

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Frères Mentouri Constantine
Faculté des Sciences et de la Technologie
Département d'électronique

N° d'ordre :

Série :

Thèse

Présentée pour obtenir le diplôme de Doctorat Troisième Cycle
En Electronique

Option

Hyperfréquences et Télécommunications

Thème

**Marches quantiques généralisées pour
l'algorithmique quantique appliquées à un
routeur optique du type WDM**

Présentée Publiquement Par:

Nadhir DJEFFAL

Devant le jury:

Président:	Mr BOUCHEMAT Mohamed	Professeur	Université Constantine 1
Rapporteur :	Mr M. BENSLAMA	Professeur	Université Constantine 1
Examineurs:	Mr Noureddine Mebarki	Professeur	Université Constantine 1
	Mr BENATIA Djamel	Professeur	Université Hadj Lakhdar Batna
	Mr FORTAKI Tarek	Professeur	Université Hadj Lakhdar Batna

ANNEE 2016

Remerciements

Ce travail de recherche a été effectué au sein de laboratoire de recherche ; le Laboratoire d'Electromagnétisme et Télécommunications (LTE) de l'Université Constantine 1, sous la direction de Professeur **Mohamed el hadi Riabi**.

Mes remerciements, avant tout, à **ALLAH** tout puissant pour la volonté, la santé et la patience qu'il m'a données durant toutes ces longues années d'études afin que je puisse arriver à ce stade.

A **Mr. BENSLAMA Malek** qu'il me soit permis de le remercier et de lui exprimer ma profonde reconnaissance pour son aide et ses encouragements au cours de ce travail, ses précieux conseils et la confiance dont il a fait preuve à mon égard et surtout pour le sujet intéressant qu'il m'a proposé.

J'exprime ma profonde reconnaissance à **Mr. BOUCHEMAT Mohamed**, Professeur au département d'Electronique de l'université Constantine 1 pour l'honneur qu'il m'a fait d'accepter de présider le jury de cette thèse.

Mes remerciements vont également à **Mr. BENATIA Djamel**, Professeur à l'Université de Batna, à **Mr. FORTAKI Tarek**, Professeur à l'Université de Batna et à **Mr. Noureddine Mebarki**, Professeur à l'Université Constantine 1 qui m'ont fait l'honneur de participer au jury de ma thèse et d'examiner ce travail.

Je tiens à exprimer mes vifs remerciements à tous mes amis chacun par son nom, sans oublier l'ensemble des enseignants ayant contribué de près ou de loin à ma formation.

Résumé

Dans ce travail de thèse, on est intéressé à l'étude de nouvelles techniques et approches pour des communications optiques et de cryptage quantiques. Dans un premier temps, on adécrit les différentes techniques de communications optiques et particulièrement celle qui est utilisée dans les systèmes à accès multiples (Optical Code Division Multiplexing Access). Dans le même contexte, on a détaillé les différents codes proposés dans la littérature pour réaliser ce type de technique d'accès, y compris les différentes étapes nécessaires pour générer des codes de types 1D et 2D. La deuxième partie est consacrée à l'étude de la notion des marches quantiques généralisées pour les applications WDM (Wavelength Division Multiplexing). En commençant par l'établissement de l'état de l'art de ce type de cryptage quantique et ensuite on présente quelques modèles étudiés dans les derniers décennies. La troisième partie est divisée en deux sous partie. Premièrement, nous proposons une nouvelle famille de code pour le système SAC-OCDMA. Puisque le concept du code est basé sur la corrélation croisée flexible (FCC), on le nomme 'Corrélation Cross Flexible Modifié' (MFCC). Les performances du système OCDMA avec le code proposé MFCC est analysé en tenant compte de l'effet du bruit de grenaille, du bruit PIIN et du bruit thermique. On constate que le code MFCC est le meilleur en termes de BER par rapport aux codes de MDW et RD. Sa simplicité dans la construction de code et la flexibilité dans le contrôle de corrélation croisée a fait ce code un candidat convenable pour les futurssystèmes OCDMA. Deuxièmes, nous étudions la capacité des réseaux quantiques pour soutenir des signaux de données à la fois aléatoire et non aléatoire sur une infrastructure partagée. L'effet de la longueur d'onde sur la couverture de distance avec le taux d'erreur binaire quantique d'un système QKD est analysé. Les résultats de la phase aléatoire ont montré une couverture à distance minimale par rapport à la phase non-aléatoire. Pour la fluctuation d'amplitude de l'émission aléatoire une amélioration dans les performances du système est réalisée. Par conséquent, on constate que les fluctuations rares ne doivent pas dégrader les performances du système de manière significative, mais le mode d'envoi des données a un effet significatif sur l'intégrité du canal.

Mots clés : les systèmes à accès multiples (OCDMA), codes de types 1D et 2D, WDM, réseaux quantiques, système QKD

ملخص

في رُءُ الشرح، تَتَمَّ نَسَاحُ قُيَاخِ وَأَسْ لِيَّةُ فَيُجَالِ تِ الِخِ نَظِيحِ وَتَلَقِي شَرَاكِي فَيُنْشِئُ، قُوتِ طَفِيحَتِ هَفَتِ كُنْجِي الِ تِ الِخِ نَظِيحِ، وَخَا طَحَتِ هَكَ لِي تِ خِي فَيِ أَطْحَ لِنِ جِ لَ تِجْدِيحِ (Optical Code Division Multiplexing Access) (فِي فَسْ لِيَا قِ) مُتَسَا حِ فِي طَحِ زِلِ يَخْتَفِ لِي صِلَ لَ شُوشِ رُ تَشْ زِي رُ الِ دَالِنِ رَا نِ عِ يِقُي حِ لِنِ جِ مَ لِي نِ كِ لَ خِطِ اِخِ الحَرِيحِ تَنِي ذِ اِ عِ 1D وَ 2D يِ رُ لِي صِلِ وَ بِيحِ طُصِ لِي صِلِ كِ اِ يَفِ يِ خِ طُضِ نِ سَا حِ فِي اِ وَ لِنِ جِ رَا كِي لَ كِ مِ طِ تِ قِ اِ WDM نِ لِنِ طِ لَ لَ خِي (بِ تَذِ اِ يِ كِ شِ عِ زَا لِ رَا نِ عِ يِ تَلَقِي شَرَاكِي، وَ يَتِي سَا حِ تِ كِ عِ نِ لَ جِ لَ طُ و حِ فَيِ لِي قِ اِ اِخِيحِ وَ قِي سِرِي لِي صِلِ كِ لَ تِ نِ اِضِي يِ اِ لَ قِ تَشِ ذِ اِ عِ فَيِ ذِ يِ تَلَقِي شَرَاكِي لَ اِ خِ نَظُو SAC-OCDMA. وَ تِ اِ رَا اِ اِخِيحِ مِي تِ فَيِ تِ اِ كِ مِ فِي اِ وَ سِرِي كِ مِ تَقِي شَرَاكِي (Corrélation Cross Flexible) (سِ يِ اِ MFCC) (و يَتِ سَوِي مِ اِ دَا اِ نَظُو OCDMA يِ عِ MFCC لَ دُونِ لِي تَشْ زِي عِ اِ لَ خِ تِ كِ اِ يِ كِ تِ شِ لَ تِ اِ تِ شَرَاكِي لَ كِ اِ عِ تِ لَ شِ طَا صِ، وَ لَ كِ اِ كِ اِ وَا سِرِي شَرَاكِي PIIN لَ كِ اِ كِ اِ. وَ تِ جِ نِ اِ شِ لَ رِي لَ تَلَقِي شَرَاكِي MFCC يِ اِ كِ مِ يِ زِي تِ BER يِقُ سِ حِ MDW. وَ RD اِ تِ قِي نِ اِ تِ اِ وَا شِ و نِ عِ فَيِ تِ سِرِي كِ كِ تِ شَرَاكِي تِ اِ يِ كِ مِ رَا لِي صِلِ قِي شَرَاكِي اِ سِ رِ يِ اِ سِ اِ خِ اِ لَ تِ اِ يِ كِ مِ تِ شَرَاكِي. وَ يِقُ تِ سَوِي مِ لَ طِ لَ لَ اِ خِ تِ اِ يِ كِ مِ يِ سِرِي لَ Xِ نَظِيحِ وَ سِ شِ حِ لَ Xِ طِ اِ لَ رُ قِ اِ يِ رَا كِي هِ هُ ظُو QKD. أَطْحَ شِ خِ اِ حِ لَ شِ زِ حِ كِ شَرَاكِي يِ نِ سِ ذِ اِ دِي يِ لَ سِرِي لَ Xِ نَظِيحِ حِ شِ رَا لِي يِ شِ زِ حِ يِ شَرَاكِي كِ شِ طِ اِ يِ سِرِي كِ اِ لَ كِ اِ تِ اِ Xِ Sِ يِ تِ زِ بِ فَيِ اِ دَا اِ نَظِيحِ تِ اِ اِ نِ تِ اِ زِ نِ كِ، كِ ذِ اِ كِ اِ Xِ نَظِيحِ يِ شِ اِ خِ يِ دِ اِ تِ قِ مِ يِ aِ دَا aِ نَظُو رَا لِي كِ نِ تِ شِ، وَ نِ كِ اِ تِ قِ حِ لَ Sِ aِ لَ Tِ اِ Xِ Tِ اِ Tِ يِ Kِ مِ يِ شِ Kِ مِ aِ لَ Xِ نَظِيحِ.

لِ مِ اِ تِ دَا لِيَّةِ: أَطْحَ لِنِ جِ لَ تِجْدِيحِ، لِي صِلَ لَ شُوشِ، لِي قِ اِ يِ رَا كِي يِ نِ هُ ظُو شِ Kِ اِ Xِ نَظِيحِ يِ شِ لَ طِ لَ لَ Xِ نَظِيحِ

Abstract

In this thesis, we are interested in the study of a new techniques and approaches for optical communications and quantum encryption. In first time, we describe the various optical communications technology particularly that used in multiple access systems (Optical Code Division Multiplexing Access). In the same context, we detailed the different codes proposed in the literature for this type of access technique, including the steps required to generate 2D and 1D code types. The second part is devoted to the study of the concept of generalized quantum walks for WDM applications (Wavelength Division Multiplexing). Starting with the establishment of the state of the art for this type of quantum encryption, and then presents some models studied in the last decades. The third part is divided into two parts. Firstly, we propose a new family code for the SAC-OCDMA system. Since the concept of the code is based on the flexible cross-correlation (FCC), is called the 'Modified Flexible Cross Correlation ' (MFCC). The OCDMA system performance with the proposed code MFCC is analyzed taking into account the effect of shot noise, noise PIIN and thermal noise. It is noted that the MFCC code is the best in terms of BER compared to MDW and RD codes. Its simplicity in the building code and flexibility in the cross-correlation control makes this code a suitable candidate for future OCDMA systems. Secondly, we study the ability of quantum networks to support both random and non-random data signals over a shared infrastructure. The effect of the wavelength on the coverage distance with the quantum bit error rate of a QKD system is analyzed. The results of the random phase showed a minimum distance to cover compared with the non-random phase. For the random emission amplitude fluctuation improvement in system performance is achieved. Therefore, we find that the few changes should not degrade significantly the performance of the system, but the mode of sending the data has a significant effect on the channel integrity.

Keywords: Optical Code Division Multiplexing Access (OCDMA), 2D and 1D code types, MDW, quantum networks, QKD system

Production Scientifique

Articles Publiés dans des Revues Internationales

- 1- Nadhir Djeffal**, Malek Benslama, "Quantum key distribution in WDM router applications for secured data transmission," *Optical and Quantum Electronics*, Vol.48, Issue N°01, Pages 68-76, ISSN:0306-8919, 2016.
- 2- Nadhir Djeffal**, Malek Benslama, Idris Messaoudene, "Generalized Quantum Key Distribution For WDM router Applications," *Review of Computer Engineering Research*. Vol.03, Issue N°01, Pages 7-12/ISSN: 2410-9142, 2016.

Articles Présentés dans des Conférences Internationales

- 1- Nadhir Djeffal**, Malek Benslama, Idris Messaoudene, " Quantum key distribution FOR Wavelength Division Multiplexing," 4th International Scientific conference on Applied Sciences and Engineering ,ISBN: 978-969-9952-20-3, Langkawi, Malaysia, 3-4, October, 2015.

Table des matières

Table des matières	i
Liste des figures	v
Liste des tableaux	x
Introduction Générale	1
<i>Chapitre I : les Communications Quantiques</i>	
I.1 Etat de L'art dans les Communications Quantiques	5
I.1.1 La mécanique quantique comme une théorie des probabilités généralisée	5
I.1.2 Contextualité	7
I.1.3 Indéterminisme et contextualité	7
I.1.4 Contextualité et variables cachées	8
I.1.5 Non localité et Contextualité	9
I.1.6 Etats de Bell	11
I.1.7 Violation de l'inégalité de Legget-Garg	12
I.1.8 Violation de l'inégalité de Bell	13
I.1.9 Paradoxe EPR	14
I.2 Concepts des communications quantiques	17
I.2.1 Limites quantiques	17
I.2.2 Qubits	20
I.2.3 Qudit et Qutrit	24
I.2.3.1 Qudit	24
I.2.3.2 Qutrit	27
I.2.4 Matrices de Pauli	28
2.4.1 Définition	28
I.2.4.2 Propriétés de ces matrices	28
I.2.5 Décohérence	30

Table des matières

I.2.6	Intrication	33
I.3	WDM	35
I.3.1	La Technologie W.D.M	35
I.3.2	Principe de fonctionnement	35
I.3.3	L'utilisation des systèmes WDM	36
I.3.4	Les réseaux DWDM	38
I.4	Algorithmes quantiques	40
I.5	Graphes Quantiques	42
I.6	La cryptographie quantique	43
I.7	Mesure d'un photon polarisé	44
I.8	Principe de la cryptographie quantique	45
I.8.1	Distribution quantique de clef	46
I.8.2	Le protocole BB84	46
I.8.3	Codage sur la polarisation	46
I.8.4	Codage sur la phase	48
I.8.5	Codage sur la polarisation de photons intriqués	50
I.9	Conclusion	51
	Références bibliographiques du chapitre I	52
	<i>Chapitre II Les systèmes optiques à Accès multiple par répartition de code</i>	
II.1	Introduction	56
II.2.1	Multiplexage dans le domaine optique	58
II.2.1.1	Accès Multiple Par Répartition Dans Les Longueurs D'onde(WDMA)	59
II.2.1.2	Accès Multiple Par Répartition Dans Le Temps	60
II.2.1.3	Accès Multiple Par Répartition De Codes Optique (OCDMA)	61
II.2.2	Types De CDMA Optique	64

Table des matières

II.2.2.1	Systèmes OCDMA Cohérent	65
II.2.2.2	Systèmes OCDMA Incohérent	67
II.3	Techniques de Codage OCDMA	72
II.3.1	Codage OCDMA Temporal	72
II.3.2	Réseau OCDMA Spectral en Amplitude	72
II.3.3	Phase spectrale et d'intensité Encodage	73
II.3.4	OCDMA a Saut de Fréquence	73
II.4	Classification Des Systèmes OCDMA	74
II.4.1	Système codage Cohérent Spectral Phase	74
II.4.2	Systèmes OCDMA Incohérent	75
II.5	Les Eléments Du Système OCDMA	77
II.5.1	Sources lumineuses	78
II.5.2	Codeur et décodeur	79
II.5.3	canal optique	80
II.5.4	Photodétecteur	80
II.5.5	optique et Processeur électronique	82
II.6	Principaux défis dans les systèmes OCDMA	82
II.7	Conclusion	83
	Références bibliographiques du chapitre II	84

Chapitre III Implémentation Résultat Numérique Et Discussion

III.1	Introduction	89
III.2	Méthodologie	90
III.3	Résultats et Discussion	92
III.4	Conclusion	98

Table des matières

III.5	Introduction	99
III.6	Concept du code	100
III.6.1	Préliminaires mathématiques	100
III.6.2	Construction de Code	101
III.7	Analyse numérique des performances du code MFCC	103
III.8	Résultats Et Discussions	105
III.9	CONCLUSION	111
	Références bibliographiques du chapitre III	112
	CONCLUSION GENERALE	114

Liste des figures

Figure.I.1.	Connexion entre la théorie quantique et la théorie des probabilités	6
Figure.I.2.	Expérience d'Einstein-Podolsky-Rosen	14
Figure.I.3.	Explication schématique du paradoxe EPR	17
Figure.I.4.	Transition bit classique vers bit quantique	20
Figure.I.5.	Photo d'un Circuit montrant l'introduction des qubits	21
Figure.I.6.	Photo d'un Circuit montrant la réalisation de qubit sur transistor	22
Figure.I.7.	Exemple de circuit capable de porter des qubits	22
Figure.I.8.	Sphère de Bloch et représentation des qubits	23
Figure.I.9.	Evolution de la Sphère de Bloch pour des multi qubits	23
Figure.I.10.	Processus expérimental d'initialisation, d'estimation de phase et de mesure des qubits	24
Figure.I.11-a	Expérimental setup	25
Figure.I.11-b	Représentation des qubits	25
Figure.I.12.	Différentes phases de mesure des qubits	27
Figure.I.13.	Représentation des qubits	28
Figure.I.14.	Comparaison des facteurs de Décohérence	31
Figure.I.15.	Représentation de l'Intrication	34
Figure.I.16.	Dispositif de génération de l'Intrication	35
Figure.I.17.	Principe d'une liaison WDM/DWDM	36
Figure.I.18.	Principe de l'amplificateur optique	36
Figure.I.19.	Combinaisons entre les différentes couches services et transports	37
Figure.I.20-a	transmission	38
Figure.I.20-b	boucle de recirculation	39
Figure.I.20-c	réception	39
Figure.I.21	le routage DWDM	40
Figure.I.22	graphe aléatoire	42
Figure.I.23	graphe aléatoire quantique de cinq nœuds	42
Figure.I.24	Schéma de la téléportation	43
Figure.I.25	Mesure d'un photon polarisé linéairement	45
Figure.I.26	Représentation des 4 états de polarisation	47
Figure.I.27	Valeur des 4 états de phase à l'émission	48
Figure.I.28	Valeurs des déphasages additifs représentant les bases de réception	49
Figure.II.1.	système d'accès multiple; WDMA, TDMA et CDMA	59
Figure.II.2.	Réseaux d'accès multiple par répartition dans les longueurs d'onde (WDMA)	59
Figure.II.3.	Réseaux d'accès multiple par répartition dans le temps (TDMA)	61
Figure.II.4.	ligne à retard basée sur CDMA optique cohérent à séquence direct	65
Figure.II.5.	L'étalement Temporel CDMA Optique	67
Figure.II.6.	Dispositifs Codage / Décodage DS-SS-CDMA	69

Figure.II.7.	la phase a induit d'intensité de bruit du système CDMA Optique	70
Figure.II.8.	Transmetteur Encodage	71
Figure.II.9.	Codage incohérent d'amplitude de spectre des réseaux (SAC)- OCDMA	73
Figure.II.10.	codeur et décodeur a Réseaux de Bragg (FBG).	74
Figure.II.11	système OCDMA de codage cohérente spectrale phase (SPE)	75
Figure.II.12.	Principe de codage d'amplitude spectrale (SAC) OCDMA	76
Figure.II.13.	Système d'étalement temporel Unidimensionnelle (1-D)	76
Figure.II.14.	système de communication OCDMA de deux dimensions (2D)	78
Figure.II.15.	Temps de cohérence de l'impulsion incohérente	79
Figure.II.16.	Temps de cohérence de l'impulsion incohérente	81
Figure.II.17.	Modèle de photo-détecteur	81
Figure.III.1	Schéma de réseau soutenant des canaux QKD et WDM	92
Figure.III.2	La réponse du QBER en fonction de la distance de propagation	93
Figure.III.3	Le débit binaire en fonction de la distance	94
Figure.III.4	Les longueurs d'onde dynamiques avec une augmentation de la couverture de la distance avec diminution de la longueur d'onde	95
Figure.III.5	La fonction $\log_{10}R$ pour le taux de transmission en fonction de la distance	95
Figure.III.6	Variation de BER en fonction du nombre des utilisateurs pour les codes MFCC, MDW and RD.	105
Figure.III.7	Variation de SNR en fonction du nombre des utilisateurs pour les codes MFCC, MDW and RD.	106
Figure.III.8	Variation de BER en fonction du nombre des utilisateurs pour le code MFCC MFCC avec différents débits de transmission de données.	106
Figure.III.9	Variation de BER en fonction de la longueur de fibre pour le code MFCC avec différents débits binaire de données (W=3, K=3)	108
Figure.III.10	Variation de BER en fonction des différents débits binaires de données (W=3, K=3)	109
Figure.III.11	Code MFCC avec différentes longueurs de code par rapport BER	109
Figure.III.12	Variation de BER en fonction du Puissance efficace pour 30 utilisateurs, w=4, w=6, w=8 & w=10	110

Liste des tableaux

Tableau I.1	fidélités moyennes pour qudits de niveau D	25
Tableau I.2	Table de vérité du protocole BB84 (polarisation)	47
Tableau I.3	Table de vérité du protocole BB84 (phase).	49
Tableau I.4	Table de vérité du protocole BB84 (EPR).	50
Tableau II.1	Comparaison de Common Schémas Multiple Access optique	64
Tableau III.1	Description des paramètres	104
Tableau III.2	Paramètres utilisés dans les calculs numériques	107

INTRODUCTION GENERALE

Introduction Générale

Les progrès récemment constatés dans les cristaux photoniques et les nanotechnologies laissent penser que le basculement des communications vers les communications quantiques est imminent. La demande de plus en plus exigeante de largeur de bande et de très haut débit dans les communications numériques a nécessité la recherche de nouveaux systèmes en mesure de répondre à ces exigences. Parallèlement à la recherche purement technologique, et par souci d'adaptation, il était devenu nécessaire de repenser les fondements même du traitement du signal [1-3].

La première réflexion qui est venue à notre esprit, est la suivante : Quelles sont les références pratiques disponibles dans la littérature qui justifient l'intérêt de l'étude des transitions, ainsi que les futurs développements annoncés. Trois domaines distincts seront considérés : les réalisations obtenues dans le traitement du signal, celles obtenues dans les communications numériques, et enfin celles qui ont trait aux communications quantiques. En effet, il nous est apparu impératif de justifier l'intérêt de cette étude sur la base de réalisations pratiques pour montrer au lecteur que ces transitions ne sont pas une vue de l'esprit uniquement, mais une réalité tangible [4-9].

Selon O'Brien et les coauteurs, des éléments de la technologie quantique sont arrivés à maturation et sont disponibles sur le plan commercial tels que les systèmes à distribution de clé quantique. D'autres éléments de la technologie quantique sont en passe de le devenir tels que les réseaux sécurisés à large échelle, la lithographie quantique et les processeurs d'information quantique. La photonique occupera un rôle central dans ces technologies en regard des transmissions à grande vitesse et des propriétés de faible bruit des photons. Nous retenons donc le fait que la technologie des photons quantiques sera une source principale du développement des communications quantiques. Ceci a été prouvé par l'intrication quantique qui a été expérimentalement testée en utilisant des photons générés à partir de cascades atomiques. Les processus non linéaires des conversions paramétriques spontanées ont été une source des paires de photons pour des expériences de génération d'états quantiques d'un faisceau laser brillant, et des états écrasés. La conversion paramétrique a été aussi utilisée pour la téléportation quantique. On peut aussi penser à l'interaction de photons singuliers avec des atomes singuliers dans une cavité optique qui sera une technique majeure pour des technologies quantiques photoniques. [10] Nous traiterons la photonique à partir des cristaux

dans un chapitre spécifique qui mettra en relief leur utilisation pour des routeurs et des démultiplexeurs de longueur d'onde (WDM).

Des dispositifs à gap de bande photonique peuvent être utilisés pour réaliser des WDM. Des sources de lumière sont exigées pour avoir une large accordabilité en longueur d'onde, un faible chirping, et une grande stabilité en température. Ces dispositifs incluent les filtres ultra sélectifs qui sont très utiles pour les WDM denses [11].

L'OCDMA est un domaine de recherche émergent qui offre de nombreux avantages par rapport aux autres techniques d'accès multiple existants tels que TDMA et WDMA. OCDMA fonctionne sur la base d'une transmission asynchrone où la transmission peut être exécutée à tout moment sans aucune coordination nécessaire de synchronisation. La fonction d'OCDMA basée sur une transmission asynchrone où la transmission peut être exécutée à tout moment sans aucune coordination nécessaire de synchronisation. Il a une capacité de rejet d'interférence c'est-à-dire de supprimer l'interférence à bande étroite. Avec l'amélioration de la sécurité de réseau, le signal original de données est élargi dans le domaine fréquentiel sans acquérir la puissance dans le domaine fréquentiel en conséquence la puissance de la densité spectrale est faible et difficile à être détectée. Il offre également la possibilité d'utilisation d'une largeur de bande efficace, la flexibilité des réseaux d'accès à grande vitesse avec un accès bas de latence, la tâche dynamique de largeur de bande, la capacité smart sur demande, la commande de réseau simplifiée et la commande accrue de qualité du service de flexibilité[12].

Plusieurs études relatives à la transposition des techniques CDMA dans les systèmes de communication optiques datent des vingt dernières années. Prenant l'avantage de la grande largeur de bande disponible dans le canal optique, la technique CDMA optique (OCDMA) vise également à accroître la capacité de multiplexage en augmentant le nombre d'utilisateurs au détriment de la détérioration de la qualité de la liaison [13-14]. On peut distinguer deux approches du OCDMA; approche cohérente et incohérente. Dans le système de OCDMA incohérent, l'interférence d'accès multiple (MAI; Multiple Access Interference) est l'une des principales limitations dues à l'utilisation des codes unipolaires. Pour réduire cet effet [15], plusieurs techniques sont proposées pour éliminer la contribution des utilisateurs indésirables. La technique d'accès multiple par répartition de codes dans le domaine spectral (Spectral Amplitude Codage - Optical Code Division Multiple Access, SAC-OCDMA) donne une

meilleure solution pour réduire l'effet des interférences par le code utilisé avec corrélation croisée flexible [16].

Organisation de la thèse:

Cette thèse est divisée en trois chapitres ;

Le premier chapitre présente les communications quantiques, les Concepts des communications quantiques ainsi que la technologie WDM le multiplexage de longueurs d'onde et l'utilisation des systèmes WDM, Algorithmes quantiques et graphes quantiques de plus, on adjoint la cryptographie quantique et le codage de la polarisation de photons intriqués.

Le deuxième chapitre est consacré aux différentes techniques d'accès multiple utilisées en optique qui sont présentées. Le concept de l'accès multiple par répartition de code, l'intérêt de son utilisation et le passage du domaine des radiofréquences en optique sont décrits par la suite. Finalement, une étude bibliographique sur les différentes techniques CDMA optique est donnée. Pour chaque technique, on décrit la source optique utilisée, le composant pour le codage/décodage ainsi que le type de détection.

Enfin, le troisième chapitre est structuré en deux parties. La première partie porte sur L'algorithmique quantique pour les réseaux adaptatifs dans les routeurs WDM, Un système et un procédé pour une distribution quantique de clés sur un réseau (WDM). Dans cette partie, le système fournit un procédé de distribution de clé quantique entre un émetteur et plusieurs récepteurs sur un réseau (WDM) avec le routage de longueurs d'onde. La deuxième partie est consacrée à l'implémentation d'un système OCDMA à séquence directe moins sensible aux perturbations cohérents. Il s'agit de développer un code unipolaires afin d'augmenter la capacité de multiplexage, le débit par utilisateur et l'efficacité spectrale du système OCDMA. Cette étude analyse les performances de système en termes de propriétés de corrélation et les différentes contraintes qui vont influencer le bon fonctionnement de système.

Une conclusion générale et des perspectives ponctuent cette thèse.

Références bibliographiques de l'Introduction Générale

- [1] E.Y. Chou, J.C. Huang, M.S.Hung, et al': Baud rate channelequalization in nanometer technologies. *IEEE Transactions on Very Large Scale Integration (VLSI) systems*, Vol.12, n°11, p.1174-1181, 2004.
- [2] P.Gupta and N.K. Jha: An algorithm for nano-pipelining of RTD Based circuits and architectures. *IEEE Transactions on Nanotechnology*, Vol.4, n°2, p.159-167, 2005.
- [3] C.J. Chang, C.W. Huang, Y.P. Lin, et al': FPGA platform for CPU design and applications. *Proceedings of 2005, 5th IEEE Conference on Nanotechnology*, Nagoya Japan, p.1-4, 2005.
- [4] V. Vankamamidi, M. Ottavi, F. Lombardi: A line based parallel memory for QCA implementation. *IEEE transactions on Nanotechnology*, Vol.4, n°6, p.690-698, 2005
- [5] J.Chen and S.T.C. Wong: Nanotechnology for genomic signal processing in cancer research. *IEEE Signal Processing Magazine*, p.111-121, 2007.
- [6] J.B. Basingthwaighte and H.J. Chizeck: The Physiome Projects and multiscale Modeling. *IEEE Signal Processing magazine*, p.121-124, 2008.
- [7] M. Pierobon and I.F. Akyildiz : A statistical physical model of interference in diffusion based molecular nanonetworks. *IEEE Transactions on Communications*, Vol.62, n°6, p.2085-2095, 2014.
- [8] T. Katayama, T. Mc. Kelvey, A. Sano, et al' : Trends in systems and signals . status report prepared by the IFAC coordinating Committee on Systems and Signal; *Annual reviews in Control*, Vol.30, p.5-17, 2006.
- [9] Hung and Y. Cheng: Cmos nonlinear signal processing circuits. *Advanced in Solid Sate circuits technologies*, edited by P.K. Chu, Intech. 2010.
- [10] J.M. Oberreuter, I. Homrighausen, S.Kehrein: Entanglement propagation and typicality of measurements in the quantum Kac ring. *Annals of physics* 2014.
- [11] J.S. Malhotra, M.Kumar, A.K Sharma: Estimation and mitigation of FWM penalties in dispersion managed 32 channel long haul DWDM soliton link. *Optik*, n°124, p.3029-3032,2013.
- [12] Prucnal, P. R., Santoro, M. A., & Fan, T. R. Spread Spectrum Fiber-Optic Local Area Network Using Optical Processing. *J. Lightwave Technol.*4,547-554.1986.
- [13] Zaccarin, D., &Kavegar, M. (1993). An Optical System Based On Spectral Amplitude Encoding of An LED. *IEEE PhotonicTechnologyLetters*, 4(4), 479-482.
- [14] Zaccarin, D., &Kavehrad, M. New Architecture for Incoherent Optical CDMA to Achieve Bipolar Capacity.*Electronics Letters*, 3(30), 258-259. 1994.
- [15] Anuar, M. S., Aljunid, S. A., Saad, N. M., &Hamzah, S. M.New Design of Spectral Amplitude Coding in OCDMA with Zero Cross-Correlation. *Optics Communications*,282, 2659–2664. 2009.
- [16] Wei, Z., Shalaby, H. M. H. & Shiraz, H. G. (2001). Modified Quadratic Congruence Codes For Fiber Bragg-Grating-Based Spectral-Amplitude Decoding Optical CDMA Systems.*J.Lightw.Technol*, 19, 1274–1281.

CHAPITRE

I

Chapitre I Les communications Quantiques

I.1 Etat de L'art dans les Communications Quantiques

I.1.1 La mécanique quantique comme une théorie des probabilités généralisée

Nous empruntons à Michel Bitbol, une partie de son analyse sur la mécanique quantique examinée en tant que théorie des probabilités. Dans son opuscule, il dit [1].

La thèse que je défendrai ici tient en deux propositions. Premièrement, la mécanique quantique n'est pas qu'une théorie physique faisant usage du calcul des probabilités; elle est elle-même une forme généralisée de calcul des probabilités, doublée d'un procédé d'évaluation probabiliste par l'utilisation réglée de symétries. Deuxièmement, la mécanique quantique n'a pas seulement une fonction prédictive comme les autres théories physiques; elle consiste en une formalisation des conditions de possibilité de n'importe quelle prédiction portant sur des phénomènes dont les circonstances de détection sont aussi des conditions de production.

Commençons par exposer rapidement, dans cet esprit, l'architecture de la mécanique quantique standard:

- Le noyau formel de cette théorie consiste en un espace vectoriel défini sur l'ensemble des nombres complexes, et doté d'un produit scalaire; autrement dit un espace de Hilbert.
- Sur cet espace sont définis des opérateurs spéciaux, appelés «observables», qui fournissent, à travers leurs «valeurs propres», la liste des résultats possibles d'une opération de mesure.
- Un vecteur de l'espace de Hilbert, appelé vecteur d'état, est associé à chaque préparation (c'est-à-dire à ce qui, dans une expérience, fixe les conditions préalables à la mesure).
- En appliquant la règle de Born à ce vecteur d'état, on obtient une fonction assignant des probabilités aux résultats d'une mesure quelconque effectuée à la suite de la préparation.
- Comme un intervalle spatio-temporel variable et diverses circonstances physiques peuvent séparer la fin du fonctionnement de la préparation et l'opération de mesure, on en tient compte à travers une équation d'évolution des vecteurs d'état. Ici, je voudrais

insister sur la différence majeure entre les fonctions de probabilités de la théorie classique des probabilités, et celles qu'on obtient à partir des vecteurs d'état de la mécanique quantique en appliquant la règle de Born. Les fonctions classiques de probabilités associent un nombre compris entre 0 et 1 à chaque «événement» au sens large, défini par Kolmogorov comme un sous-ensemble d'événements élémentaires.

L'ensemble de ces sous-ensembles-événements comprend l'ensemble vide et l'ensemble exhaustif, et il est doté d'une structure d'algèbre de Boole par les opérations de réunion et d'intersection. En d'autres termes, les fonctions classiques de probabilités sont définies sur une algèbre de Boole. Au contraire, compte tenu des propriétés des espaces de Hilbert, les fonctions quantiques de probabilités ne sont pas définies sur une algèbre de Boole; elles sont définies sur des structures différentes et plus riches qu'on appelle des «orthoalgèbres».

Cette disparité structurale entre fonctions classiques et fonctions quantiques de probabilités justifie qu'on ne se contente pas de considérer que la mécanique quantique utilise la théorie des probabilités. La mécanique quantique consiste elle-même, pour une part, en une forme nouvelle et élargie de théorie des probabilités [2].

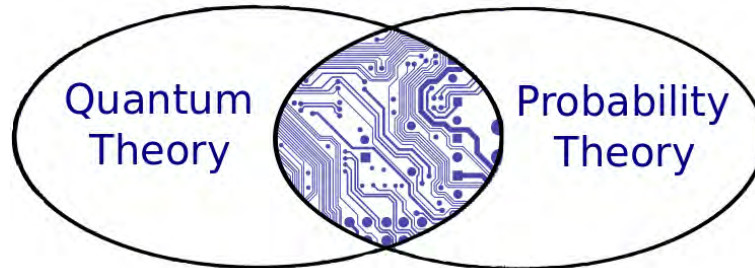


Figure.I.1 Connexion entre la théorie quantique et la théorie des probabilités.

Les références suivantes postulent pour la même vision [3-6].

Partant de cette analyse, il nous semble important d'examiner les communications quantiques à travers le socle des probabilités et des concepts afférents à cette théorie : la covariance, la corrélation [7] l'inférence, les processus aléatoires, tout en incluant certaines spécificités à la mécanique quantique : la contextualité [8], la non localité [9], les paradoxes tels que le Chat de Schrödinger, le paradoxe Einstein, Podolsky et Rosen, les inégalités de Bell [10-11], la décohérence [12]. Par la suite, il s'agit d'effectuer une synthèse entre les partisans du déterminisme et du tout aléatoire.

La mécanique quantique standard viole indéniablement la notion de séparabilité que la physique classique nous a habituée à considérer comme valide. En rapportant le phénomène de non séparabilité quantique au concept tout important de potentialité, nous fournissons efficacement une image cohérente des corrélations entre les systèmes intriqués énigmatiques spatialement séparés. Nous soutenons en outre que le phénomène généralisé de non séparabilité quantique implique la contextualité ce qui entraîne à son tour une conception relationnelle structurale des objets quantiques, considérés comme porteurs de propriétés de dispositions [13].

I.1.2 Contextualité

Les ordinateurs quantiques promettent des avantages énormes sur leurs homologues classiques, mais la source de la puissance dans l'informatique quantique est restée inaccessible. Ici, nous montrons une équivalence remarquable entre l'apparition de la contextualité et la possibilité de calcul quantique universel via l'état magique que nous appelons distillation, qui est le principal modèle pour réaliser expérimentalement un ordinateur quantique à tolérance de pannes. En outre, cette connexion suggère un paradigme unificateur pour les ressources de l'information quantique: la non-localité de la théorie quantique est un type particulier de contextualité, et la non-localité est déjà connue pour être une ressource essentielle pour la réalisation des avantages de la communication quantique. En plus de clarifier ces questions fondamentales, ce travail avance le cadre des ressources pour le calcul quantique, qui a un certain nombre d'applications pratiques, telles que la caractérisation de l'efficacité et de compromis entre les schémas théoriques et expérimentales distinctes pour atteindre un calcul quantique robuste, et de mettre des limites pour la simulation classique des algorithmes quantiques [14].

I.1.3 Indéterminisme et contextualité

Ces deux remarques historiques, l'une sur l'association du concept de probabilité au concept de qualité secondaire, et l'autre sur le calcul des probabilités conçu comme instrument de maîtrise prédictive de notre situation d'enchevêtrement dans le réseau des relations naturelles, vont à présent nous aider à défaire deux nœuds interprétatifs de la physique quantique, se rapportant l'un comme l'autre à l'indéterminisme.

Le premier concerne la notion, très répandue depuis les travaux fondateurs de Heisenberg aux alentours de 1927-1930, d'une perturbation incontrôlable qu'est censée

exercer l'agent de mesure sur l'objet microscopique mesuré. Il est intéressant de noter que cette «perturbation» s'est vue assigner un double rôle par ses concepteurs. D'une part, souligne Bohr à la fin des années 1920, la perturbation incontrôlable constitue la raison de l'indivisibilité du phénomène quantique, c'est-à-dire de l'impossibilité de séparer dans le phénomène ce qui revient à l'objet et ce qui revient à l'agent de mesure. La perturbation expliquerait en d'autres termes, empruntés cette fois à Heisenberg, que la physique quantique conduise à généraliser le modèle des qualités secondaires, avec leur référence obligée au contexte dans lequel elles se manifestent, au détriment de celui des qualités primaires intrinsèques.

Mais d'autre part, selon l'article de 1927 où Heisenberg présente pour la première fois ses relations dites d'«incertitude» [15], la perturbation est aussi ce qui rend compte de l'indéterminisme de la physique quantique. La perturbation incompressible et incontrôlable par l'agent de mesure est ce qui empêche de connaître complètement les deux groupes de variables qui composent l'état initial d'une particule; et par conséquent, conclut Heisenberg, le principe de causalité, qui lie de façon contraignante un état initial et un état final, reste inapplicable en physique quantique. Le modèle de la «perturbation» permet ainsi de mettre en évidence une étroite relation entre contextualité et indéterminisme, puisque la perturbation a pour conséquence aussi bien la contextualité des phénomènes que l'indéterminisme à leur sujet. Plus tard, au début des années 1950, Paulette

Destouches-Février démontra de façon beaucoup plus rigoureuse un théorème selon lequel toute théorie prédictive portant sur des phénomènes définis relativement à des contextes expérimentaux dont certains sont mutuellement incompatibles, est «essentiellement indéterministe» [16].

