérisée selon deux méthodes complémentaires, d'une part en régime de pompage continu, et d'autre part en régime de pompage impulsionnel.

Afin d'examiner la qualité des états intriqués produits, deux expériences d'interférométrie ont été conduites (on parle d'expériences de type "Franson", du nom de "l'inventeur" [84]), c'est-à-dire en régime de pompage soit continu soit impulsionnel, la qualité de l'intrication se mesurant alors via le contraste des franges d'interférence obtenues lorsque les deux photons sont détectés en coïncidence. Les résultats obtenus ont montré des contrastes supérieurs à 97% (pompage continu et intrication en énergie-temps) et 84% (pompage impulsionnel et intrication en 'time-bin'), donnant chacun une violation non ambiguë des inégalités de Bell, comme le discutent les Réfs.[1, 2] de la Sec. 9.1. Notons que cette dernière valeur fut portée à 96% très peu de temps après la fin de ma thèse, comme l'indique la Réf. [5] de la Sec. 9.1.

En conclusion, il fut remarqué que ces sources, basées sur un composant qui dérive d'une technologie associée à celles des télécommunications optiques standards, se posent en tant que très bonnes candidates pour l'implémentation de protocoles de communication quantique reposant sur l'intrication (en tant que ressource fondamentale) et possiblement établis sur longue distance.

Ce travail a par ailleurs donné lieu à quatre publications qui sont portées dans les Réfs. [1, 2, 5, 6] de la Sec. 9.1, et présenté lors d’une conférence SPIE en 2001 en Inde [1] (voir la Sec. 9.3), puis dans une version mettant en œuvre un encodage à trois dimensions (on parle, dans ce cas, de qtrits au lieu de qbits) lors de la conférence QCMC en 2004 [2] (voir la Sec. 9.3).

Nous allons voir par la suite combien le mariage d’une ressource fondamentale, telle que l’intrication, et de technologies éprouvées peut être hautement fructueux.

3.3 La génération de somme de fréquence au service de la communication quantique

Il n’est bien entendu pas possible de couvrir ici l’ensemble des travaux que j’ai pu mené durant ma carrière post-thèse de doctorat en ce qui concerne l’utilisation du processus de génération de somme de fréquences (SFG) pour servir la communication quantique. C’est pourquoi je me suis permis d’effectuer une sélection de travaux que je juge pertinente, ce afin de mettre en exergue les résultats les plus marquants que mes collaborateurs et moi-même avons pu obtenir. Ainsi, je propose dans ce qui suit quelques réalisations mettant en œuvre le processus SFG pour la réalisation d’une interface à conversion cohérent de longueurs d’ondes et pour la réalisation de détecteurs hybrides de photons télécoms insérés dans des cryptosystèmes quantiques.

*Période concernée essentiellement : 1^{er} mars 2002 \mapsto 30 janvier 2005,
University of Geneva, Group of Applied Physics.*

3.3.1 Interface quantique pour qbits photoniques

Comme je l’ai introduit dans l’introduction de ce manuscrit (voir Sec. 1.1), l’information quantique repose sur la possibilité de préparer des photons ou des atomes dans une superposition cohérente de plusieurs états, comme par exemple les états de polarisation vertical et horizontal du champ, les chemins court et long d’un interféromètre déséquilibré, ou encore deux ou plusieurs niveaux d’énergie. Lorsque cette superposition cohérente est faite sur deux (resp. d) états de base, on dit que l’on vient de préparer un qbit (b pour binary, resp. qdit). L’information quantique offre donc plus de possibilité que sa correspondante classique qui ne propose pour les bits que les états distincts 0 et 1, et jamais la superposition des deux. Cette information quantique repose en fait sur la cohérence existant entre les deux états choisis pour la préparation, ou en d’autres termes sur la relation de phase qui lie ces deux états. Toutefois, la nature de la particule porteuse n’a pas d’importance. En effet seules les amplitudes et les phases des états impliqués servent pour l’encodage de l’information. Il est bien entendu plus pratique d’utiliser les photons aux longueurs d’ondes des télécoms pour transporter des qbits sur de longues distances, alors que les atomes en cavité ou autres ions piégés servent préférentiellement à stocker l’information en vue de calculs quantiques [10]. C’est justement parce que la réalisation de mémoires quantiques capables de stocker cette information devient réaliste que j’ai développé, à l’Université de Genève, une interface quantique permettant une opération de transfert de cohérence entre un qbit porté par un photon télécom (appelé qbit “volant”) vers un qbit porté par un photon dont la longueur d’onde est proche des transitions atomiques de alcalins (appelé “qbit de stockage”). Le principe d’une telle interface et de sa démonstration expérimentale est montré sur la FIGURE 3.4 ci-dessous (voir aussi les Sec. 2.7.1 et 6.5 pour plus de détails sur les mémoires quantique).

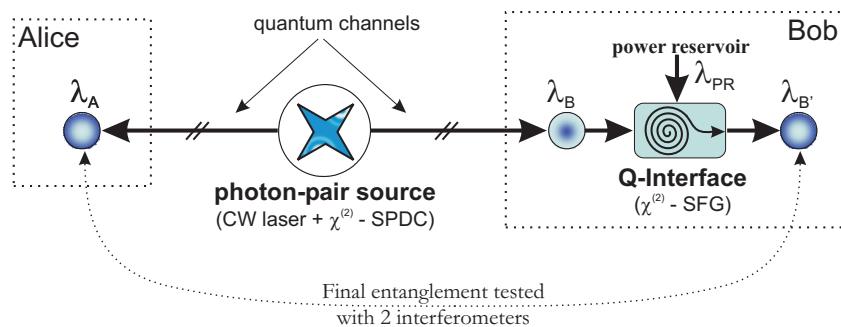


FIGURE 3.4: Principe d’une interface pour qbits photoniques.

Tout d'abord, une source produit, par conversion paramétrique (voir la Sec. 3.1.1), une paire de photons intriqués en énergie-temps dont les longueurs d'ondes sont notées λ_A et λ_B , respectivement envoyés à Alice et Bob. On peut dire ici que l'information quantique est partagée (ou cachée) entre les deux photons via cette intrication initiale. Ensuite, Bob procède au transfert de la partie de l'information entre le photon à la longueur d'onde λ_B vers un nouveau photon à la longueur d'onde $\lambda_{B'}$ via un processus de conversion de longueur d'onde basé sur la génération de somme de fréquences. Ce processus, *i.e.* inverse à la conversion paramétrique, est identique à celui qui est mis en œuvre pour la réalisation des détecteurs hybrides discutés à la Sec. 3.3.2. Toutefois, dans le cas présent, c'est la préservation de l'information quantique, autrement dit de l'intrication initiale, qui importe. En d'autres termes, il convient de vérifier que le transfert de cette intrication se fait de manière cohérente au travers du processus de conversion de longueur d'onde. L'intrication finale est par conséquent testée entre les photons λ_A et $\lambda_{B'}$ via une expérience d'interférence quantique à deux photons connue sous le nom "d'expérience de Franson" (voir la Sec. 2.4.2.2 pour plus de détails) [84]. Notons que l'idée sous-jacente est d'obtenir une longueur d'onde $\lambda_{B'}$ qui soit adaptée aux transitions atomiques permettant le stockage des qbits, comme c'est le cas certains atomes alcalins (voir la Sec. 6.5 pour plus de détails).

Plus spécifiquement et comme le montre la FIGURE 3.5 ci-dessous, l'expérience concerne le transfert d'un qbit porté par un photon à 1312 nm vers un photon à 712 nm via le processus de génération de somme de fréquence (SFG, ou "up-conversion") au sein d'un second cristal non-linéaire⁴. En effet, un multiplexeur en longueur d'onde (WDM) permet d'envoyer au sein de ce cristal les photons à 1312 nm ainsi qu'un fort réservoir de puissance à 1560 nm (laser cohérent + ampli erbium (EDFA)) qui permet cette conversion.

La cohérence de cette opération, à savoir le maintien ou non de l'intrication après le processus de conversion de longueur d'onde, est vérifiée par le test de Franson entre le nouveau photon à 712 nm et le photon restant à 1555 nm initialement intriqué avec le photon à 1312 nm et laissé au repos dans une boucle fibrée.

Ce test purement quantique nécessite l'adjonction de deux interféromètres de type Michelson déséquilibrés que j'ai développé moi-même. L'un, entièrement fibré, sert à l'analyse chez Alice de l'information portée par le photon à 1555 nm, alors que l'autre, fait d'optique standard, sert à l'analyse chez Bob de l'information portée par le photon à 712 nm. La mesure de la qualité de l'intrication finale, *i.e.* après le transfert non-linéaire, est faite sur les franges d'interférences du taux des coïncidences en sortie des deux interféromètres. Cette interférence varie en fonction de la somme des phases ϕ_A et ϕ_B appliquées dans les bras longs des interféromètres et donne une excellente visibilité de 97% (partie droite de la FIGURE 3.5). Ceci indique donc que l'état porté par les photons à 712 et 1555 nm est fidèle, à plus de 98%, à l'état intriqué initial porté par les photons à 1312 et 1555 nm.

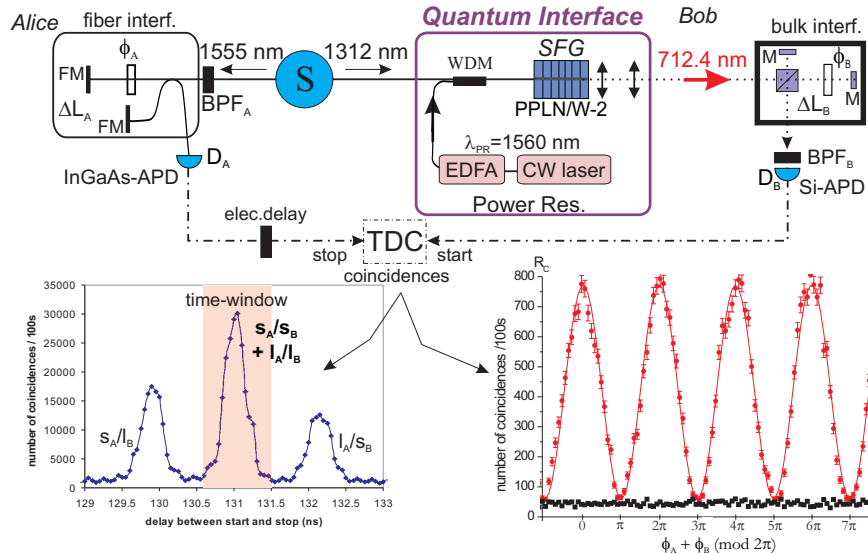


FIGURE 3.5: Schéma expérimental (haut) et résultats obtenus pour l'interface quantique. Est représenté en bas à gauche l'histogramme des coïncidences après la conversion de la longueur d'onde de l'un des deux photons, et en bas à droite, les franges d'interférence obtenues entre le photons à 712 nm (converti) et le photon à 1555 nm. La visibilité des franges approche les 100%, montrant que la conversion est bien cohérente.

Précisons que les deux cristaux non-linéaires employés dans cette expérience sont deux guides PPLN de

4. Le premier est celui qui a donné naissance à la paire de photons initiale.

type-0 (voir Tableau 3.1) qui proviennent du LPMC et qui ont été dessinés pour remplir le cahier des charges de l'expérience Interface. D'une part, le guide responsable de la génération paramétrique permet, à partir d'une pompe à 711 nm, de créer très efficacement des paires de photons dont les longueurs d'ondes sont centrées autour de 1312 et 1555 nm. D'autre part, le second guide, couplé au réservoir de puissance cohérent à 1560 nm, permet la conversion de longueur d'onde 1312 nm \mapsto 712 nm du photon chez Bob. Notons que la différence entre les longueurs d'ondes de départ (711 nm) et d'arrivée (712 nm) est un choix qui a pour but de montrer que leur identité ne revêt aucune importance. Aussi, compte tenu de la nécessité des deux interactions quadratiques successives, cette expérience ne serait pas réalisable avec des cristaux massifs trop peu efficaces comparativement à nos guides PPLN.

Notons également que c'est bien la cohérence du réservoir de puissance qui permet de transférer l'état intriqué depuis la paire initiale 1312/1555 nm vers la paire désormais constituée du photon à 712 nm et du photon à 1555 nm. Aussi, il convient de préciser que la longueur d'onde de 712 nm ne correspond à aucune transition alcaline favorable pour le stockage des qbits. Il faut donc considérer l'expérience décrite ci-dessus comme une preuve de principe.

Par ailleurs, la démonstration ci-dessus revêt un caractère "universel" dans le sens où préserver l'intrication au travers d'une opération de conversion de fréquences faite sur l'un des deux photons de la paire couvre, en une seule mesure, l'ensemble des états de qbits individuels accessibles sur la sphère de Bloch-Poincaré (voir la FIGURE 2.4). En effet, cette opération, unitaire du point de vue quantique, imposerait dans le cas de la préparation de qbits individuels d'effectuer l'expérience pour, au moins, tous les pôles bien connus de la sphère afin de prouver la pertinence de la conversion. Sachant qu'un état intriqué est non séparable (voir le Sec. 2.4.1), et donc que l'état des qbits individuels qui le composent ne sont pas définis, tous les points de la surface de la sphère sont transposés d'un seul coup grâce à l'intrication.

Les détails du principe de l'expérience, son analyse théorique, ainsi que l'ensemble des résultats qui s'y rapportent ont été publiés en 2005 dans la revue Nature, voir la Réf. [3] de la Sec. 9.1. Ces résultats ont également fait l'objet d'une sélection par la revue Optics & Photonics News dans le cadre du numéro spécial "Optics in 2005", voir la Réf. [1] de la Sec. 9.2.

Notons enfin l'existence d'une réalisation concurrente, faite en 2003 par Giorgi et ses collaborateurs, qui démontrèrent la transposition fréquentielle de qbits uniques, toujours via le processus SFG [168]. Toutefois, cette expérience perd de fait le caractère "universel" associé à la préservation de l'intrication comme c'est le cas de celle que nous venons de décrire. Des versions plus récentes (2010) de l'expérience de Giorgi ont été réalisées en régime de conversion paramétrique à photons uniques⁵ par Curtz et ses collaborateurs [169] et par Takesue [170].

3.3.2 Cryptosystèmes quantiques avec détection de photons par conversion de longueur d'onde

Les travaux discutés dans cette section concernent des projets dans lesquels j'étais engagé lors de mon séjour post-doctoral à l'Université de Genève et que j'ai suivi de très près depuis ma prise de fonction au CNRS et notamment au cours des deux dernières années. Ces travaux ont abouti à des publications dans des revues internationales au cours des années 2006 et 2008. Précisons aussi que j'étais co-responsable des deux doctorants en charge de ces réalisations expérimentales.

Les dispositifs à comptage de photons ont largement été utilisés au cours de ces dernières années et ce pour de nombreuses applications allant de l'imagerie à la spectroscopie, en passant par la métrologie. La popularité de ces compteurs de photons est en grande partie due à l'existence de photodiodes à avalanches en Silicium (APD-Si) dont les très bonnes performances peuvent être résumées ainsi : haute efficacité de détection (jusqu'à 60%) dans le domaine du visible (400-800 nm), très haute résolution temporelle (jitter aussi court que 40 ps pour certaines photodiodes), taux de comptage maximal très élevé (quelques Mcps/s), et enfin taux de coups sombres très faibles (de l'ordre de la dizaine de coups par seconde).

Toutefois, comme je l'ai laissé entendre dans la section précédente, si l'on veut détecter des photons de plus haute longueur d'onde, comme c'est le cas dans les expériences de communication quantique établies aux lon-

5. Contrairement au processus SFG, le processus SPDC en régime de photons uniques implique des photons signal de courte longueur d'onde et un laser pompe de plus grande longueur d'onde. En langage optique non-linéaire ce processus est également connu sous le nom de génération de différence de fréquences.

guez d'ondes des télécommunications, nous sommes contraints d'utiliser d'autres types de photodiodes basées sur les technologies du Germanium (photons à 1310 nm) ou de l'InGaAs (photons à 1310 et à 1550 nm). Malgré leur faible efficacité de détection (20% tout au plus), leur mauvaise résolution temporelle (300 à 400 ps de jitter), leur faible taux de comptage maximal (quelques centaines de kcps/s), et leur niveau de bruit élevé (100 à 1000 fois plus que dans les APD-Si), ces dispositifs ont été employés dans de nombreux protocoles quantiques, allant des démonstrations fondamentales de la non-localité aux expériences beaucoup plus appliquées de cryptographie quantique sur longue distance.

Encore plus problématique, il n'existe aucun dispositif permettant de compter les photons lorsque ceux-ci possèdent des longueurs d'ondes aussi hautes que celles appartenant à la bande du moyen infrarouge (MIR). Cette bande, qui s'étend de 3 à 20 μm , peut être avantageusement employée pour des protocoles de cryptographie quantique à l'air libre car elle est beaucoup moins sensible aux perturbations atmosphériques que ne le sont les longueurs d'ondes plus basses.

Nos deux projets avaient donc pour but de palier à ces problèmes de détection, aussi bien pour les photons à 1550 nm (bande C des télécoms optiques) que pour des photons à 4.6 μm (bande MIR). La solution employée fut la conversion de longueur d'onde via le processus non-linéaire de somme de fréquences afin d'abaisser la longueur d'onde initiale des photons vers la bande de détection des APD-Si décrites plus haut. C'est ce que nous avons appelé des détecteurs hybrides. Voici donc, dans ce qui suit, ce que nous avons réalisé.

Notons également que les tenants et les aboutissants en matière de cryptographie quantique sont présentés à la Sec. 2.5.

3.3.2.1 Cryptosystème quantique tout fibré à haut débit

Ce travail représente une partie de la thèse de Robert T. Thew que j'ai co-encadrée, voir la Sec. 8.2.2.3 pour plus de détails.

Nous avons développé un cryptosystème quantique pouvant pleinement bénéficier des performances des APD-Si. Le schéma de l'expérience correspondante est donnée en FIGURE 3.6.

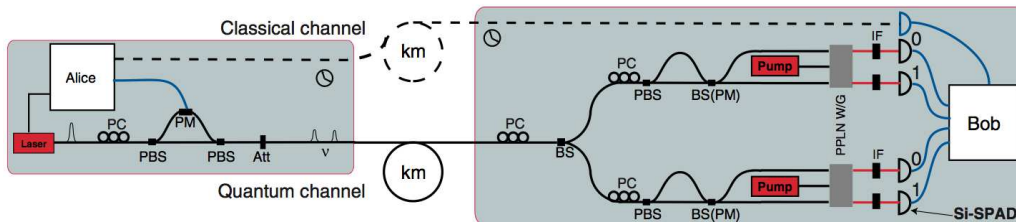


FIGURE 3.6: Schéma du cryptosystème time-bin haut débit fonctionnant à 1550 nm. Chez Alice, un laser cadencé à un taux de répétition de 1.27 GHz et fortement atténué sert de source de photons uniques. Alice dispose également d'un interféromètre afin de préparer des qbits codés en time-bin sur les photons à 1550 nm. Alice peut choisir sa base d'encodage à l'aide d'un modulateur électro-optique placé dans le bras long de son interféromètre. Ce modulateur peut être sollicité à l'aide du trigger (horloge) du laser. Les qbits photoniques sont ensuite envoyés à Bob par un canal fibre optique. Ceux-ci sont alors soumis à un choix passif de la base d'analyse grâce à un beam-splitter 50/50 qui dirige aléatoirement les photons vers l'interféromètre du haut ou du bas chez Bob. La détection des photons se fait à l'aide de détecteurs hybrides (voir FIGURE 3.7) et les événements sont enregistrés après récupération de l'horloge du laser. Ce cryptosystème, qui a nécessité une bonne part d'ingénierie, nous a permis d'établir des clés secrètes à des taux avoisinant le MHz.

En effet, l'idée était d'obtenir des hauts débits (de l'ordre du MHz) pour le taux d'établissement de clés en partant d'un laser impulsionnel cadencé au GHz. C'est ce laser qui, fortement atténué, nous a servi de source de photons uniques. Nous avons aussi utilisé des APD-Si particulières dont la résolution temporelle était de l'ordre de 40 ps, ce qui n'est pas commun. La conversion de longueur s'est faite via un guide PPLN et un laser de pompe à 980 nm, pour une longueur d'onde obtenue en sortie de cristal de 600 nm parfaitement compatible avec le silicium. La haute efficacité de conversion du guide nous a permis d'utiliser une simple diode laser de pompe de 400 mW. Ce type de diode laser est un produit standard de l'industrie des télécoms puisque ce sont elles qui servent de laser de pompe aux amplificateurs erbium. Après le guide, un dispositif de filtrage par prisme très performant a été mis en place afin de ne garder que les photons à 600 nm, tout en rejetant le reste de la pompe à 980 nm non utilisée, comme le montre la FIGURE 3.7 ci-après.

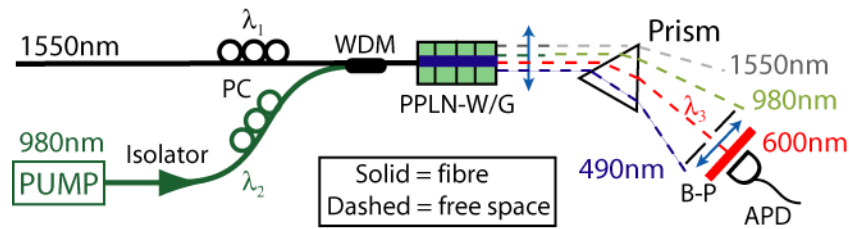


FIGURE 3.7: Schéma interne de notre détecteur hybride. Une fibre amène les photons à 1550 nm ainsi que le pompe au sein du guide PPLN où se produit la conversion non-linéaire. En sortie, un filtrage spatial et spectral permet d'éliminer toutes les longueurs d'ondes indésirables pour ne conserver que les photons à 600 nm.

Ainsi les deux détecteurs hybrides que nous avons réalisés ont montré des efficacités globales (toutes pertes dans les divers filtres incluses) comprises entre 5 et 7% et des taux de coups sombres de l'ordre 30 kcps/s. Ces caractéristiques sont exactement celles des photodiodes InGaAs communément employées pour la détection des photons à 1550 nm. Toutefois, il ne faut pas perdre de vue que nos détecteurs offrent une résolution temporelle 10 fois meilleure, un taux maximal de comptage 50 fois plus grand, et enfin qu'ils peuvent opérer en mode continu, c'est-à-dire que nous n'avons pas besoin de les déclencher comme c'est le cas avec la technologie InGaAs, voir la Réf. [7] de la Sec. 9.1.

Si l'efficacité de détection est conforme à ce que l'on s'attendait, le bruit l'était moins à l'époque où nous avons construit ces détecteurs. Plusieurs hypothèses pouvaient alors être envisagées : processus non-linéaire parasite de fluorescence paramétrique non accordé, effet Raman, effet d'un poling périodique imparfait, ou encore impuretés de type ions métalliques au sein du cristal non-linéaire.

Note :

Une étude à la fois théorique et expérimentale menée par mon équipe au LPMC sur le même type d'arrangement a permis de discriminer, au moins dans le cadre de la configuration expérimentale de la FIGURE 3.7. En effet, l'une des particularités que nous avons mis en évidence, et ce uniquement en régime comptage de photons, est que la réponse des détecteurs hybrides en termes de bruit évolue de façon non-linéaire avec la puissance de pompe, éliminant de fait les effets de génération de photons parasites via des impuretés qui aurait un comportement linéaire en fonction de la puissance de la pompe. D'autre part, les règles de sélection en polarisation liée à l'effet Raman sont incompatibles avec le fait que nos structures guidantes ne supportent que le mode de polarisation vertical. Nous avons donc conclu, via une méthodologie expérimentale adéquate, mettant en jeu un guide d'ondes PPLN fait maison, que l'effet responsable de la production de photons parasites était dû à une cascade d'effets non-linéaires. En la seule présence de la pompe à 980 nm, un photon issu de ce laser peut se convertir, par fluorescence paramétrique de type Cerenkov non accordée en phase, en une paire de photons, l'un autour de 1550 nm, et l'autre à 2660 nm par un processus de type Cerenkov. Pour ce type d'interaction, le photon de plus haute longueur d'onde n'est pas guidé dans la structure (longueur d'onde au-delà de la coupure du guide) et est donc rayonné dans le substrat de niobate de lithium, alors que celui de plus courte longueur d'onde est émis sur une largeur spectrale très large. Par suite, le photon à 1550 nm ainsi créé peut, en présence de la pompe intense, être converti vers la bande d'intérêt (600 nm) par génération de somme de fréquence. L'ensemble de ce travail est reporté dans la Réf. [5] de la Sec. 9.3.

Toutefois, il convient de mentionner que l'effet est aussi responsable de bons nombres de problèmes de bruit additionnel dans les détecteurs hybrides comme le rapportent les publications portées en Refs. [171, 172, 173]. Il est enfin intéressant de noter que la configuration de l'interface photonique discutée à la Sec. 3.3.1 ci-dessus, aurait sans doute été également polluée par du bruit Raman si les longueurs de la pompe (1560 nm) et du signal (1312 nm) n'avaient pas été aussi éloignées [174].

3.3.2.2 Détection des photons à 4.6 μm pour la cryptographie quantique à l'air libre

Ce travail représente une partie de la thèse de Guilherme Temporao que j'ai co-encadrée, voir la Sec. 8.2.2.3 pour plus de détails.

L'idée était de développer une expérience de cryptographie quantique à l'air libre grâce à l'avancée des lasers à

cascade quantique (QCL) qui émettent dans la bande du moyen infrarouge (MIR). Par le biais d'une collaboration avec l'Université de Neuchâtel qui nous a fourni un de leurs lasers à $4.6\ \mu\text{m}$ que nous avons utilisé comme source de photons uniques, nous avons pu tester la faisabilité d'une telle expérience via le développement d'un détecteur hybride lui aussi basé sur la conversion de longueur d'onde. Jusque là, les expériences de cryptographie quantique à l'air libre reposaient sur des photons aux longueurs d'ondes du visible et étaient par conséquent limitées à fonctionner uniquement les jours où le ciel est parfaitement clair.

