

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A.MIRA-BEJAIA



Faculté de Technologie
Département de Génie Electrique
Filière : télécommunication

Projet fin d'études

Pour l'obtention du diplôme de master en réseaux et télécommunications

Le concept de la distribution quantique de clé dans une liaison WDM

Réalisé par :

Haddad Kahina
Bourkeb Massilva

Encadré par :

Mr Berrah
Mme Bouchoucha

Examineurs :

Mr Azni
Mme Benjelloul

Soutenu en Octobre 2020

Remerciement

Ce travail est l'aboutissement d'un dur labeur et de beaucoup de sacrifices. Nos remerciements vont d'abord au créateur de l'univers qui nous a doté d'intelligence, et nous a maintenu en santé pour mener à bien ce projet de fin d'étude. Nous tenons aussi à adresser nos remerciements à nos encadreurs Mr Berrah, et Mme Bouchoucha pour leur patience, leur disponibilité et surtout leurs judicieux conseils, qui ont contribué à alimenter notre réflexion. Nos vifs remerciements au membre de jury Mr Agni et Mme Benjelloul pour l'intérêt qu'ils ont porté en acceptant d'examiner notre travail et l'enrichir par leurs propositions.

Nous pourrions passer outre notre reconnaissance envers nos parents, nos sœurs et nos frères, leur présence, leur écoute, leur confiance en nous et leur soutien, grâce à eux nous avons pu surmonter et surpasser tous les obstacles.

Enfin, nous tenons également à remercier toutes les personnes qui ont participé de près ou de loin à la réalisation de ce travail.

Table de matière

Introduction générale	1
1 La convergence de la cryptographie classique vers la cryptographie quantique	2
1.1 Introduction	2
1.2 Généralités sur la cryptographie.....	2
1.2.1 Terminologie	2
1.2.2 Qu'est-ce que c'est la cryptographie	2
1.2.3 L'usage de la cryptographie	3
1.2.4 Mécanismes de la cryptographie	3
1.3 Principales techniques en cryptographie	4
1.3.1 Cryptographie classique	4
1.3.1.1 La cryptographie par substitution mono alphabétique	4
1.3.1.2 La cryptographie par substitution poly alphabétique	5
1.3.2 La cryptographie moderne	6
1.3.2.1 Le chiffrement symétrique.....	6
1.3.2.2 Le chiffrement asymétrique.....	7
1.3.3 L'apport de la cryptographie quantique	8
1.3.3.1 Cryptographie quantique	8
1.4 Conclusion.....	13
2 Les protocoles de distributions quantiques de clés et l'implémentation du protocole BB84	14
2.1 Introduction	14
2.2 Les sources de photons utilisées pour la distribution quantique de clé.....	14
2.2.1 Les sources à photon unique	14
2.2.1.1 Source d'impulsions cohérente atténuée	15
2.2.1.2 Sources à la demande (déclenchée).....	15
2.3 Principe générale de distribution quantique de clé.....	16
2.3.1 Théorème de non-clonage	16
2.3.2 Relation d'incertitude de Heisenberg	16
2.4 Les protocoles de distribution de clé quantique	17
2.4.1 Le protocole BB84	17
2.4.1.1 Déroulement du protocole	17
2.4.2 Le protocole B92	19
2.4.3 Le protocole a six états	20
2.5 Implémentation du protocole BB84 sur OPTYSYSTEM	21

2.5.1	Présentation du logiciel	21
2.5.2	Simulation	21
2.6	Conclusion.....	25
3	Les liaisons de transmission optique WDM et leurs applications dans la QKD	26
3.1	Introduction	26
3.2	Principe de base d'une transmission optique	26
3.3	Liaison de transmission optique WDM.....	27
3.3.1	Composants d'un système WDM.....	27
3.3.1.1	Emetteur optique.....	27
3.3.1.2	La fibre optique	30
3.3.1.3	Multiplexeur et démultiplexeur en longueur d'onde	33
3.3.1.4	Amplificateur optique.....	34
3.3.1.5	Récepteur optique	34
3.4	Simulation d'une liaison optique WDM sous l'OPTISYSTEM	34
3.4.1	Les critères de qualité d'une transmission optique	34
3.4.1.1	Diagramme de l'œil	34
3.4.1.2	Taux d'erreur binaire (BER).....	34
3.4.1.3	Facteur de qualité (Q)	35
3.4.2	Les Composants de la liaison optique	35
3.4.3	Simulation d'une chaîne de transmission optique de base.....	38
3.4.3.1	Chaîne de transmission sans filtre	38
3.4.3.2	Chaîne de transmission avec filtre.....	39
3.4.3.3	Chaîne de transmission avec modulation interne	40
3.4.3.4	Chaîne de transmission avec modulation externe.....	41
3.4.4	Chaîne de transmission optique WDM 6x8 Gbit/s.....	42
3.5	Application du WDM dans la distribution quantique de clés	45
3.5.1	Simulation d'un système WDM-QKD.....	47
3.6	Conclusion.....	52
	Conclusion générale	53
	Références bibliographiques	1
	Résumé	1

Listes des figures

Figure 1.1 Principe de la cryptographie.	3
Figure 1.2 Système de chiffrement.	4
Figure 1.3 Exemple de chiffrement de vegenére.....	6
Figure 1.4 Principe du chiffrement symétrique.....	7
Figure 2.1 Principe d'un laser atténué.	15
Figure 2.2 Principe d'une source de photon unique déclenchée.....	16
Figure 2.3 Principe du protocole BB84.....	18
Figure 2.4 Etats de polarisation du protocole B92.	19
Figure 2.5 Etats de polarisation du protocole SSP.	20
Figure 2.6 simulation de BB84 pour un seul canal.	22
Figure 2.7 Paramètres de Stocks obtenus.....	22
Figure 2.8 Paramètres de Stocks a) au niveau de l'émetteur. b) au niveau du récepteur.	23
Figure 2.9 Simulation du protocole BB84.	24
Figure 2.10 Paramètres de Stocks a) premier analyseur. b) deuxième analyseur.	24
Figure 3.1 Principe de base d'une transmission optique.....	26
Figure 3.2 Principe d'une liaison WDM.	27
Figure 3.3 Eléments d'un émetteur optique.....	27
Figure 3.4 Symbole de la LED.....	28
Figure 3.5 Schéma d'un modulateur interne.....	29
Figure 3.6 Schéma d'un modulateur externe.	30
Figure 3.7 Composant d'une fibre optique.	30
Figure 3.8 Fibre monomode.....	31
Figure 3.9 Fibre multimode.....	31
Figure 3.10 Phénomène d'atténuation dans une fibre optique.....	32
Figure 3.11 L'atténuation en fonction de la longueur d'onde.....	32
Figure 3.12 La dispersion chromatique.....	33
Figure 3.13 Le multiplexeur et démultiplexeur utilisé dans une liaison WDM.....	33
Figure 3.14 Modèle de simulation de la séquence binaire.....	35
Figure 3.15 Modèle de simulation du générateur NRZ.....	36
Figure 3.16 Modèle de simulation de la diode laser.	36
Figure 3.17 Modèle de simulation d'une fibre optique.....	36
Figure 3.18 Modèle de simulation d'un multiplexeur WDM.	37

Figure 3.19 Modèle de simulation d'un demultiplexeur WDM.	37
Figure 3.20 Modèle de simulation d'une photodiode PIN.....	37
Figure 3.21Modèle de simulation du diagramme de l'œil.....	38
Figure 3.22 Modèle de simulation filtre passe bas Bessel.	38
Figure 3.23 Chaîne de transmission de base.	38
Figure 3.24 Diagramme de l'œil d'une chaîne de transmission pour D=1Gbps.	39
Figure 3.25Chaîne de transmission avec filtre.	39
Figure 3.26 Diagramme de l'œil d'une chaîne avec filtre.....	40
Figure 3.27 Chaîne de transmission avec modulateur externe.....	41
Figure 3.28 Diagramme de l'œil : a) modulation directe b) modulation externe.	42
Figure 3.29 simulation d'une chaîne WDM 8 x 6Gbps.	43
Figure 3.30 Diagramme de l'œil pour une liaison WDM 8 x 6Gbps.	44
Figure 3.31 Fourniture des clés secrètes pour différents utilisateurs simultanément par un système QKD-WDM.....	46
Figure 3.32 Un système QKD intégré sur une liaison WDM utilisé entre deux utilisateurs. ..	46
Figure 3.33 Chaîne de transmission avec un atténuateur.	47
Figure 3.34 Diagramme de l'œil pour une chaîne avec un atténuateur.....	48
Figure 3.35 Intégration d'un system QKD dans une liaison WDM 2*1 Gbps.	48
Figure 3.36 le diagramme de l'œil pour un system QKD intégré sur une liaison WDM 2*1 Gbps.	49
Figure 3.37 Intégration d'un system QKD dans une liaison WDM 4*1 Gbps.	50
Figure 3.38 diagramme de l'œil pour un system QKD intégré sur une liaison WDM 4*1 Gbps.	51

Liste des tableaux

Tableau 1.1 Permutation aléatoire pour le chiffrement.....	5
Tableau 1.2 Comparaison entre le chiffrement symétrique et le chiffrement asymétrique.	8
Tableau 1.3 Les probabilités qu'un photon passe au travers d'un filtre polarisant suivant	10
Tableau 1.4 Les modes de polarisation.	10
Tableau 1.5 Exemple de partage d'une clé secrète.	12
Tableau 2.1 Types de polarisations et technique d'encodage	17
Tableau 2.2 Première étape du protocole BB84.....	18
Tableau 2.3 deuxième étape du protocole BB84.....	18
Tableau 2.4 Troisième étape du protocole BB84.....	19
Tableau 3.1 Les trois grandes fenêtres d'atténuation.....	32
Tableau 3.2 Paramètres caractéristiques de la diode laser.	36
Tableau 3.3 La variation du facteur de qualité et le taux d'erreur binaire en fonction du débit.	40
Tableau 3.4 le facteur de qualité et Taux d'erreur pour une liaison WDM a 8 canaux.....	45
Tableau 3.5 Le facteur de qualité et le taux d'erreur pour un system QKD intégré sur une liaison WDM 2*1 Gbps.....	49
Tableau 3.6 Le facteur de qualité et le taux d'erreur pour un system QKD intégré sur une liaison WDM 4*1 Gbps.....	51

Introduction générale

Ce mémoire porte principalement sur l'étude de la distribution quantique de clé dans les liaisons WDM. La problématique générale se résume comme suit : il s'agit de pouvoir distribuer des clés secrètes à plusieurs utilisateurs sur une liaison WDM. L'objectif principale de ce travail est d'intégrer le système QKD dans l'infrastructure du réseau WDM dans le but de pouvoir communiquer des clés secrètes entre plusieurs utilisateurs.

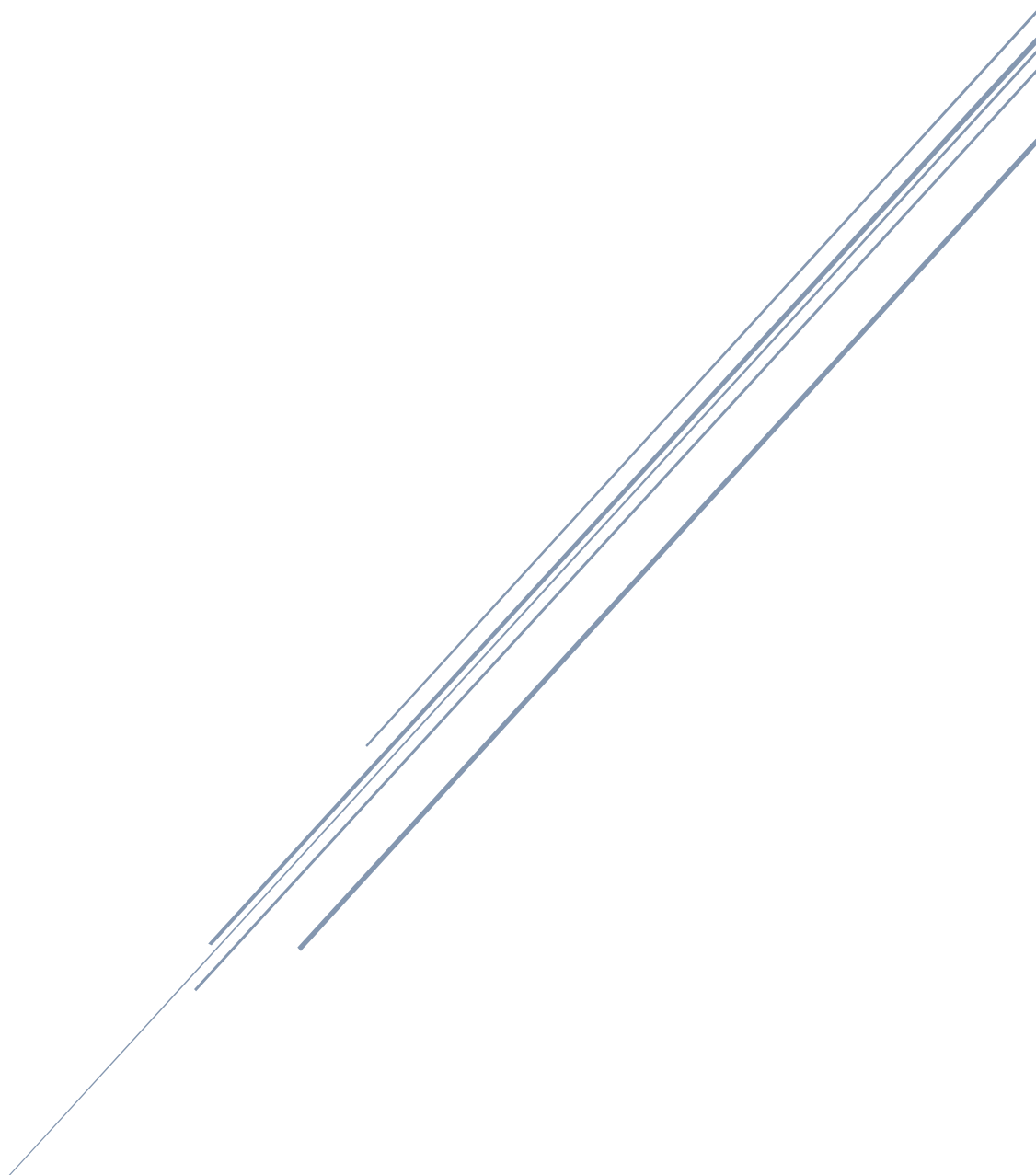
Ce travail est organisé en trois chapitre ; le premier chapitre sera consacré pour la présentation des principes de la cryptographie et les techniques utilisées pour assurer la sécurité ; d'une part la cryptographie classique, d'autre part la cryptographie moderne qui se partage en deux types : le chiffrement symétrique et le chiffrement asymétrique. Dans la dernière partie de ce chapitre nous allons nous intéresser à une nouvelle classe de cryptographie qui est la cryptographie quantique basée sur les principes physiques de la mécanique quantique utilisant le photon comme porteur d'information.

Dans le deuxième chapitre, nous détaillerons une nouvelle approche qui est la distribution quantique de clé qui résout l'un des problèmes dans les communications sécurisées en exploitant les lois de la mécanique quantique afin de parvenir à une distribution de clés certifiée sécurisée entre deux participants, Mais en premier lieu, nous nous intéresserons aux sources de générations de photon unique, qui est le premier obstacle des protocoles à photons uniques. Dans la deuxième partie de ce chapitre, nous expliquerons les différents protocoles de distribution quantique de clé qui se basent généralement sur des sources à photon unique et nous détaillerons ainsi leurs fonctionnalités. Dans la dernière partie nous simulerons le protocole BB84 en utilisant une source fortement atténué à l'aide du logiciel OPTYSYSTEM.

Dans le troisième chapitre, nous démontrons une approche généralement applicable afin d'augmenter le débit de transmission qui est les liaisons de transmission optique WDM. Dans la première partie de ce chapitre, nous expliquerons en détails ces liaisons de transmission, ensuite nous simulerons une liaison optique WDM 46Gbps en utilisant OPTISYSTEM qui permet de visualiser le signal reçu et d'évaluer la qualité de transmission grâce au diagramme de l'œil, le facteur de qualité ainsi que le taux d'erreur en tenant compte du bruit. Enfin nous évoquerons les applications des liaisons de transmission WDM dans la distribution quantique de clé ensuite nous simulerons un système WDM-QKD 4*1Gbps.

CHAPITRE N°01 :

La convergence de la cryptographie classique vers la cryptographie quantique



1 La convergence de la cryptographie classique vers la cryptographie quantique

1.1 Introduction

La cryptographie est utilisée pour protéger les messages. Au fil du temps, les techniques de cryptage se sont complexifiées. Dans ce chapitre nous allons présenter les principes de base et les généralités sur la cryptographie ainsi que les mécanismes cryptographiques. Nous verrons par la suite les principales techniques utilisées pour assurer la sécurité et la confidentialité du partage des données, à savoir la cryptographie classique et la cryptographie moderne. De ce fait, on s'intéressera à la cryptographie quantique et plus particulièrement à l'apport du photon dans ce type de cryptage.

1.2 Généralités sur la cryptographie

1.2.1 Terminologie

- ✓ **Texte en clair** : c'est le message à protéger.
- ✓ **Texte chiffré** : c'est le résultat du chiffrement du texte en clair.
- ✓ **Chiffrement** : c'est la méthode ou l'algorithme utilisé pour transformer un texte clair en texte chiffré.
- ✓ **Déchiffrement** : c'est la méthode ou l'algorithme utilisé pour transformer un texte chiffré en texte clair.
- ✓ **Clé** : représente une valeur utilisée dans un algorithme cryptographique, dans le but de chiffrer une donnée. Cette valeur s'agit d'un nombre complexe dont la taille se mesure en bits.
- ✓ **Cryptanalyse** : est la technique qui consiste à déduire un texte clair d'un texte chiffré sans posséder la clé de chiffrement [1].

1.2.2 Qu'est-ce que c'est la cryptographie

La cryptographie est une science qui permet de convertir des informations "dites messages clair" en informations codées, c'est à dire rendre le message non compréhensibles ou inintelligibles, puis restituer les informations originales à partir de ces informations codées. La méthode inverse appelée le déchiffrement, consistant à retrouver le message original à partir d'un message chiffré, comme c'est montré dans la figure 1.1.

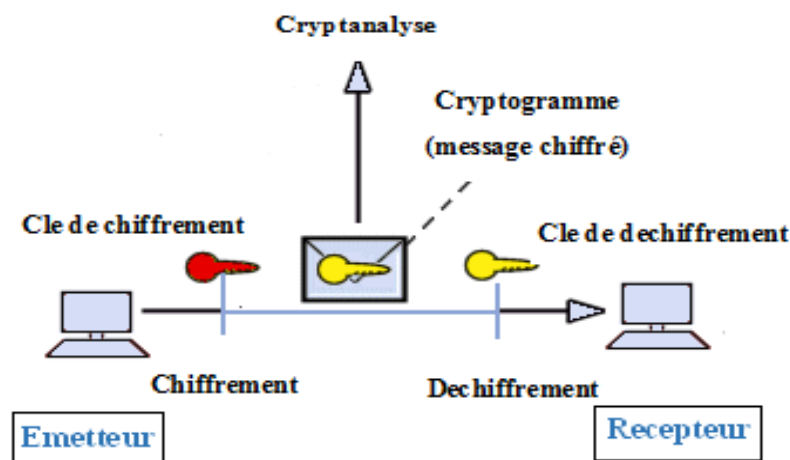


Figure 1.1 Principe de la cryptographie.

1.2.3 L'usage de la cryptographie

La cryptographie permet de résoudre les problèmes suivants :

A. La confidentialité :

Le texte chiffré ne doit être lisible que par les destinataires légitimes, c'est à dire qu'un intrus ne pourra pas le lire.

B. L'authentification :

Le destinataire du message doit pouvoir s'assurer de son origine. Un intrus ne doit pas être capable de se faire passer pour quelqu'un d'autre.

C. L'intégrité :

Le destinataire d'un message doit pouvoir vérifier que celui-ci n'a pas été modifié en chemin. Autrement dit elle consiste à vérifier que les données n'ont pas été altérées au cours de leur transmission ou de leur stockage.