I.1.4 Contextualité et variables cachées

La question de savoir si des phénomènes quantiques peuvent être expliqués par les modèles classiques avec des variables cachées est l'objet d'un débat d'une longue durée. En 1964, Bell a montré que certains types de modèles classiques ne peuvent pas expliquer les prédictions de la mécanique quantique pour les états spécifiques de particules lointains et certains types de modèles à variable cachée, ont été expérimentalement exclues. Une caractéristique intuitive des modèles classiques est non-contextualité: la propriété que toute mesure a une valeur indépendante des autres mesures compatibles étant effectuée en même temps.

Cependant, un théorème tiré par Kochen, Specker et Bell montre que la non-contextualité est en conflit avec la mécanique quantique. Le conflit réside dans la structure de la théorie qui est indépendante des propriétés des états spéciaux. On a discuté le fait de savoir si le théorème Kochen-Specker pourrait être testé expérimentalement. Les premiers tests de la contextualité quantique ont été proposés récemment, et entrepris avec des photons et neutrons. Ici, nous effectuons une expérience avec des ions piégés qui démontre un conflit d'indépendance de l'état avec la non-contextualité [17].

I.1.5 Non localité et Contextualité

Nous utilisons le langage mathématique de la théorie des faisceaux pour donner un traitement unifié de la non localité et contextualité, dans un cadre qui généralise les tables de probabilités familières utilisées dans la théorie de la non localité pour des mesures arbitraires : ceci inclut les configurations Kochen-Specker. Nous montrons que la contextualité et la non-localité comme un cas particulier, correspondent exactement aux obstacles à l'existence de sections globales. Nous décrivons une approche algébrique linéaire pour le calcul de ces obstacles, qui permet un traitement systématique de la non localité et contextualité.

On distingue une hiérarchie adéquate des forces de théorèmes de no-go, et nous montrons que les trois principaux exemples dus à Bell, Hardy et Greenberger, Horne et Zeilinger, occupent respectivement les niveaux plus élevés de cette hiérarchie. Une correspondance générale est représentée entre l'existence de réalisations variables locales cachées en utilisant des probabilités négatives, et le *no signalling*; ceci est axé sur un résultat montrant que les sous-espaces linéaires générés par le non contextuel et les modèles de *no signalling*.

Le non localité maximale est généralisé à la contextualité maximale, elle est caractérisée en termes purement qualitatifs, avec les résultats de Kochen-Specker, comme génériques. Ces modèles sont des preuves indépendantes de la contextualité maximal, et un état combinatoire nouveau est donné, il généralise les *preuves de parité* abondamment commentées dans la littérature. Ce qui montre que la mécanique quantique obéit à des familles de *no signalling* d'observables commutant qui sont représentés comme un produit tensoriel de différents facteurs [18].

La contextualité quantique est l'une des notions fondamentales en mécanique quantique. Il a été constaté, que certaines preuves du théorème Kochen-Specker, telles que

celles basées sur les rayons, peuvent être converties en une inégalité de contextualité non indépendante de l'état. Cette problématique reste ouverte, à savoir, si une preuve du théorème de Kochen-Specker peut toujours être convertie en une inégalité de non contextualité. Dans l'article de Yu, une réponse est faite à cette question.

L'auteur montre que toutes sortes de preuves du théorème Kochen-Specker, basées sur les rayons, ou tout autre observable, peuvent toujours être converties en des inégalités indépendantes de non contextualité. En outre, une preuve constructive fournit également une approche générale pour déterminer une inégalité indépendante de la non contextualité de l'état à partir d'une démonstration du théorème Kochen-Specker[19].

L'inégalité de Bell (pour l'espace), Kochen-Specker (pour la contextualité) ou Leggett-Garg (pour le temporel), ces inégalités sont basées sur des hypothèses classiques plausibles mais tout à fait distinctes. Pour chacune de ces inégalités, la réalisation est équivalente à une distribution de probabilité conjointe pour tous les observables dans l'expérience. Cela implique une distribution conjointe pour toutes les paires d'observables, et ceci reste indifférent de savoir s'ils commutent ou non Cette indifférence est à la base d'une unification des inégalités ci-dessus dans un cadre général des inégalités de corrélation.

Lorsque le scénario physique est tel que les paires corrélées sont tous compatibles, la corrélation résultante est du type 'no signalling' elle peut être locale ou à particules multiples, correspondant à la contextualité ou aux inégalités de Bell. Si les paires sont incompatibles, la corrélation résultante correspond aux inégalités de Leggett-Garg. Si la mécanique quantique viole toutes ces inégalités, cela suggère un lien étroit entre les propriétés locales, spatiales et temporelles de la théorie [20].

Winterdonne un test expérimental du théorème de Bell-Kochen-Specker suivant les démonstrations de Meyer, Kent et Clifton qui assure que les prédictions de la mécanique quantique sont indistinguables du modèle non contextuel.

En physique théorique, un théorème no-go est un théorème qui affirme qu'une certaine situation n'est pas physiquement possible. Plus spécifiquement, ce terme décrit des résultats de mécanique quantique comme le théorème de Bell et le théorème de Kochen-Specker qui contraignent les types de variables cachées admissibles qui tentent d'expliquer l'aléatoire apparent de la mécanique quantique comme étant un déterminisme impliquant des états cachés.

En théorie de l'information quantique, le théorème de non-communication est un résultat qui donne les conditions sous lesquelles le transfert instantané d'information entre deux observateurs est impossible.

Araddonne un théorème no go pour les PCP (probabilistically checkable proof), ou preuve de façon probabiliste.

I.1.6 Etats de Bell

Eli Maor dans son article précise le principe d'incertitude d'Heisenberg[23].

Plus insaisissable de tous était le principe d'incertitude de Heisenberg, salué comme peut-être le principe le plus important de la physique moderne. Vous ne pouvez pas déterminer simultanément la position et la dynamique (à savoir la vitesse) d'une particule avec une certitude absolue. Toute augmentation du déterminisme de l'un de ces quantités se fait au détriment du principe d'incertitude d'autres. Ce procédé est immédiatement devenu l'un des fondements de la physique quantique. Son influence sur la façon dont les scientifiques pensent du monde est devenu si prévisible. Dans ce qui allait bientôt au-delà de la physique est devenu une partie de notre langage quotidien.

Au cours des dernières décennies, des progrès théorique et expérimentale substantiels ont été réalisés dans la compréhension de la nature quantique des phénomènes physiques qui sert de base de technologies actuelles et futures. Les corrélations quantiques comme l'intrication des états de systèmes composites, le phénomène de la discordance quantique, qui capte d'autres aspects de corrélations quantiques, la contextualité quantique et, relié à ces phénomènes, les relations d'incertitude pour les variables et entropies conjugués, comme les entropies de Shannon et Rényi, et les inégalités pour les états de spin, comme les inégalités de Bell, reflètent les propriétés quantiques de micro et macro-systèmes. Les méthodes mathématiques nécessaires pour décrire tous les phénomènes quantiques mentionnés ci-dessus ont également fait l'objet d'études intenses à la fin du siècle dernier, et au début du nouveau siècle.

L'autre nouvelle direction dans l'élaboration de l'approche mathématique de la physique quantique est la tomographie qui offre une nouvelle vision d'états quantiques. Dans l'image tomographique de la mécanique quantique, les états sont identifiés avec des distributions de probabilités conditionnelles équitables, qui contiennent les mêmes

informations sur les états que la fonction d'onde ou de la matrice de densité. Les méthodes mathématiques de l'approche tomographique sont basées sur l'étude du produit étoile (produit associative) du schéma de quantification. Le produit tomographique étoile fournit une compréhension supplémentaire du produit associé, qui est liée à l'existence de paires spécifiques des opérateurs appelés quantificateurs et de déquantificateurs [24].

I.1.7 Violation de l'inégalité de Legget-Garg

En mesurant faiblement la polarisation d'un photon entre deux mesures de polarisations fortes, l'auteur étudie expérimentalement la corrélation entre l'apparence des valeurs anormales en mesure faible quantique [25]. Une formulation quantitative de ce dernier concept est exprimée en termes d'une inégalité L.G (Leggett-Garg) pour les résultats des mesures ultérieures d'un système quantique individuel. Nous violons expérimentalement l'inégalité Leggett-Garg sur plusieurs mesures. En outre, nous démontrons expérimentalement qu'il existe une corrélation entre une réalisation de faibles valeurs étranges et de violer l'inégalité Leggett-Garg[25].

Assano et les coauteurs interprètent l'inégalité Leggett-Garg comme une inégalité probabilistique contextuelle dans laquelle on combine les données collectées dans les expériences dans 3 contextes différents.

Dans la version originelle de cette inégalité, les contextes ont une nature temporelle, ils sont représentés par 3 paires (t_1, t_2) , (t_2, t_3) , (t_3, t_4) avec $t_1 < t_2 < t_3 < t_4$. Ils généralisent les conditions de Leggett-Garg du réalisme macroscopique et de mesurabilité non invasive dans un cadre contextuel général. Leur formulation est développée en termes purement probabilistiques, l'existence d'un contexte indépendant d'une distribution de probabilité (bidimensionnelle) et la possibilité de reconstruction de distributions de probabilités marginales à partir de P . Ils déterminent une inégalité analogue à L-G qu'ils appellent inégalité L-G contextuelle, et ils utilisent comme test de quantité des données statistiques collectées dans une série d'expérience de la reconnaissance de figures ambiguës.

Dans leur étude expérimentale, la figure sous reconnaissance est un escalier de Schrödinger qui est montrée avec des rotations de différents angles, les contextes sont codés par des rotations dynamiques dans trois sens : le sens de rotation d'une montre, le sens contraire, et un sens aléatoire. Les données démontrent une violation de l'inégalité de L-G contextuelle pour les combinaisons de contextes sus mentionnés [26].

I.1.8 Violation de l'inégalité de Bell

Les corrélations non-locales entre les systèmes séparés spatialement ont été largement discutées dans le contexte du paradoxe d'Einstein, Podolsky et Rosen (EPR) et les inégalités de Bell. Beaucoup de propositions et expériences destinées à tester les théories variables cachées et la violation des inégalités de Bell ont été signalées, habituellement ces photons consistent en corrélation, bien que récemment une expérience a été réalisée avec des Be^+ (ions de Beryllium). Néanmoins, il est d'un intérêt considérable pour montrer que ces corrélations (résultant de l'intrication quantique) ne sont pas simplement une particularité de photons. Ici, nous mesurons les corrélations entre les deux degrés de liberté (comprenant des composantes spatiales et de spin) de neutrons simples; cela supprime la nécessité d'une source de neutrons de paires enchevêtrées, qui présentent un défi technique considérable.

Une inégalité équivalente de Bell est introduite pour clarifier les corrélations qui peuvent survenir entre observables de degrés de liberté indépendants. Nous démontrons la violation de cette inégalité de Bell comme: notre valeur mesurée est $2.051 \pm 0,019$, nettement supérieur à la valeur de 2 prédite par des théories classique des variables cachées [26].

Les situations expérimentales où l'on observe les effets quantiques, posent une question fondamentale à prendre en considération : c'est la compatibilité entre la description des phénomènes et l'hypothèse d'une réalité objective. Ce document traite de l'interprétation ontologique de Bohm en mécanique quantique, en se concentrant sur l'utilisation du terme «trajectoire» et les difficultés associées à sa connexion à une trajectoire réelle (objective). La conclusion est que l'interprétation réaliste destinée des trajectoires Bohm est très discutable [27].

Bohm donne une interprétation de la théorie quantique en termes de variables cachées [28]. Un autre article aussi intéressant sur la signification des potentiels électromagnétiques dans la théorie quantique est donné par Aharonov et Bohm. Dans cet article, les auteurs discutent quelques propriétés intéressantes des potentiels électromagnétiques dans le domaine quantique [29].

I.1.9 Paradoxe EPR

C'est un article majeur connu comme le paradoxe EPR. Les auteurs stipulent que dans une théorie complétée, il y a un élément correspondant à chaque élément de la réalité. Une condition suffisante pour la réalité d'une quantité physique est la possibilité de prédiction avec une certitude sans perturber le système. Dans la mécanique quantique pour le cas de deux quantités physiques décrites par des opérateurs non commutant, la connaissance de l'un prélude à la connaissance de l'autre. Donc, ou bien la description de la réalité donnée par la fonction d'onde en mécanique quantique n'est pas complétée ou ces deux quantités ne peuvent avoir simultanément de réalité [30]. Une expérience montrant le paradoxe EPR a été réalisée par Birgit Dopfer, elle est reportée sur la figure.I.2.

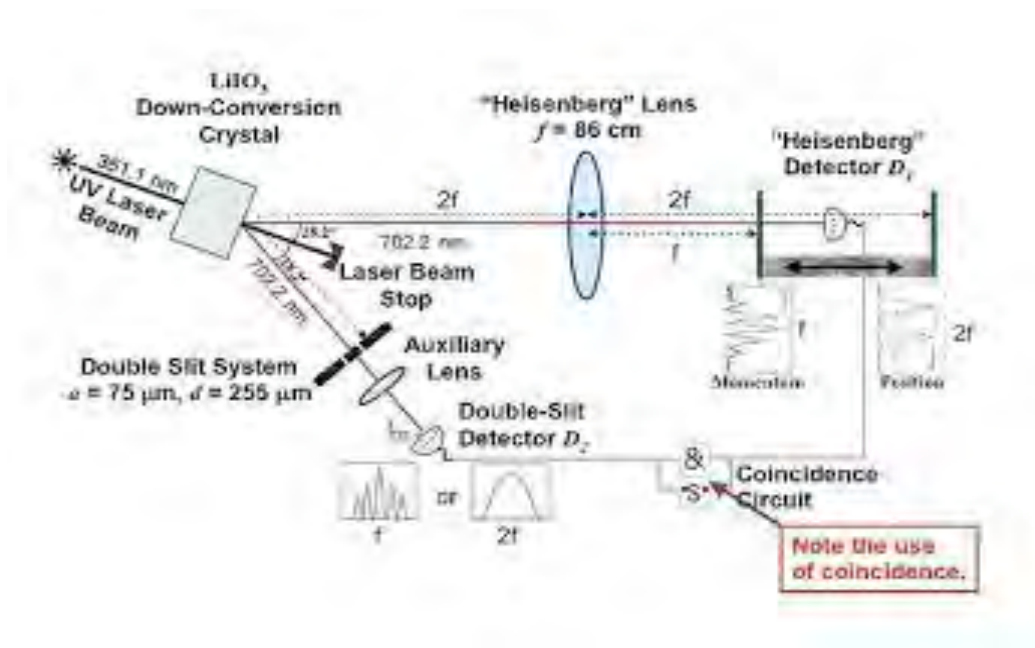


Figure.I.2 Expérience d'Einstein-Podolsky-Rosen d'après [31]

Le paradoxe EPR, abréviation de Einstein-Podolsky-Rosen, est une expérience de pensée, élaborée par Albert Einstein, Boris Podolsky et Nathan Rosen, dont le but premier était de réfuter l'interprétation de Copenhague de la physique quantique. L'interprétation de Copenhague s'oppose à l'existence d'un quelconque état d'un système quantique avant toute mesure. En effet, il n'existe pas de preuve que cet état existe avant son observation et le supposer amène à certaines contradictions.

Or, si deux particules sont émises et qu'une relation de conservation existe entre une de leurs propriétés (par exemple, la somme de leurs spins doit être nulle, c'est-à-dire qu'il y a intrication quantique de l'état du système de ces deux particules), la connaissance de l'état de

la première après une mesure effectuée sur celle-ci nous informe de l'état dans lequel se trouve la seconde particule avant une mesure effectuée sur celle-là plus tard, alors que - selon l'interprétation de Copenhague - la valeur mesurée est déterminée aléatoirement au moment de la mesure. Si la mesure sur la première particule a donné « + », et que la première particule se trouve donc dorénavant dans l'état « + », la mesure sur la seconde donnera toujours « - ».

Un des problèmes est que cette dernière particule peut, à l'instant de la mesure, se trouver à une distance aussi grande qu'on le veut dans l'univers observable de la première. La ligne d'univers qui relie les deux événements « mesure sur la particule 1 » et « mesure sur la particule 2 » de l'espace-temps peut même être une courbe de genre espace, et la seconde particule ne peut donc absolument pas, dans ce dernier cas, « être informée » de quelque façon que ce soit de l'état dans lequel se trouvait la première après la mesure. Comment croire, dans ces conditions, que l'état dans lequel on trouve la seconde particule après la mesure n'était pas déterminé dès le départ, en contradiction avec la représentation de Copenhague ?

Ce paradoxe fut élaboré par Albert Einstein et deux de ses collaborateurs Boris Podolsky et Nathan Rosen pour soulever ce qui semblait apparaître comme une contradiction dans la mécanique quantique, ou du moins une contradiction avec au moins l'une des trois hypothèses suivantes :

- ✓ impossibilité pour un signal de dépasser la vitesse c (causalité relativiste) ;
- ✓ la mécanique quantique est complète et décrit entièrement la réalité (pas de variable cachée locale) ;
- ✓ les deux particules éloignées forment deux entités pouvant être considérées indépendamment l'une de l'autre, chacune étant localisée dans l'espace-temps (localité).

L'argument EPR, tel que présenté en 1935, est fondé sur le raisonnement suivant.

Tout d'abord il faut rappeler que le principe d'incertitude interdit de connaître simultanément la valeur précise de deux quantités physiques dites incompatibles (typiquement, la vitesse et la position d'une particule). Plus on mesure avec précision une quantité, plus la mesure de l'autre est indéterminée.

En conséquence de ce principe, EPR en déduit deux affirmations mutuellement exclusives :

- ✓ La description de la réalité donnée par la mécanique quantique n'est pas complète.
- ✓ Les deux quantités physiques incompatibles n'ont pas simultanément une réalité objective.

L'interprétation de Copenhague arrive à la conclusion que 2) est vrai et 1) est faux, alors que EPR entendent démontrer que 1) est vrai et 2) est faux.

Pour cela, ils mettent au point une expérience de pensée qui mène à la détermination simultanée de deux quantités physiques non commutables, et donc à la conclusion que 2) est faux et par conséquent (les deux affirmations étant mutuellement exclusives) que 1) est vrai.

Pour démontrer que 2) est faux, il est indispensable de définir précisément ce qu'est la notion de « réalité » d'une quantité physique (par exemple la « position »). EPR mettent en évidence une condition suffisante de « réalité » :

Si, sans perturber en aucune manière l'état d'un système, on peut prédire avec certitude (avec une probabilité égale à 1) la valeur d'une quantité physique de ce système, alors il existe un élément de réalité correspondant à cette quantité physique.

Le « dispositif expérimental » (de pensée) proposé en 1935 est assez complexe, mais peut être décrit de manière plus simple sans en changer l'esprit, voir la Figure.I.3.

Soient deux photons P_1 et P_2 intriqués de manière à avoir un moment angulaire total égal à zéro (spins anti-corrélés). Les deux quantités physiques non commutables utilisées dans le raisonnement sont : 1) Le spin mesuré selon une direction S_x 2) Le spin mesuré selon une autre direction S_z . Si on mesure P_1 selon S_x , alors - sans perturber P_2 (on suppose le principe de localité) on connaît nécessairement la mesure de P_2 selon cet axe (l'opposé).

De même, si on mesure P_2 selon S_z , alors - sans perturber P_1 , on connaît nécessairement la mesure de P_1 selon cet axe (l'opposé également). Donc, la mesure de P_1 selon un axe et de P_2 selon l'autre permet de prédire avec certitude la valeur des deux quantités physiques. Ces deux quantités possèdent donc une réalité objective, et par conséquent 2) est faux et 1) est vrai. Tel est le paradoxe formulé initialement par EPR.

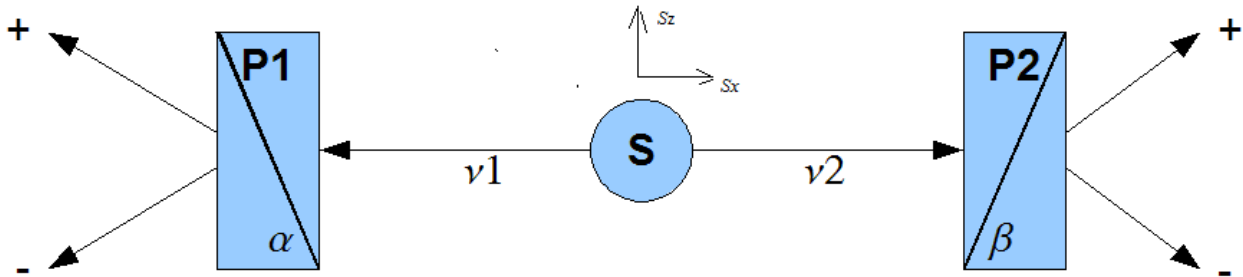


Figure.I.3 Explication schématique du paradoxe EPR.

I.2 Concepts des communications quantiques

I.2.1 Limites quantiques

Des applications de la cohérence quantique et de la corrélation quantique en optique ont été discutées par [12]. Les états cohérents représentent un outil idéal pour traiter la limite entre les propriétés classiques et quantiques ; on montre en utilisant les états cohérents que l'on peut trouver des solutions analytiques à des problèmes quantiques non linéaires précédemment insolubles.

L'optique quantique a générée de nouvelles applications qui utilisent les possibilités des états quantiques de la lumière telles que la cohérence et la corrélation quantique. Cette dernière est connue comme l'intrication. On montre comment on peut obtenir des images de faible intensité d'objets avec une sensibilité qui dépasse les limites quantiques standards. Les auteurs montrent aussi que les bi photons qui sont créés dans des processus de décroissance paramétrique exhibent un phénomène de corrélation spatiotemporel qui est appelé Intrication.

Des applications basées sur l'impossibilité du clonage d'états quantiques inconnus sont uniques, elles ont été développées dans le champ de la cryptographie quantique. Une expérience EPR avec des photons intriqués et polarisés est développée pour tester le modèle d'Eberhard. En accord avec celui-ci, les corrélations quantiques entre des événements séparés spatialement sont dues à une propagation d'un signal en communication super lumineuse dans un cadre choisi.

Les coïncidences entre les photons intriqués passent à travers deux polariseurs alignés le long d'un axe est-ouest sont mesurées comme une fonction du temps durant 21 jours sidéraux. A partir de cette prédiction de la théorie quantique aucune déviation n'est observée. Tenant compte des incertitudes expérimentales, nous inférons que si un cadre choisi pour des

signaux super lumineux existe, alors celui-ci se meut à une vitesse v en fonction de la terre. Le module de la vitesse des communications quantiques dans ce cadre est plus grand que $v_f \approx 0,6 \cdot 10^4 c$ pour $v < 0,1 c$ pour toute direction arbitraire de v . Une limite basse de la vitesse des communications quantiques a été relevée par [32]. Un autre aspect dans la détermination des limites a été observé avec le fameux facteur g dans les communications quantiques pour des semi-conducteurs [33].

Une réalisation pratique de communications quantique est attendue pour exiger la préservation de l'intrication dans des photodétectrices, dans lesquels l'information quantique est transmise par la polarisation d'un photon à travers une fibre optique et son transfert au spin d'un électron dans un semi-conducteur. Pour maintenir l'intrication, le photodétecteur doit absorber équitablement les 2 états du spin de l'électron, et ainsi le facteur g de l'électron doit être fabriqué pour $g_e \approx 0$. La structure de bande de la masse effective peut également bien contrôler le facteur g .

Transfert de l'information quantique dans un résonateur couplé avec un guide d'onde [33]. Nous proposons un schéma efficace pour l'implémentation de l'information quantique dans un résonateur unidimensionnel couplé avec un guide d'onde. Nous montrons que sur la base d'interaction dipôle-dipôle entre les atomes reliés aux modes de cavité, des transitions de Raman entre les atomes piégés dans les différents nœuds peuvent avoir lieu.

L'information quantique peut être transférée directement entre les côtés opposés du guide couplé sans l'introduction de nœuds intermédiaires via les transitions de Raman ou de passages adiabatiques de Raman stimulé. Ainsi ce schéma est en principe, une étape de protocole qui peut mener à des applications utiles en communications quantiques. Récepteurs à grande performance pour les communications optiques [35].

Les principes de la détection optique sont revus, et la réalisation pratique de dispositifs et de récepteurs pour des communications optiques numériques sont discutés. L'accentuation est placée sur les techniques de traitement de signal pour des récepteurs électroniques et optoélectroniques avancés. Ils sont en train de fournir des performances approchant les limites fondamentales imposées par des considérations de mécanique quantique.

Processus de détection directe

La détection directe peut être vue comme une simple cartographie des photons aux électrons de conduction. Soit P , le niveau de la puissance optique incidente et ν la fréquence optique reliée à la longueur d'onde en espace libre λ par $c = \nu\lambda$ où c est la vitesse de la lumière dans le vide. Si h est la constante de Planck, alors l'énergie par photon est $h\nu = hc/\lambda$ et le taux d'arrivée des photons est donné par :

$$\frac{P}{h\nu} = \frac{P\lambda}{hc} \quad (\text{I.1})$$

Chaque photon détecté, produit juste un porteur électrique extérieur, mais tous les photons ne sont pas détectés. Le taux de génération de porteur est donc plus bas que le taux d'arrivée des photons comme déterminé par la probabilité de détection connue comme l'efficacité quantique η . Le taux de génération de porteurs est donc :

$$\eta \cdot \frac{P\lambda}{hc} \quad (\text{I.2})$$

Chaque porteur électrique transporte une unité de charge électronique de q coulombs et le taux significatif de flux de charge est le photocourant I qui est donné par

$$I = \eta \cdot \frac{q\lambda}{hc} P \quad (\text{I.3})$$

Le rapport I/P en A/W est connu comme la réponse de R du détecteur. Puisque $\eta \leq 1$, la réponse est limitée supérieurement par :

$$R \leq \frac{q\lambda}{hc} \quad (\text{I.4})$$

qui est proportionnelle à la longueur d'onde.

Cette dernière caractéristique reflète simplement le fait que les grandes longueurs d'ondes correspondent aux fréquences optiques basses, que l'énergie par photon est moindre, et nous avons donc un taux de photons grand pour un niveau de puissance optique donné. Les systèmes actuels de fibre optiques opèrent dans un intervalle de longueur d'onde allant de 850 nm à 1550 nm, et les détecteurs actuels peuvent avoir des efficacités quantiques approchant l'unité. Comme conséquence, les réponses dans la région de 0.5 à 1.0 A/W sont typiques, elles dépendent de la longueur d'onde utilisée. .

I.2.2 Qubits

Un bit est un objet mathématique qui permet de décrire l'état d'un système physique classique. A un instant donné, il prend pour valeur 0 ou 1. Le bit quantique, appelé qubit, décrit l'état d'un système quantique. Il peut prendre la valeur 0 et 1 comme un bit classique, mais aussi toutes les valeurs intermédiaires, combinaison linéaire des états 0 et 1. La notation de Dirac comportant des bra et des ket est utilisée. La Figure.I.4, explique le passage de la vision classique à la vision quantique. Les principaux travaux relatifs à ce thème sont reportés sur les références suivantes [34-37].

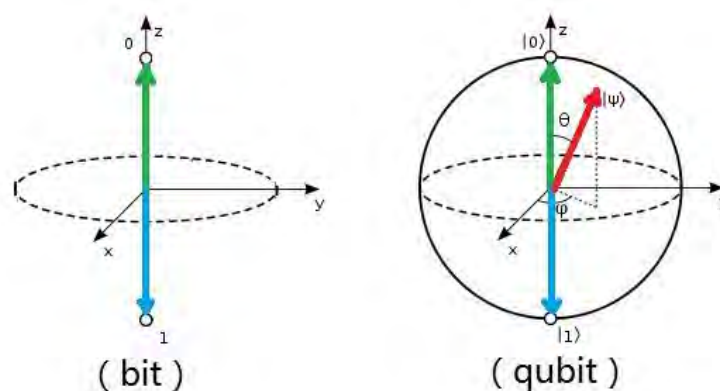


Figure.I.4 Transition bit classique vers bit quantique

Les qubits sont des vecteurs d'un espace (de Hilbert) dont la dimension 2^n croît avec leur nombre n , une grande nouveauté par rapport à l'espace classique. Ils exploitent des propriétés ondulatoires (ce qui n'est pas le cas des bits), d'intrication et de non-localité (phénomène inconnu de la physique classique). Par contre, ils sont extrêmement fragiles, étant couplés à l'environnement classique par un processus dit de décohérence. On attribue à Richard Feynman l'idée du calcul quantique pour simuler les phénomènes physiques, mais la véritable impulsion est donnée en 1994 lorsque Peter Shor démontre la possibilité de factoriser les grands nombres en temps polynomial.

Nous allons commencer par illustrer comment les théories des groupes finis et les groupes de Lie sont utiles pour comprendre l'interface classique /quantique.

Le bit classique, prend deux valeurs « 0 » ou « 1 ». Le bit quantique ou qubit, peut aussi se trouver dans deux états « 0 » ou « 1 », mais qui sont maintenant les états d'un système quantique. Pour les distinguer des états classiques, on va les noter $|0\rangle$ et $|1\rangle$

Les calculateurs sont obtenus en combinant certaines portes logiques élémentaires. Pour contourner le problème de la décohérence, on utilise le silicium, Les qubits peuvent être portés par des photons [38] ou des électrons. Nous donnons sur la Figure.I.5, une photo représentant un circuit avec l'introduction des qubits.

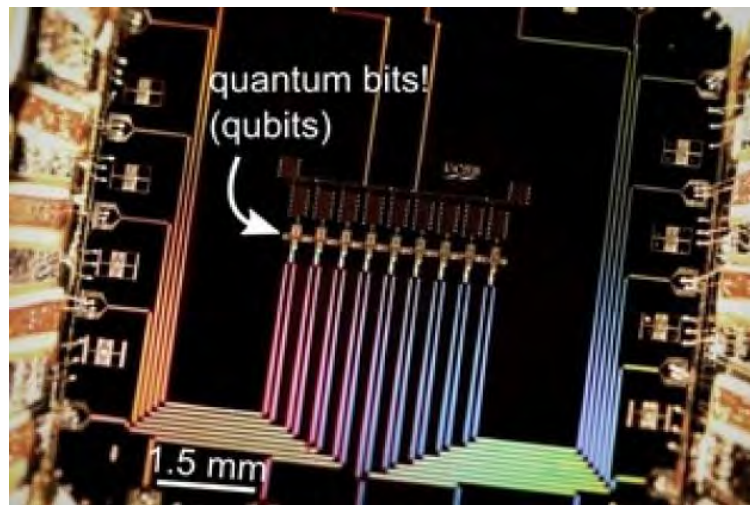


Figure.I.5 Photo d'un Circuit montrant l'introduction des qubits.

Dans certains circuits avec des qubits solides à base de semi conducteur, les physiciens rencontraient des problèmes car la présence de noyaux doués de spin perturbait les qubits portés par les électrons, mais dans le cas de l'isotope 28 du silicium, ce problème n'existe pas, car le spin du noyau de cet élément est nul. En plaçant des électrodes sur un morceau de silicium 28, les chercheurs sont parvenus à manipuler les spins des paires d'électrons piégés dans ce matériau [39]. Plus précisément, ils ont utilisé une technique connue sous le nom de résonance de spin électronique (ESR). Ils ont pu montrer que les manipulations de qubits qu'ils étaient en mesure de faire reproduisaient le traitement de l'information que l'on attendait d'une porte quantique CNot. Il s'agit d'une première avec du silicium et le résultat est encourageant.

La Figure.I.6 suivante montre cette réalisation.

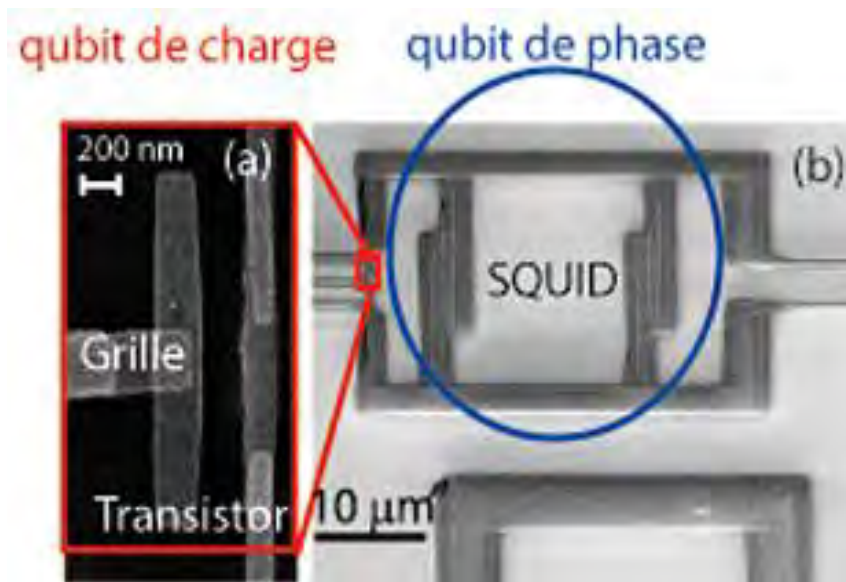


Figure.I.6 Photo d'un Circuit montrant la réalisation de qubit sur transistor.

En effet, pour qu'une telle porte CNot soit réellement utilisable, les qubits des paires d'électrons doivent être intriqués. Les chercheurs n'ont pas encore réussi à montrer que c'est le cas. S'ils parviennent, les physiciens disposeraient alors, en principe, avec cette porte et d'autres éléments, de tout ce qu'il faut pour construire une vraie puce d'ordinateur quantique en silicium pouvant contenir des millions de qubits La Figure.I.7 suivante montre cette réalisation[40].

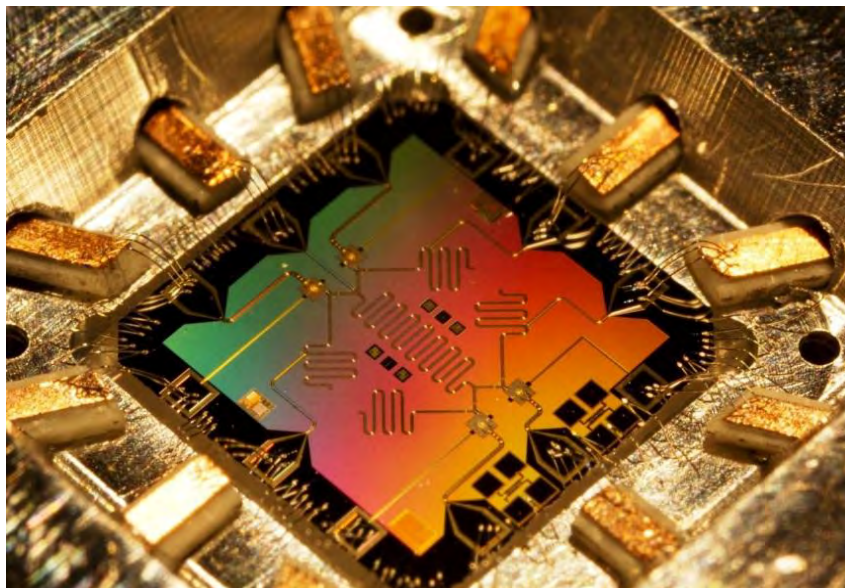


Figure.I.7 Exemple de circuit capable de porter des qubits.

Un Qubit est un système quantique à deux dimensions. Son espace de Hilbert se compose de deux états propres formant une base. Ils sont orthogonaux et sont notés $|0\rangle$ et $|1\rangle$. Tous les Qubits s'expriment dans cette base.

$$|Qubit\rangle \geq \cos\theta|0\rangle + e^{j\varphi} \sin\theta|1\rangle \tag{I.1}$$

avec $0 \leq \theta \leq \pi/2$ et $0 \leq \varphi \leq \pi/2$

Les angles θ et φ sont deux paramètres indépendants caractérisant un unique point sur une sphère unité de \mathbf{R}^3 , nommée sphère de Bloch, ayant pour coordonnées cartésiennes

$$X = \sin 2\theta \cos \varphi, \quad y = \sin 2\theta \sin \varphi, \quad z = \cos 2\theta \tag{I.2}$$

Un Qubit est représenté sur cette sphère sur la Figure.I.8. Dans cette représentation, $|0\rangle$ et $|1\rangle$ ont pour coordonnées respectives $(0, 0, 1)$ et $(0, 0, -1)$.

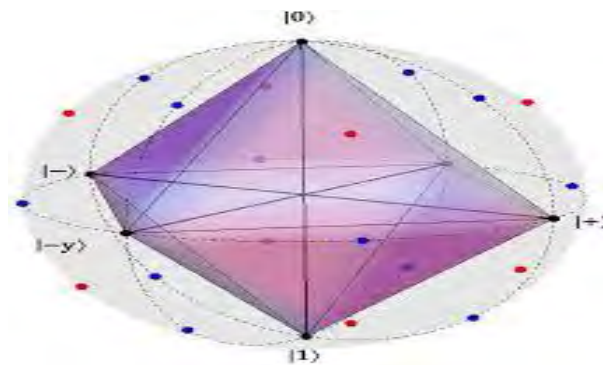


Figure.I.8 Sphère de Bloch et représentation des qubits.

Les principes de symétrie dans la théorie des systèmes multi qubit a fait l'objet d'un travail d'Herbrüggen et des coauteurs sur la contrôlabilité et l'observabilité des systèmes multispins dans des architectures de symétries variées [41]. Ce que nous notons comme principal résultat, c'est l'évolution de la sphère de Bloch suivant l'augmentation du nombre de qubits que nous montrons sur la Figure.I.9.

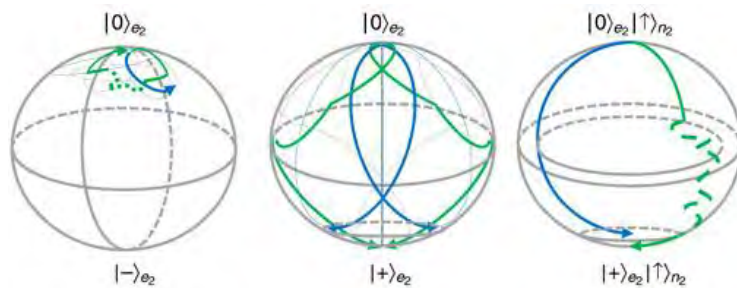


Figure.I.9 Evolution de la Sphère de Bloch pour des multi qubits.

La circuiterie utilisée pour obtenir des qubits, comporte un premier processus d'initialisation ou des impulsions sont envoyées sur un cristal optique non linéaire [44] qui servira à séparer deux rayons à travers deux séparateurs de faisceaux optiques PBS et PBS2 précédés de deux filtres. Quatre lames demi-onde HWP généreront les qubits.

Le deuxième processus comportera une estimation de phase comprenant quatre séparateurs de faisceaux et des portes CNOT. Enfin, le processus de mesure comprend des polariseurs, une plaque quart d'onde et des photodétecteurs. Le processus complet est reporté sur la Figure.I.10.