Pour la détection des photons MIR, nous avons donc employé, comme le montre la FIGURE 3.8, un cristal massif de PPLN (les guides supportent difficilement la longueur d'onde de $4.6\ \mu\text{m}$) et de nouveau une diode laser de pompe à 980 nm. L'accord de phase a été choisi de sorte à obtenir en sortie du cristal des photons à 800 nm, c'est-à-dire capable d'être vu par une photodiode Silicium. Après un système de filtrage adéquat, nous avons pu mesurer une efficacité de détection globale de $5 \cdot 10^{-5}$, ce qui est très faible mais est très proche de ce à quoi nous nous attendions. Ceci peut être amélioré grâce à l'utilisation de cristaux plus efficaces et de lasers de pompe plus puissants.

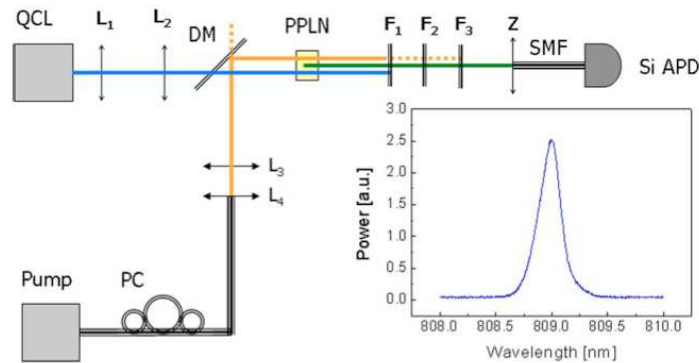


FIGURE 3.8: Schéma du détecteur hybride pour photons MIR. Un laser à cascade quantique (QCL) impulsionnel, atténué à quelques centaines de photons par impulsion, émet à la longueur d'onde de $4.6\ \mu\text{m}$ (MIR). Les photons sont envoyés au sein d'un cristal PPLN massif au travers d'un miroir dichroïque (DM) et via un télescope fait de deux lentilles en germanium (L_1 et L_2). Le laser de pompe à 980 nm est également envoyé au sein du cristal via le dichroïque. Après un étage de filtrage approprié, les photons à 800 nm, résultant de la génération de somme de fréquences, sont détectés à l'aide d'une photodiode à avalanche en silicium (Si-APD).

Le second but de cette expérience était de caractériser le bruit supplémentaire que nous pouvions obtenir à cause du rayonnement de type corps noir présent dans l'atmosphère aux longueurs d'ondes MIR et incident sur notre cristal. En faisant varier la température de notre cristal non-linéaire entre 25 et $93\ ^\circ\text{C}$ et en coupant le QCL, nous avons pu mesurer des taux de bruit allant de 88 à 133 cps/s incluant les coups sombres internes à la photodiode (50 cps/s dans notre cas). Nous en avons conclu que les effets de ce rayonnement parasite n'était pas rédhibitoire pour l'implémentation d'une expérience de cryptographie à cette longueur d'onde.

Par ailleurs, nous avons vu que la résolution temporelle de notre détecteur hybride était la même que celle de la photodiode Silicium (400 ps dans ce cas) et que par conséquent nous avons fabriqué un détecteur de photons MIR beaucoup plus rapide (facteur 50) que ce qui est disponible dans le commerce ! Ces travaux ont été publiés dans la revue *Opt. Lett.*, voir la Réf. [8] de la Sec. 9.1.

Enfin, nous avons tenu à évaluer la faisabilité ainsi que les performances d'un cryptosystème à l'air libre fonctionnant dans la bande MIR et basé sur l'utilisation du type de détecteurs que je viens juste de décrire. Nous avons donc mis en place deux interlocuteurs, Alice chez qui s'opère l'encodage de qbits sur l'observable polarisation de pseudo photons uniques émis par un QCL atténué, et Bob chez qui s'opère la détection des qbits grâce au détecteur décrit plus haut. Dans la pratique Alice et Bob étaient séparés par quelques mètres au sein d'un même laboratoire. Nous avons montré par cette expérience de principe appuyée par un modèle théorique que notre cryptosystème MIR serait très peu affecté par des conditions atmosphériques de type "brouillard" alors que les autres cryptosystèmes, basés sur la bande du proche infrarouge (NIR), ne fonctionneraient tout simplement pas. Toutefois, la faible efficacité de détection de notre détecteur, réduisant considérablement le taux qbits transmis, rend notre système MIR inefficace par rapport aux autres systèmes NIR lorsque les conditions atmosphériques sont idéales, voir la Réf. [9] de la Sec. 9.1.

Chapitre 4

Sources photoniques pour la communication quantique

Il n'est bien entendu pas possible de couvrir ici l'ensemble des travaux que j'ai pu mené durant ma carrière post-thèse de doctorat en ce qui concerne les sources photoniques pour la communication quantique. C'est pourquoi je me suis permis d'effectuer une sélection de travaux que je juge pertinente, ce afin de mettre en exergue les résultats les plus marquants que mon équipe et moi-même avons pu obtenir. Ainsi, je propose dans ce qui suit quelques réalisations concernant des sources de photons uniques annoncés, de paires de photons intriqués en polarisation, ou en time-bin, toutes émettant aux longueurs d'ondes des télécommunications et basées sur des générateurs non-linéaires intégrés.

*Période concernée : 1^{er} février 2005 (date d'entrée au CNRS) \mapsto aujourd'hui,
LPMC, CNRS & Université de Nice – Sophia Antipolis, en tant que Chargé de Recherche au CNRS.*

Notons également que le lecteur intéressé par les tenants et les aboutissants en matière de source de photons uniques et de paires de photons intriqués pourra avantageusement se diriger vers les Secs. [2.3](#) et [2.4](#).

4.1 Source de photons uniques annoncés à 1550 nm

Bien 'qu'exilé' en post-doctorat à Genève, j'ai continué à collaborer fortement avec le LPMC, notamment avec Olivier Alibart dont les travaux ci-dessous, initiés à la fin de ma thèse, représentent le cœur de la sienne.

Que ce soit pour les expériences fondamentales ou pour les cryptosystèmes quantiques, les physiciens rêvent d'implémentations efficaces de sources émettant des photons uniques à la demande. Une source de photons uniques est caractérisée par trois paramètres principaux, généralement notés P_0 , P_1 , et P_2 , pour probabilité d'émettre respectivement aucun, un, et deux photons à la fois. Notons que plus P_0 est élevée plus le rapport signal/bruit d'une éventuelle ligne de communication sera élevé, P_1 qualifie l'efficacité de la source, alors que P_2 doit être maintenue la plus petite possible pour garantir la sécurité des protocoles de cryptographie quantique. Sachant que la solution de type laser impulsif atténué présente des limitations fortes en raison de la statistique poissonnienne d'émission des photons, de nombreuses ont été explorées. L'idée est alors d'avoir un système isolé présentant deux niveaux d'énergie et permettant la génération de photons uniques. Dans ce cadre, les réalisations les plus abouties reposent sur la désexcitation des centres colorés dans le diamant ou encore d'excitons dans les boîtes quantiques semi-conductrices. Si celles-ci, de par leur principe de fonctionnement intrinsèque, correspondent bien au comportement type "photons uniques à la demande", les premières souffrent de trop faibles taux de collection des photons (quelques %) alors que les secondes opèrent à très basses températures (50 mK). Par ailleurs transposer ce type de sources dans les bandes des télécoms paraît encore aujourd'hui relativement compliqué.

C'est pourquoi la solution que nous avons retenue repose sur la création de paires de photons au sein d'un cristal non-linéaire et de l'utilisation de l'un des deux photons comme un trigger qui annonce l'existence et conditionne la détection du photon complémentaire choisi à la longueur d'onde de 1550 nm. C'est le principe d'une source de photons uniques annoncés (HSPS, acronyme anglais pour 'heralded single photon source'). A cet effet, nous avons déjà montré en 2005 une première réalisation de ce type de source montée autour d'un guide PPLN. En suivant le principe général de la source donné en FIGURE 4.1, l'idée était d'utiliser un laser de pompe CW à 710 nm afin de créer des paires de photons, par conversion paramétrique, dont les longueurs d'ondes sont respectivement centrées autour de 1310 nm (signal) et 1550 nm (idler). Pour obtenir une telle interaction, le pas d'inversion Λ du signe du coefficient non-linéaire nécessaire fut de 14 μm . Après séparation des photons

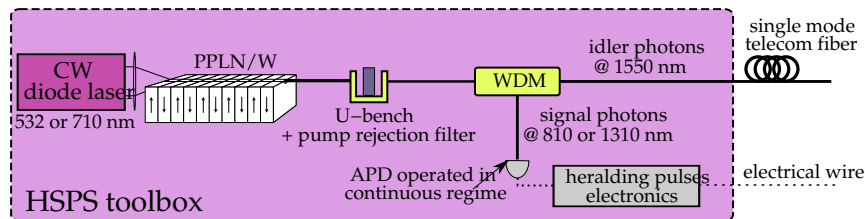


FIGURE 4.1: Source de photons annoncés (HSPS) à 1550 nm. Cette réalisation est versatile puisqu'il suffit de changer la période d'inversion du guide d'ondes PPLN et la longueur d'onde du laser de pompe pour changer la longueur d'onde du signal tout en préservant celle de l'idler à 1550 nm. Par exemple les deux interactions qui nous intéressent sont : 710 nm \mapsto {1310 & 1550 nm} et 532 nm \mapsto {810 & 1550 nm}. Notons qu'une telle source possède deux sorties : une fibre optique standard guidant les photons à 1550 nm et un câble électrique.

d'une même paire grâce à un démultiplexeur en longueurs d'ondes fibré (WDM), le photon signal à 1310 nm est détecté grâce à une photodiode à avalanche (APD) Germanium qui permet d'annoncer (trigger) le départ du photon idler à 1550 nm et par conséquent son arrivée sur un détecteur de type APD-InGaAs (non représenté). Contrairement aux lasers atténués, l'effet néfaste de la probabilité P_0 n'est ici que trop peu contrecarré car l'InGaAs ne s'ouvre que lorsqu'un photon à 1550 nm est véritablement annoncé par son compagnon. L'avantage de cette technique est toutefois double : d'une part le détecteur qui assure le trigger opère en régime continu, c'est-à-dire qu'il n'a pas besoin d'une référence temporelle pour détecter les photons à 1310 nm ; d'autre part le mode de détection déclenché sur le photon annoncé permet de réduire le bruit apparent sur la ligne à 1550 nm.

Les résultats que nous avons obtenus avec cette source donnèrent, pour une puissance de pompe de 20 μW à 710 nm et après détection du trigger à raison de 93 kcps/s, une probabilité P_1 de 0.4, c'est-à-dire quatre fois meilleure que celle du laser atténué et, dans le même temps, des probabilités P_0 et P_2 plus faibles, respectivement de 0.6 et de 5×10^{-3} . Malgré tout, P_0 reste assez élevée à cause des coups sombres dans l'APD-Ge (environ 30 kcps/s) qui déclenchent l'InGaAs pour rien. En l'état, ces résultats sont néanmoins les meilleurs obtenus à ce jour en configuration guidée. Enfin, la compacité et la stabilité de cette "boîte noire" permettra justement une insertion facile au sein d'un réseau télécom.

Ce travail a été publié dans la revue Opt. Lett. en 2005, voir la Réf. [10] de la Sec. 9.1, et notamment présentée lors de deux conférences SPIE fin 2004 et fin 2005 en Inde [3, 4] (Sec. 9.3).

4.1.1 Interférométrie de Sagnac à photons uniques

Toujours 'exilé' en post-doctorat à Genève, ce travail représente, sur l'une de mes idées, une partie de la thèse de Guillaume Bertocchi.

Posséder une source de photons uniques annoncés au laboratoire présente un certain nombre d'intérêts pouvant aller de la (simple) vitrine technologique à la calibration de détecteurs de photons, en passant par la démonstration d'effets plus intéressants liés à l'interférométrie. C'est plus particulièrement à l'effet Sagnac que nous nous sommes intéressé. D'une part, ceci nous a permis de vérifier à quel point les photons émis étaient identiques du point de vue de la cohérence. D'autre part, cette expérience a été proposée dans le but d'offrir une possible alternative aux gyroscopes à fibre dont la limitation dépend essentiellement des effets non-linéaires présents dans les fibres utilisées.

En 1913, Sagnac démontrait qu'il était possible de détecter une rotation par rapport à un référentiel de référence, avec un système optique fermé : la rotation induit en effet une différence de phase entre les 2 chemins possibles qui s'écrit, dans le cas d'une fibre optique bobinée sur un support, comme

$$\Delta\phi = \frac{2\pi LD}{\lambda c} \Omega, \quad (4.1)$$

où D est le diamètre de la bobine, $L = N\pi D$ la longueur totale de la fibre, N le nombre de tours, et Ω la vitesse angulaire de rotation du système.

L'un des problèmes rencontrés dans les gyroscopes à fibre optique est lié à un effet non-linéaire lorsque la puissance de la lumière injectée est trop forte : c'est l'effet Kerr optique qui perturbe la mesure. Une façon simple de réduire cet effet indésirable est de baisser la puissance utilisée. Dans notre cas, nous avons mis en œuvre la limite ultime puisque ce sont les photons uniques provenant de la source décrite au paragraphe précédent qui ont été utilisés. Dans ce cas, suivant une description quantique, un photon, après propagation dans l'interféromètre est dans l'état

$$|\psi\rangle = \frac{1}{\sqrt{2}} (|l\rangle + e^{i\Delta\phi}|r\rangle), \quad (4.2)$$

où $|l\rangle$ correspond au parcours de sens direct, et $|r\rangle$ au parcours de sens indirect. Comme ces 2 chemins sont indiscernables, nous attendons, en sortie du dispositif, une figure d'interférence au premier ordre, c'est-à-dire provenant de la superposition cohérente entre deux états possibles pour chacun des photons uniques envoyés. En d'autres termes, le taux de comptage des photons enregistré dans l'une des 2 sorties de l'interféromètre doit être proportionnel à $\sin^2(\Delta\phi)$ alors que dans l'autre ce taux doit osciller comme la fonction complémentaire $\cos^2(\Delta\phi)$. Une des principales difficultés rencontrées pour montrer l'effet Sagnac est que l'on doit mettre en rotation l'ensemble du montage qui inclut ici la source de photons uniques, l'interféromètre, et le système de détection comprenant des photodiodes à avalanches et l'électronique associée, ce qui est difficilement réalisable. Pour éviter cette difficulté et comme le montre la FIGURE 4.2(a), seule une partie du montage a été mise en rotation : la boucle fibrée de Sagnac. Ceci a été rendu possible grâce au fait que dans cette expérience, l'essentiel du transport des photons depuis la source jusqu'aux détecteurs, est facilité par l'utilisation de fibres optiques au standard des télécoms. Dans notre montage, nous avons utilisé une boucle fibrée de 600 m, bobinée sur une platine tournante, dont la vitesse de rotation est contrôlée.

Ces photons entrent dans l'interféromètre via un diviseur de faisceau (BS pour 'beam-splitter') qui permet d'orienter ces photons selon le sens direct ou inverse de la boucle tournante avec une probabilité de $\frac{1}{2}$. Après propagation dans l'interféromètre, ces photons ressortent et sont dirigés vers l'un des 2 détecteurs (APD, pour "avalanche photodiode") via le même diviseur de faisceau. Le circulateur (C) est là pour permettre de récupérer les photons qui prennent la sortie "gauche de l'interféromètre, c'est-à-dire en direction de la source. Avec cette astuce, on a donc accès aux deux sorties complémentaires de l'interféromètre ce qui nous a permis d'obtenir les deux figures d'interférence complémentaires décrites précédemment, chacune via l'un des détecteurs. Comme le montre la FIGURE 4.2(b), les visibilités des franges ainsi obtenues sont supérieures à 99% ce qui témoigne de l'excellente stabilité de l'interféromètre. Bien que nous ayons éliminé tout problème lié à un effet non-linéaire indésirable, une utilisation pratique de cet interféromètre au sein d'un véritable gyroscope serait limitée par les temps d'intégration des mesures qui dans ce cas, en raison du faible débit de photons uniques, sont trop longs

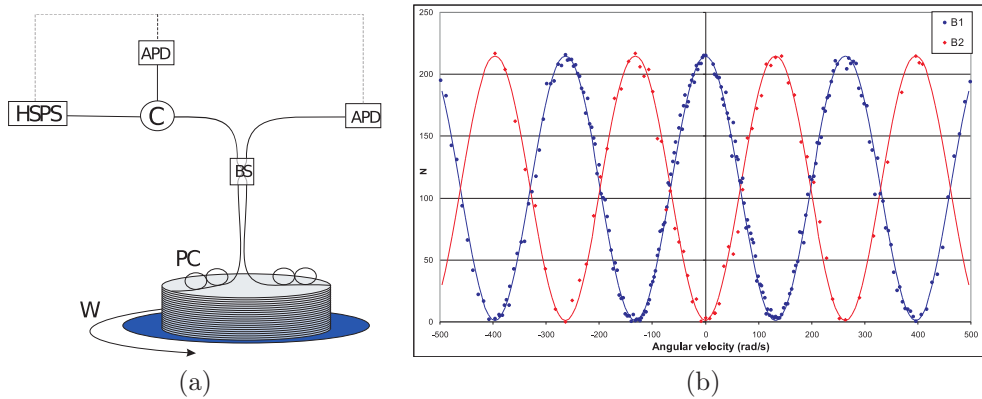


FIGURE 4.2: (a) : Synoptique de l'interféromètre de Sagnac tout fibré dans lequel entrent les photons uniques à la longueur d'onde de 1550 nm. (b) : Diagrammes d'interférence relatifs aux deux sorties complémentaires de l'interféromètre.

pour répondre aux standards actuellement requis pour ce type d'appareils. Cette expérience d'interférométrie Sagnac à photons uniques a été conduite par Guillaume Bertocchi (doctorant à l'époque), a fait l'objet d'une publication dans *J. Phys. B*, voir la Réf. [11] de la Sec. 9.1 et d'un "Research highlight" dans la revue *Nature* en 2006, voir la Réf. [2] de la Sec. 9.2.

4.1.2 Extension de la source

Ce travail les travaux de post-doctorat de Sorin Tascu, voir la Sec. 8.2.2.3 pour plus de détails.

Afin d'éviter le problème de P_0 trop élevé, il faut jouer avec un photon trigger de plus basse longueur d'onde afin de pouvoir utiliser un détecteur plus efficace et surtout moins bruité, tels que ceux reposant sur la technologie du silicium. Par exemple, en pompant un guide PPLN de période adéquate avec un laser à 532 nm, il est possible de créer des paires de photons dont les longueurs d'ondes sont centrées autour de 810 (au lieu de 1310 nm) et 1550 nm. Ainsi, nous obtenons deux avantages supplémentaires :

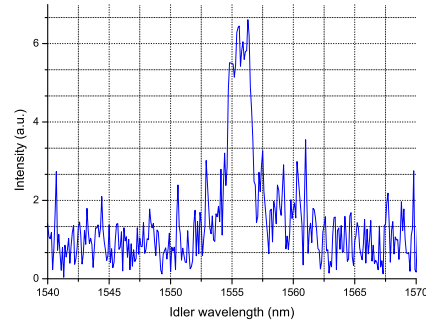
- le trigger entre dans la bande de détection des photodiodes Silicium très performantes puisque qu'en régime de fonctionnement nominal l'efficacité de détection est 10 fois meilleure qu'une APD-Ge tandis que le taux de coups sombres est 1000 fois plus faible. Ceci se transpose directement sur les performances d'une source de photons uniques annoncés. D'une part le taux de répétition de la source dépend de l'efficacité du détecteur annonceur et de son niveau de saturation, et d'autre part, plus le taux de coups sombres est faible, plus la probabilité P_0 est faible ;
- le photon capable d'établir une communication quantique conserve sa particularité télécom et donc la possibilité de voyager sur longue distance via les fibres optiques.

Dans le cadre du projet Européen SECOQC¹ [120, 121], nous avons déterminé par simulation numérique que la période d'inversion du signe du coefficient non-linéaire adaptée à cette nouvelle interaction se situait autour de $7 \mu\text{m}$ ce qui nous a permis de fabriquer un nouveau guide PPLN avec le bon jeu de paramètres. Ceci ne fut pas chose aisée puisque c'est la première fois que nous avons touché à une période si courte qui est proche de l'état de l'art international à l'aide de techniques similaires à la notre. A partir de là, nous avons caractérisé le spectre de la fluorescence paramétrique sortant de la structure guidante lorsque celle-ci est pompée par un laser à 532 nm. C'est le résultat qui est porté en FIGURE 4.3 ci-dessous.

Le spectre obtenu montre clairement que les photons idler sont bien à la longueur d'onde requise de 1550 nm, et donc par conservation de l'énergie que les photons signal sont eux à 810 nm. Par ailleurs, on peut voir, comme le prédit la théorie pour une interaction paramétrique donnant des longueurs d'ondes loin de la dégénérescence, que la largeur à mi-hauteur associée à ce spectre est de 2 nm. Ceci constitue une caractéristique essentielle pour la communication quantique sur longue distance puisque plus le spectre des photons qui transportent l'information quantique est fin, moins ces photons sont soumis à la dispersion chromatique des fibres optiques qui est l'une des sources principales de décohérence pour les qbits qu'ils portent.

1. SECOQC (programme FP6/IP) pour 'Development of a global network for Secure COmmunication based on Quantum Cryptography'.

FIGURE 4.3: Spectre de fluorescence paramétrique autour de 1550 nm. La période d'inversion du signe du coefficient est de $7\ \mu\text{m}$ et la longueur d'onde de pompe est de 532 nm. En raison d'une plage de détection limitée, seule la plus haute longueur d'onde (idler) est visible.



La source a aussi été caractérisée en régime “photons uniques”, c’est-à-dire dans le but d’obtenir les valeurs de probabilités P_0 , P_1 et P_2 dans une fenêtre de détection donnée. Des simulations numériques avaient montré dans un premier temps que nous pouvions attendre un P_1 de 0.45, un P_2 de $5 \cdot 10^{-5}$, et donc un P_0 de 0.55. En d’autres termes, cela revient à dire que la simple utilisation d’une photodiode Silicium en lieu et place d’une Germanium permet d’une part d’améliorer comme prévu le P_2 d’un ordre de grandeur, et d’autre part de réduire la nuisance liée au P_0 de quelques %. Cependant, c’est bien une amélioration significative du P_1 qui permettrait de s’affranchir de ces “fenêtres vides de photon” et ce paramètre est directement lié au couplage entre la structure guidante où sont créées les paires de photons et la fibre de collection placée en sortie du guide. A ce titre, le guide que nous avons réalisé n’est pour l’instant pas pleinement satisfaisant puisque nous avons mesuré un P_1 de 0.25 seulement. En effet la structure guidante est calculée de sorte à être monomode à la longueur d’onde de 1550 nm, ce qui induit que la pompe à 532 nm est fortement multimodale au sein de la structure. De ce fait, plusieurs interactions non-linéaires peuvent prendre place au sein de la structure, interactions associés aux divers modes de propagation de la pompe et donnant à différents couples de longueurs d’ondes dont plusieurs sont parasites. En effet, si les longueurs d’ondes d’annonce sont toutes dans la fenêtre de détection de la photodiode Silicium, celles des photons uniques ne sont quant à elles pas toutes visibles par le détecteur InGaAs en charge de la détection des photons à 1550 nm. On détecte donc plus d’annonces que de photons uniques effectifs. Pour remédier à ce problème, il faudrait réaliser un guide segmenté en entrée de structure de sorte à pouvoir sélectionner, et garantir, l’injection de la pompe dans le seul mode fondamental qui est celui qui donne naissance à l’interaction désirée. Cela dit, une telle réalisation demande un étude numérique poussée et de nombreux essais expérimentaux. Nous avons choisi de faire plus simple en procédant à un filtrage non-local qui consiste à post-sélectionner l’interaction qui nous intéresse par l’intermédiaire d’une paire de filtres étroits spectralement. Cette étude est en cours de réalisation dans le cadre d’une collaboration établie avec le groupe du Prof. John Rarity de l’Université de Bristol. l’idée est de coupler cette source à une source basée sur une fibre micro-structurée (basée sur le mélange à quatre ondes) dans le but d’observer le phénomène d’interférence à deux photons venant de sources séparées spatialement et dont la nature de l’interaction non-linéaire est différente. Ce type de signature représente l’étape préliminaire à la réalisation de la fonction relais quantique basée sur le principe de la téléportation, comme nous allons l’explicitier dans les Secs. 5.2 et 5.3 ci-dessous. L’objectif de cette coopération est de démontrer que tout utilisateur, possédant sa propre source d’intrication photonique, peut venir se connecter à un réseau de type relais quantique, et ce quel que soit le mode opératoire de sa source. L’expérience a déjà donné de très résultats comme nous le détaillerons au travers de la Sec. 6.1, voir également la Réf. [12] de la Sec. 9.2.

4.2 Sources de paires de photons intriqués en polarisation basée sur l'interaction non-linéaire de type-II

Ce travail représente une partie de la thèse d'Anthony Martin que j'ai co-dirigée, voir la Sec. 8.2.2.3 pour plus de détails.

4.2.1 Contexte de l'étude

A l'heure actuelle, la conversion paramétrique au sein de cristaux non-linéaires massifs constitue la solution la plus employée pour produire des paires de photons intriqués en polarisation et il existe une abondante littérature à ce sujet. Toutefois, la complexité grandissante des expériences requiert des interactions non-linéaires sans cesse plus efficaces avec, dans le même le temps, des largeurs spectrales toujours plus étroites pour les photons émis, que ce soit pour des raisons fondamentales ou appliquées. En effet, lorsqu'il s'agit d'établir un lien de communication quantique sur longue distance via l'utilisation de fibres optiques standards, les photons doivent non seulement être émis dans l'une des bandes des télécoms mais aussi posséder le spectre le plus fin possible afin de s'affranchir des effets indésirables que sont la dispersion chromatique et la dispersion des modes de polarisation. Les sources de paires de photons doivent aussi présenter des qualités de stabilité et de compacité de sorte à réellement servir les protocoles de communication quantique hors des laboratoires. C'est pourquoi nous avons réuni l'ensemble de ces caractéristiques au sein d'une seule et même source via l'utilisation de l'optique intégrée, et plus particulièrement d'un guide PPLN.

