République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieure et de la Recherche Scientifique

Université Abderrahmane Mira

Faculté de la Technologie

Département d'Automatique, Télécommunication et d'Electronique

Projet de Fin d'Etudes

Pour l'obtention du diplôme de Master

Filière : Télécommunication

Spécialité : Réseaux et télécommunication

Thème

Etude comparative des protocoles de distribution quantique de clé BB84 et B92.

Préparé par :

Mlle HAMATA Samia

Mlle IFFIS Kenza

Dirigé par :

*M*r BERRAH Smail

Examiné par :

*M*me OUALI

*M*r KHIREDINE A. karim

Année universitaire : **2021/2022**

Remerciements :

Avant tout, nous tenons à remercier le Seigneur Dieu tout puissant Qui nous a donné durant toutes ces années la santé, la force Et le courage, la volonté pour la réalisation de ce mémoire.

Nous ne saurions, réellement, trouver les expressions éloquentes que méritent notre encadreur le professeur **Mr BERRAH Smail** *qui nous a proposé le thème de ce mémoire et pour la confiance qu'il nous a accordée, ses orientations, ses encouragements et ses précieux conseils, ses remarques judicieuses et sa disponibilité, encouragements, aides, leur sympathie, nous tenons à lui exprimer notre profonde graduation en vue du bon déroulement du travail et leur présence totale durant l'élaboration de ce mémoire.*

Nous tenons aussi à remercier le président et les membres de jury : **Mme Ouali, M Khiredine** *d'avoir accepté d'évaluer et d'examiner notre travail.*

Nos remerciements vont également à tous les enseignants qui ont participé à ma formation.

Pour finir, nous tenons à remercier nos familles et nos amis qui nous ont soutenus et toute personne qui nous a aidés de près ou de loin à concrétiser ce travail.

Dédicace :

Je dédie ce modeste travail à :

La femme qui m'a enfanté, celle qui a sacrifié tout pour moi :

Son temps, son bonheur, sa santé : ma mère 'Dalila' noyaux de mon esprit,

Amon père 'Djamel', source d'énergie pour ma réussite,

Ecole de mon éducation et principe de la vie,

Que dieu les préserves pour moi,

A mon chère frère Fayçal : tu m'as toujours encouragé et soutenu,

Ames adorables sœurs Sabrina, Massouda et Lydia,

A mon cher binôme Kenza,

A toutes ma famille,

A tous ceux qui me sont chères,

A tous ceux qui m'aiment,

A tous ceux que j'aime.

Aucune dédicace ne saurait exprimer Mes respects,

Mes considérations et Mes grandes admirations.

Merci de m'avoir toujours soutenu et d'avoir cru en moi.

Je dédie ce travail…

Samia

Dédicace :

Je dédie ce modeste travail à :

La femme qui m'a enfanté, celle qui a sacrifié tout pour moi :

Son temps, son bonheur, sa santé : ma mère 'Meriama' noyaux de mon esprit,

Amon père 'Mouloud', source d'énergie pour ma réussite,

Ecole de mon éducation et principe de la vie,

Que dieu les préserves pour moi,

A mes chères frères Khaled et Saddik : vous m'as toujours encouragés et soutenus,

Ames adorables sœurs Nassima et Sarah,

A mon cher binôme Samia,

A toutes ma famille,

A tous ceux qui me sont chères,

A tous ceux qui m'aiment,

A tous ceux que j'aime.

Aucune dédicace ne saurait exprimer Mes respects,

Mes considérations et Mes grandes admirations.

Merci de m'avoir toujours soutenu et d'avoir cru en moi.

Je dédie ce travail…

Kenza

Sommaire :

Remerciements

Dédicace

Sommaire

Liste d'abréviation

Liste des tableaux

Liste des figures

Introduction Générale ……2

Cadre théorique

<u>Chapitre I :</u>

Rappel sur la cryptographie

Introduction ……..……5

1. Cryptologie……5

1.1. Cryptanalyse……..5

1.2. Cryptographie……..6

2. Terminologie ……6

3. *Les principaux objectifs de la cryptographie……..……6*

4. Les méthodes de chiffrements……..7

4.1 Le chiffrement classique…….. 7

4.1.1 Chiffrement par substitution……8

4.1.2 Chiffrement par transposition (permutation)……..8

4.2 Le chiffrement moderne……8

4.2.1 Chiffrement symétrique……9

4.2.2 Chiffrement asymétrique…….. 10

5. Comparaison entre les chiffrements symétriques et asymétriques.....14

6. Les limites de la cryptographie classique et moderne…….. 15

7. L'ordinateur quantique……15

Conclusion……..……16

Chapitre II :

Cryptographie quantique

*Introduction……..…….....**18***

1. Notion de base de la cryptographie quantique…….... 18

1.2. Les principes fondamentaux de la mécanique quantique……19

1. Principe d'incertitude de Heisenberg……..19

2. Théorème de non Clonage…….... 19

2. Quelques propriétés de l'information quantique…… ….. 19

1. Qubit ……..19

2. Photon ……..20

3. Cryptographie quantique par photons uniques……22

3.1. Sources de photon unique ……..22

3.2 Sources lasers atténués ……..22

4. Principe de la cryptographie quantique……23

4.1. Le canal quantique……23

4.2 Le canal classique……23

5. Etapes de la création de clés quantique……..23

5.1 Communication quantique…….23

5.2 Phase de tamisage…… 24

5.3 Phase d'estimation d'erreur……24

5.4 Correction d'erreur…… 25

6. Quelques types de protocole de distribution à clé quantique.....26

6.1 Le protocole BB84…….. 26

A. Déroulement du protocole BB84 ……27

6.2 Le protocole B92……30

A. Déroulement du protocole B92 ……31

*Conclusion……..**33***

Chapitre III :

Etude des performances du protocole BB84 et B92 dans une liaison optique

Introduction……35

Partie théorique : Généralité sur la fibre optique.

1. Structure générale d'une liaison par fibre optique……35

2. La fibre optique……36

3. Les composants d'un câble de fibre optique……36

4 Différents types de fibres optiques……36

4.1 La fibre monomode……36

4.2 La fibre multi-mode…… 37

5. Propriétés de la fibre optique……37

6 .Les critères de qualités d'une transmission optique……38

6.1 Taux d'erreur binaire……39

6.2 Facteur de qualité (Q)……39

Partie pratique : Simulation sur logiciel Optisystem.

7. Présentation de logiciel…… 39

8. Chaine de transmission optique de base……43

8.1 Simulation de la chaine de base……43

9. Etude de la qualité de transmission du protocole BB84 dans une liaison optique…… 44

9.1. L'influence des variations de la distance de propagation sur la transmission…… 45

9.2. L'influence des variations de la longueur d'onde sur la transmission……48

9.3. Effet d'un l'espion sur la transmission ……49

9.3.1. Influence de la distance en présence de l'espion……53

9.3.2. L'influence de la longueur d'onde sur la transmission en présence d'espion…… 56

10. Etude de l'effet du protocole B92 sur une liaison optique……58

10.1. L'influence de la distance de propagation sur la transmission……60

10.2. L'influence de la longueur d'onde sur la transmission…… 63

10.3. L'effet d'un espion sur la transmission ……64

10.3.1. Influence de la distance en présence de l'espion……66

10.3.2. Influence de la longueur d'onde en présence de l'espion……69

11. Comparaison entre le protocole BB84 et B92……70

Conclusion……73

Conclusion Générale……..75

Bibliographies……78

Web graphie……...…80

Résumé

Liste d'abréviation :

A : *Anti-diagonal.*

AES: *Advanced Encryptions Standard.*

Alice: *pour désigner l'émetteur du message.*

BB84: *Charles Bennett et Gilles Brassard 1984.*

B92: *Bennett 1992.*

BER: *Bit-Error Rate.*

Bob: *pour désigner le récepteur du message.*

D: *Diagonal.*

DES: *Data Encryptions Standard.*

Eve: *Eavesdropper.*

H: *Horizontal.*

IBM: *International business Machines.*

NIST: *National Institute of Standard and Technology.*

NRZ: ***Non****-Return to Zero.*

PIA *: Programme d'Investissement d'Avenir.*

Q: *facteur de qualité.*

QKD: *Quantum Key Distribution.*

Qubit: *Quantum + bit.*

RSA: *Ron Rivest, Adi Shamir, ET Leonard Adleman.*

SOHO: *Simple Office, Home Office.*

TEB: *Taux d'Erreur Binaire.*

V: *Vertical.*

WPA-PSK: Wi-Fi personnel Access -Pre-Shared Key.

Liste des tableaux :

Tableau I.1: *exemple de chiffrement par substitution……8*

Tableau I.2: *exemple de chiffrement par permutation……8*

Tableau I.3: *Chiffrement RSA……13*

Tableau I.4: *Déchiffrement RSA……14*

Tableau I.5: *Résultat d'algorithme RSA……14*

Tableau I.6: *Comparaison entre les méthodes de chiffrement symétriques et asymétriques...14*

Tableau II.1 : *Etat de polarisation associée à chaque Qubit de protocole BB84……27*

Tableau II.2: *une séquence binaire sans espion du protocole BB84……28*

Tableau II.3: *une séquence binaire avec espion du protocole BB84……30*

Tableau II.4: *Etat de polarisation associée à chaque Qubit de protocole B92……31*

Tableau II.5: *une séquence binaire sans espion du protocole B92……31*

Tableau II.6 : *une séquence binaire avec espion du protocole B92……32*

Tableau III .1 : *Les résultats du taux d'erreur et du facteur de qualité d'une chaine de base……43*

Tableau III .2: *Les résultats du taux d'erreur et du facteur de qualité d'une chaine avec BB84……45*

Tableau III.3 : *Résultats de BER et facteur de qualité en fonction de la distance……46*

Tableau III.4 : *Résultats de BER et facteur de qualité en fonction de la longueur d'onde….48*

Tableau III.5 : *Les résultats du BER et facteur de qualité dans une chaine optique avec le protocole BB84 en présence d'espion ……52*

Tableau III.6 : *Les résultats du BER et facteur de qualité en fonction de la distance avec espion……53*

Tableau III.7 : *Les résultats du BER et facteur de qualité en fonction de la longueur d'onde avec espion……56*

Tableau III .8: *Les résultats du taux d'erreur et du facteur de qualité d'une chaine avec B92……59*

Tableau III.9 : *Résultats de BER et facteur de qualité en fonction de la distance……61*

Tableau III.10 : *Résultats de BER et facteur de qualité en fonction de la longueur d'onde...63*

Tableau III.11 : *Les résultats du BER et facteur de qualité dans une chaine optique avec B92 en présence d'espion……65*

Tableau III.12 : *Les résultats du BER et facteur de qualité en fonction de la distance avec espion……67*

Tableau III.13 : *Les résultats du BER et facteur de qualité en fonction de la longueur d'onde avec espion……69*

Tableau III.14 : *Comparaison entre BB84 et B92……72*

Liste des figures :

Figure I.1: *Principe de la cryptologie……5*

Figure I.2: *Modèle simple de la cryptographie……6*

Figure I.3: *système de chiffrement……7*

Figure I.4: *Prince de chiffrement symétrique……9*

Figure I.5: *Prince de chiffrement asymétrique……11*

Figure II.1: *Les types de polarisations……21*

Figure II.2: *Polarisation du photon……21*

Figure II. 3: *Source Laser atténué……22*

Figure II.4: *Les systèmes de communication quantique……23*

Figure II.5: *transmission quantique……24*

Figure II.6: *Phase de tamisage……24*

Figure II.7: *Phase d'estimation d'erreur……25*

Figure II.8: *Phase de correction d'erreur……26*

Figure II.9: *Les bases de polarisation de protocole BB84……27*

Figure II.10: *Principe de protocole BB84……28*

Figure II.11: *Principe de protocole BB84 en présence d'espion……29*

Figure II.12: *Les bases de polarisation de protocole B92……30*

Figure II.13: *Principe de protocole B92……31*

Figure III.1: *le principe de base d'une transmission de données par une fibre optique……35*

Figure III.2: *schéma d'un câble à fibre optique……36*

Figure III.3: *Fibre monomode……37*

Figure III.4: *Fibre multimode……37*

Figure III.5: *Phénomène d'atténuation dans une fibre optique……38*

Figure III.6: *La dispersion d'une fibre optique……38*

Figure III.7: *Modèle de simulation d'un générateur de séquence binaire……40*

Figure III.8: *Modèle de simulation d'un générateur NRZ……40*

Figure III.9: *Modèle de simulation de la diode laser……41*

Figure III.10: *Modèle de simulation d'une photodiode PIN……41*

Figure III.11: *Modèle de simulation filtre passe bas Bessel……41*

Figure III.12: *Modèle de simulation d'un analyseur de BER……41*

Figure III.13: *Modèle de simulation d'une fibre optique……42*

Figure III.14: *Modèle de simulation d'un atténuateur optique……42*

Figure III.15: *Modèle de simulation d'un polariseur linéaire……..…..42*

Figure III.16: *Modèle de simulation d'un select……43*

Figure III.17: *Synoptique d'une chaine de transmission de base……43*

Figure III.18: *Synoptique d'une chaine de transmission avec le protocole BB84……44*

Figure III.19: *Diagramme de l'œil pour une distance de 17Km……45*

Figure III.20: *Taux d'erreur en fonction de la distance……46*

Figure III.21: *facteur de qualité en fonction de la distance……47*

Figure III.22: *Diagramme de l'œil pour une distance de 50Km……47*

Figure III.23:*Taux d'erreur binaire en fonction de la longueur d'onde……48*

Figure III.24: *Facteur de qualité en fonction de la longueur d'onde……49*

Figure III.25: *Synoptique d'une chaine de transmission avec le protocole BB84 en présence d'espion……51*

Figure III.26: *Diagramme d'œil pour une distance 17 Km en présence d'espion……52*

Figure III.27: *Taux d'erreur en fonction de la distance en présence d'espion……53*

Figure III.28: *facteur de qualité en fonction de la distance en présence d'espion……54*

Figure III.29: Diagramme de l'œil pour une distance de 50Km avec attaque……54

Figure III.30: *Taux D'erreur en fonction de la distance en présence et en absence d'espion……55*

Figure III.31: *Facteur de qualité en fonction de la distance en présence et en absence d'espion……55*

Figure II.32: *Taux d'erreur en fonction de la longueur d'onde en présence d'espion……56*

Figure III.33: *facteur de qualité en fonction de la longueur d'onde en présence d'espion….57*

Figure III.34: *Taux d'erreur en fonction de la longueur d'onde en présence d'espion et en absence d'espion……57*

Figure III.35: *Facteur de qualité en fonction de la longueur d'onde en présence et en absence d'espion……58*

Figure III.36: *Synoptique d'une chaine de transmission avec le protocole B92……59*

Figure III.37: *Diagramme de l'œil pour une distance de 17Km……60*

Figure III.38: *Taux d'erreur en fonction de la distance……61*

Figure III.39: *Facteur de qualité en fonction de la distance……62*

Figure III.40: *Diagramme de l'œil pour une distance de 50Km……62*

Figure III.41: *Taux d'erreur binaire en fonction de la longueur d'onde……63*

Figure III.42: *Facteur de qualité en fonction de la longueur d'onde……..64*

Figure III.43: *Synoptique d'une chaine de transmission avec le protocole B92 en présence d'espion……..65*

Figure III.44: *Diagramme de l'œil pour une distance de 17Km en présence d'espion…….66*

Figure III.45: *Diagramme de l'œil pour une distance de 50Km avec espion……67*

Figure III.46: *Taux d'erreur en fonction de la distance avec et sans espion……..68*

Figure III.47: *Facteur de qualité en fonction de la distance avec et sans espion……68*

Figure III.48: *Taux d'erreur en fonction de la longueur d'onde avec et sans espion……69*

Figure III.49: *Facteur de qualité en fonction de la longueur d'onde avec et sans espion…..70*

Figure III.50: *taux d'erreur en fonction de la distance sans espion avec BB84 et B92……71*

Figure III.51: *facteur de qualité en fonction de la longueur d'onde en présence d'espion avec BB84 et B92……..71*

Introduction Générale

Introduction générale :

L'homme a toujours ressenti le besoin de dissimuler les informations échangées avec d'autres, bien avant même l'apparition des premiers ordinateurs.

La mondialisation a entrainé beaucoup de changements dans la vie de l'être humain, en effet, l'évolution rapide des systèmes de télécommunication notamment de l'internet a beaucoup facilité la vie des individus, et a permet l'interconnexion de toutes les entreprises via le réseau étendu. Cependant, le risque des attaques et des intrusions mettent en danger les stratégiques liées aux activités des entreprises sur le web. Les transactions faites à travers les réseaux peuvent être interceptés, il faut donc garantir la sécurité de ces informations.

Ce défi se retrouve dans des domaines variés tels que : la protection des données confidentielles (bases de données, Email, ...), la sécurisation des communications, le paiement sécurisé (cartes bancaires), sécurité militaire, commerce électronique.

Ce dernier appelé également le E-commerce constitue aujourd'hui la colonne vertébrale de l'économie mondiales, la fédération e-commerce et vente à distance (Fevad) a publié l'édition 2021 de son rapport annuel sur l'état du marché du e-commerce qui a atteint 112.2 milliard d'euros [1]. L'Algérie a enregistrée 11.200 milliard de dinars pour 7.8 millions opérations de paiement via internet [2], tous ces flux d'échange nécessitent des techniques de cryptage efficaces.

La cryptographie est la science du secret, est un ensemble de techniques permettant de chiffrer des messages. Actuellement, ces techniques se classent en deux grandes familles en se basant sur le nombre de clés de cryptage utilisé, il s'agit de cryptographie symétrique (DES, AES) et asymétriques tels que : RSA.