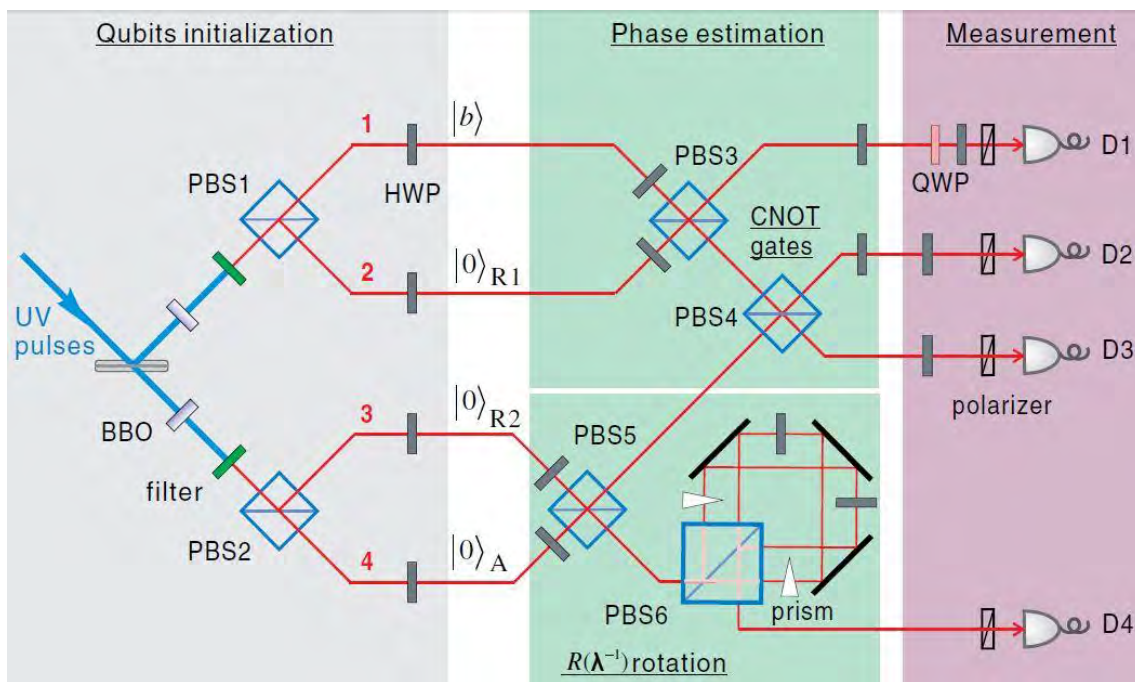


Figure.I.10 Processus expérimental d'initialisation, d'estimation de phase et de mesure des qubits.

I.2.3 Qudit et Qutrit

2.3.1 Qudit

Dans un système quantique à 2 niveaux, l'appellation de qudit est utilisée. Similaire au qudit, un qutrit est une unité d'information quantique dans un système quantique à 3 niveaux.

Dans le cas d'un système à quatre niveaux on parle de ququad. Plusieurs travaux ont mis en relief le codage des qudits en utilisant des photons émis sur demande à partir d'un système d'atomes dans une cavité [42]. La méthode utilisée est cependant limitée par la nature probabilistique des sources de la conversion paramétrique spontanée. Nous reportons sur la

Figure.I.11-a le dispositif expérimental de mesure d'après [42] et sur la Figure.I.11-b, les résultats obtenus ainsi que les différentes phases développées par [42].

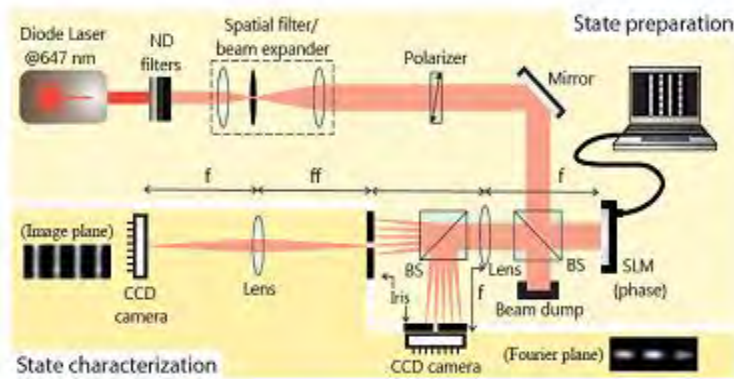


Figure.I.11-a. Expérimental setup

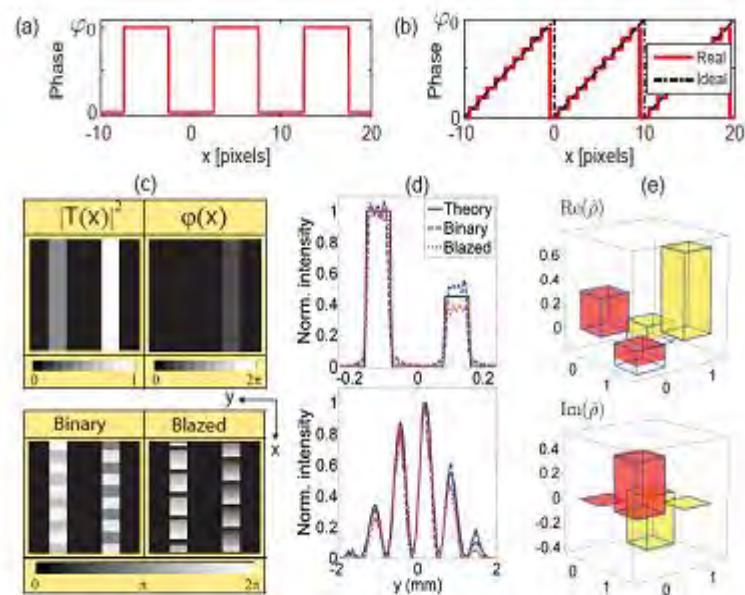


Figure.I.11-b Représentation des qudits.

D	2	3	4	5	7
# of states/grating	561	24	70	25	94
F_{bin}	0.996	0.995	0.985	0.968	0.970
F_{bla}	0.996	0.996	0.991	0.971	0.977

Table.I.1 fidélités moyennes pour qudits de niveau D .

L'inversion de canal quantique asymptotiquement optimal pour les ensembles de qudit et les états gaussiens multimodes a été faite par [43].

Une nouvelle stratégie pour l'envoi sur des distances arbitraires de deux états de qudit de manière déterministe de plusieurs expéditeurs à un récepteur a été testée avec succès [38]. Le régime est ensuite étendu de manière arbitraire à plusieurs qudits.

Dans le traitement quantique de l'information, les qudits sont une extension de qubits qui pourrait accélérer certaines tâches informatiques. On démontre le fonctionnement d'un qudit de phase supraconductrice avec un certain nombre de niveaux d jusqu'à $d = 5$ et on montre comment manipuler et mesurer l'état du qudit, y compris le contrôle simultané de plusieurs transitions [44].

Un algorithme classique permettant la conception de circuit quantique pour la simulation algorithmique quantique de canaux de qudits arbitraires est donné par [45].

Des décodeurs rapides pour des codes topologiques à base de qudits ont fait l'objet des travaux d'Anwar et des coauteurs [46]. Sur le même volet de décodage, il est important de signaler le travail de Hutter et des coauteurs sur des décodeurs de groupe de normalisation à grande décision [47]. Ces décodeurs sont utiles tout aussi bien pour les qudits que la correction d'erreur quantique pour les groupes non Abélien.

L'utilisation des systèmes quantiques élémentaires pour coder des informations est la clé de plusieurs nouvelles approches à l'informatique quantique, la technique utilisée étant linéaire, et basée sur l'optique informatique quantique (IQO) dans des circuits photoniques. Bien que cette méthode soit en principe évolutive, en pratique, elle est limitée par la nature stochastique de la conversion paramétrique spontanée des sources utilisées pour ensemençer les circuits. Ces sources produisent des paires simultanées de photons, l'un est utilisé comme un héraut, l'autre est utilisé pour initialiser un qubit.

Nous reportons sur la Figure.I.12, la partie expérimentale et les résultats obtenus par [63].

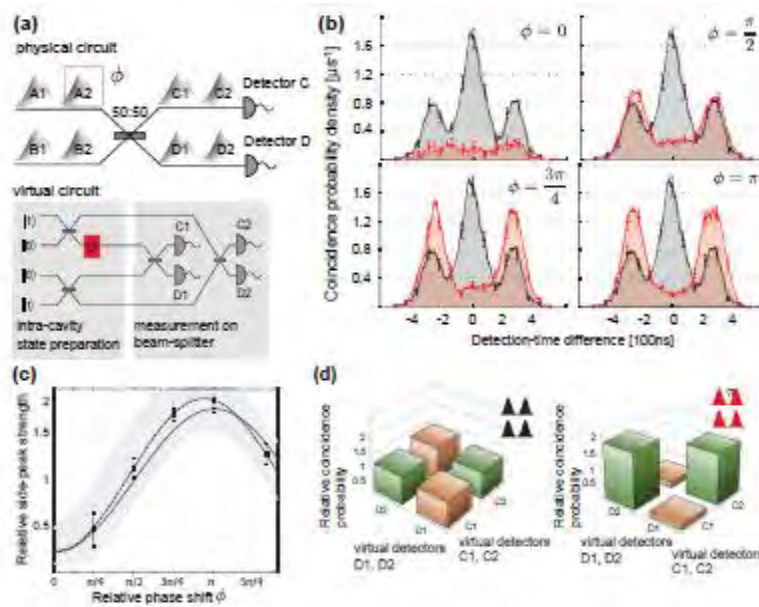


Figure.I.12 Différentes phases de mesure des qubits

I.2.3.2. Qutrit

Un qutrit a trois états de base orthogonaux, ou vecteurs souvent notés $|0\rangle$, $|1\rangle$, et $|2\rangle$ dans la notation de Dirac en bra et ket. Il est souvent représenté comme une combinaison linéaire de trois états :

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle + \gamma |2\rangle \quad (I.3)$$

Les coefficients sont des amplitudes de probabilité dont la somme quadratique est égale à un.

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1 \quad (I.4)$$

Les états de base des qutrits sont orthogonaux. Les qubits sont obtenus en utilisant les espaces de Hilbert H_2 , correspondant au spin up et au spin down. Les qutrits exigent un espace de Hilbert de dimension supérieur connu comme H_3 . Une chaîne de n qutrits représente 3^n états simultanément différents.

Les qutrits ont plusieurs caractéristiques particulières lorsqu'ils sont utilisés pour le stockage de l'information quantique. Par exemple, ils sont plus robustes à la décohérence sous certaines interactions environnementales. En réalité, la manipulation directe des qutrits pourrait être difficile, et une façon de le faire est d'utiliser un enchevêtrement avec un qubit comme ce qui est montré dans la Figure.I.13.

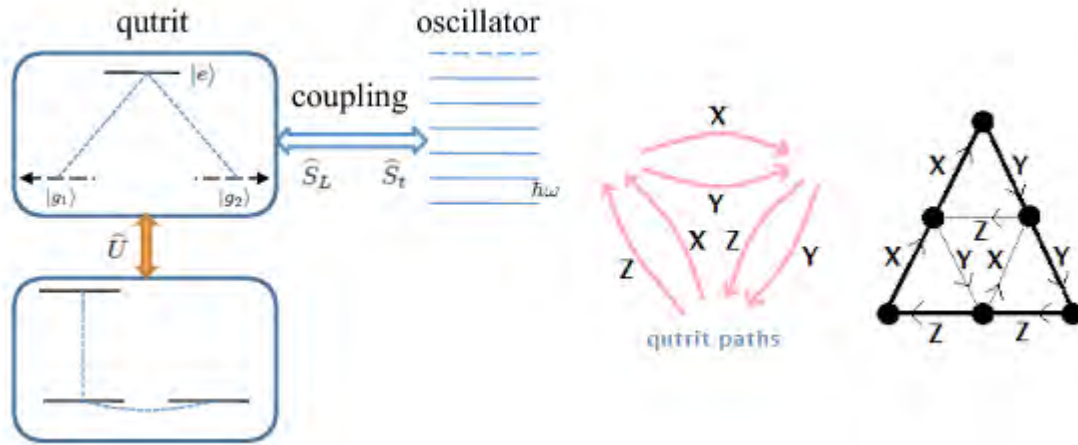


Figure.I.13 Représentation des qutrits.

I.2.4 Matrices de Pauli

I.2.4.1 Définition

Les matrices de Pauli forment une base de l’algèbre de Lie du groupe SU(2). Le groupe SU(2) constitue un groupe unitaire de degré 2 qui est le groupe des matrices unitaires à coefficients complexes de dimensions 2x2 et de déterminant 1. L’algèbre de Lie correspondante a SU(2) est notée su(2). Il s’agit de l’algèbre des matrices complexes 2x2 anti hermitiennes de trace nulle, le commutateur standard servant de crochet de Lie.

Les matrices de Pauli sont définies comme l’ensemble de matrices complexes de dimensions 2x2 suivantes :

$$\begin{aligned} \sigma_1 = \sigma_x &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ \sigma_2 = \sigma_y &= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \\ \sigma_3 = \sigma_z &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned} \tag{I.5}$$

Ces matrices sont utilisées en mécanique quantique pour représenter le spin des particules

I.2.4.2 Propriétés de ces matrices

$$\sigma_1^2 = \sigma_2^2 = \sigma_3^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2 \tag{I.6}$$

$\sigma_1\sigma_2=i\sigma_3, \sigma_3\sigma_1=i\sigma_2, \sigma_2\sigma_3=i\sigma_1, \sigma_i\sigma_j=-\sigma_i\sigma_j$ pour $i \neq j$.

$$\begin{aligned} \det(\sigma_i) &= -1 \\ Tr(\sigma_i) &= 0 \\ \text{pour } i \in \{1; 2; 3\} \end{aligned} \tag{I.7}$$

Par conséquent, les valeurs propres de chaque matrice sont ± 1 .

Les matrices de Pauli obéissent aux relations de commutation et d'anti commutation suivantes :

$$[\sigma_i, \sigma_j] = 2i\epsilon_{ijk} \sigma_k \quad (\text{I.8})$$

$$[\sigma_i, \sigma_j] = 2\delta_{ij} \cdot I$$

Où ϵ_{ijk} est le symbole de Levi Civita, δ_{ij} est le symbole de Kronecker et I la matrice identité.

Les relations précédentes peuvent être vérifiées en utilisant :

$$\sigma_i \sigma_j = i\epsilon_{ijk} \sigma_k + \delta_{ij} I \quad (\text{I.9})$$

Ces relations de commutativité sont semblables à celles de l'algèbre de Lie SU(2). SU(2) peut être interprétée comme l'algèbre de Lie de toutes les combinaisons linéaires de l'imaginaire i fois les matrices de Pauli $i\sigma_j$, autrement dit comme les matrices anti hermitiennes 2x2 avec une trace nulle. Dans ce sens, les matrices de Pauli génèrent SU(2). Par conséquent, $i\sigma_j$ peut être vu comme les générateurs infinitésimaux du groupe de Lie correspondant SU(2).

Pour un vecteur de rotation en trois dimensions $\vec{\omega}$ et $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$, le vecteur composé des matrices de Pauli, on a la relation suivante :

$$e^{-i\vec{\sigma}\frac{\vec{\omega}}{2}} = I \cos\left(\frac{\omega}{2}\right) - i\hat{\omega}\vec{\sigma} \sin\left(\frac{\omega}{2}\right) \quad (\text{I.10})$$

Où ω est l'angle de rotation (la norme de $\vec{\omega}$) et $\hat{\omega} = \frac{\vec{\omega}}{\omega}$

Les $i\sigma_j$ représentent les générateurs des rotations sur les particules de spin $\frac{1}{2}$. L'état de ces particules est représenté par des spinors à deux composantes, ce qui est la représentation fondamentale de SU(2). Une propriété intéressante des particules de spin $1/2$ est qu'elles doivent subir une rotation de 4π radians afin de revenir dans leur configuration d'origine. Ceci est dû au fait que SU(2) et SO(3) ne sont pas globalement isomorphes, malgré le fait que leur générateur su(2) et so(3) soient isomorphes. SU(2) est en fait un revêtement de degré deux de SO(3), à chaque élément de SO(3) correspondent deux éléments de SU(2).

I.2.5 Décohérence

Le calcul quantique des probabilités porte sur des phénomènes dont l'occurrence est suspendue à l'intervention d'un contexte approprié. Le problème est qu'en tant que théorie physique, la mécanique quantique a une vocation à l'universalité. Le calcul des probabilités méta-contextuel, qui est son élément constitutif principal, devrait dans ces conditions pouvoir s'appliquer sans restriction et à toute échelle. Mais, dans notre environnement familier, la théorie classique (kolmogorovienne) des probabilités n'est-elle pas parfaitement utilisable? Et cette théorie classique ne fonctionne-t-elle pas, contrairement à son équivalent quantique, de telle sorte que rien n'interdit de considérer qu'elle exprime une ignorance partielle au sujet de propriétés intrinsèques et d'événements autonomes?

Un problème de compatibilité se pose alors, entre le calcul quantique des probabilités, valable en principe à toute échelle, et le calcul classique des probabilités, valable en pratique à notre échelle. Les théories de la décohérence ont pour principal objet de prouver cette compatibilité. Elles permettent en effet de montrer comment appliquer à des processus complexes faisant intervenir un objet, un appareil de mesure, et un vaste environnement.

Le calcul quantique des probabilités se ramène à une très faible approximation près au calcul classique des probabilités. Ceci se manifeste par une quasi-disparition de termes d'interférence typiques du calcul quantique des probabilités, et isomorphes à ceux d'un processus ondulatoire, au profit d'une quasi-validité de la règle classique d'additivité des probabilités d'une disjonction.

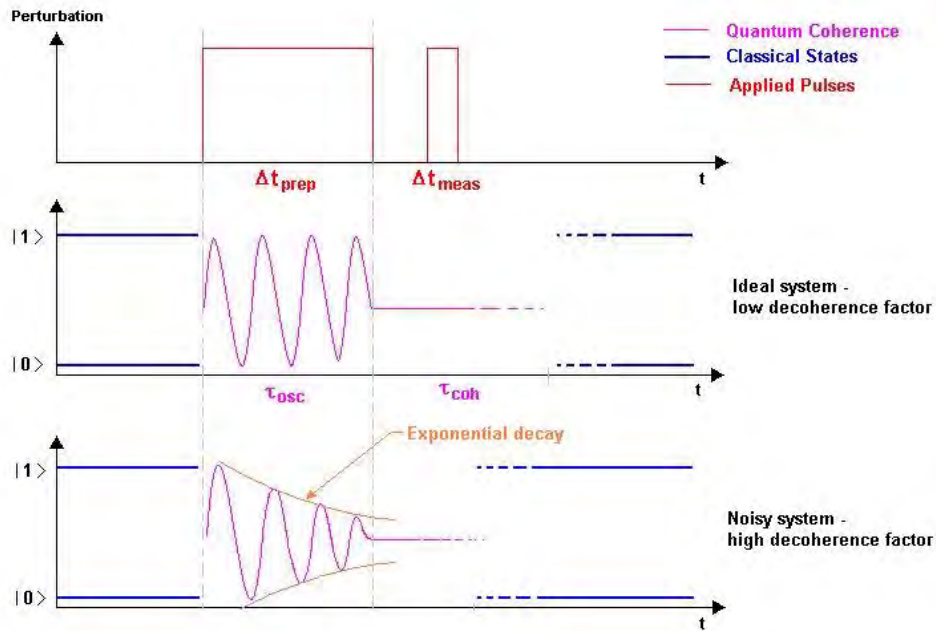


Figure.I.14 Comparaison des facteurs de Décohérence.

La théorie de la décohérence a été introduite par H. Dieter Zeh en 1970 [48]. Elle a reçu ses premières confirmations expérimentales en 1996 [49]. Un ouvrage de référence sur la décohérence, clair et d'une grande précision [50].

La décohérence quantique est une théorie susceptible d'expliquer la transition entre les règles physiques quantiques et les règles physiques classiques telles que nous les connaissons, à un niveau macroscopique. Plus spécifiquement, cette théorie apporte une réponse, considérée comme étant la plus complète à ce jour, au paradoxe du chat de Schrödinger et au problème de la mesure quantique.

Zeh fait remarquer que les niveaux d'énergie des systèmes macroscopiques sont tellement proches les uns des autres que même de toutes petites fluctuations peuvent les affecter. Ils ne peuvent donc jamais être considérés comme réellement isolés de leur environnement. Il en résulte que dans ce que nous avons appelé le deuxième point de vue lors d'une mesure, le grand système S doit inclure aussi cet environnement. Il faut donc appliquer l'équation de Schrödinger à la fonction d'ondes du système S, de l'appareil A et de l'environnement E. On aboutit alors après l'instant t , à un état enchevêtré du système, de l'appareil et de l'environnement. Cependant, lors d'une mesure, on se contente en fait, d'observer le système et l'appareil et on laisse de côté l'environnement. La raison en est d'une part que l'environnement ne nous intéresse pas et d'autre part, qu'on serait bien incapable de mesurer les grandeurs attachées à ses différentes composantes. On sépare donc le système et

l'appareil de leur environnement. Or, la mécanique quantique nous dit que lorsqu'on ne s'intéresse qu'à un sous-système d'un grand système, il est possible d'obtenir son état à partir de l'état du grand système en faisant une opération mathématique — qui s'appelle « prendre la trace partielle » — sur l'état global. Et c'est là que la suggestion de Zeh montre sa pertinence, puisqu'il est possible de montrer — Zurek a été un des premiers à le faire au début des années 80 — que l'état ainsi obtenu est identique — à certaines réserves près que nous verrons plus loin — à celui qu'on obtient par le principe de réduction du paquet d'ondes.

L'évolution par l'équation de Schrödinger et celle par le principe de réduction du paquet d'ondes sont enfin réconciliées. La théorie de la décohérence est une énorme avancée dans la résolution du problème de la mesure. Tout d'abord, l'état qu'on obtient pour le système et l'appareil par l'utilisation de la décohérence n'est pas exactement identique à celui qu'on obtient par application du principe de réduction du paquet d'ondes.

La décohérence nous dit que les corrélations entre les différents états possibles deviennent très rapidement négligeables, ces corrélations ne disparaissent pas totalement. Simplement, elles deviennent trop faibles pour être mesurables. Par ailleurs, si on s'intéresse à un système unique et non pas à un ensemble de systèmes, l'état qu'on obtient après décohérence doit être interprété comme le fait que le système est dans une sorte de coexistence, sans corrélation, des différents états possibles plutôt que comme dans un seul état choisi parmi les états possibles. Cette difficulté, est appelée problème du « ou-et » par Bell. Il nous suffit de signaler que ces deux différences entre les états produits par application de la décohérence et ceux produits par application du principe de réduction montrent que la réponse n'est pas si immédiate que certains physiciens paraissent le croire.

La décohérence ne modifie en rien la mécanique quantique et garde en son sein les mêmes défauts.

Elle permet d'expliquer selon le même formalisme pourquoi on ne peut pas mesurer des effets d'intrications dans des objets macroscopiques ou pourquoi de tels objets sont dans des états bien définis. Seulement, on est obligé, à un moment ou à un autre, d'utiliser les calculs de probabilités et le postulat de la mesure, inhérents à la mécanique quantique. En d'autre mot, la décohérence n'est rien d'autre qu'une mesure faite par l'environnement via un mécanisme compliqué caché dans le formalisme de la matrice densité du système total.

Le formalisme de la matrice densité (ou matrice de Pauli) est utilisé par Benenti et les coauteurs [51] pour illustrer la décohérence d'un qubit dans un environnement à deux qubits (le qubit et le milieu environnant). Les auteurs supposent que le système est initialement dans l'état $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, de la matrice densité. Les termes diagonaux correspondent aux « populations » des qubits $|0\rangle$ et $|1\rangle$, tandis que les termes hors diagonale n'existent que pour un état contenant une superposition « cohérente » des états de calcul $|0\rangle$ et $|1\rangle$. Les auteurs supposent, ensuite que le couplage système / environnement s'exprime par une porte logique CNOT, qui a pour effet de porter le système initial global de l'état.

I.2.6 Intrication

L'intrication quantique (ou enchevêtrement quantique) est un phénomène observé en mécanique quantique dans lequel l'état quantique de deux objets doit être décrit globalement, sans pouvoir séparer un objet de l'autre, bien qu'ils puissent être spatialement séparés. Lorsque des objets quantiques sont placés dans un état intriqué (ou état enchevêtré), il existe des corrélations entre les propriétés physiques observées de ces objets qui ne seraient pas présentes si ces propriétés étaient locales. En conséquence, même s'ils sont séparés par de grandes distances spatiales, deux objets intriqués O_1 et O_2 ne sont pas indépendants et il faut considérer $\{O_1+O_2\}$ comme un système unique.

Le phénomène de l'intrication et le paradoxe EPR ont mystifié les physiciens depuis qu'Einstein, Podolsky et Rozen ont publié leur idée en 1935 [30]. Depuis lors, l'existence de l'intrication est maintenant théoriquement et expérimentalement bien établie. En effet, l'intrication quantique est vue comme une ressource cardinale de la communication quantique. En utilisant les quaternions, Singh [52] étudie la géométrie d'un seul ou de 2 états de qubits du calcul quantique. A Travers les fibrations de Hopf [53], il identifie les manifestations géométriques de la séparabilité et de l'intrication de 2 qubits. Par la suite, il présente les traits saillants de l'expérience EPR et de la version de Bohm en termes de spins [28],[29]. Des schémas possibles de la résolution du paradoxe EPR en termes du principe de complémentarité de Bohr, du temps de rétroaction et du potentiel quantique de Bohm, sont aussi discutés. Des anomalies résultant du schéma (Figure.I.15) de Von Neumann des mesures quantiques sont aussi abordés.

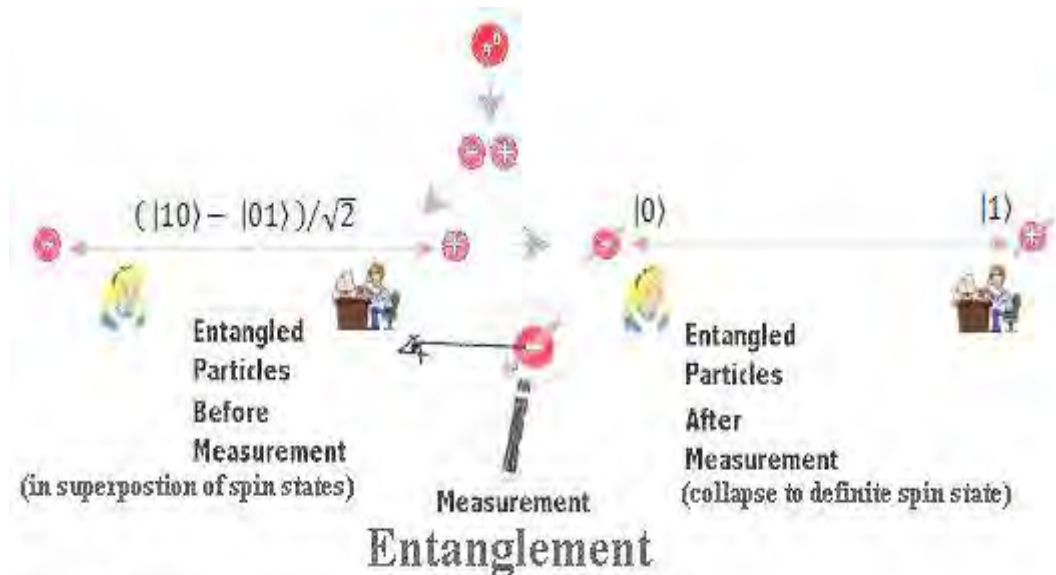


Figure.I.15. Représentation de l'Intrication.

Des chercheurs de l'ESA ont réussi à battre un nouveau record de téléportations quantique en parvenant à maintenir un état d'intrication quantique entre deux particules distantes de 143 km. Cette avancée majeure ouvre la voie vers la possibilité de transmettre et de crypter des informations en utilisant les lois de la physique quantique.

Conformément à la théorie quantique, les deux particules en question, bien que séparées en apparence par une grande distance, restent corrélées et forment en fait une entité commune. De ce fait, toute action sur l'une de ces particules aura instantanément un effet sur l'autre, quelle que soit la distance qui les sépare et sans pour autant que ce phénomène ne viole la vitesse limite de la lumière.

Pour cette nouvelle expérience, les chercheurs sont parvenus à produire et à émettre des photons (le constituant fondamental de la lumière et le vecteur de l'interaction électromagnétique) dans des directions opposées en maintenant jusqu'à cette distance de 143 km, leur état intriqué, leur "cohérence" quantique.

Cette expérience confirme donc qu'il est possible d'envisager des communications quantiques sur de grandes distances et les chercheurs de l'ESA vont à présent tenter de réaliser une communication quantique entre la Terre et un satellite en orbite. Mais le véritable enjeu de ces recherches est la mise au point d'un mode de cryptage quantique des informations.

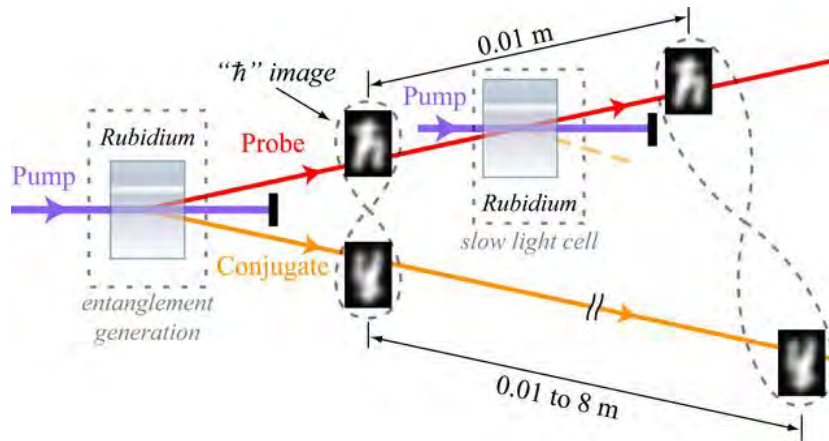


Figure.I.16. Dispositif de génération de l'Intrication.

I.3 WDM

I.3.1 La Technologie W.D.M

Alors que les systèmes de transmission sur fibres optiques ne reposaient que sur l'utilisation du multiplexage temporel (ou TDM pour Time Division Multiplexing), une nouvelle génération de systèmes est apparue au début des années 90, mettant en oeuvre le multiplexage de longueurs d'onde (ou WDM pour Wavelength Division Multiplexing).

I.3.2 Principe de fonctionnement

La technologie WDM est née de l'idée d'injecter simultanément dans la même fibre optique plusieurs trains de signaux numériques à la même vitesse de modulation, mais chacun à une longueur d'onde distincte.

A l'émission, on multiplexe n canaux au débit nominal D , à la réception, on démultiplexe le signal global $n \times D$ en n canaux nominaux.

L'espacement entre deux longueurs d'ondes est définie par la norme internationale ITU-T G 692 (Interfaces optiques pour systèmes multi-canaux avec amplificateurs optiques). Elle définit un peigne de longueurs d'onde autorisées dans la seule fenêtre de transmission 1530-1565 nm. Cet espacement en nanomètre (nm) ou en Gigahertz (GHz) entre deux longueurs d'onde a été fixé à 200 GHz ou 1,6 nm et 100 GHz ou 0,8 nm.

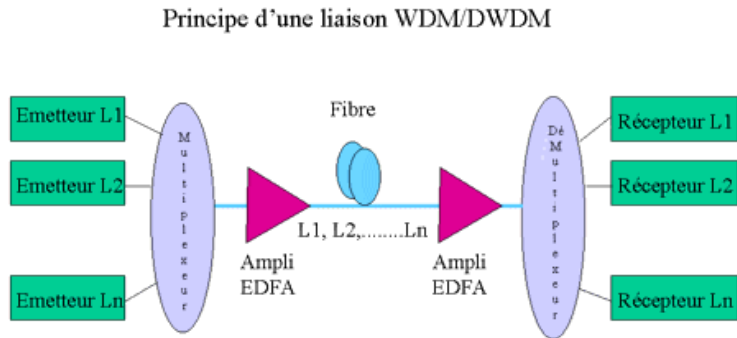


Figure.I.17. Principe d'une liaison WDM/DWDM

La technologie WDM est dite dense (DWDM) lorsque l'espacement utilisé est égal ou inférieur à 100 GHz. Des systèmes à 50 GHz (0,4 nm) et à 25 GHz (0,2 nm) ont déjà été testés.

Un des composants clés du WDM/DWDM est l'amplificateur à fibre dopée erbium (EDFA) qui permet de compenser les pertes d'insertion dues aux multiplexage/démultiplexage des longueurs d'onde.

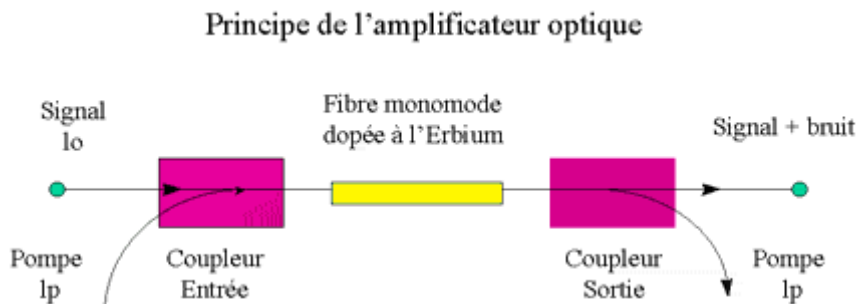


Figure.I.18. Principe de l'amplificateur optique

Néanmoins le DWDM introduit des phénomènes non linéaires qui ont notamment pour conséquence de limiter en pratique la distance entre amplificateurs entre 50 et 100 Km.

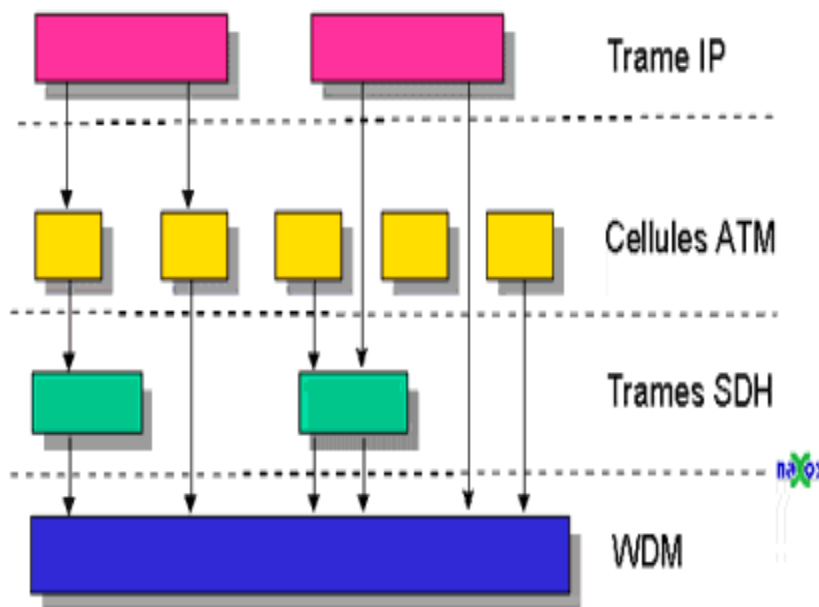
I.3.3 L'utilisation des systèmes WDM

Les systèmes WDM / DWDM commercialisés aujourd'hui comportent 4, 8, 16, 32 voire 80 canaux optiques, ce qui permet d'atteindre des capacités de 10, 20, 40, 80 voire 200 Gb/s en prenant un débit nominal de 2,5 Gb/s par canal, débit pour lequel les composants d'émission / réception sont très répandus.

Pour fixer les idées, un système à 16 canaux 2,5 Gb/s permet de transmettre 500 000 conversations téléphoniques simultanées sur une fibre.

Compte tenu des nombreux avantages que le DWDM apporte, l'intégration de cette nouvelle technologie dans un réseau d'opérateur nécessite de repenser son architecture avec le double objectif, de ménager les investissements déjà réalisés tout en préparant un proche avenir où simplicité, fiabilité et faible coût seront les clés du succès.

L'approche faite par de nouveaux opérateurs aux Etats-Unis de bâtir aujourd'hui directement leur réseau avec de l'IP (Internet Protocol) sur la SDH, voire IP directement sur le DWDM est un signe révélateur de cette tendance qui devrait voir le jour en Europe dans les prochaines années.



Combinaisons entre les différentes couches services et transports

Figure.I.19. Combinaisons entre les différents couches services et transports

Ainsi, il apparaît certain que demain la longueur d'onde optique deviendra un élément à part entière du réseau et que la technologie DWDM n'a pas encore atteint ses limites.

De nouvelles techniques en cours de développement permettront de multiplier encore plus les capacités des systèmes optiques :

- la transmission SOLITON permettant le transport d'impulsions très étroites sur des milliers de Km sans déformation, tout en conservant une bande passante très large.
- la modulation des impulsions, ou transmission duo-binaire, permettant la multiplication par deux ou trois fois du débit électronique, en utilisant des impulsions à 2 ou 3 niveaux binaires.

I.3.4 Les réseaux DWDM

Le multiplexage en longueur d'onde repose sur l'envoi d'ondes lumineuses multiples (fréquences) dans une même fibre optique. L'information est transmise par chaque onde, appelée voie, par modulation d'intensité (ou d'amplitude) ou par modulation de phase. A la réception un prisme optique ou un dispositif semblable sépare les fréquences de manière à extraire séparément l'information transmise par chaque voie. Un signal numérique binaire, plus précisément un signal de modulation d'intensité par tout ou rien, peut également être acheminé par chaque voie individuelle. On peut mélanger les porteuses sur un seul support car la lumière d'une fréquence donnée ne brouille pas celle d'une autre fréquence à l'intérieur de l'ordre linéaire d'approximation. Dans les Figure.I.20 (a, b, c) représente le Montage expérimental.

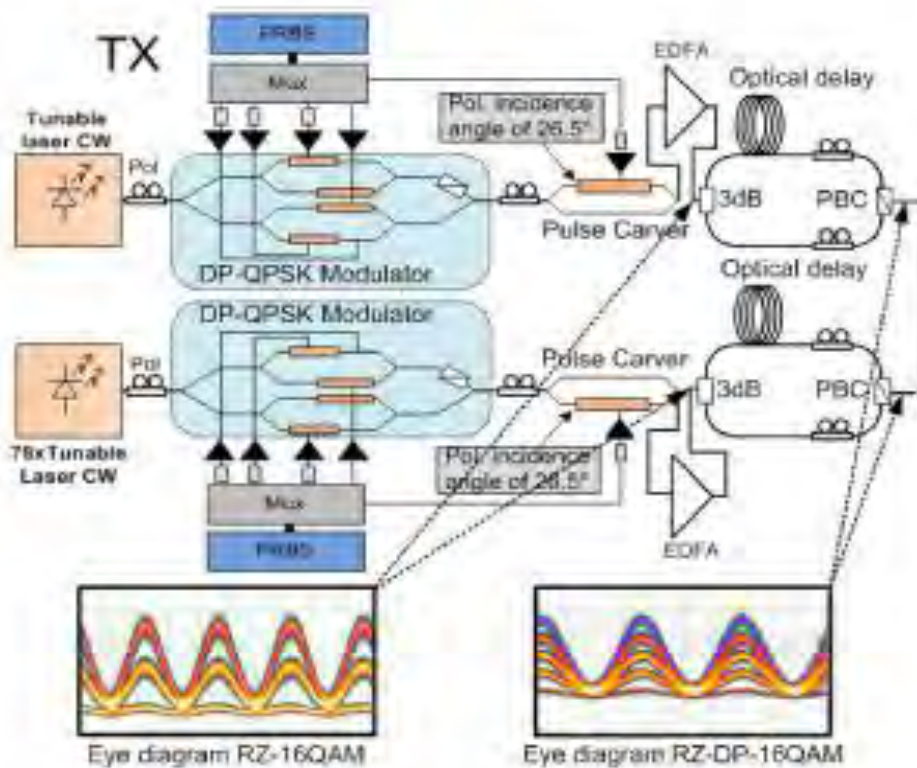


Figure.I.20-a. transmission

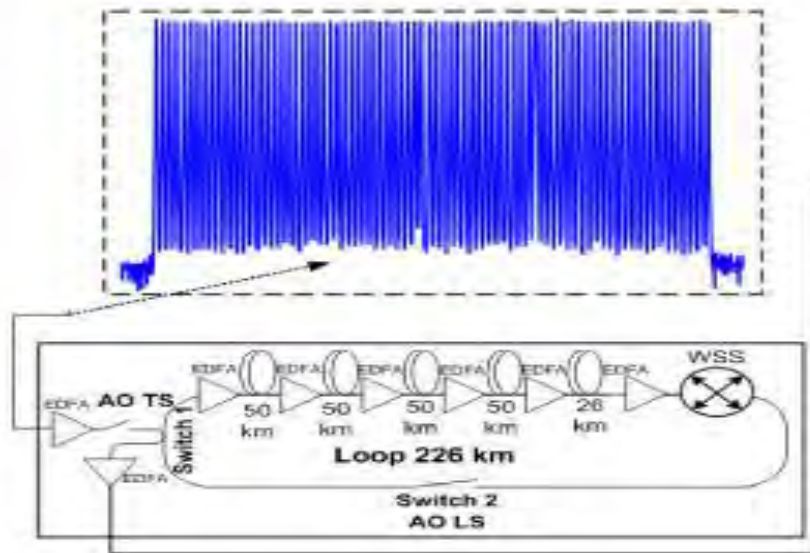


Figure.I.20-B. boucle de recirculation

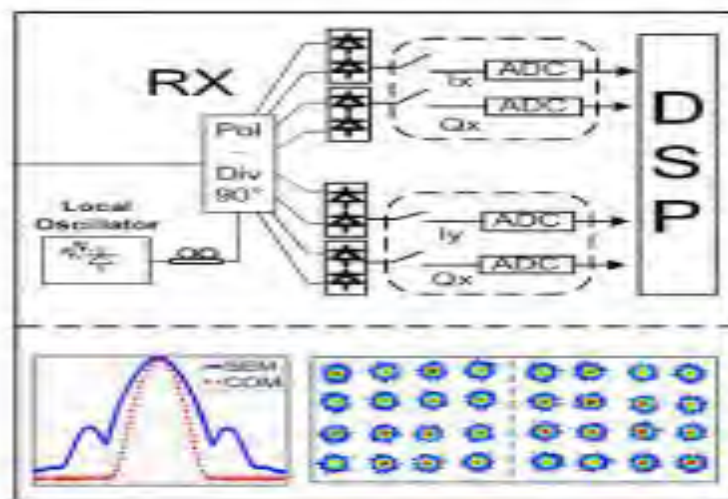


Figure.I.20-C. réception

Figure.I.20. Le spectre de transmission DWDM, ainsi que le spectre de canal testé avec et sans pré-filtrage et la constellation reçue, sont également illustrés

Dans le cas du DWDM, le routage se fait de manière sélectif des signaux optiques en fonction de leur longueur d'onde lors de leur cheminement dans les éléments de réseaux situés entre l'émetteur et le récepteur. Le routage des longueurs d'onde à deux caractéristiques, il détermine la raie spectrale du signal optique et en cas d'émission de signaux multiples à partir d'un même nœud, chaque signal peut être destiné à un récepteur distinct.