1.2.4 Mécanismes de la cryptographie

Un algorithme de cryptographie est une fonction mathématique utilisée lors du processus de cryptage et de décryptage. Cet algorithme est associé à une clé. La sécurité des données chiffrées repose entièrement sur deux éléments essentiels : l'invulnérabilité de l'algorithme de cryptographie et la confidentialité de la clé. Un système cryptographique est constitué d'un algorithme de cryptographie, ainsi que de toutes les clés et tous les protocoles nécessaires à son fonctionnement.

1.3 Principales techniques en cryptographie

De nombreuses méthodes de chiffrement ont été imaginées pour se protéger de la curiosité et de la malveillance de ses ennemis depuis de nombreux siècles. On peut classer ces méthodes en trois grandes classes, comme nous le montre la figure 1.2 :

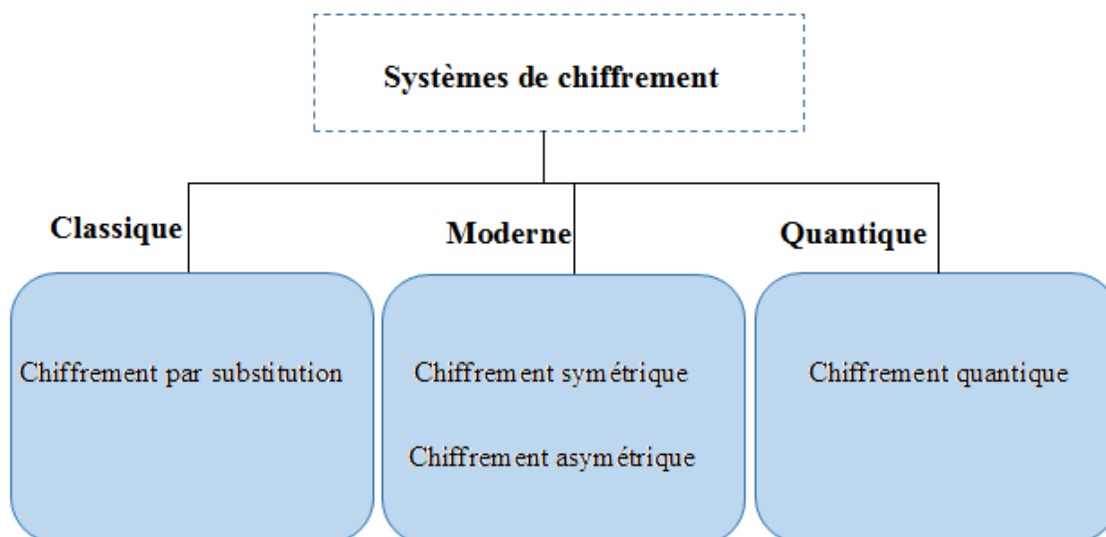


Figure 1.2 Système de chiffrement.

1.3.1 Cryptographie classique

La cryptographie classique décrit la période avant les ordinateurs. Elle traite des systèmes reposant sur des lettres et des caractères d'une langue [2]. Des techniques de cryptage utilisés remplacent les caractères par d'autres caractères et les transposent dans un ordre différent.

1.3.1.1 La cryptographie par substitution mono alphabétique

Le codage par substitution mono-alphabétique est très simple. Dans le message clair, on remplace chaque lettre par une lettre différente. Tel qu'il est illustré dans la tableau 1.1.

➤ **Application :**

Texte clair	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Texte chiffré	W	X	E	H	Y	Z	T	K	C	P	J	I	U	A	D	G	L	Q	M	N	R	S	F	V	B	O

Tableau 1.1 Permutation aléatoire pour le chiffrement.

Le texte clair : Cryptographie

Le texte chiffré : EQBGNDTQWGKCY

Un des problèmes avec le remplacement des codes est de se souvenir de la clé (permutations). Ce n'est pas facile de se souvenir de 26 lettres, c'est pourquoi on a recouru à d'autres variantes comme le code de César.

➤ **Le code de César :**

Le code de César est la méthode de cryptage la plus ancienne. Il consiste en une substitution mono-alphabétique, où la substitution est définie comme un décalage de la lettre. Par exemple, si nous remplaçons D par A, puis remplaçons B par E, et remplaçons C par F, D par G etc... Il n'y a que 26 façons de crypter les messages en utilisant le code de César. Par conséquent, il s'agit d'un code peu sûr, car il est facile de tester toutes les possibilités.

1.3.1.2 La cryptographie par substitution poly alphabétique

a. Le chiffrement de Vigenère :

Le chiffrement de Vigenère est un système de chiffrement par substitution poly alphabétique, cela signifie qu'une même lettre du message clair peut être remplacée par des lettres différentes, contrairement à un système de chiffrement mono alphabétique qui se contente d'utiliser la même lettre de substitution.

Un exemple de chiffrement de Vigenère est donné dans la figure 1.3 :

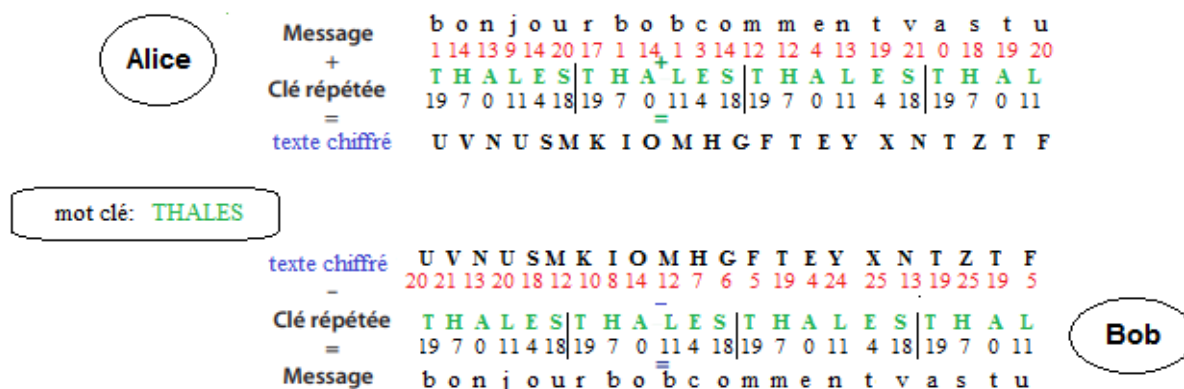


Figure 1.3 Exemple de chiffrement de vegenère.

1.3.2 La cryptographie moderne

L'arrivé de la cryptographie moderne rend la technologie de cryptage actuelle plus sécurisée. Elle utilise des méthodes modernes, à savoir des ordinateurs et manipule des bits, contrairement aux anciennes méthodes qui opéraient sur des caractères alphabétiques, il ne s'agit donc que d'un changement de taille car nous n'utilisons que deux éléments au lieu des 26 lettres de l'alphabet. La sécurité de ces méthodes modernes est désormais basé sur la clé de chiffrement, cette méthode contient deux principaux types d'algorithmes de chiffrement. Chiffrement à clé publique et chiffrement à clé privée :

1.3.2.1 Le chiffrement symétrique

Le chiffrement symétrique ou chiffrement à clé privée consiste à utiliser la même clé pour le chiffrement et le déchiffrement, comme il est illustré sur la figure 1.4. Le chiffrement symétrique consiste à appliquer une opération (algorithme) sur les données à chiffrer à l'aide de la clé privée, afin de les rendre inintelligibles.



Figure 1.4 Principe du chiffrement symétrique.

1.3.2.2 Le chiffrement asymétrique

Le chiffrement asymétrique (ou chiffrement à clés publiques) consiste à utiliser une clé publique pour le chiffrement et une clé privée pour le déchiffrement.

La cryptographie asymétrique ou chiffrement à clé publique est souvent utilisée pour désigner une méthode de chiffrement d'un message en utilisant une clé publique pour obtenir un message chiffré qui sera transféré via un canal. A la réception, ce message chiffré sera déchiffré en utilisant une clé privée (ou secrète) pour retrouver le message d'origine (message clair) comme le montre la figure 1.5. Dans ce type de cryptographie, le problème du transfert de la clé secrète posé par la cryptographie à clé secrète est réglé.

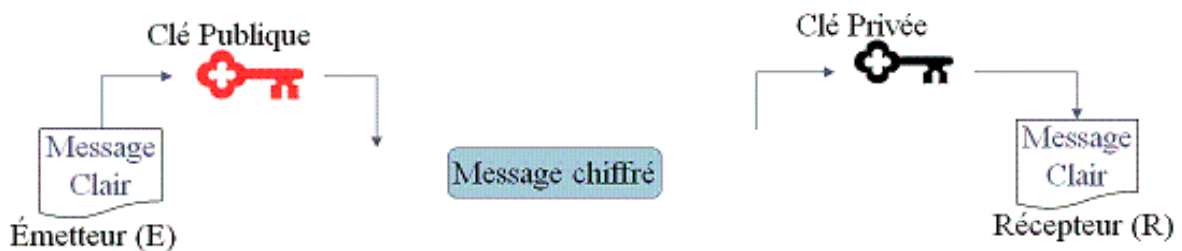


Figure 1.5 Principe du chiffrement asymétrique.

- **Table de comparaison :**

	Cryptage Symétrique	Cryptage Asymétrique
Définition	Le cryptage symétrique utilise une seule clé pour le cryptage et le décryptage.	Le cryptage asymétrique utilise une clé différente pour le cryptage et le décryptage.
Performance	Le cryptage symétrique est rapide en exécution.	Le cryptage asymétrique est lent à l'exécution en raison de la charge de calcul élevée.
Objectif	Le cryptage symétrique est utilisé pour la transmission de données en masse.	Le cryptage asymétrique est souvent utilisé pour l'échange de clés secrètes.

Tableau 1.2 Comparaison entre le chiffrement symétrique et le chiffrement asymétrique.

1.3.3 L'apport de la cryptographie quantique

Jusqu'à présent, les différents algorithmes présentés reposent principalement sur les mathématiques. Le majeur inconvénient de ces algorithmes c'est qu'une découverte mathématique permettant d'accélérer le calcul d'une opération particulière peut détruire le processus de cryptage.

Une nouvelle classe d'algorithmes est en train d'émerger, elle s'agit de la cryptographie quantique qui se base sur les principes physiques de la mécanique quantique. De ce fait aucune découverte technologique ne peut contredire les principes du physique quantique.

1.3.3.1 Cryptographie quantique

La différence entre la cryptographie quantique et le chiffrement standard réside dans le fait que la clé est transmise sous forme de photons (particules de la lumière).

➤ Le bit quantique

En informatique classique, le message est codé grâce à des bits (1 ou 0). En informatique quantique, on utilisera le bit quantique appelé également le qubit qui représente la plus petite unité de stockage d'information quantique.

➤ **Superposition d'état**

Le qubit peut se trouver dans l'un des deux états de base $|0\rangle$ ou $|1\rangle$. Cette notation est appelée « notation de Dirac ». Dans la base rectiligne l'état $|0\rangle$ sera associé à l'état de polarisation horizontal et l'état $|1\rangle$ à l'état de polarisation vertical.

La différence particulière avec les bits classiques (0 ou 1) c'est que le bit quantique peut se trouver dans n'importe quel état intermédiaire, qui est exprimé par une superposition de ces deux états.

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \quad (1.1)$$

tel que $|\alpha|^2 + |\beta|^2 = 1$.

➤ **Les propriétés quantique d'un photon**

Les protocoles d'échanges de clés utilisent souvent un codage d'information quantique basé sur les propriétés quantiques du photon polarisé. La compréhension de ces propriétés est indispensable pour comprendre la cryptographie quantique.

Afin de détecter la polarisation des photons, un filtre polarisant devra être utilisé, et les résultats seront interprétés de la manière suivante :

- Si le filtre est orienté précisément dans l'axe de polarisation du photon, la probabilité que le photon traverse le filtre est égale à 1, c'est-à-dire qu'il traverse le filtre.
- Si le filtre est orienté à 90° de l'axe de polarisation du photon, la probabilité que le photon traverse le filtre est égale à 0, c'est-à-dire qu'il est absorbé.
- Si le filtre est orienté à 45° de l'axe de polarisation du photon, la probabilité que le photon traverse le filtre est égale à $1/2$, c'est-à-dire que le photon a une chance sur deux de passer le filtre. Le tableau 1.3 représente les probabilités qu'un photon passe à travers un filtre polarisant suivant les différents angles de polarisation.





	Filtre polarisé à 0°	Filtre polarisé à 45°	Filtre polarisé à 90°	Filtre polarisé à 135°
Photon polarisé à 0° 	1	$\frac{1}{2}$	0	$\frac{1}{2}$
Photon polarisé à 45° 	$\frac{1}{2}$	1	1/2	0
Photon polarisé à 90° 	0	$\frac{1}{2}$	1	$\frac{1}{2}$
Photon polarisé à 135° 	$\frac{1}{2}$	0	1/2	1

Tableau 1.3 Les probabilités qu'un photon passe au travers d'un filtre polarisant suivant les différents angles de polarisation

➤ **Transmission de la clé**

La transmission ou le partage de la clé consiste à transmettre une série de bits aléatoires (0 ou 1). Alice transmet à Bob chaque bit en choisissant aléatoirement un des deux modes de polarisation possibles comme c'est montré dans le tableau 1.4:



Mode de polarisation	symbole
Base rectiligne	
Base diagonale	

Tableau 1.4 Les modes de polarisation.

Chapitre 1 : La convergence de la cryptographie classique vers la cryptographie quantique

- **Base rectiligne** : consiste à envoyer un photon polarisé à 0° pour un qubit 0 et à 90° pour le qubit 1.
- **Base diagonale** : consiste à envoyer un photon polarisé à 45° pour un qubit 0 et à 135° pour un qubit 1.

Alice et Bob doivent disposer de deux canaux d'échanges pour qu'ils puissent échanger la clé secrète constitué de 0 et 1 :

- **Un canal quantique** : où ils peuvent s'échanger des photons polarisés.
- **Un canal classique** : non protégé, où ils peuvent discuter.

Le partage de clé se fait de la manière suivante :

- Alice émet une séquence binaire aléatoire à l'aide d'une source de lumière, ou chaque bit est codé sur un état de polarisation suivant deux bases différentes (rectiligne et diagonale)
- A la réception Bob dispose d'un analyseur qui mesure l'état de polarisation de chaque photon reçu dans une base sélectionnée au hasard (rectiligne ou diagonale) avec une probabilité de $\frac{1}{2}$ de choisir la bonne base qu'Alice.

Pour chacun des photons reçus, il y a deux possibilités :

- 1- Alice et Bob ont par hasard choisi la même base de polarisation. Dans ce cas, le photon reçu correspond au bit émis.
- 2- Alice et Bob ont choisi une base de polarisation différent et dans ce cas le photon reçu est interprété de mauvaise manière.

➤ Une fois que tous les bits sont transmis, Alice communique à Bob, les base de polarisation employé pour chacun des bits, Bob peut donc alors connaître les Qbits pour lesquels les bases de polarisation ont été les mêmes

➤ Enfin Alice et Bob auront une chaine de qubits identiques formant une clé secrète. Un exemple est illustré dans le tableau 1.5.

Exemple :

Bits envoyés par Alice	1 1 0 0 1 0 1 0 1 1 1 1 1 1 1 0 1 1 0 1 1 1 1 0 1 0 1
Polarisation choisie par Alice	+ x + x + x + + + + x x x + x x x + x + x + + x + x x
Polarisation choisie par Bob	+ x x x + x + x + + x x + + + + x x x + x x + x x + x
Valeurs lu par Bob	1 1 0 0 1 0 1 0 1 1 1 1 0 1 0 0 1 0 0 1 1 0 1 0 0 0 1
Bits retenus	1 1 - 0 1 0 1 - 1 1 1 1 - 1 - - 1 - 0 1 1 - 1 0 - - 1

Tableau 1.5 Exemple de partage d'une clé secrète.

De cette manière, il est possible de partager théoriquement, des clés secrètes avec une parfaite sécurité, pour crypter/décrypter des messages. Cette méthode est connue sous le nom : Distribution quantique de clé (QKD : Quantum Key Distribution)

➤ **But de la cryptographie quantique**

Le système de cryptographie quantique est utilisé pour la transmission de la clé, et non le message en lui-même, pour deux raisons essentielles :

✓ Les bits d'informations communiqués par les mécanismes de la cryptographie quantique ne peuvent être qu'aléatoires. Ceci ne convient pas pour un message, mais à une clé secrète, qui doit être aléatoire [3].

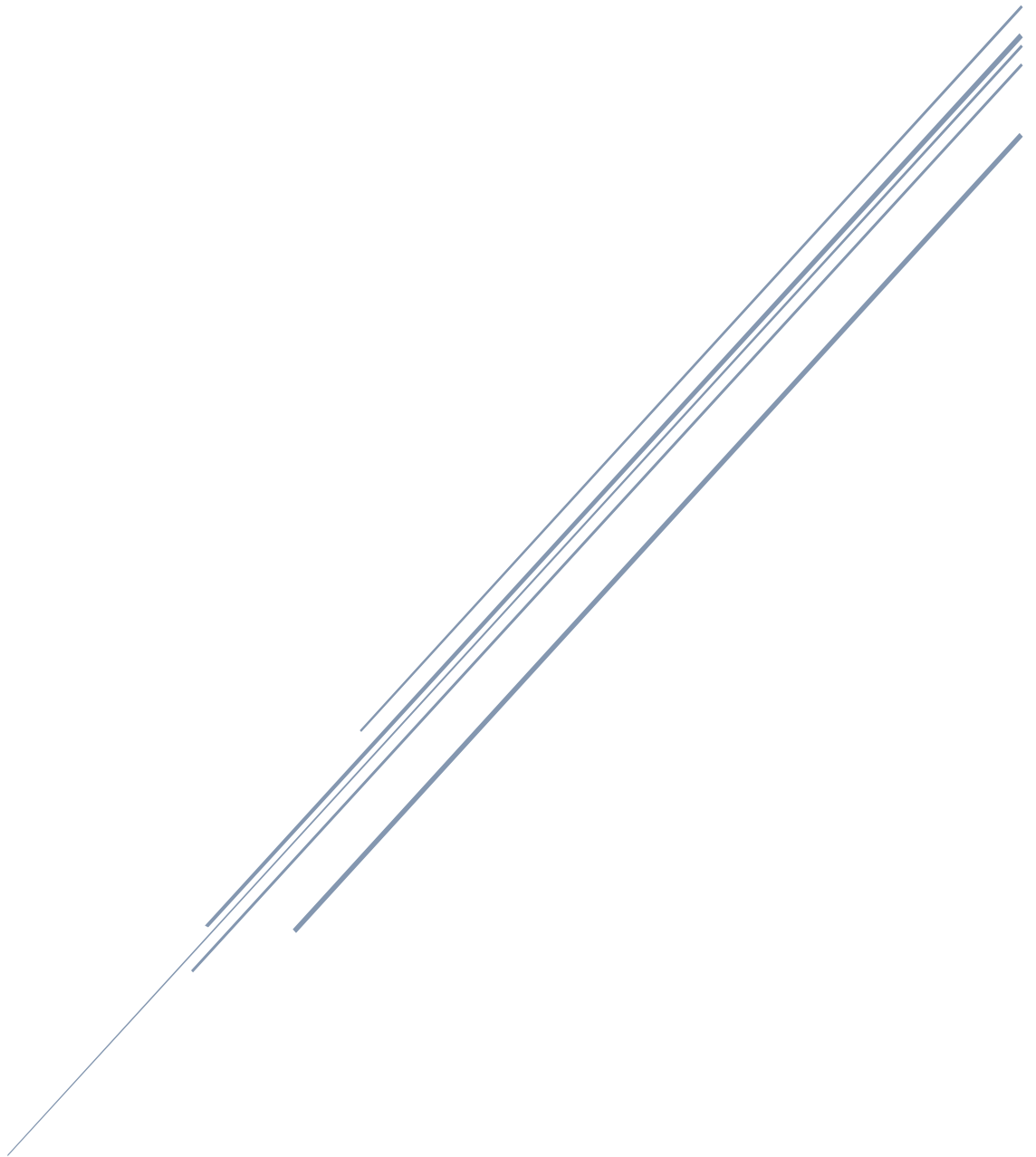
✓ Même si le mécanisme de la cryptographie quantique garantit que l'espionnage de la communication sera toujours détecté, il est possible que des bits d'informations soient interceptés par l'espion avant que celui-ci ne soit détecté. Ceci est inacceptable pour un message, mais sans importance pour une clé aléatoire qui peut être simplement jetée en cas d'interception.