Au début, la cryptographie était essentiellement reposée sur des lettres et des caractères, puis elle était orientée vers l'utilisation de l'arithmétique qui sert à transformer un texte en une succession de bit dans le cas de l'informatique, c'est la cryptographie moderne.

L'algorithme cryptographique le plus utilisé est le RSA qui est nécessaire par exemple dans la sécurisation des comptes bancaires. Cet algorithme utilise des codes mathématiques de plus en plus complexes avec des clefs publiques de plus en plus longues. Avec l'avènement possible de l'ordinateur quantique, les algorithmes classiques ne seront

plus efficaces donc il serait indispensable d'introduire de nouvelles techniques de cryptage qui conviennent à cette technologie.

La cryptographie quantique est basée sur des concepts de la physique quantique et de la théorie de l'information où elle montre comment les photons peuvent être utilisés pour transmettre de l'information. Ce type de cryptographie est en cours de développement, à titre d'exemple, la France a consacré un budget énorme de 1,8 milliard d'euros via le programme d'investissements d'Avenir (PIA) au développement des technologies quantiques sur la période 2021-2025 [3].

L'objectif de notre travail est l'étude des performances des deux protocoles essentiels le BB84 et le B92 sur une liaison optique, l'étude sera faite en présence et en absence d'espion.

Ce mémoire est organisé en trois chapitres :

Le premier chapitre présente quelques généralités sur la cryptographie, ensuite les méthodes de chiffrement classique et moderne. À la fin nous intéresserons aux limites de ces dernières qui nous mènent à une nouvelle approche nommé « cryptographie quantique ».

Le deuxième chapitre présente les principes de la théorie de l'information et la mécanique quantique qui sont la base de la cryptographie quantique. Ensuite, nous aborderons les deux protocoles BB84 et B92 avec leurs principes et leurs déroulements en présence et en absence d'espion.

Le troisième chapitre portera en première partie quelques généralités sur la fibre optique, ensuite une partie sur la simulation d'une chaine de transmission avec le protocole BB84 et le protocole B92 sur Optisystem, afin d'étudier la qualité de transmissions de ces derniers. À la fin nous nous effectuerons une comparaison entre les deux protocoles.

Ce mémoire est clôturé par une conclusion et des perspectives.

Chapitre I :

Rappel sur la cryptographie

Introduction :

La cryptographie est utilisée depuis des milliers d'années pour assurer les communications militaires et diplomatiques, afin de protéger les informations échangées. Elle permet de chiffrer des messages, il existe plusieurs systèmes : classique, moderne…

Dans ce chapitre, nous allons présenter quelques généralités sur la cryptographie et ses objectifs, et nous nous mettrons l'accent sur les différents algorithmes classiques et modernes existants, à la fin nous nous aborderons quelques notions de l'ordinateur quantique.

I.1 La cryptologie :

Le mot « cryptologie » vient du mot grec « cryptos » qui veut dire « secret » et du mot « logie » qui signifie « science ». Étymologiquement, « La science de secret » est une science mathématique plus élargie qui comporte deux branches : la cryptographie et la cryptanalyse.

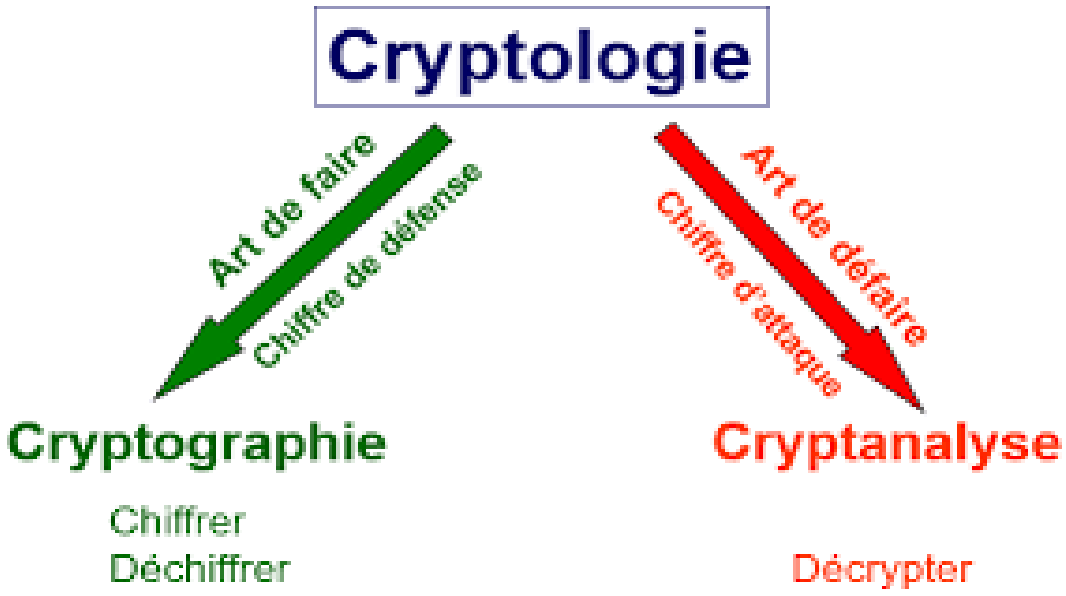

Figure I.1 : Principe de la cryptologie.

I.1.1 La cryptanalyse :

La cryptanalyse est l'art de casser des algorithmes de chiffrement dans le but de trouver des faiblesses et pouvoir décrypter des messages chiffrés sans connaitre la clé de déchiffrement [4].

I.1.2 La cryptographie :

La cryptographie est un terme générique désignant l'ensemble des règles permettant de crypter et chiffrer des messages, afin de protéger les données sensibles (c'est-à-dire les rendre non compréhensibles) lors de leur transmission qui permet de transmettre les données de manière confidentielle.

I.2. Terminologie :

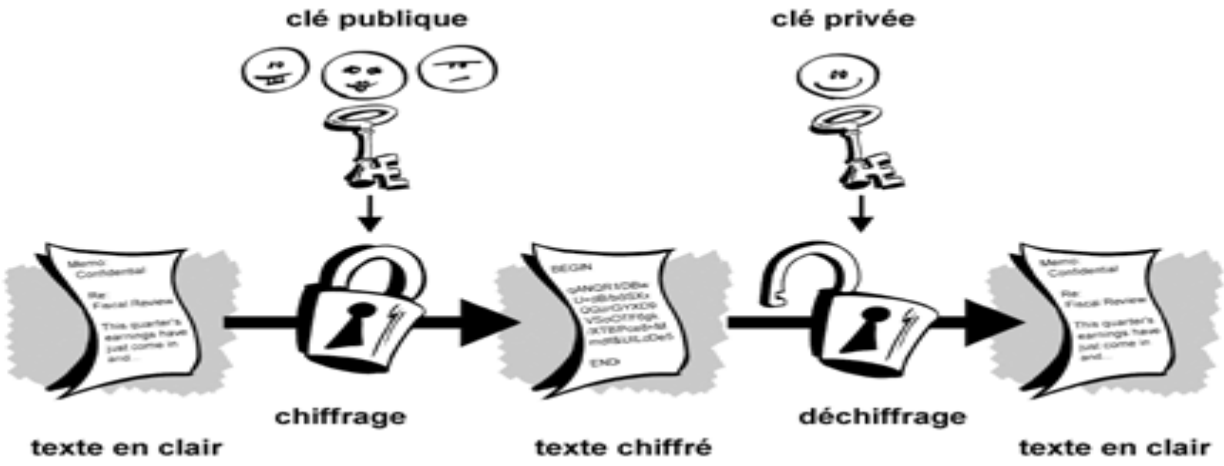

Figure I.2 : Modèle simple de la cryptographie.

- ***Texte en clair* :** est le message à envoyer.
- ***Texte chiffré* :** résultat de chiffrement.
- ***Chiffrement* :** le processus de transformation du texte clair au texte chiffré.
- ***Déchiffrement* :** l'opération inverse de chiffrement qui permet de transformer le texte chiffré en texte clair.
- ***Clef* :** c'est un paramètre implique et autorise des opérations de chiffrement et/ou déchiffrement, Il existe : clé publique et clé privé [5].
- ***Algorithme* :** présente les fonctions mathématiques utilisées pour le chiffrement et le déchiffrement.

I.3. *Les principaux objectifs de la cryptographie :*

L'objectif de la cryptographie est de protéger des messages. Principalement, il s'agit de les rendre incompréhensibles à toute personne à qu'il n'est pas destiné. Le but de la cryptographie est de respecter les objectifs suivants :

- **La confidentialité :** conserver les données secrètes et empêcher qu'une personne non autorisée ait accès à des données stockées ou transmises, ce qui rend l'information intelligible à d'autres personnes.

- **L'intégrité :** est la prévention d'une modification non autorisé de l'information qui permet de vérifier si les données n'ont pas été altérées durant la communication.
- **L'authentification :** permet de prouver l'authenticité par la confirmation de l'identité d'une entité afin qu'une tierce personne ne doit pas se faire passer pour quelqu'un d'autre (usurpation d'identité).
- **La non-répudiation de l'information :** est un mécanisme qui signifie que l'expéditeur peut vérifier qu'un certain destinataire a reçu un message particulier, cela consiste à garantir qu'aucun des partenaires ne puisse nier la transaction effectuée.

➢ La confidentialité est assurée par le chiffrement, par contre l'authenticité, l'intégrité et la non répudiation sont vérifiées par une signature numérique.

I.4. Les méthodes de chiffrements :

On distingue trois méthodes de chiffrement comme illustre la figure suivante :

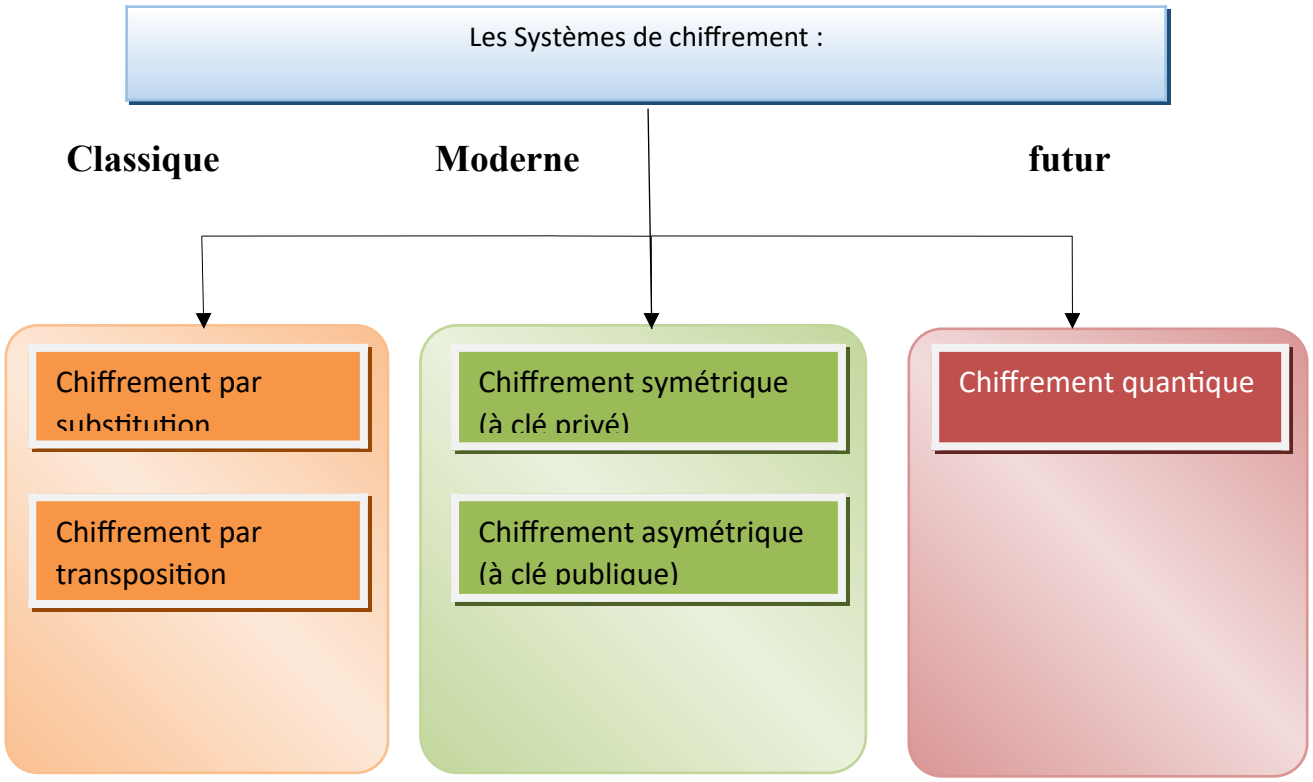

Figure I.3 : Méthodes de chiffrement.

I.4.1 Le chiffrement classique :

Le chiffrement classique est né avant l'apparition des ordinateurs. Il traite des systèmes reposant sur les lettres et les caractères d'une telle langue, son principe consiste à remplacer des caractères par des autres et/ou les transposer dans différents ordres, cela

suppose que les procédures de chiffrement et déchiffrement soient gardées secrètes, sinon le système devient inefficace.

Le chiffrement par substitution et par transposition sont les principaux modes du chiffrement classique.

I.4.1.1 Chiffrement par substitution :

Le chiffrement par substitution est le premier type de chiffrement, il est le plus simple car il consiste à remplacer les caractères ou les lettres de message clair par des symboles tel qu'il est illustré dans l'exemple ci-dessous.

Exemple :

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

Tableau I.1 : Exemple de chiffrement par substitution.

Texte en clair : Mémoire.

Texte chiffré : RJRDSBJ.

I.4.1.2 Chiffrement par transposition (permutation) :

La transposition consiste à changer l'ordre des lettres du message clair comme est indiqué dans l'exemple ci-dessous.

Exemple : m=9 (La taille du message)

Texte en clair	Q	U	A	N	T	I	Q	U	E
Position	1	2	3	4	5	6	7	8	9
Permutation	7	8	5	6	1	3	9	2	4
Texte chiffré	Q	U	T	I	Q	A	E	U	N

Tableau I.2 : Exemple de chiffrement par permutation.

I.4.2 Le chiffrement moderne :

Depuis la deuxième guerre mondiale, les besoins en cryptographie sont devenus plus qu'une nécessité. Cependant, ces techniques se sont orientées vers des applications civiles (banques, télécommunications, informatique…) qui sont un élément moteur essentiel de

progrès qui remédies l'inefficacité des techniques de cryptographie classique. La généralisation de l'outil informatique a permis d'exploiter des algorithmes bien plus complexes issus des techniques de cryptographie moderne.

Cette dernière manipule des bits car on utilise des ordinateurs [6], on distingue deux grandes catégories :

- Chiffrement symétrique ou à clé secrète (privé).
- Chiffrement asymétrique ou à clé publique.

I.4.2.1 Chiffrement symétrique :

Le chiffrement symétrique est la méthode de chiffrement la plus facile à comprendre et à réaliser. L'émetteur et le destinataire partagent une même clé secrète sur un canal physique sûr [6], tel qu'il est illustré sur la figure suivante.

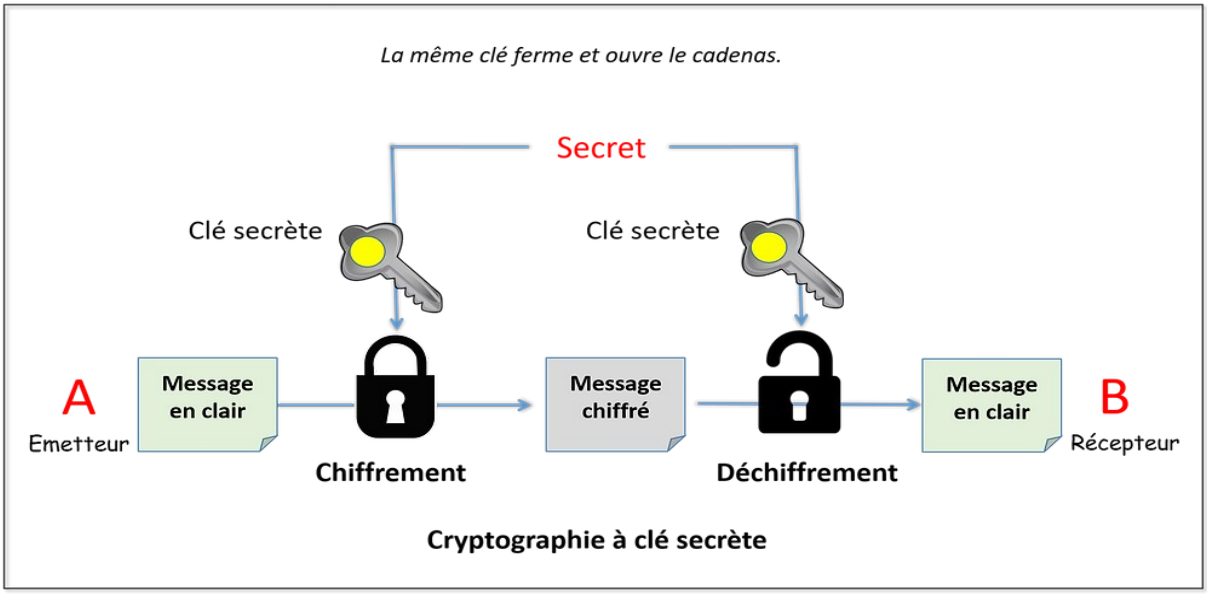

Figure I.4 : Prince de chiffrement symétrique.