D'un point de vue quantique, nous désirons obtenir en sortie de la source l'état $|\Psi\rangle = \frac{1}{\sqrt{2}} \left[|H\rangle_a |V\rangle_b \pm |V\rangle_a |H\rangle_b \right]$ pour lequel on remarque que les deux photons a et b possèdent des polarisations orthogonales. Il convient donc d'utiliser un guide d'ondes capable de supporter les deux modes de polarisation H et V ce qui est le cas lorsque celui-ci est réalisé par la technologie de la diffusion titane sur le substrat PPLN. Notons que cette condition n'est pas remplie par les structures obtenues au LPMC par échange protonique qui ne guident que le mode V. C'est donc par le biais d'une collaboration forte, dans le cadre du projet ERA-SPOT "WASPS²" (voir la Sec. 8.2.2.2 relative aux contrats), avec le groupe d'optique intégrée de l'Université de Paderborn dirigé par le Prof. Sohler que nous avons pu avoir accès à une telle structure guidante non-linéaire.

4.2.2 Principe de fonctionnement et détails de la source

L'interaction non-linéaire, en régime de conversion paramétrique, qui prend place dans les échantillons de Paderborn est de type-II (voir Sec. 3.1). Dans ce cas, la mise en jeu du coefficient d_{24} du cristal conduit, au point de dégénérescence, à la production de photons appariés aux caractéristiques strictement identiques (longueur d'onde, spectre, mode spatial) sauf sur l'observable polarisation : l'un est polarisé H et l'autre V. Comme l'indique la FIGURE 4.4 ci-dessous (dans une version déjà avancée), les photons d'une même paire sont séparés spatialement via un diviseur de faisceau 50/50 (BS) dont les sorties sont labellisées a et b . En cas de séparation effective, les possibilités de sortie $|H\rangle_a |V\rangle_b$ et $|V\rangle_a |H\rangle_b$ sont équiprobables. Mais plus important encore, si les photons a et b sont strictement indiscernables hormis sur l'observable polarisation, il devient possible de décrire la paire par l'état $|\Psi\rangle$ purement intriqué défini plus haut. Nous avons donc, pour créer un tel état, deux étapes successives pouvant se résumer comme suit :

$$|H\rangle_p \xrightarrow{\text{type-II}} \eta |H\rangle_s |V\rangle_i \xrightarrow{BS} \eta^* \frac{1}{\sqrt{2}} [|H\rangle_a |V\rangle_b + |V\rangle_a |H\rangle_b], \quad (4.3)$$

où η représente l'efficacité du processus de conversion, η^* celle de la source dans son intégralité (comprenant l'ensemble des pertes), et BS la séparation des photons par un coupleur 50/50.

Pour obtenir l'émission des photons à la longueur d'onde dégénérée de 1310 nm, les simulations montrent que la condition de QPM (acronyme anglais pour 'quasi phase matching') doit être satisfaite pour une période d'inversion (Λ) de $6,6 \mu\text{m}$, la largeur (W) et la température du guide (T) étant les autres paramètres qui permettent d'optimiser l'interaction désirée. Le point de fonctionnement a été identifié pour l'ensemble des paramètres suivants : $\Lambda = 6,60 \mu\text{m}$, $W = 7 \mu\text{m}$ et $T \simeq 70^\circ\text{C}$. De plus, l'étude des spectres de fluorescence en régime comptage de photons (non représentés ici mais disponible dans la Réf. [13] de la Sec. 9.1) nous permet

2. Acronyme anglais pour 'waveguide single photon sources'.

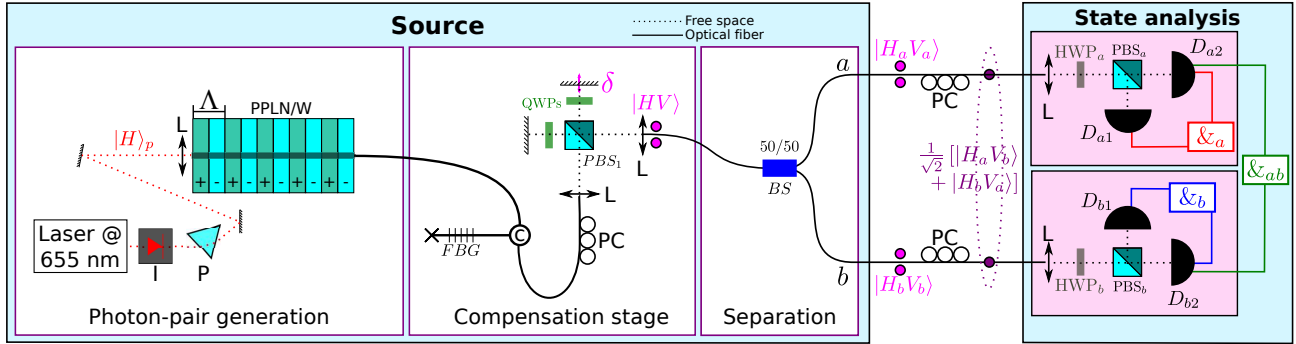


FIGURE 4.4: Schéma de la source de paires de photons intriqués en polarisation. Nous avons introduit un étage de compensation permettant d’optimiser le recouvrement spatial, spectral et temporel des photons via respectivement une fibre optique monomode, un filtre de Bragg fibré (FBG) et un arrangement de type interféromètre de Michelson. L’étage d’analyse a également été complété de sorte à pouvoir, sans aucune autre modification expérimentale, tester à la fois l’indiscernabilité des photons lorsque les paires ne sont pas séparées par le BS, et l’intrication directement lorsque les paires sont effectivement séparées. Les deux analyseurs, un chez Alice et un chez Bob, sont tout à fait standards, c’est-à-dire composés d’un cube polarisant (PBS) et d’une lame demi-onde (HWP) placée en amont afin de pouvoir choisir la base d’analyse des états de polarisation selon le type de mesure à effectuer.

de déterminer la largeur spectrale des photons qui est, dans notre cas, d’environ 0.7 nm. Ceci correspond à un temps de cohérence d’environ 4 ps, ce qui est en parfait accord avec la théorie et les simulations pour un guide de 3,6 cm de long.

De là, la condition fondamentale pour que l’état quantique porté par les paires soit effectivement intriqué est que les deux photons soient strictement indiscernables sur l’ensemble de leurs caractéristiques autres que l’état de polarisation en arrivant au coupleur 50/50. Plus précisément, cela signifie que les photons produits doivent posséder exactement la même longueur d’onde, le même temps de cohérence, et bien sûr arriver simultanément sur le coupleur dans ce temps de cohérence. Pour nous assurer de cette indiscernabilité, nous avons réalisé une première expérience d’interférence à deux photons de type “Hong-Ou-Mandel” (HOM) comme celle décrite en Sec. 5.1 [175]. En voici le principe : tout d’abord les deux photons d’une même paire sont séparés par un cube polarisant, c’est-à-dire en fonction de leur état de polarisation ; puis, ceux-ci sont recombinaés sur un coupleur 50/50 fibré après avoir tourné la polarisation de l’un des deux photons de 90deg. Nous avons alors observé un trou (le “dip”) dans le taux de coïncidences donné par deux détecteurs placés en sortie du coupleur ayant une visibilité nette, c’est-à-dire en soustrayant le bruit donné les coïncidences accidentelles, d’environ 85%. Obtenus en 2008, ces résultats plaçaient alors cette source à l’état de l’art international vis à vis des réalisations similaires, et ont fait l’objet d’un papier ‘post-deadline’ à la conférence internationale ECIO’08, d’un papier invité à la conférence ICQO’08, et d’une publication dans la revue Opt. Express, voir la Réf. [14] de la Sec. 9.1.

4.2.3 Discussion et améliorations des résultats - mesures d’intrication

Toutefois, la visibilité du HOM dip, limitée à 85%, représente par conséquent la signature d’un certain degré de discernabilité entre les photons appariés. Ceci réduit de fait la qualité de l’intrication espérée et donc l’utilité de la source pour implémenter tout protocole quantique. Après avoir identifié les sources d’indiscernabilité, nous avons profondément modifié la configuration expérimentale afin d’obtenir non seulement une indiscernabilité parfaite mais également une intrication de très haute qualité. C’est ce que je propose de discuter dans ce qui suit.

Tout d’abord, il a fallu faire l’inventaire des origines de la discernabilité des photons d’une même paire lors de la génération, et ce afin de pouvoir compenser ou effacer ces différences. Trois origines ont été identifiées :

- La première est liée à la position des modes H et V dans la profondeur du guide. En effet, les modes H et V ne voient pas le même indice de réfraction en raison de la biréfringence du cristal, si bien que le mode H se situe plus en profondeur dans la section transverse du guide que le mode V, comme en atteste la simulation reportée en FIGURE 4.5(a).
- La deuxième est liée au spectre émis par le guide lorsque celui-ci est pompé par un laser à 655 nm. En effet, la FIGURE 4.5(b) montre, outre le recouvrement spectral des photons H et V au point de dégénérescence (1310 nm), deux lobes supplémentaires, l’un à 1308.5 nm et l’autre à 1311 nm. Ces lobes sont parfaitement discernables car respectivement associés aux polarisations H et V.

- La dernière, de nouveau liée à la biréfringence du guide, amène une discernabilité temporelle sachant que le photon H voit un indice de réfraction plus petit et possède donc une vitesse de groupe plus élevée que le photon V. Ainsi, le photon H sort toujours du guide avant le photon V, rendant de fait la création de l'intrication sur le BS non optimale et donc imparfaite.

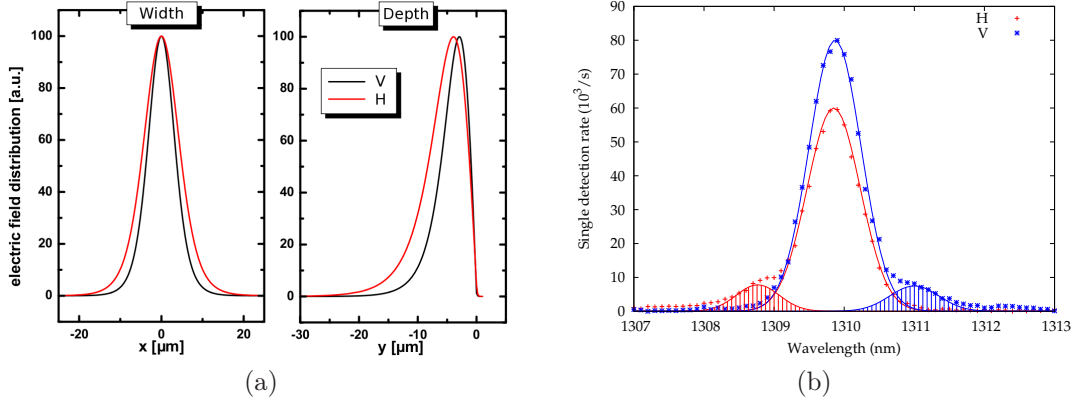


FIGURE 4.5: (a) : Simulation numérique montrant la différence de positions entre les modes H et V dans la profondeur du guide (partie droite), donnant lieu à une discernabilité spatiale. (b) : Spectre obtenu en régime de comptage de photons en sortie du guide permettant d'observer deux lobes de part et d'autre de la dégénérescence, l'un associé au mode H (à gauche, en rouge) et l'autre au mode V (à droite, en bleu), donnant lieu à une discernabilité spectrale dramatique si tout le spectre est utilisé.

Suite à cette étude, et comme l'indique la FIGURE 4.4, nous avons découpé la source en divers étages connectés les uns aux autres par fibre optique, à savoir : la génération des photons (laser et guide PPLN), la création de l'intrication (BS) et la mesure (polariseurs et détecteurs). L'organe du milieu, appelé étage de compensation, permet d'effacer toute discernabilité entre les deux photons d'une même paire. En effet, la discernabilité spatiale est compensée via l'utilisation d'une fibre optique monomode à 1310 nm, les lobes spectraux additionnels sont écartés grâce à l'utilisation d'un filtre de Bragg fibré (FBG), alors que la discernabilité temporelle est éliminée par un compensateur de biréfringence possédant l'arrangement d'un interféromètre de Michelson.

Nous avons donc pu procéder à deux nouvelles caractérisations quantiques afin de qualifier la source. D'une part, lorsque les paires de photons ne sont pas séparées par le BS, nous avons de nouveau effectué un test d'indiscernabilité de type HOM à la fois chez Alice (voie a , voir FIGURE 4.4) et Bob (voie b). Grâce au nouvel étage de compensation, les photons sont effectivement rendus indiscernables et nous avons obtenu deux HOM dips, un par voie d'analyse, donnant chacun 100% de visibilité nette comme l'indique la FIGURE 4.6(a). Le principe de cette mesure est différent d'une mesure de type HOM standard (voir Sec. 5.2). En effet, les photons non séparés conservent des polarisations orthogonales si bien que la mesure de type HOM s'effectue dans la base des polarisation croisées (diagonale (D) et antidiagonale (A)). La lame demi-onde, chez Alice ou chez Bob, est orientée de sorte à tourner l'état H en état D et l'état V en état A. Par projection dans la base $\{H, V\}$ sur le PBS, les deux photons coalescent et se dirigent ensemble, s'ils sont indiscernables sur toutes les observables autres que la polarisation, vers le même port de sortie. C'est le principe d'une mesure de type HOM en polarisation. Forts de ces résultats quasi parfaits, nous avons testé l'intrication portée par les paires effectivement séparées par le BS. Une telle mesure, qualifiée de standard, revient pour Alice à orienter successivement son analyseur selon les polarisations H, V, D, et A tandis que Bob fait tourner le sien pour chacune de ces orientations. Si les mesures dans la base $\{H, V\}$ qualifient la qualité du montage expérimental, celles faites dans la base $\{D, A\}$ sont la signature d'une interférence quantique à deux photons relatant la superposition cohérente des contributions $|H_a, V_b\rangle$ et $|V_a, H_b\rangle$ à l'état intriqué. Les quatre courbes correspondantes, données en FIGURE 4.6(b), montrent des franges d'interférence dont la visibilité nette approche les 100%. L'intrication est donc quasi-parfaite.

Notons également que cette expérience nous a aussi permis d'évaluer l'efficacité normalisée de la source en régime de comptage de photons qui s'élève à 10^5 paires de photons émises par seconde, par GHz de largeur spectrale, et par mW de puissance de pompe.

L'ensemble des résultats obtenus place aujourd'hui notre source au tout premier plan international pour des configurations identiques, c'est-à-dire relatives à la génération, dans l'une des fenêtres des télécoms, de paires de photons intriqués en polarisation via un guide d'onde de type-II. Ces travaux ont fait l'objet d'une publication dans la revue *New J. Phys.*, voir la Réf. [13] de la Sec. 9.1, et de plusieurs participations dans des conférences nationales et internationales. Pour se faire une idée de l'état de l'art des sources de paires de photons basées sur l'optique intégrée, le lecteur pourra se reporter au papier concurrent [100] ainsi qu'à l'article de revue porté en

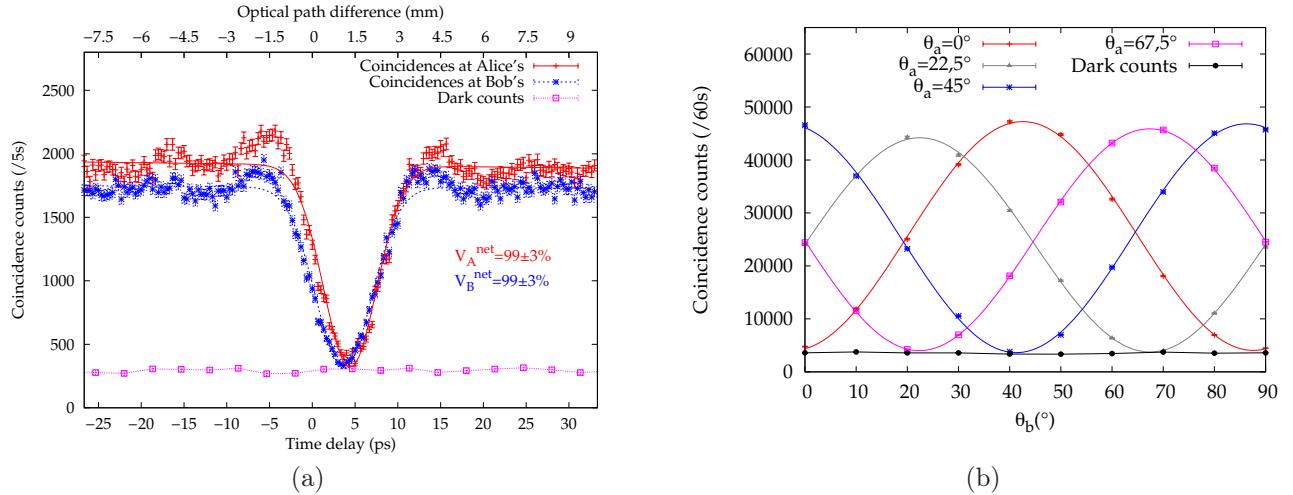


FIGURE 4.6: (a) : HOM dips obtenus chez Alice (courbe rouge) et Bob (courbe bleue) montrant chacun 100% de visibilité nette. (b) : Mesures de l'intrication en polarisation. Toutes les courbes, obtenues lorsqu'Alice oriente successivement son analyseur selon les polarisations H, V, D, et A tandis que Bob fait tourner le sien, correspondent à des figures d'interférence montrant chacune une visibilité nette approchant les 100%. La qualité de l'intrication mesurée est donc quasi-parfaite, voir aussi la Réf. [13] de la Sec. 9.1.

Réf. [4] de la Sec. 9.1. Cet article de revue met notamment en exergue le fort potentiel de ce type de sources, et de l'optique intégrée en général, pour la communication et le traitement de l'information quantique.

4.2.4 Améliorations potentielles

Malgré la pertinence de ces résultats, je propose dans ce qui suit de discuter quelques améliorations et/ou extensions possibles pour cette source. Celles-ci sont au nombre de cinq (au moins) :

- Tout d'abord, nous avons fait, en collaboration avec le groupe du Prof. Krishna Thyagarajan à IIT Delhi, une étude théorique et numérique visant à rendre l'interaction de type-II exploitable hors du point de dégénérescence. Nous avons donc montré qu'une structure PPLN aperiodique permettrait, en un seul passage de la pompe, de générer l'état intriqué de l'Eq. 4.3 sur des photons non dégénérés en longueur d'onde (par exemple 810 et 1550 nm), voir la Réf. [15] de la Sec. 9.1. Ceci trouve des applications dans les protocoles où l'un des photons reste dans le local où se trouve la source (traitement de l'information, stockage, etc.) et l'autre est amené à voyager au sein d'une fibre optique sur une grande distance.
- Enfin, la bande spectrale d'émission ($0.7 \text{ nm} \leftrightarrow \sim 1 \text{ THz}$) est encore loin d'être compatible avec les bandes d'absorption des mémoires quantiques actuelles qui sont de quelques MHz pour les ensembles d'atomes froids, de quelques dizaines de MHz pour les cristaux dopés aux ions terre-rares, et d'environ 1 GHz pour les vapeurs atomiques à température ambiante. Compte tenu de la brillance, certes bonne mais limitée que nous avons obtenu, filtrer plus étroitement les photons en sortie du générateur de type-II est impossible à moins d'utiliser des puissances de pompe de l'ordre de la dizaine de W, ce qui est bien entendu à exclure afin de ne pas détruire le cristal non-linéaire. Nous avons donc développé une nouvelle source, proposant une véritable ingénierie de l'état intriqué en polarisation en sortie d'un guide d'onde PPLN autorisant une interaction non-linéaire de type-0 et dont la brillance est au moins 2 ordres de grandeur plus importante que pour le type-II. Cette source fait partie intégrante du projet ANR/Région PACA "e-QUANET" que je discute au travers des Secs. 4.3, 6.4, et 8.2.2.2.
- Rendre la source exploitable hors de la dégénérescence peut également être obtenu par filtrage WDM (acronyme anglais pour 'wavelength division multiplexer'), c'est-à-dire via la sélection, de part et d'autre de la dégénérescence, de deux bandes spectrales corrélées. Grâce aux filtres WDM fibrés opérant dans les bandes ITU des télécoms (125 GHz de séparation inter-bande), ceci permettrait de remplacer avantageusement le beam-splitter de la FIGURE 4.4 et d'éviter, par conséquent, la perte de la moitié des paires de photons.
- Par ailleurs, le plus gros défaut de la source présentée plus haut réside dans l'utilisation d'un étage de compensation de la biréfringence du guide d'ondes. Si cet étage est obligatoire pour obtenir une bonne

qualité d'intrication, il conviendrait d'en réduire l'encombrement à sa plus simple expression. C'est ce à quoi nous travaillons aujourd'hui à l'aide d'une simple fibre à maintien de polarisation (fibre PANDA).

- Une extension extrêmement intéressante de cette source consiste à exploiter l'interaction de type-II pour générer des paires de photons intriqués en time-bin (temps d'émission) comme le fait le groupe de Genève, et non plus, donc, en polarisation. Revisiter l'observable time-bin est donc possible, notamment en vue d'une utilisation pour la cryptographie quantique.

4.2.5 Finalisation pertinente de la source

Ce travail représente une partie des travaux de thèse de Florian Kaiser, d'Amandine Issautier et de Lutfi Arif Ngah que je co-dirige, et de celle d'Anthony Martin que j'ai co-dirigée, voir la Sec. 8.2.2.3 pour plus de détails.

Nous venons tout juste de solutionner les 3 derniers points expérimentaux mentionnés ci-dessus en passant vers l'émission des paires de photons dans la bande C des télécoms (~ 1550 nm). D'une part, c'est en simplifiant considérablement le schéma de la FIGURE 4.4 que nous avons solutionné les 2 premiers points. La source dispose aujourd'hui d'un étage de compensation fait d'une simple fibre optique à maintien de polarisation (PANDA), tout en proposant une séparation déterministe des photons intriqués via l'emploi d'une paire de filtres appariés de type démultiplexeurs denses en longueurs d'ondes (DWDM) au standard des télécoms. Le schéma de cette source véritablement de nouvelle génération est porté en FIGURE 4.7(a) et la sélection spectrale des photons est décrite en FIGURE 4.7(b). En référencant les bandes respectives des filtres utilisés par + (bande ITU³ 46) et – (bande ITU 47), l'état obtenu en sortie de la source peut s'écrire :

$$|\Psi(\phi)\rangle = \frac{1}{\sqrt{2}} (|H\rangle_+ |V\rangle_- + e^{i\phi} |V\rangle_+ |H\rangle_-). \quad (4.4)$$

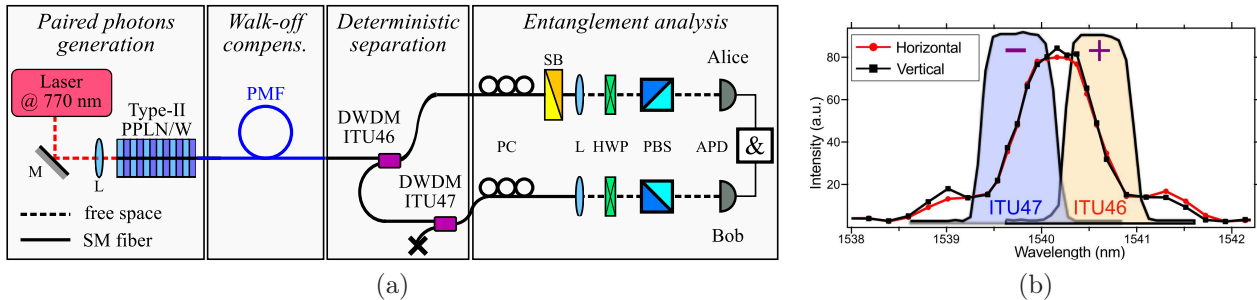


FIGURE 4.7: (a) Extension de la source de la Sec. 4.2 proposant un étage de compensation entièrement fibré et une séparation déterministe des photons générés. Un laser à 770 nm pompe le guide PPLN de type-II dont l'accord de phase est ajusté afin créer des paires de photons autour de 1540 nm, c'est-à-dire dans la bande C des télécoms. L'étage de compensation est constitué d'une simple fibre à maintien de polarisation (PANDA) dont la longueur a été identifiée par l'intermédiaire d'une mesure de type HOM comparable à celle décrite aux FIG. 4.4 et 4.6(a). La séparation déterministe est effectuée via l'emploi de deux filtres WDM denses centrés dans les bandes télécoms ITU 46 & 47, dénotés respectivement – et +. (b) Spectre naturel d'émission du guide d'ondes à 1540 nm. Sont également représentées les sélections spectrales complémentaires fournies par les filtres WDM ITU 46 (+) & 47 (–). Pour plus de détails, voir également la Réf. [16] de la Sec. 9.1.

Les pertes totales, depuis la sortie du guide d'ondes jusqu'aux analyseurs (non compris) ont donc été réduites par un facteur 4. Aussi, toutes les paires de photons émises sont exploitables grâce à cette séparation déterministe, le tout à efficacité normalisée comparable à ce qui a été discuté à la Sec. 4.2.3. Avec ce dispositif de nouvelle génération, nous avons également obtenu une qualité d'intrication encore meilleure que précédemment, *i.e.* proche des 100% théoriques même dans les données non corrigées du bruit (courbes non représentées ici). Ce travail, relativement ingénieux, a récemment été accepté pour publication dans la revue *New J. Phys.*, voir la Réf. [16] de la Sec. 9.1 (disponible sur arXiv).

4.2.6 Extension de la source à l'observable time-bin

Ce travail représente une partie de la thèse d'Anthony Martin que j'ai co-dirigée et de celle de Florian Kaiser que je co-dirige, voir la Sec. 8.2.2.3 pour plus de détails. Cette réalisation fait partie intégrante du projet

3. Bandes télécoms normalisées, voir en ligne le site de la '[International Telecommunication Union](http://www.itu.int)'.

“e-QUANET” décrit à la Sec. 6.4.