1.4 Conclusion

A partir de ce chapitre, nous avons montré que le premier objectif de la cryptographie est la protection de l'information. En mettant le point sur quelques généralités de la cryptographie et ces principales techniques à savoir la cryptographie classique qui décrit la période avant les ordinateurs, la cryptographie moderne qui utilise la puissance des ordinateurs et qui présente deux classe importante des méthodes de chiffrement, d'une part les cryptage symétrique, d'autre part le cryptage asymétrique. La dernière section de ce chapitre décrit la cryptographie quantique qui est basé sur les propriétés quantique du photon polarisé pour le partage d'une clé secrète avec une parfaite sécurité.

CHAPITRE N°02 :

Les protocoles de distribution quantique de clé et
l'implémentation de protocole BB84.



2 Les protocoles de distributions quantiques de clés et l'implémentation du protocole BB84.

2.1 Introduction

La cryptographie quantique ou la distribution quantique de clés permet la génération d'une clé secrète, en codant les informations qui la constituent sur les états quantiques de la lumière (quanta), cette clé sera partagée entre deux participants appelés Alice et Bob.

Dans ce chapitre nous allons voir en premier lieu les sources de lumière (photon) utilisées dans la distribution quantique de clé, et plus particulièrement les sources à photons uniques. Nous nous intéresserons ensuite aux principes de la mécanique quantique sur lesquelles les protocoles de distributions sont fondus. Nous allons voir ainsi les protocoles de distribution de clé quantique les plus fonctionnels dans le domaine de la cryptographie et expliquer chaque protocole ainsi que les fonctionnalités qui ont été utilisées dans chaque d'eux. Dans la dernière partie nous allons simuler le protocole BB84 en utilisant une source laser à l'aide du logiciel OPTYSYSTEM.

2.2 Les sources de photons utilisées pour la distribution quantique de clé

L'idée fondamentale sur laquelle repose la distribution de clé quantique (Quantum Key Distribution) est d'utiliser des sources qui émettent des photons uniques au lieu de paquets de photons. de cette façon une tierce personne ne peut pas simplement détourner les photons qui sont envoyés d'une personne à une autre.

2.2.1 Les sources à photon unique

Les sources à photons uniques s'agissent des sources de lumière ou dispositifs qui émettent des impulsions contenant un et un seul photon.

On distingue plusieurs types de sources à photons uniques qui sont les sources d'impulsions cohérentes atténuées et les sources déclenchées.

2.2.1.1 Source d'impulsions cohérente atténuée

En plaçant sur le chemin d'un laser impulsif un atténuateur ; tel que dans chaque pulse laser, il y a un certain nombre de photons. En supprimant une grande partie de ces photons on aurait alors une source qui émet des impulsions fortement atténuées contenant en moyenne un photon par impulsion, on obtient alors une source cohérente atténuée ou chaque impulsion $\mu \leq 1$, tel qu'il est représenté sur la figure 2.1.

On rappelle la distribution des photons dans chaque impulsion suit une loi de Poisson :

$$P(n, \mu) = \frac{\mu^n}{n!} e^{-\mu} \quad (2.1)$$

Avec :

n : le nombre de photon.

μ : le nombre moyen de photons par impulsion.

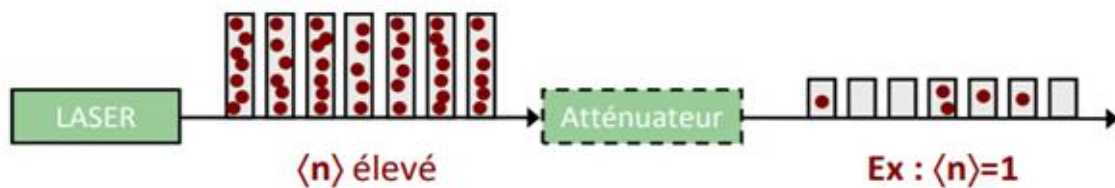


Figure 2.1 Principe d'un laser atténué.

2.2.1.2 Sources à la demande (déclenchée)

La façon la plus simple pour créer une source lumineuse pouvant émettre des photons uniques à la demande est de cibler un seul centre d'émission et de lui appliquer une excitation d'impulsion appropriée. Pour chaque impulsion d'excitation, un tel système entre dans son état d'excitation, provoque l'émission d'un photon et d'un seul de manière synchrone des tops d'horloge correspondants aux excitations impulsives [4].

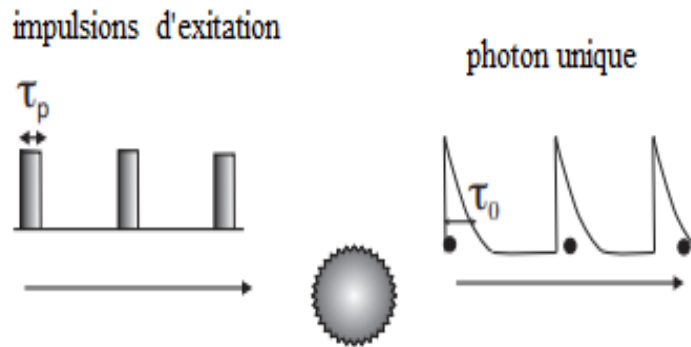


Figure 2.2 Principe d'une source de photon unique déclenchée.

Lorsqu'un émetteur entre dans son état excité, il va générer un seul photon dans une durée typique de l'ordre de τ_0 , dont l'émission a été déclenchée par l'impulsion d'excitation. Comme le montre la figure 2.2.

2.3 Principe générale de distribution quantique de clé

L'idée d'utiliser les photons dans la distribution quantique de clé est venu du fait que le photon est soumis à deux lois importantes posées par la mécanique quantique : le théorème de non clonage et la relation d'incertitude de Heisenberg.

2.3.1 Théorème de non-clonage

Le théorème d'impossibilité du clonage quantique explique l'impossibilité de dupliquer parfaitement une fonction d'onde.

Dans le cas d'un photon, il est impossible de le copier ou de réaliser des copies parfaites (des clones) de ce photon lorsqu'il se trouve dans un état superposé. L'avantage de ce théorème c'est qu'on oblige l'espion d'effectuer ses mesures sur le qubit échangé entre Alice et Bob et il peut se faire détecter facilement c'est-à-dire qu'on ne peut pas mesurer les états quantiques sans les perturber fondamentalement.

2.3.2 Relation d'incertitude de Heisenberg

En mécanique quantique, il est impossible de tout savoir sur les propriétés physiques d'un objet microscopique tel qu'un photon, d'où sa position est reliée intrinsèquement à sa vitesse. De sorte qu'on ne puisse jamais mesurer simultanément deux observables complémentaires avec précision. Ce principe montre que si on mesure très précisément une

Chapitre 2 : Les protocoles de distributions quantiques de clés et l'implémentation du protocole BB84

observable, on détruira complètement l'information sur l'autre, autrement dit si on connaît très précisément où se trouve le photon à un instant donné, on ne peut pas connaître précisément sa vitesse et vice versa. De cette façon on peut interdire à un espion d'apprendre quoi que ce soit d'utile sur une transmission d'information et ceci n'est pas dû à la limitation de notre technologie mais c'est une loi de la physique.

2.4 Les protocoles de distribution de clé quantique

Depuis 1984, plusieurs tentatives expérimentales de conception de protocoles d'échanges ont été développées sur la base de la règle de la mécanique quantique. Il existe plusieurs protocoles de distribution fonctionnels dans le domaine de la cryptographie.

2.4.1 Le protocole BB84

Le protocole BB84 est le premier protocole de distribution quantique de clés [3]. Il a été proposé en 1984 par Charles Bennett et Gilles Brassard. Il permet à deux utilisateurs distants appelés Alice et Bob de générer une clé secrète en codant les informations qui la constituent sur les quantas de la lumière émise par une source de photon unique.

Le codage est effectué sur quatre états correspondant aux axes de deux bases perpendiculaires appelées base rectiligne et base diagonale, tel qu'il est illustré sur le tableau 2.1.

Mode de polarisation	symbole	Etat de polarisation	Qubit
Base rectiligne	+	horizontale 0°	Qubit 0
		verticale 90°	Qubit 1
Base diagonale	X	Diagonale 45°	Qubit 0
		Anti diagonale -45°	Qubit 1

Tableau 2.1 Types de polarisations et technique d'encodage .

2.4.1.1 Déroulement du protocole

Le protocole BB84 se déroule en plusieurs étapes, et permet à deux participants d'établir une clé secrète, comme c'est illustré dans la figure 2.3.

Chapitre 2 : Les protocoles de distributions quantiques de clés et l'implémentation du protocole BB84

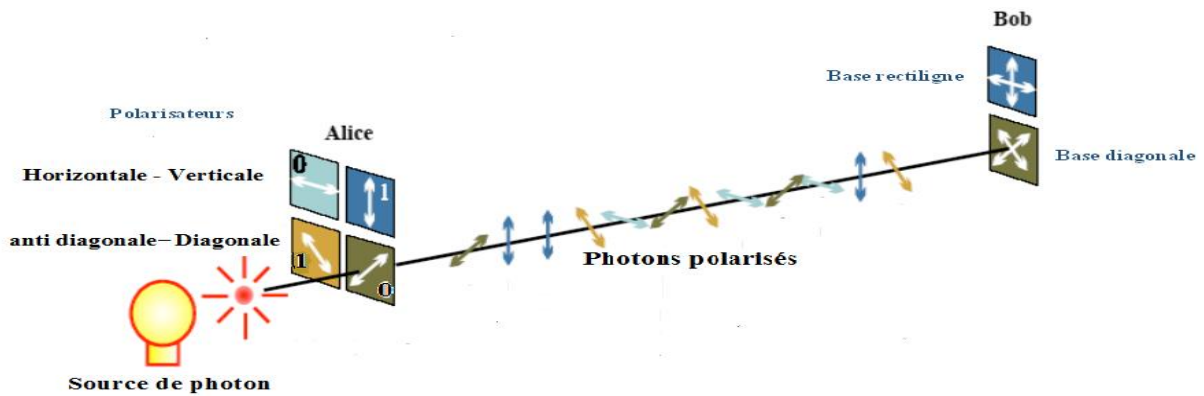


Figure 2.3 Principe du protocole BB84.

➤ **Première étape :**

Alice émet une séquence de bits aléatoire à l'aide d'une source à photon unique, où chaque bit $\in \{0,1\}$ est codé sur un état de polarisation d'un photon, en utilisant deux polarisateurs optiques de base différentes (B_+ ou B_x) choisie au hasard. Bob de son côté, choisit une base de réception aléatoire pour chaque photon, avec une probabilité de $\frac{1}{2}$ de choisir la bonne base qu'Alice. Cette première étape est représentée dans le tableau 2.2.

Bits d'Alice (b)	0	1	1	0	1	0	0	1
Base d'Alice (B)	+	+	X	+	X	X	X	+
Polarisation du photon	→	↑	↖	→	↖	↗	↗	↑

Tableau 2.2 Première étape du protocole BB84.

➤ **Deuxième étape :**

Bob reçoit et mesure l'état de polarisation de chaque photon reçu à l'aide de deux analyseurs, en sélectionnant au hasard la base de mesure, avec une probabilité de $\frac{1}{2}$ de choisir la bonne base qu'Alice. Ce processus est illustré dans le tableau 2.3.

Bits d'Alice (b)	0	1	1	0	1	0	0	1
Base d'Alice (B)	+	+	X	+	X	x	X	+
Polarisation du photon	→	↑	↖	→	↖	↗	↗	↑
Base de Bob	+	X	X	X	+	x	+	+
Photon reçu par Bob	→	↖ Ou ↗	↖	↖ Ou ↗	↑ ou →	↗	↑ Ou →	↑

Tableau 2.3 deuxième étape du protocole BB84.

➤ **Troisième étape :**

Bob annonce à Alice la base de mesure choisie en utilisant le canal classique, puis ils comparent leurs résultats en sauvegardant les bases identiques et rejetant celle qui se diffèrent. Enfin Alice et Bob auront une chaîne de qubit identiques formant une clé secrète. Dans cet exemple la clé $C= 0101$, comme c'est montré dans le tableau 2.4.

Bits d'Alice (b)	0	Jeté	1	Jeté	Jeté	0	Jeté	1
Base d'Alice (B)	+		X			x		+
Polarisation du photon e_b^B	→		↖			↗		↑
Base de Bob (r)	+		X			x		+
Photon reçu par Bob	→	Jeté	↖	Jeté	Jeté	↗	Jeté	↑

Tableau 2.4 Troisième étape du protocole BB84.

2.4.2 Le protocole B92

Le protocole B92 a été proposé en 1992, par Charles Bennett. Ce protocole est une version modifiée du protocole BB84, la principale différence c'est qu'il utilise la phase des photons pour coder les bits 0 et 1 sur deux états non orthogonaux de deux bases (un de la base rectiligne et un de la base diagonale), comme c'est montré dans la figure 2.4.

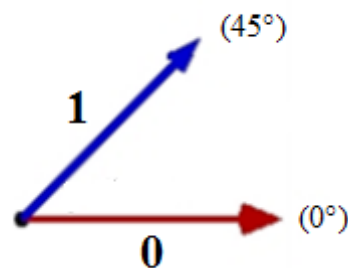


Figure 2.4 Etats de polarisation du protocole B92.

Le principe du protocole B92 est identique à celui du protocole BB84. A l'émission, Alice choisit une séquence binaire aléatoire qu'elle code sur la phase du photon. A la réception, Bob mesure les qubits dans des bases choisit au hasard et il aura deux possibilités :

- Si le choix de base est différent de celui d'Alice, aucune mesure ne sera effectuée et le qubit sera ignoré.
- Mais si le choix de base coïncide avec celui d'Alice et leur donnée sont corrélées, alors le qubit sera conservé et contribuera à construction de la clé secrète.

2.4.3 Le protocole a six états

Le protocole a six états (SSP) est une amélioration du protocole BB84 à quatre états, avec deux états de polarisation supplémentaire représenté sur une base circulaire ($|C\rangle$, $|C'\rangle$) tel qu'il est illustré dans la figure 2.5.

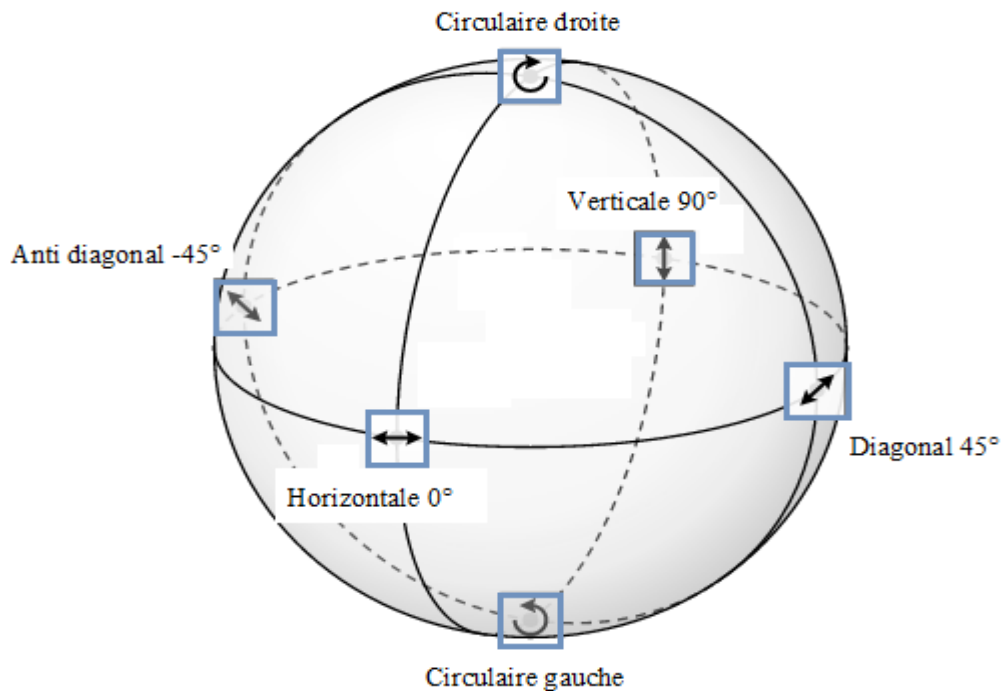


Figure 2.5 Etats de polarisation du protocole SSP.

La procédure du protocole SSP est similaire à celle du protocole BB84. À l'émission Alice envoie une séquence de bits aléatoire codé sur l'une des trois bases (6 états possibles). A la réception, Bob mesure les états reçus sur l'une des trois bases de polarisation choisit au hasard. La probabilité d'avoir sélectionné la bonne base est réduite à 1/3 au lieu de 1/2, ce qui signifie qu'ils rejettent 2/3 des qubits avant d'extraire la clé, et cela représente un avantage important. En revanche, il représente un inconvénient majeur lié à la diminution du taux de clés générées qui est dû au temps écoulé dans le choix des bases.

2.5 Implémentation du protocole BB84 sur OPTYSYSTEM

2.5.1 Présentation du logiciel

L'analyse des systèmes de communications optique, comprend des dispositifs très complexes et coûteux, de ce fait ces tâches ne peuvent être effectuées rapidement et efficacement qu'avec l'aide de nouveaux outils logiciels.

Dans notre travail, nous avons opté pour un logiciel de simulation des systèmes de communications optique. Il s'agit de l'Optisystem 7.0 « Optical Communications System Design Software », qui est un simulateur basant sur la modélisation réaliste des systèmes de communications par fibre optiques. En plus sa vaste bibliothèque contient plusieurs composants nécessaires à la réalisation d'une liaison WDM, comme il permet de visualiser le signal reçu et d'évaluer la qualité de transmission à la réception.

La démarche à suivre se décompose de deux étapes :

- Construire le schéma bloc.
- Analyser le schéma.

2.5.2 Simulation

Afin de simuler le protocole BB84. On utilise quatre diodes laser à une longueur d'onde de 1550 nm. Chacune est reliée à un atténuateur optique réglé à 0.1 dB, qui permet de créer un photon unique par impulsion. Par la suite, chaque photon est polarisé par un polariseur (0° , 90° , 45° , -45°). Ensuite l'un des quatre états sera choisi aléatoirement par un sélectionneur et l'envoi sur une fibre optique de 100 km.

A la réception, on utilisera un analyseur de polarisation et un compteur de photon pour visualiser l'état du photon reçu sur l'une des deux bases choisies aléatoirement.

Pour la réalisation de notre travail, nous l'avons divisé en 2 parties afin de bien comprendre le choix de base et les états de polarisations :

➤ Première partie :

Dans cette partie, nous avons choisi un seul canal qui émet un seul état polarisé à 45° comme c'est représenté dans la figure 2.6.

Chapitre 2 : Les protocoles de distributions quantiques de clés et l'implémentation du protocole BB84

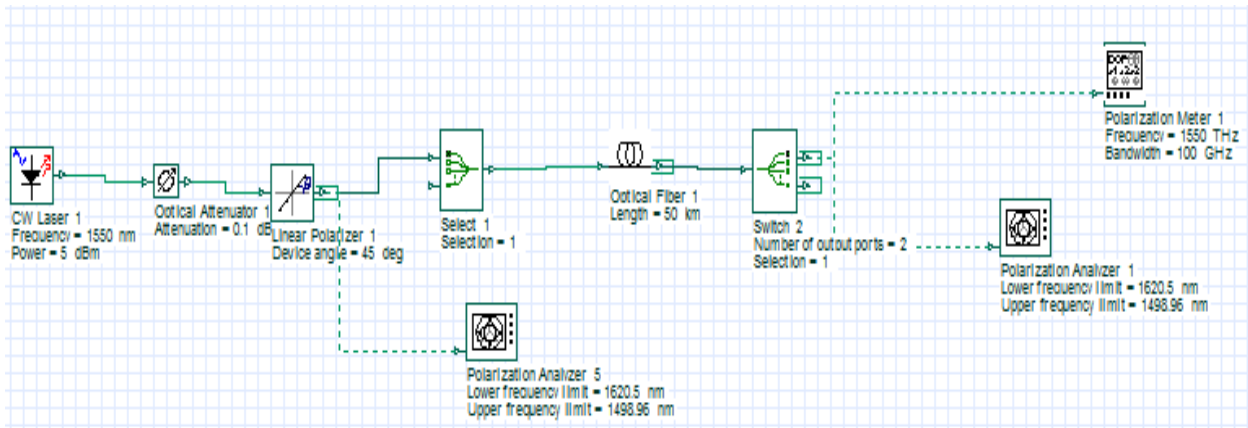


Figure 2.6 simulation de BB84 pour un seul canal.