➢ L'émetteur (A) chiffre les données avec une clé de chiffrement et il envoie le résultat de chiffrement au récepteur (B) où il utilise la même clé pour déchiffrer le message.

a. Les types de chiffrement symétrique :

Il existe deux modes de ce type de chiffrement :

- **Le chiffrement par bloc** : (Block Cipher en anglais)

C'est tout système de chiffrement symétrique dans lequel le message clair est découpé en bloc d'une taille fixe et chacun de ces blocs est chiffré.

- **Le chiffrement par flots** : (Stream-Cipher en anglais) :

Ces algorithmes chiffrent les messages bit par bit, quelle que soit la longueur du message à coder sans besoin de les découper.

b. Les exemples d'algorithmes symétriques :

On distingue plusieurs algorithmes, mais les plus utilisés sont : DES, AES.

1. DES (Data Encryptions Standard) :

Le Data Encryption Standard a été publié en 1977 par NIST (National Institue of Standard and Technology). Il est le premier algorithme cryptographique à petite clé secrète de 56 bits utiles, en fait une clé de 64 bits dont les bits 8, 16,24, 32, 40, 48, 56 ne sont pas utilisés pour la clé mais participent à un code correcteur qui permet de vérifier que la clé n'a pas été altérée, qui sert à la fois au chiffrement et au déchiffrement, d'où le message à chiffrer est découpé en blocs de 64 bits, chacun d'eux est séparé en deux sous blocs de 32 bits [7].

2. AES (Advanced Encryptions Standard) :

L'Advanced Encryption Standard est un standard américain qui remplace le DES, Proposé en 1998 par J. Daemen et V. Rijmen sous le nom de Rijndael. Les données sont de128 bits, les clés : 128, 196 ou 256 bits [5].

I.4.2.2 Chiffrement asymétrique :

La cryptographie à clé publique est apparue en 1976 par Diffie et Hellman [5], dans lequel l'émetteur et le récepteur ne partagent plus la même clé, dans un tel crypto-système les clés existent en paires d'où l'appellation bi-clés : une clé publique pour le chiffrement et une clé privé pour le déchiffrement. Il existe de nombreux algorithmes qui sont basés sur des problèmes mathématiques difficiles à résoudre, mais l'algorithme le plus connu est le RSA.

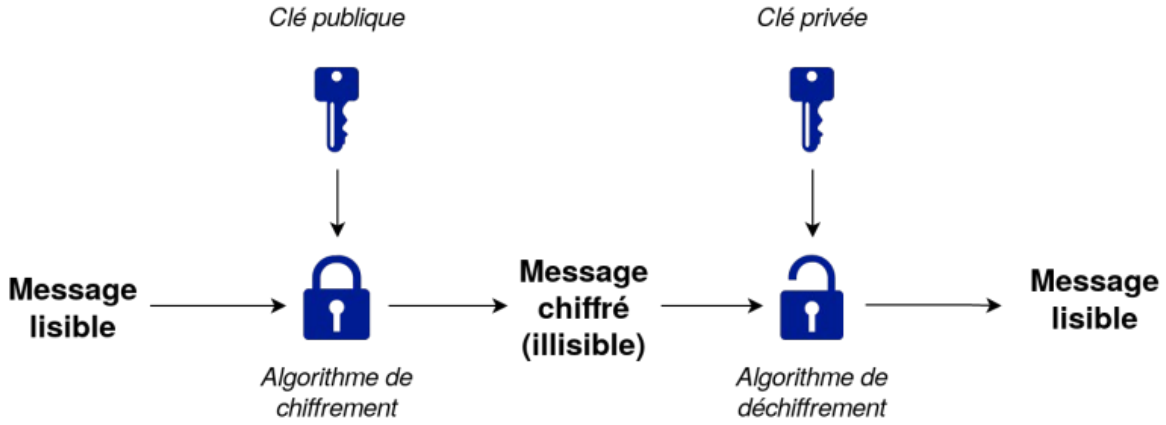

Figure I.5 : Prince de chiffrement asymétrique.

➢ Si l'émetteur veut envoyer un message confidentiel au récepteur, il se procure la clé publique du récepteur et chiffre le message, il envoie ensuite sur le canal non sûr le message chiffré au récepteur, d'où lui-même utilise la clé privé pour déchiffré le message [4].

L'algorithme RSA :

C'est le premier système à clé publique, publié en 1977 par Ron Rivest, Adi Shamir, et Leonard Adleman [7], il est solide car il est basé sur la difficulté de factoriser un produit de deux nombres premiers et la fonction à sens unique, cet algorithme fonctionne de la manière suivante :

Etape 1 : **Préparation des clés.**

1-1Choix de deux nombres premiers :

- Bob effectue les Operations suivantes :
  - ✓ Choix de deux nombres premiers ' p' ' q '.
  - ✓ Calcul de n=p*q.
  - ✓ Calcul de φ(n)= (p-1)*(q-1).

1-2Choix d'un exposant, et calcul de son inverse :

- Bob choisit un exposant ''e'' (entier) tel que : PGCD(e,φ (n))=1.
- Bob calcul l'inverse de ''e'' qui est ''d''.
- Modulo φ(n) par l'algorithme d'Euclide étendu :

  d*e=1(mod φ(n)).

1-3 Clé publique :

La clé publique de Bob est constituée des deux nombres : ‘’n’’, ‘’e’’.

1-4 Clé privé :

La clé privée de Bob est constituée des deux nombres : ‘’n’’, ‘’d’’, Bob garde à lui seul sa clé privée ‘’d’’.

Etape 2 : Chiffrement du message ’’m’’.

Pour que Alice envoie un message à Bob, elle doit chercher la clé publique de Bob, et elle calcule le message chiffré $C=m^e \pmod n$, et ce dernier nombre qu’elle envoie à Bob.

Etape 3 : Déchiffrement de message.

- Bob reçoit C chiffrée par Alice.
- Bob le déchiffre à l’aide de sa clé privée ‘’d’’ (donc il obtient le message initiale).

  $m=C^d \pmod n$.

Exemple :

- Pour se faire un couple de clés, Bob commence par choisir deux nombres premiers aléatoires soient : p=31, q=53.Il peut alors calculer n et φ(n), n=1643,φ (n)=1560.
- Bob choisit aléatoirement l’exposant publique ‘e’ inferieur à φ(n) et premier avecφ(n), soit e=11.
- Reste à calculer ‘d’ l’inverse de ‘e’ modulo φ(n).Pour cela, Bob peut utiliser l’algorithme d’Euclide étendu :

  $e*d \bmod \varphi(n)=1$.

  $d=e^{-1} \pmod{\varphi(n)}$

  $d=11^{-1} \pmod{1560}=851$.
- La clé publique est donc (11, 1643) et la clé privée est (851, 1643).
- Bob peut maintenant publier sa clé publique constitué de ‘n’ et’ e’. Il détruit ‘p’ et’ q’ et conserve précieusement la clé privée ‘d’ qui permet de déchiffrer les messages qui lui seront envoyés.

Le chiffrement :

- Alice utilise la clé publique de Bob pour chiffrer le message ''MEMOIRE 22''. Pour commencer elle convertit son texte en chiffres en prenant par exemple a=01, b=02, c=03, …, z=26, espace=00, 0=30, 1=31, 2=32, …
  Ce qui lui donne : 13 05 13 15 09 18 05 00 32 32.
- On procède selon deux conditions :

1. Découpage en mots de même longueur, on ajoute des zéro si nécessaire :
   013 051 315 091 805 003 232.
2. Découpage en morceaux de valeur inférieure à n (Regroupe ce nombre en tranches ayant moins de chiffres que la clé n=1643), soit en tranches de trois chiffres :
   M1=013, M2=051, M3=315, M4=091, M5=805, M6=003, M7=232.

‘ 013 051 315 091 805 003 232 ‘

- Le premier bloc est chiffré avec la clé publique de Bob :

  $C1=M^{e}_{1} \bmod n=13^{11} \bmod 1643=1553$.

$C1=M^{e}_{1} \bmod n=013^{11} \bmod 1643$	1553
$C2=M^{e}_{2} \bmod n=051^{11} \bmod 1643$	1185
$C3=M^{e}_{3} \bmod n=315^{11} \bmod 1643$	0986
$C4=M^{e}_{4} \bmod n=091^{11} \bmod 1643$	0587
$C5=M^{e}_{5} \bmod n=805^{11} \bmod 1643$	0309
$C6=M^{e}_{6} \bmod n=003^{11} \bmod 1643$	1346
$C7=M^{e}_{7} \bmod n=232^{11} \bmod 1643$	0542

Tableau I.3 : Chiffrement RSA.

- Alice répète cette opération sur les autres blocs et obtient :

  1553 1185 986 587 309 1346 542
- Elle peut maintenant envoyer ce message à Bob par un canal qui n’a pas besoin d’être sécurisé.

Le déchiffrement :

- Pour déchiffrer le message, Bob utilise sa clé privé.

  $m = C^{d} \bmod n$

$M1=C_1^{851} \bmod n= 1553^{851} \bmod 1643$	013
$M2=C_2^{851} \bmod n= 1185^{851} \bmod 1643$	051
$M3=C_3^{851} \bmod n=986^{851} \bmod 1643$	315
$M4=C_4^{851} \bmod n=587^{851} \bmod 1643$	091
$M5=C_5^{851} \bmod n=309^{851} \bmod 1643$	805
$M6=C_6^{851} \bmod n=1346^{851} \bmod 1643$	003
$M7=C_7^{851} \bmod n=542^{851} \bmod 1643$	232

Tableau I.4 : Déchiffrement RSA

Lors du déchiffrement, sachant qu'il faut obtenir des blocs de 2 éléments (grâce au codage particulier de l'exemple), on a bien :

13	05	13	15	09	18	05	00	32	32
M	E	M	O	I	R	E	Espace	2	2

Tableau I.5 : Résultat d'algorithme RSA

I.5. Comparaison entre le chiffrement symétrique et asymétrique :

Le tableau ci-dessous présente une comparaison entre les systèmes de chiffrement symétrique et les systèmes de chiffrement asymétrique, en énumérant les principaux avantages et inconvénients de chaque mode de cryptage, et leurs applications.

Cryptographie :	***Avantage :***	***Inconvénients :***	***Utilisation :***
Symétrique (DES, AES)	-Simple et facile à implémenter. - Nécessite moins de ressource de calcul. - Adapté aux grand flux de données à chiffrer. -Rapidité du système de chiffrement et déchiffrement.	- Nécessite un canal physique sûr. - Nécessite la connaissance de la clé par l'émetteur et par le récepteur. - Moins sécurisé car lorsque une personne interceptent la clé lors d'une communication peut ensuite lire ou même modifier toutes les informations chiffrer.	-Il est fréquemment mis en œuvre dans des installations de type SOHO (Simple Office, Home Office) et se retrouve dans des solutions « grand public » (par exemple dans les Wifi sécurisés en WPA-PSK ou Pre-Shared Key).
Asymétrique (RSA)	- L'utilisation de deux clés rend les algorithmes utilisés plus sécurisés. - Permettant l'authentification des messages par signature numérique. - L'émetteur et le récepteur n'ont pas besoin de partager des clés secrètes.	-Le traitement des données est lent et demande beaucoup plus de calcul. -Problème de gestion des clés publiques.	-Est très utilisé dans le commerce électronique, et plus généralement pour échanger des données confidentielles sur Internet.

Tableau I.6 : Comparaison entre les méthodes de chiffrement symétriques et asymétriques.

I.6. Les limites de la cryptographie classique et moderne :

Le système de chiffrement le plus utilisé et le plus connu dans le monde informatique est le chiffrement asymétrique (RSA) qui est basé sur la complexité de la factorisation, mais cette dernière prend millions de millions d'années pour un nombre de 600 chiffres.

En 1994 Peter Shor [4], à découvert un algorithme qui permet la factorisation d'un grand nombre qui utilise un calcul polynomial, il a démontré que les ordinateurs quantiques sont capables de factoriser des grands nombres plus efficacement que les ordinateurs classiques.

Avec l'avènement de l'ordinateur quantique, les algorithmes cryptographiques classiques et même modernes sont devenue inefficaces, dans ce contexte, la cryptographie quantique est apparue comme nouvelle solution pour assurer la sécurité des données, et elle détecte et empêche tout type d'espionnage, ce qui n'est pas le cas dans le cryptage classique et moderne. Cette nouvelle technique est basée sur la mécanique quantique et la théorie de l'information.

I.7. L'ordinateur quantique :

Un ordinateur quantique est l'équivalent d'un ordinateur classique, sauf que ses calculs sont effectués à l'échelle atomique. Il se base sur les lois de la physique quantique, qui s'intéresse au comportement de la matière et de la lumière au niveau microscopique.

Les états quantiques sont extrêmement fragiles, le fait même de les observer les perturbe. Pour manipuler les Qubits, il faut ainsi généralement utiliser des atomes froids, (à une température frisant les 4,2 k) [8].

L'apparition des ordinateurs quantiques s'évolue comme suit :

- **Les années 80** : Début des travaux dans domaine d'informatique quantique par Richard Feynman.
- **Les années 90** : L'apparition des premiers algorithmes quantiques.
- **Les années 2000** : Les premiers prototypes d'ordinateurs quantiques.
- **A partir début 2010** : mise sur le marché de premier ordinateur quantique par D-wave System, la mise à disposition d'un ordinateur quantique dans le Cloud par IBM [9].

Conclusion :

Durant ce chapitre, nous avons présenté quelques notions de base de la cryptographie avec la mention des différentes méthodes de chiffrement : classique, moderne d'où nous avons cité quelques exemples pour chaque méthode. On déduit que la cryptographie classique est très limitée, la cryptographie moderne se subdivise en deux autres types : symétrique et asymétrique dans lequel nous avons expliqué les algorithmes utilisé : DES, AES, RSA.

On conclut qu'avec l'apparition des ordinateurs quantiques, il est nécessaire de s'orienter à la cryptographie quantique.

Chapitre II :
Cryptographie quantique

Introduction :

La distribution de clé quantique « QKD »n'est pas de la cryptographie, car elle n'est pas une méthode de cryptage d'un message. Il s'agit en effet d'un ensemble de protocoles permettant de distribuer une clé de chiffrement entre deux interlocuteurs distants, tout en assurant la sécurité de la transmission grâce aux lois de la mécanique quantique et de la théorie de l'information.

L'objectif de ce deuxième chapitre est de discuter les principes de la mécanique quantique et des généralités sur la théorie de l'information quantique, et enfin nous nous intéresserons aux quelques protocoles existants de la cryptographie quantique.

II.1 Notion de base de la mécanique quantique :

La mécanique classique atteint ses limites à l'échelle microscopique, c'est dans ce contexte que la mécanique quantique est parvenue. Elle englobe la théorie mathématique et physique décrivant la structure et l'évolution dans le temps et dans l'espace des propriétés à l'échelle atomique.

À un système quantique est associé un espace vectoriel complexe muni d'un produit scalaire appelé espace de Hilbert H. L'état d'un système est un vecteur d'état de l'espace H appelé vecteur "Ket", décrit par la notation de Dirac$|\psi\rangle$, à lequel on lui associe un élément noté¿$\varphi\vee$¿, appelé *Bras* [10].

✓ ***Propriétés :***

L'action d'un Bras ¿$\varphi\vee$¿ sur un Ket, ¿ψ>¿est égale à un produit scalaire, ¿ψ>¿ et ¿$\varphi\vee$¿:

¿$\varphi\vee\psi\geq\int\varphi*.\psi\,.dv$ (II, 1)

- Le conjugué de ¿:

¿¿ (II, 2)

- Un système d'état est normé :

¿$\psi\vee\psi$>¿1 (II.3)

- Le module d'un état est défini par :

$\|\psi\|=\sqrt{¿\psi\vee\psi>¿¿}$ (II.4)

II.1.2 Les principes fondamentaux de la mécanique quantique :

L'échange de clé quantique est basé sur deux théorèmes physiques qui aident à produire une clé sécurisée entre Alice et Bob et qui sont : le principe d'incertitude d'Heisenberg et le théorème de non-clonage.

1. Principe d'incertitude de Heisenberg :

Ce principe a été énoncé par Werner Heisenberg en 1926 [4], dans lequel il montra qu'une particule ne pourra jamais avoir une position et une vitesse avec précision au même temps car la mesure perturbe le système.

2. Théorème de non Clonage :

Énoncé en 1982 par Wootters et Zugnrek [4], le célèbre théorème de non-clonage, suppose qu'il est impossible de concevoir un cloneur quantique qui puisse cloner parfaitement, n'importe quel état (c.-à-d. qu'il n'est pas possible de copier un photon de manière à obtenir deux photons identiques). Contrairement, en monde de l'information classique dans lequel est facile de réaliser une copie d'un bit.

II.2 Quelques propriétés de l'information quantique :

L'information quantique est la théorie de l'utilisation des spécificités de la physique quantique pour le traitement et la transmission de l'information.

II.2.1. Qubit :

Un bit classique est la plus petite unité de stockage d'information qui peut se trouver soit dans l'état 1, soit dans l'état 0. Avec l'analogie quantique, le Qubit (quantum bit), est l'état quantique qui représente la plus petite unité de stockage d'information quantique. Il se compose d'une superposition de deux états [11].

A. Définition :

Un Qubit est un vecteur unitaire d'un espace de Hilbert.

L'expression de l'état d'un Qubit est donnée par :

$$\psi = \alpha|0\rangle + \beta|1\rangle \qquad \textbf{(II.5)}$$

Où α et β sont des coefficients complexes, ils représentent les amplitudes de probabilité d'obtenir l'état 1 et l'état 0 respectivement lors d'une mesure de l'état ψ. Ces deux états

constituent une base orthogonale de l'espace de Hilbert du système. Ces coefficients satisfont la condition de normalisation suivante :

$$|\alpha|^2 + |\beta|^2 = 1 \qquad \textbf{(II.6)}$$

$|\alpha|^2$: représente la probabilité d'avoir le bit 0.