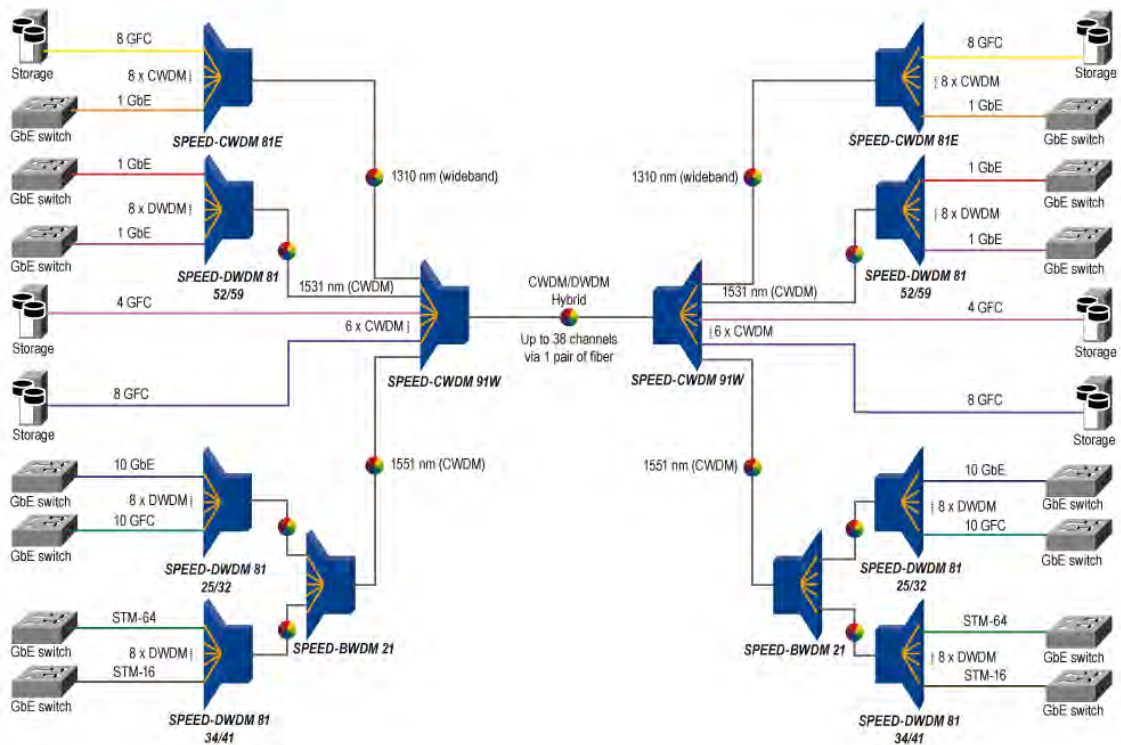


Figure.I.21. le routage DWDM

I.4 Algorithmes quantiques

Les ordinateurs quantiques sont connus pour être qualitativement plus puissant que les ordinateurs classiques, mais jusqu'à présent, seul un petit nombre d'algorithmes ont été découverts qui utilise effectivement ce potentiel. Il serait donc hautement souhaitable de développer d'autres types d'algorithmes quantiques qui élargissent l'éventail des possibles applications. Ici, nous proposons un algorithme quantique efficace et précis pour trouver la partie carré libre d'un grand nombre entier - un problème pour lequel aucun algorithme classique efficace n'existe.

L'algorithme repose sur les propriétés des sommes de Gauss, il utilise la transformée de Fourier quantique. Nous donnons un réseau quantique explicite pour l'algorithme. Notre algorithme introduit de nouveaux concepts et des méthodes qui ne sont pas utilisés dans le traitement quantique de l'information à ce jour et peuvent être applicables à une catégorie plus large de problèmes. Principe fondamental de l'informatique classique est basé sur la thèse de Church-Turing, qui affirme que tout dispositif de calcul pratiquement réalisable peut être simulé par un ordinateur universel connu sous le nom turing machine¹

Cependant, cette hypothèse repose implicitement sur les lois de physique classique et était contestée par Feynman et d'autres qui ont suggéré que les dispositifs de calcul se comporter selon mécanique quantique pourraient être qualitativement plus puissant que les ordinateurs classiques. Une première preuve de cette conjecture était donnée en 1993 par Bernstein et Vazirani⁴. Ils ont montré que la machine de Turing mécanique quantique est capable de simuler d'autres systèmes mécaniques quantiques en temps polynomial, une amélioration exponentielle de calcul par rapport à la machine de Turing classique. Leur preuve n'a pas donné un algorithme quantique rapide réel, mais dans l'année suivante, Peter Shor est venu avec son célèbre algorithme⁵ de factorisation, ce qui résout le problème de factorisation d'entier à temps polynomial, exponentiellement plus rapide que tous les algorithmes classiques connus. La partie essentielle de cet algorithme est une solution du problème de recherche, qui peut être formulé comme un problème de sous-groupes masqué (HSP)⁶. Un problème de sous-groupe caché est de savoir la période d'une fonction périodique donnée.

La périodicité de la fonction peut être si compliquée qu'il ne peut pas être facilement déterminée par des moyens classiques. L'importance de la HSP est que l'équation de différentes instances (par ex. Pell, le problème principal idéal, le groupe de base informatique) et des variantes comme le problème de décalage caché et les structures non linéaires cachées englobent la plupart des algorithmes quantiques trouvés jusqu'à présent qui sont exponentiellement plus vite que leurs équivalents⁷ classiques. Cette relativement étroite gamme d'algorithmes quantiques rapides existants montre le besoin urgent pour les différents types d'algorithmes quantiques qui feraient d'autres classes de problèmes accessibles à des solutions efficaces.

Nous décrivons ici un tel algorithme quantique qui ne tombe pas dans le cadre de HSP. Elle résout deux problèmes théorétiques en temps polynomial, à savoir, tester le carré-liberté et le calcul de la partie sans carré d'un entier donné. En comparaison avec les algorithmes classiques connus, ceci fournit une augmentation exponentielle de l'efficacité. Bien que ces problèmes soient liés au problème de factorisation résolu par Shor, notre algorithme repose sur une approche différente. En outre, alors que l'algorithme de Shor est probabiliste, l'algorithme présenté ici est exact et sa complexité de calcul est inférieure.

I.5 Graphes Quantiques

Severin [54] dans une présentation détaillée de la fonction de Lovaszen mécanique quantique, montre tout l'intérêt de l'application de cette fonction pour aboutir à une théorie de l'information à erreur nulle ainsi qu'à certains aspects du non contextualité. Son application dans la transmission de clé quantique en cryptographie a été prouvée.

Nous montrons sur la Figure.I.22, le processus d'évolution pour un graphe aléatoire classique avec $N=10$ nœuds. Partant de nœuds isolés, nous ajoutons aléatoirement des bords en augmentant la probabilité p , pour obtenir éventuellement un graphe complet K_{10} pour $p=1$.



Figure.I.22 graphe aléatoire

Nous donnons un exemple d'un graphe aléatoire quantique de cinq nœuds dans la Figure.I.23. Sur la partie A, chaque nœud est en possession de quatre qubits qui sont intriqués avec des qubits appartenant à d'autres nœuds. Toutes les connexions sont pures et identiques mais les paires intriquées ne sont pas maximales. Sur la partie B, des paires non parfaites peuvent être converties en paires intriquées maximales avec une probabilité de succès de $p=0.25$. Cette stratégie minimise le comportement des graphes aléatoires classiques.

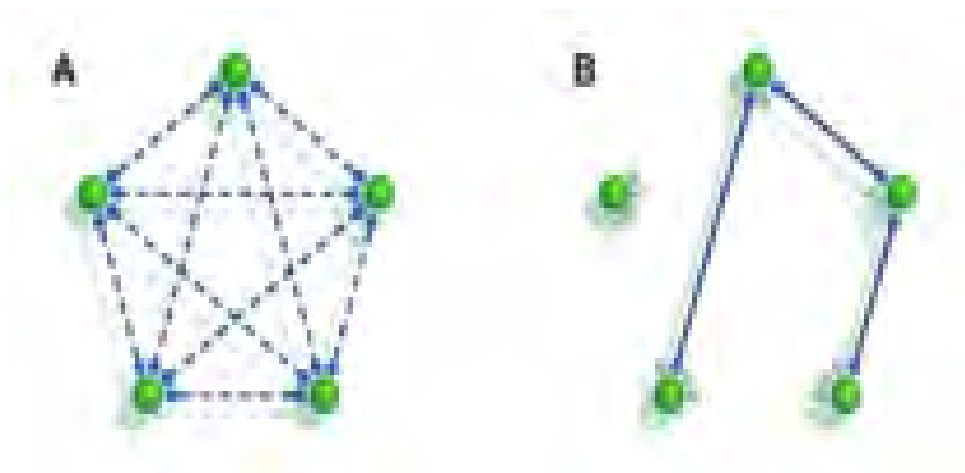


Figure.I.23 graphe aléatoire quantique de cinq nœuds

I.6 La cryptographie quantique

La cryptographie quantique n'est pas en soi un nouveau procédé de cryptographie. En effet, elle ne permet pas directement la communication de messages intelligibles, mais autorise (principalement) la distribution de clef cryptographique, ce qui conduit souvent à désigner la distribution quantique de clef (Quantum Key Distribution) par le terme plus général de cryptographie quantique. Elle apparaît donc comme un complément de la cryptographie classique, puisqu'elle répond à son besoin de distribution de clef privée.

La sécurité de cette méthode repose sur les lois de la mécanique quantique et est considérée comme inconditionnellement sûre.

L'équipe d'Anton Zeilinger (Institut d'optique et d'information quantique à l'université de Vienne, Autriche) vient de présenter une étude affirmant qu'ils ont démontré une "téléportation quantique" sur une distance de 143 km dans les îles Canaries. Si elle est confirmée, ce record de distance fixe un nouveau palier dans l'univers de la téléportation quantique et ouvre également la voie pour un futur réseau quantique globale destinée aux communications sécurisées par satellite.

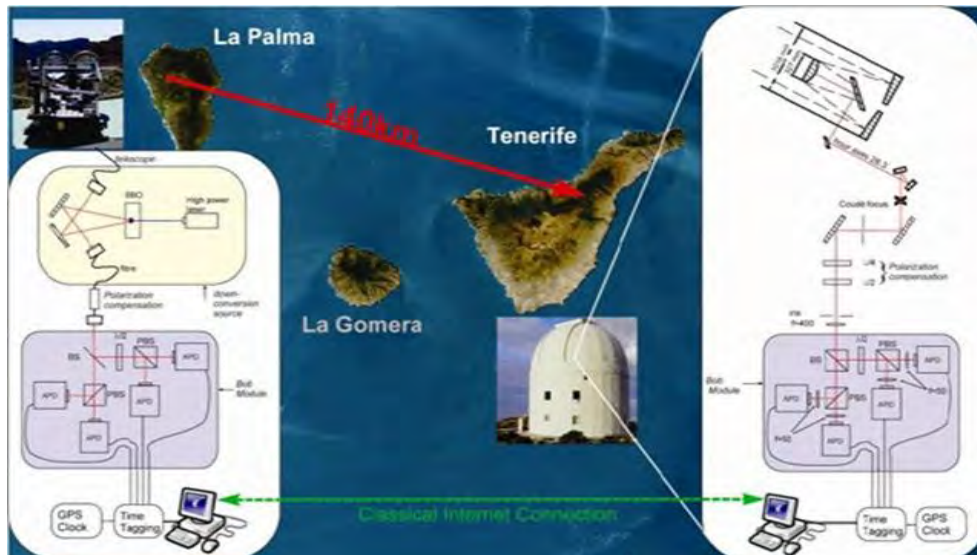


Figure.I.24. Schéma de la téléportation.

Des chercheurs de l'université des Sciences et Technologies de Chine, à Shanghai, ont affirmé qu'ils avaient démontré la téléportation quantique sur une distance de 97 km à travers un lac en Chine. La téléportation quantique, ne concerne pas la matière, c'est plutôt le processus de transfert de l'information exacte sur une particule, d'un endroit à un autre, en utilisant l'intrication quantique, la particule ne voyageant pas à travers l'espace intermédiaire.

La démonstration chinoise, de téléportation quantique, a confirmé que 1171 photons ont été téléportés en quatre heures, enregistrant une perte de 35 à 53 dB sur une distance de 97 km.

La démonstration autrichienne a confirmé que 605 photons ont été téléportés en environ 6,5 heures, en enregistrant une perte de 28 à 39 dB sur une distance de 143 km. La DARPA demande aux chercheurs de démontrer une transmission soutenue de clés quantiques sécurisées, clés au taux de 1 à 10 gigabits par seconde, à des distances de 1 000 à 10 000 km, *un véritable bond quantique (...)*.

Et il demande que les communications ne subissent aucune perte, face aux décohérences environnementales (décohérence quantique) que présente une atmosphère sale pour toute expérience. Selon la DARPA : « Les techniques actuelles de communication quantique sont très sensibles à la perte, avec une augmentation de la perte conduisant à une baisse correspondante du taux de bits (par exemple, 10 dB de perte résulte en un facteur de diminution de 10 en débit sécurisé). Les programmes sélectionnés sont tenus de présenter une méthode pour le découplage de la perte de débit sécurisé. »

Le programme a deux objectifs secondaires : de démontrer, de façon concluante, que la sécurité des communications quantiques peut être étendue à de nouveaux domaines, même sous l'eau et dans une atmosphère viciée, et d'étendre entièrement les communications quantiques macroscopiques à de nouveaux domaines.

I.7 Mesure d'un photon polarisé

De la lumière polarisée peut être obtenue en faisant passer un rayon de lumière à travers un polariseur. L'axe de polarisation du faisceau est déterminé par l'orientation du polariseur d'où émerge le faisceau. La production de photons polarisés isolés est théoriquement possible mais n'est, à l'heure actuelle, pas réalisable d'un point de vue technologique. Pour simplifier, nous ferons comme s'il était réaliste d'obtenir de tels photons isolés avec une polarisation définie.

Si un faisceau lumineux avec un angle de polarisation (α) traverse un filtre orienté selon un angle (β), les photons individuels se répartissent de manière dichotomique et probabiliste, chacun étant transmis avec une probabilité $\cos^2(\alpha-\beta)$ ou absorbé avec une probabilité complémentaire $\sin^2(\alpha-\beta)$. Les photons se comportent de manière déterministe

seulement lorsque les deux axes sont parallèles (transmission certaine) ou perpendiculaires (absorption certaine) [55].

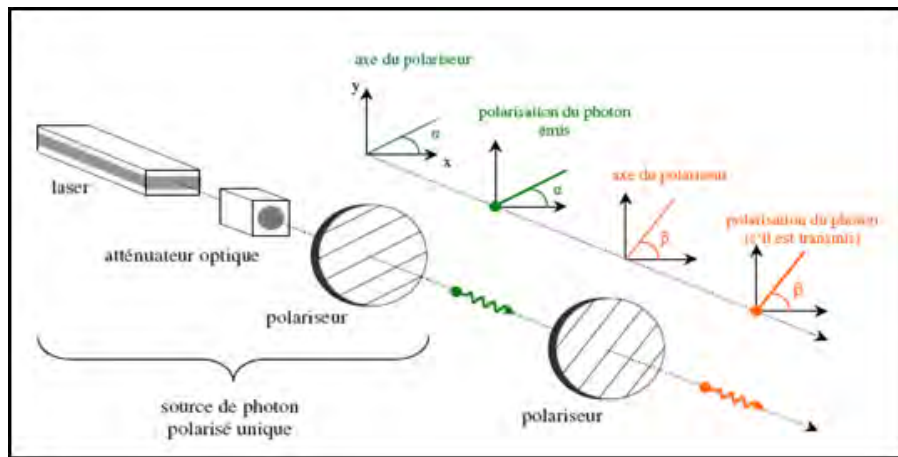


Figure.I.25 Mesure d'un photon polarisé linéairement.

Il est important de souligner que les photons perdent leurs polarisations initiales une fois qu'ils passent au travers d'un polariseur. A la sortie d'un polariseur orienté selon un angle α , les photons portent la polarisation α du polariseur, ce qui interdit une nouvelle mesure. Par contre, il est possible d'effectuer plusieurs mesures différentes sur des photons distincts d'un même faisceau de manière à déterminer la polarisation des photons du faisceau. Mais cela suppose que le faisceau soit constitué de plusieurs photons de polarisation identique. Cette approche ne peut donc pas aider à mesurer la polarisation d'un photon isolé.

I.8 Principe de la cryptographie quantique

La cryptographie quantique repose sur ces principales notions de mécanique quantique pour interdire à un espion de connaître des informations échangées entre deux entités, Alice et Bob. Si Eve tente d'intercepter les signaux envoyés par Alice, elle doit effectuer une mesure sur ceux-ci, et obligatoirement les perturber. Cette perturbation peut être évaluée par Bob, ce qui lui permet de détecter la présence d'Eve.

La cryptographie quantique repose sur l'utilisation de deux canaux. L'un est obligatoirement quantique, i.e. capable de transmettre des objets régis par les lois de la mécanique quantique (par exemple un photon transmis par fibre optique), le second est un canal classique qui peut être écouté par Eve, mais qu'elle ne peut modifier.

Il est impossible d'empêcher Eve d'écouter discrètement le canal quantique, mais il est possible de le savoir. Par conséquent, la cryptographie quantique ne permet pas d'échanger directement des messages, mais permet l'échange de données aléatoires qui constituent une clef. Si la ligne n'a pas été écoutée, il est alors possible de se servir de la clef pour chiffrer

classiquement le message en utilisant la technique du masque jetable appliquée à une transmission de données binaires, encore appelé *one-time pad* [56].

I.8.1 Distribution quantique de clef

Dans une première partie, nous présenterons le principe du protocole BB84 codant la polarisation ou la phase de photons uniques ou de photons intriqués. Puis nous définirons la sécurité de ce protocole dans les cas idéaux d'une absence totale de bruit sur la ligne et de l'utilisation de composants parfaits. En fin, nous évaluerons la confidentialité d'une transmission utilisant ce protocole face à l'intervention d'un espion.

I.8.2 Le protocole BB84

Le protocole de distribution quantique de clef, élaboré en 1984 par Charles Bennett et Gilles Brassard, permet à deux correspondants d'échanger une clef de chiffrement. De nombreuses réalisations expérimentales utilisant des variables physiques à valeurs discrètes, codées sur des photons uniques, reposent sur l'utilisation de ce protocole [56][57][58]. Alice et Bob disposent d'un canal de transmission quantique (fibre optique, espace libre) et d'un canal public (radio, internet).

I.8.3 Codage sur la polarisation

Alice et Bob adoptent la même convention pour les bases et les symboles Figure 26. Alice transmet à Bob une série de bits choisis aléatoirement afin de constituer une clef de chiffrement unique. Chaque choix de bits est codé par modulation d'un paramètre physique, la polarisation sur un système quantique, un photon unique.

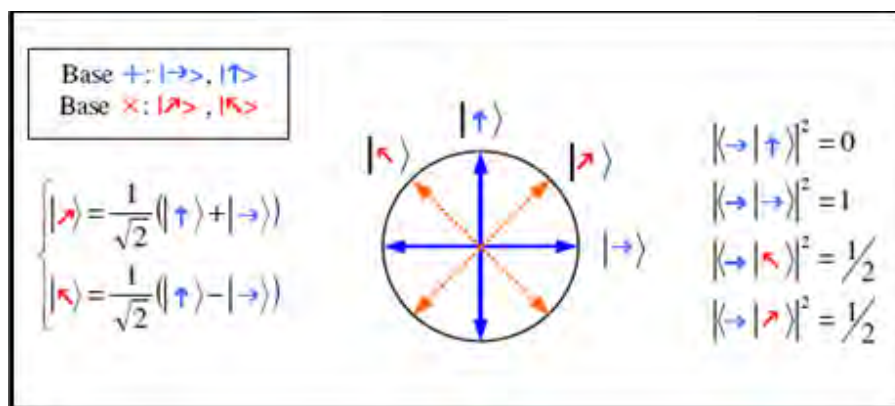


Figure.I.26 Représentation des 4 états de polarisation.

Bob détermine chaque bit transmis en mesurant l'état du photon. Pour assurer la sécurité de cette communication, Alice et Bob utilisent deux bases dites conjuguées, notées + et x, dans lesquelles les vecteurs propres correspondent aux deux symboles notés 0 et 1. Par définition, deux bases conjuguées sont telles que toute mesure d'un photon sur une des bases et codé dans l'autre donne un résultat complètement aléatoire et entraîne la perte de toute information.

Le protocole BB84 nécessite quatre états de codage qui constituent deux bases conjuguées. Chaque état est codé par une polarisation linéaire.

Alice (étape 1)			Bob (étape 2)			Alice et Bob (étape 3)	
choix de base	choix de symbole	état du photon émis	choix de base	résultat de la mesure	clef brute	coïncidence de base	clef finale
+	0	→	x	↖	1		
				↗	0		
			+	→	0	✓	0
x	1	↖	x	↖	1	✓	1
			+	→	0		
				↑	1		
+	1	↑	x	↖	1		
				↗	0		
			+	↑	1	✓	1
x	0	↗	x	↗	0	✓	0
			+	→	0		
				↑	1		

Tableau.I.2. Table de vérité du protocole BB84 (polarisation).

Ce protocole se décompose en trois étapes.

1. Alice choisit aléatoirement l'un des deux symboles (0 ou 1) et l'une des deux bases (+ et x). Elle code ses choix sur la polarisation d'un photon et le transmet à Bob via un canal quantique.

2. Bob choisit aléatoirement une base (+ et x) pour effectuer sa mesure.

Les étapes 1 et 2 sont reproduites plusieurs fois afin qu'Alice et Bob aient une première série de bits. Les bits de Bob étant le résultat d'une mesure effectuée dans une base choisie aléatoirement, ne sont pas identiques à ceux d'Alice. Par conséquent, la série de Bob comporte en principe 25 % d'erreurs, résultant des antis coïncidences de bases et est appelée clef brute (*rawkey*).

3. Sur un canal public, Bob révèle à Alice son choix de base pour chaque photon reçu. Si leurs choix de bases coïncident, Bob déduit de sa mesure le bit transmis par Alice.

Sinon, Alice et Bob écartent le bit correspondant. A la fin de cette étape de réconciliation, Alice et Bob ont en commun une série de bits identiques constituant la clef de chiffrement appelée clef raffinée (*siftedkey*).

Avant l'étape 3, la série de bit de Bob présente un taux d'erreur moyen de 25 % par rapport à celle d'Alice. L'étape de réconciliation (étape 3) permet de ramener en principe le taux d'erreur à 0. En contrepartie, la taille de leur série commune est réduite de moitié par rapport à la série émise par Alice.

I.8.4 Codage sur la phase

L'idée de coder la valeur d'un bit quantique sur la phase d'un photon a été mentionnée pour la première fois par *Bennett*[59] en 1992. Il utilisait alors le protocole B92 nécessitant deux états non orthogonaux. Le codage sur la phase optique d'un photon peut être étendu au protocole BB84 à la condition d'utiliser un système de détection adapté.

A l'émission, le protocole BB84 nécessite deux bases conjuguées, notées A_1 et A_2 . Les vecteurs propres de ces bases codent les deux symboles binaires (0 et 1) et adoptent, dans l'espace des phases, quatre valeurs différentes Figure 27. A la réception, Bob se place dans l'une des deux bases (notées B_1 et B_2) pour effectuer sa mesure Figure 28.

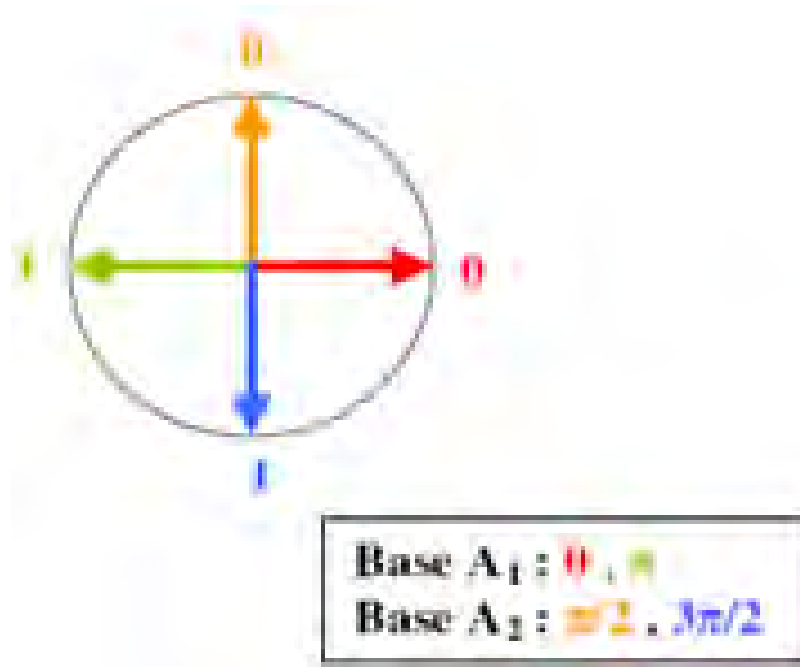


Figure.I.27. Valeur des 4 états de phase à l'émission

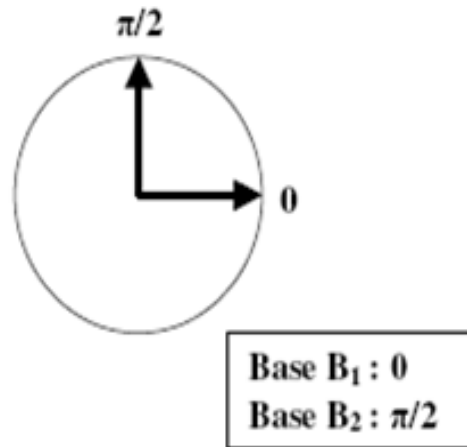


Figure.I.28. : Valeurs des déphasages additifs représentant les bases de réception.

Le fonctionnement du protocole BB84 par codage de phase est identique à celui par codage sur la polarisation.

1. Alice transmet une séquence binaire, résultat d'une suite de choix aléatoires de la base et des symboles. Elle encode chaque bit sur la phase d'un photon.
2. Bob mesure l'état quantique du photon sur une des deux bases qu'il choisit aléatoirement.
3. Puis sur un canal classique, Alice et Bob échangent publiquement leur choix de base définitive. Lorsqu'il y a coïncidence, ils conservent alors les symboles correspondants, constituant ainsi une clef de chiffrement commune.

Le Tableau 3 présente la table de vérité relative au protocole BB84 par codage de phase.

Alice			Bob			Alice et Bob	
choix de base	choix de symbole	ϕ_{Alice}	choix de base	ϕ_{Bob}	$\phi_{Alice+Bob}$	coïncidence	clef finale
A_1	0	0	B_1	0	0	✓	0
			B_2	$\pi/2$	$\pi/2$		
	1	π	B_1	0	π	✓	1
			B_2	$\pi/2$	$3\pi/2$		
A_2	0	$\pi/2$	B_1	0	$\pi/2$		
			B_2	$\pi/2$	π	✓	0
	1	$3\pi/2$	B_1	0	$3\pi/2$		
			B_2	$\pi/2$	0	✓	1

Tableau.I.3 Table de vérité du protocole BB84 (phase).

I.8.5 Codage sur la polarisation de photons intriqués

Le protocole E.P.R. (*Einsten, Podolski, Rosen*) est une variante du protocole BB84 par codage de polarisation. Il nécessite quatre états quantiques distincts. Le canal de transmission du photon entre Alice et Bob est remplacé par un canal ayant en son milieu une source de paires de photons intriqués. Les deux photons intriqués sont émis dans des directions différentes ; l'un vers Alice, l'autre vers Bob [60].

Le fonctionnement de ce protocole suit trois étapes.

1. La source émet une paire de photons intriqués codée dans l'un des quatre états qu'elle choisit aléatoirement (choix aléatoires de la base et du symbole),
2. Alice et Bob mesurent l'état du photon qu'ils reçoivent dans une des deux bases qu'ils choisissent aléatoirement et séparément,
3. Alice et Bob ne conservent leurs mesures que si leurs choix de base de mesure coïncident avec le choix de base de la source.

Source EPR			Alice	Bob	Alice et Bob	
choix de base	choix de symbole	état	choix de base	choix de base	coïncidence des 3 bases	clef finale
+	0	→	+	+	✓	0
			+	×		
	×		+			
	×		×			
1	↑	+	+	✓	1	
		+	×			
×	0	↖	+	+		
			+	×		
×	+					
×	×		✓	0		
1	↗	+	+			
		+	×			
×	+	×	+			
×	×	×	×	✓	1	

Tableau.I.4. Table de vérité du protocole BB84 (EPR).

I.9 Conclusion

La cryptographie quantique exploite les relations d'incertitude de Heisenberg afin d'interdire à un espion d'apprendre quoi que ce soit d'utile sur une transmission d'information. Pour fixer les idées, on appelle habituellement Alice et Bob les personnes qui veulent échanger un message secret, et Eve l'espion. Lorsqu'Eve tente d'intercepter les signaux quantiques envoyés par Alice, elle doit nécessairement les mesurer, ce qui les perturbe. Cette perturbation permet à Alice et Bob de détecter et de quantifier l'attaque d'Eve : plus la transmission entre Alice et Bob est perturbée, plus Eve a pu obtenir d'information. Un traitement des données partagées par Alice et Bob leur permet alors d'en extraire une clé cryptographique parfaitement sûre.

Les principes de la cryptographie quantique sont bien connus depuis 1984 et la proposition de Bennett et Brassard d'un protocole, BB84, fondé sur le codage en polarisation de photons uniques. Cependant, en prouver la sécurité dans des conditions réalistes reste l'objet de nombreuses recherches. Nécessitant l'application de la théorie de l'information aux systèmes physiques.

Le but essentiel est donc de permettre à Alice et Bob d'échanger une clé secrète avec l'assurance que toute écoute de la part d'une tierce personne pourra être détectée. Si cette clé secrète a été correctement transmise, Alice et Bob peuvent l'utiliser en combinaison avec le code de protocole BB84 décrit plus haut, afin d'obtenir un système cryptographique inconditionnellement sûr et ce, même à distance.

Références bibliographiques du chapitre I

- [1] M. Bitbol, “LA MECANIQUE QUANTIQUE COMME THEORIE DES PROBABILITES GENERALISEE,” *E. Klein Y. Sacquin (eds.), Prévision Probab. dans les Sci. Ed. Front.*, 1998.
- [2] N. M. BLIGH, “THE EVOLUTION OF THE NEW QUANTUM MECHANICS,” *Sci. Prog. Twent. Century*, vol. 23, no. 92, pp. 619–632, 1929.
- [3] K. Thapliyal, S. Banerjee, A. Pathak, S. Omkar, and V. Ravishankar, “Quasiprobability distributions in open quantum systems: Spin-qubit systems,” *Ann. Phys. (N. Y.)*, vol. 362, pp. 261–286, 2015.
- [4] C. Ferrie and J. Emerson, “Frame representations of quantum mechanics and the necessity of negativity in quasi-probability representations,” *J. Phys. A Math. Theor.*, vol. 41, no. 35, p. 352001 (11pp), 2008.
- [5] C. Ferrie and J. Emerson, “Framed Hilbert space: Hanging the quasi-probability pictures of quantum theory,” *New J. Phys.*, vol. 11, 2009.
- [6] C. Ferrie, “Quasi-probability representations of quantum theory with applications to quantum information science,” *Reports Prog. Phys.*, vol. 74, no. 11, p. 116001, 2011.
- [7] S. Furuichi and K. Yanagi, “Schrödinger uncertainty relation, Wigner-Yanase-Dyson skew information and metric adjusted correlation measure,” *J. Math. Anal. Appl.*, vol. 388, no. 2, pp. 1147–1156, 2012.
- [8] E. N. Dzhafarov and J. V. Kujala, “Contextuality is about identity of random variables,” *Phys. Scr.*, vol. T163, no. 1, p. 014009, 2014.
- [9] R. Rabelo, C. Duarte, A. J. Lopez-Tarrida, M. T. Cunha, and A. Cabello, “Multigraph approach to quantum non-locality,” vol. 424021, p. 21, 2014.
- [10] A. Khrennikov, “Classical probability model for Bell inequality,” *J. Phys. Conf. Ser.*, vol. 504, no. 1, p. 12019, 2014.
- [11] A. E. Rastegin, “On generalized entropies and information-theoretic Bell inequalities under decoherence,” *Ann. Phys. (N. Y.)*, vol. 355, pp. 241–257, 2015.
- [12] J. F. Koksmá, T. Prokopec, and M. G. Schmidt, “Decoherence in quantum mechanics,” *Ann. Phys. (N. Y.)*, vol. 326, pp. 1548–1576, 2011.
- [13] V. Karakostas, “Nonseparability, Potentiality, and the Context-Dependence of Quantum Objects,” *J. Gen. Philos. Sci.*, vol. 38, no. 2, pp. 279–297, 2007.
- [14] M. Howard, J. Wallman, V. Veitch, and J. Emerson, “Contextuality supplies the ‘magic’ for quantum computation,” *Nature*, vol. 510, no. 7505, pp. 351–355, Jun. 2014.
- [15] W. Heisenberg, “Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik,” *Zeitschrift für Phys.*, vol. 43, no. 3, pp. 172–198, 1927.
- [16] P. Bernays, “Paulette Destouches-Février, Sur les rapports entre la logique et la physique théorique, logique adaptée aux théories quantiques,” *J. Symb. Log.*, vol. 14,

- no. 2, pp. 128–129, 1949.
- [17] G. Kirchmair, F. Zähringer, R. Gerritsma, M. Kleinmann, O. Gühne, A. Cabello, R. Blatt, and C. F. Roos, “State-independent experimental test of quantum contextuality,” *Nature*, vol. 460, no. 7254, pp. 494–497, Jul. 2009.
- [18] S. A. and A. Brandenburger, “The sheaf-theoretic structure of non-locality and contextuality,” *New J. Phys.*, vol. 13, no. 11, p. 113036, 2011.
- [19] X. D. Yu, Y. Q. Guo, and D. M. Tong, “A proof of the Kochen-Specker theorem can always be converted to a state-independent noncontextuality inequality,” *New J. Phys.*, vol. 17, no. 9, pp. 1–10, 2015.
- [20] S. Das, S. Aravinda, R. Srikanth, and D. Home, “Unification of Bell, Leggett-Garg and Kochen-Specker inequalities: A hybrid spatio-temporal inequality,” *Europhys. Lett.*, vol. 1, pp. 1–7, 2013.
- [21] A. Winter, “What does an experimental test of quantum contextuality prove or disprove?,” *J. Phys. A Math. Theor.*, vol. 47, no. 42, p. 424031, 2014.
- [22] I. Arad, “A note about a partial no-go theorem for quantum PCP,” *Quantum Inf. Comput.*, vol. 11, no. 11–12, pp. 1019–1027, 2011.
- [23] E. Maor, “How I got to understand Heisenberg’s Uncertainty Principle.”
- [24] M. a. Man’ko, “Mathematical methods of studying physical phenomena,” *Phys. Scr.*, vol. 87, no. 3, p. 030201, 2013.
- [25] M. E. Goggin, M. P. Almeida, M. Barbieri, B. P. Lanyon, J. L. O’Brien, a G. White, and G. J. Pryde, “Violation of the Leggett-Garg inequality with weak measurements of photons,” *Proc. Natl. Acad. Sci. U. S. A.*, vol. 108, no. 4, pp. 1256–1261, 2011.
- [26] Y. Hasegawa, R. Loidl, G. Badurek, M. Baron, and H. Rauch, “Violation of a bell-like inequality in single-neutron interferometer experiments: Quantum contextuality,” *J. Mod. Opt.*, vol. 51, no. 6–7, pp. 967–972, Apr. 2004.
- [27] M. C. Boscá, “Some Observations upon _ Realistic ‘ Trajectories cance of a mathematical formalism , provided that it is empirically correct , is irrelevant . entific discipline becomes mature , but modern quantum physics continues to reject,” *Theor. Rev. Teoría, Hist. y Fundam. la Cienc.*, vol. 28, no. 76, pp. 45–60, 2013.
- [28] D. Bohm, “A Suggested Interpretation of the Quantum Theory in Terms of _Hdden‘ Variables. I,” *Phys. Rev.*, vol. 85, no. 2, pp. 166–179, Jan. 1952.
- [29] Y. Aharonov and D. Bohm, “Significance of Electromagnetic Potentials in the Quantum Theory,” *Phys. Rev.*, vol. 115, no. 3, pp. 485–491, Aug. 1959.
- [30] A. Einstein, B. Podolsky, and N. Rosen, “Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?,” *Phys. Rev.*, vol. 47, no. 10, pp. 777–780, May 1935.
- [31] B. Dopfer, “Zwei experimente interferenz von zwei photonen zuständer ein Heisenbergmikroshop und pendellönsung,” *Thèse Dr. Univerité Innsbruck*, 1998.
- [32] R. Coquereaux, “Classical and quantum polyhedra: A fusion graph algebra point of

- view,” *Arxiv Prepr. hep-th/0105239*, p. 24, 2001.
- [33] F. K. Li and R. M. Goldstein, “Studies of multibaseline spaceborne interferometric synthetic aperture radars,” *IEEE Transactions on Geoscience and Remote Sensing*, vol. 28, no. 1. pp. 88–97, 1990.
- [34] Y. C. Eldar and A. V Oppenheim, “Quantum signal processing,” *IEEE Signal Processing Magazine*, vol. 19, no. 6. pp. 12–32, 2002.
- [35] Y. C. Eldar, “Quantum signal Processing,” *Ph.D MIT*, 2001.
- [36] E.Knill, R.Laflamme, and et al H.Barnum, *Introduction to Quantum Information Processing*. 2011.
- [37] F. Nielsen and R. Nock, “Quantum Voronoi diagrams and Holevo channel capacity for 1-qubit quantum states,” *2008 IEEE International Symposium on Information Theory*. pp. 96–100, 2008.
- [38] H. F. Wang, J. J. Wen, A. D. Zhu, S. Zhang, and K. H. Yeon, “Deterministic CNOT gate and entanglement swapping for photonic qubits using a quantum-dot spin in a double-sided optical microcavity,” *Phys. Lett. Sect. A Gen. At. Solid State Phys.*, vol. 377, no. 40, pp. 2870–2876, 2013.
- [39] D. Maslov, S. M. Falconer, and M. Mosca, “Quantum Circuit Placement: Optimizing Qubit-to-qubit Interactions through Mapping Quantum Circuits into a Physical Experiment,” *2007 44th ACM/IEEE Design Automation Conference*. pp. 962–965, 2007.
- [40] J. Xu, “Analytical expressions of global quantum discord for two classes of multi-qubit states,” *Phys. Lett. A*, vol. 377, no. 3–4, pp. 238–242, 2013.
- [41] T. Schulte-Herbruggen, U. Sander, and R. Zeier, “Symmetry principles in quantum system theory of multi-qubit systems made simple,” *Communications, Control and Signal Processing (ISCCSP), 2010 4th International Symposium on*. pp. 1–5, 2010.
- [42] A. Holleczek, O. Barter, P. B. R. Nisbet-Jones, J. Dilley, and A. Kuhn, “Quantum networking with time-bin encoded qu-d-its using single photons emitted on demand from an atom-cavity system,” *Lasers and Electro-Optics Europe (CLEO EUROPE/IQEC), 2013 Conference on and International Quantum Electronics Conference*. p. 1, 2013.
- [43] P. B. and M. G. and G. Adesso, “Asymptotically optimal quantum channel reversal for qudit ensembles and multimode Gaussian states,” *New J. Phys.*, vol. 14, no. 11, p. 113041, 2012.
- [44] M. Neeley, M. Ansmann, R. C. Bialczak, M. Hofheinz, E. Lucero, A. D. O’Connell, D. Sank, H. Wang, J. Wenner, A. N. Cleland, M. R. Geller, and J. M. Martinis, “Emulation of a Quantum Spin with a Superconducting Phase Qudit,” *Science (80-.)*, vol. 325, no. 5941, pp. 722–725, Aug. 2009.
- [45] D. S. Wang and B. C. Sanders, “Quantum circuit design for accurate simulation of qudit channels,” *New J. Phys.*, vol. 17, p. 043004, 2015.