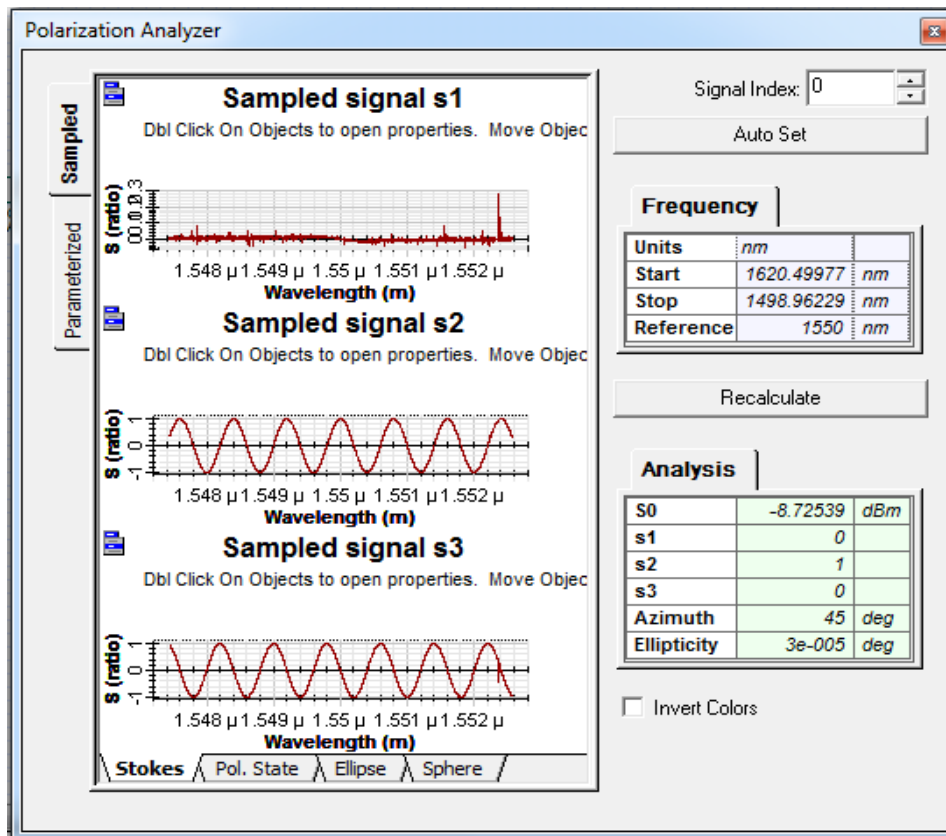


Figure 2.7 Paramètres de Stocks obtenus.

D'après les résultats obtenus dans la figure 2.7. Nous constatons que les paramètres de Stocks affichent quatre valeurs dérivant l'état de polarisation du photon ou chaque paramètre correspond à une différence de puissance :

- S0 représente la puissance totale transporté.
- S1 est la différence de puissance entre les polarisations verticale et horizontales.

Chapitre 2 : Les protocoles de distributions quantiques de clés et l'implémentation du protocole BB84

- S2 représente la différence de puissance entre la polarisation linéaire orientées à $+45^\circ$ et -45° de la polarisation verticale.
- S3 représente la différence de puissance entre la polarisation circulaire gauche et droite.

Dans cette simulation nous avons obtenu $S1=0$, $S2=1$, $S3=0$. Ces paramètres caractérisent l'angles 45° .

En comparant les résultats au niveau de l'émetteur tel qu'il est représenté dans la figure 2.8.a et au niveau du récepteur tel qu'il est illustré sur la figure 2.8.b, nous constatons que les polarisations sont identiques, c'est à dire qu'il n'y a pas de changement de polarisation entre l'état émis et celui reçu.

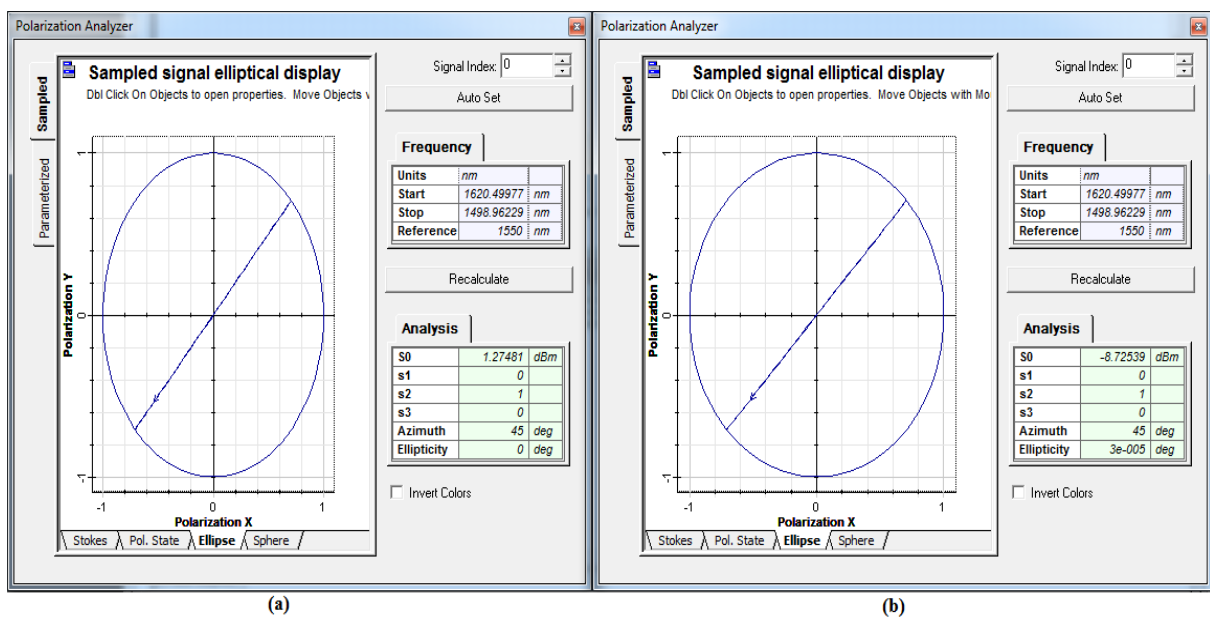


Figure 2.8 Paramètres de Stocks a) au niveau de l'émetteur. b) au niveau du récepteur.

➤ Deuxième partie

Dans cette partie on simulera le protocole BB84 à 4 états de polarisation ($0^\circ, 90^\circ, 45^\circ, -45^\circ$) tel qu'il est représenté sur la figure 2.9. Nous rajoutons un sélectionneur d'états. Et au niveau de récepteur, nous utilisons un Switch avec deux ports. Chaque port est relié à un compteur et un analyseur de polarisation, le résultat s'affichera d'une façon aléatoire sur l'un des analyseurs.

Chapitre 2 : Les protocoles de distributions quantiques de clés et l'implémentation du protocole BB84

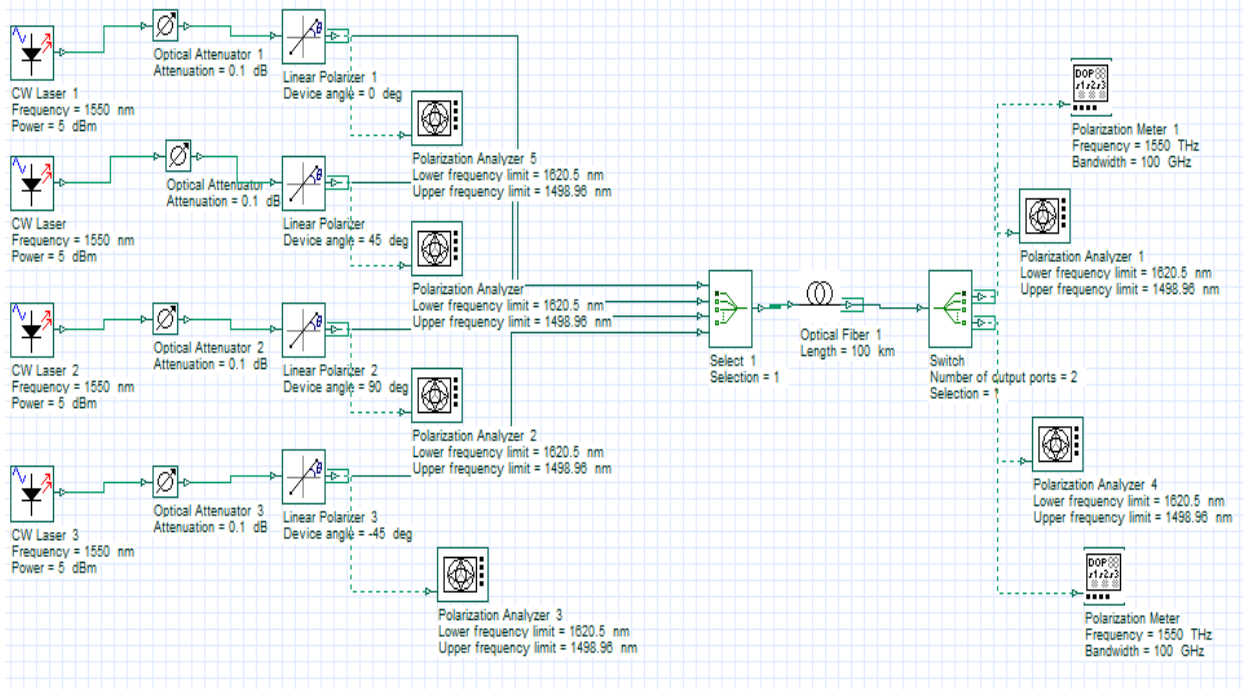


Figure 2.9 Simulation du protocole BB84.

Nous remarquons que le premier analyseur de polarisation au niveau du récepteur a choisis aléatoirement la polarisation horizontale (qubit 0) avec les paramètres de stocks suivant : $S_1=1$, $S_2=0$, ET $S_3=0$ comme c'est représenté dans la figure 10.a. Le deuxième analyseur n'affiche aucun résultat comme c'est représenté dans la figure 10.b.

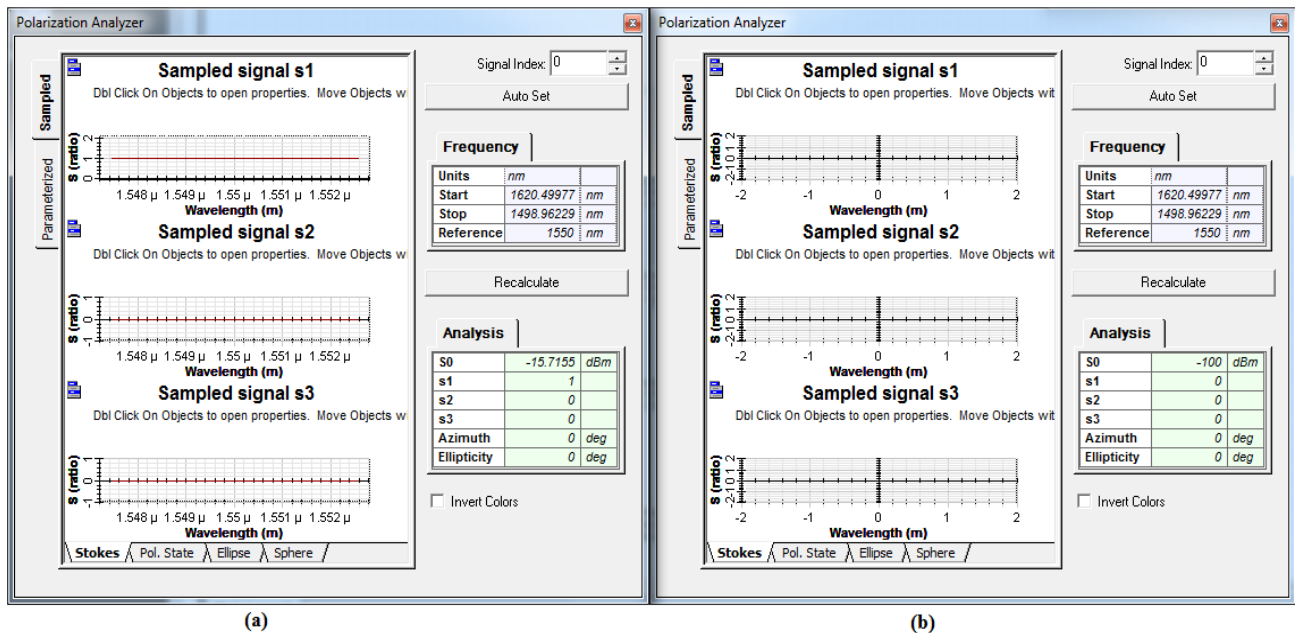


Figure 2.10 Paramètres de Stocks a) premier analyseur. b) deuxième analyseur.

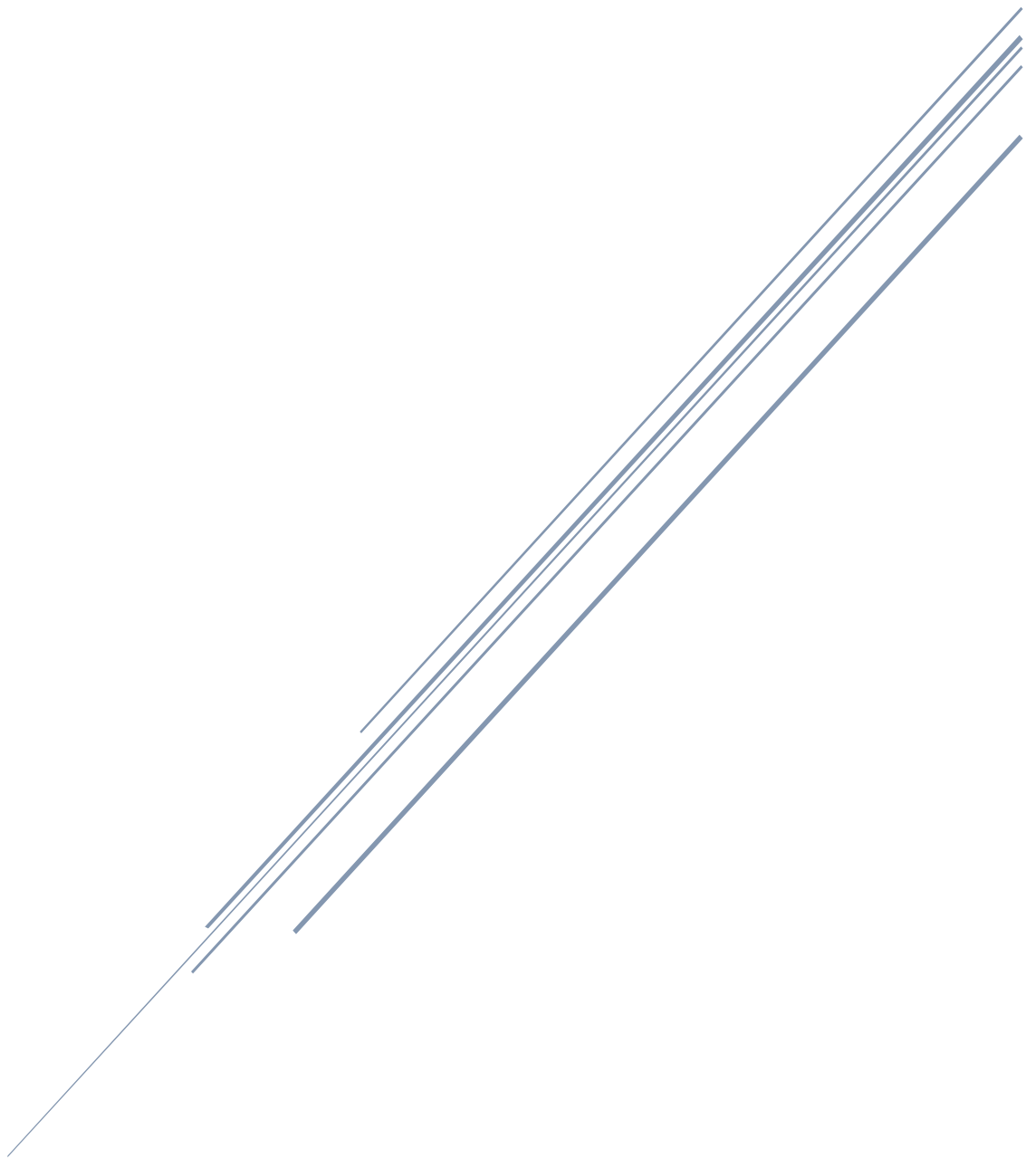
2.6 Conclusion

La distribution de clés quantiques est l'avenir du monde de la cryptographie, elle a été inventé pour augmenter le taux de sécurité lors de l'échange d'une clé privée.

Nous venons de voir dans ce chapitre que la distribution quantique de clé est basée sur l'utilisation des sources qui émettent des photons uniques. Ce chapitre décrit principalement les deux lois de la mécanique quantique sur lesquelles se base la cryptographie quantique, à savoir le théorème de non-clonage et le principe d'incertitude qui assurent la détection d'un espion qui tente d'intercepter les états quantiques envoyé par les deux participants. Nous avons présenté le protocole de distribution le plus connu qui est BB84 publié par Bennett et Brassard en 1984, puis divers protocoles QKD ont été développés à savoir leprotocole B92 et le protocole a six états. Ce dernier est similaire à celui de BB84 mais cette fois en utilisant seulement deux états non orthogonaux des quatre états de BB84. En dernier lieu nous avons implémenté le protocole BB84 sur une liaison optique en utilisant une source à photon très fortement atténuée pour enfin aboutir à des résultats similaires à la théorie.

CHAPITRE N°03 :

Les liaisons de transmission optique WDM et leurs applications dans la QKD



3 Les liaisons de transmission optique WDM et leurs applications dans la QKD

3.1 Introduction

Les réseaux optiques ont connu un développement rapide dû à l'augmentation de la demande de débit de transmission. De ce fait, les chercheurs ont préconisé comme solution d'augmenter le débit l'utilisation des liaisons de transmission optique WDM.

Dans la première section de ce chapitre, nous évoquerons le principe de base d'une transmission optique. Nous présenterons par la suite les liaisons WDM et l'avènement de la fibre optique comme support de transmission privilégié ainsi que ses différents composants à savoir l'émetteur et le récepteur optique ainsi que le canal de transmission, en donnant quelques caractéristiques. Nous poursuivons dans la deuxième section par une conception d'une liaison de transmission WDM à un débit égal à 46 Gb/s à l'aide du logiciel de simulation OPTISYSTEM, en définissant les éléments servant de critère de qualité pour évaluer la qualité de transmission du signal reçu. La troisième section sera consacrée pour les applications du WDM dans la distribution quantique de clés.

3.2 Principe de base d'une transmission optique

Un système de transmission optique est constitué de trois parties essentielles : un émetteur qui traduit les signaux électriques en impulsions optiques, un récepteur qui effectue l'opération inverse, ainsi qu'un canal de transmission (fibre optique) via lequel les informations sont portées.

Des amplificateurs et des répéteurs sont placés afin de régler les problèmes dus à l'atténuation et la déformation du signal lors de son parcours dans la fibre optique. La figure 3.1 illustre le principe de base d'une transmission de données par une fibre optique.

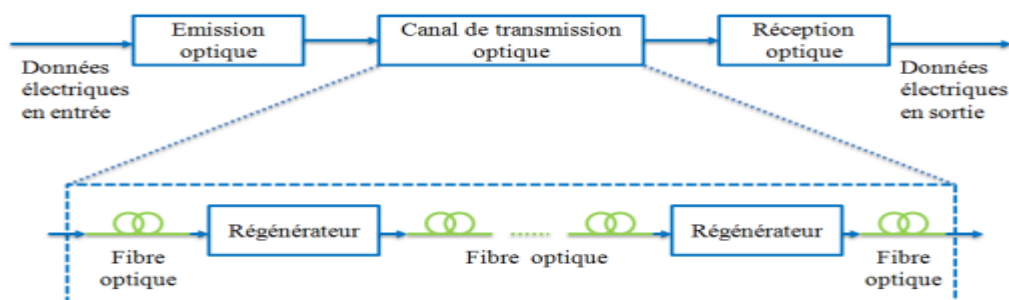


Figure 3.1 Principe de base d'une transmission optique.