$|\beta|^2$: représente la probabilité d'avoir le bit 1.

$|0\rangle et\ |1\rangle$: représentent deux états orthogonaux dans le système quantique.

B. Particularité du Qubit :

En plus de la particularité du Qubit par rapport à un bit classique qu'il ne peut pas être dupliqué.

• Une mesure d'un Qubit ne donne aucune information sur $\alpha et \beta$ puisque le résultat est soit$|0\rangle$soit$|1\rangle$ ce qui équivaut à $(\alpha, \beta) = (1,0)$ ou $(0,1)$ ce qui ne correspond pas aux valeurs initiales de α et β.

C. Etats intriqués :

L'intrication 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.

II.2.2. Photon :

A. Comportement des photons :

La lumière est constituée des photons qui sont des particules élémentaires (quantum) portant chacune une énergie hv, tel que h est la constante de Planck et v est la fréquence et ayant des propriétés physiques particulières (polarisation, position, etc. …) sur lesquelles toute la cryptographie quantique se repose.

B. Polarisation de photon :

Dans une onde électromagnétique, le champ électrique et le champ magnétique oscillent simultanément dans des directions différentes. Par convention, la polarisation de la lumière décrit la vibration du champ électrique E dans le plan orthogonal à la direction de propagation.

- **Les types de polarisation :**

Polarisation rectiligne **:** Le champ électrique oscille dans une seule direction.

Polarisation circulaire ou elliptique **:** Le champ peut tourner autour de l'axe de propagation de l'onde.

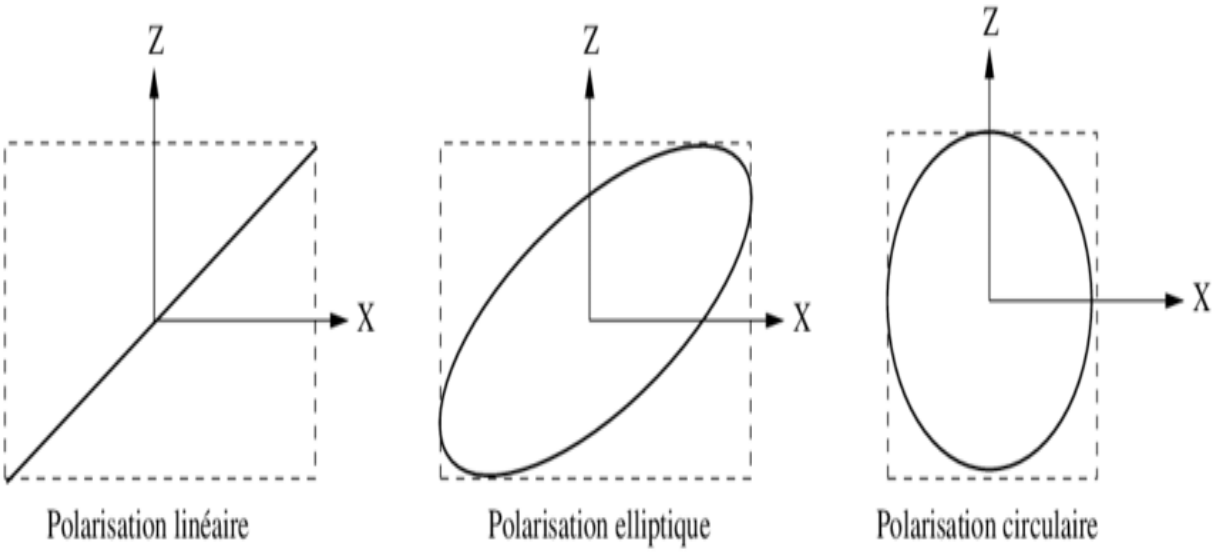

Figure II.1 : Les types de polarisations.

- **Détection de la polarisation des photons :**

Lorsque l'on fait passer la lumière à travers un filtre polarisant suivi d'un détecteur de photons, les photons seront absorbés ou transmis selon leurs polarisations :

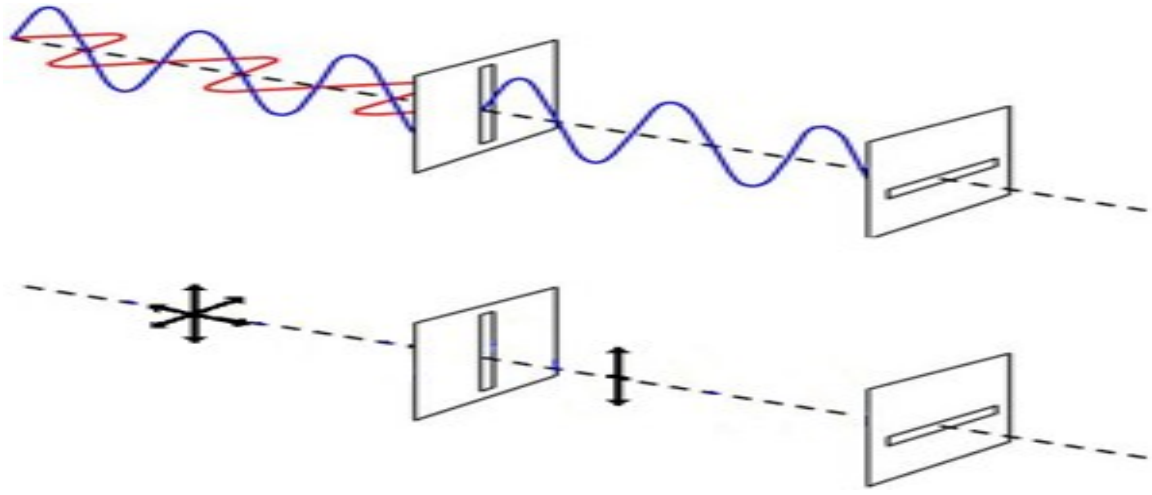

Figure II.2 : Polarisation du photon

✓ Si le photon est polarisé parallèlement à l'angle d'orientation du filtre, alors ce photon sera transmis sans changement de polarisation.

- ✓ Si le photon est polarisé perpendiculairement à l'angle d'orientation du filtre, alors ce photon sera absorbé.
- ✓ Si le photon est polarisé selon une direction intermédiaire, alors ce photon sera transmis avec probabilité cos2 (α), où α est l'angle de polarisation du photon mesuré par rapport à l'angle d'orientation du filtre. C'est-à-dire que si le photon est polarisé selon un angle γ et que le filtre est orienté selon un angle β, alors α = γ - β. Si le photon est transmis, alors sa nouvelle polarisation correspondra à l'angle d'orientation du filtre [4].

II.3 Cryptographie quantique par photons uniques :

Cette section traite les différents protocoles basés sur des Qubits utilisés lors de la phase de transmission quantique. Dans le principe de la cryptographie quantique, il est fondamental de ne transmettre les informations du type clés de cryptage que sous la forme de photon unique afin de garantir la fiabilité de canal quantique à toute tentative d'espionnage.

II.3.1. Source de photon unique :

La source de photon unique représente tout dispositif capable d'émettre des impulsions lumineuses contenant un seul photon par impulsion [13]. Afin d'obtenir un photon unique, il existe quelques moyens, d'où le choix des sources lasers atténués est nécessaire pour garantir la sensibilité de canal quantique à toute tentative d'espion.

II.3.2 Sources lasers atténués :

Les sources lasers atténués sont les premières sources utilisées dans les protocoles de distribution quantique de clé [13]. Elles ont un grand avantage par rapport aux autres sources, car elles ne nécessitent pas des modifications au niveau de l'émission. Ces sources sont réalisées en ajoutant un atténuateur optique à la source laser.

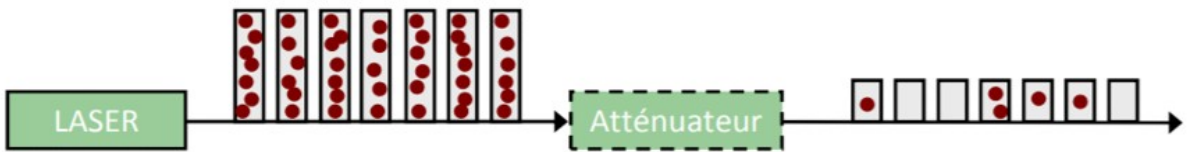

Figure II.3 : Source Laser atténué.

La distribution de photon dans chaque impulsion suit une loi de Poisson, en fonction du nombre de photons (n) et du nombre moyen de photon μ par impulsion :

$$p(n,u)=\frac{e^{-u}.u^{n}}{n!} \qquad \textbf{(II.10)}$$

En réduisant le nombre moyen de photon par impulsion à μ= 0.1, la probabilité d'obtenir un photon par impulsion sera augmentée $P(1) \approx \mu$ [13].

II.4 Principe de la cryptographie quantique :

La cryptographie quantique est basée sur les lois de la mécanique quantique qui permettent de sécuriser la transmission des données en utilisant des clés générées et échangées à l'aide d'une particule quantique nommée : Photons et interdire un espion de connaître des informations échangées entre deux entités, Alice et Bob. Si Eve tente d'intercepter les signaux envoyés par Alice, Bob pourra détecter la présence d'espion (Eve).

Dans les systèmes de télécommunication quantique, les transmissions se font généralement par l'intermédiaire de deux canaux d'échanges différents :

II.4.1. Le canal quantique :

C'est le canal qui permet le partage de la clé. Il s'agit d'un câble de fibre optique permettant la transmission des photons.

II.4.2. Le canal classique :

Il s'agit généralement d'un réseau internet. Il permet de procéder à des vérifications et de transmettre le message une fois qu'il est crypté.

Figure II.4 : Les systèmes de communication quantique.

II.5 Etapes de la création de clé quantique :

II.5.1 Communication quantique :

Dans la création de la clé quantique, l'information est transmise par des photons. Alice et Bob échangent des Qubits sur le canal quantique. Alice choisit alors une chaine de bit

aléatoire et une séquence de base de polarisation. Elle prépare les photons polarisés et les transmettent à Bob. De même Bob tente de mesurer correctement les Qubits envoyés par Alice en choisissant aléatoirement l'une des bases de polarisation utilisées [14]. La clé obtenue dans cette étape est appelée la clé crue, comme illustre la figure II.5.

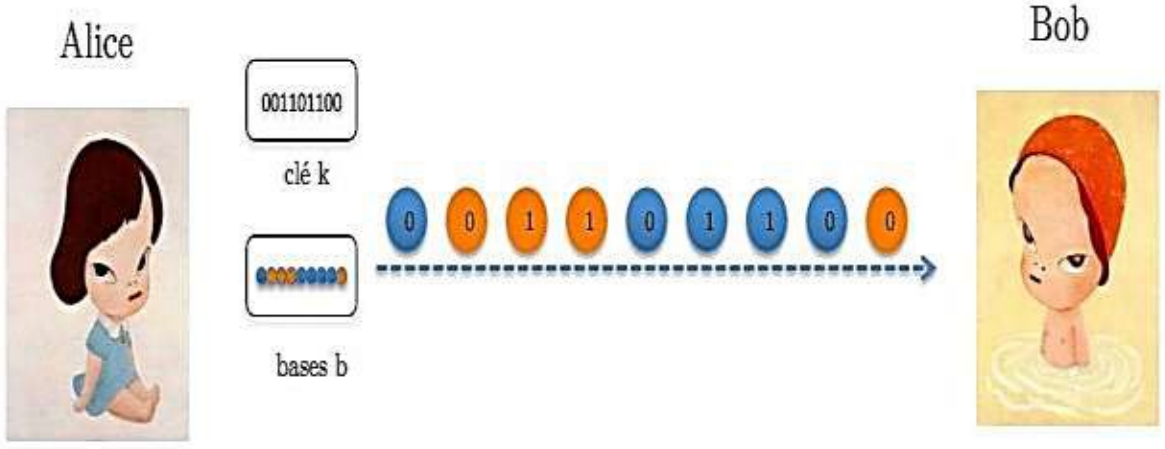

Figure II.5 : transmission quantique.

II.5.2 Phase de tamisage :

Alice et Bob partagent leur choix de base à travers le canal classique. Ils comparent leurs résultats et rejettent toutes les positions des bits où Bob n'a pas fait le bon choix. En moyenne ces chaînes sont donc deux fois plus courtes que les chaînes de départ. La clé obtenue dans cette étape est appelée la clé tamisée, tels que représente la figure suivante.

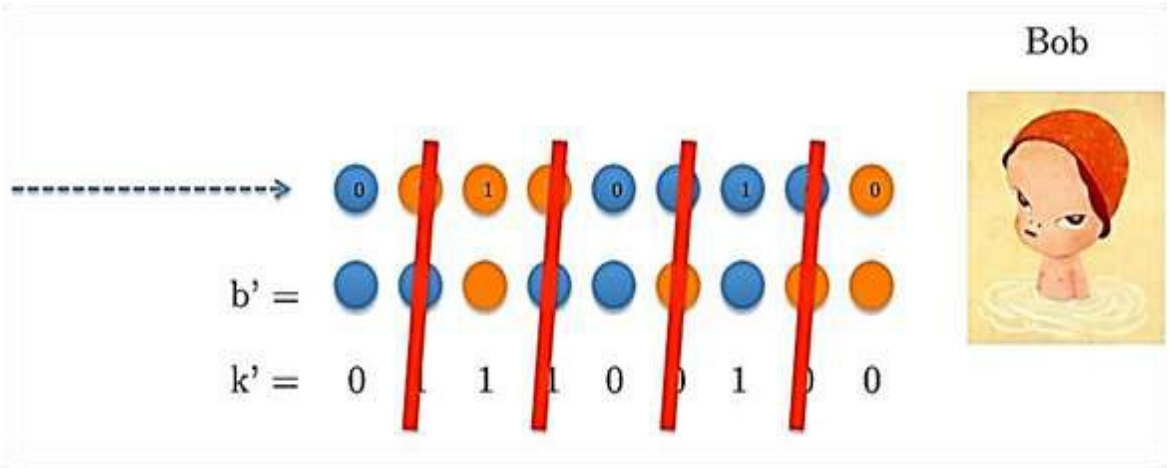

Figure II.6 : Phase de tamisage

II.5.3 Phase d'estimation d'erreur :

Afin de réduire la différence entre la clé crue et la clé tamisée obtenue qui est due soit à l'imperfection d'appareil ou bien à la présence d'espion, il est nécessaire de corriger les

erreurs, c'est la phase d'estimation des erreurs qui s'en charge. Alice et Bob annoncent au hasard un sous-ensemble sélectionné dans leur données et ils doivent calculer le taux d'erreurs observées et gardent cette transmission si le taux d'erreur est moins a un seuil désiré, sinon la clé sera ignorée [14]. L'exemple de la figure II.7 illustre le déroulement de cette phase.

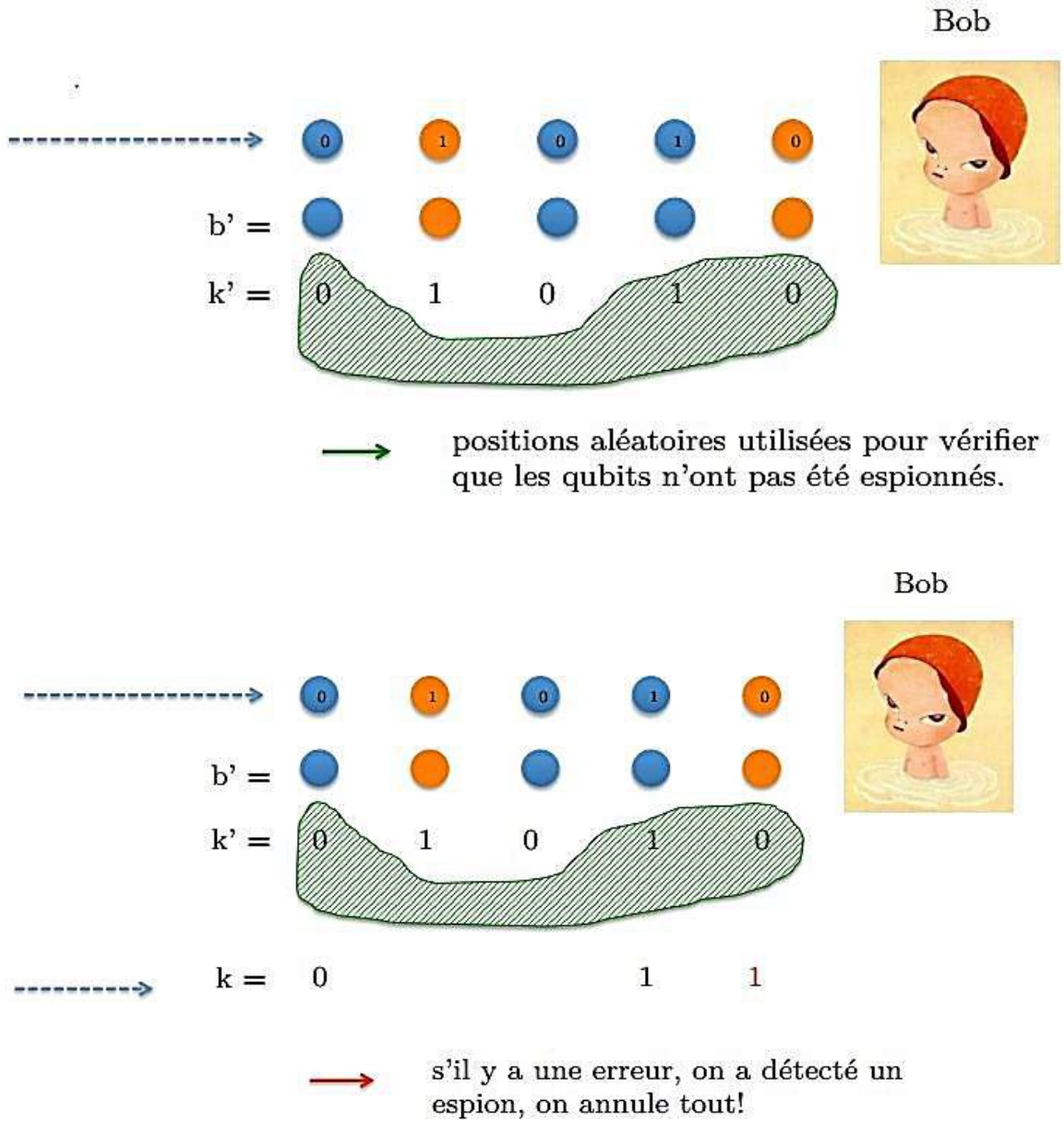

Figure II.7 : Phase d'estimation d'erreur

II.5.4 Correction d'erreur :

En fonction du taux d'erreur estimé lors de la phase précédente, Alice et Bob modifient les informations publiques et se mettent d'accord sur une chaine de bits commune afin de réduire la quantité d'information espionnée par Eve et de supprimer tous les bruits dus au canal de communication, ainsi ceux causés par les appareils de mesure. Alice et Bob

peuvent abandonner le protocole, si la quantité totale d'informations écoutées par l'espion après toutes les étapes précédentes est supérieure à la taille de la chaine de bits commune [15]. La figure ci-dessus présente la correction d'erreur détectée dans la phase précédente.