- [46] H. Anwar, B. J. Brown, E. T. Campbell, and D. E. Browne, “Fast decoders for qudit topological codes,” *New J. Phys.*, vol. 16, 2014.
- [47] P. B. R. Nisbet-Jones, J. Dille, A. Holleczek, O. Barter, and A. Kuhn, “Photonic qubits, qutrits and ququads accurately prepared and delivered on demand,” *New J. Phys.*, vol. 15, p. 053007, 2013.
- [48] H. D. Zeh, “On the interpretation of measurement in quantum theory,” *Found. Phys.*, vol. 1, no. 1, pp. 69–76, 1970.
- [49] W. Zurek, “Decoherence and the transition from quantum to classical,” *Séminaire Poincaré*, pp. 1–22, 2005.
- [50] M. Schlosshauer, *Decoherence and the Quantum-To-Classical Transition*. 2007.
- [51] G. Benenti, G. Casati, and G. Strini, *Principles of Quantum Computation and Information*. 2004.
- [52] J. P. Singh, “Quantum Entanglement – A Primer,” *African J. Math. Phys.*, vol. 7, pp. 71–98, 2009.
- [53] R. M. and R. Dandoloff, “Geometry of entangled states, Bloch spheres and Hopf fibrations,” *J. Phys. A: Math. Gen.*, vol. 34, no. 47, p. 10243, 2001.
- [54] S. Severini, “The Lovász ϑ -function in Quantum Mechanics,” *UCL Semin. Oxford*, 2013.
- [55] I. Peterson, “Bits of uncertainty: Quantum security,” *Sci. News*, vol. 137, no. 2, pp. 342–343, 1990.
- [56] P. D. Townsend and I. Thompson, “A Quantum Key Distribution Channel Based on Optical Fibre,” *J. Mod. Opt.*, vol. 41, no. 12, pp. 2425–2433, Dec. 1994.
- [57] C. Gobby, Z. L. Yuan, and A. J. Shields, “Unconditionally secure quantum key distribution over 50km of standard telecom fibre Unconditionally secure quantum key distribution over 50km of standard telecom fibre,” vol. 40, no. 25, pp. 1603–1605, 2004.
- [58] 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 - At. Mol. Opt. Plasma Phys.*, vol. 30, no. 1, pp. 143–148, 2004.
- [59] B. C. Jacobs and J. D. Franson, “Quantum cryptography in free space,” *Opt. Lett.*, vol. 21, no. 22, pp. 1854–1856, Nov. 1996.
- [60] J. D. Franson and H. Ilves, “Quantum Cryptography Using Polarization Feedback,” *J. Mod. Opt.*, vol. 41, no. 12, pp. 2391–2396, Dec. 1994.

CHAPITRE

II

Chapitre II Les systèmes optiques à Accès multiple par répartition de code

II.1 Introduction

Dans l'histoire au début des années 80 c'est l'étalement de spectre par accès multiple par répartition en code sans fil (CDMA), la technologie a été initialement développée pour les applications de télécommunications militaires pour augmenter la transmission de l'information de sécurité robuste. Le succès dans le CDMA a inspiré l'énorme intérêt pour la recherche dans le CDMA optique (OCDMA). Principalement, la capacité de systèmes de télécommunication optique peut atteindre jusqu'à 10 Tbps dû à la disponibilité du porteur optique de fréquence énorme. Cependant, en 1995, la réalisation de la communication optique est limitée à 10 Gbps parce qu'il ya un problème avec les dispersions, les non-linéarités et goulot d'étranglement dans les composants électroniques. Aujourd'hui, la capacité de transmission des canaux optiques multiples peut être prolongée au-delà 1 Tbps [1]. La fibre optique est une technologie prometteuse qui devrait répondre à la demande de bande passante des futurs réseaux d'information grâce à l'optimisation de la bande passante disponible par flux de données à faible taux de multiplexage sur fibre optique. A cet effet, les schémas d'accès multiples; OCDMA, Accès multiple à répartition dans le temps (TDMA) et la division de longueur d'onde d'accès multiple (WDMA), sont requis pour le flux de données de multiplexage et de démultiplexage.

L'OCDMA est un domaine de recherche émergent qui offre de nombreux avantages par rapport aux autres techniques d'accès multiple existants tels que TDMA et WDMA. L'OCDMA fonction basée sur une transmission asynchrone où la transmission peut être exécutée à tout moment sans aucune coordination nécessaire de synchronisation. Il a une capacité de rejet d'interférence de supprimer l'interférence à bande étroite. Avec l'amélioration de la sécurité de réseau, le signal original de données est élargi dans le domaine fréquentiel sans acquérir la puissance dans le domaine fréquentiel en conséquence la puissance de la densité spectrale est basse et difficile à être détectée. Il offre également la grande utilisation de largeur de bande efficace, la flexibilité des réseaux d'accès à grande vitesse avec le bas accès de latence, la tâche dynamique de largeur de bande, la capacité douce sur demande, la

commande de réseau simplifiée et la commande accrue de qualité du service de flexibilité [2-3].

Récemment l'intérêt énorme de recherches dans OCDMA a été inspiré par l'avancée récente dans la technologie photonique et l'intégration photonique. En plus de celle les avancées dans le réseau optique permettent la réalisation de la technologie aux utilisateurs. Au contraire, l'opération du système TDMA exige la synchronisation et la commande centralisée où les utilisateurs sont assignés avec la fente d'instant spécifique. Cependant dans le système OCDMA, les utilisateurs peuvent opérer asynchrone et accéder au réseau indépendamment. Le WDMA offre la grande largeur de bande passante. On le prévoit que le futur réseau optique d'accès exige un système très évolutive et la flexibilité dont WDMA et TDMA est négligeable. TDMA limite l'exécution de système due à la disponibilité de l'intervalle de temps. L'avance en amplificateurs à fibre dopée à l'erbium (EDFA) et le filtre augmente la disponibilité de la longueur d'onde, de toute façon le nombre d'utilisateurs sont encore limitées. L'avantage d'OCDMA est qu'il offre une disponibilité énorme des codes à l'élargissement, de plus que le besoin. OCDMA est le candidat le plus attirant comparé à TDMA et à WDMA. Ce sera une solution de technologie viable pour la future télécommunication optique.

Il y a deux catégories de schème OCDMA ; OCDMA incohérent et OCDMA cohérent. L'OCDMA Incohérent manipule la puissance dans le codage et le processus de décodage et écarté la cohérence de la source lumineuse. L'OCDMA cohérent essaye de coder des signaux en changeant la phase de la source lumineuse même si elle est difficile à réaliser. Cependant les résultats du OCDMA cohérent dans de meilleures performances se comparent à incohérent à son coût et à la complexité élevés.

L'OCDMA rencontre plusieurs défis au niveau d'exécution. Les défis sont dus à l'interférence d'accès multiple (MAI) des morceaux chevauchés, l'augmentation des nombres d'utilisateurs simultanés, bas débit binaire afin de compenser des augmentations de longueur et de poids de code. OCDMA on peut implémenter dans le codage unidimensionnel (1-D) et bidimensionnel (2-D) par le domaine spatial, le domaine spectral ou le domaine spectral-spatial simultanément, et l'hybride. L'inconvénient conventionnel du système de 1-D OCDMA est cette exigence de débit de données pour envoyer certaine quantité de données est élevé. Dans la comparaison le même montant de données on peut envoyer par le 2-D OCDMA système avec au bas débit de données. Les divers résultats désignant les développements et

les réalisations sont la capacité de réseau dans la limite de la cardinalité élevée, code compatible avec de diverses demandes de largeur de bande, sortie et acceptable minimum d'erreur BER. Les points difficiles finaux dans la construction du système OCDMA sont ; l'interférence élevée entre les sources d'incohérence à l'MAI de récepteur de photo détecteur et l'élimination de la phase induit d'intensité de bruit (PIIN)[4]. Il est essentiel de rechercher de nouvelles implémentations d'OCDMA qui peuvent répondre à la performance attendue de manière simple et efficace. En termes de propriétés de corrélation, l'autocorrélation maximum, la corrélation croisée minimum et l'architecture de système sont le but de l'étalement de spectre à séquence [5]. Le choix faisable des composants de réseau est essentiel aussi. La grande longueur de code et la basse propriété de corrélation croisée peuvent améliorer MAI performance de système, le taux d'erreur bits (BER) et le débit.

De divers types d'ordres de signature ont été développés pour 1-D utilisant les algorithmes qui peuvent adapter un grand nombre d'utilisateurs [6]. Cependant, la performance du système est limitée par le BER et le MAI. Le code 1-D OCDMA nécessite une grande longueur des séquences de signature avec une forte corrélation croisée et de poids pour surmonter la dégradation des performances du système lié au BER et MAI[6-7]. La réalisation du système OCDMA avec des dispositifs optiques et optoélectroniques peu coûteux devient difficile, l'optoélectronique devient le goulot d'étranglement Il est fortement souhaitable d'assurer une transmission sans interférence de bruit pour un nombre plus élevé d'utilisateurs au détriment du petit rapport signal-bruit (SNR) pénalité.

II.2.1 Multiplexage dans le domaine optique

Aujourd'hui, il y a un besoin croissante des technologies permettant à plusieurs utilisateurs partageant les mêmes spectres de fréquences grâce à l'utilisation de la bande passante de la fibre où de nombreux canaux optiques peuvent être transmis simultanément sur une fibre. Figure.II.1 illustre la représentation des trois techniques d'accès multiple, où chaque utilisateur occupe les ressources de différentes couleurs. Les systèmes d'accès multiples sont classés en trois types;

- ✓ Accès Multiple Par Répartition Dans Les Longueurs D'onde (WDMA),
- ✓ accès multiple par répartition dans le temps (TDMA) et
- ✓ Accès multiple par répartition décodés optiques(OCDMA).

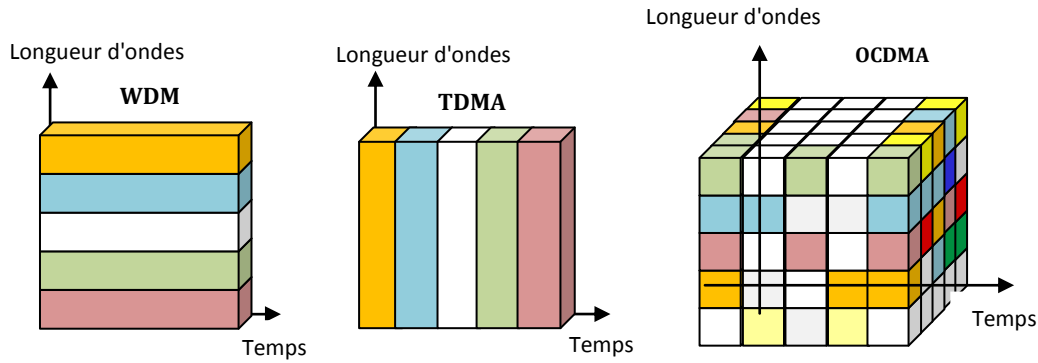


Figure.II.1 système d'accès multiple; WDMA, TDMA et CDMA.

II.2.1.1 Accès Multiple Par Répartition Dans Les Longueurs D'onde(WDMA)

La capacité du lien de fibre à un accès multiple par répartition dans les longueurs d'onde peut être augmentée en occupant plus de porteurs ou de longueurs d'onde. Dans WDMA, la bande passante est divisée en plusieurs petits canaux de longueur d'onde lorsque le canal optique utilise une bande passante étroite inférieure à 100 GHz autour de la fréquence centrale ou de la longueur d'onde [8-9]. WDMA utilise des lasers pour transmettre de multiples longueurs d'onde sur une seule fibre optique. Chaque canal est transmis avec une longueur d'onde distincte et classifiée en utilisant un filtre optique. Les utilisateurs seront également affectés à des longueurs d'onde spécifiques de la bande passante. En conséquence ceci exige des amplificateurs et des filtres optiques que fonctionnent à une longueur d'onde prolongée [10].

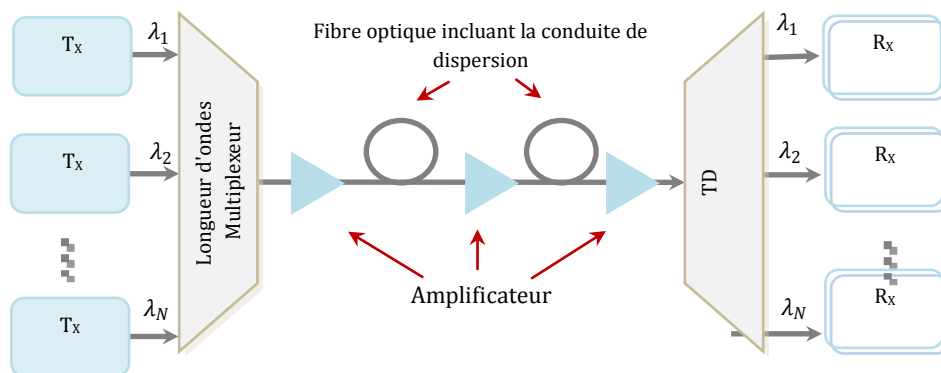


Figure.II.2 Réseaux d'accès multiple par répartition dans les longueurs d'onde(WDMA).

Les lasers sont modulés à l'extérieur avant que le multiplexeur de longueur d'onde est combiné dans tous les canaux de longueur d'onde sur une seule fibre. La synchronisation ou le contrôle de synchronisation ne sont pas nécessaires en raison de la nature de WDMA. Pendant

aucune transmission de données, la transmission continue de fréquence va être perdue. Au niveau du récepteur, le démultiplexeur sépare la longueur d'onde différente et convertit au domaine électronique. Les utilisateurs avec des longueurs d'onde assignées transmettront sans interruption comme sur la figure.II.2. La capacité du WDMA peut être améliorée en augmentant la longueur d'onde cependant ceci est soumis au 10^{-9} BER seuil d'erreur admissible.

Chaque canal de longueur d'onde peut avoir un format et une vitesse distincts de modulation. Matrice et le filtre accordable peuvent être utilisés dans le WDMA. Acousto-optique, cristaux liquides et la fibre à réseau de Bragg sont des exemples de filtres accordables [3], [11-12]. La capacité de liaison des fibres peut être augmentée en occupant plusieurs transporteurs et une longueur d'onde qui nécessite des amplificateurs et des filtres optiques pour fonctionner dans la longueur d'onde prolongée [10]. La capacité de WDMA peut être augmentée en utilisant Dense WDM (DWDM) avec l'espacement de canal réduit. Par conséquent, cela nécessite un filtre optique pointu, la longueur d'onde des composants stables, l'amplificateur optique à gain plat et fibre optique capables d'adapter au nombre élevé de canaux sans distorsion. Le routage de longueur d'onde est une nouvelle dimension dans la commutation de canaux DWDM [13], où la diaphonie interférométrique joue un rôle important dans la réalisation des connexions croisées basées sur l'espace et la longueur d'onde. Le routage de longueur d'onde est le facteur de limitation dominant de la flexibilité de réseau qui dicte la taille et la flexibilité de commutation.

II.2.1.2 Accès Multiple Par Répartition Dans Le Temps

L'accès multiple par répartition dans le temps (TDMA) alloue la bande passante de chaque canal avec intervalle de temps assigné et précis, où ils entrelacent avec intervalle de temps d'autres canaux. TDMA exige la synchronisation appropriée ou la commande de synchronisation due à des utilisateurs partage la bande passante dans le domaine fréquentiel Figure.II.3. Le nombre de canaux de bande passante est petit en conséquence l'interférence est négligeable.

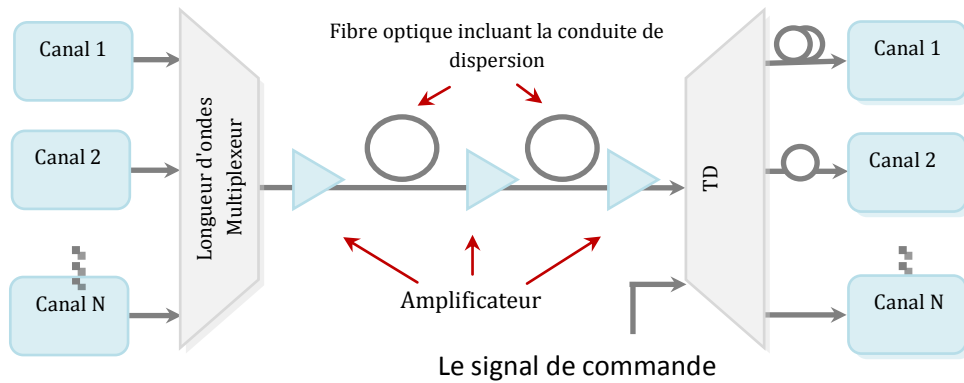


Figure.II.3 Réseaux d'accès multiple par répartition dans le temps (TDMA).

Les dernières transmissions et le multiplexage pour les signaux à grande vitesse utilise la hiérarchie numérique synchrone (SDH) [14]. TDMA optique (OTDMA) peuvent être classifiés dans la topologie d'émission ou de commutation optique [15]. Réseau de diffusion n'offre aucune commutation dans le réseau où la commutation se produit par l'émetteur accordable et le récepteur réseau précédent. Le réseau de commutation optique exécute l'opération de commutation au sein du réseau pour produire des services à commutation de paquets à des débits binaires élevés [16]. Le multiplexage dans le temps est exécuté dans le domaine électrique, avant la conversion électrique-optique (E/O). Le démultiplexage est effectué après la conversion opto-électrique (O/E). Le goulot d'étranglement électronique réside dans la conversion électrique-optique (E/O) et (O/E) où les dispositifs doivent fonctionner au maximum multiplex au débit binaire. Le goulot d'étranglement électronique est résolu en plaçant le (E/O) et (O/E) dans des canaux en bande de base [17]. Alors même que CDMA offre le nombre élevé de l'adresse ou des utilisateurs, les natures temps-périodiques du système dictent la performance du système. Un autre inconvénient de TDMA est que l'intervalle de temps et l'opération de synchronisation exigent le système avec la commande fortement centralisée.

II.2.1.3 Accès Multiple Par Répartition De Codes Optique (OCDMA)

Récemment, OCDMA a attiré un énorme intérêt de la recherche dans l'application de ces techniques dans les réseaux OCDMA. L'idée d'appliquer le concept sans fil de CDMA dans OCDMA retourne aux années 80 [2], [18-19]. OCDMA est origine à partir à techniques de communication à étalement de spectre [20]. Où chaque utilisateur est assigné un code unique pour la modulation de signal et transmet l'information au-dessus d'un réseau fibre-optique. Où seulement le récepteur destiné avec la connaissance spécifique de code peut rechercher l'information codée. Traditionnellement, nous maximisons l'utilisation du signal

utile avec une bande passante minimale. Cependant, dans le spectre étalé, le concept de bande passante l'utilisation est largement répandue.

Ce domaine de recherche émergent attire un énorme intérêt de la recherche. Il offre une large bande passante de la fibre optique et la flexibilité des réseaux d'accès de haute vitesse pour satisfaire la demande de bande passante dans les réseaux futurs. En multiplexant des données à faible débit des flux en fibre optique, le nombre élevé d'abonnés peut être accueilli. L'OCDMA a certains avantages uniques tels que; la transmission asynchrone avec le bas accès de latence, l'affectation dynamique de bande passante, la souple capacité à la demande, le protocole d'accès aléatoire est simultanée, le contrôle de réseau simplifié, une utilisation efficace de la bande passante, l'augmentation de la qualité du contrôle des services de flexibilité [2] et la nature de l'étalement de spectre OCDMA fournit la sécurité de transmissions dans l'environnement flexible à utilisateurs multiples [21]. Efficaces systèmes d'accès multiple sont exigés pour la transmission simultanée du nombre élevé des utilisateurs au-dessus du milieu existant de transmission [22].

Dans TDMA et WDMA les utilisateurs utilisent le réseau en assignant le temps et le spectre respectivement. Les utilisateurs sont alors multiplexés. En revanche, OCDMA est un multiplexage de plusieurs techniques d'accès où les différents utilisateurs accèdent en même temps avec des séquences de codes distincts. Un schéma générique de réseau OCDMA où un signal optique modulé est codé au codeur optique avant d'appliquer au réseau OCDMA avec N paires d'émetteurs-récepteurs ($N \times N$) du coupleur en étoile et décodeur au décodeur et à la diffusion vers des nœuds. L'encodeur convertit le signal optique en une faible intensité, la propagation du temps, le bruit-comme, la forme d'onde est permet à beaucoup d'utilisateurs d'être transmis simultanément pendant la même fibre optique. Au niveau du récepteur, les différentes séquences de code des signaux émis par les différents utilisateurs sont décodées. Les données désirées sont récupérées par décodage où les codes attribués sont corrélés avec le signal reçu. En conséquence, le pic d'auto-corrélation du signal récupéré est produit pour distinguer les flux de données d'interférences provenant d'autres utilisateurs.

La capacité de transmission de TDMA et WDMA est déterminé par la disponibilité des intervalles de temps, de systèmes et des canaux de longueur d'onde. Cependant, en OCDMA le nombre d'utilisateurs simultanés peut être augmenté au maximum par l'affectation de code flexible en permettant une limite souple sur la capacité. Le code des séquences est un concept de multiplexage étend l'utilisation de la bande passante du spectre de

communication, mais les limites électroniques sont possibles à réaliser[23]. Contrairement à TDMA et WDMA, l'OCDMA a un avantage de supporter des débits de données variables à l'environnement de la circulation plantureuse dans une même infrastructure de réseau.

L'OCDMA occupe beaucoup de dispositifs uniques et donne un avantage par rapport aux autres arrangements. Un protocole d'accès asynchrone permet à OCDMA d'être aléatoirement et simultanément accessible sans synchronisation temporelle. L'OCDMA n'exige aucun arrangement de synchronisation comme TDMA. Une allocation dynamique de bande passante et souple capacité à la demande rendent le contrôle de longueur d'onde flexible, et en ajoutant et en supprimant les abonnés facilement. Par rapport à TDMA, OCDMA technique d'accès multiple permet simultanément d'évaluer la largeur de bande sans exiger le traitement à grande vitesse de donnée électronique de circuits. En termes d'évolutivité, OCDMA peut accueillir un plus grand nombre d'utilisateurs par rapport à TDMA ou WDMA. Particulièrement dans les 2-D systèmes de longueur d'onde-temps où les deux dimensions peuvent être exploitées pour augmenter plus loin l'exécution de système. Les techniques multi proportion OCDMA permettent aux canaux de taux de bits faibles et élevés appliqués sur le même réseau d'OCDMA. Cela peut répondre à la demande actuelle de débit binaire variable.

L'architecture décentralisée est un protocole sans contrôle de réseau centralisé. Une auto-routage est un code avec les utilisateurs affectés où la bande passante est utilisée efficacement. Ceci réduit l'algorithme de routage complexe également dans d'autres techniques d'accès multiple.

Les OCDMA possèdent la sécurité élevée de l'information, les données de l'information sont protégées dans le milieu de transmission physiquement et au niveau de code. OCDMA est exempt des collisions et des résultats de paquet dans des latences très basses. L'envoi d'informations de données en utilisant des codes différents protège l'indiscret d'intercepter les données d'information sans connaissance du code utilisé. Cependant, pour un seul utilisateur actif est en réseau, il n'y a aucune garantie de sécurité de la couche physique d'être protégée. Grâce à un code de photodétecteurs la bande limitée peut être décodée.

La sécurité peut être améliorée par longueur d'onde élevée et des temps séquences de code par lequel la largeur de bande spectrale chip unique est réduite. En comparaison, la sécurité de TDMA et WDMA exige le cryptage au niveau électrique [22-23]. Elles peuvent être classifiées dans deux types basés sur le mécanisme où le signal optique est codé et décodé

; Le système d'OCDMA est cohérent et incohérent. Le tableau suivant résume la comparaison entre les trois schémas: TDMA, WDMA et CDMA.

Table.II.1 Comparaison de Schémas Commun de L'Access Multiple optique

Schémas d'accès multiples	Avantages	Inconvénients
1. TDMA	<ul style="list-style-type: none"> a. canaux consacrés fournis b. haut débit c. accès déterministes 	<ul style="list-style-type: none"> a. Synchronisation précise nécessaire b. Pas efficace du trafic en rafales c. La bande passante gaspillée d. Canal pas utilisé efficacement e. Performance se dégrade avec le nombre d'utilisateurs simultanés
2. CDMA	<ul style="list-style-type: none"> a. Utilisateurs simultanés acceptés b. accès Asynchrones c. Aucun retard ou l'ordonnancement d. Efficacité élevée de largeur de bande e. Efficace pour le trafic en rafales. f. canaux consacrés fournis 	<ul style="list-style-type: none"> a. Performance se dégrade avec le nombre d'utilisateurs simultanés
3. WDMA	<ul style="list-style-type: none"> a. canaux consacrés fournis 	<ul style="list-style-type: none"> a. diaphonie de canal b. Canal au repos la plupart du temps c. effets non linéaires d. Faible efficacité de la bande passante

II.2.2 Types De CDMA Optique

Le système optique CDMA (OCDMA) se compose de deux catégories de base, à savoir cohérents [24] et non cohérents[20], [25], qui est également connu sous le nom OCDMA positif, tandis que le système CDMA tout-optique est désigné comme un système incohérent.

II.2.2.1 Systèmes OCDMA Cohérent

Dans le procédé de codage qui comprend l'amplitude et la phase, la forme complexe du champ optique est utilisée. Dans le système OCDMA cohérent, la phase est cruciale dans sa conception et dans les propriétés de code. Dans cette catégorie OCDMA, un ensemble de lignes à retard optiques et déphaseurs sont utilisés dans une technique. Le système optique cohérent CDMA peut être l'une des parties ou tout-optique. Dans le cas du système optique précédemment, pour moduler la porteuse optique (par exemple, modulation par changement de phase (PSK)), les valeurs de la chip sont utilisées, tandis que la séquence de la chip est produite électroniquement. De même, le récepteur optique produit la séquence de chip électrique qui est également identifié électroniquement. Retardé ligne-basé à séquence directe OCDMA cohérente et la propagation de temps OCDMA sont deux instances des systèmes de OCDMA cohérents.

Ligne à Retard basée sur CDMA optique Cohérent à Séquence Direct

Le premier type de systèmes OCDMA cohérents est connu comme la ligne à retard basée sur CDMA optique cohérent à la séquence direct. La figure.II.4 ci-dessous montre que dans ce type, chaque impulsion est modulée par la valeur des données verrouillées on-off qui est ensuite divisée en sous-impulsions le long des chemins optiques distingués.

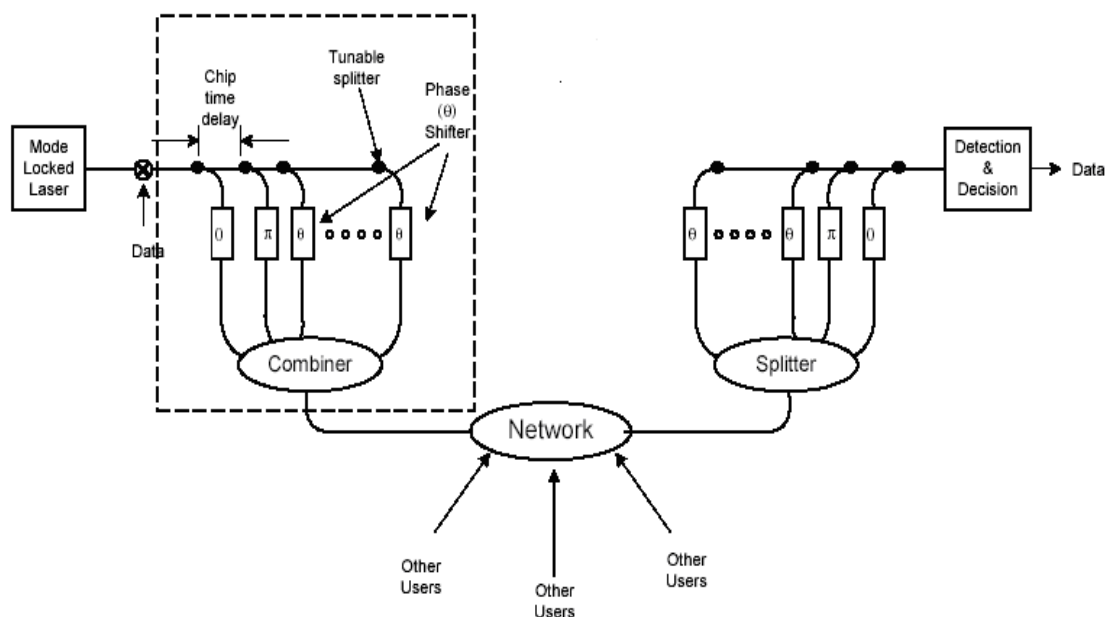


Figure.II.4 ligne à retard basée sur CDMA optique cohérent à séquence direct

Toutes les sous-impulsions accumulées par un combineur ou un coupleur passif sont placées dans la même fibre. Pour s'assurer que tous ces sous-impulsions peuvent être mises correspondants à un code prédéterminé ou modèle, les longueurs de ces chemins optiques sont dimensionnées.

Un arrangement identique est accumulé au récepteur afin d'exiger un signal codé pour l'utilisateur. Le récepteur peut avoir nécessité de plusieurs cruciales les opérations de traitement compliqué une fois que le signal est décodé. Cette complexité est principalement causée par l'incapacité de l'électronique pour faire un ensemble de traitement de très grande vitesse nécessaire pour finaliser l'opération de réception. Pour décider de la valeur du bit de données, le signal décodé doit être comparé à un niveau de seuil. Cependant, cette technique présente certains inconvénients qui comprennent la nécessité d'une synchronisation et elle est également très coûteuse en raison de la source laser.

L'étalement temporel CDMA optique

La Figure.II.5 affiche le système de travail de l'étalement temporel CDMA optique qui a été développé par Weiner au début des années 1990 [26-27], [2]. Un mode Verrouillé laser boucle équipé d'une large bande passante cohérente est nécessaire pour permettre que cette technique fonctionne. En même temps, ceci est la première fois que l'axe des fréquences utilisées en tant que ressource de codage. Le (OOK) la modulation par les données binaires sont utilisés pour moduler la sortie du laser avec la lumière focalisée sur un réseau de Bragg utilisé pour séparer les fréquences ou longueurs d'onde des composants de la lumière. La phase de chaque composante spectrale est ensuite décalée en utilisant un programmable Modulateur à cristaux liquides (LCM) masque de phase basé sur le code bipolaire prédéfini. La procédure est terminée quand la lumière accumulée est injecté dans la fibre, après que les composantes spectrales séparées sont combinées par le second réseau de diffraction de Bragg. Cet agencement d'un masque de phase, des deux objectifs et des réseaux de diffraction est appelé un diagramme 4-F (Fourier), est utilisé dans l'impulsion de mise en forme des applications dans la classification OCDMA. En outre, les ultra-courtes impulsions optiques sont requises dans l'un des exemples où 62 impulsions femto secondes sont utilisées pour obtenir un haut débit de données. En outre, les ultra-courtes impulsions optiques sont requises dans l'un des exemples où 62 impulsions femto-secondes sont utilisées pour obtenir un haut débit de données. Ceci est réalisé en utilisant une longueur de fibre à dispersion décalée qui est appropriée pour l'utilisation dans l'emplacement particulier.

En raison de leur simplicité et facile à utiliser, la modulation d'intensité et la détection directe sont proposées comme les systèmes OCDMA les plus appropriés. Cette intensité contribue aux valeurs positives du signal optique et, par conséquent, amène les codes bipolaires orthogonaux peu convenables pour être utilisés dans les systèmes sans fil de CDMA. Ce fait mène à la recherche de codes unipolaires qui possèdent une orthogonalité supérieure.

Système à Séquence Directe

L'une des propositions CDMA optique les plus anciennes et renommées est le DS-SS-SSB incohérente. Il a été le principal objectif d'un corps significatif de recherches pendant au moins quinze années. Des lignes à retard à prises ont été utilisées dans l'ancienne architecture de codeur [21],[18], [27], comme illustré sur la Figure.II.6a. Ce système fonctionne lorsque les signaux des données optiques entrent dans le codeur sous la forme de trains d'impulsions courtes modifiées dans le format OOK. Chaque élément à retard va envoyer une sous-impulsion de chip à partir de l'impulsion de bit d'incident dans une position temporelle déterminée par la longueur de ligne correspondante, lorsque la valeur de données est 1. Dans ce système, le poids du code est équivalent au nombre de lignes à retard dans le codeur (le nombre de ceux dans le code).

Lorsque le processus de codage traverse les coupleurs d'entrée et de sortie, une double division de puissance se produit, conduisant à une perte significative. Par conséquent, pour résoudre ce problème de pénalité de puissance, un réseau de contacts a été inventé et proposé Figure.II.6b. Néanmoins, les deux architectures interdisent la reconfiguration, car ils acceptent seulement des codes fixes. Par conséquent, seul un réseau particulier d'échelle Figure.II.6c, dont ses coupleurs sont substitués avec un 2: 2 commutateurs cross/bar, permet une telle reconfiguration fournit une meilleure conservation de puissance.

Le récepteur décodeur et le codeur sont identiques dans leurs caractéristiques, mais les fonctions antérieurement inversées. Pour permettre la chip-composantes du signal à passer par le même chemin, les chips impulsions reçues à l'avance sont retardées. Par conséquent, un temps-porte rapide est nécessaire parce que les impulsions de l'émetteur souhaité sont superposées dans la même durée de chip.

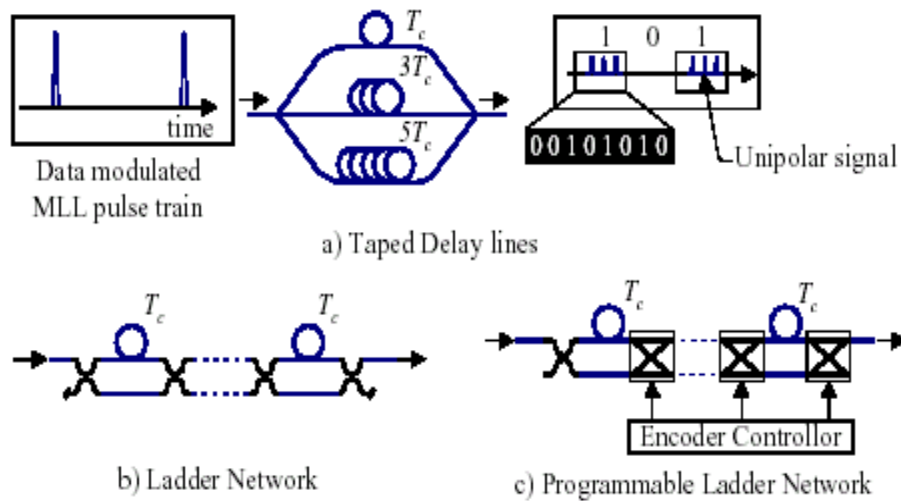


Figure.II.6 Dispositifs Codage / Décodage DS-CDMA [28]

Afin de minimiser le bruit de distraction, les codes unipolaires spéciaux destinés à être long avec un faible poids à un niveau acceptable, sont proposés pour être utilisés dans ce système. Les codes proposés ne sont pas orthogonaux parce que la valeur positive de l'intensité est modulée. À ce jour, plusieurs groupes importants de codes ont été suggérés comprenant la famille OOC [21], [18], [27], [24], [29], qui a été le premier à être proposé, et un autre groupe connu sous le nom de prime séquence codes [30-31]. Habituellement, les codes mentionnés ci-dessus sont symbolisés par $(n, w, \lambda_a, \lambda_c)$, avec n, w, λ_a et λ_c représentant respectivement la longueur, le poids du code, le lobe latéral maximum dans la fonction d'autocorrélation, ainsi que la valeur maximale de la fonction de corrélation croisée.

Néanmoins, en raison de la nécessité de codes longs ayant un poids faible, le système DS-CDMA est considéré comme inefficace. Dans son opération, s'ajoute le nombre d'utilisateurs actifs simultanément qui va certainement exiger des codes plus longs, menant à la perte de plus grande puissance. D'autre part, la réduction du bruit d'interférence est possible seulement quand le poids du code est réduit, ce qui diminue malheureusement, le rapport signal sur bruit, menant à une dégradation de la performance globale du système.