D’autre part, le dernier point mentionné à la Sec. 4.2.4, à savoir générer de l’intrication en time-bin à partir de l’interaction de type-II, a également été étudié et réalisé. Nous avons donc étendu la source par le biais d’un dispositif interférométrique simple mais ingénieux qui permet de “convertir” l’intrication depuis l’observable polarisation vers l’observable time-bin. Le schéma de cette source étendue est porté en FIGURE 4.8.

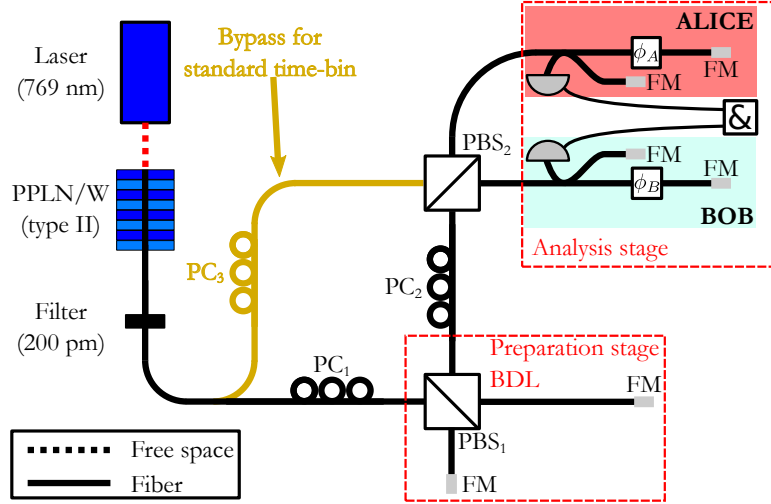


FIGURE 4.8: Schéma de la source permettant d’exploiter le processus de génération de type-II pour créer de l’intrication sur l’observable time-bin. Un interféromètre de préparation, ou boucle de délai biréfringent (BDL), entièrement fibré et placé en aval du générateur sépare, par le biais d’un cube polarisant (PBS₁), les photons appariés en fonction de leur polarisation $|H\rangle$ et $|V\rangle$. Le photon $|V\rangle$ est alors mis dans le time-bin long (bras long du dispositif), par rapport au photon $|H\rangle$ qui reste dans le time-bin court (bras court du dispositif). À la sortie de l’interféromètre, les états de polarisation des deux photons sont tournés dans la base diagonale ($\{|D, A\rangle\}$) par l’intermédiaire d’un contrôleur de polarisation (PC₂) et projetés sur un cube polarisant (PBS₂), créant l’état intriqué en time-bin désiré. L’analyse d’un tel état se fait alors par l’intermédiaire de deux interféromètres fibrés placés l’un chez Alice et l’autre chez Bob. La différence de chemin de ces interféromètres doit être identique à celle de l’interféromètre de préparation, dans la longueur de cohérence près des photons individuels (pour plus de détails, voir la Réf. [2] de la Sec. 9.1 et également la Réf. [1] de la Sec. 9.4.

L’opération effectuée par cet interféromètre dit de préparation permet d’effacer les états de polarisation portés initialement par les photons et de créer un état intriqué en time-bin du type :

$$|\Psi(\phi)\rangle = \frac{1}{\sqrt{2}} (|0\rangle_a |1\rangle_b + e^{i\phi} |1\rangle_a |0\rangle_b), \quad (4.5)$$

où la phase ϕ est donnée par la somme des phases $\phi_a + \phi_b$ dans les interféromètres d’analyse placés chez Alice et Bob (voir FIGURE 4.8). Il est important de remarquer que ϕ ne dépend absolument pas de la phase induite dans l’interféromètre de préparation, contrairement aux schémas de préparation d’intrication en time-bin usuels (pour s’en convaincre, voir la Réf. [2] de la Sec. 9.1). Cet état est un état “croisé” en time-bin qui n’a, à notre connaissance, encore jamais été étudié.

Les résultats quant à la qualité de l’intrication obtenue sont excellents si bien qu’une telle source pourrait être avantageusement utilisée dans des schémas de distribution quantique de clés de cryptographie. En effet, les ressources technologiques nécessaires à l’implémentation d’un protocole de cryptographie quantique basé sur cette source time-bin sont moins importantes que celles liées aux sources time-bin et énergie-temps standards [86, 111, 135, 136]. Seuls deux interféromètres stabilisés (les analyseurs) au lieu de trois et quatre détecteurs au lieu de potentiellement huit pour l’énergie-temps sont requis ici. Le papier correspondant, comprenant l’analyse expérimentale de l’état ainsi que l’étude théorique relative à l’implémentation de la source dans un protocole de cryptographie quantique, a récemment été soumis à Phys. Rev. Lett., comme l’indique la Réf. [17] de la Sec. 9.1.

Notons enfin que ce travail est le fruit d’une collaboration avec Alexios Beveratos (CNRS/Laboratoire de Photonique & Nanostructures à Marcoussis) et Valerio Scarani (Centre for Quantum Technologies and Department of Physics, National University of Singapore).

4.3 Source de paires de photons intriqués en polarisation basée sur l'interaction non-linéaire de type-0

Ce travail représente une grosse partie des travaux de thèse de Florian Kaiser que je co-dirige, une partie de celle d'Anthony Martin que j'ai co-dirigée, et une petite partie de celles d'Amandine Issautier et de Lutfi Arif Ngah que je co-dirige, voir la Sec. 8.2.2.3 pour plus de détails.

4.3.1 Contexte de l'étude

Les travaux commencés au LPMC dans le cadre du projet ANR "e-QUANET", voir les Secs. 6.4 et 8.2.2.2 ont déjà bien avancé. La source, d'un genre nouveau par rapport à celles présentées en Sec. 4.2, affiche un potentiel de versatilité encore jamais atteint, du moins à ma connaissance, pour la génération de paires de photons intriqués en polarisation. À ce titre, voici en bref les caractéristiques de versatilité que propose cette réalisation dont le principe est donné en FIGURE 4.9 :

- (i) La possibilité de créer de l'intrication sur une plage de longueurs d'ondes pouvant couvrir presque toute la courbe d'accord de phase de guide PPLN de type-0 utilisé, c'est-à-dire environ 50 nm d'ajustement pour les longueurs d'ondes des photons émis (correspond à la bande C des télécoms dans son intégrité).
- (ii) L'arrangement expérimental est tel que nous avons la possibilité d'ajuster à volonté, et ce via un simple changement de filtre, la largeur spectrale des photons sur 5 ordres de grandeur, plus spécifiquement depuis ~ 20 MHz (accessible par filtrage) jusqu'à 4 THz (émission naturelle du guide PPLN).
- (iii) Enfin, grâce à un contrôle en temps réel et ultra-précis de la phase de l'état intriqué généré, la source peut créer, à la demande, tout état maximalement ou non maximalement intriqué, elliptique ou non (voir la Réf. [18] de la Sec. 9.1), ce qui inclue bien entendu les 4 états de Bell bien connus (voir le système d'Eq 2.6).

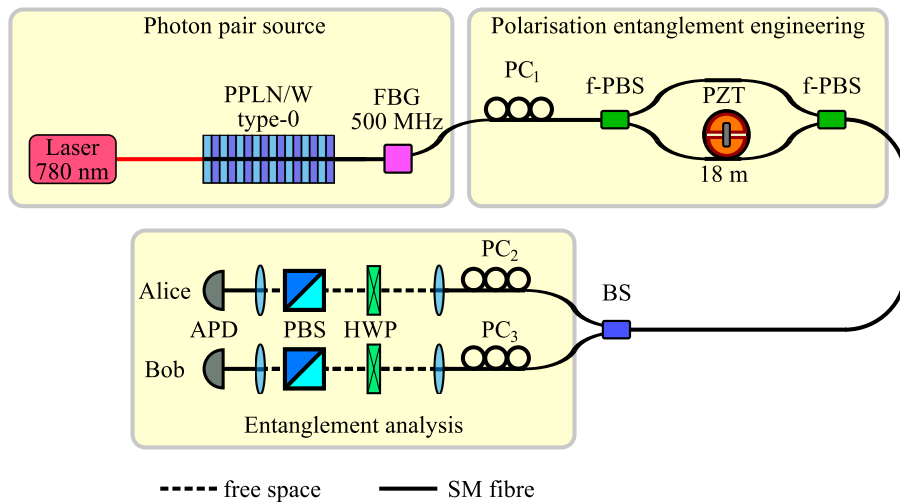


FIGURE 4.9: Schéma de principe de la source e-QUANET réalisée au laboratoire. Tous les organes principaux sont stabilisés sur des transitions atomiques appropriées. Le laser de pompe à 780 nm est stabilisé via une cellule de rubidium et l'interféromètre servant à créer l'intrication est stabilisé via un second laser émettant à 1590 nm (bande L des télécoms, non représenté), lui-même stabilisé sur une cellule de rubidium après doublage en fréquence. Un beam-splitter fibré (BS) sert à séparer les photons appariés.

4.3.2 Principe de fonctionnement de la source

Un guide d'onde de type-0 crée des paires de photons polarisés $|V, V\rangle$ (vertical) à la longueur d'onde de 1560 nm par interaction avec un laser de pompe à 780 nm stabilisé sur la ligne D_2 du ^{87}Rb et polarisé verticalement. Les photons sont ensuite récoltés au sein d'une fibre optique monomode et affinés (ou non) spectralement par l'intermédiaire d'un filtre de Bragg fibré (FBG) ou d'un WDM. A ce stade, c'est en jouant avec la température du cristal, mais sans changer la longueur d'onde de pompe, que nous pouvons ajuster la longueur d'onde

d'émission des photons sur environ 20 nm. Par ailleurs, la finesse spectrale de ces photons ne dépend que du filtre employé. En effet, après le guide d'ondes, l'intrication en polarisation n'est pas encore établie puisque les photons possèdent le même état de polarisation. Il est donc possible d'utiliser n'importe quel type de filtre, *i.e.* de Bragg fibré ou simple WDM, dont les propriétés de biréfringence importe peu. La largeur spectrale du filtre employé peut alors couvrir une plage extrêmement étendue, ici presque 5 ordres de grandeur, allant depuis la limite basse imposée par le dispositif qui sert à créer l'incitation (~ 20 MHz), jusqu'à la largeur émise naturellement par l'interaction non-linéaire (~ 2 THz). Pour ce faire, partant de l'état $|V, V\rangle$ généré par le guide d'onde, nous procédons à une véritable "ingénierie quantique" de l'état intriqué, comme le montrent les FIGS. 4.9 et 4.10.

Tout d'abord, un contrôleur de polarisation fibré (PC_1) permet de tourner l'état de polarisation des photons pour arriver à l'état $|D, D\rangle$ (diagonal). Une boucle de délai biréfringent ayant la forme d'un interféromètre de Mach-Zehnder fibré sert à ensuite projeter l'état de la paire sur un état intriqué de type

$$|\Psi\rangle = \frac{1}{\sqrt{2}} [|H_a, H_b\rangle + |V_a, V_b\rangle], \quad (4.6)$$

où, comme d'habitude, les labels a (Alice) et b (Bob) représentent les utilisateurs à qui sont envoyés les photons. Comme l'indique la FIGURE 4.10, cette boucle de délai est composée de deux cubes polarisant fait de fibre optique (f-PBS) et d'une ligne à retard faite d'une fibre à maintien de polarisation dont la longueur vaut 18 m.

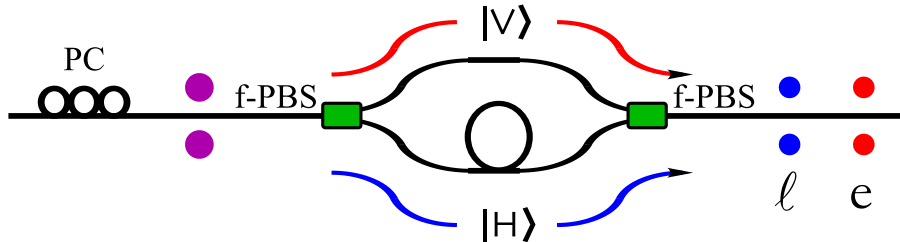


FIGURE 4.10: Schéma de principe de la boucle de délai biréfringente entièrement fibrée. Les modes de polarisation sont séparés par le PBS d'entrée et recombinés par celui placé en sortie. Dans le cas où les deux photons d'une paire ressortent ensemble du dispositif, ils se voient conférer l'état intriqué en polarisation donné par l'Eq. 4.6. Les labels e et l , mis respectivement pour 'early' et 'long time-bin', décrivent les temps relatifs de sortie de deux photons dont la différence doit être plus petite que l'incertitude sur le temps d'émission de la paire.

D'un point de vue quantique, ce dispositif permet de projeter l'état de la paire sur l'état intriqué de l'Eq. 4.6 dans le cas où les photons ne sont pas séparés par le PBS d'entrée. En effet, le laser de pompe étant continu, si une paire de photons est détectée en coïncidence entre Alice et Bob, il n'est pas possible de discriminer entre une contribution de type $|H_a, H_b\rangle$ ou de type $|V_a, V_b\rangle$. Pour que cette idée fonctionne correctement, il faut néanmoins respecter une condition fondamentale issue des sources de paires de photons intriqués sur l'observable time-bin. En effet, garantir que les contributions $|H_a, H_b\rangle$ et $|V_a, V_b\rangle$ sont indiscernables revient à avoir un temps de séparation entre ces contributions qui soit plus petite que l'incertitude liée au temps de l'émission de la paire. Dans notre cas, la longueur de 18 m fournit un temps de séparation d'environ 80 ns entre les composantes H et V ce qui est 40 fois plus petit que le temps de cohérence du laser de pompe qui est porté à $3 \mu\text{s}$ grâce à la procédure de stabilisation. Notons enfin que la boucle est stabilisée activement, par l'intermédiaire d'un laser de référence lui-même stabilisé sur une transition atomique (ligne D_1 du ^{87}Rb) après doublage en fréquence, afin d'éviter toutes les dérives de phase qui pourraient dégrader la qualité de l'intrication. Mais plus encore, nous arrivons, grâce à cette méthode, à maintenir la différence de chemin entre les bras de l'interféromètre à moins de $\frac{\lambda}{200}$. Ceci permet un véritable contrôle en temps réel de la phase l'état intriqué.

4.3.3 Résultats obtenus et versatilité d'emploi

Avec ce système que je qualifierai volontiers de versatile, nous avons pu obtenir, à l'aide d'un WDM de 125 GHz, puis d'un FBG de 500 MHz, et enfin d'un FBG de 25 MHz à chaque une qualité d'intrication presque parfaite comme en atteste, par exemple pour le FBG de 500 MHz, la FIGURE 4.11 ci-dessous. Le Tableau 4.1 résume l'ensemble des performances obtenues.

Les résultats obtenus montrent, je pense, la pertinence de notre approche, puisque dans le même temps, nous avons porté la brillance de la source, comparativement à celle de la Sec. 4.2 à 300 paires de photons créées par seconde, par mW de puissance de pompe et par MHz de largeur spectrale. L'ensemble de ces résultats place

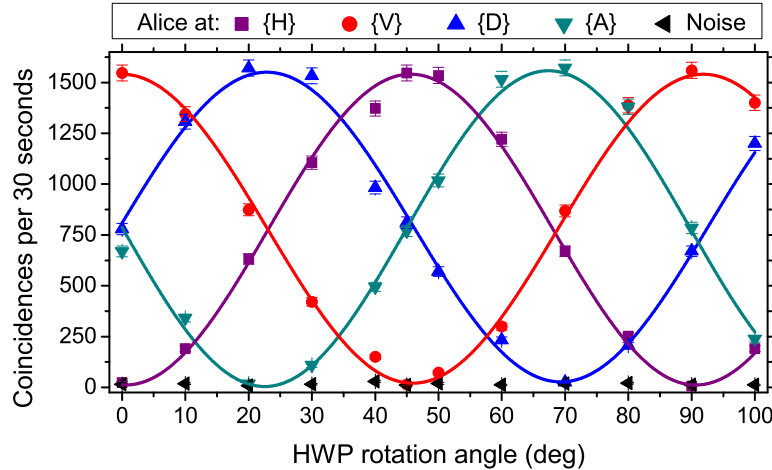


FIGURE 4.11: Résultats obtenus pour la mesure de l'intrication en sortie de la source présentée en FIGURE 4.9 lorsqu'un filtre de type FBG de 500 MHz est employé. Le principe de la mesure est le même que celui utilisé pour caractériser la source de la Sec. 4.2. Nous obtenons, pour les quatre orientations de mesure chez Alice (H,V,D,A), des visibilités d'interférence à deux photons qui dépassent 99%, que ce soit nette ou brute. La qualité de l'intrication produite est donc quasi parfaite.

	$\Delta\nu = 2$ THz (naturels)	$\Delta\nu = 125$ GHz	$\Delta\nu = 500$ MHz	$\Delta\nu = 25$ MHz
V_{brute} (%)	99	99	99	87
V_{nette} (%)	99	99	99	99

TABLE 4.1: Tableau comparatif des résultats obtenus avec la source décrite par les FIGS. 4.9 et 4.10 pour 4 largeurs spectrales ($\Delta\nu$) couvrant 5 ordres de grandeur. Les notations V_{brute} et V_{nette} indiquent respectivement les visibilités des franges d'interférence associées à une mesure de type inégalités de Bell, comme celles reportées à la FIGURE 4.11. La désignation “nette” indique que seules les coïncidences accidentelles dues au bruit dans les détecteurs ont été retranchées. Notons que la visibilité brute obtenue pour la largeur spectrale de 25 MHz est réduite par rapport aux autres. En effet, plus le filtre est fin, plus le nombre de paires de photons qui passent au travers est faible, donc plus le bruit dans les détecteurs de photons joue un rôle important dans les données brutes.

notre source au sommet de l'état de l'art, rattrapant d'ailleurs le retard des sources d'intrication en polarisation vis à vis des sources d'intrication en time-bin. Le lecteur intéressé par les détails de cette réalisation pourra consulter la Réf. [19] de la Sec. 9.1, en cours d'évaluation par la revue Nature Photon. mais disponible sur arXiv. Notons enfin que cette réalisation ramène, en termes de performances de brillance et de qualité de l'intrication, l'observable polarisation au niveau des réalisations time-bin basées soit sur des configurations standards [102] soit sur des générateurs placés au sein d'une cavité résonante⁴ [103], et devient comparable, en termes de largeur spectrale, aux réalisations d'intrication en polarisation basées soit sur des ensembles d'atomes froids de rubidium [176, 33, 177], soit sur des cristaux placés au sein d'une cavité [178, 179].

4.3.4 Test quantique, à choix retardé, de la complémentarité des photons uniques

Ce travail représente une partie de la thèse de Florian Kaiser que je co-dirige, voir la Sec. 8.2.2.3 pour plus de détails.

Nous avons récemment développé, en collaboration avec Thomas Coudreau et Perola Milman du Laboratoire Matériaux et Phénomènes Quantiques (Université Paris-VII Diderot), une expérience destinée à tester la complémentarité des photons uniques, en d'autres termes leurs propriétés à la fois corpusculaire et ondulatoire, comme l'a discuté Wheeler dans les années 80 [180]. De nombreuses expériences ont été déclinées dans la littérature, si bien que les citer toutes dépasse le cadre de ce manuscrit. C'est pourquoi je citerais volontiers, et uniquement, celle faite en 2007 par Jacques et ses collaborateurs [49] (et les Réfs. incluses).

Par ailleurs, les résultats de cette expérience sont trop récents pour les décliner ci-après dans leur intégrité. Je mentionnerai toutefois que l'originalité de notre réalisation réside dans le fait que nous utilisons avantagusement

4. On parle de configurations de type oscillateur paramétrique optique (OPO) sous le seuil.

l'intrication en polarisation, provenant de la source décrite ci-dessus. Ainsi, nous disposons de deux photons dont les états de polarisation ne sont pas définis puisqu'ils sont intriqués. L'un des photons (appelé photon 'test') est alors envoyé vers un dispositif interférométrique proposant une voie fermée (test du caractère ondulatoire) pour la polarisation V, et une voie ouverte (test du caractère corpusculaire) pour la polarisation H. Le photon test peut donc être soumis, au hasard d'un beam-splitter, à un test de complémentarité selon qu'il prend la voie fermée ou la voie ouverte. Le second photon (appelé photon 'témoin') est envoyé quant à lui vers un analyseur standard de polarisation comme ceux utilisés pour mesurer l'intrication. Il est tout à fait remarquable de noter que dans notre expérience, le photon témoin est détecté *avant* le photon test, alors que le photon test est détecté *d'une façon retardée par un intervalle du genre espace* par rapport au photon témoin. Ainsi, en faisant varier l'angle d'analyse de l'état de polarisation du photon témoin et la phase de l'interféromètre associé au photon test, le résultat de notre expérience montre un 'morphing' complet, selon les valeurs de ces deux paramètres, entre le caractère ondulatoire et le caractère corpusculaire du photon test.

Le lecteur intéressé par cette réalisation pourra se reporter à la Réf. [20] de la Sec. 9.1, en cours d'évaluation par la revue Science mais disponible sur arXiv.

4.4 Étude d'un générateur paramétrique intégré sur semi-conducteur entouré d'un réseau de Bragg.

L'un des problèmes rencontrés lorsqu'il s'agit de créer des paires de photons par conversion paramétrique au sein d'un cristal non-linéaire pompé par un laser en régime d'impulsions courtes (fs) réside dans le fait que la conversion ne s'opère que sur une partie limitée du spectre de la pompe, réduisant par conséquent l'efficacité du processus. Cette fraction est fixée par la condition d'accord de phase qui régit la conversion non-linéaire. En d'autres termes, à puissance moyenne constante, plus le spectre de la pompe est large, autrement dit plus la durée de l'impulsion est courte (dans le cas d'impulsions limitées par le critère de Fourier), plus l'efficacité de conversion est faible, comme le montre la Réf. [6] de la Sec. 9.1 (période post-doctorale à Genève). Par ailleurs, lorsque le spectre de la pompe est large, les photons issus de la conversion paramétrique sont aussi émis sur une large bande qui peut aller jusqu'à une centaine de nm. Ceci impose généralement aux expérimentateurs de procéder à un filtrage fin, adapté aux besoins de l'expérience, qui consiste le plus souvent à ramener ces photons sur une largeur spectrale inférieure au nm, surtout pour s'affranchir des problèmes liés à la dispersion chromatique lorsqu'il s'agit de faire voyager les photons sur de longues distances au sein de fibres optiques. Ce filtrage induit naturellement une réduction importante de l'efficacité globale de la source.

Dans le cas particulier d'un guide d'ondes, une solution au problème peut être de moduler le confinement des modes transverses du guide par le biais d'un réseau de Bragg dont les caractéristiques de dispersion sont convenablement choisies. Toutefois, sachant qu'il faut combiner sur un même composant la présence d'une partie permettant la génération des paires de photons et un réseau de Bragg placé au dessus du guide, la technologie de l'optique intégrée sur niobate de lithium n'est pas appropriée.

Dans le cadre d'une collaboration avec le groupe d'Optique Guidée du Prof. Krishna Thyagarajan de l'Indian Institute of Technology (IIT) à Delhi, nous avons étudié les possibilités offertes par les semi-conducteurs, et plus spécifiquement le GaN périodiquement polarisé ($pp - GaN$) pour ce qui concerne la partie non-linéaire associé à l'AlGaIn pour ce qui concerne le réseau de Bragg. L'idée était d'étudier une possible augmentation de l'acceptance en longueur d'onde de pompe lors de la génération de paires de photons au sein d'une telle structure. Dans ce contexte, l'équipe de Delhi a apporté son savoir-faire numérique et ses connaissances sur ce type de dispositifs en traitant les idées et les données que nous leur avons fournies concernant les propriétés essentielles que doivent posséder les photons lorsqu'il s'agit d'effectuer un protocole de communication quantique sur longue distance.

Nous avons donc montré avec ce type de structure, plus précisément un réseau de Bragg dont le cœur est un guide fait de $pp - GaN$ entouré d'une "gaine" faite alternativement de couches d' $Al_{0.02}Ga_{0.98}N$ et d' $Al_{0.45}Ga_{0.55}N$ (voir FIGURE 4.12 ci-dessous), qu'il était possible de reporter tout le spectre de la pompe sur l'un des deux photons de la paire et d'obtenir, à la limite de Fourier, des largeurs spectrales sur l'autre photon aussi fine que 0.25 nm. L'ensemble de cette étude et les résultats qui s'y rapportent ont été publiés dans la revue Opt. Express, voir la Réf. [21] de la Sec. 9.1.

Notons qu'un tel dispositif peut trouver des applications en cryptographie quantique à paires de photons, où l'on choisit un accord de phase donnant lieu à la génération de paires de photons à 810 et à 1550 nm par le biais d'une pompe à 532 nm. Dans ce cas, les conditions de dispersion dans le réseau de Bragg sont choisies telles que l'élargissement de la pompe se reporte sur le photon à 810 nm qui restera dans un environnement local alors que le photon à 1550 nm, spectralement fin, pourra voyager sur une longue distance au sein d'une fibre optique

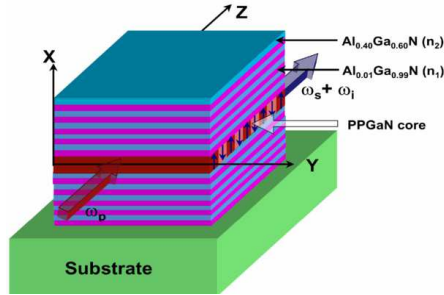


FIGURE 4.12: Schéma de principe de notre guide non-linéaire fait de $pp - GaN$ entouré d'un réseau de Bragg fait de couches successives d' $AlGaIn$ ayant des compositions sensiblement différentes afin d'ajuster les propriétés de dispersion du réseau.

sans subir les effets de perte d'information temporelle liée à la dispersion chromatique.

4.5 Analyse d'états intriqués en polarisation particuliers

Je me suis également intéressé à comment analyser de façon optimale des états intriqués en polarisation.