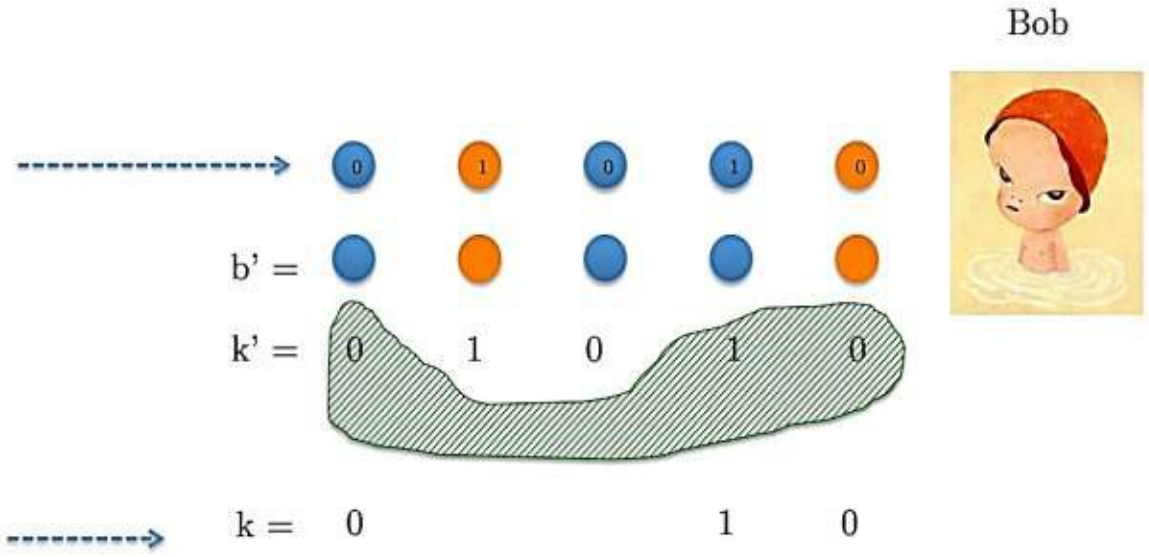

Figure II.8 : Phase de correction d'erreur.

II.6 Quelques types de protocole de distribution à clé quantique :

Dans cette section, on présentera les protocoles essentiels utilisés et qui sont fondés sur le codage des photons uniques. Les sources sont ici supposées être des sources idéales, où leur approximation par des sources lasers émettant des états cohérents fortement atténués de sort à avoir un seul photon par impulsion.

II.6.1 Le protocole BB84 :

Le protocole BB84 est le premier protocole de distribution de clé quantique élaboré par C.H. Bennett et G. Brassard en 1984 [18]. Ce protocole est le plus couramment utilisé et assez simple à comprendre. Il utilise quatre états différents qui font une paire des états de base. BB84 est un protocole non déterministe. Cela signifie qu'il distribue une suite aléatoire des bits [19].

Le but de ce protocole est de distribuer une clé de chiffrement secrète entre deux interlocuteurs distant, tout en assurant la sécurité de la transmission. Cette clé secrète peut être utilisée dans un algorithme de chiffrement symétrique, afin de chiffrer et déchiffrer des données confidentielles.

Le principe relativement simple de ce protocole est d'utiliser quatre états non-orthogonaux. Les données sont encodées en utilisant la polarisation de photons, avec les valeurs binaires '0' '1'.

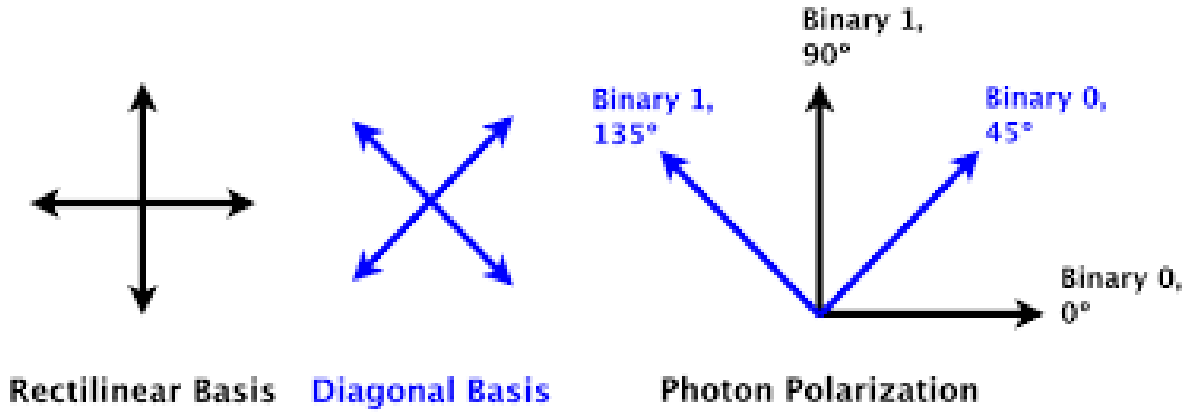

Figure II.9 : Les bases de polarisation de protocole BB84.

Les états de polarisation de photon appartiennent à deux bases alors comme illustre le tableau suivant :

Mode de polarisation :	**Symbole**	**Etat de polarisation**	**Qubit**	**Notation de Dirac**
Base rectiligne	+	Horizontale 0° →	Qubit 0	**|H⟩**
		Verticale 90° ↑	Qubit 1	**|V⟩**
Base diagonale	×	Diagonale 45° ↗	Qubit 0	**|D⟩**
		Anti-diagonale 135° ↖	Qubit 1	**|A⟩**

Tableau II.1 : Etat de polarisation associée à chaque Qubit.

II.6.1.1 Déroulement du protocole BB84 :

A. En absence d'espion :

Le protocole BB84 se déroule en six étapes :

- Alice encode sa séquence de bits en sélectionnant aléatoirement la base rectiligne ou la base diagonale sans révéler ses choix à personnes. Les photons sont ensuite envoyés à Bob via le canal quantique.

- Bob reçoit les photons et enregistre les résultats en choisissant de manière aléatoire une des deux bases.
- Alice échange avec Bob ses choix de bases via un canal public, mais pas la valeur binaire associée à chaque photon.
- Bob compare ses choix de bases avec ceux d'Alice et identifie le sous ensemble de bits correspondants aux cas où ils ont tous les deux choisis la même base. Bob communique ensuite à Alice via le canal publique les positions correspondantes dans la séquence, les autres bits sont alors éliminés.
- Bob transmet ensuite à Alice via le canal publique un sous ensemble de ses résultats. Alice compare cette séquence de bits avec sa propre séquence et réalise alors une analyse d'erreurs.
- Si le taux d'erreurs est plus faible que 11% [4], Alice déduit alors qu'il n'y a pas eu d'acte d'espionnage durant la procédure, et que par conséquent la communication à travers le canal quantique était sécurisée. Alice et Bob ont alors la possibilité de conserver les bits restant qui forment leur clé privée. Si le BER est supérieur à 11% on abandonne alors la procédure et on recommence le protocole à l'étape1.

Figure II.10 : Principe de protocole BB84.

Exemple d'une séquence binaire sans espion :

Bit d'Alice	***1***	***0***	***1***	***1***	***0***	***1***	***1***	***0***	***1***	***0***
Base d'Alice	+	×	×	+	×	+	+	+	×	+
Polarisation d'Alice	**V**	**D**	**A**	**V**	**D**	**V**	**V**	**H**	**A**	**H**
Base de Bob	+	+	×	×	×	+	×	+	×	+
Polarisation de Bob	***V***	***H***	***A***	***D***	***D***	***V***	***A***	***H***	***A***	***H***

Bit de Bob	***1***	***0***	***1***	***0***	***0***	***1***	***1***	***0***	***1***	***0***
La clé secrète	***1***	***-***	***1***	***-***	***0***	***1***	***-***	***0***	***1***	***0***

Tableau II.2 : une séquence binaire sans espion du protocole BB84.

D'après les résultats obtenus, on remarque que uniquement les Qubits de même polarisation qui passent, donnant la clé suivante : 1101010.

B. En présence d'espion :

L'action d'Eve est d'écouter le canal quantique entre Alice et Bob à travers la stratégie d'intercepter-renvoyer.

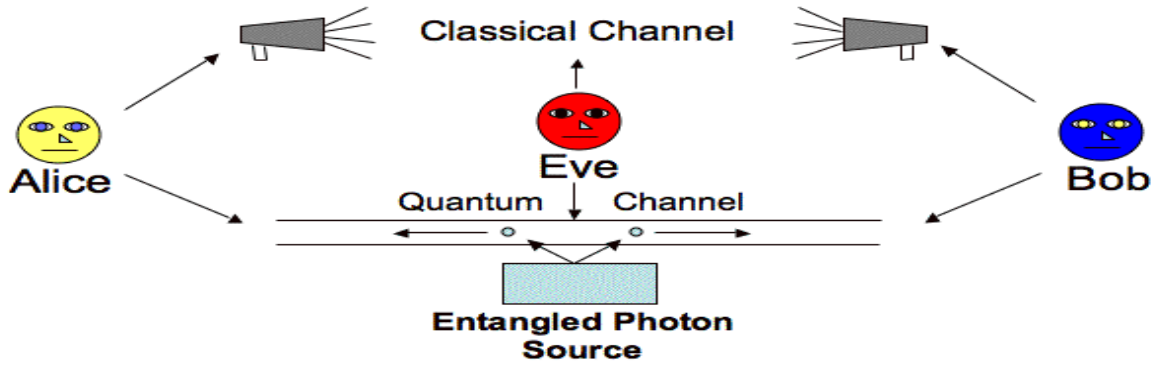

Figure II.11 : Principe de protocole BB84 en présence d'espion.

Le déroulement de ce protocole en présence d'espion se fait comme ceci :

- L'émission des photons par Alice ne change pas, elle reste identique à une Communication simple, car Alice ne sait pas qu'il y a un espion sur le canal quantique.
- Cette fois-ci Eve (l'espion) va utiliser une des deux bases et faire comme Bob dans une communication simple afin de mesurer et comprendre les Qubits envoyés par Alice.
- Pour ne pas être repérée, l'espion essayera de renvoyer le même photon qu'Alice dans le canal quantique.
- Comme pour l'échange simple, Bob va utiliser une des deux bases afin de trouver la clé envoyée par Alice, mais cette fois-ci Bob a une chance sur deux pour utiliser une mauvaise base et tomber sur un résultat erroné dû à l'envoi du photon par Eve.
- Alice et Bob vont ensuite réaliser la phase de tamisage à l'aide du canal classique pour avoir la clé finale reconstituée.
- Afin de vérifier qu'ils ne se sont pas faits espionnés, Bob et Alice vont réaliser la phase «Estimation d'erreur», ils vont choisir de dévoiler et comparer les Qubits publiquement sur le canal de communication : Si sur les Qubits comparés, il y'a des Qubits différents, la

clé n'est plus identique, ils ont une preuve qu'ils ont été écoutés. Ils vont abandonner et ne pas utiliser cette clé.

Exemple d'une séquence binaire avec espion :

Bit d'Alice	*1*	*0*	*1*	*1*	*0*	*1*	*1*	*0*	*1*	*0*
Base d'Alice	+	x	x	+	x	+	+	+	x	+
Polarisation d'Alice	V	D	A	V	D	V	V	H	A	H
Base d'Eve	x	x	+	+	x	+	x	+	x	+
Mesure d'Eve	A	D	H	V	A	V	D	H	D	H
Bit d'Eve	-	0	-	1	-	1	-	0	-	0
Bit d'Eve modifié	*0*	*1*	*1*	*0*	*0*	*0*	*0*	*1*	*1*	*1*
Nouvelle base d'Eve	x	+	x	x	+	x	+	+	x	x
Polarisation d'Eve	D	V	A	D	H	D	H	V	A	A
Base de Bob	+	+	x	+	x	x	x	+	+	x
Mesure de Bob	V	H	A	H	D	D	A	H	V	D
Bit de Bob	1	-	1	-	0	0	-	0	-	-
Clé secrète	1	-	1	-	0	0	-	0	-	-

Tableau II.3 : une séquence binaire avec espion du protocole BB84.

La quantité totale d'informations écoutées par l'espion '0' est inférieur à la taille de la chaine de bits commune entre Alice et Bob '1100'. Alors ils vont utiliser cette clé '11000'.

II.6.2 Le protocole B92 :

Le protocole B92 est proposé par Charles Bennet en 1992 [20], est un protocole de distribution quantique de clés, est la version simple du protocole BB84. L'idée principale de ce protocole est d'utiliser deux bases non orthogonales au lieu de quatre.

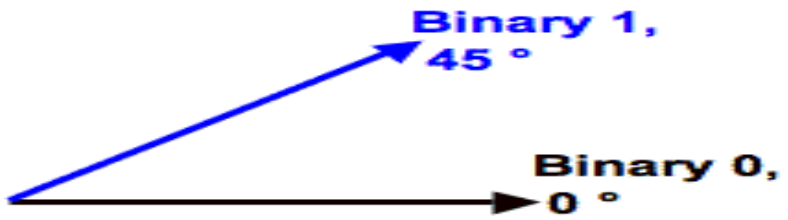

Figure II.12 : Les bases de polarisation de protocole B92.

Toutefois en pratique, ce protocole est simple à réaliser, néanmoins reste inefficace en termes de sécurité, cela on peut le constater clairement au coût d'une certaine perte.

Le principe de ce protocole est d'utiliser une base non orthogonale pour coder des bits, comme montre le tableau ci-dessous :

Qubit :	**En émission :**	**En réception :**
0	Horizontal (0°)	Anti-diagonal (135°)
1	Diagonal (45°)	Vertical (90°)

Tableau II.4 : Etat de polarisation associée à chaque Qubit.

II.6.2.1 Déroulement du protocole B92 :

Le principe et la procédure du ce protocole 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 des Qubits, Bob les mesure dans des bases au hasard qui en résulte deux cas : Si le choix est différent, aucune mesure ne sera effectuée et le Qubit sera ignoré. Mais si le choix coïncide et les données d'Alice et Bob sont corrélées, alors le Qubit sera conservé et contribuera à construction de la clé secrète.

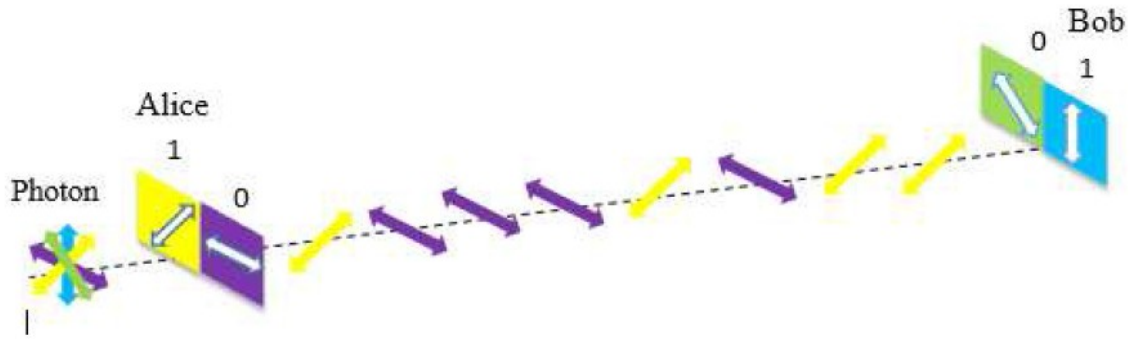

Figure II.13 : Principe de protocole B92.

Exemple d'une séquence binaire sans espion :

Bit d'Alice	*1*	*0*	*1*	*1*	*0*	*1*	*1*	*0*	*1*	*0*
Base d'Alice										
Polarisation d'Alice	**D**	**H**	**D**	**D**	**H**	**D**	**D**	**H**	**D**	**H**
Base de Bob										
Mesure de Bob	**V**	**V**	**A**	**V**	**A**	**V**	**A**	**A**	**A**	**V**
Bit de Bob	**1**	**-**	**-**	**1**	**0**	**1**	**-**	**0**	**-**	**-**

Tableau II.5 : une séquence binaire sans espion du protocole B92.

D'après les résultats obtenus, on remarque qu'uniquement les valeurs des Qubits pour lesquels leurs choix ont coïncidés qui passe, donnant la clé suivante : 11010.