✚ Incohérence de L'intensité Spectrale du Code du Système CDMA Optique

Ce système OCDMA particulier a été démontré par Zaccarin et KAVEHRAD [24], [29]. Aussi bien le système OCDMA et le système CDMA de codage de phase spectrale cohérente possèdent la même conception d'encodeur et de décodeur. Cependant, un masque

d'amplitude qui permet seulement des composantes de fréquences particulières à passer par est utilisée au lieu du modulateur programmable liquide réseau de phase cristalline du codeur pour le codage spectral de phase cohérente. La figure.II.7 illustre l'utilisation de la source lumineuse dans la source de lumière incohérente de la bande passante large, et la diode électroluminescente (LED) ou une émission spontanée amplifiée (ASE) source d'émission peut également être utilisée. Cette source de lumière produit le signal optique qui est modulé en OOK avec les données binaires avant le codage du signal.

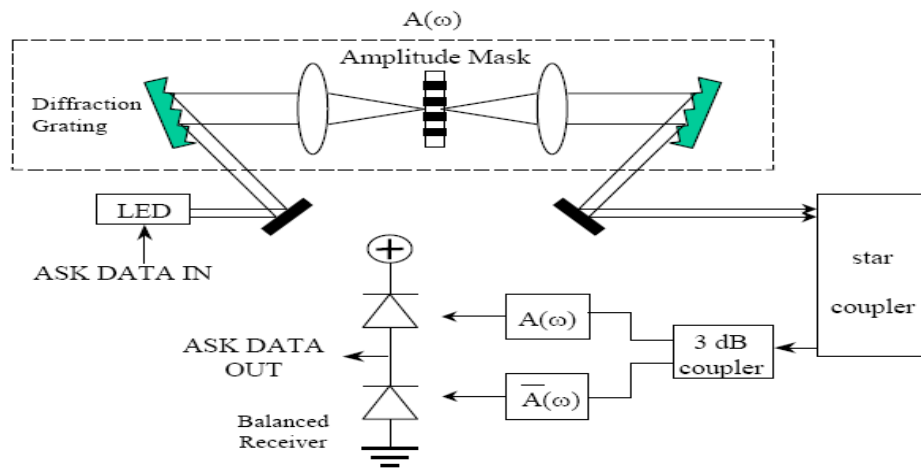


Figure.II.7 la phase a induit d'intensité de bruit du système CDMA Optique [29], [24]

Ce système utilise un récepteur équilibré comprenant deux photodétecteurs en tant que partie de son récepteur qui sert à filtrer les signaux avec le même filtre d'amplitude spectrale également connu sous le filtre direct, qui sert à la fois à l'émetteur et un filtre supplémentaire. Ces deux photo-détecteurs, liés et attachés d'une manière équilibrée, détectent les sorties des filtres complémentaires. Dans ce processus, la moitié des composantes spectrales transmises dans un émetteur inégal correspondra le filtre direct et la moitié restante correspondra au filtre complémentaire. D'un autre côté, les canaux non appariés seront annulés dans le récepteur équilibré et le canal correspondant est démodulé, en raison du fait que la sortie est la représentation de la différence entre les deux sorties de photo-détecteurs.

Avec l'utilisation de l'approche incohérente de codage d'intensité spectrale, la conception de codes pour atteindre la pleine orthogonalité est possible dans ce système car il y a une soustraction entre les deux photo-détecteurs. L'orthogonalité est nécessaire pour éviter la diaphonie ou d'accès multiples interférences par d'autres utilisateurs dans ce système. Zaccarin et al. (1994a) et Nguyen et al. (1997) suggèrent que lorsque les signaux spectralement complémentaires codés sont envoyés, la signalisation bipolaire, constituée

d'une puissance 3 dB avantage, peut être obtenue. Selon divers chercheurs [32], le rapport signal sur bruit est moins dépendant de la puissance reçue en comparaison avec le rapport de la largeur de bande optique à une bande passante de données.

Cette technique présente des avantages et des inconvénients. Aucune horloge système est nécessaire dans la technique et il utilise une LED et sans lignes à retard à prises. Sur l'autre côté, elle est sujette à la perte d'orthogonalité parfaite entre les utilisateurs en raison de la forme gaussienne du spectre LED et en même temps, des filtres accordables, elle est nécessaire pour remodeler le spectre. À travers le déphasage, qui est optiquement complexe, la technique bipolaire peut être obtenue.

✚ Code Division Accès Multiple de spectre optique du Système OSCDMA

Proakis et al. (1995) indiquent que les systèmes de communication à étalement de spectre, rend l'utilisation de très grandes largeurs de bande par rapport à d'autres systèmes, importants dans les applications de communication d'aujourd'hui. Bien qu'une grande quantité de bande passante soit nécessaire dans des communications à étalement de spectre, ce qui conduit à des avantages s'il y a plus d'utilisateurs des réseaux de télécommunication. Ce système particulier, le Code Division Accès Multiple du spectre optique (OSCDMA) utilise une technique connue sous le nom d'une transmission familiale à spectre étalé excepté.

Il y a des utilisateurs N avec émetteurs optiques et récepteurs dans les systèmes OSCDMA. Pour tirer ses canaux, ce système permet notamment l'utilisation d'une source de lumière à large bande incohérente en obstruant sélectivement et à rejeter certaines parties de la lumière, et en révélant l'illustration d'un code à barres comme le montre la figure.II.8 ci-dessous:

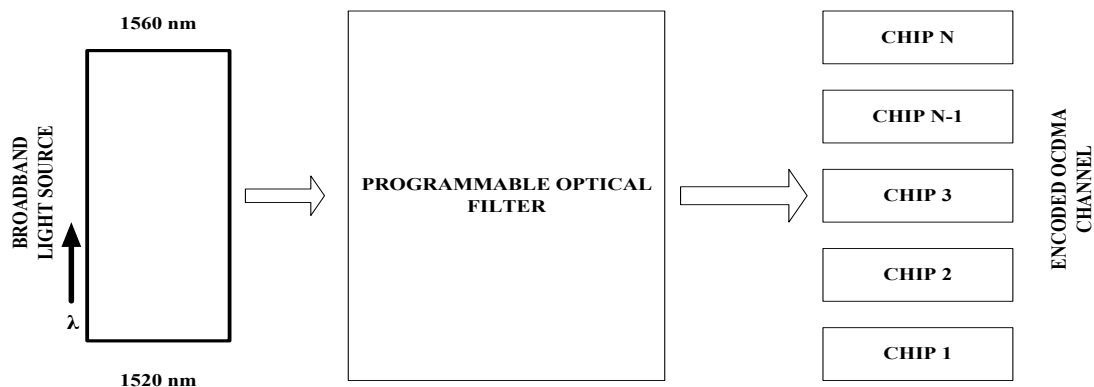


Figure.II.8 Transmetteur Encodage OSCDMA

En utilisant un canal particulier, l'ensemble du spectre codé est transformé conjointement avec des données à transmettre. Ensuite, en utilisant un coupleur optique passif et un couplage fractionnaire convenable, la lumière émise par l'émetteur est inséré dans le réseau. Chaque émetteur dans le système OSCDMA se compose d'un seul code à barres qui modifie un signal sur chaque paire de fibres.

Ce système permet également l'utilisation d'une source optique commune liée à un brin de fibre qui fournit de l'énergie couvrant tous les points du réseau. Chaque émetteur-récepteur puise dans cette énergie à tout moment, ce qui permet des informations complémentaires à la fois envoyées et reçues partout sur le réseau. Dans ce procédé, le récepteur avec le code à barres correspondant se connecte à l'émetteur à l'extrémité de réception, et prend le signal qui lui est envoyé de manière à récupérer les messages transmis.

Ces techniques ne nécessitent pas la synchronisation, tandis que en même temps, elles utilisent des LED qui impose à moindre coût, sans lignes à retard à prises et beaucoup plus simples modèles de codeur et du décodeur.

II.3 Techniques de Codage OCDMA

En OCDMA, le signal optique peut être codé et classifié de plusieurs manières différentes, comme OCDMA temporelle et spectrale d'amplitude de codage (SAC) de réseau OCDMA, la phase et l'intensité spectrale de codage, le 2-D du spectre de codage hybride et codage à saut de fréquence CDMA optique approche.

II.3.1 Codage OCDMA Temporal

La séquence directe ou le codage temporel est également connu comme système d'épandage de temps. En bits de codage temporel sont divisées en intervalles de temps plus petits, appelés jetons de temps. En plaçant l'impulsion de lumière en poids (w) de copeaux de temps produit un code.

II.3.2 Réseau OCDMA Spectral en Amplitude

L'idée d'un codage de fréquence dans OCDMA premier est décrite et démontre par Zacarrin et KAVEHRAD [24], [29]. Spectral codage d'amplitude (SAC) est similaire à l'encodage temporel à l'exception des composantes de fréquence qui sont divisées en fente spectrale selon laquelle les composantes temporelles sont divisées en temps-chip. La figure.II.9 représente le schéma synoptique du SAC, à l'émetteur, le codeur ne transmet que

certaines composantes de fréquence en fonction du code d'étalement. Le signal entrant au niveau du récepteur équilibré du récepteur est filtré en fonction de filtre utilisé à l'émetteur et il est complémentaire. Le filtre direct et le filtre complémentaire vont filtrer les composantes spectrales transmises inégales. La sortie du récepteur équilibrée représente la différence entre les deux sorties du détecteur de photo. Le canal correspondant est détecté lorsque les canaux inégaux sont annulés.

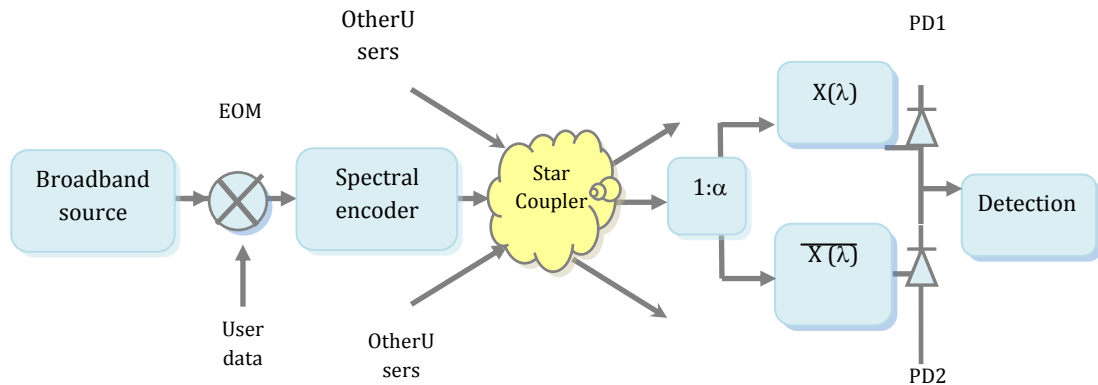


Figure.II.9 Codage incohérent d'amplitude de spectre des réseaux(SAC)-OCDMA

II.3.3 Phase spectrale et d'intensité Encodage

Le codage est effectué directement dans le domaine des fréquences optiques. Spectrum est divisé en tranches W et codé comme des séquences de codes de W . Combinaison de différentes techniques et des schémas de modulation de production de nouvelles solutions. Saut de fréquence rapide (FFH) est une combinaison de temps d'étalement et l'encodage spectral, et la combinaison des temps d'étalement et de décalage de phase (PSK) régime a donné lieu à PSK encodage-décodage [33]. En général, le système se réfère à OCDMA incohérent DS-CDMA.

II.3.4 OCDMA a Saut de Fréquence

Le saut de fréquence (FH) OCDMA est une combinaison de codage temporel et spectral, où le codage est effectué dans les deux dimensions [26], [34]. La FH-CDMA utilise FBG pour générer les CDMA saut de fréquences séquences de code. La sélection du temps de saut de fréquence est déterminée par l'ordre des fréquences de réseau dans la fibre. Au niveau du décodeur, les fréquences de réseau sont à l'inverse du codeur de telle sorte que l'opération de filtrage correspondant est atteinte.

Figure.II.10 indique un concept simple de l'étoile réseau couplé de l'utilisation de FBG à l'encodeur et le décodeur.

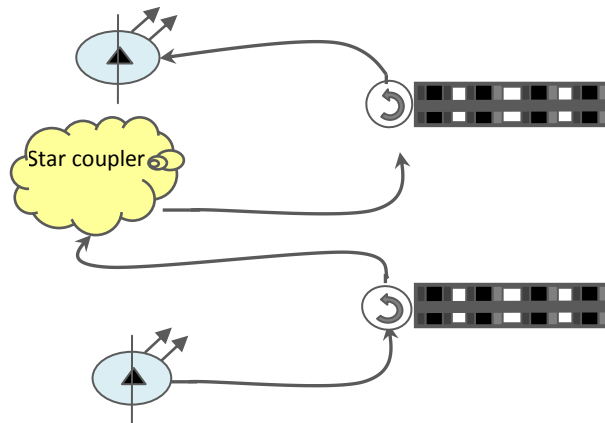


Figure.II.10: codeur et décodeur à Réseaux de Bragg (FBG).

II.4 Classification Des Systèmes OCDMA

En général, les techniques de OCDMA peuvent être classées en deux catégories; systèmes de OCDMA cohérents et systèmes de OCDMA incohérentes.

II.4.1 Système codage Cohérent Spectral Phase

Le codage cohérent spectrale phase (SPE) a été proposée par [27] et [35]. Cohérent SPE OCDMA fonctionne sur la base du principe de signal optique OCDMA où le système est codé par SPE en utilisant système cohérent, nécessitant une phase de codage de signal dans le domaine fréquentiel [36-37]. Les signaux de données sont codés par SPE en appliquant des codes de phase à spectre du signal optique sur la Figure.II.11. Dans spectrale en phase codeur, le signal optique modulé est généré à partir de la source optique à large bande est spectralement alloué en différentes composantes de fréquence. Spectrum est séparé N spectrale et distincte déphasage sont appliqués à chaque spectrale. La SPE manipule la phase dans le domaine spectral par source laser haute multi-longueur d'onde cohérente mode verrouillé. La sortie du laser à verrouillage de mode se présente comme un peigne d'ondes de verrouillage de phase et de fréquence équidistants. Le spectre sera modulé et séparé en compartiments spectraux et plus tard sera recombinaison pour créer des codes [38].

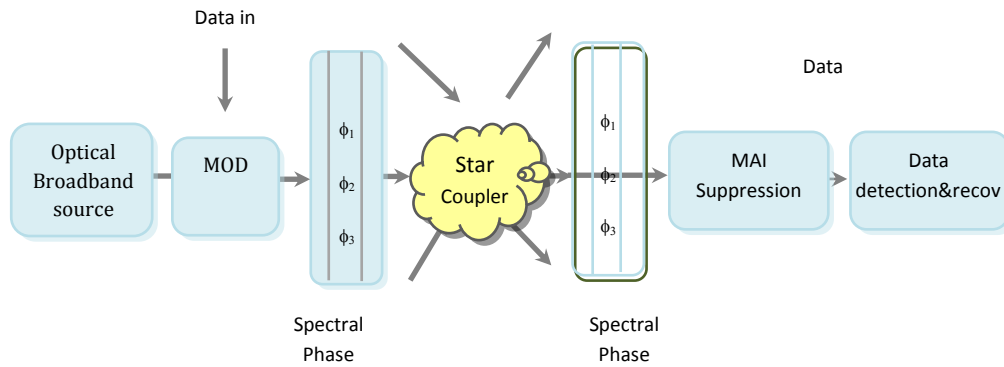


Figure.II.11 système OCDMA de codage cohérent spectrale phase (SPE).

L'encodage temporel-phase (TPE) manipule la phase optique dans le domaine temporel en utilisant l'impulsion courte de lasers à mode bloqué. Les impulsions retardées entraînent également l'espace-temps. Ensuite, chaque impulsion avec une phase spécifique est créée et combinée pour produire un code. Dans l'ensemble, la performance OCDMA cohérente est incohérente par rapport à une meilleure OCDMA opérations de codage en raison de caractéristique bipolaire. La détérioration des performances du système cohérent est due à une modulation de phase croisée. Le système cohérent est plus cher comparé à un système incohérent.

II.4.2 Systèmes OCDMA Incohérent

La base de l'OCDMA incohérente est fondée sur la modulation d'intensité et de détection directe. La OCDMA incohérente peut être mis en œuvre à un débit binaire relativement faible, où le codage est effectué dans un unipolaire. Les inconvénients sont une si petite taille du code, de faible puissance et de l'efficacité de la bande passante et haute corrélation croisée [32]. Bien que ce problème puisse être surmonté électriquement [39], la bande passante optoélectronique est le goulot d'étranglement du problème. Le codage des données peut être effectuer dans divers schémas différents, par exemple; SAC [24], SPE [40], le codage temporel[2], 2-D longueur d'onde en temps de codage [25], [31], [41] et le codage hybride.

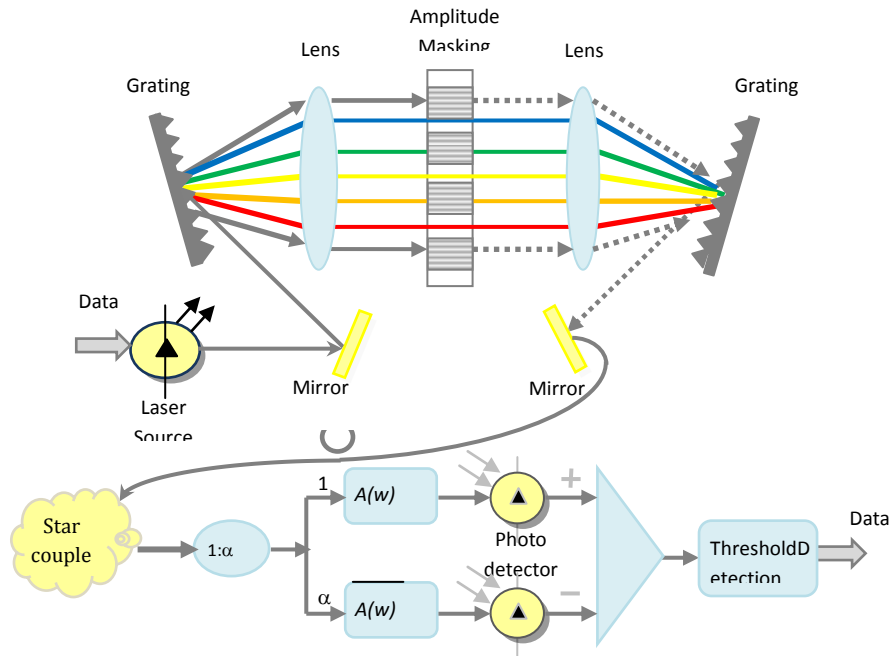


Figure.II.12 Principe de codage d'amplitude spectrale (SAC) OCDMA.

Le codage spatial utilise le système multi-fibres pour créer le modèle spatial où les utilisateurs transmettent le modèle d'impulsion optique sur la fibre. Dans le codage temporel où le temps bits système d'étalement sont divisés en NT intervalle de temps appelé à puce, Figure.II.12. En positionnant le poids impulsion courte (w) de la lumière dans NT, le code est produit.

Unidimensionnel (1-D), le codage temporel et 2 dimensions (2-D) sont la méthode de codage d'étalement des deux temps communs. L'encodage hybride est un processus de codage qui implique plus d'une dimension ou multi dimension. L'impulsion lumineuse est codée dans une combinaison de temps, d'espace et de fréquence.

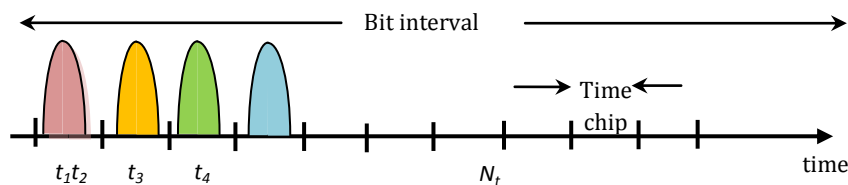


Figure.II.13 système d'étalement temporel Unidimensionnelle (1-D).

La Figure.II.13 est un exemple d'étalement temporel où le poids est égal à quatre. En 1986, le principal démontré le premier temps c'est OCDMA 1-D étalement [2]. L'analyse des performances a indiqué que 1-D codage de limitation en terme d'auto-corrélation de lobe latéral face lorsque les séquences de code sont dépensées. Le faible débit binaire et la cardinalité sont la question aussi. La fréquence domaine 2-D des schémas de codage offre une nouvelle alternative en raison de l'amélioration des performances de corrélation croisée [42], mais la dispersion est toujours un problème dans l'application à large bande.

Dans OCDMA incohérente chaque intervalle de bits est divisé en nombre égal de fentes appelées chips. La transmission du bit de donnée "1" est indiquée par certaines puces prédéterminées avec de courtes impulsions de lumière où le train d'impulsions est transmis. Pas de transmission si le bit est "0". Les positions des impulsions sont informées de séquence d'étalement unipolaire. Pour supprimer l'interférence d'accès multiple (MAI) et à faciliter la synchronisation, les séquences de codes attribuées à des émetteurs présentent une corrélation croisée minimum et le minimum hors pointe d'auto-corrélation. Diverses techniques ont été proposées pour construire de telles séquences [43].

II.5 Les Eléments Du Système OCDMA

Les détails CDMA optique descriptions bloc système de diagrammes sont présentés à la figure.II.14. Il se compose de plusieurs paires émetteur-récepteur; sources de lumière, codeur, décodeur, traitement optique, détecteur de photo, et de traitement électronique. Les données envoyées par les émetteurs sont récupérées par les récepteurs. Les sources de lumière génèrent des impulsions lumineuses ayant une durée plus courte que des bits de données de telle sorte que la bande passante du signal sera plus grande que le débit de données. Le système utilise OCDMA on-off pour moduler la source de lumière; l'impulsion lumineuse est générée lorsque le bit de données "1" est transmis. Cependant, d'autres schémas, les impulsions lumineuses sont produites pour tous les bits de données où le codeur de différentes formes d'onde de sortie pour "1" et "0".

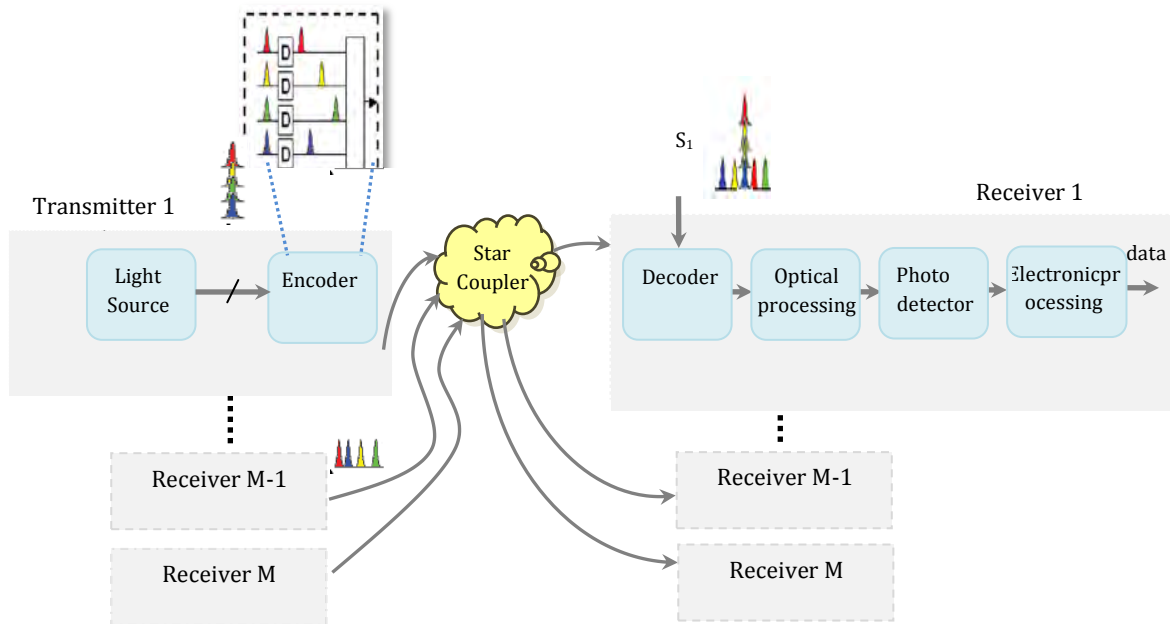


Figure.II.14 système de communication OCDMA de deux dimensions (2D).

II.5.1 Sources lumineuses

Les sources de lumière peuvent être classées comme cohérentes ou incohérentes. Les sources de lumière cohérentes produisent le temps de bande passante égale à 1. Le laser de modèle à verrouillage est un exemple de source de lumière cohérente. Le champ électrique de la source cohérente d'une impulsion peut être exprimé sous la forme;

$$E_p(t) = \sqrt{p(t)} \exp j[\omega t + \phi(t)] \quad (\text{II.1})$$

où $p(t)$ est le profil de puissance d'impulsion, ω est la fréquence porteuse de lumière et $\phi(\cdot)$ indique le bruit de phase. Puisque la fonction d'autocorrélation $\phi(\cdot)$ est inchangé, l'équation peut être réécrite sous la forme;

$$E_p(t) = \sqrt{p(t)} \exp j[\omega t + \phi] \quad (\text{II.2})$$

L'impulsion cohérente est égale à la durée d'impulsion. Dans les sources de lumière cohérentes, la production du temps-largeur de bande est supérieure à 1. Telle est la raison pour laquelle la LED et l'émission spontanée amplifiée (ASE) qui tombe dans cette région est utilisée. Le champ électrique de la source incohérente d'une impulsion peut être exprimé sous la forme;

$$E_p(t) = \sqrt{p(t)}u(t) \exp j\omega t \quad (\text{II.3})$$

Où est le profil de puissance d'impulsion de la puce, et le processus complexe gaussien aléatoire stationnaire avec zéro variance moyenne et l'unité. La fréquence porteuse de lumière indique le bruit de phase. Puisque la fonction d'auto-corrélation est inchangée. La source incohérente temps de l'impulsion peut être exprimée en termes de densité de puissance spectrale à bande latérale unique (PSD) d'incidence de la lumière à la photodiode [44]:

$$\tau_c = \frac{\int_{-\infty}^{\infty} [S^2(f)df]}{\left[\int_{-\infty}^{\infty} S(f)df \right]^2} = \frac{1}{[R_u(0)]^2} \int_{-\infty}^{\infty} |R_u(\tau)|^2 d\tau \quad (\text{II.4})$$

Où S f est la densité spectrale de puissance de l'impulsion. Le temps de cohérence est illustré sur la figure.II.15;

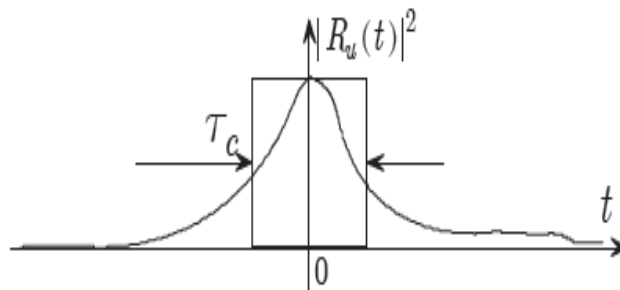


Figure.II.15 temps de cohérence de l'impulsion incohérente.

La bande passante des deux impulsions cohérente et incohérente est approximativement réciproque des temps de cohérence, $B = \frac{1}{\tau_c}$. Pour soit le schéma cohérent ou incohérent, les deux peuvent utiliser des sources de lumière cohérente ou des sources de lumière incohérente de façon interchangeable. La classification soit cohérente ou incohérente ne dépend pas de types de sources lumineuses utilisées. Les schémas cohérents ou incohérents peuvent utiliser des sources de lumière cohérente ou incohérente de sources interchangeables[20].

II.5.2 Codeur et décodeur

Le codeur et le décodeur sont l'émetteur et le récepteur de dispositifs de réseau de transport OCDMA. La sortie d'impulsion de lumière du modulateur est transmise à l'encodeur.

Le codeur convertit l'impulsion lumineuse dans une forme d'onde optique, basée sur S_k , la séquence d'étalement est attribuée à l'émetteur. Le train d'impulsions est généré en utilisant soit une ligne à retard optique ou fibre des réseaux de Bragg. Divers schémas différents convertissent les amplitudes ou phases des composantes de fréquence et fonctionnent dans le domaine fréquentiel. Le code processus OCDMA est similaire au processus de communication d'étalement à séquence directe sans fil CDMA. Afin de supprimer l'AMI, les signaux entrants provenant d'émetteurs doivent posséder la propriété d'orthogonalité [50]. Au niveau du décodeur du récepteur il permet de détecter le signal de l'émetteur souhaité pour générer une sortie de bit de données détecté. Le décodeur est constitué d'une paire de filtres réflecteurs ou conjointement avec d'autres appareils avec la configuration spécifique. Il se comporte comme un filtre linéaire adapté aux émetteurs encodeur désiré. En raison du facteur de débit de données rapide, il est préférable que OCDMA codeur et le décodeur devant être réalisé par tous les dispositifs optiques [43].

II.5.3 canal optique

Le canal optique se compose de coupleurs en étoile qui agit comme les multiples dispositifs de sortie multiples d'entrée qui distribuent les signaux d'impulsion aux sorties. Dans le canal, l'AMI est la source d'interférence. Les signaux dans la fibre optique sont soumis à des évanouissements, la dispersion, et non linéarités effets. En général, la demande est OCDMA concentrée sur des réseaux locaux (LAN) où l'utilisation de fibres de longueur est à quelques deux kilomètres. La demande de communication de longue distance pourrait contribuer à la distorsion. Cependant la déformation peut être compensée par l'amplificateur optique et la fibre à dispersion compensée (DCF) [43].

II.5.4 Photodétecteur

Dans les communications optiques, le récepteur détecte la puissance de la lumière entrante par photo-détecteur. L'énergie contenue dans l'impulsion de lumière est convertie en courant électrique par le détecteur photoélectrique en raison des effets photo-électriques. La figure.II.16 est la réponse impulsionnelle d'un photo-détecteur à la moitié du maximum de grande largeur (FWHM) indique la période de temps où la forme d'onde est à la moitié de sa valeur maximale. La réponse photo-détecteur est d'environ une picoseconde [30].

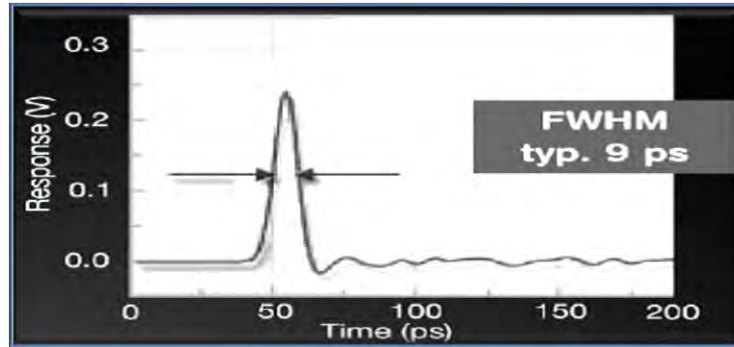


Figure.II.16: temps de cohérence de l'impulsion incohérente[30].

Dans le récepteur photo-détecteur est modélisée comme un convertisseur quadratique idéal et intégrateur, Figure.II.17. Entrée du champ électrique entre le convertisseur quadratique et la sortie est une puissance optique instantanée. T_r est le temps de réponse photodétecteur. L'énergie optique est la sortie de l'intégrateur.

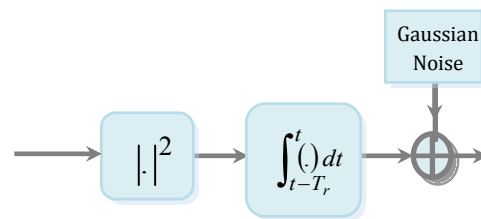


Figure.II.17Modèlede photo-détecteur.

Sources de bruit photo-détecteur sont constituées de bruit de grenaille, le bruit courant d'obscurité, et le bruit thermique. Ces bruits sont estimés comme un bruit gaussien additif. En règle générale, le signal entrant est fort et les effets quantiques, le bruit thermique et le bruit de courant d'obscurité dans le photo-détecteur sont ignorés. Le facteur de la performance du système limité est seulement MAI.

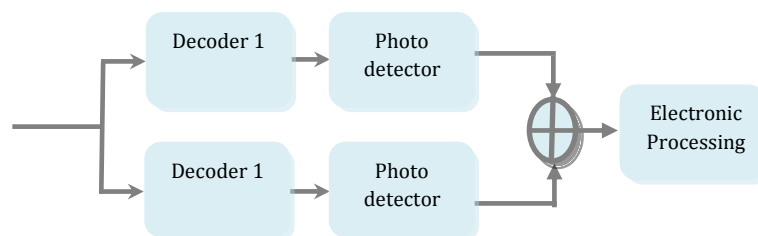


Figure.II.18Modèle de détection de l'équilibre.

Les décodeurs correspondent aux formes d'onde entrant dans le récepteur. La figure.II.18 montre que les sorties des décodeurs sont détectées par des photo-détecteurs. La

différence entre le photodétecteur (PD1) et le photodétecteur (PD2) sortie va aux transformateurs électroniques pour la poursuite du processus. On appelle cela la détection de l'équilibre qui sera décrit plus en détail dans la section plus tard [43].

II.5.5 Optique et Processeur électronique

Les schémas OCDMA rencontrent un problème en raison d'un signal OCDMA codeur ou longueur d'interférence qui est plus petite comparé aux photo-détecteurs temps de réponse. Le photo-détecteur devra faire face à des difficultés à différencier correctement le signal décodé et l'interférence. Pour surmonter ce problème, des dispositifs optiques non linéaires ou «traitement optique», qui est situé avant le photo-détecteur sont nécessaires de telle sorte que les formes d'onde optiques de "1" et "0" peuvent être différenciées. Le traitement électronique est représenté sur la figure.II.10. Les signaux électroniques générés par photo-détecteur sont convertis en bits de données par le traitement optique [45].

II.6 Principaux défis dans les systèmes OCDMA

Le CDMA sans fil se concentre sur la communication à faible débit de données. Cependant, OCDMA explore l'énorme disponibilité de la bande passante pour les communications à haut débit de données. Telle est la raison pour laquelle les interférences et les bruits doivent être au maximum supprimés pour obtenir une faible BER. Le taux d'erreur binaire admissible (BER) exige de plancher d'erreur typique pour un système est à 10^{-9} ou un bit errant sur un milliard. Il est de nature un système qui peut loger un grand nombre d'utilisateurs et se traduira par une forte interférence ou BER détérioration.

La mise au point du système OCDMA est de réduire la corrélation croisée, en conséquence, la cardinalité peut être renforcée par l'atténuation des interférences. D'autre part même de bons schémas de codage à faible corrélation croisée permettent également de limiter le nombre d'utilisateurs généré. Aujourd'hui, la cardinalité optimale du système 1-D est dans la plage de 100 à 180 le nombre d'utilisateurs simultanés. Zéro Code Croix-Corrélation avec la propriété unique zéro corrélation croisée peuvent accueillir 100 numéros simultanés des utilisateurs [46]. Le 1-D modifié Zéro corrélation croisée (MZCC) [47] et 1-D Cyclique [48] code avec la corrélation croisée flexible et la longueur de code ne peuvent atteindre des optimaux moins de 150 numéros simultanés des utilisateurs respectivement.

Le bruit de phase induite par l'intensité (PIIN) ou de battre le bruit est généré lorsque l'émission spontanée de séquences de codes d'impulsions à longueur d'onde fermée est alignée au niveau du détecteur. Les séquences de code avec une faible corrélation croisée suppriment la douleur, améliore la performance SNR et BER. Un système de détection permet également d'atténuer l'MAI.

L'MAI [22] est l'interférence ultime qui dégrade les performances du système. L'augmentation du nombre d'évolutivité d'utilisateurs simultanés induit AMI et limite sévèrement la capacité du système. L'atténuation de l'MAI peut être faite par système de détection d'équilibre. Cependant, le problème inhérent de bruit, PIIN sera toujours disponible [34]. Le défi aujourd'hui réside dans l'expansion de la cardinalité de code admissible et en gardant les performances de BER au plus bas possible. Afin d'atteindre cet objectif, la bonne combinaison de séquences de code d'étalement, les techniques de détection et de codage de canal sont obligatoires.

II.7 Conclusion

Ce chapitre donne un aperçu de la technologie d'accès multiple spécifiquement sur OCDMA. Divers OCDMA techniques de codage sont décrites. La classification des OCDMA; cohérent et incohérent, et les éléments du système sont décrits OCDMA. Le défi majeur d'aujourd'hui c'est la technologie OCDMA du système de multiplexage qui a attiré divers intérêts de recherche sur l'utilisation de la bande passante de la fibre spectre de fréquences par rapport à la WDMA optique classique et TDMA optique. OCDMA propose diverses fonctionnalités et avantages tels que la grande et l'utilisation efficace de la bande passante, de haute sécurité, la flexibilité des réseaux d'accès à haut débit et l'affectation dynamique de bande passante. Les défis que le système OCDMA doit surmonter sont à supprimer de manière optimale aux interférences et fonctionner à haut débit de données. Il est prévu que OCDMA sera le prochain réseau d'accès de génération dans les réseaux d'accès à large bande d'application future.

Références bibliographiques du chapitre II

- [1] G. P. Agrawal, *Fiber-Optic Communications Systems, Third Edition.*, vol. 6. 2002.
- [2] P. Prucnal, M. Santoro, and T. Fan, "Spread spectrum fiber-optic local area network using optical processing," *Journal of Lightwave Technology*, vol. 4, no. 5. pp. 547–554, 1986.
- [3] K. W. Cheung, D. A. Smith, J. E. Baran, and B. L. Heffner, "Multiple channel operation of integrated acousto-optic tunable filter," *Electronics Letters*, vol. 25, no. 6. pp. 375–376, 1989.
- [4] B. C. Yeh, C. H. Lin, and J. Wu, "Noncoherent Spectral/Time/Spatial Optical CDMA System Using 3-D Perfect Difference Codes," *Journal of Lightwave Technology*, vol. 27, no. 6. pp. 744–759, 2009.
- [5] M. M. Karbassian and F. Kueppers, "Synchronous Optical CDMA Networks Capacity Increase Using Transposed Modified Prime Codes," *Journal of Lightwave Technology*, vol. 28, no. 17. pp. 2603–2610, 2010.
- [6] M. S. Anuar, S. A. Aljunid, N. M. Saad, and S. M. Hamzah, "New design of spectral amplitude coding in OCDMA with zero cross-correlation," *Opt. Commun.*, vol. 282, no. 14, pp. 2659–2664, 2009.
- [7] C.-C. Yang, "The Application Of Spectral-Amplitude-Coding Optical CDMA In Passive Optical Network. Optical Fiber Technol," *Opt. Fiber Technol*, vol. 14, pp. 134–142, 2008.
- [8] M. S. Borella, J. P. Jue, D. Banerjee, B. Ramamurthy, and B. Mukherjee, "Optical components for WDM lightwave networks," *Proceedings of the IEEE*, vol. 85, no. 8. pp. 1274–1307, 1997.
- [9] C. Systems, "Introduction to DWDM for metropolitan networks," *Networks*, no. 6387, p. 80, 2001.
- [10] P. R. Morkel, M. Tachibana, R. I. Laming, and D. N. Payne, "Erbium-doped fiber amplifier with flattened gain spectrum," *IEEE Photonics Technology Letters*, vol. 3, no. 2. pp. 118–120, 1991.