3.3 Liaison de transmission optique WDM

Le multiplexage en longueur d'onde (WDM) consiste à mélanger plusieurs signaux optiques sur une même fibre optique afin de multiplier la bande passante de celle-ci[5]. Les signaux sont portés par des longueurs d'ondes différentes, et espacées assez largement afin de ne pas interférer les unes avec les autres. Le principe d'une liaison WDM est illustré dans la figure 3.2.

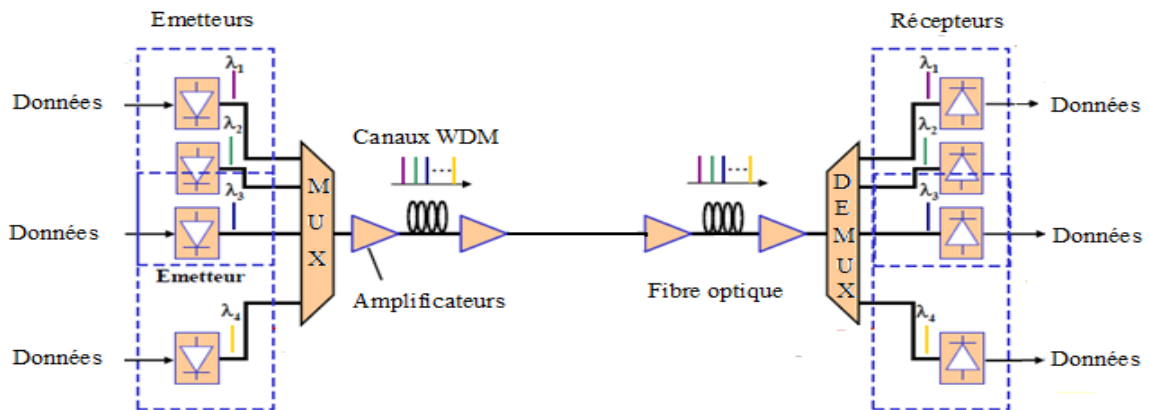


Figure 3.2 Principe d'une liaison WDM.

3.3.1 Composants d'un système WDM

Un système WDM est composé de :

3.3.1.1 Emetteur optique

Un émetteur optique comprend une source de lumière à longueur d'onde variable qui sert à générer un signal optique et un modulateur utilisé pour moduler et émettre la lumière émise de la source comme c'est représenté dans la figure 3.3.

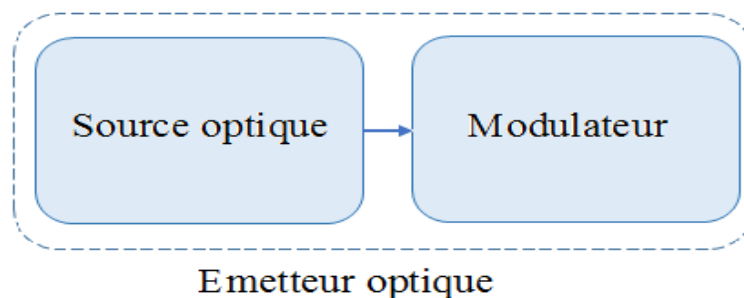


Figure 3.3Éléments d'un émetteur optique.

- **Source optique**

La fonction fondamentale d'une source optique est de convertir une énergie électrique en une énergie optique (conversion électro-optique). Les deux catégories de sources les plus adaptées sont les diodes électroluminescentes (LED) et le laser. Dans le cas des liaisons haut débit, seules les diodes laser sont utilisées.

- A. La diode électroluminescente (LED) :**

Une diode électroluminescente (light-emitting diode) est un dispositif ou composant optoélectronique capable d'émettre de la lumière lorsqu'elle est parcourue par un courant électrique [6]. Son principe est basé sur l'émission spontanée. Son symbole est représenté dans la figure 3.4.



Figure 3.4 Symbole de la LED.

Généralement, La diode électroluminescente est utilisée avec les fibres multimodes.

- B. Laser (Light Amplification by Stimulated Emission of Radiation):**

Le laser est un composant essentiel dans les transmissions par fibre optique. Il est basé sur le principe d'amplification par émission stimulée donnant un rayonnement cohérent.

- **Le modulateur**

Afin de transmettre des informations dans une liaison optique, il faut imprimer ces informations sur un signal physique et l'envoyer sur une fibre, ce procédé s'appelle la modulation.

On peut distinguer deux type de modulations :

- A. Modulation directe**

Dans la modulation directe, on utilise un laser d'où son avantage réside dans le fait qu'il est possible de modifier le courant d'injection au sein du même laser, comme c'est représenté dans la figure 3.5.

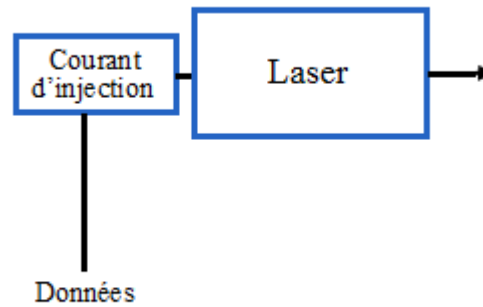


Figure 3.5 Schéma d'un modulateur interne.

Dans cette technique le courant qui traverse le laser entraîne d'une manière directe une modulation en intensité de la lumière émise, autrement dit plus le courant reçu par le laser est important, plus l'intensité lumineuse qu'il délivrera sera puissante.

Ce type de modulation connaît beaucoup d'avantages, en particulier un coût de mise en œuvre très faible.

B. Modulation externe

En utilisant une source laser, la modulation directe est satisfaisante jusqu'à 5 GHz, mais qu'au-delà de cette valeur cette méthode entraîne des dégradations et limite la capacité de transmission.

La modulation externe est obtenue en modulant directement le faisceau lumineux en sortie du laser et non plus le courant d'alimentation à l'entrée du laser [5]. Ce type de modulation est effectuée par un modulateur externe (Mach Zehnder,...). Lorsque le signal optique émis par le laser traverse le modulateur, il subit des modifications du facteur de transmission et le signal à la sortie du modulateur externe se trouve donc modulé comme c'est montré dans la figure 3.6.

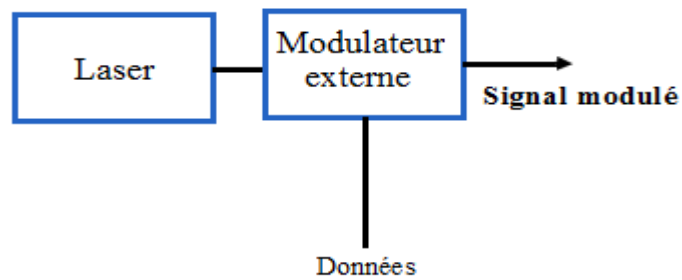


Figure 3.6 Schéma d'un modulateur externe.

3.3.1.2 La fibre optique

La fibre optique est un support de transmission en verre ou en plastique très fin, capable de conduire la lumière (impulsions lumineuses) en offrant un débit de transmission de données très important.

Elle est constituée de :

- **Cœur :**

Le cœur de la fibre optique est composé de silice très pure, il possède un diamètre compris entre 10 à 85 μ m selon le type de fibre et un indice de réfraction n_1 .

- **Gaine optique :**

La gaine optique est aussi constitué de silice, mais avec un indice de réfraction n_2 inférieur à celui du cœur

- **Revêtement externe :**

La gaine protège de la fibre optique et facilite la manipulation. Elle joue ainsi le rôle d'isolateur contre le milieu extérieur (pluie, humidité...). Comme c'est représenté dans la figure 3.7.

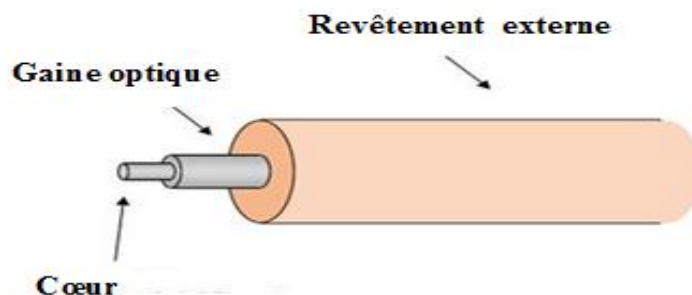


Figure 3.7 Composant d'une fibre optique.

Il existe deux types de fibre optique :

A. Fibre monomode :

Dans une telle fibre, il existe un seul mode de propagation c'est le mode en ligne droite comme c'est montré dans la figure 3.8. La dimension de son cœur est très faible (un diamètre environ $10\mu\text{m}$)



Figure 3.8 Fibre monomode.

Ce type de fibre est utilisé dans les liaisons à longues distances.

B. Fibre multimode :

Dans les fibres multimodes, plusieurs modes peuvent se propager comme c'est montré dans la figure 3.9. Ce type de fibre a un cœur important (de $50\mu\text{m}$ jusqu'à $85\mu\text{m}$).

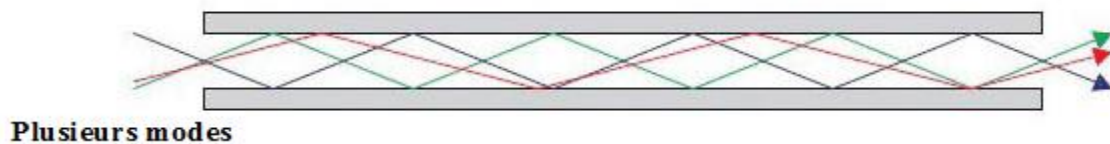


Figure 3.9 Fibre multimode.

Elles sont généralement utilisées pour de courtes distances.

➤ **Propriétés de la fibre**

La fibre optique possède deux propriétés importantes : l'atténuation et la dispersion.

A. Atténuation :

L'atténuation représente la réduction de la puissance du signal au cours de sa propagation [7]. Cet effet limite la capacité de transmission.

Lors de la propagation de la lumière dans une fibre optique, elle s'atténue progressivement tel qu'il est illustré dans la figure 3.10. Plus la distance parcouru est importante plus le signal s'affaiblit.

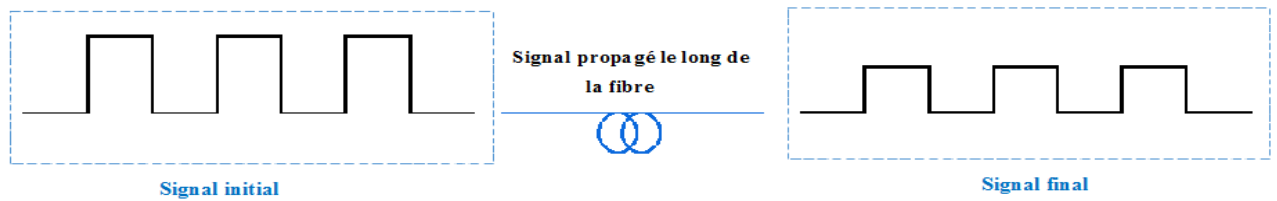


Figure 3.10 Phénomène d'atténuation dans une fibre optique.

La longueur d'onde de la lumière utilisée pour la transmission d'un signal dans une fibre optique correspond à un minimum d'atténuation. On distingue trois fenêtres, comme le montre la figure 3.11. Le tableau 3.1 récapitule les trois grandes fenêtres de transmission utilisées.

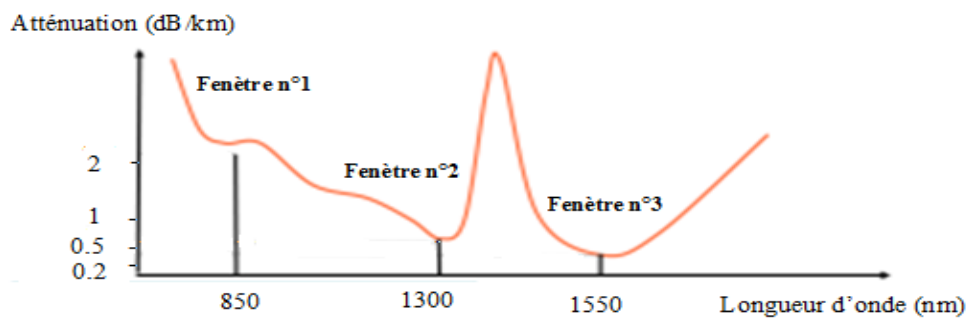


Figure 3.11 L'atténuation en fonction de la longueur d'onde.

	Fenêtre n°1	Fenêtre n°2	Fenêtre n°3
Longueur d'onde	780 à 900 nm	1300 nm	1500 à 1600 nm
Atténuation	Forte (2 à 4 dB/km)	Faible (0.4 à 1 dB/km)	Très faible (0.2 dB/km)
Type de fibre	Multimode	Multimode et monomode	Monomode
Type d'émetteur	Diode électroluminescente diode laser	Diode électroluminescente (fibre multimode) Diode laser (fibre monomode)	Diode laser
Application	Transmission courte distance et réseaux locaux.	Transmission courte et moyenne, réseaux LAN et MAN.	Transmission longue distance

Tableau 3.1 Les trois grandes fenêtres d'atténuation.

B. La dispersion :

La dispersion d'un signal optique se manifeste par une distorsion du signal causant un élargissement temporel des impulsions au cours de leur propagation dans la fibre optique [8], comme c'est illustré dans la figure 3.12

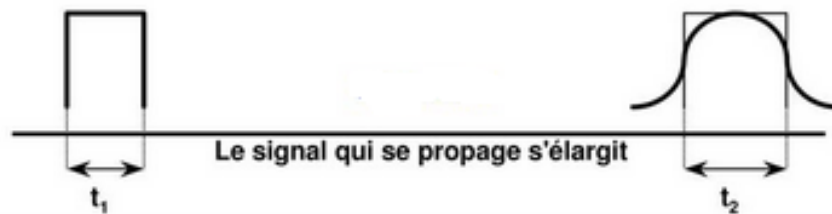


Figure 3.12 La dispersion chromatique.

➤ Avantages

La fibre optique possède une atténuation moins importante que les autres canaux de transmission (faisceaux Hertziens et les lignes en cuivres), ce qui permet une transmission sur de plus longues distances, elle permet d'atteindre des capacités de transport plus élevées et avec plus de sécurité.

3.3.1.3 Multiplexeur et démultiplexeur en longueur d'onde

Le multiplexeur permet d'additionner les signaux sur une fibre optique et le démultiplexeur permet de séparer ces différents signaux pour disposer sur chaque sortie l'un de ces signaux avec la même longueur d'onde qu'à l'entrée, comme c'est illustre dans la figure 3.13.

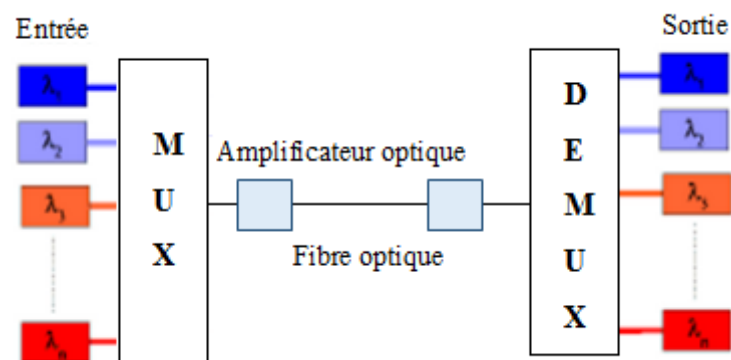


Figure 3.13 Le multiplexeur et démultiplexeur utilisé dans une liaison WDM.

3.3.1.4 Amplificateur optique

Avant le multiplexage en longueur d'onde, la seule manière d'augmenter la capacité d'une liaison optique était de rajouter des lignes de transmission et des répéteurs-régénérateurs. En technologie WDM, un seul amplificateur optique remplace plusieurs régénérateurs.

La distance de propagation d'un signal sur une fibre optique est limitée par l'atténuation et la dispersion [9]. C'est pour cela qu'on utilise les amplificateurs optiques dans les liaisons à longue distance.

3.3.1.5 Récepteur optique

Après propagation le long d'une série de tronçons de fibres optiques et d'amplificateurs, le signal arrive au niveau du récepteur [10].

Un récepteur optique ou photo-détecteur est un capteur de lumière qui permet de convertir un signal optique provenant dans la fibre optique en un signal électrique.

Chaque photo-détecteur a des caractéristiques propres à son utilisation et ses matériaux de fabrication.

3.4 Simulation d'une liaison optique WDM sous l'OPTISYSTEM

3.4.1 Les critères de qualité d'une transmission optique

Au vu de toutes les dégradations que peut subir le signal lors de son transport via la fibre optique, il s'est avéré nécessaire d'établir des critères pour juger de la qualité d'une transmission. Les trois principaux critères de qualité d'un signal transmis sont le diagramme de l'œil, le taux d'erreur binaire (BER) et le facteur de qualité(Q) [11].

3.4.1.1 Diagramme de l'œil

La meilleure façon de juger la qualité un signal est d'observer le diagramme de l'œil qui représente la superposition synchrone de tous les symboles binaires de la séquence transmise [12].

3.4.1.2 Taux d'erreur binaire (BER)

Une qualité de transmission numérique est simple à évaluer ; il suffit donc de comparer la séquence de symboles envoyés à celle de symboles reçus, et de compter les erreurs (nombre de fois où "0" est détecté pour un "1" émis ou vice versa. Le taux d'erreurs binaires 'Bite Error

Rate' est défini par le rapport entre le nombre de bits erronés et le nombre de bits transmis :
alité de transmission pour un TEB inférieur à 10^{-12} [13].

$$BER = \frac{\text{nombre de bits erronés}}{\text{nombre de bits transmis}} \quad (3.1)$$

3.4.1.3 Facteur de qualité (Q)

Le facteur de qualité (Q) obtenu à partir des statistiques de bruit (moyennes et écarts-types) des niveaux « 1 » et « 0 » du signal à détecter. C'est un paramètre permettant d'estimer le taux d'erreur binaire sans avoir à compter de les erreurs, mais en considérant tout simplement l'amplitude moyenne des bits 1 et 0 et la valeur de leur écart type σ_1 et σ_2 ce facteur est défini par :

$$Q = \frac{I_1 - I_2}{\sigma_1 + \sigma_2} \quad (3.2)$$

Où, I_1 et I_2 sont respectivement les valeurs moyennes des niveaux 1 et 0, σ_1 et σ_2 les écart-type du bruit sur le signal des symboles 1 et 0.

3.4.2 Les Composants de la liaison optique

Dans Cette partie nous présenterons les différents composants présents et nécessaires pour notre simulation. Ces composants sont choisis en fonction des objectives de simulation.

➤ Générateur de séquence binaire

Il représente les données numériques qui vont servir pour la génération du courant électrique à l'entrée du laser. Son modèle de simulation est représenté dans la figure 3.14.

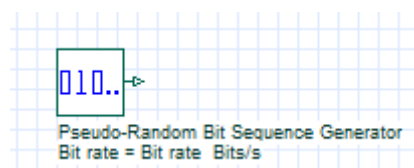


Figure 3.14 Modèle de simulation de la séquence binaire.

➤ Générateur NRZ

Le générateur d'impulsions NRZ permet de créer une séquence d'impulsions codée par un signal numérique d'entrée, et prend uniquement deux valeurs ou le (0) est codé par un signal faible puissance et le (1) est codé par un signal fort puissance. Son modèle de simulation est représenté dans la figure 3.15.

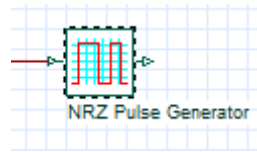


Figure 3.15 Modèle de simulation du générateur NRZ.

➤ **Diode laser**

La diode laser sert comme source optique, son modèle de simulation est représenté dans la figure 3.16.

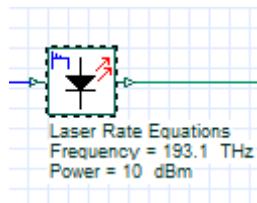


Figure 3.16 Modèle de simulation de la diode laser.

Les paramètres caractéristiques de la diode laser sont représentés dans le tableau 3.2.

Name	Value	Units
Frequency	193.1	THz
Calculate current	<input checked="" type="checkbox"/>	
Power	10	dBm
Power at bias current	0	dBm
Bias current	38	mA
Modulation peak current	28	mA
Threshold current	33.45723247941	mA
Threshold Power	0.01541301355644	mW

Tableau 3.2 Paramètres caractéristiques de la diode laser.

➤ **Fibre optique**

Nous avons utilisé une fibre optique d'une longueur de 50km, son modèle de simulation est représenté dans la figure 3.17.