Exemple d'une séquence binaire en présence d'espion :

Bit d'Alice	*1*	*0*	*1*	*1*	*0*	*1*	*1*	*0*	*1*	*0*
Base d'Alice										
Polarisation d'Alice	**D**	**H**	**D**	**D**	**H**	**D**	**D**	**H**	**D**	**H**
Base d'Eve										
Mesure d'Eve	**V**	**V**	**A**	**V**	**A**	**V**	**A**	**A**	**A**	**V**
Bit d'Eve	**1**	**-**	**-**	**1**	**0**	**1**	**-**	**0**	**-**	**-**
Nouvelle base d'Eve										
Polarisation d'Eve	**H**	**D**	**H**	**H**	**D**	**H**	**H**	**D**	**D**	**H**
Bits d'Eve Modifié	**0**	**1**	**0**	**0**	**1**	**0**	**0**	**1**	**1**	**0**
Base de Bob										
Polarisation de Bob	***A***	**A**	**V**	***A***	***V***	***V***	***V***	***V***	***A***	***V***
Bit de Bob	***0***	**0**	**1**	***0***	***1***	***1***	***1***	***1***	**-**	**-**
Clé finale	***0***	**0**	**1**	***0***	***1***	***1***	***1***	***1***	**-**	**-**

Tableau II.6 : une séquence binaire avec espion du protocole B92.

La quantité totale d'informations écoutées par l'espion '0011' est égale à la taille de la chaine de bits commune entre Alice et Bob '0111'. Alors ils vont négliger cette clé '00101111'.

Conclusion :

Les principes de la mécanique quantique et de la théorie d'information sont la base de la cryptographie quantique. Durant ce chapitre, nous avons exposé ses principes, puis nous avons mis l'accent sur les principaux protocoles de distribution de clé quantique à photon unique BB84 et B92 ainsi que leur fonctionnement, à travers lesquels un éventuel espion peut être détecté par l'émetteur 'Alice' et le récepteur 'Bob 'cela grâce aux deux principes de la mécanique quantique à savoir le théorème de non clonage et le principe d'incertitude d'Heisenberg.

Chapitre III :

Etude des performances du protocole BB84 et B92 dans une liaison optique

Introduction :

La fibre optique est un support de transmission privilégié pour le transport de diverses types de données publiques, privées et confidentielles .La cryptographie quantique est utilisée pour sécuriser ces données grâce à la distribution quantique de clés « Quantum Key Distribution » notamment les protocoles BB84 (Charles Bennett et Gilles Brassard 1984), B92 (Bennett 1992) pour le partage des clés de cryptage rendant l'information : inviolable, impossible à cloner et surtout offre la possibilité de détection d'intrusion.

Notre simulation sur le logiciel Optisystem a pour but de simuler un comportement équivalent d'une liaison optique illustrant le principe de base du QKD et l'analyse des taux d'erreur (QBER) et le facteur de qualité (Q) en fonction de la distance et la longueur d'onde sans et avec présence d'un espion.

Partie théorique : Généralité sur la fibre optique.

III.1 Structure générale d'une liaison par fibre optique :

Le principe dans les communications optiques consiste à transporter de l'information sous forme lumineuse d'un point à un autre à travers un guide diélectrique.

L'information à transmettre est convertie d'un signal électrique en signal optique grâce à un émetteur électro-optique, elle est ensuite injectée dans une fibre optique. A la réception, le signal subira le traitement inverse à savoir la conversion optique-électrique grâce à un récepteur électro-optique [21].

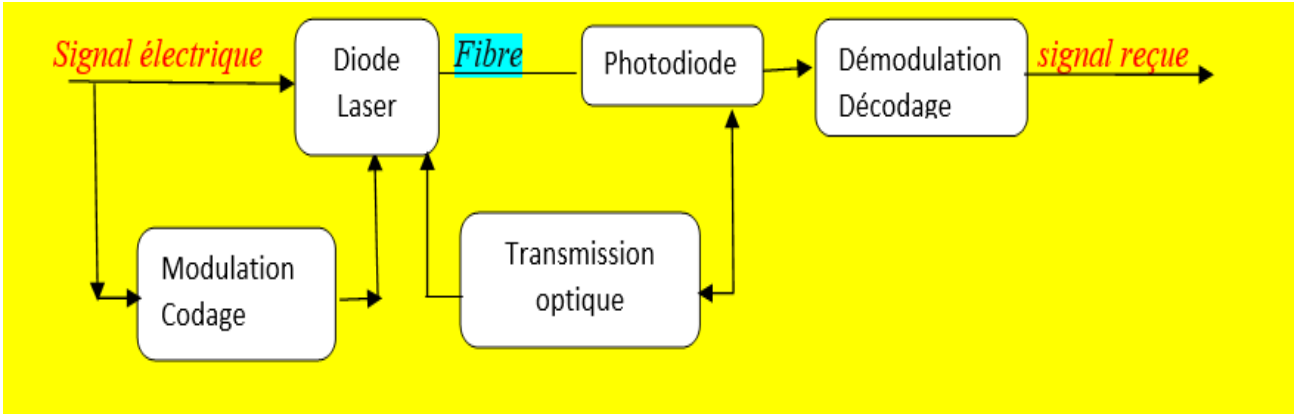

Figure III.1 : le principe de base d'une transmission de données par une fibre optique.

III.2 La fibre optique :

La fibre optique est un fil en verre ou en plastique très fin. Représente le support de propagation de la lumière (canal de communication) dans les systèmes optiques, est de forme cylindrique.

III.3 Les composants d'un câble de fibre optique :

- ***le cœur*** : est la région de la fibre dans laquelle se propage la lumière. Dans ce milieu, l'indice de réfraction n1 est le plus élevé.
- ***La gaine optique*** **:** est un milieu d'indice n2 légèrement plus faible, qui se comporte ainsi comme un ''miroir réfléchissant'' pour la lumière à l'interface cœur-gaine.
- ***Le revêtement*** **:** est une couche de plastique qui entoure la fibre optique pour la renforcer. Elle aide à absorber les chocs et permet une protection complémentaire contre des courbures excessives.
- ***L'armature en fibre*** : permet de protéger le cœur contre les forces d'écrasement et les tensions mécaniques excessives lors de l'installation.
- ***La gaine extérieure :*** complète la protection mécanique du cœur [22].

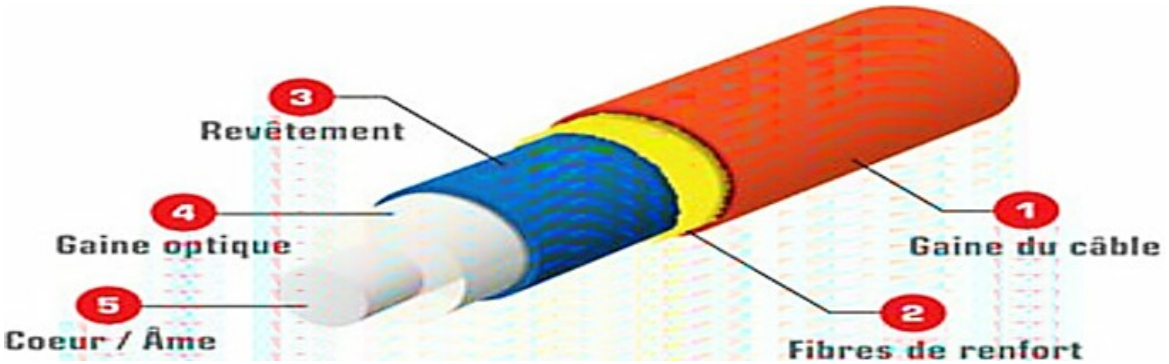

Figure III.2 : schéma d'un câble à fibre optique.

III.4 Différents types de fibres optiques :

III.4.1 La fibre monomode :

Dans une fibre monomode, un seul mode est autorisé c'est le mode fondamentale, elle possède un cœur très étroit (diamètre <10µm), est utilisée pour les systèmes de télécommunications à très longues distances à grands débits, elle possède une bande passante très élevée (de l'ordre du Thz/Km).

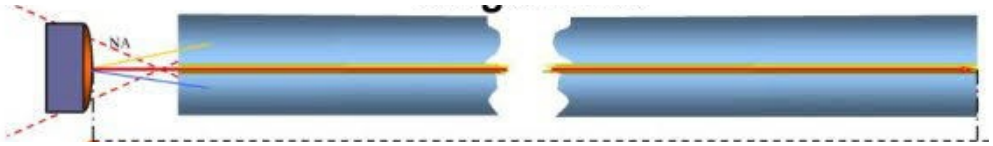

Figure III.3 : Fibre monomode.

III.4.2 La fibre multi-mode :

La fibre multi-mode a été la première utilisée sur le marché, Elle a un diamètre du cœur entre 50µm ou 62.5µm elle est limitée en bande passante. Elle permet la propagation de plusieurs modes, elle est employée dans les systèmes à courtes distances notamment les réseaux locaux [23]. Elle existe sous deux formes :

a. La fibre à saut d'indice :

Le cœur et la gaine présentent des indices de réfraction différents et constants. Le passage d'un milieu vers l'autre est caractérisé par un saut d'indice. Le faisceau lumineux injecte à l'entrée de la fibre va atteindre la sortie en empruntant des chemins optiques différent, ce qui se traduit par des temps de propagation différents et donc un étalement du signal transmis, ce phénomène est appelé dispersion modale.

b. La fibre à gradient d'indice :

Le cœur se caractérise par un indice variable qui augmente progressivement de l'interface gaine-cœur jusqu'à au centre de la fibre, les rayons lumineux vont arriver en même instant à la sortie de la fibre, le phénomène de dispersion modale est éliminé [24].

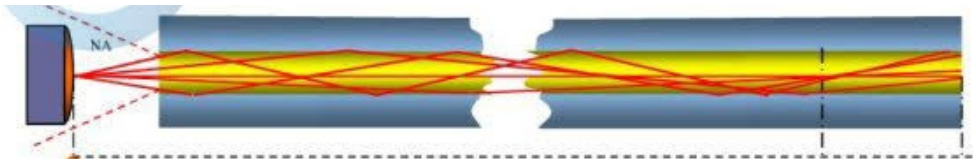

Figure III.4 : Fibre multi-mode.

II.5 Propriétés de la fibre optique :

a. Atténuation :

L'atténuation correspond à une diminution de la puissance du signal transmis. Elle s'exprime très souvent en décibels (dB/km).Cet affaiblissement (Atténuation) du signal est moins forte dans les systèmes optiques à base de fibre optique que dans les systèmes électriques ou radio, elle dépend en particulier de la longueur d'onde des impulsions lumineuses.

Selon l'atténuation, les fibres peuvent être utilisées pour la transmission essentiellement dans deux « fenêtres en longueur d'onde » : les fenêtres 1300 nm et 1500 nm. La fenêtre 850nm est réservée pour des courtes distances avec des LED [24].

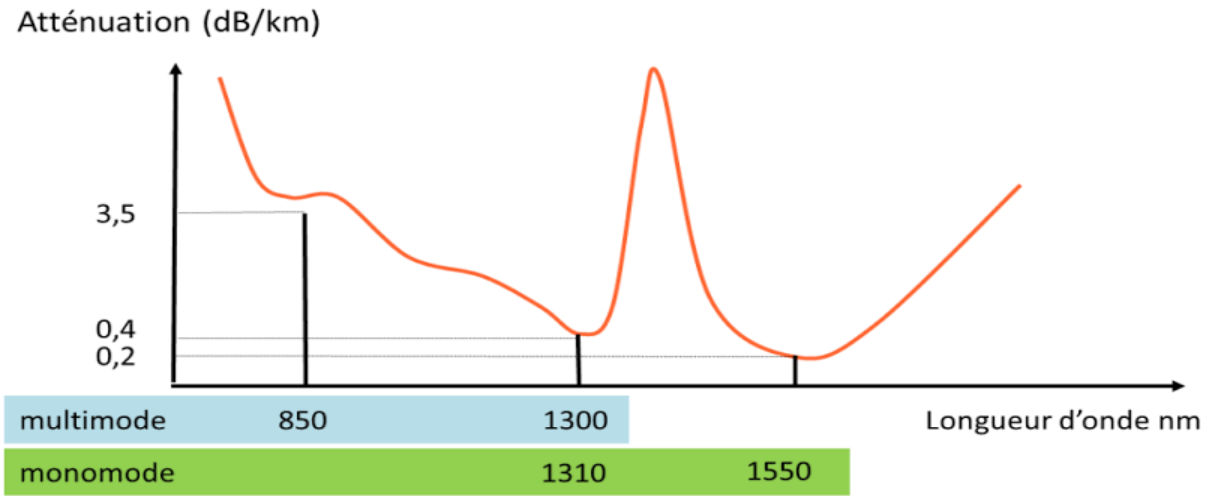

Figure III.5 : Phénomène d'atténuation dans une fibre optique.

b. Dispersion :

Quand on veut transmettre une impulsion sur une fibre optique, on produit l'impulsion avec un émetteur laser. Cette impulsion n'est pas idéale car elle présente une durée dans le temps. Dans une transmission idéale, on espère avoir à la sortie la même impulsion, mais cette impulsion a une durée plus grande que la durée initiale [24].

Il y a plusieurs causes pouvant expliquer ce phénomène :

a. Dispersion chromatique.

b. Dispersion intermodale.

Figure III.6 : La dispersion d'une fibre optique.

III.6 Les critères de qualités d'une transmission optique :

Pour évaluer les performances d'un système de transmission optique, il est nécessaire de disposer de trois critères de qualité qui sont : le diagramme de l'œil, le taux d'erreur binaire et le facteur de qualité.

III.6.1 Taux d'erreur binaire :

Le TEB (Taux d'Erreur Binaire) est un paramètre clé utilisé pour évaluer les systèmes qui transmettent des données numériques d'un emplacement à un autre, Il est utilisé dans les télécommunications, les réseaux et les systèmes radio pour caractériser un canal transportant des données.

Comme son nom l'indique TEB (ou Bit-Error Rate BER en anglais) est défini comme étant le taux auquel les erreurs se produisent dans un système de transmission. Ceci peut être traduit directement par le nombre d'erreur qui se produisent dans un train d'un nombre déterminé de bits. La définition du taux d'erreur binaire peut être traduite en une formule simple :

$$TEB = \frac{Nombre\ de\ bits\ erronés}{Nombre\ de\ bits\ transmis} \qquad \text{(III.1)}$$

III.6.2 Facteur de qualité (Q) :

Le facteur de qualité est un paramètre qui permet l'estimation du taux d'erreur binaire sans avoir à mesurer les erreurs. Il représente le rapport signal sur bruit électrique en entrée du circuit de décision du récepteur. Sachant que le rapport signal sur bruit du récepteur d'un système de transmission par fibre optique a un impact direct sur les performances du système [25].

Le facteur de qualité est souvent utilisé plutôt que le taux d'erreur binaire dès lors que ce dernier est trop faible pour être mesuré. Il est exprimé comme suit :

$$Q = \frac{\mu_1 - \mu_2}{\sigma_1 - \sigma_2} \qquad \text{(III.2)}$$

Où μ_1 et μ_2 sont respectivement les tensions moyennes des symboles «1» et «0», $\sigma_1$et σ_2 sont les variances des probabilités de puissance des symboles «1» et «0» [26].

Partie pratique : *Simulation sur logiciel Optisystem.*

III.7 Présentation du logiciel :

La conception et l'analyse des systèmes de communications optiques nécessitent des dispositifs non-linéaires et des sources de bruit non gaussiennes qui sont complexes et couteux, d'où la nécessité d'utiliser un logiciel performant est indispensable afin d'effectuer les taches rapidement et efficacement.

Il s'agit du logiciel Optisystem version 2019 qui a été développé par une société canadienne Optiwave (Optical Communication System Design Software), est un logiciel innovant permettant de tester et optimiser pratiquement n'importe quel type de liaison optique réelle, en plus de sa riche bibliothèque et ces capacités permettant d'introduire les différents paramètres de simulation [27].

Les composantes principales utilisées dans notre simulation sont les suivants :

- ***Générateur de séquence binaire :***

PRBS (pseudo-Random Bit Sequence Generator) est utilisé pour former et générer des séquences binaires de 0 et1. Dans la simulation optique, la séquence de bits pseudo-aléatoire est utilisée à la place d'un signal numérique à transmettre dans le réseau.

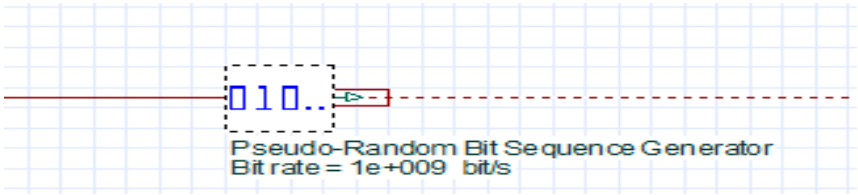

Figure III.7 : Modèle de simulation d'un générateur de séquence binaire.

- ***Générateur NRZ :***

Le générateur d'impulsion NRZ génère un signal électrique codé sans retour à zéro qui dépend d'une entrée de séquence de bits. Nous allons connecter un générateur de séquence de bits défini par l'utilisateur a son entrée. Son modèle de simulation est représenté dans la figure III.8 :

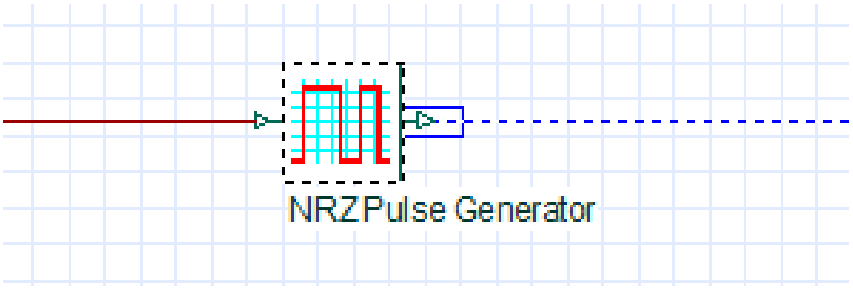

Figure III.8 : Modèle de simulation d'un générateur NRZ.