- [11] A. Sneh and K. M. Johnson, "High-speed Tunable Liquid Crystal Optical Filter For WDM Systems," *Integrated Optoelectronics, 1994., Proceedings of IEE/LEOS Summer Topical Meetings*: pp. 3_59–3_60, 1994.
- [12] M. Ito, M. Inai, Y. Hattori, A. Inoue, M. Shigehara, and T. Mizunami, "Fabrication And Application Of Fiber Bragg Grating A Review," *Optoelectron Devices Technol.*, vol. 10, pp. 119–130, 1995.
- [13] H. S. Hinton, "Photonic switching fabrics," *IEEE Communications Magazine*, vol. 28, no. 4. pp. 71–89, 1990.
- [14] H. G. Perros, "Connection-oriented networks : SONET/SDH, ATM, MPLS, and optical networks," *John Wiley Sons*, 2005.
- [15] R. Ramaswami and K. Sivarajan, "Optical Networks, a practical perspective," *USA Morgan Kaufmann*, no. 2nd Ed, 1998.
- [16] S. Yao, B. Mukherjee, and S. Dixit, "Advances in photonic packet switching: an overview," *IEEE Communications Magazine*, vol. 38, no. 2. pp. 84–94, 2000.
- [17] R. S. Tucker, G. Eisenstein, and S. K. Korotky, "Optical time-division multiplexing for very high bit-rate transmission," *Journal of Lightwave Technology*, vol. 6, no. 11. pp. 1737–1749, 1988.
- [18] J. A. Salehi, "Code division multiple-access techniques in optical fiber networks. I. Fundamental principles," *IEEE Transactions on Communications*, vol. 37, no. 8. pp. 824–833, 1989.
- [19] J. Hui, "Pattern Code Modulation and Optical Decoding - A Novel Code-Division Multiplexing Technique for Multifiber Networks," *IEEE Journal on Selected Areas in Communications*, vol. 3, no. 6. pp. 916–927, 1985.
- [20] G. J. Pendock and D. D. Sampson, "Increasing the transmission capacity of coherence multiplexed communication systems by using differential detection," *IEEE Photonics Technology Letters*, vol. 7, no. 12. pp. 1504–1506, 1995.
- [21] F. R. K. Chung, J. A. Salehi, and V. K. Wei, "Optical orthogonal codes: design, analysis and applications," *IEEE Transactions on Information Theory*, vol. 35, no. 3.

- pp. 595–604, 1989.
- [22] A. Stok and E. H. Sargent, “Lighting the local area: optical code-division multiple access and quality of service provisioning,” *IEEE Network*, vol. 14, no. 6. pp. 42–46, 2000.
- [23] N. Karafolas, “Optical Fiber Code Division Multiple Access Networks: A Review,” *Opt. Fiber Technol.*, vol. 2, no. 2, pp. 149–168, 1996.
- [24] D. Zaccarin and M. Kavehrad, “An optical CDMA system based on spectral encoding of LED,” *IEEE Photonics Technology Letters*, vol. 5, no. 4. pp. 479–482, 1993.
- [25] L. Tancevski and I. Andonovic, “Wavelength hopping/time spreading code division multiple access systems,” *Electronics Letters*, vol. 30, no. 17. pp. 1388–1390, 1994.
- [26] H. Fathallah, L. A. Rusch, and S. LaRochelle, “Optical frequency-hop multiple access communications system,” *Communications, 1998. ICC 98. Conference Record. 1998 IEEE International Conference on*, vol. 3. pp. 1269–1273 vol.3, 1998.
- [27] J. A. Salehi, A. M. Weiner, and J. P. Heritage, “Coherent ultrashort light pulse code-division multiple access communication systems,” *Journal of Lightwave Technology*, vol. 8, no. 3. pp. 478–491, 1990.
- [28] H. Fathallah, “Spectral Amplitude Coding Optical CDMA: Performance Analysis of PIIN Reduction Using VC Code Family,” *IEEE/OSA J. Light. Technol.*, vol. 17, no. 3, pp. 397–405, 1999.
- [29] D. Zaccarin and M. Kavehrad, “New architecture for incoherent optical CDMA to achieve bipolar capacity,” *Electronics Letters*, vol. 30, no. 3. pp. 258–259, 1994.
- [30] S. Y. Chou and M. Y. Liu, “Nanoscale Tera-Hertz Metal-Semiconductor-Metal Photodetectors,” *IEEE J. Quantum Electron.*, vol. 28, no. 10, pp. 2358–2368, 1992.
- [31] G.-C. Yang and W. C. Kwong, “Two-dimensional spatial signature patterns,” *IEEE Transactions on Communications*, vol. 44, no. 2. pp. 184–191, 1996.
- [32] D. D. Sampson, G. J. Pendock, and R. A. Griffin, “Photonic code-division multiple-access communications,” *Fiber Integr. Opt.*, vol. 16, no. 2, pp. 129–157, Jan. 1997.

- [33] M. Zhang, "DESIGN AND PERFORMANCE ANALYSIS OF NOVEL SIGNATURE CODE IN TWO-DIMENSIONAL OPTICAL CDMA SYSTEMS," 2012.
- [34] H. Fathallah, L. A. Rusch, and S. LaRochelle, "Passive optical fast frequency-hop CDMA communications system," *Journal of Lightwave Technology*, vol. 17, no. 3. pp. 397–405, 1999.
- [35] C. C. Chang, H. P. Sardesai, and A. M. Weiner, "Code-division multiple-access encoding and decoding of femtosecond optical pulses over a 2.5-km fiber link," *IEEE Photonics Technology Letters*, vol. 10, no. 1. pp. 171–173, 1998.
- [36] S. Etemad, P. Toliver, R. Menendez, J. Young, T. Banwell, S. Galli, J. Jackel, P. Delfyett, C. Price, and T. Turpin, "Spectrally efficient optical CDMA using coherent phase-frequency coding," *IEEE Photonics Technology Letters*, vol. 17, no. 4. pp. 929–931, 2005.
- [37] Z. Jiang, D. S. Seo, S. D. Yang, D. E. Leaird, R. V Roussev, C. Langrock, M. M. Fejer, and A. M. Weiner, "Four-user, 2.5-Gb/s, spectrally coded OCDMA system demonstration using low-power nonlinear processing," *Journal of Lightwave Technology*, vol. 23, no. 1. pp. 143–158, 2005.
- [38] C. S. Bres, "Optical CDMA for Access Networks: Design, Simulation and Analysis," *Princet. Univ.*, 2007.
- [39] E. D. J. Smith, R. J. Blaikie, and D. P. Taylor, "Performance enhancement of spectral-amplitude-coding optical CDMA using pulse-position modulation," *IEEE Transactions on Communications*, vol. 46, no. 9. pp. 1176–1185, 1998.
- [40] A. A. Hassan, J. E. Hershey, and N. A. Riza, "Spatial optical CDMA," *IEEE Journal on Selected Areas in Communications*, vol. 13, no. 3. pp. 609–613, 1995.
- [41] R. Yim, *New Approaches to Optical Code-Division Multiple Access*, no. September. 2002.
- [42] S. Yegnanarayanan, A. S. Bhushan, B. Jalali, and S. Member, "Fast Wavelength-Hopping Time-Spreading Encoding / Decoding for Optical CDMA," *IEEE Photonics Technol. Lett.*, vol. 12, no. 5, pp. 573–575, 2000.

- [43] B. Ni, “The Performance of Optical Code-Division Multiple Access Systems,” *Purdue Univ.*, 2005.
- [44] M. S. Anuar, A. AlJunid, S. A., J. A. R., M. N., and N. Saad, “PIN versus Avalanche Photodiode Gain Optimization in Zero Cross Correlation Optical Code Division Multiple Access System,” *Opt. J.*, 2012.
- [45] S. Dewra and A. Grover, “Fabrication and Applications of Fiber Bragg Grating- A Review,” vol. 25, no. 2, pp. 15–25, 2015.
- [46] A. R. Arief, S. A. Aljunid, M. S. Anuar, M. N. Junita, R. B. Ahmad, and F. Ghani, “Enhanced performance of new family Modified Double Weight codes spectral amplitude coding optical CDMA system network,” *Control System, Computing and Engineering (ICCSCE), 2011 IEEE International Conference on*. pp. 488–494, 2011.
- [47] C. B. M. Rashidi, S. A. Aljunid, F. Ghani, M. S. Anuar, H. Al-Khafaji, M. N. Junita, and A. R. Arief, “New design of Zero Cross Correlation Codes for Spectral Amplitude Coding in OCDMA systems,” *2011 2nd International Conference on Photonics*. pp. 1–5, 2011.
- [48] T. H. Abd, S. A. Aljunid, H. A. Fadhil, R. B. Ahmad, and M. N. Junita, “Enhancement of performance of a hybrid SAC-OCDMA system using dynamic cyclic shift code,” *Ukr. J. Phys. Opt.*, vol. 13, no. 1, p. 12, 2012.

CHAPITRE

III

Chapitre III implémentation résultat numérique et discussion

III.1 Introduction

L'algorithmique quantique pour les réseaux adaptatifs dans les routeurs WDM (Wavelength Division Multiplexing) pour la voix, les données et les applications multimédia ont apporté un nouveau domaine dans le soutien des réseaux de communication prévisibles et garantis. De nos jours, la communication multimédia pour l'échange de données fiables exige la communication pour répondre aux normes rigoureuses où l'information peut être facilement transmis et reçu des commentaires avec facilité et confort [1]. La forte demande du réseau a mener à une augmentation rapide de la bande passante de communication, malheureusement, il est fait avec des dépense sur le trafic de communication et de confisquer la sécurité de la circulation de données [2-3]. Afin de résoudre ce problème, la cryptographie quantique est proposée comme une solution alternative et de la distribution quantique de clés (QKD) utilise la mécanique quantique pour garantir des données de communication sécurisée[4].

En général, un modèle de communication est constitué d'un système implique une source de données d'entrée sur un support d'acheminement et d'un récepteur où la modulation et la démodulation se produisent [5]. L'information est obtenue à partir des porteuses de source. Celle-ci est l'information initiale qui utilise des symboles à partir de données d'ensemble fini (alphabet, chiffres ou son équivalent) et le mode de transmission peut se faire soit en un seul coup ou les envoie à intervalles réguliers [6].

Dans ce cas, chacune des données du symbole transmis n'est pas dépendant aux précédents [7]. Les canaux discrets transmettent des symboles à partir d'un ensemble spécifique (alphabet d'entrée), et ils génèrent dans leur sortie un autre ensemble de symboles (alphabet de sortie) [8]. Comme l'alphabet d'entrée et l'alphabet de sortie peuvent être différents, il est nécessaire d'utiliser un codage qui maximise l'efficacité de la transmission [9]. Fondamentalement, le codage consiste à affecter un mot spécifique à chacun des symboles dans l'entrée (construite avec des éléments de l'alphabet de sortie) [10].

Ceci doit être effectué en trouvant une longueur moyenne du code à être réduits au minimum, mais également un décodage unique au récepteur. En outre, le canal est généralement non idéal, les informations reçues diffèrent des informations envoyées, et cette différence se traduit par une probabilité d'erreur dans le comportement du récepteur; dont la

mission est tout simplement de récupérer les informations d'origine, avec une fidélité maximale possible [11].

Dans l'approche de communication quantique, les concepts mentionnés ci-dessus sont encore utilisées, mais avec quelques changements intenses. Dans un premier temps, une donnée quantique est en rapport avec le symbole généré par la source d'entrée. La signification des données à travers le canal est un espace de Hilbert (dimensions de qubits). Généralement, Il est également nécessaire que le codage de source attribue à chaque état-symbole une représentation dans la forme de qubits[12].

Dans un second lieu, tout processus lié à la transmission de l'information qui altère son état, se caractérise par un super-opérateur [8]. Mais dans ce cas, la chose habituelle est d'inclure le comportement de bruit du canal, en raison de l'interaction entre le système et l'environnement (plus ou moins actif) dans les données d'entrée. Dans les canaux sans erreur, l'état pur est associé à chaque symbole [13], quant à lui dans les canaux bruités un état mixte est utilisé. Ils ont fermé les systèmes quantiques, composé de sous-systèmes associés à l'information (système ouvert) et à l'environnement bruyant [4].

III.2 Méthodologie

Le réseau de commutation (WDM) est constitué de nœuds de commutation avec une communication qui relie ces nœuds. Chaque canal de liaison comporte un certain nombre de longueurs d'onde et chaque longueur d'onde est en outre divisée en un certain nombre de tranches de temps pour commander le transfert du paquet. L'architecture de nœud pour sous-longueur d'onde exige un mode de transfert de données multicast supportant trois liens avec la congestion et des liens gratuits. Le paquet de longueurs d'onde du lien et de trois intervalles de temps pour tous les canaux et le nœud pour la détermination des sessions en utilisant la tranche de temps de la bande passante.

Un réseau de communication quantique se compose de la source d'entrée, un canal de communication et de la sortie, tout comme le mode classique et la sécurité des données dépend de l'ensemble des trois étapes de la communication. La recherche actuelle démontre que le mode de transmission de données dépend de l'intégrité du canal et sa capacité [14]. De la théorie classique de l'information, nous avons des bits qui peut être 0 ou 1. Dans la théorie de l'information quantique est l'équivalent des bits quantiques ou qubits [11, p. 80]. Ce sont deux états quantiques dimensionnelles.

Nous pouvons coder les bits comme qubits utilisant états orthogonaux, avec la notation 0 et 1 [13]. D'après la théorie classique de l'information, nous avons des bits qui peuvent être 0 ou 1. Dans la théorie de l'information quantique est l'équivalent des bits quantiques ou qubits [11, p. 80]. Ce sont deux états quantiques dimensionnels. Nous pouvons coder les bits comme qubits utilisant états orthogonaux, avec la notation 0 et 1 [13].

L'avantage des qubits est qu'ils peuvent être en superposition et à travers le canal pendant la transmission des données; le combineur combine les deux données de polarisation orthogonale en les orientant vers le bon canal [12]. Cependant, le combineur et le diviseur peuvent différer les polarisations seulement par une valeur finie, en introduisant la diaphonie [14]. Cela signifie qu'une petite partie de l'impulsion adressée pourrait encore injecter, et vice versa.

Dans un interféromètre équilibré, cela affecterait une interférence, depuis lors, une petite partie serait modulée qui ne devrait pas avoir été, et vice versa. Dans cette configuration où l'interférence est déséquilibré, la différence de longueur de trajet optique effectue les impulsions partent de l'émetteur et arrivent au récepteur avec un décalage temporel [14]. Ceci dirige la diaphonie pour arriver à des moments différents dans le canal de couplage pour identifier le signal de données requis. L'onde de réseau converti ou un convertisseur de longueur d'onde est un dispositif qui permet la conversion d'un signal d'une longueur d'onde à une autre longueur d'onde.

Dans les réseaux optiques dépourvus de convertisseurs de longueur d'onde, chaque message ne peut être activé à partir d'une certaine longueur d'onde à un port d'entrée à la même longueur d'onde sur un port de sortie [13]. Bien que les convertisseurs de longueur d'onde améliorent les performances du réseau, il est bien connu que tous les convertisseurs optiques de longueur d'onde sont coûteux [14].

$$\text{Function } [P_x, P_y] = \text{rhoxyNonUPhase}(1,2,N) \dots \dots \dots \text{(III.1)}$$

L'équation 1 montre la représentation du transfert de données non uniforme le long d'un canal

$$\text{Function } [P_x, P_y] = \text{rhoxyUPhase}(1,2,N) \dots \dots \dots \text{(III.2)}$$

L'équation 2 montre la représentation du transfert de données uniforme le long d'un canal où P_x est la probabilité de chemin de données à l'axe X et P_y probabilité de chemin de données à l'axe Y et ρ représente la concentration de données.

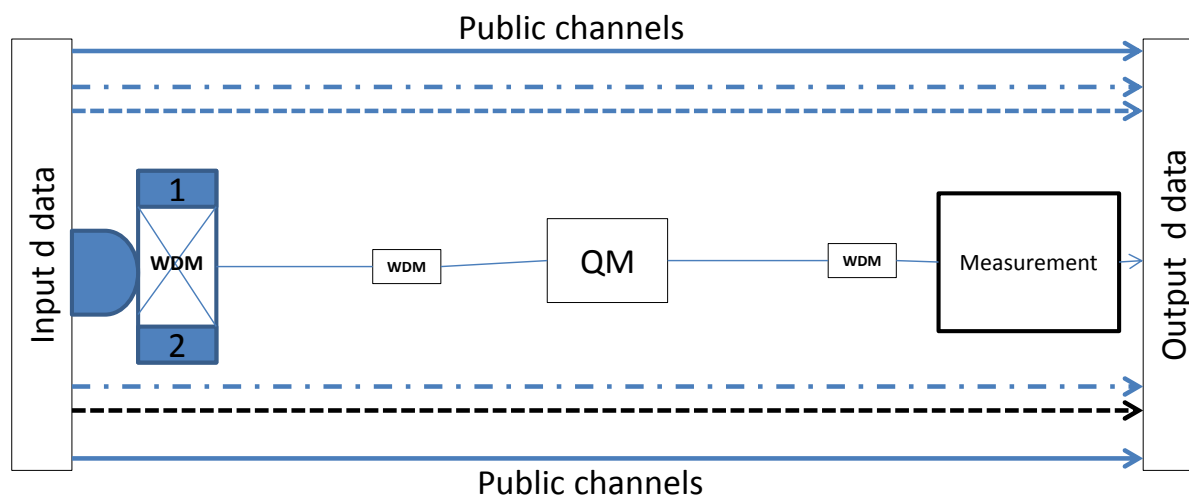


Figure.III.1 Schéma de réseau soutenant des canaux QKD et WDM.

III.3 Résultats et Discussion

Un système et un procédé pour une distribution quantique de clés sur un réseau (WDM) en sont représentés dans la Figure.III.1. La Figure.III.2 montre le taux d'erreur binaire quantique (QBER) en fonction de la distance de propagation en km, les canaux sont variés entre -10 et -30 dBm. L'émetteur peut sélectionner un récepteur parmi les récepteurs à communiquer avec celui-ci, et transmet des signaux quantiques au récepteur sélectionné sur le réseau WDM.

Les signaux quantiques sont d'une longueur d'onde égale à une longueur d'onde de réception, du récepteur. Par conséquent, le réseau WDM permet aux signaux quantiques à communiquer entre l'émetteur et les récepteurs avec un routage de longueur d'onde. Un réseau de communication comporte une pluralité de nœuds interconnectés par un milieu de transmission optique. Le support de transmission est capable de supporter une pluralité de longueurs d'onde organisées en bandes. Un filtre à chaque nœud pour passer une bande qui lui est associée, et passivement transmet d'autres bandes à travers le support de transmission [4].

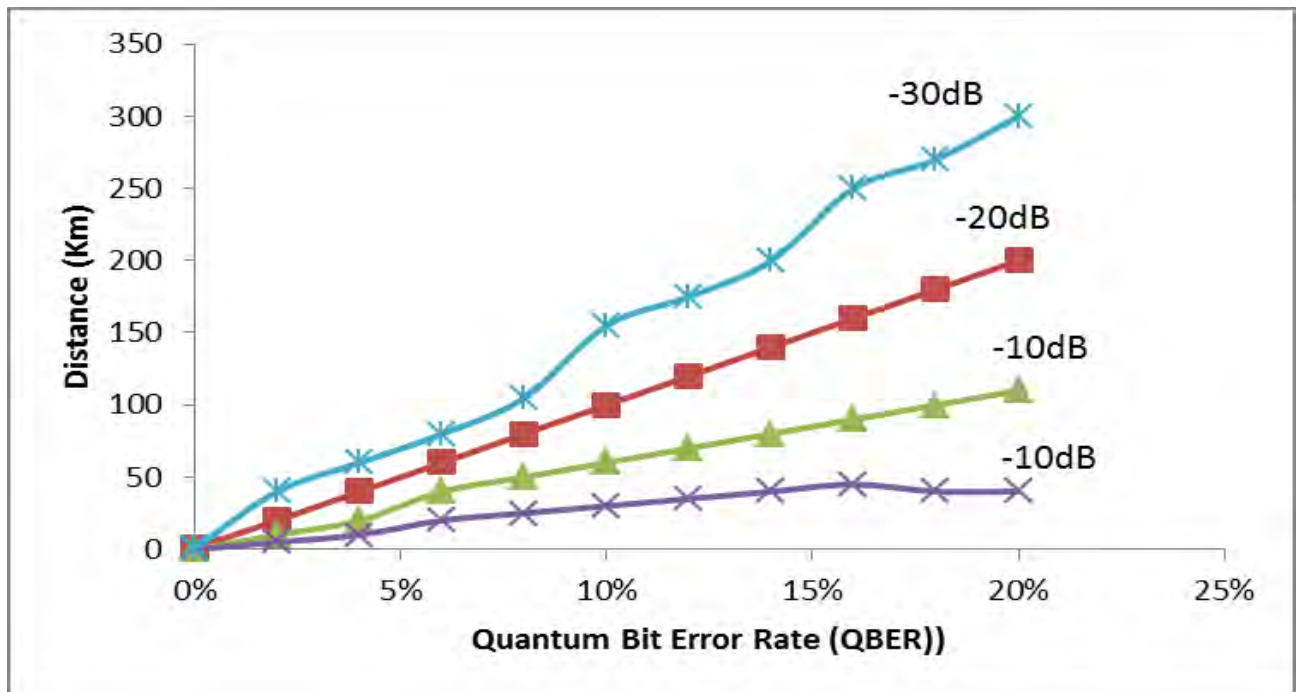


Figure.III.2 La réponse du QBER en fonction de la distance de propagation

Un dispositif est prévu au niveau de chaque nœud pour l'ajout d'une bande au support de transmission. La communication peut être établie directement entre une paire de nœuds dans le réseau partageant une bande commune sans l'intervention active d'un nœud intermédiaire. Cela permet au réseau d'être indépendant du protocole. En outre, les faibles pertes subies par les filtres passifs permettent relativement un long trajet sans amplification optique.

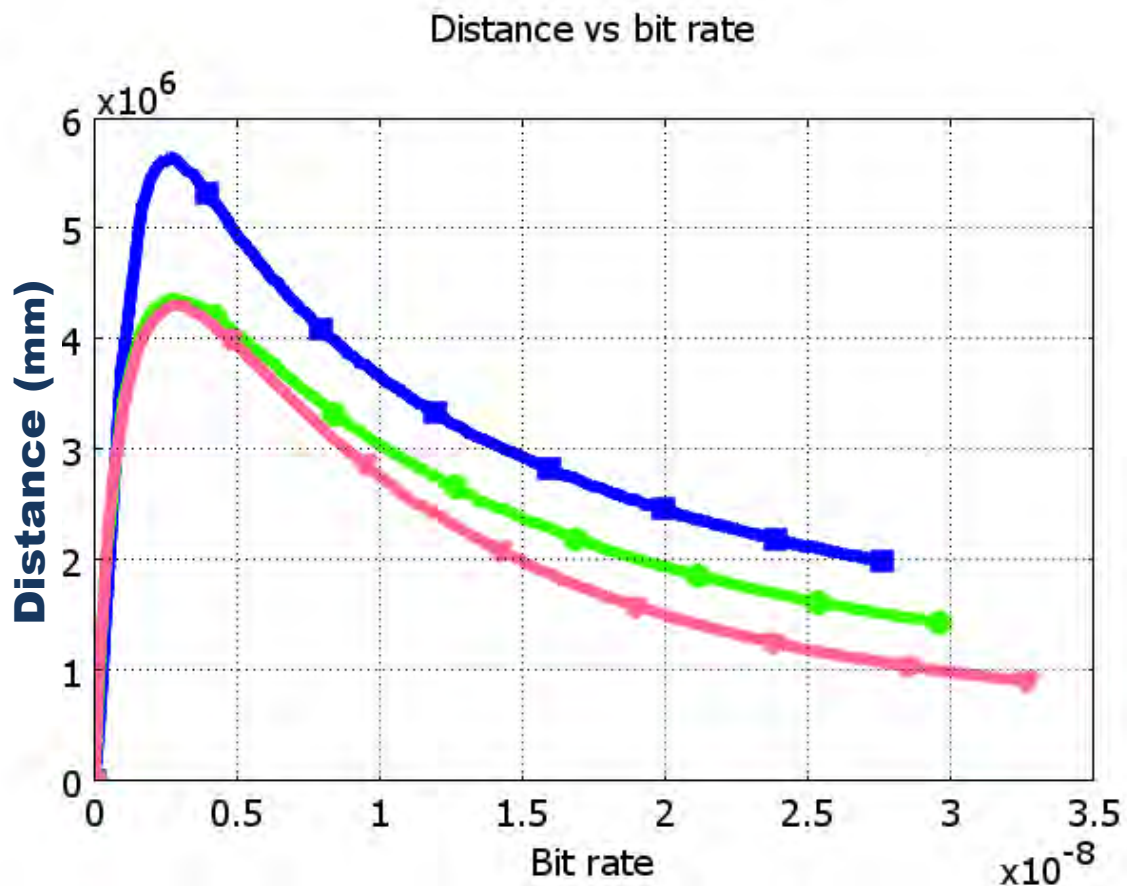


Figure.III.3 Le débit binaire en fonction de la distance

La Figure.III.3 montre le taux de génération de clé qui est le débit binaire quantique en fonction de la distance en ligne avec les paramètres de transmission et avant le canal de réduction de la distance de transmission. La transmission maximale est d'environ 6 km et qui est prévu, le taux est d'une amplitude stable, alors que le minimum est obtenu pour l'échange de données aléatoires ou fluctuante.

La différence entre la phase aléatoire et uniforme est tout à fait évidente donc bien que les deux sont tracés, seule la phase de données uniforme est visible et atteint une longue distance. Comme mentionné ci-dessus que la distance maximale de transmission est atteinte à un taux d'environ 6 Km, avec un débit binaire plus faible autour de 2.5×10^{-7} . Cela est en accord avec le principe général des phénomènes congestionnées et décongestionnées; si le canal est entièrement occupé par des données aléatoires, le canal sera certainement faible, et aussi par ce que les données sont entièrement limitée à voyager loin [12], [14]. Pour trouver le taux de génération de clé de transmission maximale, le débit binaire pour chaque distance a

été calculé pour tous les modèles trouvés et on peut constater que l'amplitude stable donne le meilleur taux de génération de clé [4].

Pour une amplitude variable, les fluctuations non-aléatoires semblent d'être mieux. Il donne en fait à la même distance de transmission maximale, seulement avec un taux inférieur autour de 2.5×10^{-7} . La raison de ceci peut être que au moins une ces valeurs est la valeur optimale. Par conséquent, de nombreuses impulsions seront des amplitudes non-optimales, qui ont le taux le plus bas. La fluctuation aléatoire donne un taux plus faible pour toutes les distances, et une distance maximale plus courte. Lors de la présence des fluctuations aléatoires, le modèle n'a aucune connaissance préalable de l'amplitude. Ainsi, après avoir les fluctuations annoncées donnent un autre modèle, cette connaissance préalable devrait donner un avantage au modèle, et le taux de génération de clé devient inférieur. Cependant, nous devons rappeler que, dans ces deux situations, les canaux partagent la même connaissance de l'amplitude en tant que troisième dose. Par conséquent, nous pouvons interpréter de ce complot qu'il vaut mieux que tous donné l'amplitude que rien.

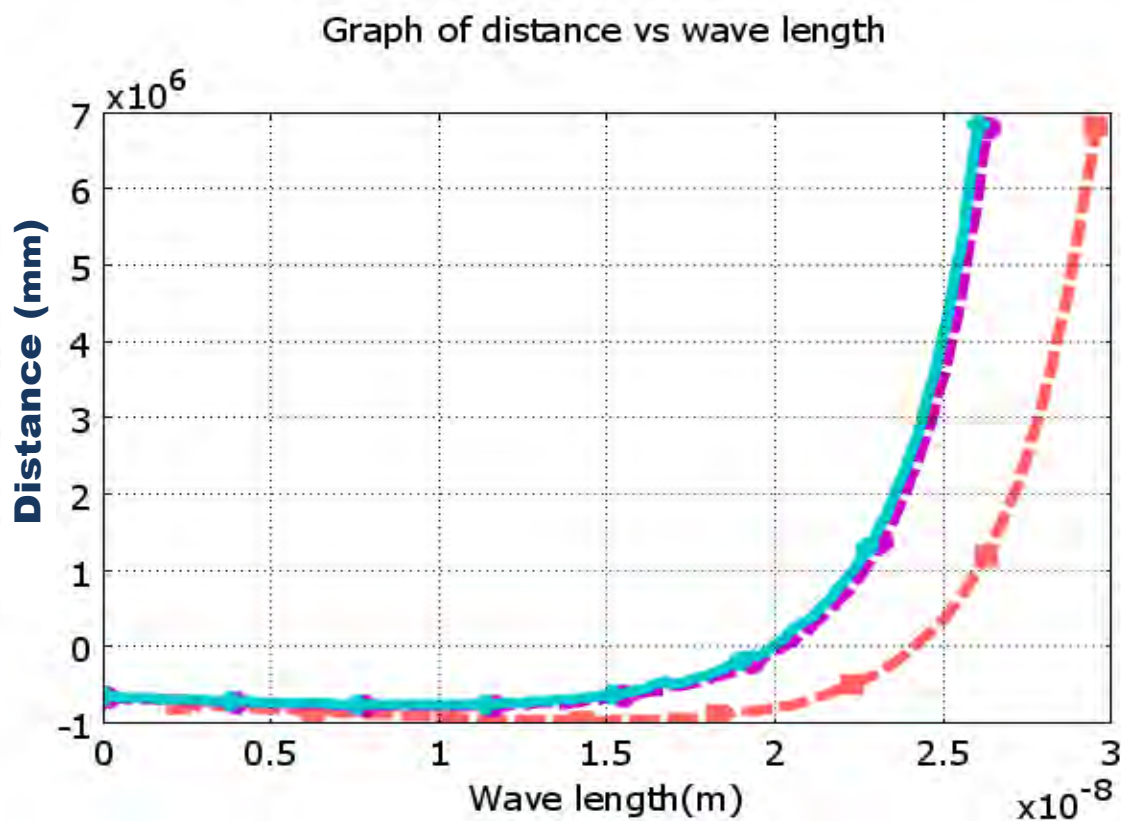


Figure.III.4 Les longueurs d'onde dynamiques avec une augmentation de la couverture de la distance avec diminution de la longueur d'onde

Les différentes longueurs d'onde de distribution quantique (QKD) sont mesurées en fonction de la distance en kilomètres, comme illustré sur la figure.III.4. Le taux d'erreur binaire quantique est en grande partie dépend de l'intégrité du canal et le système d'exploitation sur le même milieu que le conventionnel entre 200 à 250 nm de longueur d'onde du canal, la couverture à distance rapide a été remarqué pour trois modèles avec un seul modèle surpasse le système d'exploitation en la même bande que près de 250 nm et bien sûr, lorsque la longueur d'onde augmente. Il est prévu que la couverture à distance devrait augmenter, bien que tous les modèles de meilleures performances du plus loin, il est à partir du signal classique comme la longueur d'onde augmente [4]. On peut déduire que les longueurs d'onde principales de fonctionnement optimum de distribution quantique se trouvent dans la région supérieure à 250 nm.

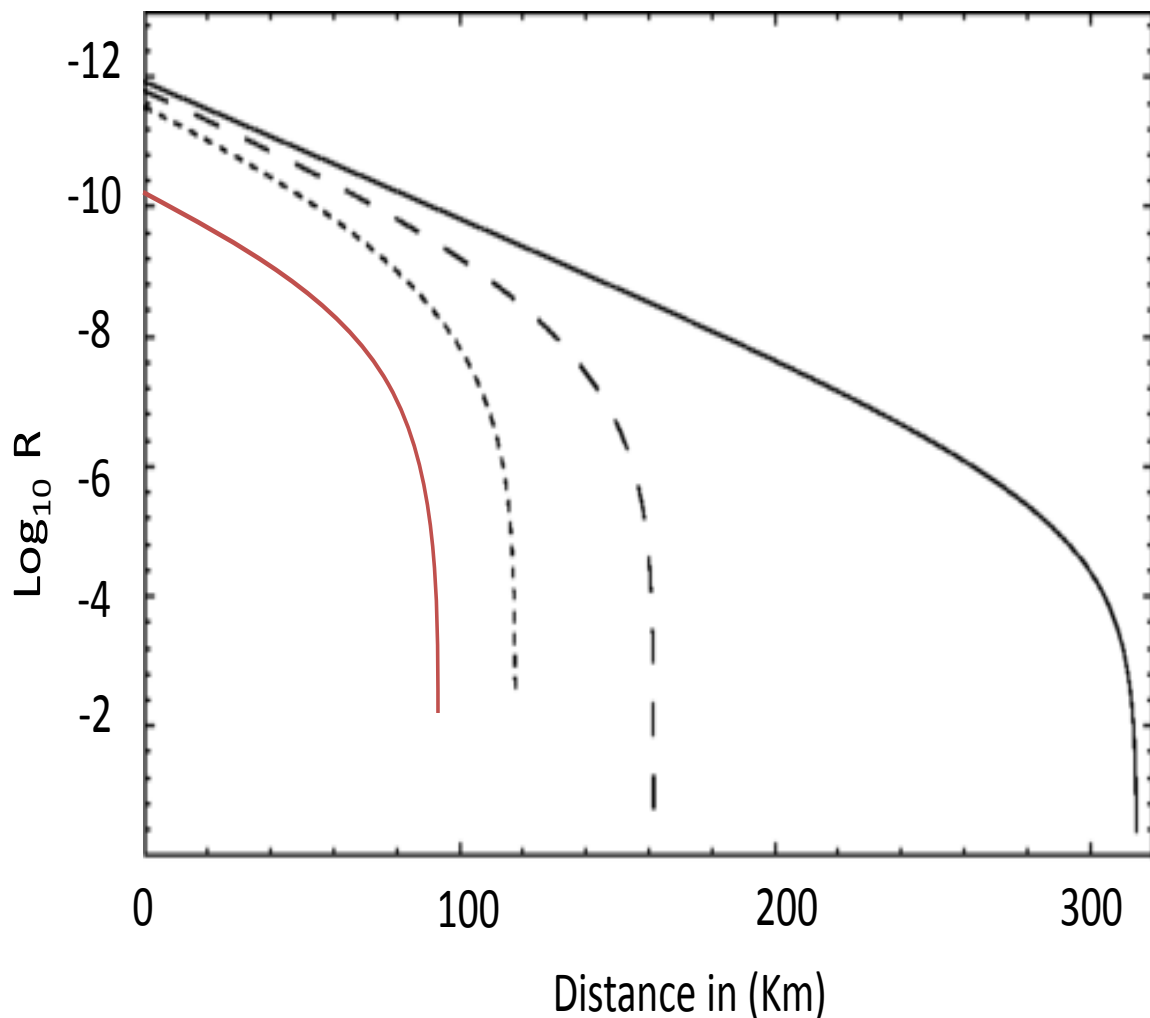


Figure.III.5 La fonction $\log_{10} R$ pour le taux de transmission en fonction de la distance

La figure.III.5 fournit un système de communication pour la distribution de clé quantique avec une structure relativement simple et une grande efficacité de la communication pour 4 utilisateurs différents avec un débit de transmission différent. Le système fournit un procédé de distribution de clé quantique entre un émetteur et plusieurs récepteurs sur un réseau (WDM) avec le routage de longueurs d'onde qui comprend. Il a été identifié par l'attribution d'un récepteur de longueur d'onde différente pour chacun des récepteurs, où la sélection d'un récepteur parmi les récepteurs à communiquer avec l'émetteur et de transmission de signaux de clé quantique de l'émetteur vers le récepteur sélectionné sur le réseau WDM. Les quatre récepteurs sont situés à 300 km dans lequel les signaux de clé quantique sont sur une longueur d'onde identique à la réception de la longueur d'onde du récepteur de la Figure.III.5.

Le système de communication est constitué d'un émetteur de plusieurs récepteurs, chaque récepteur ayant une longueur d'onde distincte; et un réseau WDM reliant l'émetteur au récepteur, l'émetteur sélectionne dans celui-ci un récepteur parmi les récepteurs à communiquer avec celui-ci, et transmet des signaux quantiques du récepteur sélectionné sur le réseau WDM. Les signaux quantiques sont transmis sur une longueur d'onde égale à la longueur d'onde de réception, du récepteur et cette distance, il peut couvrir par fidélité du canal.

Selon la présente figure, une technologie de routage de longueur d'onde est utilisée pour l'implémentation de la distribution quantique de clé pour une pluralité de récepteurs et peuvent être identifiés en communication de données sûres. Le routage de longueur d'onde peut être réalisé par une division de longueur d'onde, qui peut être sous la forme d'un réseau de guide d'onde (AWG). En outre, le système peut utiliser alternativement relié par un moyen, qui est adapté à l'utilisateur du réseau. Toujours à partir de Figure.III.5, la lumière à onde continue est utilisée dans le système, ce qui peut améliorer la sécurité du système. En plus, la détection de phase différentielle est également employé est l'un des aspects les plus importants afin de surmonter l'influence d'un changement de paramètre et de décalage de phase dans le système, qui peut en outre rendre le système simple et stable.

III.4 Conclusion

En général, la présente étude démontre un système de communication pour le réseau de distribution quantique de clé, le mode de phase de transmission aléatoire et uniforme ont été étudiés pour une amplitude stable. Les résultats de la phase aléatoire ont montré une couverture de distance minimale sur la phase non-aléatoire. Pour la fluctuation d'amplitude de spectacles aléatoires montre un changement dans les performances du système amélioré. Par conséquent, il est conclu que les fluctuations rares ne doivent pas dégrader les performances du système de manière significative, mais le mode d'envoi de données a un effet significatif sur l'intégrité du canal. Bien que, l'étude n'a pas l'accent sur l'aspect de la sécurité de la chaîne, mais on peut être entendu que, les fluctuations non-aléatoires devrait donner une meilleure performance que les fluctuations aléatoires.

Il semble que c'est mieux pour le mode 1 et de partager leurs informations sur l'amplitude avec un troisième mode. Dans lequel un émetteur peut communiquer via un réseau de communication quantique classique avec plusieurs récepteurs; en utilisant une clé secrète différente émis à une longueur d'onde différente pour chaque récepteur différent.

III.5 Introduction

Pour la densification du trafic de données sur les réseaux de télécommunications, de multiples techniques d'accès, tels que l'accès multiple à répartition de fréquence (FDMA: Frequency Division Multiple Access) et l'accès multiple à répartition du temps (TDMA : Time Division Multiple Access), ont été développés. Ces procédés de multiplexage sont utilisés dans les transmissions RF, ainsi que dans les systèmes de communication optiques.

Le multiplexage par répartition en longueur d'onde (WDM : wavelength division multiplexing) représente une transposition de AMRF dans des réseaux optiques. L'accès multiple à répartition du code (CDMA : Code Division Multiple Access) est un système de multiplexage défini comme un étalement du spectre[15]. Cette technique a été initialement conçu pour des applications militaires. Elle permet, par l'étalement de la puissance sur une large bande de fréquences de canal, une meilleure résistance aux phénomènes d'évanouissement et donne le signal transmis la forme d'un bruit, ce qui lui rend difficile à détecter par des récepteurs non destinataires.

Plusieurs études relatives à la transposition des techniques CDMA dans les systèmes de communication optiques datent des vingt dernières années. Prenant l'avantage de la grande largeur de bande disponible dans le canal optique, la technique CDMA optique (OCDMA) vise également à accroître la capacité de multiplexage en augmentant le nombre d'utilisateurs au détriment de la détérioration de la qualité de la liaison [16-17].

On peut distinguer deux approches du OCDMA; approche cohérente et incohérente. Dans le système de OCDMA incohérent, l'interférence d'accès multiple (MAI; Multiple Access Interference) est l'une des principales limitations dues à l'utilisation des codes unipolaires. Pour réduire cet effet [18], plusieurs techniques sont proposées pour éliminer la contribution des utilisateurs indésirables. La technique d'accès multiple par répartition de codes dans le domaine spectral (Spectral Amplitude Codage - Optical Code Division Multiple Access, SAC-OCDMA) donne une meilleure solution pour réduire l'effet des interférences par le code utilisé avec corrélation croisée flexible [19].