D'une part, durant mon post-doctorat à l'université de Genève (GAP), j'ai effectué un séjour de 2 mois au sein du département de physique de la University of Illinois at Urbana-Champaign (USA), plus précisément au sein du groupe du Prof. Paul Kwiat (laboratoire LOOMIS). Durant ce séjour, j'ai pu, en collaboration avec deux doctorants présents sur place, tester l'inégalité de Collins-Gisin destinée à quantifier les degrés d'intrication et de non-localité présents dans une certaine classe d'états, à savoir des états non purs et non maximalelement intriqués. Ce type d'étude ne peut être mené qu'à l'aide d'une source d'intrication photonique extrêmement versatile, c'est-à-dire capable de produire tous les états possibles et imaginables (*i.e.*, états plus ou moins intriqués, et contenant plus ou moins de bruit). Grâce à la source de paires de photons intriqués en polarisation développée au laboratoire LOOMIS, nous avons non seulement pu créer l'état et violer l'inégalité proposée par Collins-Gisin, mais également pu tester de nombreux autres témoins d'intrication ('entanglement witnesses') comme notamment la tomographie complète. Ces travaux ont été publiés en 2005 dans la revue Phys. Rev. Lett., comme l'indique la Réf. [22] de la Sec. 9.1.

Par ailleurs, lorsque mon équipe a commencé à travailler sur l'observable polarisation (voir les Secs. 4.2 et 4.3), il nous a fallu comprendre comment analyser les états produits par nos sources. En effet, la production d'un état maximalelement intriqué en polarisation s'accompagne souvent d'une phase entre les deux contributions à l'état. Il faut donc, pour violer les inégalités de Bell correctement, non seulement maintenir cette phase constante pendant la durée de la mesure, mais également la contrôler de façon adéquate afin que les paramètres d'analyse soit correctement adaptés à la valeur de la phase en question. C'est l'objet du travail que nous avons publié dans la revue Laser Phys., reporté en Réf. [18] de la Sec. 9.1. *Ce second travail représente une petite partie des travaux de thèse d'Anthony Martin, de Florian Kaiser et d'Amandine Issautier, voir la Sec. 8.2.2.3 pour plus de détails.*

Chapitre 5

Les relais quantiques

Comme je l'ai déjà indiqué au long de cette discussion, l'heure est à la manipulation de l'information, c'est-à-dire que l'on désire étendre les protocoles de communication quantique hors du laboratoire et poser les premières pierres d'un ordinateur quantique qui ne soit pas une usine à gaz.

Dans le cadre de la communication quantique, il faut, avant d'établir un protocole sur longue distance, s'intéresser aux limitations des technologies employées. D'une part, malgré des performances et des capacités exceptionnelles, les fibres optiques télécoms présentent des pertes à la propagation ($\simeq 0.2$ dB/km). D'autre part, les détecteurs de photons uniques habituellement employés aux longueurs d'ondes des télécoms (technologie InGaAs) sont assez peu efficaces ($\leq 20\%$) et assez bruités ($P_{\text{bruit}} \simeq 10^{-6}/\text{ns}$). Ces deux effets combinés limitent le rapport signal à bruit (S/B) du lien de communication quantique constitué et par là même la distance potentielle sur laquelle peut se faire la communication. Or il a été théoriquement démontré que la fonction relais quantique, basé sur le protocole de téléportation, permet à deux interlocuteurs d'augmenter la distance qui les sépare grâce à une amélioration significative de rapport S/B. Ceci est tout simplement lié au fait que le relais fournit, comme son nom l'indique, un signal confirmant la présence des qubits transmis en un ou plusieurs endroits sur la ligne de communication quantique. Ceci permet de venir, au final, déclencher le détecteur placé en bout de ligne uniquement lorsque les photons qui portent les qubits, désormais liés à ce signal de confirmation, sont effectivement attendus. Ainsi, mettre en cascade, par exemple, une source de photons uniques annoncés et la fonction relais quantique revient à faire un ET logique sur les deux annonces et donc restreindre le nombre de fois où les photons sont annoncés mais non présents en bout de ligne. En d'autres termes, plus le nombre de nœuds où l'on sait que l'information existe encore est grand, plus la distance de communication peut être importante.

Je vais discuter dans ce qui suit deux expériences de principe de type relais quantique, la première destinée à implémenter le protocole de téléportation de l'intrication, et la seconde mettant en œuvre une véritable puce optique dédiée à la fonction téléportation, et ayant un format adapté aux réseaux télécoms standards.

Notons également que les tenants et les aboutissants en matière de relais quantiques sont présentés à la Sec. 2.6.3.

5.1 L'interférence quantique à deux photons

Les premières expériences d'interférence à deux photons furent réalisées à la fin des années 1980 par le groupe du Prof. Mandel à l'Université de Rochester (USA). L'idée, tout d'abord fondamentale, était de vérifier la théorie qui prédit que lorsque deux photons parfaitement identiques entrent chacun par un port différent d'un beam-splitter¹ (BS), ils empruntent toujours le même port de sortie : c'est la coalescence ou interférence quantique à 2 photons. Pour que l'interférence soit maximale, le mot "identiques" signifie que les deux photons doivent posséder la même longueur d'onde, le même temps de cohérence, le même mode de polarisation, le même temps d'arrivée sur le BS, et enfin que leur recouvrement spatial sur le BS soit optimal. Si ces conditions sont remplies, et dans le cas où le BS est 50/50, l'effet est tel que les deux possibilités qu'ont les photons de sortir séparément du dispositif s'annulent, c'est-à-dire interfèrent destructivement comme l'indique la FIGURE 5.1. De là, si deux détecteurs sont placés en sortie du BS, ceux-ci ne pourront jamais se déclencher simultanément, si bien que si l'on fait varier le temps d'arrivée de l'un des photons par rapport à l'autre, il s'ensuit l'observation d'un trou dans le taux de coïncidences entre les deux détecteurs. Ce trou, ou "dip" en anglais, porte le nom de ses auteurs Hong, Ou, et Mandel (HOM) [175].

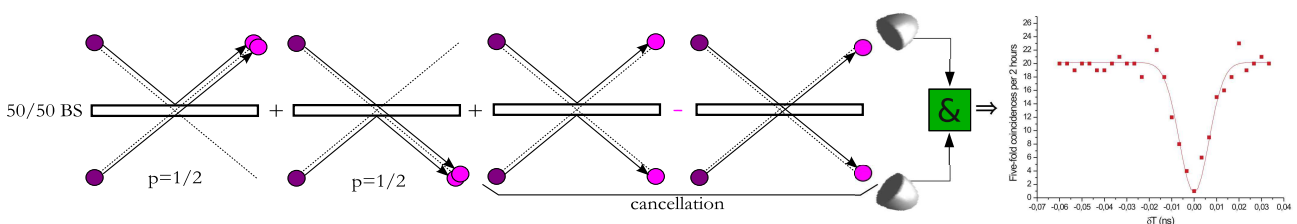


FIGURE 5.1: Principe du phénomène de coalescence lorsque 2 photons identiques sont incidents en même temps sur un beam-splitter (BS) mais chacun via un port différent. On voit que si le BS est de type 50/50, il se produit une interférence quantique destructive qui fait sortir les deux photons toujours par le même port de sortie, faisant chuter le taux de coïncidence entre les deux détecteurs placés en sortie. Le trou dans les coïncidences porte le nom de HOM dip.

Suite aux premières expériences de type HOM, de nombreuses répliques ont été faites et ce dans diverses configurations expérimentales. La littérature est très abondante en ce sens si bien qu'il serait impossible d'établir une liste exhaustive des expériences déjà réalisées. En effet, les photons qui arrivent sur le BS peuvent provenir de n'importe quel type de source, pourvu qu'ils soient uniques et identiques en amont du BS (pré-) ou des détecteurs (post-sélection). Le lecteur pourra se reporter à la Réf. [23] de la Sec. 9.1 qui relate une expérience de coalescence à laquelle j'ai activement participé lors de mon séjour post-doctoral à Genève.

5.2 Relais quantique basé sur la téléportation de l'intrication en régime picoseconde - preuve de principe

Ce travail représente une partie de la thèse de Pierre Aboussouan j'ai co-encadrée, voir la Sec. 8.2.2.3 pour plus de détails.

Depuis quelques années, la coalescence est devenue plus qu'un "simple" effet fondamental puisqu'elle se trouve à la base de ce que l'on appelle, dans le domaine de la communication quantique, la "configuration relais quantique". Il faut donc comprendre la coalescence comme un moyen d'intriquer deux photons indépendants ce qui revient à connecter deux interlocuteurs distants par un canal quantique. Le protocole qui régit cette intrication "forcée et à distance" est celui de la téléportation d'états qui implique, au delà de la coalescence, une mesure de l'état intriqué obtenu à la sortie du BS comme nous l'avons vu à la Sec. 5.3. La configuration relais quantique la plus couramment étudiée expérimentalement consiste à créer deux paires de photons intriqués via deux cristaux non-linéaires séparés spatialement, de séparer les paires, et de mixer deux photons, chacun issu d'une paire, sur un BS. A ce titre, plusieurs réalisations ont déjà été faites et, outre les astuces expérimentales développées par chaque groupe, les différences résident surtout dans 4 points primordiaux :

1. "Beam-splitter" est une appellation, certes anglaise, mais communément utilisée en raison de son acronyme "BS". La correspondance en français est "séparateur de faisceau" ou "lame séparatrice". Notons que l'on parle aussi volontiers de coupleur directionnel lorsque le dispositif est fait de fibres optiques ou en optique intégrée.

- (i) le régime de pompage des milieux non-linéaires pour la génération des paires de photons, à savoir femto-seconde (fs), continu (cw), ou picoseconde (ps) ;
- (ii) le filtrage spectral nécessaire des photons générés qui est directement lié au régime de pompage ;
- (iii) le type de milieux non-linéaires utilisés, à savoir cristaux massifs, guides PPLN, ou encore fibres micro-structurées ;
- (iv) et enfin, les longueurs d’ondes mises en œuvre.

Sans entrer dans trop de détails techniques, remarquons que la fonction relais n’a d’intérêt que si celle-ci s’opère sur de grandes distances. Ainsi il convient d’émettre des photons dans l’une des fenêtres des télécoms, comme par exemple autour de 1550 nm, autorisant le transport des photons par fibre optique. De plus, cette génération doit pouvoir se faire de façon efficace et de façon parfaitement ajustable du point de vue des longueurs d’ondes émises (accord de phase). Pour ce faire, nous disposons de guides PPLN ayant déjà montré ces qualités à de nombreuses reprises. Enfin, si l’on désire avoir deux sources de photons parfaitement indépendantes, il faut répondre à la question la plus importante : le mode de pompage. Initialement, les équipes travaillant dans le domaine ont choisi le régime fs et pompaient deux cristaux séparés mais à l’aide d’un seul laser [153, 157, 181]. La raison essentielle à cela réside dans la relative souplesse du filtrage spectral à appliquer aux photons émis qui est dans ce cas de l’ordre de quelques nm, c’est-à-dire ramené à la largeur spectrale du laser de pompe dans la limite de Fourier. Toutefois, lorsque deux lasers fs doivent être utilisés pour pomper deux cristaux non-linéaires, il convient de les synchroniser et la tâche est particulièrement difficile comme l’a reporté le groupe du Prof. Zeilinger à Vienne (Autriche) [148, 149]. Depuis l’avènement des filtres de Bragg fibrés offrant des largeurs spectrales aussi faibles que 10 pm, l’équipe du Prof. Gisin à Genève s’est rendu compte qu’il devenait possible de pomper les cristaux à l’aide de deux lasers CW [102, 147]. En effet, pour que la coalescence ait bien lieu dans ce cas, il faut que les photons soient temporellement plus “grands” que le jitter des détecteurs, ce qui requiert des largeurs spectrales de l’ordre de la dizaine de pm et l’utilisation de détecteurs hybrides (voir la Sec. 3.3.2) ou, pire, supraconducteurs. On s’affranchit du coup de toute synchronisation, mais au prix de stabiliser les deux lasers sur des transitions atomiques et d’un filtrage drastique. Finalement, il existe un compromis qui me semble quasiment idéal et qui a le bon goût de n’avoir pas été trop étudié : le régime ps. Dans ce cas en effet, d’une part le filtrage appliqué aux photons peut être beaucoup moins fin qu’en régime CW, c’est-à-dire de l’ordre de quelques centaines de pm. Ceci permet notamment d’utiliser des détecteurs de photons de type APD-InGaAs tout à fait standards et disponibles dans le commerce. D’autre part, si les besoins de l’expérience le demandent, la synchronisation de deux lasers ps est beaucoup plus aisée par rapport à deux lasers fs [151, 150].

Nous avons donc réalisé une expérience de coalescence en utilisant deux guides d’ondes PPLN fabriqués au laboratoire, pompés en régime ps, et dont les conditions de quasi-accord de phase sont portées à l’identique. L’idée est non seulement de montrer l’intérêt de ce mode de pompage via l’utilisation de composants disponibles dans le commerce (filtres de Bragg, détecteurs de photons, *etc.*) mais aussi d’évaluer le potentiel d’un tel schéma pour la réalisation d’un relais quantique réel. Le montage est schématisé sur la FIGURE 5.2(a). Nous utilisons un laser de pompe mode-locké (Coherent MIRA 900D) qui délivre des impulsions d’une durée de 1.2 ps à un taux de répétition de 76 MHz. La longueur d’onde centrale est ajustée à $\lambda_p = 768.15$ nm et la largeur spectrale a été mesurée à $\Delta\lambda_p = 0.24$ nm. Une lame de microscope permet de prélever une partie du faisceau et de le diriger vers une APD en silicium afin de créer une horloge artificielle moins rapide que le taux de répétition du laser et qui permettra de trigger les APD-InGaAs responsables de la détection des photons créés.

Le faisceau de pompe est ensuite envoyé sur un BS 50/50 dont les deux sorties sont utilisées pour pomper nos deux guides PPLN. Ceux-ci font 21 mm de long et sont chauffés à 90°C. Le quasi-accord de phase visé, c’est-à-dire permettant la génération de photons appariés à la longueur d’onde de 1536 nm en partant de la pompe à 768 nm, est obtenu pour un pas d’inversion de la non-linéarité de $\Lambda = 16.3$ μm . Du point de vue classique, le spectre de fluorescence émis en sortie des guides et correspondant à l’accord de phase fait environ 80 nm de large à mi-hauteur autour de 1536 nm (spectre non représenté ici). La longueur d’onde centrale d’émission représente un pré-requis essentiel pour l’expérience de type HOM décrite à la FIGURE 5.2(b). Notons enfin que les paires de filtres représentés en FIGURE 5.2(a) viennent sélectionner une paire de bandes spectrales corrélées autour de la longueur d’onde de dégénérescence.

Afin de rendre indiscernables d’un point de vue quantique deux photons provenant chacun d’un guide différent, il convient de sélectionner deux bandes étroites de part et d’autre de la dégénérescence obtenue à 1536 nm à l’aide d’un même système de filtrage composé de deux circulateurs et d’une paire de filtres de Bragg entièrement fibrés. En plus du rôle de filtrage, ce type de système est astucieux dans le sens où l’ajustement de la longueur d’onde centrale de chaque paire de filtres permet une séparation simple des paires de photons en sortie des guides comme le ferait un démultiplexeur en longueur d’ondes. En sortie de chaque entité “guide + système

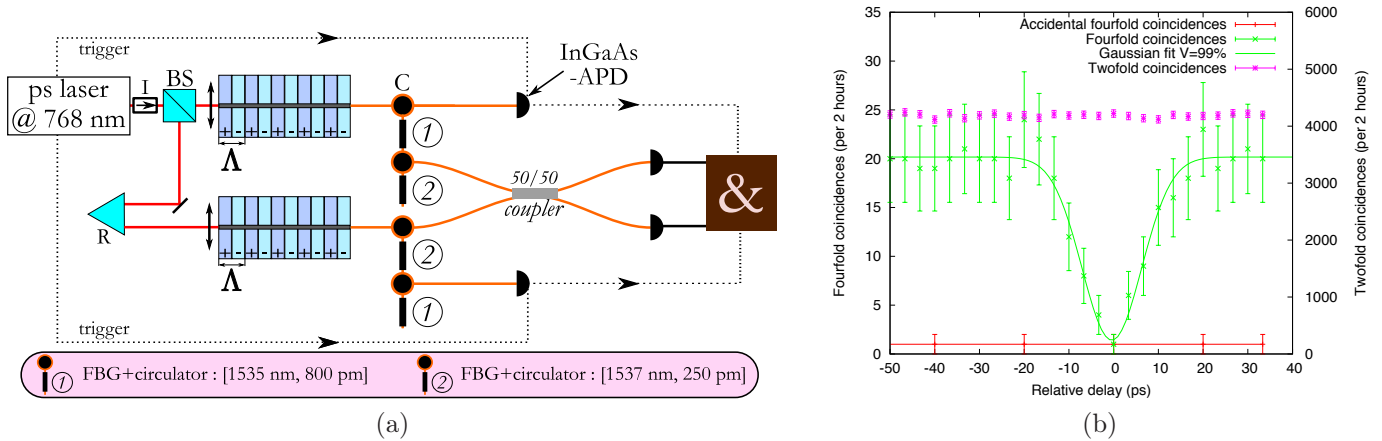


FIGURE 5.2: (a) : Schéma simplifié de l'expérience de type HOM mettant en jeu deux guides PPLN pompés par un même laser en régime ps. FBG : Fiber Bragg Grating filter ; C : circulator. Les paires de filtres ① et ② permettent de venir sélectionner, de part et d'autre du spectre d'émission des paires de photons, des bandes de longueurs d'onde corrélées faisant respectivement 800 et 200 pm. (b) : HOM dip en sortie du montage de gauche après filtrage des photons et ajustement temporel via le rétroreflécteur. Est représenté le taux de quadruples coïncidences en fonction de la position du rétroreflécteur pour une puissance de pompe de 0.98 mW.

de filtrage”, nous avons donc à notre disposition des paires de photons appariés de longueur d'onde de 1537 et 1535 nm, respectivement associés à des largeurs spectrales de 800 et 200 pm. Pour observer l'interférence de type HOM, les deux photons à spectres larges sont détectés par deux APD-InGaAs qui viennent déclencher la détection, via deux autres APD-InGaAs, des deux photons à spectres fins après que ceux-ci aient été combinés sur un BS 50/50. Nous enregistrons les détections en coïncidences relatives à ces 4 détecteurs associés à l'horloge donnée par l'APD en silicium décrite plus haut. L'évolution de ces coïncidences quadruples est donnée en FIGURE 5.2(b) où l'on voit la présence d'un dip remarquable lorsque les deux photons à 1535 nm entrent au même instant dans le BS (l'ajustement temporel se fait par l'intermédiaire d'un rétroreflécteur (R)).

Plusieurs caractéristiques importantes sont à noter. Tout d'abord, la visibilité ou profondeur brute du dip vaut ici environ 91% alors que la visibilité nette, c'est-à-dire lorsque les coïncidences accidentelles sont retranchées, est supérieure à 99%. Par ailleurs, la largeur temporelle à mi-hauteur de notre dip vaut environ $\Delta\tau = 0,007$ ns, ce qui donne une longueur de cohérence pour les photons qui coalescent d'environ 4 mm ce qui est en parfait accord avec les 5 mm que l'on est en droit d'attendre des filtres². Enfin, les oscillations de part et d'autre du dip sont explicables par le fait que le phénomène de coalescence revient à faire, dans le domaine temporel, un produit de convolution de deux signaux de type “porte” dans le domaine des fréquences (fonction filtrage) ce qui revient à obtenir un résultat oscillant de type “sinus cardinal”.

Notons enfin que les résultats obtenus avec cette expérience sont de tout premier plan à l'international puisque la visibilité nette représente la meilleure valeur jamais atteinte pour des configurations similaires. Ceci nous permet d'envisager pour la première fois la possibilité de sortir le relais quantique hors du laboratoire. Ces travaux ont été publiés en tant que 'Rapid Com.' dans la revue Phys. Rev. A, voir la Réf. [24] de la Sec. 9.1.

En parallèle, et ce via une collaboration avec le GAP à Genève, nous avons obtenu des résultats prometteurs pour la fonction relais en régime picoseconde, mais cette fois avec deux lasers synchronisés l'un sur l'autre selon un schéma de type Maître/Esclave, pompant deux guides PPLN niçois (chacun un). Pour le moment, la visibilité du HOM dip reste limitée à environ 80% mais nous avons montré que ceci n'est pas lié à la configuration de synchronisation choisie, voir la Réf. [25] de la Sec. 9.1.

Nous verrons dans la Sec. 6.1 comment transposer ce régime de fonctionnement picoseconde à un véritable schéma de synchronisation pour les relais quantiques, précis et autonome, basé uniquement sur des composants télécoms éprouvés et de l'optique non-linéaire standard. L'idée maîtresse sous-jacente suscite l'intérêt de deux industriels et a fait l'objet d'un dépôt de brevet via le CNRS (voir Sec. 8.5 pour plus de détails).

2. On définit la longueur de cohérence par $\mathcal{L} = 0.44 \cdot \frac{\lambda^2}{\Delta\lambda}$, où λ et $\Delta\lambda$ représentent la longueur d'onde et le spectre des photons, respectivement, c'est-à-dire ici 1536 nm et 200 pm.

5.3 Relais quantique intégré basé sur la téléportation - preuve de principe

Ce travail représente une partie de la thèse d'Anthony Martin que j'ai co-dirigée, voir la Sec. 8.2.2.3 pour plus de détails. Cette réalisation fait partie intégrante du projet européen QUANTIP décrit à la Sec. 6.3.

J'ai proposé, lors de mon entrée au CNRS, de tirer profit de l'ensemble des atouts offerts par la technologie de l'optique intégrée pour la réalisation de la fonction relais quantique sous la forme d'une véritable interface qui puisse s'insérer aisément au sein des réseaux de communication standards. De fait, l'intérêt d'une démonstration expérimentale de la fonction relais quantique en des termes de compacité, de robustesse et de simplicité d'utilisation constitue une étape essentielle dans le futur développement de réseaux de communication quantique hors du laboratoire. Il paraît en effet comme plutôt évident que réaliser ce type d'interface ne peut aboutir que grâce à l'adjonction d'une technologie forte et éprouvée telle que l'optique intégrée sur niobate de lithium. Nous allons voir que grâce à cette technologie, nous avons pu intégrer l'ensemble des fonctions optiques utiles au protocole de téléportation, le tout sur un même substrat.

Afin de mieux en appréhender le fonctionnement de l'interface, ou puce, relais, portons notre attention sur la puce de la FIGURE 5.3-(a).

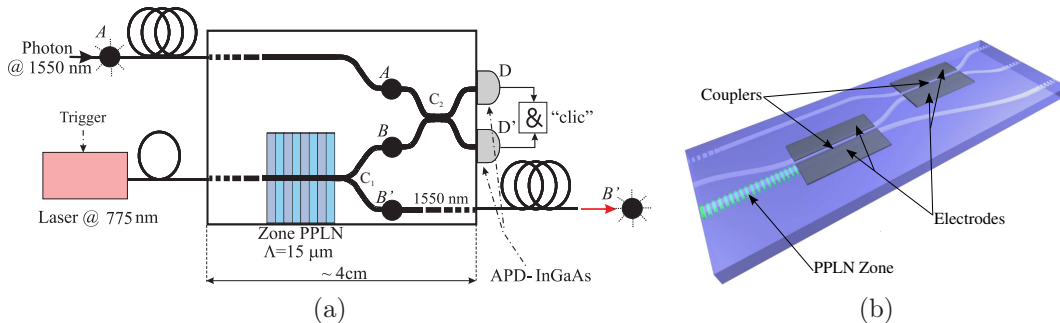


FIGURE 5.3: (a) : Une puce pour la réalisation d'un relais quantique intégré. Le photon A provient d'une HSPS comme celle décrite en Sec. 4.1. (b) : Représentation en 3D de la puce relais sur laquelle on peut voir les coupleurs C_1 et C_2 et leurs paires d'électrodes associées.

Supposons qu'il existe un qbit A provenant par exemple de la HSPS de la FIGURE 4.1 ou de l'une des sources configurée en HSPS de la Sec. 5.2. Celui-ci est encodé sur un photon de longueur d'onde 1550 nm et circule dans une fibre télécom reliée à la puce de relais. Dans le même temps, un trigger témoin de l'instant de création de ce qbit déclenche un laser impulsif à 775 nm qui va permettre, par interaction avec le guide PPLN de la puce ($\Lambda \simeq 16 \mu\text{m}$), la création d'une paire de photons notés B et B' de nouveau à la longueur d'onde de 1550 nm. Par suite, un coupleur intégré C_1 assure la séparation de ces photons de sorte que l'un d'entre eux (B par exemple) entre, au même instant que A , dans le second coupleur C_2 placé en aval (nécessité de synchroniser l'arrivée du photon A et l'émission de l'impulsion laser). Cette opération consiste à perdre l'information sur la provenance des deux photons entrant qui portent la même longueur d'onde. Dans le cas où les deux photons empruntent un bras de sortie différent, il se produit une coïncidence entre les détecteurs InGaAs D et D' . On peut dire que l'on vient d'intriquer ces photons de manière artificielle. Ainsi, il ne reste en sortie du relais intégré que le photon B' qui porte la longueur d'onde de 1550 nm, et qui s'est vu conférer, suite à la coïncidence, l'état du photon A initial : c'est le principe de la téléportation. Ce dernier, qui avait sûrement parcouru des kilomètres de fibre avant d'arriver là, a disparu dans le processus de détection. Bien entendu, l'efficacité d'un tel système est sujette au couplage guides-fibres, aux pertes au sein des structures guidantes et notamment des virages, et à l'efficacité de l'interaction non-linéaire ainsi qu'à celle des détecteurs. Toutefois, l'intérêt réside dans le fait que la mesure d'une coïncidence entre A et B atteste que le photon A était bien entré dans la puce relais. Son état ayant été transféré sur B' , c'est comme si l'on venait de faire sur A une mesure non destructive au milieu de notre canal quantique. Au final, on perdra des photons mais la preuve de leur "survie" en un endroit donné permet d'augmenter les distances utiles au transfert d'information.