- ***Diode laser :***

C'est une source de lumière constante et non modulée. Les paramètres d'entrée clés incluent la fréquence centrale, la puissance de sortie. Son modèle de simulation est représenté dans la figure III.9 :

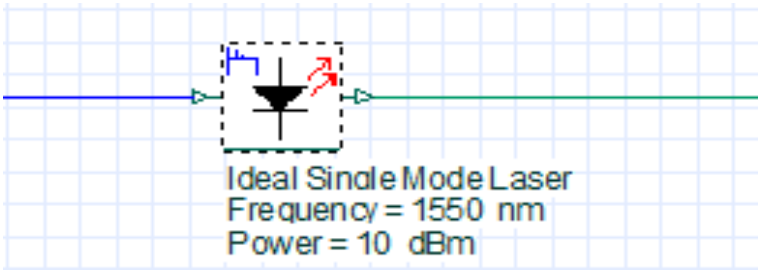

Figure III.9 : Modèle de simulation de la diode laser.

- ***Photodiode PIN :***

Est un modèle utilisée en réception du signal optique (récepteur optique) qui convertit la puissance optique en courant électrique. Son modèle de simulation est représenté dans la figure III.10 :

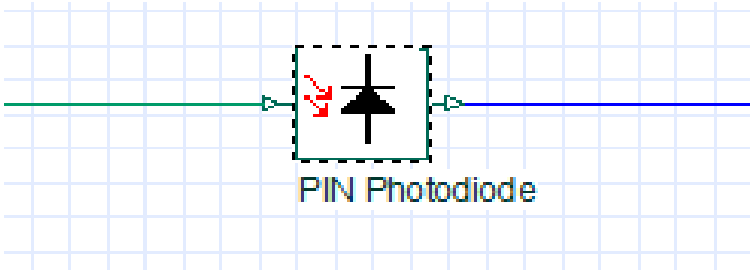

Figure III.10 : Modèle de simulation d'une photodiode PIN.

- ***Filtre passe bas :***

Cet équipement utilisé pour filtrer le signal et pour limiter le signal en bande de base.

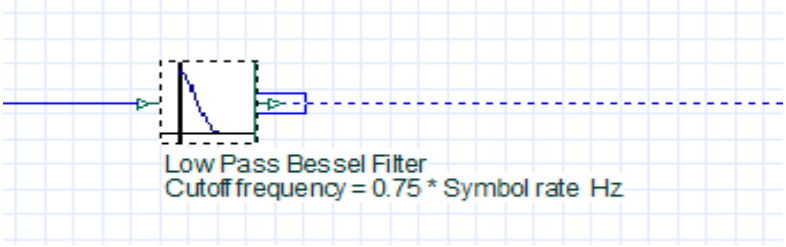

Figure III.11 : Modèle de simulation filtre passe bas Bessel.

- ***Analyseur de BER :***

Le modèle utilisé pour visualiser le résultat obtenue à la réception.

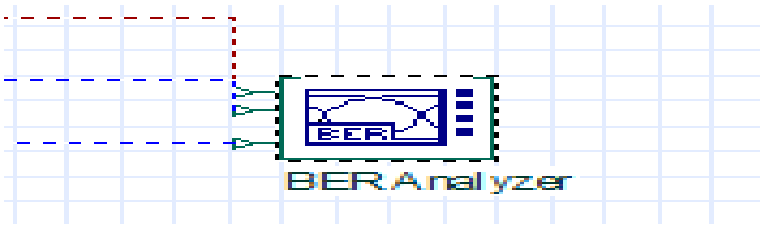

Figure III.12 : Modèle de simulation d'un analyseur de BER.

- ***Fibre optique :***

Pour la transmission, nous utilisons la fibre optique. Son modèle de simulation est représenté dans la figure III.13 :

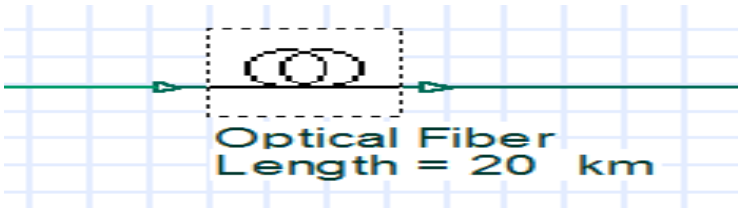

Figure III.13 : Modèle de simulation d'une fibre optique.

- ***Atténuateur optique :***

L'atténuateur optique est un équipement qui s'ajoute à la source laser afin d'obtenir des photons uniques qui sont utilisés dans la cryptographie quantique. Son modèle de simulation est représenté dans la figure III.14 :

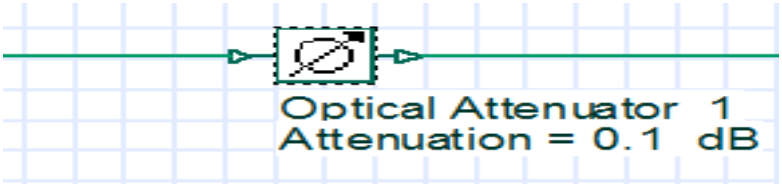

Figure III.14 : Modèle de simulation d'un atténuateur optique.

- ***Le polariseur linéaire :***

Son but est de polariser linéairement la lumière entrante selon un angle. Son modèle de simulation est représenté dans la figure III.15 :

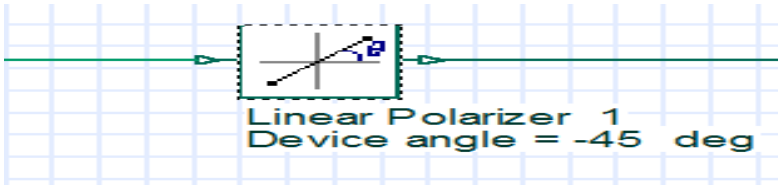

Figure III.15 : Modèle de simulation d'un polariseur linéaire.

- ***Le select :***

Le select est un composant de sélection aléatoire, l'un des signaux entrant dans les ports d'entrée sera envoyé au port de sortie.

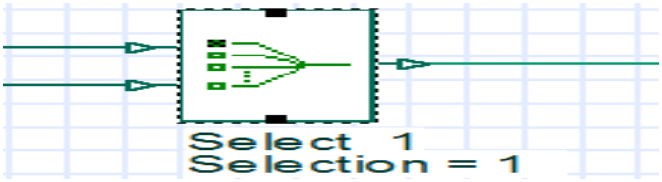

Figure III.16 : Modèle de simulation d'un select.

III.8 Chaine de transmission optique de base :

Un système de télécommunications optique est donné par le synoptique d'une chaine de transmission de base (plus générale et plus simple possible), tel qu'il est illustré sur la figure III.17 :

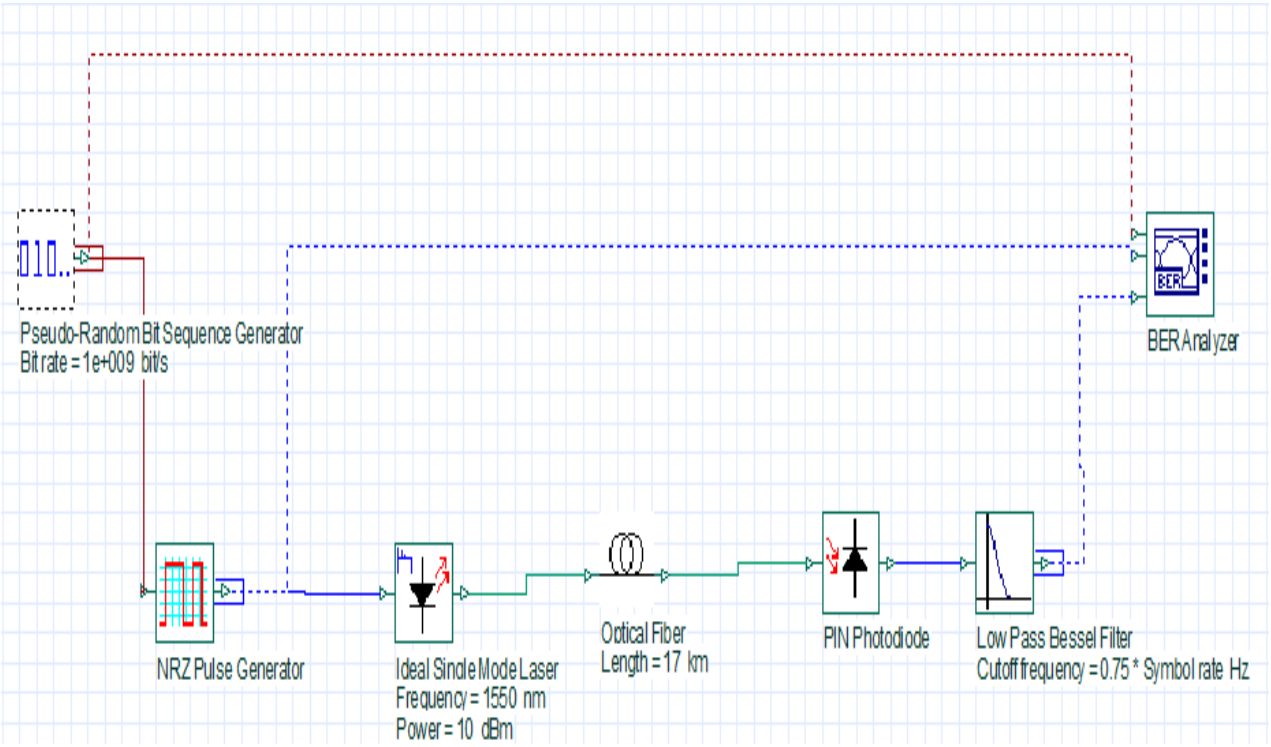

Figure III.17 : Synoptique d'une chaine de transmission de base.

III.8.1 Simulation de la chaine de base :

Nous avons évalué les performances de la liaison optique en utilisant le facteur de qualité (Q) et le taux d'erreur (BER).

La simulation de cette chaine pour un débit de 2,5Gbit/s donne le résultat suivant :

Distance :	**BER :**	**Facteur de qualité :**
17Km	$3{,}10399e^{-286}$	36,1351

Tableau III .1 : Les résultats du taux d'erreur et du facteur de qualité d'une chaine de base.

➢ **Commentaire :**

D'après la simulation de la chaine optique de base, on a obtenu un facteur de qualité égale à 36,1351 et un taux d'erreur binaire égale à $3{,}10399^{e\text{-}286}$ pour un débit de 2,5Gbit/s et une distance de 17km. Ces valeurs décrivent la qualité de transmission d'une chaine de base.

III.9 Etude de la qualité de transmission du protocole BB84 dans une liaison optique :

Nous allons simuler le protocole BB84 à quatre états (0° 45° 90° -45°), tel qu'il est représenté sur la figure III.18, en envoyant une séquence de bits à travers l'équipement PRBS suivie d'un générateur NRZ qui génère des impulsions qui seront injectées dans la diode laser qui est une source de lumière (photon) auquel on ajoute un atténuateur optique, afin d'avoir des photons uniques.

Ce dernier est relié à un polariseur linéaire. Ces quatre états seront rassemblés grâce au « select » qui sera ensuite transmises à travers la fibre, un autre select est ajouté au niveau du récepteur qui va choisir au hasard l'un des signaux envoyés qui sera enfin détecté par la photodiode PIN puis on visualise la simulation sur le BER analyseur.

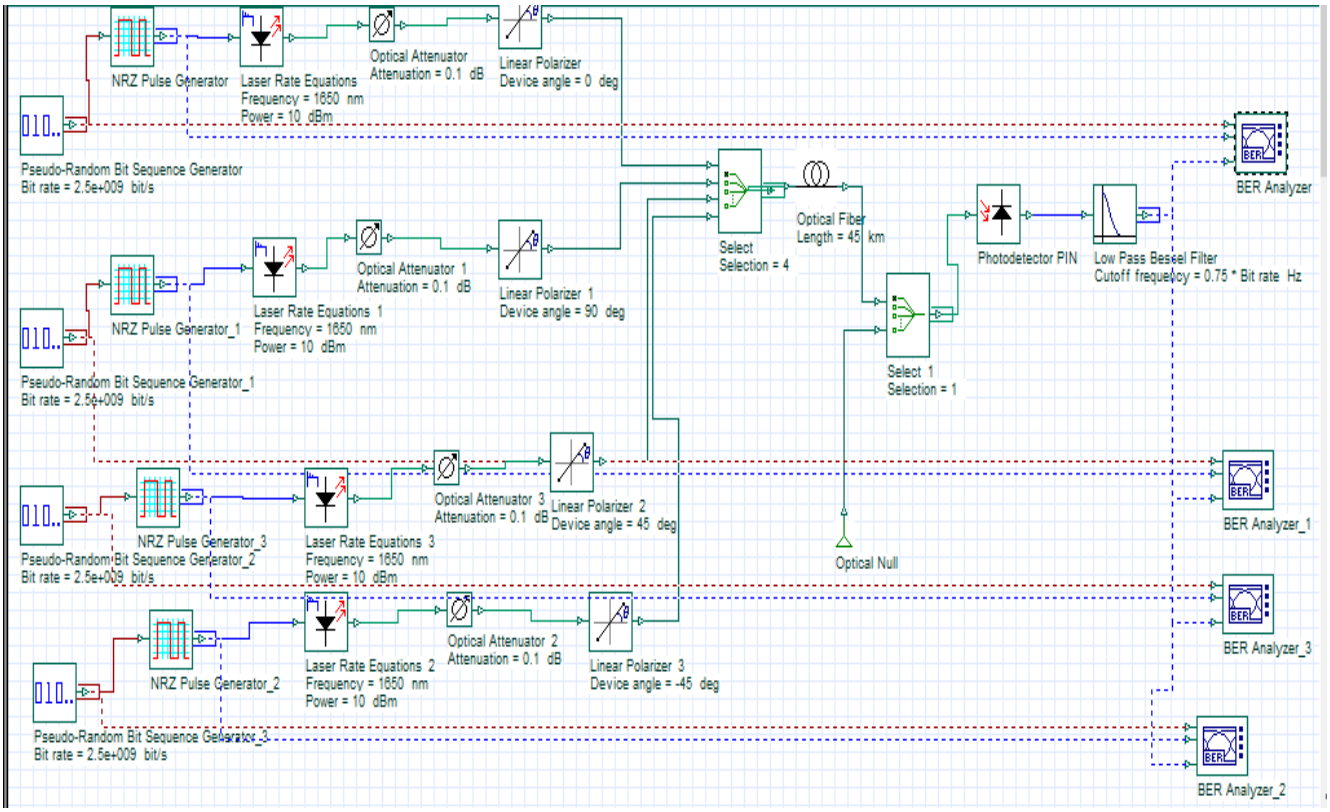

Figure III.18 : Synoptique d'une chaine de transmission avec le protocole BB84 [28].

Pour voir le comportement du protocole BB84, on a simulé cette chaine avec les mêmes paramètres de distance et débit de la chaine de base, on a obtenu les résultats suivants :

Facteur de qualité :	40,1288
BER :	2,11027 e^{-319}

Tableau III .2: Les résultats du taux d'erreur et du facteur de qualité d'une chaine avec BB84.

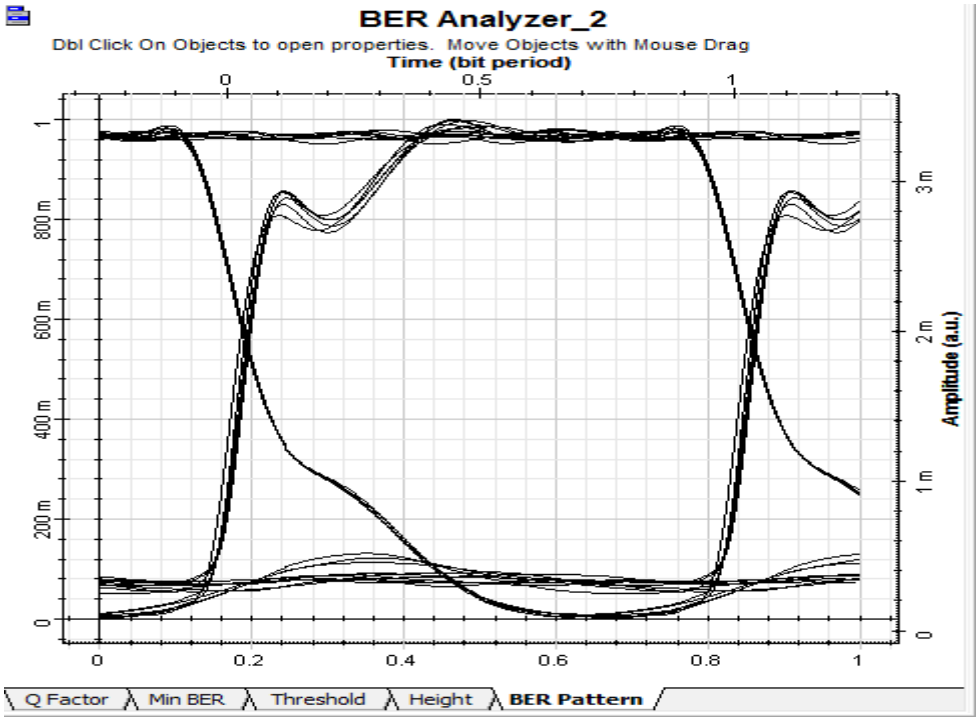

Figure III.19 : Diagramme de l'œil pour une distance de 17Km.