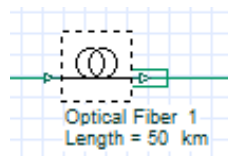


Figure 3.17 Modèle de simulation d'une fibre optique.

➤ **Multiplexeur WDM**

Nous avons placé un multiplexeur optique afin de regrouper sur une même sortie plusieurs longueurs d'ondes issues de différentes entrées. Son modèle de simulation est représenté dans la figure 3.18.

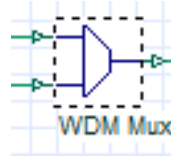


Figure 3.18 Modèle de simulation d'un multiplexeur WDM.

➤ **Démultiplexeur WDM**

Nous avons utilisé un démultiplexeur optique dans le but de séparer les différentes longueurs d'onde, il fait l'opération inverse du multiplexeur. Son modèle de simulation est représenté dans la figure 3.19.

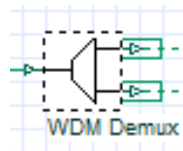


Figure 3.19 Modèle de simulation d'un demultiplexeur WDM.

➤ **Photodiode PIN**

Elle est utilisée comme un récepteur du signal optique. Son modèle de simulation est représenté dans la figure 3.20.

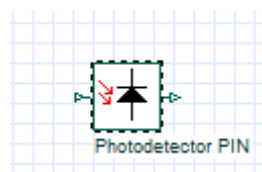


Figure 3.20 Modèle de simulation d'une photodiode PIN.

➤ **Diagramme de l'œil**

Il nous permet de visualiser la qualité du signal reçu dans le domaine temporel. Lorsque l'ouverture de l'œil est bien ouverte cela signifie que le signale est bien transmit et lorsque L'ouverture est fermée cela se traduit par de nombreuse erreurs de transmission. Son modèle de simulation est représenté dans la figure 3.21.

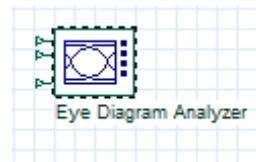


Figure 3.21 Modèle de simulation du diagramme de l'œil.

➤ **Filtre passe bas**

Afin de réduire le bruit engendré tout au long de la traversée du signal dans les divers composants, on place un filtre à la sortie du récepteur. Son modèle de simulation est représenté dans la figure 3.22.

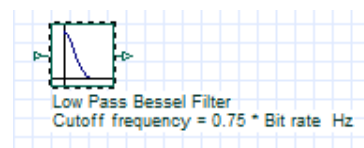


Figure 3.22 Modèle de simulation filtre passe bas Bessel.

3.4.3 Simulation d'une chaîne de transmission optique de base

3.4.3.1 Chaîne de transmission sans filtre

Dans cette partie, nous simulerons une chaîne de transmission de base qui contient une séquence binaire de 1 Gbps codée en NRZ. L'information générée va se propager dans une fibre monomode de longueur de 50 Km. À la réception, nous placerons une photodiode PIN afin de détecter le signal optique, la qualité de transmission sera ensuite visualisée par le diagramme de l'œil. Cette chaîne de transmission est représentée dans la figure 3.23.

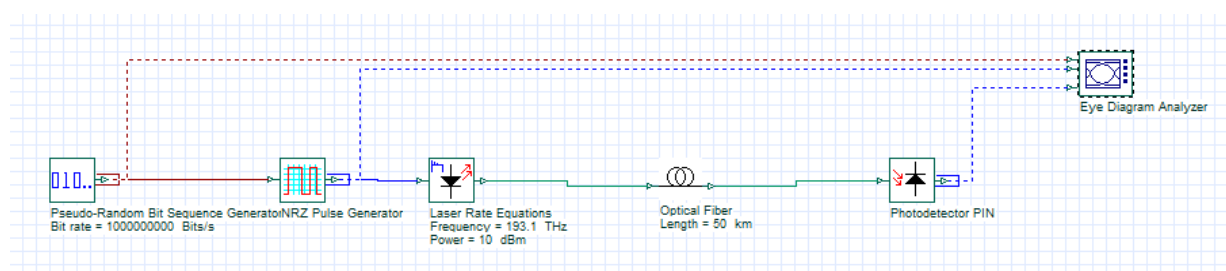


Figure 3.23 Chaîne de transmission de base.

La simulation de cette chaîne nous a donné le diagramme de l'œil représenté sur la figure 3.24.

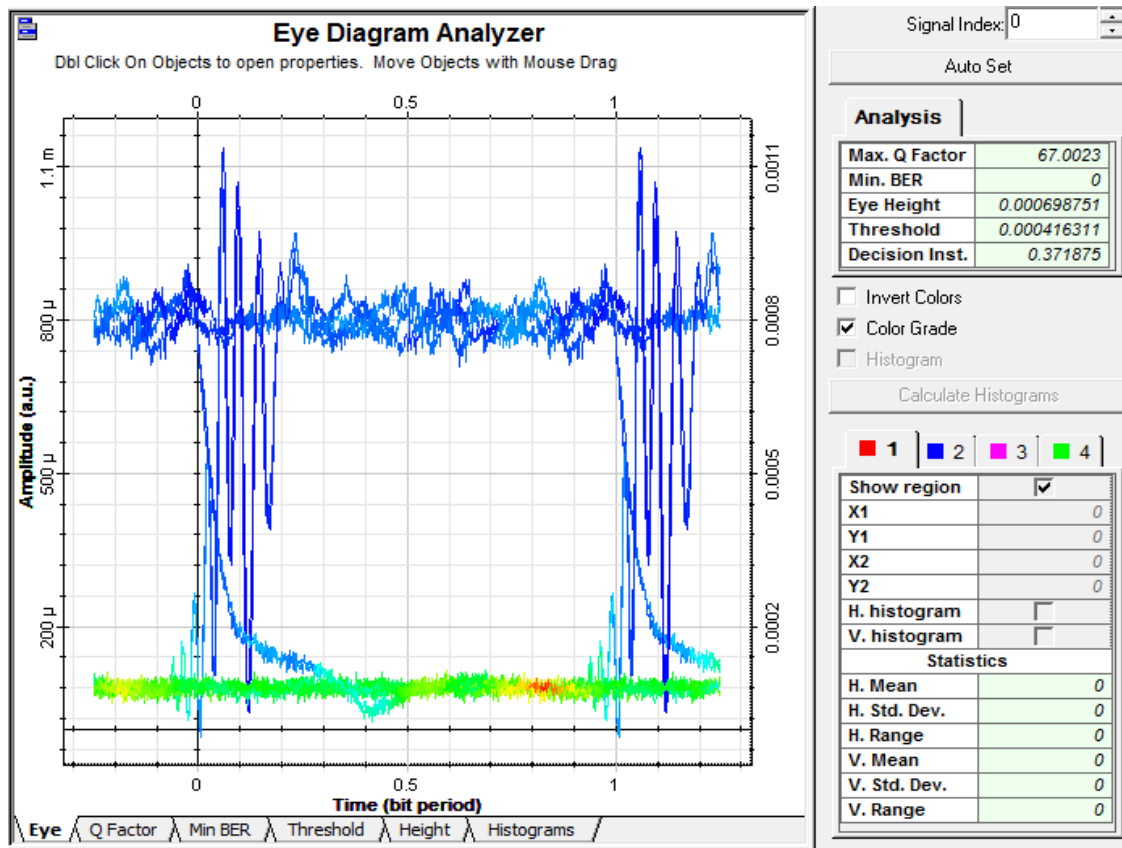


Figure 3.24 Diagramme de l'œil d'une chaîne de transmission pour D=1Gbps.

✓ **Interprétation des résultats**

La simulation d'une chaîne de transmission optique pour un débit de 1Gbps a permis d'obtenir un diagramme de l'œil ouvert avec un facteur de qualité égale à 67, ce qui montre que la qualité de transmission est bonne. On observe aussi la présence du bruit ce qui conduit à l'ajout d'un filtre.

3.4.3.2 Chaîne de transmission avec filtre

Dans cette partie nous avons rajouter un filtre passe bas à la chaîne de transmission précédente comme c'est montré dans la figure 3.25.

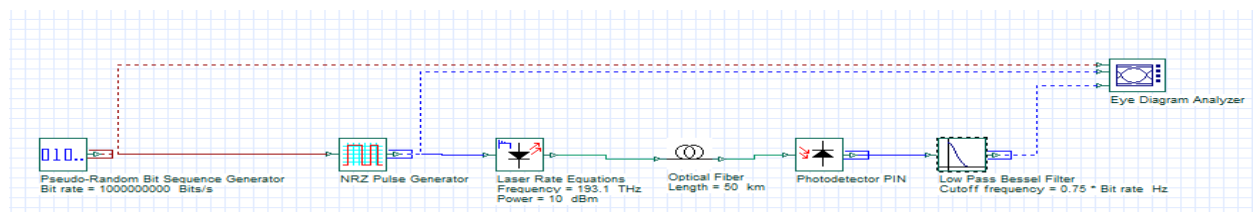


Figure 3.25 Chaîne de transmission avec filtre.

La simulation de cette chaîne de transmission avec le même débit de 1Gbps a donné le diagramme de l'œil représenté dans la figure 3.26.

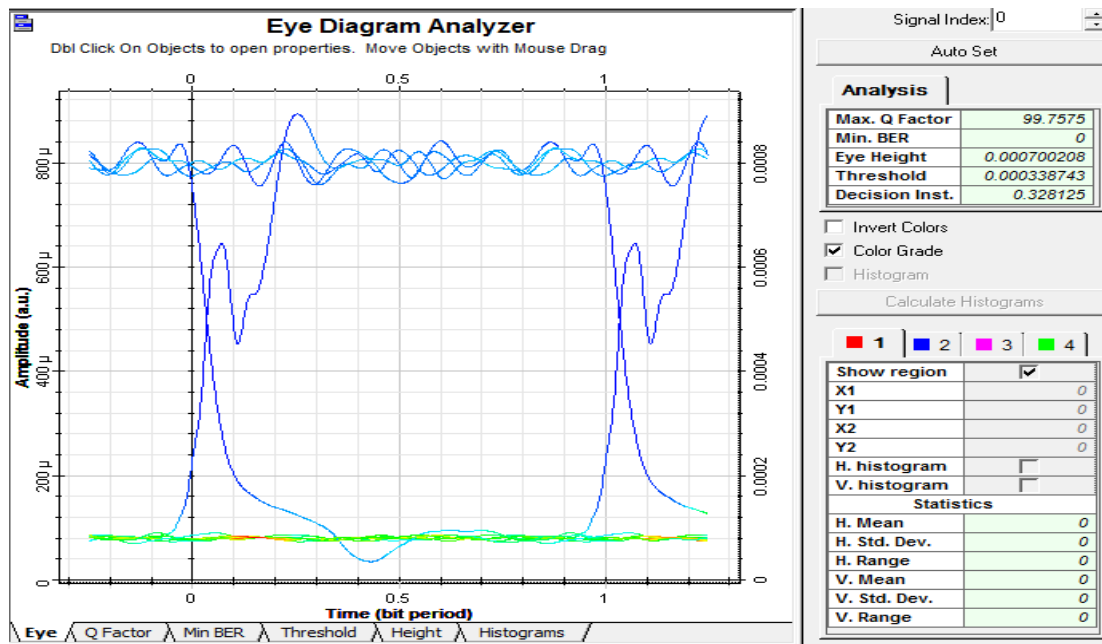


Figure 3.26 Diagramme de l'œil d'une chaîne avec filtre.

✓ **Interprétation des résultats**

L'ajout du filtre a permis d'avoir un diagramme de l'œil plus ouvert et sans bruit avec un facteur de qualité de 99.75, par conséquent la qualité de transmission devient meilleure.

3.4.3.3 Chaîne de transmission avec modulation interne

Afin de déterminer les limites de la modulation directe, nous allons augmenter le débit de transmission en visualisant le diagramme de l'œil ainsi que le facteur de qualité à chaque fois, et les résultats obtenus sont représentés dans le tableau 3.3.

Débit (D)	Facteur de qualité (Q)	Taux d'erreur (TEB)
1 Gbps	99.75	0
2 Gbps	44.28	0
3 Gbps	18.28	$5.128 \cdot 10^{-75}$
3.5 Gbps	10.40	$1.13 \cdot 10^{-25}$
4 Gbps	5.52	$1041 \cdot 10^{-8}$

Tableau 3.3 La variation du facteur de qualité et le taux d'erreur binaire en fonction du débit.

✓ **Interprétation des résultats**

D'après les résultats obtenus dans le tableau 3.3, nous remarquons que lorsque le débit augmente, le facteur de qualité Q diminue et la qualité de transmission devient mauvaise. Cette diminution est due aux pertes et à l'atténuation de la fibre optique.

On remarque que pour un débit de 4 Gbps on a obtenu un facteur de qualité inferieur a 6 Sachant que les normes fixées dans le domaine de télécommunications demandent, un facteur supérieur à 6 pour maintenir la qualité de transmission, on peut donc en déduire qu'avec la modulation directe on ne peut pas transmettre au-delà de 3.5 Gbps.

Bien que la modulation interne est simple à utiliser parce qu'elle ne comporte pas trop de composants mais elle a une limitation par rapport au débit qui ne dépasse pas 3.5 Gbps, ce qui signifie qu'au-delà de cette valeur, des effets d'atténuation vont apparaitre. Dans le but de résoudre ce problème on utilisera une modulation externe.

3.4.3.4 Chaîne de transmission avec modulation externe

Dans cette partie, nous allons remplacer la modulation interne par une modulation externe afin d'atteindre les hauts débits en rajoutant le modulateur Match Zehnder comme c'est montré dans la figure 3.27.

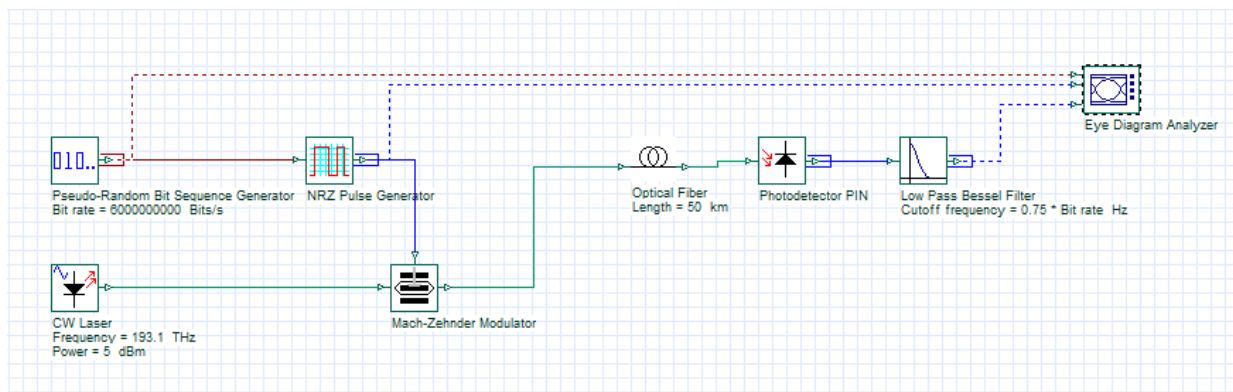


Figure 3.27 Chaîne de transmission avec modulateur externe.

La simulation de cette chaine de transmission avec un débit de 6 Gbps a donné un facteur de qualité de 15.81.

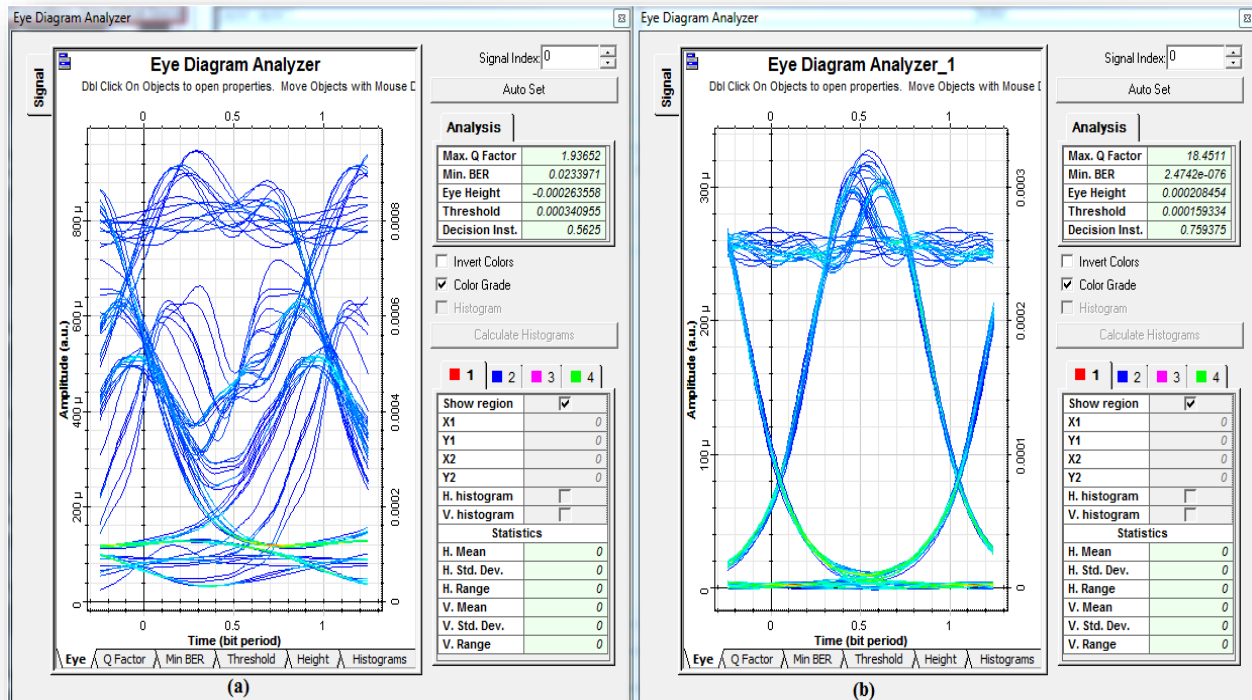


Figure 3.28 Diagramme de l'œil : a) modulation directe b) modulation externe.

Avec l'utilisation de la modulation externe le facteur de qualité a augmenté de 1.84 à 15.81 comme c'est montré dans les figures 3.28.a et 3.28.b.

3.4.4 Chaîne de transmission optique WDM 6x8 Gbit/s

Dans cette partie, nous allons simuler une chaîne de transmission optique WDM de 8 canaux avec un débit pour chacun de 6 Gbps espacé de 100GHz. La chaîne de transmission est représentée dans la figure 3.29.