Fabriquer un tel composant revient à maîtriser plusieurs étapes technologiques très difficiles mais cruciales en termes de micro-structuration du niobate de lithium. Si j'ai déjà mentionné que notre équipe est capable de fabriquer des guides PPLN à la demande, il faut dans ce nouveau cas pouvoir aussi intégrer des composants actifs en termes de contrôle électro-optique tels que des coupleurs directionnels et des guides segmentés aux entrées/sorties de la puce. Bien entendu, la difficulté de la tâche consiste justement à intégrer tous les composants

requis pour le fonctionnement de la puce relais. Il faut notamment ajouter plusieurs étapes technologiques lors de la fabrication d'un tel circuit par rapport à un guide PPLN standard. Il faut également arriver à un certain niveau de maîtrise de ces processus puisque, par exemple, les coupleurs C_1 et C_2 doivent montrer des rapports de couplage exactement égaux à 50/50 afin de garantir un fonctionnement quantique optimal de la puce. C'est pourquoi, afin de palier à tout défaut lié à la fabrication, nous avons placé, de part et d'autre des guides couplés, des paires d'électrodes qui, pilotées par un générateur de tension, permettent d'optimiser les rapports de couplage. Ces électrodes sont représentées sur la vue en 3D de la puce en FIGURE 5.3-(b).

D'un point de vue technologique, l'intégration des coupleurs et de leurs paires d'électrodes représente le plus gros de l'effort, mais cette étape est toutefois indispensable si l'on veut garantir une bonne séparation des photons B et B' (via C_1) et une bonne intrication modale des photons A et B (via C_2). Ainsi, des paramètres tels que la forme des coupleurs, la longueur des virages et la longueur d'interaction ont tous été préalablement simulés via la "beam propagation method" (BPM) non seulement dans un souci d'optimisation de l'espace sur la puce en termes de taille des composants, mais aussi dans un but plus essentiel de minimisation des pertes à la propagation au sein de l'ensemble de ces structures guidantes. Les mesures que nous avons effectuées sur nos premières puces relais montrent des pertes à la propagation raisonnables à 1550 nm, c'est-à-dire de l'ordre de 6 dB entrée/sortie, et en bon accord avec nos prédictions. Plus spécifiquement, pour des virages de 10 mm de long nous avons montré que les pertes sont de l'ordre du dB. Par ailleurs, nous avons pour la première fois au laboratoire montré le bon fonctionnement de coupleurs directionnels dont les rapports de couplage dépendent fortement de l'espace laissé entre les deux guides juxtaposés et validé l'obtention des rapports 50/50 requis pour l'expérience grâce au contrôle de la tension appliquée sur les électrodes. A ce titre, la technologie d'intégration par échange protonique doux développée au LPMC autorise ce contrôle via des tensions allant de quelques à plusieurs dizaines de Volts en fonction des coupleurs testés. D'autre part, nous avons montré que notre technologie d'intégration des guides était très bien adaptée à ces nouvelles structures dans le sens où les étapes de fabrication des composants semblent bien reproductibles et que leur stabilité dans le temps dépasse plusieurs jours. Les paramètres que nous avons finalement sélectionnés sont des séparations entre les guides des coupleurs d'environ $5 \mu\text{m}$ pour des largeurs de guides typiques de $6 \mu\text{m}$. Ces paramètres mènent à des puces relais dont la longueur fait environ 5 cm

Finalement, si l'on prend en compte l'ensemble des mesures expérimentales que nous avons effectué sur notre puce relais, nous pouvons simuler en situation réelle une augmentation de la distance de communication quantique par un facteur 1.8, ce qui représente une avancée significative dans le domaine.

Dans un premier temps, nous avons réalisé une puce relais et procédé à une caractérisation classique des diverses fonctions en présence. Du point de vue optique non-linéaire, ceci revient à tester les zones PPLN qui servent à produire les paires de photons intriqués. Nous avons obtenus des spectres de fluorescence paramétrique montrant une dégénérescence autour de 1536 nm ce qui convient parfaitement pour notre application puisque nous avons besoin de paires de photons intriqués (B et B') ayant des longueurs d'ondes appartenant à la bande C des télécoms (voir FIGURE 5.4(a)). Ceci correspond également à la longueur d'onde du photon A entrant par le port haut de la puce et dont on veut téléporter l'état sur le photon B' . La validation du spectre de fluorescence, en même temps que la validation du bon fonctionnement des coupleurs, est d'une importance capitale pour la réalisation de de notre relais. C'est pourquoi nous avons vérifié que les coupleurs présents sur la puce pouvaient bien fonctionner selon le rapport de couplage 50/50 désiré. Nous avons donc envoyé des photons uniques à 1536 nm, issus de l'une des sources discutées à la Sec. 5.2 précédente, tantôt sur le port d'entrée de l'un des coupleurs, tantôt sur le port d'entrée de l'autre, et appliqué une tension sur les électrodes correspondantes permettant de faire varier le rapport de branchement. La courbe FIGURE 5.4(b) atteste du bon fonctionnement des coupleurs intégrés puisque le taux de 50/50 est atteint pour des tensions d'environ 40 V. Ces tensions sont toutefois 10 fois plus importantes que les valeurs auxquelles on s'attend avec la technologie d'intégration utilisée, et ceci en incombe très probablement à un processus d'intégration des électrodes non encore optimal.

Dans un deuxième temps, nous avons procédé à la caractérisation quantique de la puce relais. Le choix de la longueur d'onde de travail prend ici tout son sens puisque les photons uniques qui entrent par le port A doivent être identiques à ceux générés par la zone PPLN intégrée sur la puce. C'est pourquoi nous avons pris soin de faire se correspondre les longueurs d'ondes émises par la puce à celles émises par les sources utilisées dans la Sec. 5.2 précédente. Ainsi, nous avons fait fonctionner l'une de ces sources en régime de "photons annoncés à 1536 nm" et, selon le montage porté en FIGURE 5.5(a) (similaire à celui de la FIGURE 5.2(a)), nous avons validé l'étape préliminaire à la fonction relais en établissant un HOM dip au niveau du coupleur C_2 de la puce entre un photon venant de la source de photons annoncés et un photon issu de la zone PPLN de la puce. Le résultat de cette mesure est donné en FIGURE 5.5(b) ci-dessous, sur laquelle on voit clairement un trou dans les coïncidences (points de couleur rouge sur la FIGURE 5.5(b)) montrant une visibilité nette d'environ 79%. Notons

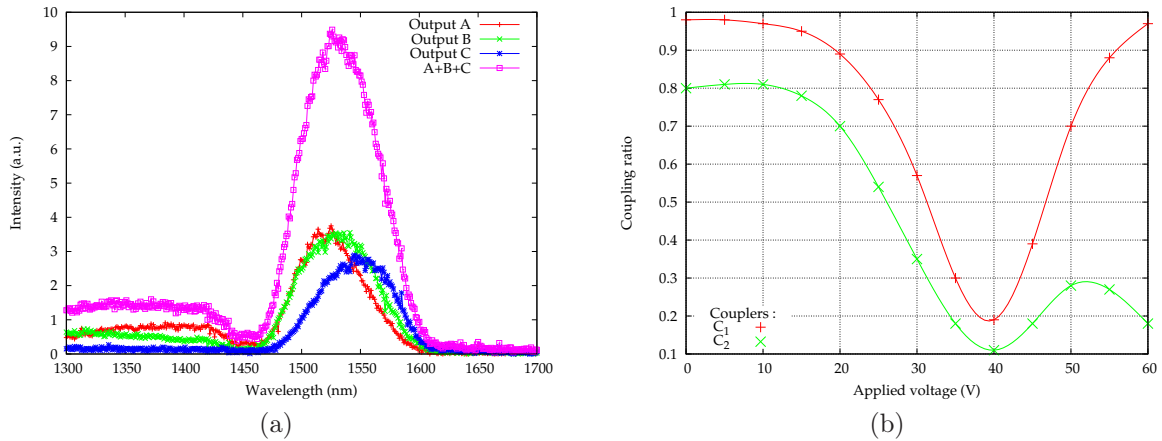


FIGURE 5.4: (a) : Spectres obtenus dans la zone PPLN de notre relais quantique. Les différentes courbes sont toutes issues d'une zone possédant un pas d'inversion de $17 \mu\text{m}$ et correspondent à des mesures prises à différentes sorties des coupleurs. Lorsque l'on somme les spectres sur les différentes sorties, nous obtenons bien une émission dans la bande C des télécoms avec une largeur de spectre d'environ 80 nm. (b) : Exemple d'obtention de coupleurs 50/50 par application d'une tension de commande aux bornes des électrodes placées de part et d'autre des zones de couplage (zone où les guides se rapprochent, comme indiqué sur la FIGURE 5.3(b)). On dit que les coupleurs sont contrôlables par effet électro-optique et reconfigurables à la demande.

que l'ajustement théorique sur le dip (ligne rouge sur la FIGURE 5.5(b)) est tiré d'un modèle théorique que nous avons développés nous-mêmes, voir la Réf. [26] de la Sec. 9.1. La visibilité brute quand à elle est beaucoup moins bonne, d'environ 27%, et est essentiellement limitée par les pertes trop importantes au sein de la puce associée à des niveaux de coups sombres trop élevés dans nos détecteurs de photons.

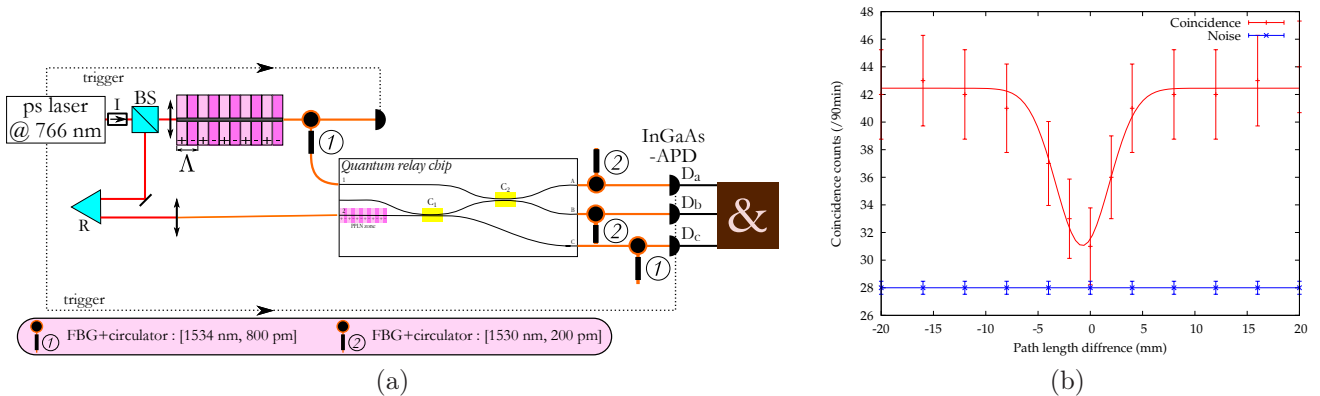


FIGURE 5.5: (a) : Schéma expérimental permettant de mettre en évidence un HOM dip au niveau du coupleur C_2 . Une source de photons uniques annoncés à 1536 nm (voir la Sec. 5.2) est connectée sur le port A de la puce (voir FIGURE 5.3(a)) et la coalescence doit se produire entre ces photons et ceux provenant de la zone PPLN de la puce après séparation des paires au niveau du coupleur C_1 . (b) : Obtention d'un HOM dip dans les coïncidences à 4 photons, impliquant un photon annoncé par une source externe et un photon de la zone PPLN intégrée sur la puce, et les 2 photons complémentaires aux 2 premiers, comme montré sur le schéma de gauche. La visibilité nette de la figure d'interférence est de 79%.

Bien que les visibilités nette et brute puissent être améliorées, les résultats obtenus, à la fois aux niveaux classique et quantique, sont très prometteurs en vue de l'intégration de certaines fonctions de l'optique quantique. Nous venons de publier ces résultats qui ont fait l'objet de commentaires élogieux sur ce véritable "tour de force", voir la Réf. [26] de la Sec. 9.1. En effet, nous sommes en présence, et ce pour la première fois, d'une véritable puce tout optique intégrée permettant la réalisation d'une fonction quantique particulière rendue possible par l'association de plusieurs fonctions de base. Avec une telle réalisation, nous nous situons au-delà de l'état de l'art dans le domaine, notamment grâce au fait que notre composant est parfaitement reconfigurable via le contrôle électro-optique des coupleurs. Notons également que ce "module quantique intégré" est une véritable boîte noire, possédant des fibres optiques en entrées/sorties, capable d'offrir stabilité, compacité, bon rendement et simplicité d'utilisation. Ceci répond donc à la tournure actuelle que prend la communication quantique.

Dans ce domaine qu'est l'optique quantique intégrée, les étapes à plus long terme concernent notamment la manipulation de l'information quantique via des puces intégrées configurables à volonté par l'utilisateur, voir la

Réf. [4] de la Sec. 9.1. L'idée est alors de procéder à une véritable ingénierie des états quantiques via l'ingénierie de l'optique intégrée. Ceci rentre dans le cadre du projet européen QUANTIP dont je suis le porteur LPMC, et dont les tenants et les aboutissants sont présentés en Sec. 6.3.

Chapitre 6

Résumé des projets en cours de développement

N.B. : L'ordre dans lequel sont présentés les projets ci-dessous ne reflète en rien un caractère prioritaire mais plutôt une progression naturelle dans leur réalisation.

Chapitre 7

Conclusion générale

Depuis les test pionniers du théorème de Bell (parmi d'autres), destinés à prouver l'existence de corrélations non-locales induites par l'intrication, le domaine de l'information quantique et de la physique quantique en général a véritablement explosé. À l'heure actuelle, la superposition cohérente des états et l'intrication, piliers fondamentaux de la physique quantique, sont devenues des ressources "consommables" au sein de protocoles tels que la cryptographie, la téléportation ou bien encore le calcul quantiques. La cryptographie quantique est même déjà disponible dans le commerce. Il est donc nécessaire de développer des outils simples, fiables, compacts, performants et capables de produire ces ressources fondamentales avec un degré de pureté le plus haut possible.

C'est dans cette veine que l'auteur, son équipe et ses collaborateurs proches, ont œuvré au cours des années qui viennent de s'écouler, en proposant d'adjoindre à la communication quantique et à l'optique quantique fondamentale une technologie forte basée sur l'intégration de guides d'ondes linéaires et non-linéaires sur des substrats de niobate de lithium. Ce sont donc à la fois des sources de photons uniques, de paires de photons intriqués en time-bin et en polarisation, des interfaces quantiques pour qbits photoniques, des détecteurs de photons uniques en configuration hybride, des schémas de type relais quantiques déployé et intégré, qui ont été développés avec les résultats et les succès que l'on connaît. Aujourd'hui, ce sont d'autres techniques expérimentales, celles des atomes froids, qui viennent s'ajouter au paysage du laboratoire dans le but de réaliser des mémoires quantiques permettant à la fois l'annonce du stockage et une relecture à la demande.

Mais l'histoire est loin d'être terminée, car au-delà des réalisations et des approches expérimentales d'optique quantique appliquée et fondamentale qui ont été discutées tout au long de ce manuscrit, il existe aujourd'hui un gap monumental entre les promesses "faites par les théoriciens" et l'état de l'art expérimental. Les prouesses de l'information quantique sont également encore très loin des performances de l'information classique, que ce soit en termes de communication ou de traitement des bits conventionnels. Bien que la cryptographie quantique jouisse déjà d'un certain niveau de commercialisation, le domaine de l'information quantique doit encore aller de l'avant, et ce de façon conséquente. Son évolution passera certainement par une exploitation intensive, par un mariage savant, voire par une mutation importante, des technologies et des techniques expérimentales qui s'y rapportent. Il est d'ailleurs tout à fait probable que certaines technologies existantes n'aient pas encore été identifiées par les "expérimentateurs quantiques" comme étant d'intérêt pour le domaine, ou que d'autres n'aient tout simplement pas encore vu le jour. Il est par exemple particulièrement difficile d'imaginer de futurs réseaux quantiques de communication au sein desquels la détection des photons serait assurée par des détecteurs supraconducteurs refroidis à l'hélium liquide, ou encore que le stockage des qbits se ferait par le biais de mémoires quantiques basées sur des ensembles d'atomes froids piégés dans des chambres à vide d'un demi mètre cube.

L'optique guidée en général et l'optique intégrée en particulier représentent des voies à fort potentiel, et c'est dans ce cadre que s'est inscrit le présent manuscrit. Mais ce ne sont pas les seules (on parle volontiers des 'enabling technologies'), si bien que l'avenir du domaine, s'il en est un, nécessitera certainement, en plus des développements novateurs et originaux, un couplage adéquat entre les supports et les systèmes quantiques les plus pertinents et les plus aboutis. En d'autres termes, les caractéristiques d'adaptabilité et de versatilité des briques de bases qui constitueront les réseaux quantiques du futur sont aujourd'hui considérées comme les verrous technologiques à surmonter.

La transversalité du domaine de l'information quantique est un fait avéré depuis le tout début, puisque de nombreuses disciplines sont impliquées, combinant à souhait recherche fondamentale et appliquée. Il va juste falloir être capable d'exploiter cette transversalité efficacement, mais c'est là que les difficultés commencent... Pour s'en convaincre, le lecteur pourra avantageusement parcourir le site web du GDR "Information Quantique, Fondements & Applications" (N° 3322 du CNRS, voir en ligne [IQFA](#)).

Chapitre 8

Résumé de la carrière scientifique

N.B. 1 : Le lecteur intéressé par la Science uniquement pourra avantageusement éviter cette partie.

N.B. 2 : Les textes ou acronymes qui apparaissent ci-dessous en couleur cyan contiennent des liens vers les sites web associés. Ainsi, en cliquant sur ces textes depuis un lecteur de fichiers PDF standard (Acrobat Reader, Mac Preview, *etc.*), le lecteur est renvoyé vers les sites correspondants.

Chapitre 9

Liste des productions scientifiques / Track records

9.1 Papiers publiés dans, soumis à, ou en préparation pour, des revues internationales à comité de lecture

- [1] S. Tanzilli, H. De Riedmatten, W. Tittel, H. Zbinden, P. Baldi, M. P. De Micheli, D. B. Ostrowsky, and N. Gisin, “Highly efficient photon-pair source using a periodically poled lithium niobate waveguide”, *Electron. Lett.*, vol. **37**, pp. 26–28, 2001.
- [2] S. Tanzilli, W. Tittel, H. De Riedmatten, H. Zbinden, P. Baldi, M. P. De Micheli, D. B. Ostrowsky, and N. Gisin, “PPLN waveguides for quantum communication”, *Eur. J. Phys. D*, vol. **18**, pp. 155–160, 2002.
- [3] S. Tanzilli, W. Tittel, M. Halder, O. Alibart, P. Baldi, N. Gisin, and H. Zbinden, “A photonic quantum information interface”, *Nature (London)*, vol. **437**, pp. 116–120, 2005.
- [4] S. Tanzilli, A. Martin, F. Kaiser, M. P. De Micheli, O. Alibart, and D. B. Ostrowsky, “On the genesis and evolution of quantum integrated optics”, *Laser & Photon. Rev.*, vol. **6**, pp. 115–143, 2012, published online the 1st of August 2011.
- [5] R. T. Thew, S. Tanzilli, W. Tittel, H. Zbinden, and N. Gisin, “Experimental investigation of the robustness of partially entangled qubits over 11 km”, *Phys. Rev. A*, vol. **66**, pp. 062304, 2002.
- [6] I. Marcicic, H. De Riedmatten, W. Tittel, V. Scarani, A. Acín, S. Tanzilli, H. Zbinden, and N. Gisin, “Studies of femtosecond time-bin entangled qubits for quantum communications”, *Fortschr. Phys.*, vol. **51**, pp. 428–434, 2003.
- [7] R. T. Thew, S. Tanzilli, L. Krainer, S. C. Zeller, A. Rochas, I. Rech, S. Cova, H. Zbinden, and N. Gisin, “Low jitter up-conversion detectors for telecom wavelength GHz QKD”, *New J. Phys.*, vol. **8**, pp. 32, 2006.
- [8] G. Temporão, S. Tanzilli, H. Zbinden, N. Gisin, T. Aellen, M. Giovannini, and J. Faist, “Mid-infrared single-photon counting”, *Opt. Lett.*, vol. **31**, pp. 1094–1096, 2006.
- [9] G. Temporão, H. Zbinden, S. Tanzilli, N. Gisin, T. Aellen, M. Giovannini, J. Faist, and J.-P. Von der Weid, “Feasibility study of free-space quantum key distribution in the mid-infrared”, *Quant. Inf. & Comput.*, vol. **8**, pp. 01–11, 2008.
- [10] O. Alibart, D. B. Ostrowsky, P. Baldi, and S. Tanzilli, “High-performance guided-wave asynchronous heralded single-photon source”, *Opt. Lett.*, vol. **30**, pp. 1539–1541, 2005.
- [11] G. Bertocchi, O. Alibart, D. O. Ostrowsky, S. Tanzilli, and P. Baldi, “Single-photon sagnac interferometer”, *J. Phys. B.*, vol. **39**, pp. 1011–1016, 2006.
- [12] A. McMillan, L. Labonté, B. Bell, A. Clark, A. Martin, O. Alibart, W. Wadsworth, J. R. Rarity, and S. Tanzilli, “Two-photon interference between disparate sources for quantum networking”, 2012, In preparation.
- [13] A. Martin, A. Issautier, H. Herrmann, W. Sohler, D. O. Ostrowsky, O. Alibart, and S. Tanzilli, “A polarization entangled photon-pair source based on a type-II ppln waveguide emitting at a telecom wavelength”, *New J. Phys.*, vol. **12**, pp. 103005, 2010.
- [14] A. Martin, V. Cristofori, P. Aboussouan, H. Herrmann, W. Sohler, D. O. Ostrowsky, O. Alibart, and S. Tanzilli, “Integrated optical source of polarization entangled photons at 1310 nm”, *Opt. Express*, vol. **17**, pp. 1033–1041, 2008.
- [15] K. Thyagarajan, J. Lugani, S. Ghosh, K. Sinha, A. Martin, D. O. Ostrowsky, O. Alibart, and S. Tanzilli, “Generation of polarization-entangled photons using type-II doubly periodically poled lithium niobate waveguides”, *Phys. Rev. A*, vol. **80**, pp. 052321, 2009.
- [16] F. Kaiser, A. Issautier, L. A. Ngah, O. Dănilă, H. Herrmann, W. Sohler, A. Martin, and S. Tanzilli, “High-quality polarization entanglement state preparation and manipulation in standard telecommunication channels”, *New J. Phys.*, vol. **14**, pp. 085015, 2012.
- [17] A. Martin, F. Kaiser, Vernier A., A. Beveratos, V. Scarani, and S. Tanzilli, “Cross time-bin photonic entanglement for quantum key distribution”, 2012, Submitted to Nature Com., e-print arXiv : 1207.6586.
- [18] A. Martin, J. L. Smir, F. Kaiser, E. Diamanti, A. Issautier, O. Alibart, R. Frey, I. Zaquine, and S. Tanzilli, “Analysis of elliptically polarized maximally entangled states for Bell inequality tests”, *Laser Phys.*, vol. **22**, pp. 1–8, 2012.
- [19] F. Kaiser, A. Issautier, L. A. Ngah, O. Alibart, A. Martin, and S. Tanzilli, “A versatile source of polarization entanglement for quantum network applications”, 2012, Submitted to Nat. Photon., e-print arXiv :1111.5683.
- [20] F. Kaiser, T. Coudreau, P. Milman, D. B. Ostrowsky, and S. Tanzilli, “Entanglement-enabled delayed choice experiment”, *Science*, vol. **338**, pp. 637–640, 2012.
- [21] K. Thyagarajan, R. Das, O. Alibart, M. P. De Micheli, D. B. Ostrowsky, and S. Tanzilli, “Increased pump acceptance bandwidth in spontaneous parametric downconversion process using Bragg reflection waveguides”, *Opt. Express*, vol. **16**, pp. 3577–3582, 2008.
- [22] J. B. Altepeter, E. R. Jeffrey, P. G. Kwiat, S. Tanzilli, N. Gisin, and A. Acín, “Experimental methods for detecting entanglement”, *Phys. Rev. Lett.*, vol. **95**, pp. 033601, 2005.
- [23] M. Halder, S. Tanzilli, H. De Riedmatten, A. Beveratos, H. Zbinden, and N. Gisin, “Photon-bunching measurement after two 25-km-long optical fibers”, *Phys. Rev. A*, vol. **71**, pp. 042335, 2005.
- [24] P. Aboussouan, O. Alibart, D. O. Ostrowsky, P. Baldi, and S. Tanzilli, “Picosecond regime quantum interference using separated sources at telecom wavelength”, *Phys. Rev. A*, vol. **81**, pp. 021801(R), 2010.
- [25] O. Landry, J. van Houwelingen, P. Aboussouan, A. Beveratos, S. Tanzilli, H. Zbinden, and N. Gisin, “Simple synchronization of independent picosecond photon sources for quantum communication experiments”, 2010, e-print arXiv :1001.3389.
- [26] A. Martin, O. Alibart, M. P. De Micheli, D. B. Ostrowsky, and S. Tanzilli, “A quantum relay chip based on telecommunication integrated optics technology”, *New J. Phys.*, vol. **14**, pp. 025002, 2012.
- [27] A. Martin, O. Alibart, J.-C. Flesch, J. Samuel, S. Sinha, S. Tanzilli, and A. Kastberg, “Non-local geometric phase in two-photon interferometry”, *EPL*, vol. **97**, pp. 10003, 2012.

9.2 'Research Highlights' de certaines publications

- [1] N. Gisin, S. Tanzilli, W. Tittel, M. Halder, O. Alibart, P. Baldi, and H. Zbinden, "A photonic quantum information interface", *Opt. & Photon. News*, vol. **16**, pp. 40, 2006, Special Issue "Optics in 2005".
- [2] Eds Nature, "Research highlights on 'loopy fibres'", *Nature (London)*, vol. **440**, pp. 40, 2006.