De nombreuses recherches ont été rapportés dans la littérature pour le but de développer de nouveaux codes pour le système SAC-OCDMA tels que; les codes orthogonaux optiques 'OOC', le code 'Prime' [20], le code ; Frequency-Hopping 'MFH' [21], le code Double-Weight 'DW' [22], le code Double-Weight modifié 'MDW' [23], le code

Random diagonal 'RD' [24] et le code Flexible Cross Correlation „FCC“ [25]. Toutefois, ces codes souffrent de diverses limitations telles que; la complication de la construction, la faible corrélation croisée, et la longueur de code trop longue.

Dans cette partie, nous proposons une nouvelle famille de code le système SAC-OCDMA. Puisque le concept du code est basé sur la corrélation croisée flexible (FCC), on le donne le nom Corrélation Cross Flexible Modifié (MFCC). Ce chapitre est organisé comme suit; le concept du code proposé et la partie analyse sont décrites respectivement dans la deuxième et la troisième section. Les résultats et les discussions sont inclus dans la section quatre. Enfin, une conclusion de ce travail est fournie dans la dernière section.

III.6 Concept du code

III.6.1 Préliminaires mathématiques

Les codes optiques sont de famille de K (K utilisateurs) séquences binaires $[0, 1]$ de longueur N , une corrélation croisée maximale, λ_{\max} et un poids w . Le jeu de code optimal est celui qui a des propriétés de corrélation croisée minimum pour supporter un nombre maximal d'utilisateurs avec une longueur minimale du code [21]. Cela garantit une meilleure qualité de services avec de faible probabilité d'erreur pour un nombre d'utilisateurs donné au moins pour les réseaux optiques à courte distance.

Il est montré que le goulot d'étranglement majeur dans la mise en œuvre de tous les réseaux optiques est fondamentalement le MAI lorsque tous les utilisateurs essaient de transmettre leurs données simultanément. Ce problème peut être surmonté par la conception des séquences de code de telle sorte qu'ils peuvent causer moins de chevauchement entre les chips de données [26].

Soient $A = \{a_i\}$ et $B = \{b_i\}$ les séquences de longueur N tel que:

$$\left. \begin{array}{l} \{a_i\} = '0' \text{ or } '1', \quad i = 0, \dots, N-1 \\ \{b_i\} = '0' \text{ or } '1', \quad i = 0, \dots, N-1 \end{array} \right\} \quad (\text{III.3})$$

Les fonctions d'auto-corrélation et de corrélation croisée de ces séquences sont définies, respectivement, par

$$\lambda_a(\tau) = \sum_{n=0}^{N-1} a_n a_{n+\tau} \quad (III.4)$$

$$\lambda_{ab}(\tau) = \sum_{n=0}^{N-1} a_n b_{n+\tau} \quad (III.5)$$

où a_n est une séquence binaire $\{0, 1\}$, la valeur maximale de $\lambda_a(\tau)$ dans l'équation (2) est pour $\tau = 0$ et est égal à w , le poids de la séquence. Donc,

$$\lambda_a(0) = w \quad (III.6)$$

Si λ_{xm} et λ_{xym} désignent les valeurs maximales d'auto-corrélation et de corrélation croisée respectivement, puis un code optique de longueur 'N' et de poids «W» peut être écrit comme $(N, W, \lambda_{xm}, \lambda_{xym})$ ou $X_{\max} = \max \{\lambda_{xm}, \lambda_{xym}\}$. Il peut également être noté que pour un code optique avec un poids 'W', l'auto-corrélation peut être écrit comme suit;

$$\lambda_{a \max} = \sum_{n=0}^{N-1} a_n a_n = w \quad (III.7)$$

En pratique pour K utilisateurs, il est nécessaire d'avoir un nombre K de codes dans un ensemble de valeurs données de N, W, λ_{am} et λ_{abm} . Les codes décrits par l'équation (III.3) peuvent également être représentés sous forme de vecteur, comme;

$$\left. \begin{array}{l} A = \{a_i\} \text{ for } i = 0, \dots, N-1 \\ B = \{b_i\} \text{ for } i = 0, \dots, N-1 \end{array} \right\} \quad (III.8)$$

Où A et B sont des vecteurs de longueur 'N' avec des éléments tels que définis par l'équation (6). En terme de vecteurs A et B, l'équation (III.4) et l'équation (III.5) sont écrites comme suit;

$$\lambda_A(0) = AA^T = w \quad (III.9)$$

III.6.2 Construction de Code

Le code MFCC est conçu en utilisant trois paramètres; N, w et λ_c qui représentent respectivement la longueur du code, le poids de code (le nombre de "1" dans chaque mot de code) et la propriété de corrélation croisée du code MFCC proposé. Le nouveau code MFCC

optique est représenté dans une matrice $K \times N$ où K lignes représentent le nombre d'utilisateurs et N colonnes représentent la longueur minimale du code. Il se compose de deux sous-matrices A et B, comme suit:

$$MFCC = [A||B]_{K \times N} \quad (III.10)$$

Certaines propriétés sont notées durant la construction du code proposé, y compris:

La première sous-matrice A est conçu de telle sorte que la corrélation croisée (λ_c) entre deux cubes consécutifs est égal à 0. Bien que la matrice B est conçue avec $\lambda_c=1$.

La longueur de la matrice doit être égale à K , où K représente le nombre d'utilisateurs. Tandis que la longueur de la matrice B doit être égale à $K + 1$. Ainsi, la longueur totale du code MFCC est égale à;

$$N = 2(K - 1) + w \quad (III.11)$$

La propriété d'auto-corrélation et de la corrélation croisée peuvent être écrites comme:

$$\sum_{i=1}^N C_k(i)C_l(i) = \begin{cases} w; & k = l \\ 1; & k \neq l \end{cases} \quad (III.12)$$

où $C_k(i)$ représente la $i^{\text{ième}}$ composante du $K^{\text{ième}}$ MFCC code.

En utilisant les propriétés mentionnées ci-dessus, le code MFCC pour trois utilisateurs peut être écrit comme suit;

$$MFCC = \begin{bmatrix} 1 & 0 & 0 & | & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & | & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & | & 0 & 0 & 1 & 1 \end{bmatrix} \quad (III.13)$$

dans ce cas $K=3$ and $N=7$ for $w=3$.

Le mot de code pour chaque utilisateur d'après (III.13) devient;

$$MFCC = \begin{cases} User1; & \lambda_1, \lambda_4, \lambda_5 \\ User2; & \lambda_2, \lambda_5, \lambda_6 \\ User3; & \lambda_3, \lambda_6, \lambda_7 \end{cases} \quad (III.14)$$

III.7 Analyse numérique des performances du code MFCC

Pour évaluer les performances du code MFCC proposé, le rapport signal sur bruit (SNR) et le taux d'erreur binaire (BER) doivent être calculé en utilisant les équations suivantes:

$$SNR = I^2 / \sigma^2 \quad (III.15)$$

où I représente le courant incident, exprimé par:

$$I = \Re \int_0^{\infty} G(\nu) d\nu \quad (III.16)$$

et σ^2 est la variance du bruit, qui est la somme des puissances du bruit de grenaille 'Shot', de bruit PIIN (Phase Induced Intensity Noise) et de bruit thermique;

$$\sigma^2 = I_{shot}^2 + I_{PIIN}^2 + I_{thermal}^2 \quad (III.17)$$

A partir de l'équation (III.16), le \Re représente la photodiode PIN.

En outre, la densité spectrale de puissance est donnée à partir de la référence [27] par

$$G(\nu) = \sum_{k=1}^k d_k \left(\sum_{i=1}^N C_k(i) C_l(i) - \sum_{i=1}^N C_k(i) (C_k(i) C_l(i)) \right) \left\{ u \frac{\Delta\nu}{N} \right\} \quad (III.18)$$

où

$$\sum_{i=1}^N C_k(i) C_l(i) = \begin{cases} W; & k = l \\ 1; & k \neq l \end{cases} \quad (III.19)$$

$$\sum_{i=1}^N C_k(i) (C_k(i) C_l(i)) = \begin{cases} 1; & k = l \\ 1; & k \neq l \end{cases} \quad (III.20)$$

$$\sum_{i=1}^N C_k(i) C_l(i) - \sum_{i=1}^N C_k(i) (C_k(i) C_l(i)) = \begin{cases} W-1; & k = l \\ 0; & k \neq l \end{cases} \quad (III.21)$$

A partir des équations (III.16) et (III.19), le courant incident devient;

$$I = \Re \frac{P_{sr}}{\Delta\nu} (W-1) \quad (III.22)$$

et les puissances de bruit sont données comme suit;

$$I_{shot}^2 = 2eBI = 2eB\Re \int_0^{\infty} G(\nu) d\nu \quad (III.23)$$

$$I_{shot}^2 = 2eB\Re \frac{P_{sr}}{\Delta\nu} (W + 3) \quad (III.24)$$

$$I_{PIN}^2 = B I^2 \tau_c = B \int_0^{\infty} G(\nu)^2 d\nu \quad (III.25)$$

$$I_{PIN}^2 = \frac{B\Re^2 P_{sr}^2 KW}{N^2 \Delta\nu} (W + 3) \quad (III.26)$$

et

$$I_{thermal}^2 = \frac{4K_b T_n B_r}{R_L} \quad (III.27)$$

A partir des équations ci-dessus le SNR peut être écrit comme suit:

$$SNR = \frac{\left(\Re P_{sr} (W - 1) \right)^2}{N} \quad (III.28)$$

$$\left[\frac{2eB_r \Re P_{sr}}{N} (W + 3) + \frac{B\Re^2 P_{sr}^2 KW}{N^2 \Delta\nu} (W + 3) + \frac{4K_b T_n B_r}{R_L} \right]$$

Tous les paramètres de l'équation (III.28) sont décrits dans le tableau.III.1

Tableau.III.1.Description des paramètres.

Paramètre	Description
E	La charge d'électron
B	Bande passante
Kb	La constante de Boltzmann
Tn	La température absolue
RL	Résistance de charge

Le taux d'erreur binaire est obtenu en utilisant le SNR par l'équation suivante;

$$BER = \frac{1}{2} \operatorname{erfc} \left(\sqrt{\frac{SNR}{8}} \right) \quad (\text{III.29})$$

III.8 Résultats Et Discussions

Les performances du système est analysé en utilisant les paramètres énumérés dans le tableau.III.II.2 et les résultats numériques sont présentés aux figures III.6-III.7.

Afin de comparer les performances de notre code avec ceux existants, nous avons tracé le taux d'erreur binaire (BER) en fonction du nombre d'utilisateurs pour notre code et deux autres codes; le code 'MDW' et le code 'RD' avec un poids $W = 4$, comme illustré sur la figure.III.6. A partir cette figure, on peut constater que notre code offre des performances améliorées par rapport aux codes de MDW et RD, avec un faible taux d'erreur binaire BER (moins de 10^{-9}).

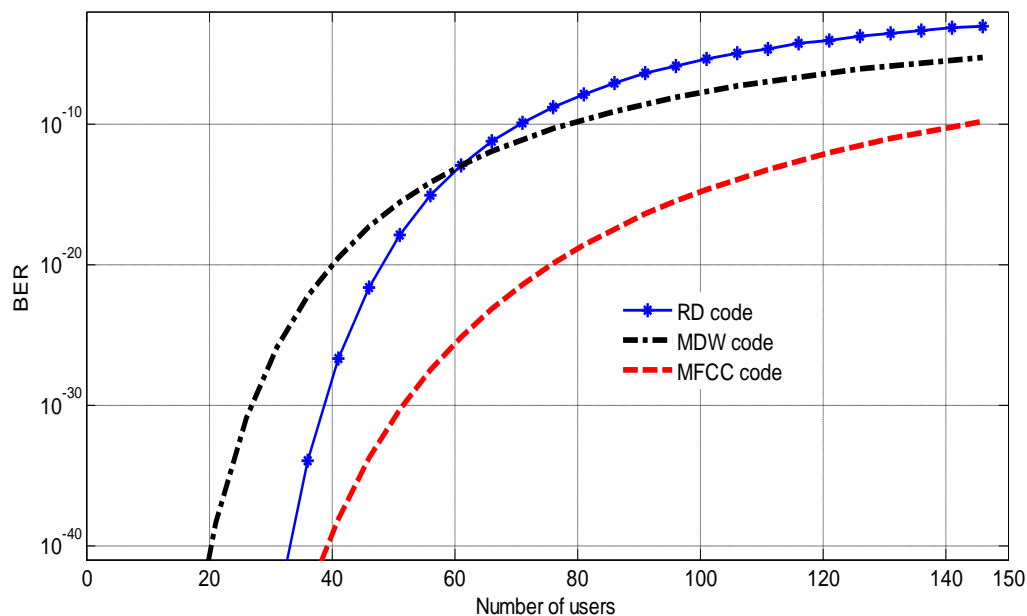


Figure.III.6 Variation de BER en fonction du nombre des utilisateurs pour les codes MFCC, MDW and RD.

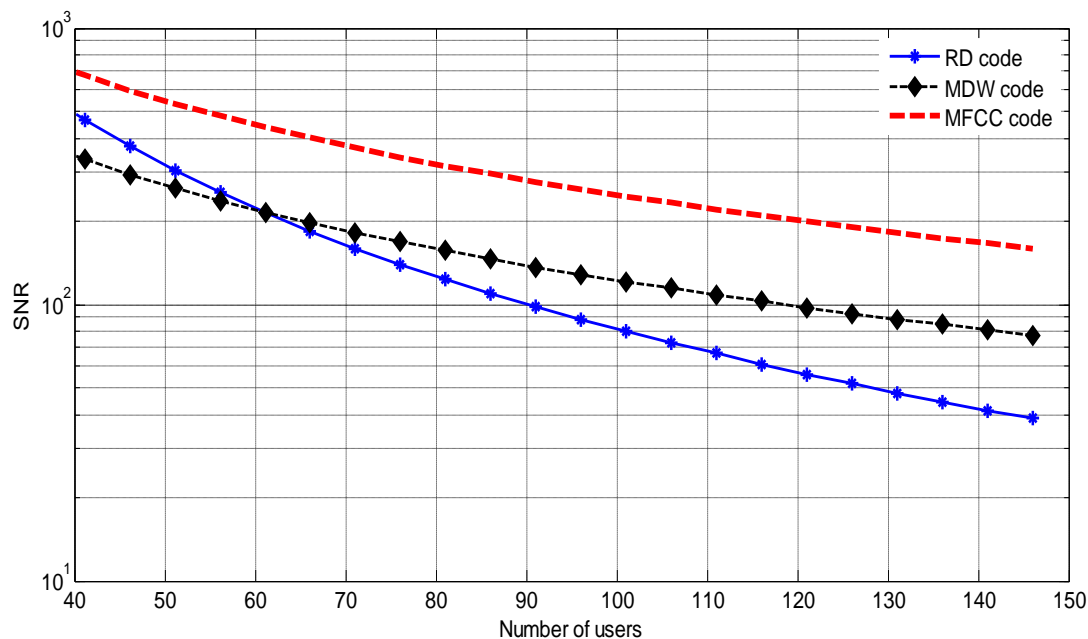


Figure.III.7. Variation de SNR en fonction du nombre des utilisateurs pour les codes MFCC, MDW and RD.

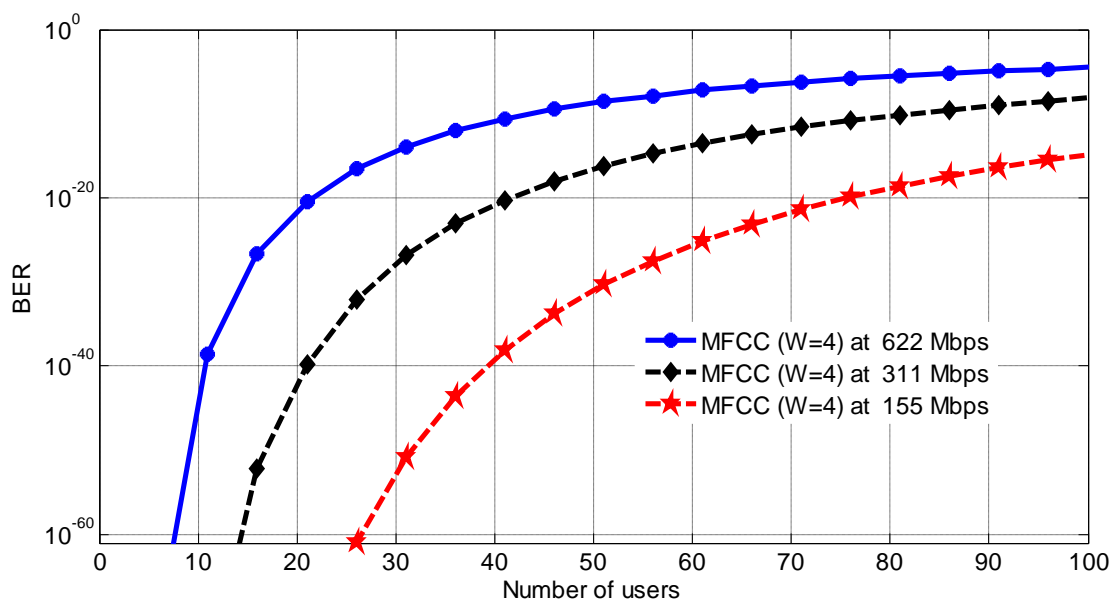


Figure.III.8. Variation de BER en fonction du nombre des utilisateurs pour le code MFCC MFCC avec différents débits de transmission de données.

Table.III.2. Paramètres utilisés dans les calculs numériques :

Efficacité quantique	$\eta = 0.75$
Spectral width of broadband light source	$\Delta\lambda = 30\text{nm}$ ($\Delta\lambda = 3.75 \text{ THz}$)
La longueur d'onde d'opération	$\lambda_o = 1550\text{nm}$
La bande passante	$B = 155 \text{ MHz}$
Débit de transmission de données	$R_b = 622 \text{ Mbps}$
Température du bruit de récepteur	$T_n = 300\text{K}$
La résistance de charge	$R_L = 1030\Omega$
Constante de Boltzmann	$K_b = 1.38 \times 10^{-23} \text{ W/K/Hz}$
La charge d'électron	$e = 1.60217646 \times 10^{-19} \text{ coulombs}$
Célérité de la lumière	$C = 3 \times 10^8 \text{ m/s}$

La Figure.III.7 présente une comparaison de la performance des codes MFCC avec les MDW et RD codes en terme de la variation du rapport signal sur bruit (SNR) et le nombre d'utilisateurs, il peut être constaté que le code proposé 'MFCC' présente des performances significativement mieux (avec un SNR élevé) que celles des autres codes. Ce qui assure une bonne qualité de transmission des données.

Enfin, l'effet débit de transmission des données sur les performance du code MFCC proposé est étudié, en traçant le taux d'erreur binaire 'BER' pour différentes valeurs du R_b , comme il est illustré sur la figure.III.8. A partir de ces courbes, on conclut l'augmentation de débit de transmission de données et la dégradation et il est sur les performances du système.

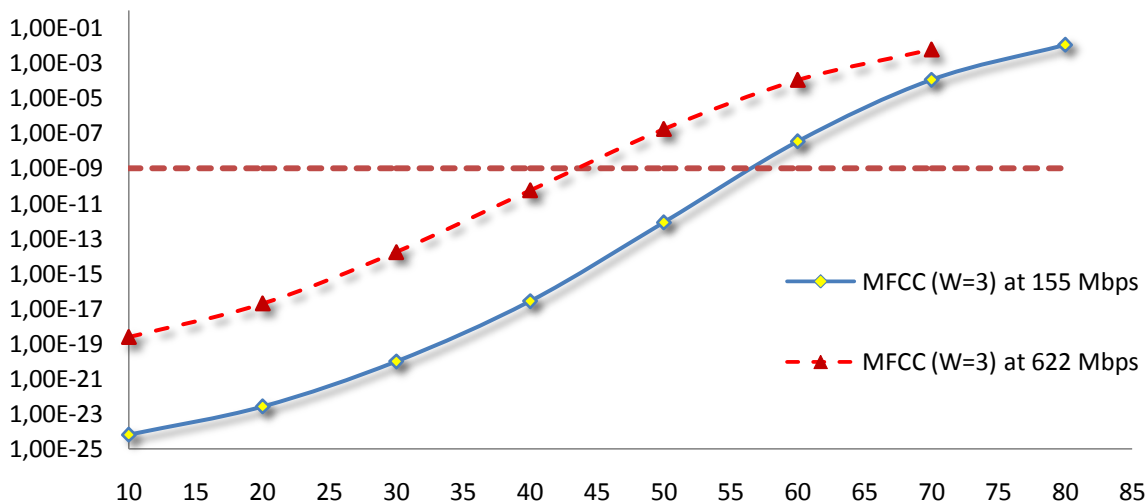


Figure.III.9Variation de BER en fonction de la longueur de fibre pour le code MFCC avec différents débits binaire de données($W=3, \kappa=3$)

On observe sur la figure.III.9, la conception entre la longueur de la fibre et les performances du système BER pour le code MFCC ($W=3$) pour différentes débits binaires 155 Mbps et 622 Mbps. On peut voir que à la performance du système BER 10^{-9} MFCC ($W=3$) 155 Mbps avoir de manière significative de meilleurs BER d'exécution de système où il est capable d'atteindre un BER acceptable d'exécution de système jusqu'à une longueur de fibre 55 km. Il est différent lorsque la MFCC ($W=3$)622 Mbps, seulement peut exécuter jusqu'à une longueur de fibre 44 km avec le même BER d'exécution de système de seuil. De cette observation, M FCC ($W = 3$) à 155 Mbps peut éliminer avec succès et supprimé les effets de *PIIN* et MAI pour le système de codage SAC-OCDMA.

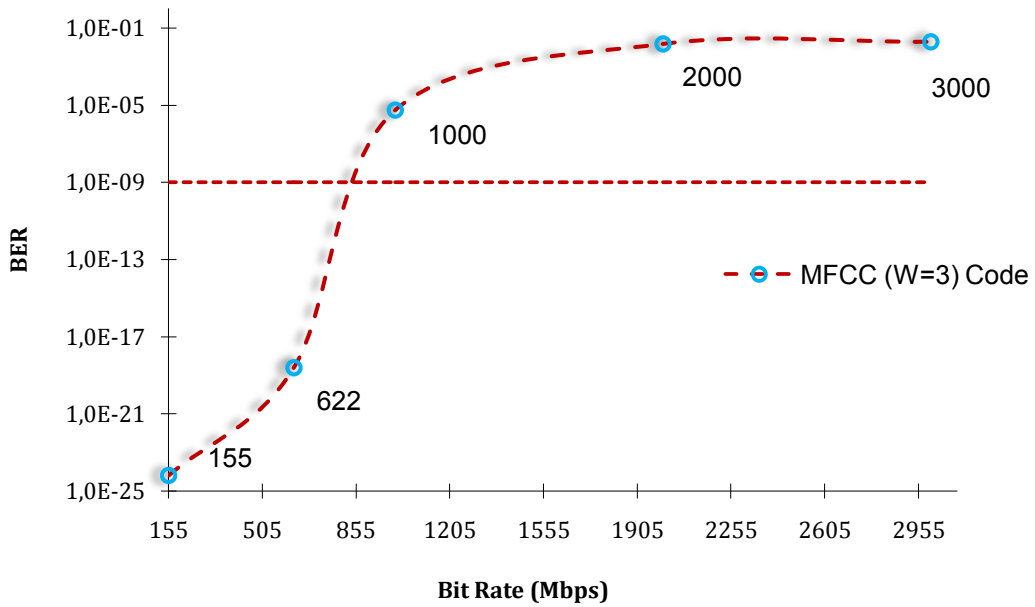


Figure.III.10 Variation de BER en fonction des différents débits binaires de données (W=3, K=3)

La figure.III.10 montre la variation du BER contre différents débits binaires utilisant le code MFCC. Le débit varie de 155 Mbps à 3Gbps avec même Hemming poids $w=3$; Il a montré que l'augmentation du débit binaire, BER va diminuer. Nous peut déterminer ce que lorsque l'on augmente le débit binaire de la largeur d'impulsion diminue également, produisant ainsi des bits sensibles signalé à la dispersion effet.

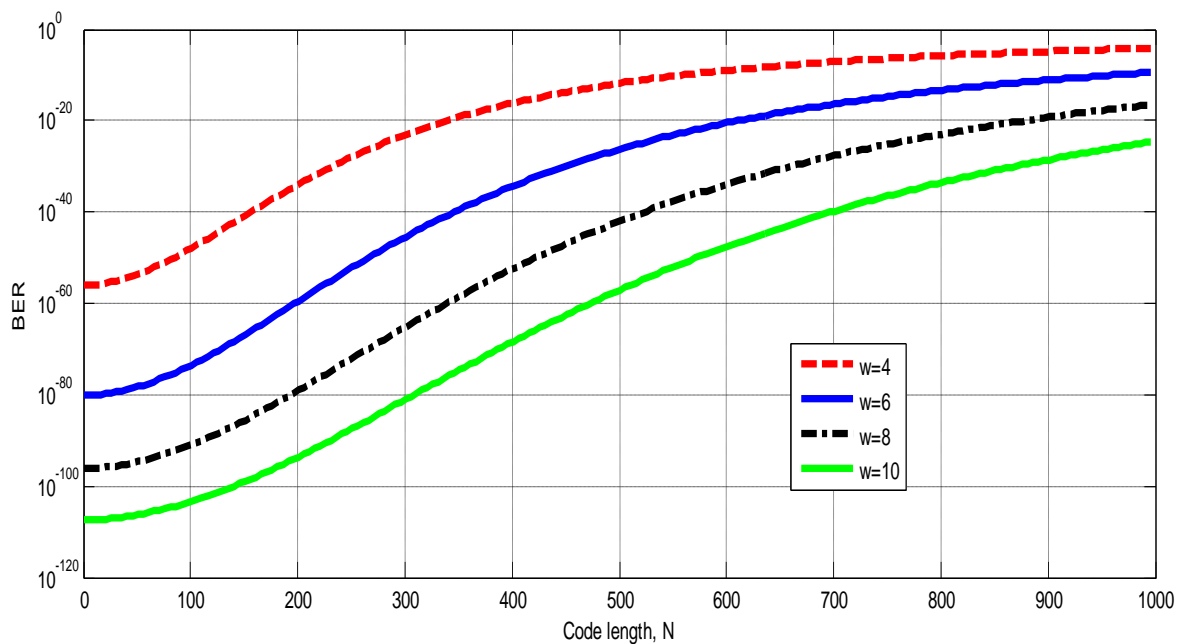


Figure.III.11 Code MFCC avec différentes longueurs de code par rapport BER

La figure.III.11 montre le BER augmentera comme une augmentation de la longueur du code. Chaque courbe représente une autre valeur du poids. Il est évidemment montré que le BER est plus faible pour un plus grand poids, $w = 10$ en tant que comparaison avec un poids égal à 4, 6 et 8, pour un nombre constant d'utilisateurs et d'une puissance égale de chaque composante spectrale. Le nombre élevé de longueur de code, sans augmenter le poids, il faudra un grand nombre de la bande passante et produira plus d'effets de bruit. En outre, le poids de plus en plus permettra d'améliorer BER en raison de l'efficacité pouvoir recevoir, P_{sr} dans le spectre.

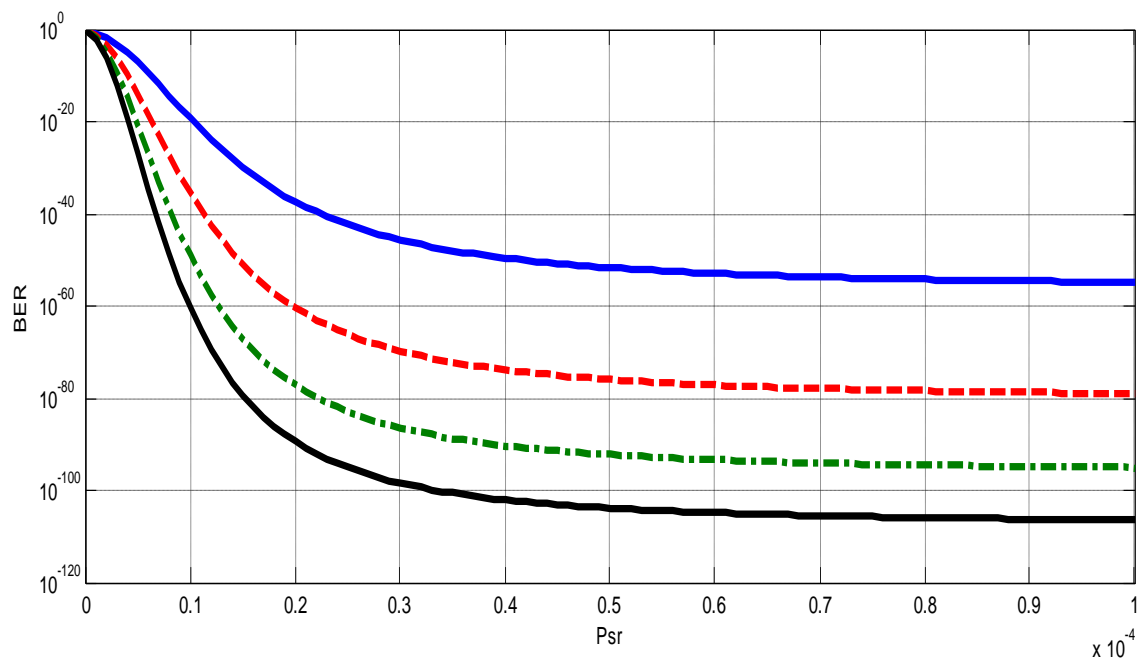


Figure.III.12 Variation de BER en fonction de la Puissance efficace pour 30 utilisateurs, $w=4$, $w=6$, $w=8$ & $w=10$

Figure.III.12 montre l'impact de l'utilisateur effectif puissance sur le taux d'erreur binaire au poids de code $w = 4, 6, 8$ et 10 pour 30 utilisateurs. L'impact du poids de code est observé sur une large gamme de puissance efficace. Il est clair à partir de cette graphique que lorsque plus le nombre d'utilisateurs tente d'accéder au canal optique avec une puissance effective importante reçu au niveau du récepteur, le taux d'erreur binaire est diminué de manière significative.

III.9 CONCLUSION

Un nouveau code Corrélation Cross Flexible (MFCC) été étudié et proposé pour le système de transmission optique OCDMA. L'analyse est effectuée en calculant le rapport signal sur bruit (SNR) et le taux d'erreur binaire (BER), en tenant compte de l'effet du bruit de grenaille, PIIN et sources de bruit thermique. Afin d'évaluer la performance du code proposé, les résultats numériques obtenus à partir de l'implémentation de ce code sont comparés à ceux de deux autres codes; codes MDW et RD.

De cette comparaison, il est constaté que le code MFCC est le meilleur en termes de BER par rapport aux codes MDW et RD. En outre, la simplicité dans la construction de code proposé et la flexibilité dans le contrôle de corrélation croisée a fait ce code un candidat adéquat pour les futures applications basant sur la technique OCDMA.

Références bibliographiques du chapitre III

- [1] A. Vaziri, G. Weihs, and A. Zeilinger, “Experimental Two-Photon, Three-Dimensional Entanglement for Quantum Communication,” *Phys. Rev. Lett.*, vol. 89, no. 24, p. 240401, Nov. 2002.
- [2] Y. Chen and W. Tang, “Reconfigurable asymmetric optical burst switching for concurrent DWDM multimode switching: architecture and research directions [Topics in Optical Communications],” *IEEE Communications Magazine*, vol. 48, no. 5. pp. 57–65, 2010.
- [3] G. V Chowdhary, C. Siva, and R. Murthy, “Dynamic Multicast Traffic Engineering in {WDM} Groomed Mesh Networks,” *Proc. {IEEE Broadnets} '2004*, 2004.
- [4] A. Khalil, C. Assi, A. Hadjiantonis, G. Ellinas, and M. A. Ali, “On multicast traffic grooming in WDM networks,” *Computers and Communications, 2004. Proceedings. ISCC 2004. Ninth International Symposium on*, vol. 1. pp. 282–287 Vol.1, 2004.
- [5] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, “Loss-tolerant quantum cryptography with imperfect sources,” *Phys. Rev. A*, vol. 90, no. 5, p. 52314, Nov. 2014.
- [6] M. A. Nielsen and I. L. Chuang, “Quantum information and quantum communication,” *Cambridge, U.K Cambridge Univ. Press*, 2000.
- [7] Ø. Marøy, L. Lydersen, and J. Skaar, “Security of quantum key distribution with arbitrary individual imperfections,” *Phys. Rev. A - At. Mol. Opt. Phys.*, vol. 82, no. 3, pp. 1–7, 2010.
- [8] N. Gisin and R. Thew, “Quantum communication,” *Nat Phot.*, vol. 1, no. 3, pp. 165–171, Mar. 2007.
- [9] I. de Miguel, R. Vallejos, A. Beghelli, and R. J. Duran, “Genetic Algorithm for Joint Routing and Dimensioning of Dynamic WDM Networks,” *IEEE/OSA Journal of Optical Communications and Networking*, vol. 1, no. 7. pp. 608–621, 2009.
- [10] J. M. Arrazola and N. Lütkenhaus, “Quantum communication with coherent states and linear optics,” *Phys. Rev. A*, vol. 90, no. 4, p. 42335, Oct. 2014.
- [11] N. Gisin and R. Thew, “Quantum communication technology,” *Electron. Lett.*, vol. 46, no. 14, p. 961, 2010.
- [12] N. K. Singhal and B. Mukherjee, “Protecting multicast sessions in WDM optical mesh networks,” *Journal of Lightwave Technology*, vol. 21, no. 4. pp. 884–892, 2003.
- [13] K. Zhu, H. Zang, and B. Mukherjee, “A comprehensive study on next-generation optical grooming switches,” *IEEE Journal on Selected Areas in Communications*, vol. 21, no. 7. pp. 1173–1186, 2003.
- [14] A. Al Natsheh, S. A. Gbadegeshin, A. Rimpiläinen, I. Imamovic-Tokalic, and A. Zambrano, “Identifying the Challenges in Commercializing High Technology: A Case Study of Quantum Key Distribution Technology,” *Technol. Innov. Manag. Rev.*, vol. 5, no. 1, 2015.
- [15] S. Glisic and B. Vucetic, “Spread Spectrum CDMA Systems for Wireless Communications,” *Artech House*, p. 383, 1997.

- [16] P. Prucnal, M. Santoro, and T. Fan, "Spread spectrum fiber-optic local area network using optical processing," *Journal of Lightwave Technology*, vol. 4, no. 5. pp. 547–554, 1986.
- [17] S. V Maric, Z. I. Kostic, and E. L. Titlebaum, "A new family of optical code sequences for use in spread-spectrum fiber-optic local area networks," *IEEE Transactions on Communications*, vol. 41, no. 8. pp. 1217–1221, 1993.
- [18] M. S. Anuar, S. A. Aljunid, N. M. Saad, and S. M. Hamzah, "New design of spectral amplitude coding in OCDMA with zero cross-correlation," *Opt. Commun.*, vol. 282, no. 14, pp. 2659–2664, Jul. 2009.
- [19] Z. Wei, H. Ghafouri-Shiraz, and H. M. H. Shalaby, "New code families for fiber-Bragg-grating-based spectral-amplitude-coding optical CDMA systems," *IEEE Photonics Technology Letters*, vol. 13, no. 8. pp. 890–892, 2001.
- [20] C.-S. Weng and J. Wu, "Optical orthogonal codes with nonideal cross correlation," *Journal of Lightwave Technology*, vol. 19, no. 12. pp. 1856–1863, 2001.
- [21] M. S. Anuar, S. A. Aljunid, N. M. Saad, A. Mohammed, and E. I. Babekir, "Development of a Zero Cross-Correlation Code for Spectral-Amplitude Coding Optical Code Division Multiple Access (OCDMA)," *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 6, no. 12, pp. 180–184, 2006.
- [22] S. Anuar, M. A. Aljunid, S. R. Badlishah, M. Saad, N, and I. Andonovic, "Performance Analysis of Optical CDMA System Based on Zero Cross Correlation (ZCC) Code Using OFDM Modulation.pdf," *J. Appl. Sci.*, vol. 7, no. 23, pp. 3819–3822, 2007.
- [23] S. A. Aljunid, M. D. A. Samad, M. Othman, M. H. Hisham, A. H. Kasiman, and M. K. Abdullah, "Development of modified double-weight code and its implementation in multi-rate transmissions," *2005 13th IEEE International Conference on Networks Jointly held with the 2005 IEEE 7th Malaysia International Conf on Communic*, vol. 1. p. 5 pp., 2005.
- [24] F. Hilal, A. A. Aljunid, S, and B. Ahmad, R, "Design and Demonstration of a Novel Spectral Amplitude Coding OCDMA Code for Suppression Phase Intensity Induced Noise," *J. Commun.*, vol. 4, no. 1, 2009.
- [25] c. B. M. Rashidi, S. A. Aljunid, H. A. Fadhil, and M. S. Anuar, "Encoder-decoder design for SAC-OCDMA using Flexible Cross Correlation (FCC) code algorithms," *2013 IEEE 4th International Conference on Photonics (ICP)*. pp. 166–168, 2013.
- [26] M. Kavehrad and D. Zaccarin, "Optical code-division-multiplexed systems based on spectral encoding of noncoherent sources," *Journal of Lightwave Technology*, vol. 13, no. 3. pp. 534–545, 1995.
- [27] T. H. Abd, S. A. Aljunid, H. A. Fadhil, R. B. Ahmad, and M. A. Rashid, "New approach for evaluation of the performance of spectral amplitude coding-optical code division multiple access system on high-speed data rate," *IET Communications*, vol. 6, no. 12. pp. 1742–1749, 2012.

CONCLUSION

GENERALE

CONCLUSION GENERALE

L'objectif de cette thèse était de modéliser, de concevoir des nouveaux codes optiques en SAC-OCDMA et d'étudier la capacité des réseaux quantiques. Ce travail est constitué de deux axes ; des études analytiques, des analyses numériques et des simulations sur Matlab et Comsol pour la partie de quantique et Matlab et OptiSystem pour l'OCDMA. Dans un premier lieu, nous avons détaillé les notions propres aux communications quantiques.

Comme dans les télécommunications classiques, les photons sont bien adaptés pour transmettre l'information quantique, étant donné leur grande vitesse de propagation et leur faible décohérence. Néanmoins, leur avantage constitue également leur faiblesse : les photons ne peuvent être utilisés que d'une façon probabiliste pour le calcul quantique ou la transmission entre différents porteurs d'information est nécessaire.

Finalement, les photons sont difficiles à stocker. Par conséquent, beaucoup d'applications dans le domaine de la communication et du calcul quantique demandent le transfert réversible des états photoniques non-classiques sur des excitations électroniques d'atomes ou de solides. Une telle mémoire quantique permettrait par exemple la réalisation de sources de photons uniques. À la demande, basées sur des sources de photons uniques annoncées.

De plus, cette thèse servirait de tampon pour le codage temporel de l'information quantique et représenterait un élément clef pour le calcul quantique bas sur une méthode pour les systèmes à distribution de clé quantique.

Ensuite, Dans ce travail, le système SAC avec une phase de corrélation croisée est utilisé pour réaliser l'atténuation des interférences MAI. L'arrangement de plusieurs FBGs dans les résultats en cascade à faible insertion perdue comparé parallèle. Les FBGs en cascade introduisent le retard aller-retour en raison de la longueur d'onde ne sont arrivés à la photodiode synchroniquement.

CONCLUSION GENERALE

Les 1-D MFCC équilibre détecteurs avec une configuration en cascade ont été conçus avec succès pour supprimer PIIN et atténuer MAI dans le système MFCC OCDMA 1-D. La simulation montre la performance du code et la détection de la balance 1-D MFCC du système OCDMA peut être réalisé avec de bonnes performances. La bonne conception de la simulation en tenant compte de l'environnement optique réel peut être réalisée à l'avenir à distance.