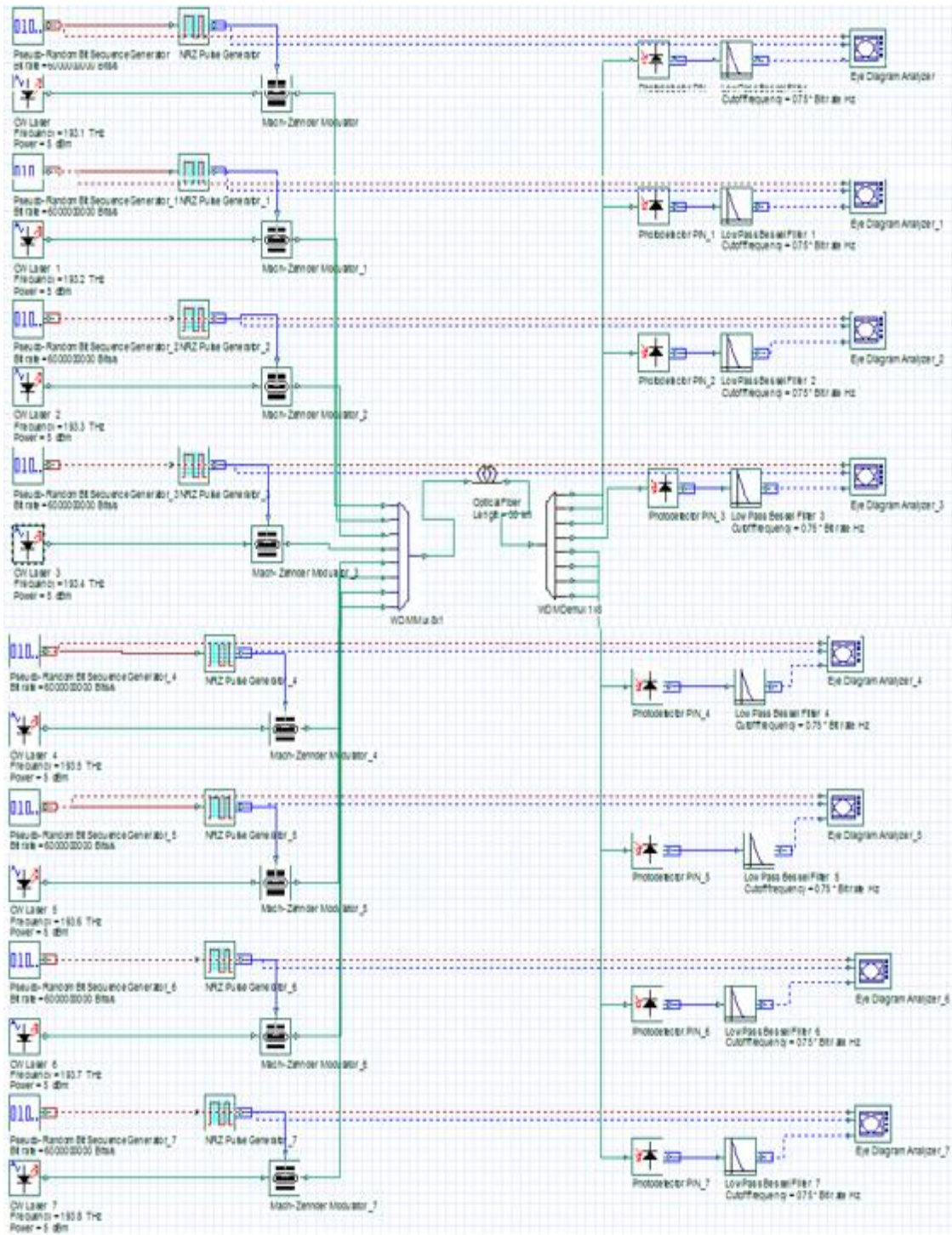


Figure 3.29 simulation d'une chaine WDM 8 x 6Gbps.

Le diagramme de l'œil de l'un des huit canaux est représenté dans la figure 3.30.

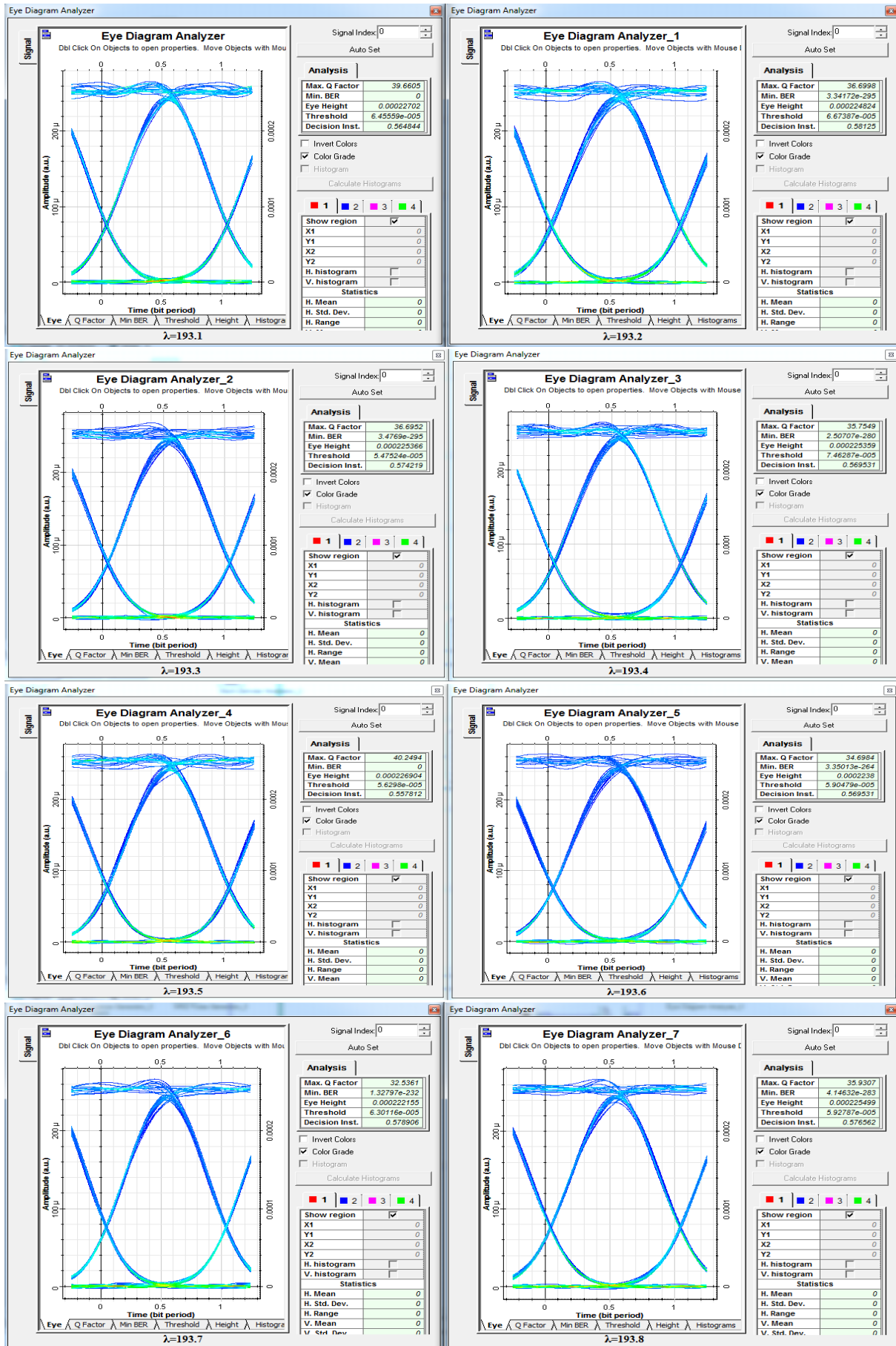


Figure 3.30 Diagramme de l'œil pour une liaison WDM 8 x 6Gbps.

Nous remarquons dans cette simulation que le diagramme de l'œil est bien ouvert et le facteur de qualité est supérieur à 6 pour tous les utilisateurs, le TEB est inférieur à 10^{-12} ce qui signifie que la transmission est sans erreur comme c'est montré dans le tableau 3.4. Cela montre que chaque utilisateur peut transmettre avec un débit de 6 Gbps et que le système fonctionne correctement.

Fréquences	Facteur de qualité (Q)	Taux d'erreur (TEB)
193.1	39.66	0
193.2	36.69	$3.34 \cdot 10^{-295}$
193.3	36.69	$3.47 \cdot 10^{-295}$
193.4	35.75	$2.50 \cdot 10^{-280}$
193.5	40.24	0
193.6	34.69	$3.35 \cdot 10^{-264}$
193.7	32.53	$1.32 \cdot 10^{-232}$
193.8	35.93	$4.14 \cdot 10^{-283}$

Tableau 3.4 le facteur de qualité et Taux d'erreur pour une liaison WDM a 8 canaux.

3.5 Application du WDM dans la distribution quantique de clés

Les techniques de distribution quantique de clés reposent sur l'exploitation des lois de la mécanique quantique, d'où leurs fonctionnalités ont été largement développées et les dernières recherches ont mené pour augmenter le taux de clé secrète en utilisant le multiplexage en longueur d'onde. Les systèmes QKD multiplexés ont deux objectifs : augmenter le taux de clé et fournir des clés secrètes à différents utilisateurs simultanément comme c'est montré sur la figure 3.31.

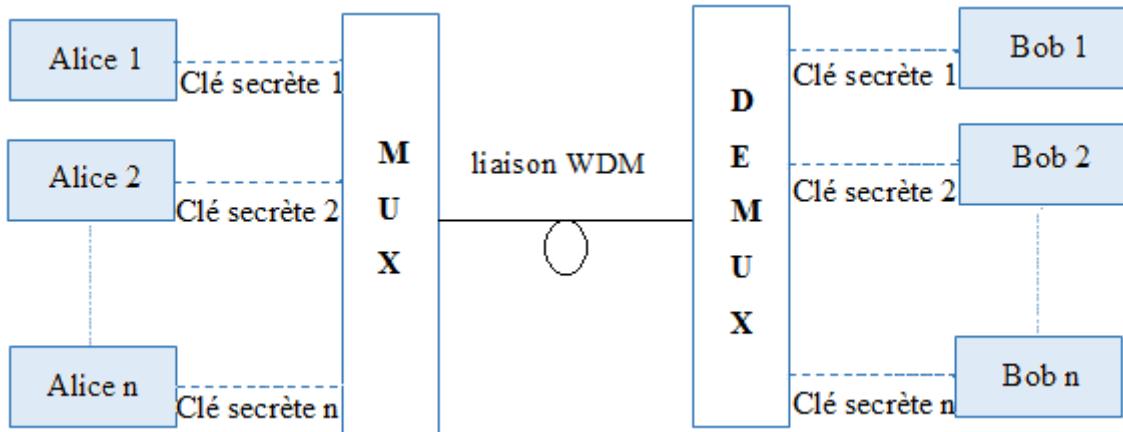


Figure 3.31 Fourniture des clés secrètes pour différents utilisateurs simultanément par un système QKD-WDM.

En principe, l'approche WDM-QKD est très intéressante parce qu'elle est compatible avec les techniques utilisées dans la transmission des canaux d'information classique et l'intégration du système QKD dans l'infrastructure existante du réseau WDM est un moyen pratique pour réduire la difficulté et le cout du réseau QKD.

Un système QKD intégré sur une liaison WDM peut aussi être utilisé entre deux utilisateurs (Alice et Bob) en fournissant un ou plusieurs canaux quantiques et un ou plusieurs canaux classiques et attribuer différentes longueurs d'onde pour chaque canal comme il est montré dans la figure 3.32. Sur les canaux quantiques se fait la transmission des clés secrètes, et sur les canaux classiques se fait la transmission des données, ces données comprennent soit des signaux de déclenchement pour synchroniser la transmission des clés.

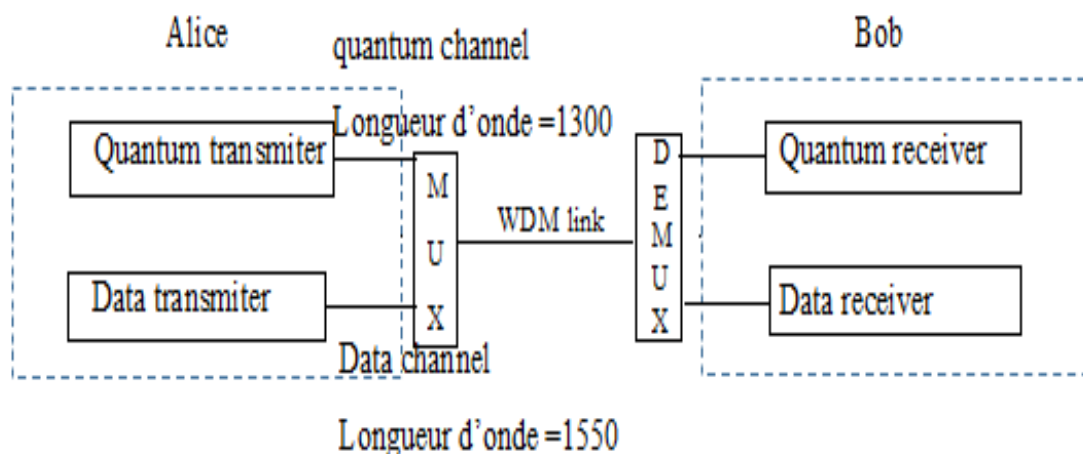


Figure 3.32 Un système QKD intégré sur une liaison WDM utilisé entre deux utilisateurs.

3.5.1 Simulation d'un système WDM-QKD

➤ Liaison 1 Gbps

Dans cette partie nous allons intégrer un système QKD sur une liaison WDM 1 Gbps en utilisant une diode laser spécial (SLRE), ce type de diode est conçues pour les faibles signaux, elle a un facteur de bruit très faible, et elle est utilisée pour des système de haute précision. Ensuite relier à un atténuateur optique régler à 0.1 dB qui permet de créer un seul photon par impulsion comme c'est représenté dans la figure 3.33.

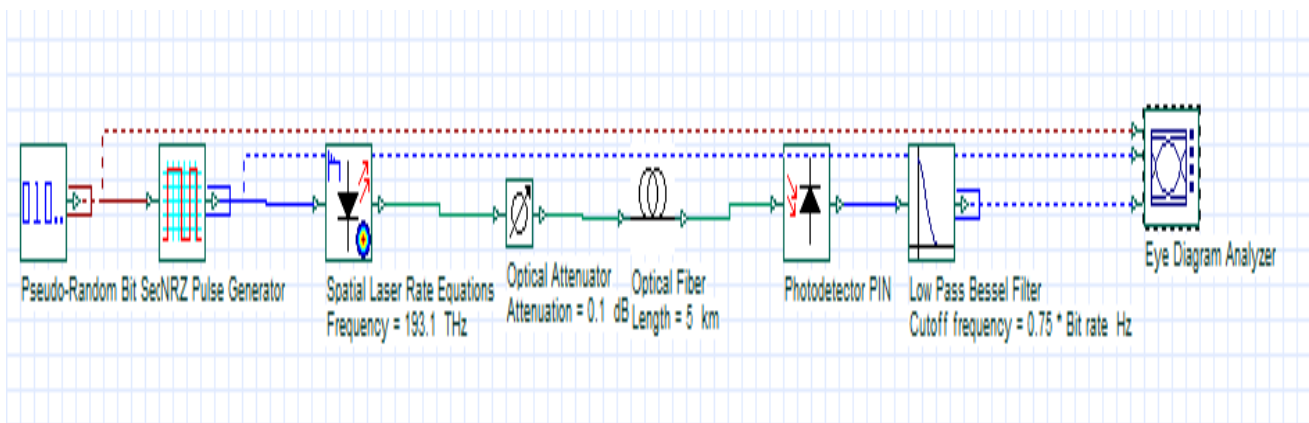


Figure 3.33 Chaîne de transmission avec un atténuateur.

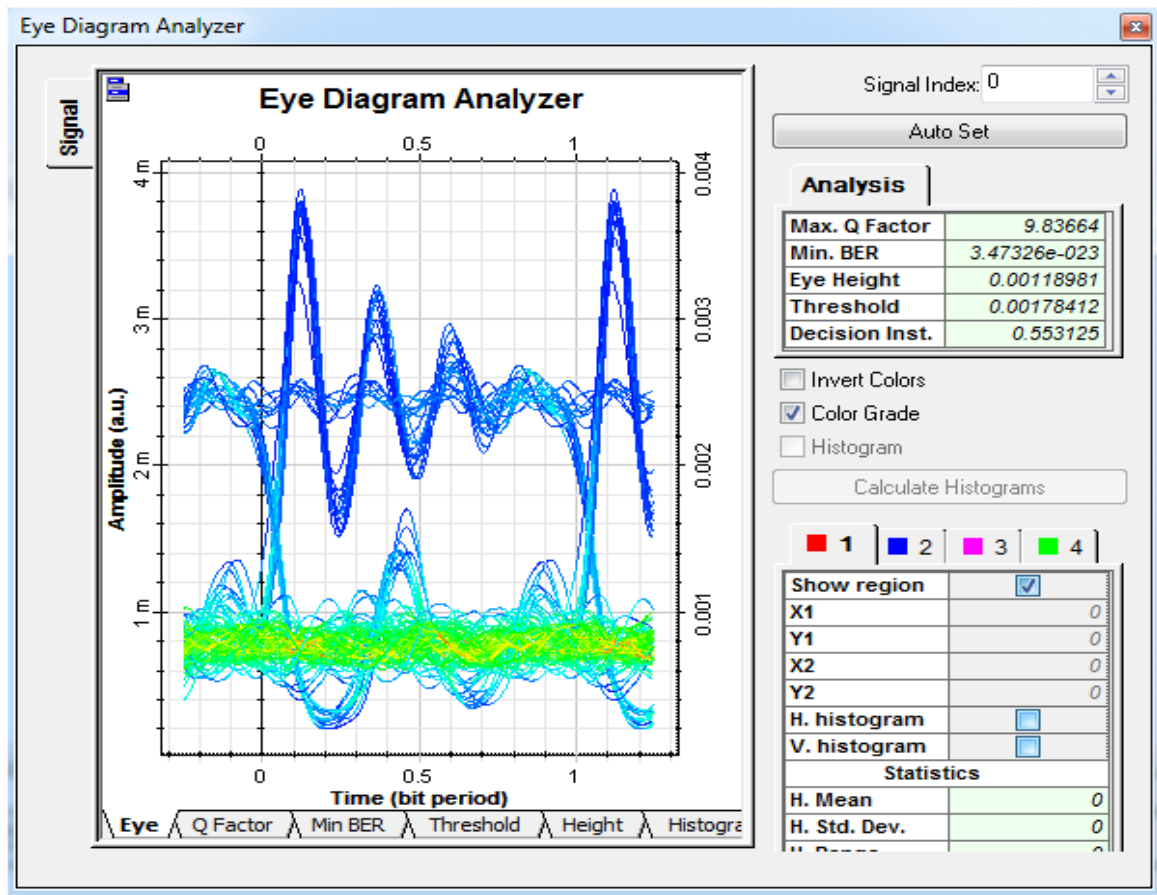


Figure 3.34 Diagramme de l'œil pour une chaîne avec un atténuateur.

D'après figure 3.34 nous remarquons que le facteur de qualité est de 9.83 qui est supérieur à 6 et le TEB est de $3.47 \cdot 10^{-23}$ qui est inférieur à 10^{-12} .

➤ Simulation d'un système WDM-QKD

• Liaison WDM 2*1 Gbps

Dans cette partie nous utiliserons deux diodes laser spatiales espacées de 100 GHz pour une liaison de 2 Gbps comme c'est représenté dans la figure 3.35.

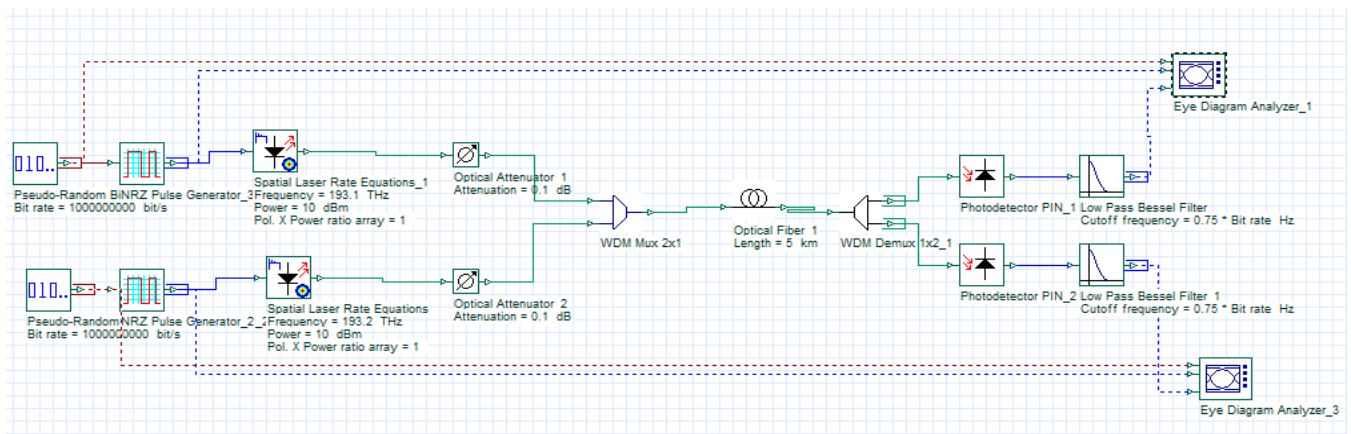


Figure 3.35 Intégration d'un système QKD dans une liaison WDM 2*1 Gbps.

Nous avons obtenu un diagrammes d’œil ouvert comme montré dans la figure 3.36 avec un facteur de qualité supérieur à 6 et un taux d’erreur inférieur à 10^{-12} pour les 2 canaux comme c’est représenté dans le tableau 3.5.