9.3 Papiers publiés dans des proceedings internationaux avec comité de lecture

- [1] D. B. Ostrowsky, P. Baldi, M. P. De Micheli, S. Tanzilli, H. De Riedmatten, W. Tittel, H. Zbinden, and N. Gisin, "Introduction to guided-wave quantum optics (GWQO) : science, technology, and magic", *Proc. SPIE*, vol. 4417, pp. 12, 2001.
- [2] R. T. Thew, S. Tanzilli, A. Acin, H. Zbinden, and N. Gisin, "Energy-time entangled qutrits : Bell tests and quantum communication", *Quantum Communication, Measurement and Computing*, vol. **734**, pp. 249–252, 2004, 7th International Conference on Quantum Communication, Measurement and Computing.
- [3] D. B. Ostrowsky, O. Alibart, P. Baldi, and S. Tanzilli, "Guided-wave heralded single photon source at telecom wavelength", *Proc. SPIE*, vol. 5451, pp. 124, 2004.
- [4] O. Alibart, S. Tanzilli, M. P. De Micheli, D. B. Ostrowsky, and P. Baldi, "High performance guided-wave heralded single photon source at telecom wavelength", *Proc. SPIE*, vol. 5840, pp. 592, 2005.
- [5] M. Tournier, O. Alibart, F. Dautre, S. Tascu, M. P. De Micheli, D. B. Ostrowsky, K. Thyagarajan, and S. Tanzilli, "Up-conversion detectors at 1550 nm for quantum communication : review and recent advances", *EAS Pub. S.*, vol. 37, pp. 311–339, 2009.

9.4 Thèse de doctorat & participation à des ouvrages scientifiques

En plus de mon manuscrit de thèse de doctorat "Optique Intégrée pour les Communications Quantiques" (février 2002) [1], j'ai écrit, en collaboration avec Alexios Beveratos (LPN, Marcoussis), à l'écriture du chapitre 23 de l'édition VI du recueil "Advances in Information Optics and Photonics" produit chaque année par SPIE [2] et effectué, en collaboration avec mon collègue Olivier Alibart (LPMC) la traduction du livre de N. David Mermin intitulé "Quantum Computer Science" [3].

- [1] S. Tanzilli, *Optique intégrée pour les communications quantiques*, PhD thesis, Université de Nice - Sophia Antipolis, 2002.
- [2] A. Beveratos and S. Tanzilli, *Entanglement based quantum communication*, vol. **VI** of *Advances in Information Optics and Photonics*, chapter 23, pp. 457–488, SPIE, Eds. A. T. Friberg and R. Dändliker, Washington USA, 2008.
- [3] N. David Mermin, *Calculs & Algorithmes Quantiques, méthodes & exemples*, Collection Savoirs Actuels. EDP Sciences, Washington USA, cnrs editions edition, 2010, Traduction française par O. Alibart and S. Tanzilli de "Quantum Computer Science" de N. David Mermin.

9.5 Tutoriaux & cours

- "On the genesis and evolution of guided-wave quantum optics", [S. Tanzilli](#), International Workshop on Quantum Manipulation of Atoms and Photons (QMAP), October 16-22 2011, Shanghai, China.
- Short course on "Quantum Information : Photonic Technologies and Applications", [P. Kumar & S. Tanzilli](#), PHOTONICS'08 – 9th International Conference on Fiber Optics and Photonics, New Delhi, India, December 13-17, 2008.
- Tutorial on "Quantum communication", [S. Tanzilli](#), Symposium for young researchers on "Quantum Manipulation of Photons and Atoms", Beijing & Shanghai, China, October 14-22, 2008.
- Lecture on "Quantum communication : from the guided-wave point of view", [S. Tanzilli](#), CEFIPRA, Indo-French "Workshop on Lasers, Non-Linear Optics, Quantum Optics, and Cold Atoms", Gif-sur-Yvette, France, October 28-November 02, 2007.

9.6 Talks invités dans des conférences internationales et nationales

- “Engineering polarisation entanglement for quantum network applications”,
F. Kaiser, A. Issautier, L. A. Ngah, O. Alibart, A. Martin, and S. Tanzilli,
Quantum 2012, Torino, Italy, May 20-26, 2012.
- “La cryptographie : de l’antique à l’intrication quantique”, S. Tanzilli
Conférence Société Française de Physique (SFP), March 21 2012, Marseille, France.
- “Quantum communication based on integrated nonlinear optics”,
V. D’Auria, F. Kaiser, A. Martin, L. Labonté, D. B. Ostrowsky, O. Alibart, S. Tanzilli,
Int. Workshop on Quantum Manip. of Atoms and Photons (QMAP), Oct. 16-22 2011, Shanghai, China.
- “Narrowband polar. entangled photon-pair source in the telecom C-band for quantum networking”,
F. Kaiser, A. Issautier, O. Alibart, A. Martin, and S. Tanzilli,
Int. Workshop on Quantum Manip. of Atoms and Photons (QMAP), Oct. 16-22 2011, Shanghai, China.
- “Enabling quantum communication using integrated nonlinear optics”,
V. D’Auria, F. Kaiser, A. Martin, L. Labonté, M.P. De Micheli, O. Alibart, and S. Tanzilli,
SPIE Conference on Optical Complex Systems (OCS’2011), September 5-8 2011, Marseille, France.
- “Narrowband polar. entanglement sources based on IO for quantum appl. at telecom wavelength”,
F. Kaiser, A. Martin, A. Issautier, L. Labonté, V. D’Auria, O. Alibart, and S. Tanzilli,
IEEE Photonics Society, Summer Topicals on “Entanglement Distribution in Quantum Communication and Beyond” (SUM’2011),
July 18-20 2011, Montréal, Canada.
- “Analysis of elliptically polarized, maximally entangled states”,
A. Martin, J.-L. Smirr, F. Kaiser, V. D’Auria, R. Frey, O. Alibart, I. Zaquine, and S. Tanzilli,
LPHYS’11, July 11-15 2011, Sarajevo, Bosnia and Herzegovina.
- “Source de paires de photons intriqués en polar. émis en bande étroite aux longueurs d’ondes des télécoms”,
F. Kaiser, A. Martin, L. Labonté, V. D’Auria, M. P. De Micheli, O. Alibart, et S. Tanzilli,
COLOQ’12, July 4-7 2011, Marseille, France.
- “Fully fibred polar. entangled photon pair source at a telecom wavelength for quantum networking”,
F. Kaiser, A. Martin, V. D’Auria, M.P. De Micheli, O. Alibart, and S. Tanzilli,
ICTON’13, June 26-30 2011, Stockholm, Sweden.
- “Polar. entangled photon-pair source based on a type-II PPLN/W emitting at a telecom wavelength”,
A. Martin, A. Issautier, A. Thomas, H. Herrmann, W. Sohler, D. B. Ostrowsky, O. Alibart, and S. Tanzilli,
ICTON’12, Munich, Germany, June 27 - July 1, 2010.
- “Guided-wave optics for real quantum relay applications”,
A. Martin, F. Kaiser, O. Alibart, D. B. Ostrowsky, and S. Tanzilli,
Quantum 2010, Torino, Italy, May 23-29, 2010.
- “Optique guidée pour la communication quantique sur longue distance”, S. Tanzilli,
Colloque Optique Guidée et Photonique de l’AFCAS, Montréal, Canada, May 10-14, 2010.
- “Guided-wave optics for long distance quantum communication”,
O. Alibart, A. Martin, D. B. Ostrowsky, and S. Tanzilli,
WE-Heraeus-Seminar, Bad Honnef, Germany, March 22-25, 2010.
- “Vers un relais quantique hors du laboratoire”,
P. Aboussouan, O. Alibart, D. B. Ostrowsky, P. Baldi and S. Tanzilli,
COLOQ’11 - Nice, Mouans-Sartoux, France, September 07-09, 2009.
- “Interférence quantique à l’aide de deux photons à 1550 nm : vers un relais quantique réel”,
P. Aboussouan, O. Alibart, D. B. Ostrowsky, M. P. De Micheli, P. Baldi, and S. Tanzilli,
OPTIQUE 2009 - Journées Nationales d’Optique Guidée (JNOG), Lille, France, July 6-9, 2009.
- “Source optique intégrée de paires de photons intriqués en polarisation à 1310 nm”,
A. Martin, V. Cristofori, H. Herrmann, W. Sohler, D. B. Ostrowsky, O. Alibart et S. Tanzilli,
Colloque du GdR “Photonique NL et Milieux Microstructurés”, Montpellier, France, May 13-15, 2009.
- “Integrated optics for quantum communications toolbox : high visibility two-photon interference”,
A. Martin, P. Aboussouan, V. Cristofori, P. Baldi, M. P. De Micheli, D. B. Ostrowsky, H. Herrmann, W. Sohler, O. Alibart,
and S. Tanzilli,
PHOTONICS’08, New Delhi, India, December 13-17, 2008.
- “Counter propagating optical parametric interactions”,
P. Baldi, O. Alibart, P. Aschieri, M. P. De Micheli, and S. Tanzilli,
PHOTONICS’08, New Delhi, India, December 13-17, 2008.

- “Two-photon interference using integrated optical sources”,
O. Alibart and S. Tanzilli,
Colloque du GDR “Information et communication quantiques”, Paris, France, October 06-08, 2008.
- “Integrated optical source of polarization entangled photons at 1310 nm”,
A. Martin, V. Cristofori, D. B. Ostrowsky, H. Herrmann, W. Sohler, O. Alibart, and S. Tanzilli,
ICQO’08, Vilnius, Lithuania, September 20-23, 2008.
- “Integrated optics for quantum communication toolbox”,
O. Alibart, P. Aboussouan, A. Martin, P. Baldi, M. P. De Micheli, D. B. Ostrowsky, and S. Tanzilli,
LPHYS’08, Trondheim, Norway, June 30-July 4, 2008.
- “Advances in Quantum Communication using Integrated Optics : first results with a quantum relay chip”,
S. Tanzilli, S. Tascu, P. Aboussouan, O. Alibart, M. P. De Micheli, D. B. Ostrowsky, and P. Baldi,
ECIO’08, Eindhoven, The Netherlands, June 11-13, 2008.
- “Advances in Quantum Communication using integrated Optics”, S. Tanzilli,
LPHYS’07, León, Guanajuato, Mexico, August 20-24, 2007.
- “Advances in guided-wave quantum communication”, S. Tanzilli,
PHOTONICS’06, Hyderabad, India, December 10-13, 2006.
- “Quantum operations based on SFG : from IR light detection to quantum interfaces”, S. Tanzilli,
ECOC, CLEO focus meeting on Quant. Info. and Comm. Technol., Cannes, France, Sept. 24-28, 2006.
- “Quantum Communication with Integrated Optics”, S. Tanzilli,
NATO Advanc. Research Work. on Quant. Comm. and Secur., Gdansk, Poland, September 10-13, 2006.
- “Quantum communication and computation : a marriage of science and technology”,
D. B. Ostrowsky, O. Alibart, M. P. De Micheli, S. Tanzilli, and P. Baldi,
ICOL, Dehradun, India, December 12-15, 2005.
- “La téléportation quantique sur longue distance”,
S. Tanzilli, A. Beveratos, M. Halder, J.A.W. van Houwelingen, H. de Riedmatten, I. Marcikic, W. Tittel, H. Zbinden et N. Gisin,
Horizons de l’Optique, Chambéry, France, November 08-10, 2005.
- “Long Range Quantum Communication”,
A. Beveratos, M. Halder, J. Van Houwelingen, S. Tanzilli, N. Gisin, and H. Zbinden,
ECOC, Glasgow, Scotland, September 25-29, 2005.
- “Une Interface pour Qubits Photoniques”, S. Tanzilli,
Réunion du GDR 2285 “Information Quantique”, Palaiseau, France, October 19-20, 2005.
- “Integrated Optics for Quantum Communication”, S. Tanzilli,
Workshop on Atoms and Photons for Quantum Information, Shanghai, China, July 25-26, 2005.
- “Transfert de l’information quantique par conversion de longueurs d’ondes”,
S. Tanzilli, W. Tittel, M. Halder, O. Alibart, P. Baldi, N. Gisin, and H. Zbinden,
Réunion du GDR 2285 “Information Quantique”, Orsay, France, December 01-03, 2004.
- “Long distance entanglement swapping, perspectives for a real world quantum relay”,
Alexios Beveratos, H. de Riedmatten, I. Marcikic, M. Halder, J. van Houwelingen, S. Tanzilli, W. Tittel, H. Zbinden, and N. Gisin,
Réunion du GDR 2285 “Information Quantique”, Orsay, France, December 01-03, 2004.
- “Source optique intégrée pour les communications quantiques”,
P. Baldi, S. Tanzilli, O. Alibart, and D. B. Ostrowsky,
Réunion du GDR 2285 “Information Quantique”, Orsay, France, December, 01-03, 2004.
- “Photonic Quantum Information Interfaces”,
S. Tanzilli, A. Beveratos, W. Tittel, M. Halder, O. Alibart, P. Baldi, N. Gisin, and H. Zbinden,
ICSSUR, Besançon, France, May 02-06, 2005.
- “Non classical light sources for quantum communications using PPLN waveguides”,
P. Baldi, S. Tanzilli, O. Alibart, and D. B. Ostrowsky,
ICSSUR, Besançon, France, May 02-06, 2005.
- “Quantum information transfer in a wavelength conversion experiment”, S. Tanzilli,
QUIPROLO II, Workshop on Quant. Inf. Process. with Linear Optics, Bristol, UK, March 29-31, 2005.
- “Photonic technology for quantum communication”,
O. Alibart, D. B. Ostrowsky, S. Tanzilli, and P. Baldi,
PHOTONICS’04, Kochi, India, December 09-11, 2004.

- “Photonic integrated circuits for quantum communication and computation”,
D. B. Ostrowsky, O. Alibart, P. Baldi, and S. Tanzilli,
PHOTONICS’04 Europe, Strasbourg, France, April 26-30, 2004.
- “Quantum optics with short pulses”,
S. Tanzilli, P. Baldi, M. P. De Micheli, D. B. Ostrowsky, H. De Riedmatten, H. Zbinden, and N. Gisin,
Workshop on Quantum Optics, Bangalore, India, November 15-16, 2001.
- “PPLN waveguides for Quantum Communication”,
S. Tanzilli, W. Tittel, H. De Riedmatten, H. Zbinden, N. Gisin, P. Baldi, M. P. De Micheli, and D. B. Ostrowsky, QUICK,
Cargese, Corsica, France, April 07-13, 2001.
- “An Introduction to Guided Wave Quantum Optics (GWQO) : Science, Technology and Magic”,
D. B. Ostrowsky, P. Baldi, S. Tanzilli, H. De Riedmatten, W. Tittel, H. Zbinden, and N. Gisin,
ECIO’01, Paderborn, Germany, April 04-06, 2001.
- “Guided Wave Quantum Optics”,
D. B. Ostrowsky, S. Tanzilli, W. Tittel, H. Zbinden, P. Baldi, M. P. De Micheli, and N. Gisin,
Photonics’00, Calcutta, India, December 14-18, 2000.
- “Du paradoxe E.P.R. à l’Optique Quantique Intégrée”,
S. Tanzilli, P. Baldi, M. P. De Micheli, D. B. Ostrowsky, W. Tittel, H. Zbinden, and N. Gisin,
Réunion du GDR 1852 “Mx et Fonctions de l’ONL”, Lyon, France, November 8-10, 2000.
- “Integrated quantum optics : science, technology and magic”,
D. B. Ostrowsky, P. Baldi, M. P. De Micheli, and S. Tanzilli,
Photonics’98, New-Delhi, India, December 12-16, 1998.

Chapitre 10

Bibliographie générale

- [1] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems”, *Com. of the ACM*, vol. **21**, pp. 120–126, 1978.
- [2] R. L. Rivest, A. Shamir, and L.M. Adleman, “Cryptographic communications system and method”, 1983, US Patent 4,405,829.
- [3] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer”, *SIAM J. Sci. Statist. Comput.*, vol. **26**, pp. 1484–1509, 1997.
- [4] N. D. Mermin, *Quantum Computer Science : An Introduction*, Cambridge University Press, Cambridge, 2007, Traduction française chez EDP Sciences “Calculs et algorithmes quantiques : Méthodes et exemples”, O. Alibert and S. Tanzilli (traducteurs), ISBN-13 : 978-2759803958.
- [5] W. Tittel, J. Brendel, B. Gisin, T. Herzog, H. Zbinden, and N. Gisin, “Experimental demonstration of quantum correlations over more than 10 km”, *Phys. Rev. A*, vol. **57**, pp. 3229, 1998.
- [6] S. Tanzilli, A. Martin, F. Kaiser, M. P. De Micheli, O. Alibert, and D. B. Ostrowsky, “On the genesis and evolution of integrated quantum optics”, *Laser & Photon. Rev.*, vol. **6**, pp. 115–143, 2012, and references therein.
- [7] W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned”, *Nature (London)*, vol. **299**, pp. 802–803, 1982.
- [8] V. Bužek and M. Hillery, “Quantum copying : Beyond the no-cloning theorem”, *Phys. Rev. A*, vol. **54**, pp. 1844–1852, 1996.
- [9] V. Scarani, S. Iblisdir, N. Gisin, and A. Acín, “Quantum cloning”, *Rev. Mod. Phys.*, vol. **77**, pp. 1225–1256, 2005.
- [10] W. Tittel and G. Weihs, “Photonic entanglement for fundamental tests and quantum communication”, *Quant. Inf. Comp.*, vol. **1**, pp. 3–56, 2001.
- [11] Y. Makhlin, G. Schön, and A. Shnirman, “Josephson-junction qubits with controlled couplings”, *Nature (London)*, vol. **398**, pp. 305–307, 1999.
- [12] Y. Makhlin, G. Schön, and A. Shnirman, “Quantum-state engineering with josephson-junction devices”, *Rev. Mod. Phys.*, vol. **73**, pp. 357–400, 2001.
- [13] Y. Kubo *et al.*, “Strong coupling of a spin ensemble to a superconducting resonator”, *Phys. Rev. Lett.*, vol. **105**, pp. 140502, 2010.
- [14] 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, 1995.
- [15] F. Schmidt-Kaler *et al.*, “Realization of the cirac-zoller controlled-not quantum gate”, *Nature (London)*, vol. **422**, pp. 408–411, 2003.
- [16] D. Leibfried *et al.*, “Experimental demonstration of a robust, high-fidelity geometric two ion-qubit phase gate”, *Nature (London)*, vol. **422**, pp. 412–416, 2003.
- [17] M. D. Barrett *et al.*, “Deterministic quantum teleportation of atomic qubits”, *Nature (London)*, vol. **429**, pp. 737–739, 2004.
- [18] D. Leibfried *et al.*, “Creation of a six-atom ‘Schrodinger cat’ state”, *Nature (London)*, vol. **438**, pp. 639–642, 2005.
- [19] J. Beugnon, M. P. A. Jones, J. Dingjan, B. Darquié, G. Messin, A. Browaeys, and P. Grangier, “Quantum interference between two single photons emitted by independently trapped atoms”, *Nature (London)*, vol. **440**, pp. 779–782, 2006.
- [20] T. Wilk, A. Gaëtan, C. Evellin, J. Wolters, Y. Miroshnychenko, P. Grangier, and A. Browaeys, “Entanglement of two individual neutral atoms using Rydberg blockade”, *Phys. Rev. Lett.*, vol. **104**, pp. 010502, 2010.
- [21] L. Isenhower, E. Urban, X. L. Zhang, A. T. Gill, T. Henage, T. A. Johnson, T. G. Walker, and M. Saffman, “Demonstration of a neutral atom controlled-not quantum gate”, *Phys. Rev. Lett.*, vol. **104**, pp. 010503, 2010.
- [22] S. Ritter *et al.*, “An elementary quantum network of single atoms in optical cavities”, 2009, e-print arXiv :1202.5955.
- [23] A. I. Lvovsky, B. C. Sanders, and W. Tittel, “Optical quantum memory”, *Nat. Photon.*, vol. **3**, pp. 706–714, 2009, and references therein.
- [24] C. Simon *et al.*, “Quantum Memories”, *Eur. Phys. J. D*, vol. **58**, pp. 1–22, 2010.
- [25] T. Chanelière, J. Ruggiero, M. Bonarota, M Afzelius, and J.-L. Le Gouët, “Efficient light storage in a crystal using an atomic frequency comb”, *New J. Phys.*, vol. **12**, pp. 023025, 2010.
- [26] E. Saglamyurek, N. Sinclair, J. Jin, J. A. Slater, D. Oblak, F. Bussières, M. George, R. Ricken, W. Sohler, and W. Tittel, “Broadband waveguide quantum memory for entangled photons”, *Nature (London)*, vol. **469**, pp. 512–515, 2011.
- [27] C. Clausen, I. Usmani, F. Bussières, N. Sangouard, M. Afzelius, H. de Riedmatten, and N. Gisin, “Quantum storage of photonic entanglement in a crystal”, *Nature (London)*, vol. **469**, pp. 508–511, 2011.
- [28] K. F. Reim, J. Nunn, V. O. Lorenz, B. J. Sussman, K. C. Lee, N. K. Langford, D. Jaksch, and I. A. Walmsley, “Towards high-speed optical quantum memories”, *Nature Photon.*, vol. **4**, pp. 218–221, 2010.
- [29] T. Chanelière *et al.*, “Quantum telecommunication based on atomic cascade transitions”, *Phys. Rev. Lett.*, vol. **96**, pp. 093604, 2006.
- [30] B. Zhao *et al.*, “A millisecond quantum memory for scalable quantum networks”, *Nat. Phys.*, vol. **5**, pp. 95–99, 2009.

- [31] J. Cviklinski, J. Ortalo, J. Laurat, A. Bramati, M. Pinard, and E. Giacobino, “Reversible quantum interface for tunable single-sideband modulation”, *Phys. Rev. Lett.*, vol. **101**, pp. 133601, 2008.
- [32] H. Tanji, S. Ghosh, J. Simon, B. Bloom, and V. Vuletić, “Heralded single-magnon quantum memory for photon polarization states”, *Phys. Rev. Lett.*, vol. **103**, pp. 043601, 2009.
- [33] Y. O. Dudin, A. G. Radnaev, R. Zhao, J. Z. Blumoff, T. A. B. Kennedy, and A. Kuzmich, “Entanglement of light-shift compensated atomic spin waves with telecom light”, *Phys. Rev. Lett.*, vol. **105**, pp. 260502, 2010.
- [34] A. S. Sheremet, L. V. Gerasimov, I. M. Sokolov, D. V. Kupriyanov, O. S. Mishina, E. Giacobino, and J. Laurat, “Quantum memory for light via a stimulated off-resonant raman process : Beyond the three-level λ -scheme approximation”, *Phys. Rev. A*, vol. **82**, pp. 033838, 2010.
- [35] T. Golubeva, Yu. Golubev, O. Mishina, A. Bramati, J. Laurat, and E. Giacobino, “High-speed spatially multimode atomic memory”, *Phys. Rev. A*, vol. **83**, pp. 053810, 2011.
- [36] M. Lettner, M. Mücke, S. Riedl, C. Vo, C. Hahn, S. Baur, J. Bochmann, S. Ritter, S. Dürr, and G. Rempe, “Remote entanglement between a single atom and a Bose-Einstein condensate”, *Phys. Rev. Lett.*, vol. **106**, pp. 210503, 2011.
- [37] C. Sayrin *et al.*, “Real-time quantum feedback prepares and stabilizes photon number states”, *Nature*, vol. **477**, pp. 73–77, 2011.
- [38] S. Haroche and J.-M. Raimond, *Exploring the Quantum : Atoms, Cavities, and Photons*, Oxford Univ. Press, 2006.
- [39] C. Weedbrook *et al.*, “Gaussian quantum information”, *Rev. of Mod. Phys.*, vol. **84**, pp. 621–669, 2012.
- [40] P. Siyushev, V. Jacques, I. Aharonovich, F. Kaiser, T. Müller, L. Lombez, M. Atatüre, S. Castelletto, S. Praver, F. Jelezko, and J. Wrachtrup, “Low-temperature optical characterization of a near-infrared single-photon emitter in nanodiamonds”, *New J. Phys.*, vol. **11**, pp. 113029, 2009.
- [41] E. Moreau, I. Robert, L. Manin, V. Thierry-Mieg, J. M. Gérard, and I. Abram, “Quantum cascade of photons in semiconductor quantum dots”, *Phys. Rev. Lett.*, vol. **87**, pp. 183601, 2001.
- [42] J. Vučković, D. Fattal, C. Santori, G. S. Solomon, and Y. Yamamoto, “Quantum cascade of photons in semiconductor quantum dots”, *Appl. Phys. Lett.*, vol. **82**, pp. 3596–3598, 2003.
- [43] P. Grangier, G. Roger, and A. Aspect, “Experimental evidence for a photon anticorrelation effect on a beam splitter : A new light on single-photon interferences”, *EPL*, vol. **1**, pp. 173, 1986.
- [44] S. Fasel, O. Alibart, S. Tanzilli, P. Baldi, A. Beveratos, N. Gisin, and H. Zbinden, “High-quality asynchronous heralded single-photon source at telecom wavelength”, *New J. Phys.*, vol. **6**, pp. 163, 2004.
- [45] O. Alibart, D. B. Ostrowsky, P. Baldi, and S. Tanzilli, “High-performance guided-wave asynchronous heralded single-photon source”, *Opt. Lett.*, vol. **30**, pp. 1539–1541, 2005.
- [46] M. Förtsch, J. Fürst, C. Wittmann, D. Strelakov, A. Aiello, M. V. Chekhova, C. Silberhorn, G. Leuchs, and C. Marquardt, “A versatile source of single photons for quantum information processing”, 2012, e-print arXiv :1204.3056.
- [47] M. Medic, J. B. Altepeter, M. A. Hall, M. Patel, and P. Kumar, “Fiber-based telecommunication-band source of degenerate entangled photons”, *Opt. Lett.*, vol. **35**, no. 6, pp. 802–804, 2010.
- [48] A. R. McMillan, J. Fulconis, M. Halder, C. Xiong, J. G. Rarity, and W. J. Wadsworth, “Narrowband high-fidelity all-fibre source of heralded single photons at 1570 nm”, *Opt. Express*, vol. **17**, no. 8, pp. 6156–6165, 2009.
- [49] V. Jacques, E. Wu, F. Grosshans, F. Treussart, P. Grangier, A. Aspect, and J.-F. Roch, “Experimental realization of Wheeler’s delayed-choice Gedanken experiment”, *Science*, vol. **315**, pp. 966–968, 2007.
- [50] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, “Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors”, *Nature Photon.*, vol. **1**, pp. 343–345, 2007.
- [51] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gary, C. R. Towerty, and S. Ten, “High rate, long-distance quantum key distribution over 250 km of ultra low loss fibers”, *New J. Phys.*, vol. **11**, pp. 075003, 2009.
- [52] J. E. Baggott, *The meaning of quantum theory*, Oxford University Press, New York, 1992.
- [53] A. Einstein, B. Podolsky, and N. Rosen, “Can quantum-mechanical description of physical reality be considered complete?”, *Phys. Rev.*, vol. **47**, pp. 777–780, 1935.
- [54] D. Bohm, “A suggested interpretation of the quantum theory in terms of “hidden” variables. I and II”, *Phys. Rev.*, vol. **85**, pp. 166–193, 1951.
- [55] J. S. Bell, “On the Einstein-Podolsky-Rosen paradox”, *Physics (Long Island City, N.Y.)*, vol. **1**, pp. 195–200, 1964.
- [56] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, “Proposed experiment to test local hidden-variable theories”, *Phys. Rev. Lett.*, vol. **23**, pp. 880–884, 1969.
- [57] C. Ruhla, *La physique de hasard. De Blaise Pascal à Niels Bohr*, Hachette-CNRS, 1989.
- [58] J. Harthong, *Probabilités et statistiques. De l’intuition aux applications*, Diderot Editeur, Arts et Sciences, 1996.
- [59] F. Laloë, *Comprenons-nous vraiment la mécanique quantique ?*, EDP Sciences, 2011.
- [60] S. J. Freedman and J. F. Clauser, “Experimental test of local hidden-variable theories”, *Phys. Rev. Lett.*, vol. **28**, pp. 938–941, 1972.
- [61] G. Faraci, D. Gutkowski, S. Notarrigo, and A. Pennisi, “An experimental test of the EPR paradox”, *Nuovo Cimento*, vol. **9**, pp. 607–611, 1974.
- [62] L. Kasday, J. D. Ullman, and C. Wu, “Angular correlation of Compton-scattered annihilation photons and hidden variables”, *Nuovo Cimento B*, vol. **25**, pp. 633–661, 1975.
- [63] R. A. Holt and F. M. Pipkin, “Quantum mechanics vs hidden variables : polarization correlation measurement on an atomic mercury cascade”, Preprint, Physics Dept., University of Southern Ontario, Canada ; See also R. A. Holt, PhD thesis, Harvard University, 1973 (unpublished).

-
- [64] J. F. Clauser, “Experimental investigation of a polarization correlation anomaly”, *Phys. Rev. Lett.*, vol. **36**, pp. 1223–1226, 1976.
- [65] E. S. Fry and R. C. Thompson, “Experimental test of local hidden-variable theories”, *Phys. Rev. Lett.*, vol. **37**, pp. 465–468, 1976.
- [66] A. R. Wilson, J. Lowe, and D. K. Butt, “Measurement of the relative planes of polarization of annihilation quanta as a function of separation distance”, *J. Phys. G : Nucl. Phys.*, vol. **2**, pp. 613–624, 1976.
- [67] M. Laméhi-Rachti and W. Mittig, “Quantum mechanics and hidden variables : A test of Bell’s inequality by the measurement of the spin correlation in low-energy proton-proton scattering”, *Phys. Rev. D*, vol. **14**, pp. 2543–2555, 1976.
- [68] A. Aspect, P. Grangier, and G. Roger, “Experimental tests of realistic local theories via Bell’s theorem”, *Phys. Rev. Lett.*, vol. **47**, pp. 460–463, 1981.
- [69] A. Aspect, P. Grangier, and G. Roger, “Experimental realization of Einstein-Podolsky-Rosen-Bohm gedankenexperiment : A new violation of Bell’s inequalities”, *Phys. Rev. Lett.*, vol. **49**, pp. 91–94, 1982.
- [70] A. Aspect, J. Dalibard, and G. Roger, “Experimental test of Bell’s inequalities using time-varying analyzers”, *Phys. Rev. Lett.*, vol. **49**, pp. 1804–1807, 1982.
- [71] J. B. Altepeter, E. R. Jeffrey, P. G. Kwiat, S. Tanzilli, N. Gisin, and A. Acín, “Experimental methods for detecting entanglement”, *Phys. Rev. Lett.*, vol. **95**, pp. 033601, 2005.
- [72] A. Martin, J. L. Smirr, F. Kaiser, E. Diamanti, A. Issautier, O. Alibart, R. Frey, I. Zaquine, and S. Tanzilli, “Analysis of elliptically polarized maximally entangled states for bell inequality tests”, *Laser Phys.*, vol. **22**, pp. 1–8, 2012.
- [73] D. Collins and N. Gisin, “A relevant two qubit Bell inequality inequivalent to the CHSH inequality”, *J. Phys. A*, vol. **37**, pp. 1775, 2004.
- [74] D. F. V. James, P. G. Kwiat, W. J. Munro, and A. G. White, “Measurement of qubits”, *Phys. Rev. A*, vol. **64**, pp. 052312, 2001.
- [75] “NuCrypt (USA)”, <http://www.nucrypt.net/>.
- [76] K. Sanaka, K. Kawahara, and T. Kuga, “Experimental probabilistic manipulation of down-converted photon pairs using unbalanced interferometers”, *Phys. Rev. A*, vol. **66**, pp. 040301, 2002.
- [77] F. Kaiser, A. Issautier, L. A. Ngah, O. Alibart, A. Martin, and S. Tanzilli, “A versatile source of polarization entanglement for quantum network applications”, 2012, e-print arXiv :1111.5683.
- [78] G. Ribordy, J. Brendel, J.-D. Gautier, N. Gisin, and H. Zbinden, “Long-distance entanglement-based quantum key distribution”, *Phys. Rev. A*, vol. **63**, pp. 012309, 2000.
- [79] Z. Y. Ou and L. Mandel, “Violation of Bell’s inequality and classical probability in a two-photon correlation experiment”, *Phys. Rev. Lett.*, vol. **61**, pp. 50–53, 1988.
- [80] Y. H. Shih and C. O. Alley, “New type of Einstein-Podolsky-Rosen-Bohm experiment using pairs of light quanta produced by optical parametric down conversion”, *Phys. Rev. Lett.*, vol. **61**, pp. 2921–2924, 1988.
- [81] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, “New high-intensity source of polarization-entangled photon pairs”, *Phys. Rev. Lett.*, vol. **75**, pp. 4337–4341, 1995.
- [82] P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard, “Ultrabright source of polarization-entangled photons”, *Phys. Rev. A*, vol. **60**, pp. R773–R776, 1999.
- [83] R. Ursin *et al.*, “Entanglement-based quantum communication over 144 km”, *Nat. Phys.*, vol. **3**, pp. 481–486, 2007.
- [84] J. D. Franson, “Bell inequality for position and time”, *Phys. Rev. Lett.*, vol. **62**, pp. 2205–2208, 1989.
- [85] S. Tanzilli, W. Tittel, H. de Riedmatten, H. Zbinden, P. Baldi, M. P. De Micheli, D. B. Ostrowsky, and N. Gisin, “PPLN waveguide for quantum communication”, *Eur. Phys. J. D*, vol. **18**, pp. 155–160, 2002.
- [86] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden, “Pulsed energy-time entangled twin-photon source for quantum communication”, *Phys. Rev. Lett.*, vol. **82**, pp. 2594–2597, 1999.
- [87] R. T. Thew, S. Tanzilli, W. Tittel, H. Zbinden, and N. Gisin, “Experimental investigation of the robustness of partially entangled qubits over 11 km”, *Phys. Rev. A*, vol. **66**, pp. 062304, 2002.
- [88] J. G. Rarity and P. R. Tapster, “Experimental violation of Bell’s inequality based on phase and momentum”, *Phys. Rev. Lett.*, vol. **64**, pp. 2495–2498, 1990.
- [89] J. Brendel, E. Mohler, and W. Martienssen, “Experimental test of Bell’s inequality for energy and time”, *Europhys. Lett.*, vol. **20**, pp. 1923–1926, 1992.
- [90] P. G. Kwiat, A. M. Steinberg, and R. Y. Chiao, “High-visibility interference in a Bell-inequality experiment for energy and time”, *Phys. Rev. A*, vol. **47**, pp. R2472–R2475, 1993.
- [91] J. G. Rarity, J. Burnett, P. R. Tapster, and R. Paschotta, “High-visibility two-photon interference in a single-mode-fibre interferometer”, *Europhys. Lett.*, vol. **22**, pp. 95–100, 1993.
- [92] J. G. Rarity, P. R. Tapster, and P. C. M. Owens, “Violation of Bell’s inequality over 4 km of optical fiber”, *Phys. Rev.*, vol. **73**, pp. 1923–1926, 1994.
- [93] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, “Violation of Bell inequalities by photons more than 10 km apart”, *Phys. Rev. Lett.*, vol. **81**, pp. 3563–3566, 1998.
- [94] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, “Long distance Bell-type tests using energy-time entangled photons”, *Phys. Rev. A*, vol. **59**, pp. 4150–4163, 1999.
- [95] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, “Violation of Bell’s inequality under strict einstein locality conditions”, *Phys. Rev. Lett.*, vol. **81**, pp. 5039–5043, 1998.
- [96] A. Aspect, “Bell’s inequality test : more ideal than ever”, *Nature*, vol. **398**, pp. 189–190, 1999.

- [97] P. Eberhard, “Background level and counter efficiencies required for a loophole-free Einstein-Podolsky-Roser experiment”, *Phys. Rev. A*, vol. **47**, pp. R747–R750, 1993.
- [98] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland, “Experimental violation of a Bell’s inequality with efficient detection”, *Nature (London)*, vol. **409**, pp. 791–794, 2001.
- [99] A. Martin, A. Issautier, H. Herrmann, W. Sohler, D. B. Ostrowsky, O. Alibart, and S. Tanzilli, “A polarization entangled photon-pair source based on a type-II PPLN waveguide emitting at a telecom wavelength”, *New J. Phys.*, vol. **12**, pp. 103005, 2010, and references therein.
- [100] T. Zhong, X. Hu, F. N. C. Wong, K. K. Berggren, T. D. Roberts, and P. Battle, “High-quality fiber-optic polarization entanglement distribution at 1.3 μm telecom wavelength”, *Opt. Lett.*, vol. **35**, pp. 1392–1394, 2010.
- [101] F. Kaiser, A. Issautier, L. A. Ngah, O. Dănilă, H. Herrmann, W. Sohler, A. Martin, and S. Tanzilli, “High-quality polarization entanglement state preparation and manipulation in standard telecommunication channels”, 2012, To appear in *New J. Phys.*, e-print arXiv : 1206.3809.
- [102] M. Halder, A. Beveratos, R. T. Thew, C. Jorel, H. Zbinden, and N. Gisin, “High coherence photon pair source for quantum communication”, *New J. Phys.*, vol. **10**, 2008.
- [103] E. Pomarico, B. Sanguinetti, N. Gisin, R. Thew, H. Zbinden, G. Schreiber, A. Thomas, and W. Sohler, “Waveguide-based OPO source of entangled photon pairs”, *New J. Phys.*, vol. **11**, pp. 113042, 2009.
- [104] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré, and N. Gisin, “Distribution of Time-Bin entangled qubits over 50 km of optical fiber”, *Phys. Rev. Lett.*, vol. **93**, pp. 180502, 2004.
- [105] J. Dynes, H. Takesue, Z. Yuan, A. Sharpe, K. Harada, T. Honjo, H. Kamada, O. Tadanaga, Y. Nishida, M. Asobe, and A. Shields, “Efficient entanglement distribution over 200 kilometers”, *Opt. Express*, vol. **17**, pp. 11440, 2009.
- [106] T. Suhara, “Generation of quantum-entangled twin photons by waveguide nonlinear-optic devices”, *Laser & Photon. Rev.*, vol. **3**, pp. 370–393, 2009.
- [107] A. Dousse, J. Suffczynski, A. Beveratos, O. Krebs, A. Lemaître, I. Sagnes, J. Bloch, P. Voisin, and P. Senellart, “Ultrabright source of entangled photon pairs”, *Nature (London)*, vol. **466**, pp. 217–220, 2010.
- [108] X. Caillet, A. Orioux, A. Lemaître, P. Filloux, I. Favero, G. Leo, and S. Ducci, “Two-photon interference with a semiconductor integrated source at room temperature”, *Opt. Express*, vol. **18**, pp. 9967–9975, 2010.
- [109] J. Fulconis, O. Alibart, J. L. O’Brien, W. J. Wadsworth, and J. G. Rarity, “Nonclassical interference and entanglement generation using a photonic crystal fiber pair photon source”, *Phys. Rev. Lett.*, vol. **99**, pp. 120501, 2007.
- [110] C. H. Bennett and G. Brassard, “Quantum cryptography : Public key distribution and coin tossing”, *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India*, p. 175, 1984.
- [111] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography”, *Rev. Mod. Phys.*, vol. **74**, pp. 145–195, 2002.
- [112] 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, 2009.
- [113] “ID Quantique (Switzerland)”, <http://idquantique.com>.
- [114] “MagiQ Technology (usa)”, <http://www.magiqtech.com/>.
- [115] “SeQureNet (France)”, <http://www.sequirenet.fr/>.
- [116] “Auréa Technologie (France)”, <http://aureatechnology.fr/>.
- [117] “QuTools (Germany)”, <http://www.qutools.com/>.
- [118] “QuintessenceLabs (Australia)”, <http://qlabsusa.com/>.
- [119] D. Stucki *et al.*, “Long-term performance of the swissquantum quantum key distribution network in a field environment”, *New J. Phys.*, vol. **13**, pp. 123001, 2011.
- [120] “SECOQC”, European project in the FP6 program, duration 1.4.2004/10.10.2008, <http://www.secoqc.net/>.
- [121] M. Peev *et al.*, “The SECOQC quantum key distribution network in vienna”, *New J. Phys.*, vol. **11**, pp. 075001, 2009.
- [122] M. Sasaki *et al.*, “Field test of quantum key distribution in the Tokyo QKD network”, *Opt. Express*, vol. **19**, pp. 10387–10409, 2011.
- [123] S. Singh, *Histoire des codes secrets*, LGF - Le livre de poche, 1999.
- [124] G.S. Vernam, “Secret signaling system”, 1919, US patent 1,310,719.
- [125] C. E. Shannon, “Communication theory of secrecy systems”, *Bell Syst. Tech. J.*, vol. **28**, pp. 656–715, 1949.
- [126] A. Kerckhoffs, “La cryptographie militaire”, *Journal des sciences militaires*, vol. **9**, pp. 5–38, 1883.
- [127] A. K. Ekert, “Quantum cryptography based on Bell’s theorem”, *Phys. Rev. Lett.*, vol. **97**, pp. 661–664, 1991.
- [128] C. H. Bennett, “Quantum cryptography using any two non-orthogonal states”, *Phys. Rev. Lett.*, vol. **68**, pp. 3121–3124, 1992.
- [129] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, “Experimental quantum cryptography”, *J. Cryptol.*, vol. **5**, pp. 3–28, 1992.
- [130] A. Muller, H. Zbinden, and N. Gisin, “Quantum cryptography over 23 km in installed under-lake telecom fibre”, *EPL*, vol. **33**, pp. 335, 1996.
- [131] R. Alléaume, F. Treussart, G. Messin, Y. Dumeige, J.-F. Roch, A. Beveratos, R. Brouri-Tualle, J.-P. Poizat, and P. Grangier, “Experimental open-air quantum key distribution with a single-photon source”, *New J. Phys.*, vol. **6**, no. 1, pp. 92, 2004.
- [132] R. T. Thew, S. Tanzilli, L. Krainer, S. C. Zeller, A. Rochas, I. Rech, S. Cova, H. Zbinden, and N. Gisin, “Low jitter up-conversion detectors for telecom wavelength GHz QKD”, *New J. Phys.*, vol. **8**, pp. 32, 2006.
- [133] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, “Quantum Cryptography with entangled photons”, *Phys. Rev. Lett.*, vol. **84**, pp. 4729–4732, 2000.

- [134] D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat, “Entangled state quantum cryptography : Eavesdropping on the ekert protocol”, *Phys. Rev. Lett.*, vol. **84**, pp. 4733–4736, 2000.
- [135] W. Tittel, J. Brendel, N. Gisin, and H. Zbinden, “Quantum Cryptography using entangled photons in energy-time Bell states”, *Phys. Rev. Lett.*, vol. **84**, pp. 4737–4740, 2000.
- [136] 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”, *Eur. Phys. J. D*, vol. **30**, pp. 143–148, 2004.
- [137] H. Takesue, K.-I. Harada, K. Tamaki, H. Fukuda, T. Tsuchizawa, T. Watanabe, K. Yamada, and S.-I. Itabashi, “Long-distance entanglement-based quantum key distribution experiment using practical detectors”, *Opt. Express*, vol. **18**, no. 16, pp. 16777–16787, 2010.
- [138] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, “Device-independent security of quantum cryptography against collective attacks”, *Phys. Rev. Lett.*, vol. **98**, pp. 230501, 2007.
- [139] L. Masanes, S. Pironio, and A. Acín, “Secure device-independent quantum key distribution with causally independent measurement devices”, *Nature Commun.*, vol. **2**, pp. 238, 2011.
- [140] I. Gerhardt, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, “Full-field implementation of a perfect eavesdropper on a quantum cryptography system”, *Nat. Comm.*, vol. **2**, pp. 349, 2011.
- [141] R. H. Hadfield, “Single-photon detectors for optical quantum information application”, *Nature Photon.*, vol. **3**, pp. 696–705, 2009.
- [142] 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-Podolsky-Rosen channels”, *Phys. Rev. Lett.*, vol. **70**, pp. 1895–1899, 1993.
- [143] D. Bouwmeester, J. W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, “Experimental quantum teleportation”, *Nature (London)*, vol. **390**, pp. 575–579, 1997.
- [144] D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu, “Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels”, *Phys. Rev. Lett.*, vol. **80**, pp. 1121–1125, 1998.
- [145] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, and N. Gisin, “Long-distance teleportation of qubits at telecommunication wavelengths”, *Nature (London)*, vol. **421**, pp. 509–513, 2003.
- [146] O. Landry, J. A. W. van Houwelingen, A. Beveratos, H. Zbinden, and N. Gisin, “Quantum teleportation over the Swisscom telecommunication network”, *J. Opt. Soc. Am. B*, vol. **24**, pp. 398–403, 2007.
- [147] M. Halder, A. Beveratos, N. Gisin, V. Scarani, C. Simon, and H. Zbinden, “Entangling independent photons by time measurement”, *Nature Phys.*, vol. **3**, pp. 692–695, 2007.
- [148] R. Kaltenbaek, B. Blauensteiner, M. Zukowski, M. Aspelmeyer, and A. Zeilinger, “Experimental interference of independent photons”, *Phys. Rev. Lett.*, vol. **96**, no. 24, pp. 240502–4, 2006.
- [149] R. Kaltenbaek, R. Prevedel, M. Aspelmeyer, and A. Zeilinger, “High-fidelity entanglement swapping with fully independent sources”, *Phys. Rev. A*, vol. **79**, pp. 040302, 2009.
- [150] P. Aboussouan, O. Alibart, D. B. Ostrowsky, P. Baldi, and S. Tanzilli, “High-visibility two-photon interference at a telecom wavelength using picosecond-regime separated sources”, *Phys. Rev. A*, vol. **81**, pp. 021801(R), 2010.
- [151] O. Landry, J. A. W. van Houwelingen, P. Aboussouan, A. Beveratos, S. Tanzilli, H. Zbinden, and N. Gisin, “Simple synchronization of independent picosecond photon sources for quantum communication experiments”, *arXiv preprint arXiv :1001.3389*, 2010.
- [152] D. Collins, N. Gisin, and H. de Riedmatten, “Quantum relays for long distance quantum cryptography”, *J. Mod. Opt.*, vol. **52**, pp. 735–753, 2005.
- [153] H. de Riedmatten, I. Marcikic, W. Tittel, H. Zbinden, D. Collins, and N. Gisin, “Long distance quantum teleportation in a quantum relay configuration”, *Phys. Rev. Lett.*, vol. **92**, pp. 047904, 2004.
- [154] N. Lütkenhaus, “Security against individual attacks for realistic quantum key distribution”, *Phys. Rev. A*, vol. **61**, pp. 052304, 2000.
- [155] “SCONTEL - SuperCOducting NanoTEchnoLoGY (Russia)”, [http://http://www.scontel.ru](http://www.scontel.ru).
- [156] A. Martin, O. Alibart, M. P. De Micheli, D. B. Ostrowsky, and S. Tanzilli, “A quantum relay chip based on telecommunication integrated optics technology”, *New J. Phys.*, vol. **14**, pp. 025002, 2012.
- [157] H. de Riedmatten, I. Marcikic, J. A. W. Van Houwelingen, W. Tittel, H. Zbinden, and N. Gisin, “Long-distance entanglement swapping with photons from separated sources”, *Phys. Rev. A*, vol. **71**, pp. 050302(R), 2005.
- [158] H. Takesue and B. Miquel, “Entanglement swapping using telecom-band photons generated in fibers”, *Opt. Express*, vol. **17**, pp. 10748, 2009.
- [159] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, “Long-distance quantum communication with atomic ensembles and linear optics”, *Nature (London)*, vol. **414**, pp. 413–418, 2001.
- [160] C. Simon *et al.*, “Quantum memories”, *Eur. Phys. J. D*, vol. **58**, pp. 1–22, 2010, and references therein.
- [161] N. Sangouard, 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, 2011.
- [162] J. C. F. Matthews, A. Politi, A. Stefanov, and J. L. O’Brien, “Manipulation of multiphoton entanglement in waveguide quantum circuits”, *Nat. Photon.*, vol. **3**, pp. 346–350, 2009.
- [163] A. Politi, J. C. F. Matthews, and J. L. O’Brien, “Shor’s quantum factoring algorithm on a photonic chip”, *Science*, vol. **325**, pp. 1221, 2009.
- [164] L. K. Grover, “A fast quantum mechanical algorithm for database search”, in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, New York, NY, USA, 1996, STOC ’96, pp. 212–219, ACM.

-
- [165] B. P. Lanyon *et al.*, “Towards quantum chemistry on a quantum computer”, *Nature Chem.*, vol. **2**, pp. 106–111, 2010.
- [166] S. Tanzilli, *Optique intégrée pour les communications quantiques*, PhD thesis, Université de Nice – Sophia Antipolis, 2002, <http://tel.archives-ouvertes.fr/tel-00008814>.
- [167] L. Chanvillard, P. Aschiéri, P. Baldi, D. B. Ostrowsky, M. P. De Micheli, L. Huang, and D. J. Bamford, “Soft proton exchange on periodically poled LiNbO₃ : A simple waveguide fabrication process for highly efficient nonlinear interactions”, *Appl. Phys. Lett.*, vol. 76, no. **9**, pp. 1089–1091, 2000.
- [168] G. Giorgi, P. Mataloni, and F. De Martini, “Frequency hopping in quantum interferometry : Efficient up-down conversion for qubits and ebits”, *Phys. Rev. Lett.*, vol. **90**, pp. 027902, 2003.
- [169] N. Curtz, R. Thew, C. Simon, N. Gisin, and H. Zbinden, “Coherent frequency-down-conversion interface for quantum repeaters”, *Opt. Express*, vol. **18**, pp. 22099–22104, 2010.
- [170] H. Takesue, “Single-photon frequency down-conversion experiment”, *Phys. Rev. A*, vol. **82**, pp. 013833, 2010.
- [171] R. V. Roussev, C. Langrock, J. R. Kurz, and M. M. Fejer, “Periodically poled lithium niobate waveguide sum-frequency generator for efficient single-photon detection at communication wavelengths”, *Opt. Lett.*, vol. **29**, pp. 1518–1520, 2004.
- [172] C. Langrock, E. Diamanti, R. V. Roussev, Y. Yamamoto, and M. M. Fejer, “Highly efficient single-photon detection at communication wavelengths by use of upconversion in reverse-proton-exchanged periodically poled limbo3 waveguides”, *Opt. Lett.*, vol. **30**, pp. 1725–1727, 2005.
- [173] J. S. Pelc, Q. Zhang, C. R. Phillips, L. Yu, Y. Yamamoto, and M. M. Fejer, “Cascaded frequency upconversion for high-speed single-photon detection at 1550 nm”, *Opt. Lett.*, vol. **37**, pp. 476–478, 2012.
- [174] S. Tanzilli, W. Tittel, M. Halder, O. Alibart, P. Baldi, N. Gisin, and H. Zbinden, “A photonic quantum information interface”, *Nature (London)*, vol. **437**, pp. 116–120, 2005.
- [175] 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, 1987.
- [176] X.-H. Bao, Y. Qian, J. Yang, H. Zhang, Z.-B. Chen, T. Yang, and J.-W. Pan, “Generation of narrow-band polarization-entangled photon pairs for atomic quantum memories”, *Phys. Rev. Lett.*, vol. **101**, pp. 190501, 2008.
- [177] Hui Yan, Shanchao Zhang, J. F. Chen, M. M. T. Loy, G. K. L. Wong, and Shengwang Du, “Generation of narrow-band hyperentangled nondegenerate paired photons”, *Phys. Rev. Lett.*, vol. **106**, pp. 033601, 2011, and references therein.
- [178] C. E. Kuklewicz, F. N. C. Wong, and J. H. Shapiro, “Time-bin-modulated biphotons from cavity-enhanced down-conversion”, *Phys. Rev. Lett.*, vol. **97**, pp. 223601, 2006.
- [179] N. Piro, A. Haase, M. W. Mitchell, and J. Eschner, “An entangled photon source for resonant single-photon-single-atom interaction”, *J. Phys. B*, vol. 42, pp. 114002, 2009.
- [180] J. A. Wheeler and W. H. Zurek, *Quantum Theory and Measurement*, Eds. (Princeton Univ. Press, Princeton, NJ), 1984.
- [181] H. de Riedmatten, I. Marcikic, W. Tittel, H. Zbinden, and N. Gisin, “Quantum interference with photon pairs created in spatially separated sources”, *Phys. Rev. A*, vol. **67**, pp. 022301, 2003.