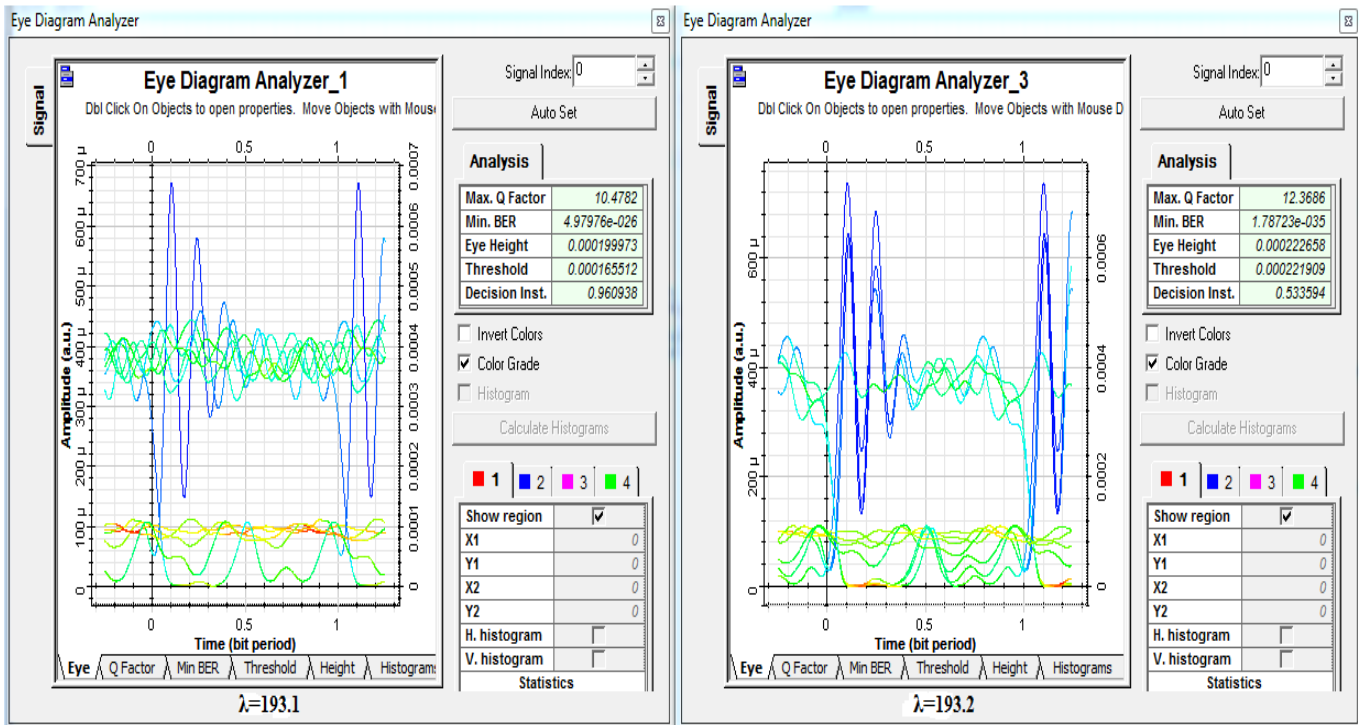


Figure 3.36 le diagramme de l’œil pour un system QKD intégré sur une liaison WDM 2*1 Gbps.

Fréquences	Facteur de qualité (Q)	Taux d’erreur (TEB)
193.1	10.47	$4.97 \cdot 10^{-26}$
193.2	12.36	$1.78 \cdot 10^{-35}$

Tableau 3.5 Le facteur de qualité et le taux d’erreur pour un system QKD intégré sur une liaison WDM 2*1 Gbps

- **Liaison WDM 4*1 Gbps**

Dans cette partie, nous utiliserons 4 diodes laser spatiales espacé de 100Ghz en vue de transmettre un débit de 4 Gbps sur une longueur de fibre de 5 km, comme c’est montré dans la figure 3.37

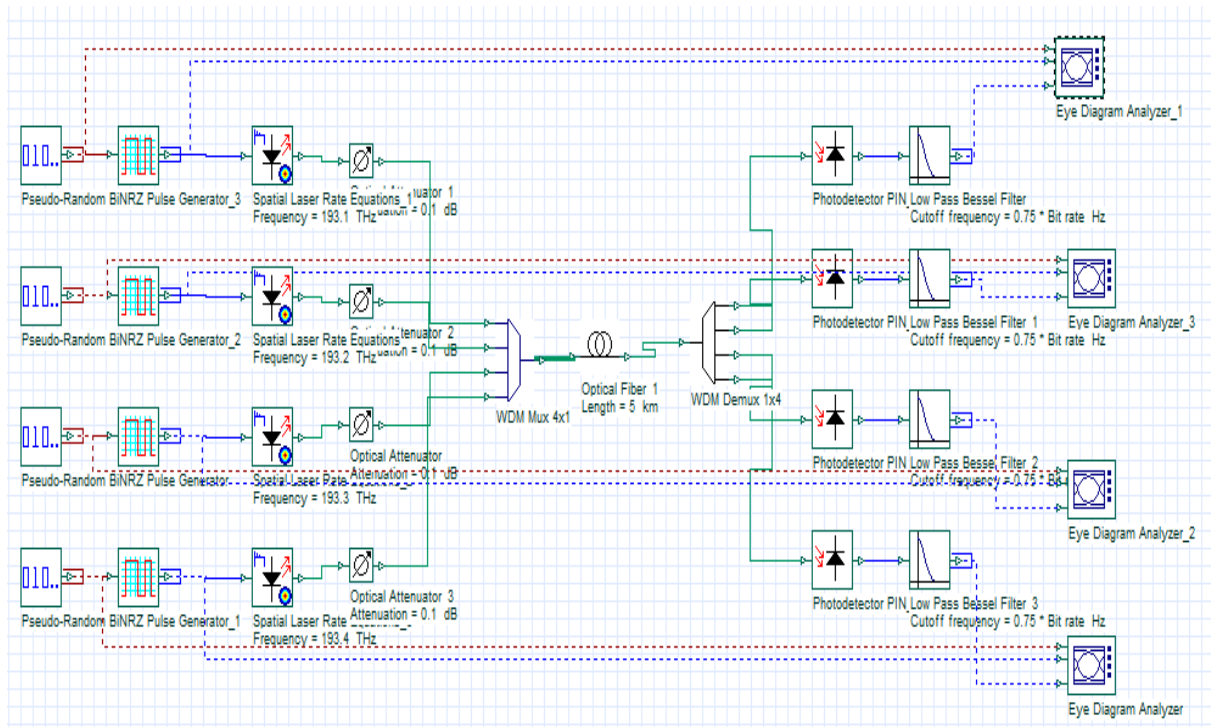


Figure 3.37 Intégration d'un system QKD dans une liaison WDM 4*1 Gbps.

Nous avons obtenu un diagramme d'œil ouvert comme montré dans la figure 3.38 avec un facteur de qualité supérieur à 6 et un taux d'erreur inférieur à 10^{-12} pour les 4 canaux comme c'est représenté dans le tableau 3.6.

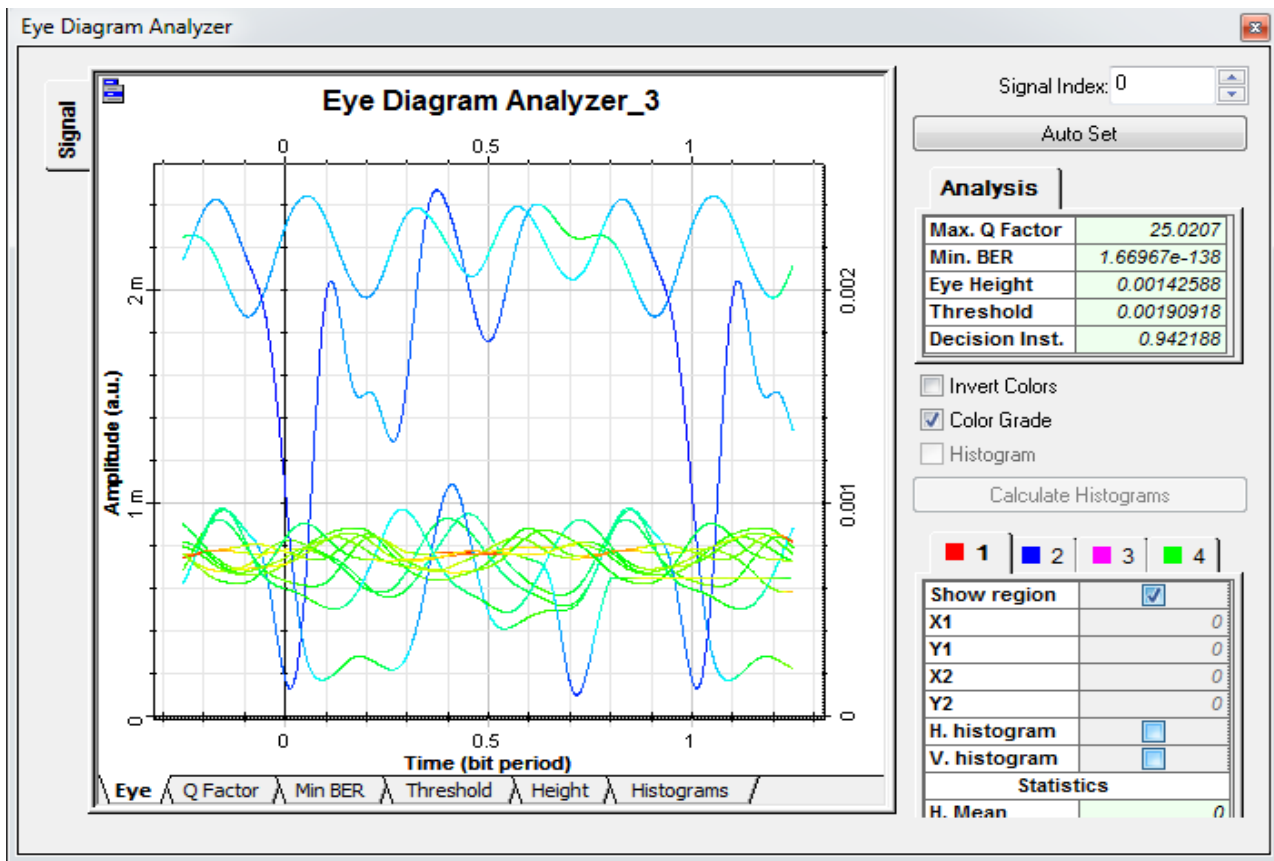


Figure 3.38 diagramme de l'œil pour un system QKD intégré sur une liaison WDM 4*1 Gbps.

Fréquences	Facteur de qualité (Q)	Taux d'erreur (TEB)
193.1	15.27	$5.19 \cdot 10^{-53}$
193.2	25.02	$1.66 \cdot 10^{-138}$
193.3	16.72	$4.21 \cdot 10^{-63}$
193.4	13.03	$3.44 \cdot 10^{-39}$

Tableau 3.6 Le facteur de qualité et le taux d'erreur pour un system QKD intégré sur une liaison WDM 4*1 Gbps

Cette simulation a prouvé la possibilité d'intégrer un system QKD sur une liaison WDM et d'avoir un débit plus élevées avec une bonne qualité de transmission.

3.6 Conclusion

Dans ce chapitre nous avons vu l'importance des liaisons de transmission optique WDM dans la transmission de données à haut débit. Dans la première partie nous avons présenté la spécificité de ces liaisons qui réside dans la possibilité d'envoyer différents types de données sur des réseaux de fibres optiques sous forme de lumière grâce à des sources optiques tel que les diodes lasers. Ainsi, différents canaux de lumière, chacun avec une longueur d'onde spécifique sont envoyés simultanément sur une seule fibre optique. Nous avons précédé la deuxième partie par les différents composants nécessaires pour une liaison optique, ensuite nous avons simulé une chaîne de transmission de base avec et sans filtre qui nous a permis de discerner son efficacité à éliminer le bruit. Dans la partie suivante, nous avons effectué notre simulation en agissant sur la variation du débit afin de voir l'importance de la modulation externe dans la transmission de haut débits en évaluant la qualité de transmission. Par la suite nous avons conçu une liaison WDM à 46 Gbps permettant la communication simultanée de 8 utilisateurs avec une bonne qualité de transmission. La dernière partie de ce chapitre était consacré pour les applications du WDM dans la distribution quantique de clé, d'où le système WDM-QKD est une approche intéressante qui offre une meilleure sécurité avec un débit important.

Conclusion générale

Conclusion générale

Dans ce mémoire de fin d'étude ; nous avons tout d'abord introduit le concept de base de la cryptographie quantique qui permet de dissimiler les données confidentiel en masquant son contenu afin de ne la rendre accessible qu'au personne autorisé et cela par l'utilisation de photons guidés dans la fibre optique, nous avons ensuite vu la possibilité d'utiliser le multiplexage en longueur d'onde WDM dans le but d'élaborer un réseau optique permettant de transmettre simultanément plusieurs canaux sur une même fibre.

Le premier chapitre était consacré pour la description de la cryptographie et les méthodes de cryptage les plus connue à savoir la cryptographie classique qui concerne la période de l'antiquité précédant les ordinateurs, et la cryptographie moderne qui est essentiellement basé sur les mathématiques. On distingue deux classes : chiffrement symétrique qui utilise une seule clé pour le chiffrement et déchiffrement et le chiffrement asymétrique qui utilise une paire de clé : une clé publique pour le chiffrement et une clé privé pour le déchiffrement, et en dernier lieu la cryptographie quantique basée sur les propriétés quantiques des photons polarisés qui permet de partager des clés en toute sécurité.

Dans le deuxième chapitre nous avons vu qu'avec la distribution quantique de clé y'a plus de sécurité avec l'utilisation de sources émettant un seul photon. Cela est possible grâce aux principes de la mécanique quantique : le théorème de non-clonage et de l'incertitude d'Heisenberg qui assurent la détection de tout espionnage et d'empêcher toute tentative d'intrusion. Puis, nous avons cité les protocoles de distributions à savoir le protocole BB84 qui offre un canal de transmission inviolable, l'impossibilité de clonage et surtout un moyen efficace pour la détection d'intrusion. Nous avons pu décrire l'application des sources à photon unique dans la mise en œuvre d'une distribution quantique de clé en utilisant le protocole BB84, grâce au logiciel OPTISYSTEM. Les résultats de notre simulation ont montré la possibilité d'envoyer une clé de cryptage en toute sécurité et d'établir un secret commun entre deux utilisateurs, et on a pu déduire que la réalisation d'une expérience de cryptographie est très intéressante pour assurer une transmission de données sécurisées.

Pour le troisième chapitre, nous avons décrit les principes de base de la transmission par fibre optique et nous avons présenté les liaisons optiques WDM qui permettent d'exploiter la bande passante de la fibre optique, pour atteindre des très hauts débits. Nous avons mis en œuvre un système WDM 8x6 Gbit/s. Cette étude prouve que les performances du taux d'erreur binaire BER et le facteur de Q sont les indicateurs clés permettant de suivre la qualité

Conclusion générale

du réseau et déterminer toute dégradation pouvant affecter la qualité de service et que l'utilisation d'un filtre assure l'élimination du bruit, ainsi que l'intégration d'un modulateur externe permet d'avoir des débits élevés.

L'objectif principale de ce travail était d'étudier les liaisons WDM, leurs performances ainsi l'intérêt qu'elle apporte pour établir une bonne communication. Nous concluons que cette étude montre la possibilité d'intégrer un système QKD dans une liaison WDM c'est à dire pouvoir distribuer des clés secrètes à plusieurs utilisateurs simultanément en utilisant une seule fibre, et c'est dans le but d'avoir des débit plus importants et une meilleure sécurité.

En perspectives, il serait intéressant d'étudier l'effet de la distance, du débit et de l'atténuation sur un système WDM-QKD. Par ailleurs, l'association d'un amplificateur optique (EDFA,...) apportera une nouveauté dans les systèmes WDM-QKD.

Références bibliographiques

- [1] RAMM-0000. Introduction à la cryptographie : <https://ram0000.developpez.com/Tutoriels/cryptographie/>,2009.
- [2] Rezkallah, L. Cryptographie classique à la cryptographie moderne théorie et application. Mémoire de fin d'étude, Université Houari Boumediene,2007.
- [3] (s.d.). Récupéré sur <https://fr.wikipedia.org/wiki/Wikip%C3%A9dia>.
- [4] Alléaume, R. Réalisation expérimentale de sources de photons uniques, caractérisation et application à la cryptographie quantique. Thèses de doctorat, Université Pierre et Marie Curie - ParisVI, Paris,novembre 2004.
- [5] Benammar, A & Miloudi, W. Etude d'une liaison optique WDM Radio sur Fibre. Mémoire de fin d'étude, Université Aboubakr Belkaïd, Tlemcen,12 juin 2017.
- [6] Atatama, E. B. Les différents principes de transmission des données par fibre optique : https://www.memoireonline.com/09/13/7350/m_Les-differents-principes-de-transmission-des-donnees-par-fibre-optique19.html,2011.
- [7] Beauquier, B. Communications dans les réseaux optiques par multiplexage en longueur d'onde. Thèses de doctorat, Université de NICE-SOPHIA ANTIPOLIS, Nice,17janvier 2000.
- [8] Katia, B &Ghania, D. Simulation d'une liaison haut débit par fibre optique sur logiciel COMSIS.Mémoire de fin d'étude, Université Mouloud Mammeri, Tizi ousou,2012.
- [9] MOKRETAR, M. A & NOURA., N. Étude et Conception d'un Système de Transmission Optique en Utilisant la Technologie WDM 4 x 20 Gbit/s. Mémoire de fin d'étude, Université Hassiba Benbouali,Chlef,juin 2019.
- [10] François, M. L. Étude de technologies avancées pour l'optimisation des systèmes de transmission optique multiplexés en longueur d'onde au débit de 40 Gbit. Thèse de doctorat, Université Paris Sud - Paris XI, Paris,2007.
- [11] MOKRETAR, M. A & NOURA, N. Étude et Conception d'un Système de Transmission Optique en Utilisant la Technologie WDM 4 x 20 Gbit/s. MEMOIRE DE MASTER , UNIVERSITE HASSIBA BENBOUALI , CHLEF,2019.
- [12] Semghouni, Y, & Deghab Mokhtaria, W. (2019). Caractérisation et simulation fréquentielle de la liaison RoF. MEMOIRE DE FIN D'ETUDES, UNIVERSITE Dr. TAHAR MOULAY, SAIDA.
- [13] ARRIBI, M., & ELMAHI, A. La technique WDM en télécoms optiques avancées. Mémoire de fin d'étude, UNIVERSITÉ MUSTAPHA STAMBOUL, MASCARA,2016.

Résumé

Ce mémoire porte principalement sur l'étude de la distribution quantique de clé dans les liaisons WDM. La problématique générale est la suivante : il s'agit de pouvoir distribuer des clés secrètes à plusieurs utilisateurs d'une manière simultanée sur une liaison WDM. L'objectif est d'intégrer le système QKD dans l'infrastructure existante du réseau WDM afin d'avoir des débits élevés et une grande sécurité.

Dans le premier chapitre nous présentons un aperçu sur l'évolution de la cryptographie ainsi que les méthodes de cryptage les plus connues en passant de la cryptographie classique jusqu'à la cryptographie quantique. Dans le deuxième chapitre nous décrivons les protocoles de la QKD les plus fonctionnelles basant sur les lois de la mécanique quantique. Dans le troisième chapitre nous décrivons les liaisons WDM et leurs applications dans la QKD, ainsi qu'une synthèse des résultats obtenus dans la simulation d'une liaison optique WDM 8*6 Gbps et ses performances. La dernière partie est consacré pour la simulation d'un système WDM-QKD ce qui confirme la possibilité d'intégrer des systèmes QKD dans l'infrastructure existante de ces liaisons.

Abstract

This dissertation focuses on the study of quantum key distribution in WDM links. The general problem is as follows: it is a matter of being able to distribute secret keys to several users simultaneously on a WDM link. The goal is to integrate the QKD system into the existing infrastructure of the WDM network to have high throughput and security.

In the first chapter we present an overview on the evolution of cryptography as well as the most famous encryption methods from classical cryptography to quantum cryptography. In the second chapter we describe the most functional QKD protocols based on the laws of quantum mechanics. In the third chapter we describe WDM links and their applications in QKD, as well as a synthesis of the results obtained in the simulation of an 8 * 6 Gbps WDM optical link and its performance. The last part is devoted to the simulation of a WDM-QKD system which confirms the possibility of integrating QKD systems into the existing infrastructure of these links.