➢ **Commentaire :**

A partir de la simulation, on a obtenu 40,1288 comme facteur de qualité et 2,11027 e^{-319} comme taux d'erreur pour un débit de 2.5Gbit/s et une distance de 17 Km sur le BER-Analyzer-2, dans lequel Bob a reçu le photon (Qubit) envoyé par Alice polarisé avec l'angle -45°. Ce qui traduit le bon fonctionnement du protocole BB84.

III.9.1 L'influence des variations de la distance de propagation sur la transmission :

Dans cette partie, nous avons fait varier la distance de propagation de 1 à 50Km en fixant la longueur d'onde à 1550nm et le débit à 2,5Gbit /s, les résultats obtenues sont représentés dans le tableau suivant :

Distance :	***BER :***	***Facteur de qualité :***
1 Km	0	57,1624
5 Km	0	52,4632
10 Km	0	49,7662
15 Km	0	45,0314
20 Km	$9{,}85936\ e^{-298}$	39,8597
25 Km	$5{,}36029\ e^{-293}$	36,5639
30 Km	$2{,}83118\ e^{-283}$	35,9424
35 Km	$3{,}52091\ e^{-277}$	34 ,9914
40 Km	$8{,}13055\ e^{-267}$	33,9712
45 Km	$1{,}94781\ e^{-256}$	30,1801
50 Km	$2{,}2893\ e^{-246}$	28,5015

Tableau III.3 : Résultats de BER et facteur de qualité en fonction de la distance.

A partir des résultats obtenus, nous avons tracé les courbes suivant en fonction de la distance de propagation :

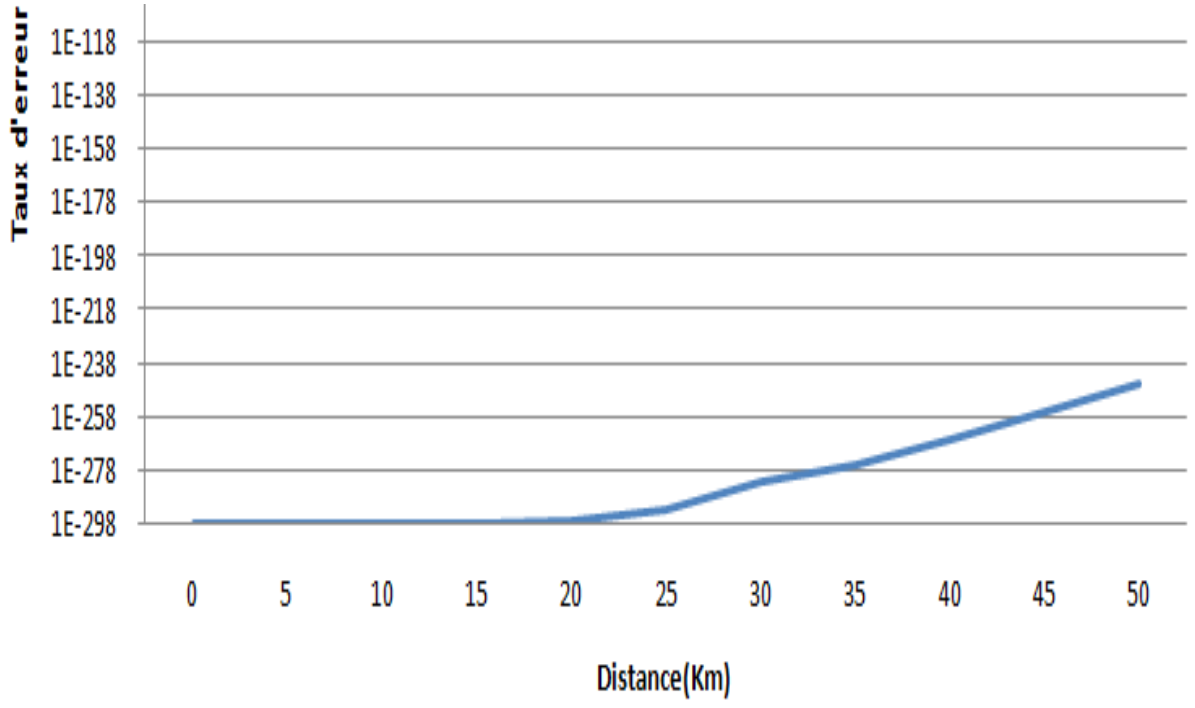

Figure III.20 : Taux d'erreur en fonction de la distance.

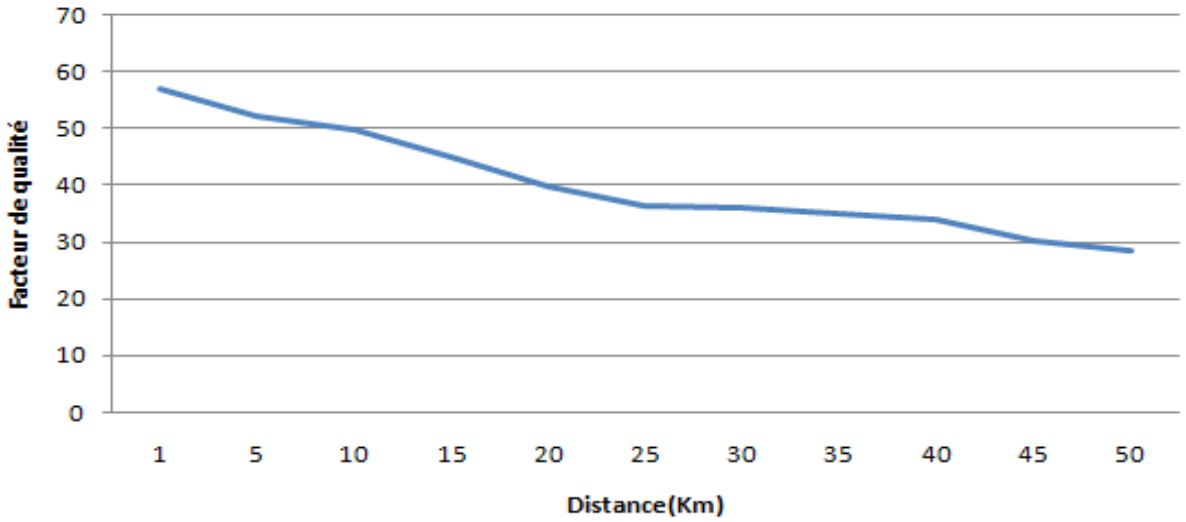

Figure III.21 : facteur de qualité en fonction de la distance.

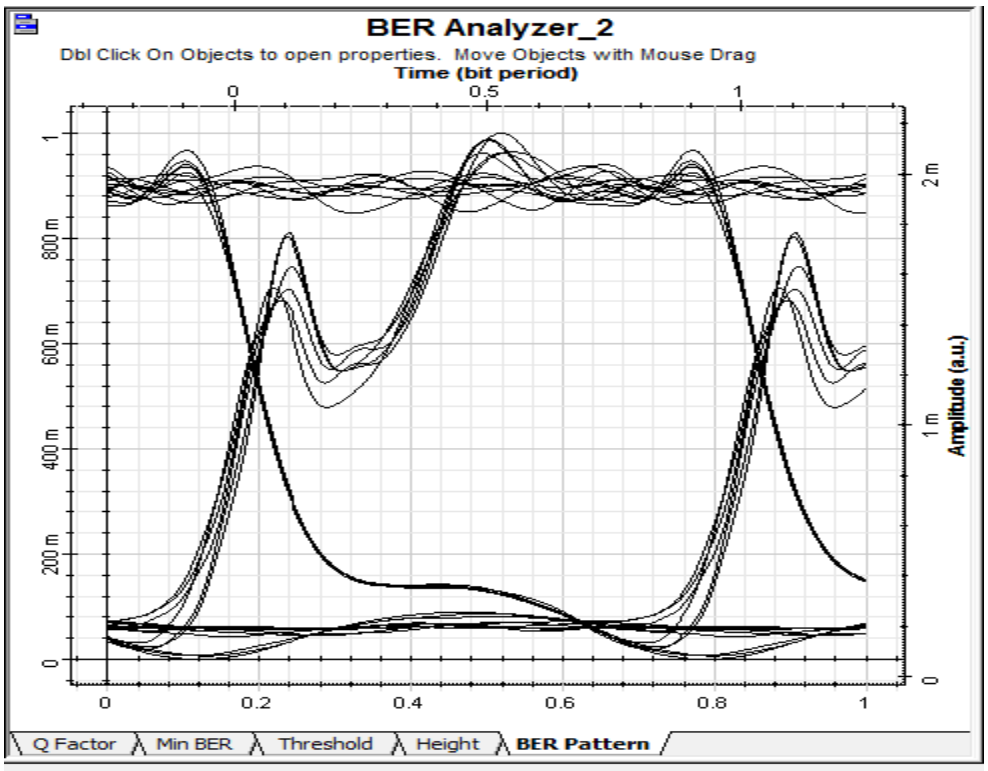

Figure III.22 : Diagramme de l'œil pour une distance de 50Km.

➢ **Commentaire :**

D'après les résultats obtenus, nous remarquons qu'à chaque fois la longueur de la fibre augmente, la qualité de transmission diminue d'où le taux d'erreur augmente plus en plus et le facteur de qualité diminue.

Selon les normes internationales, cette dégradation reste acceptable pour des valeurs de BER inférieur à 10^{-9} et facteur de qualité supérieur à 6 [28].

III.9.2 L'influence des variations de la longueur d'onde sur la transmission :

Pour cette étape, nous avons varié la longueur d'onde de la fibre pour un débit de 2.5Gbit/s et une distance de 17Km.

Nous avons obtenus les résultats présentés dans le tableau ci-dessous :

Longueur d'onde :	**BER :**	**Facteur de qualité :**
900 nm	1	0
1300 nm	1,30533 e^{-208}	30,7994
1450 nm	1,59515 e^{-295}	36,7197
1550 nm	2,11027 e^{-319}	40,1288
1650 nm	0	47,6136

Tableau III.4 : Résultats de BER et facteur de qualité en fonction de la longueur d'onde.

Avec les résultats obtenus, nous avons tracé les courbes suivantes :

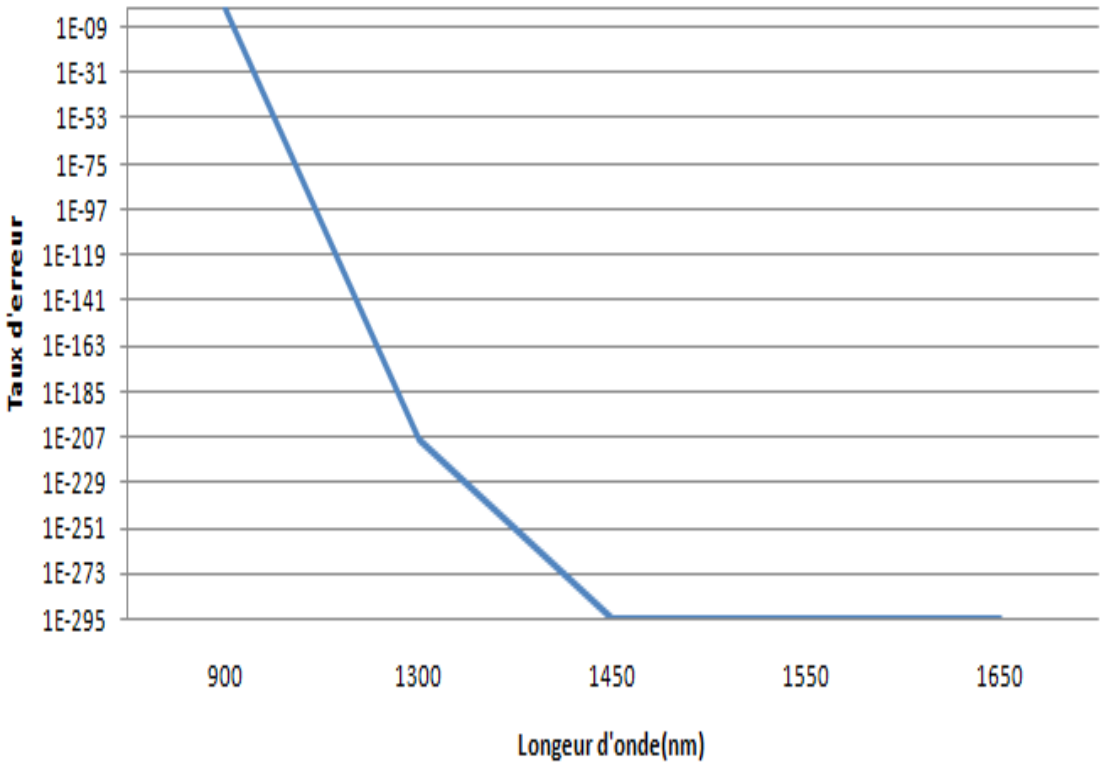

Figure III.23 : Taux d'erreur binaire en fonction de la longueur d'onde.

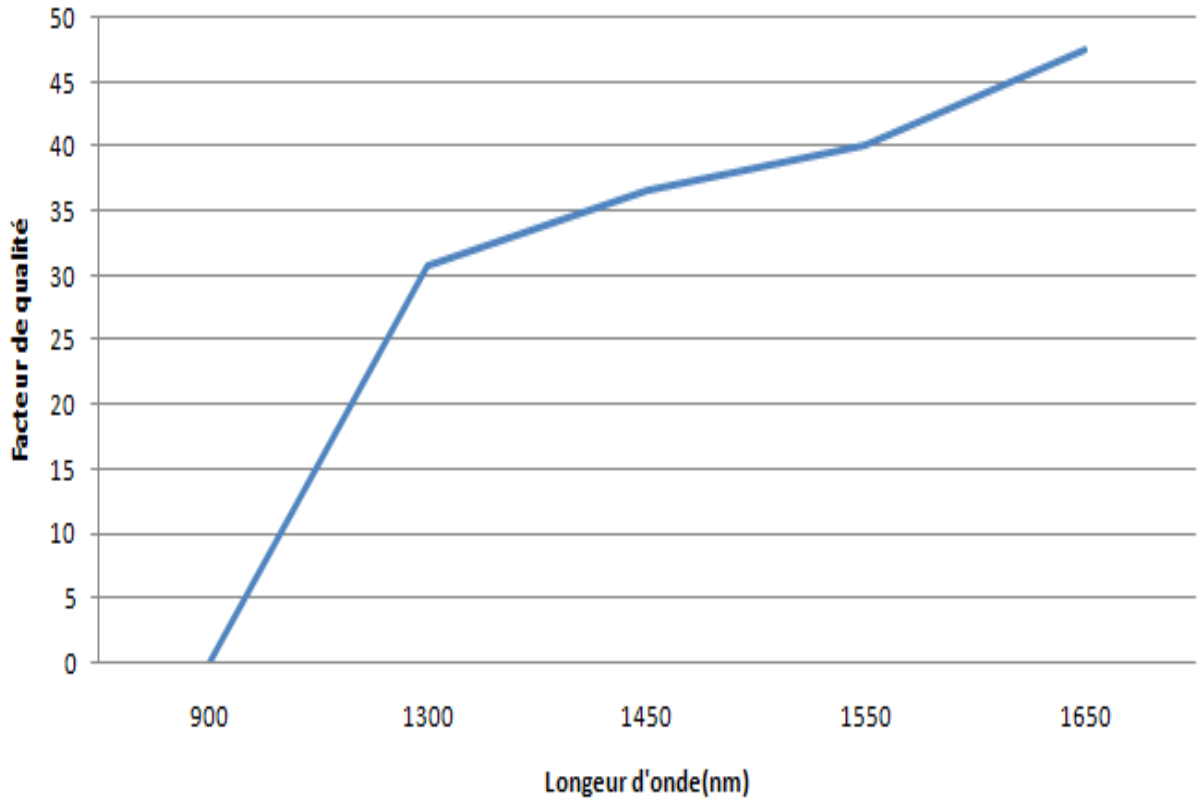

Figure III.24 : Facteur de qualité en fonction de la longueur d'onde.

➢ **Commentaire :**

D'après cette courbe, nous remarquons que la qualité de transmission augmente avec l'augmentation de la longueur d'onde d'où le taux d'erreur diminue .On distingue pour les 3 fenêtres :

- **La première fenêtre (900nm) :** est la mauvaise fenêtre car le taux d'erreur est trop élevé et supérieur à 10^{-9} d'où l'erreur devient inacceptable.
- **La deuxième fenêtre (1300nm) :** reste acceptable car les valeurs du TEB (taux d'erreur binaire) et le facteur de qualité satisfont les normes internationales.
- **Les troisièmes fenêtres (1450 à 1650nm) :** est la meilleure fenêtre grâce au taux d'erreur qui est plus faible et la qualité de transmission qui est amélioré car elle présente le minimum d'atténuation et une dispersion minimale.

III.9.3 L'effet d'un espion sur la transmission :

Dans cette simulation, nous allons simuler une chaine de transmission avec le protocole BB84 avec attaque afin d'étudier l'effet de l'espion (Eve) pour un débit de 2,5Gbit/s et une distance de 17Km.

Eve dispose d'une infrastructure comme celle de l'émetteur (Alice), qui se base sur la stratégie 'intercept-resend'. Eve est connectée entre Alice et Bob, il peut intercepter les qubits entrants et les mesurer avec des polariseurs rectiligne, déphasage ou rotateurs de photons, puis les envoyer après leurs modifications ou bien les retransmettre tels qu'ils sont vers Bob.

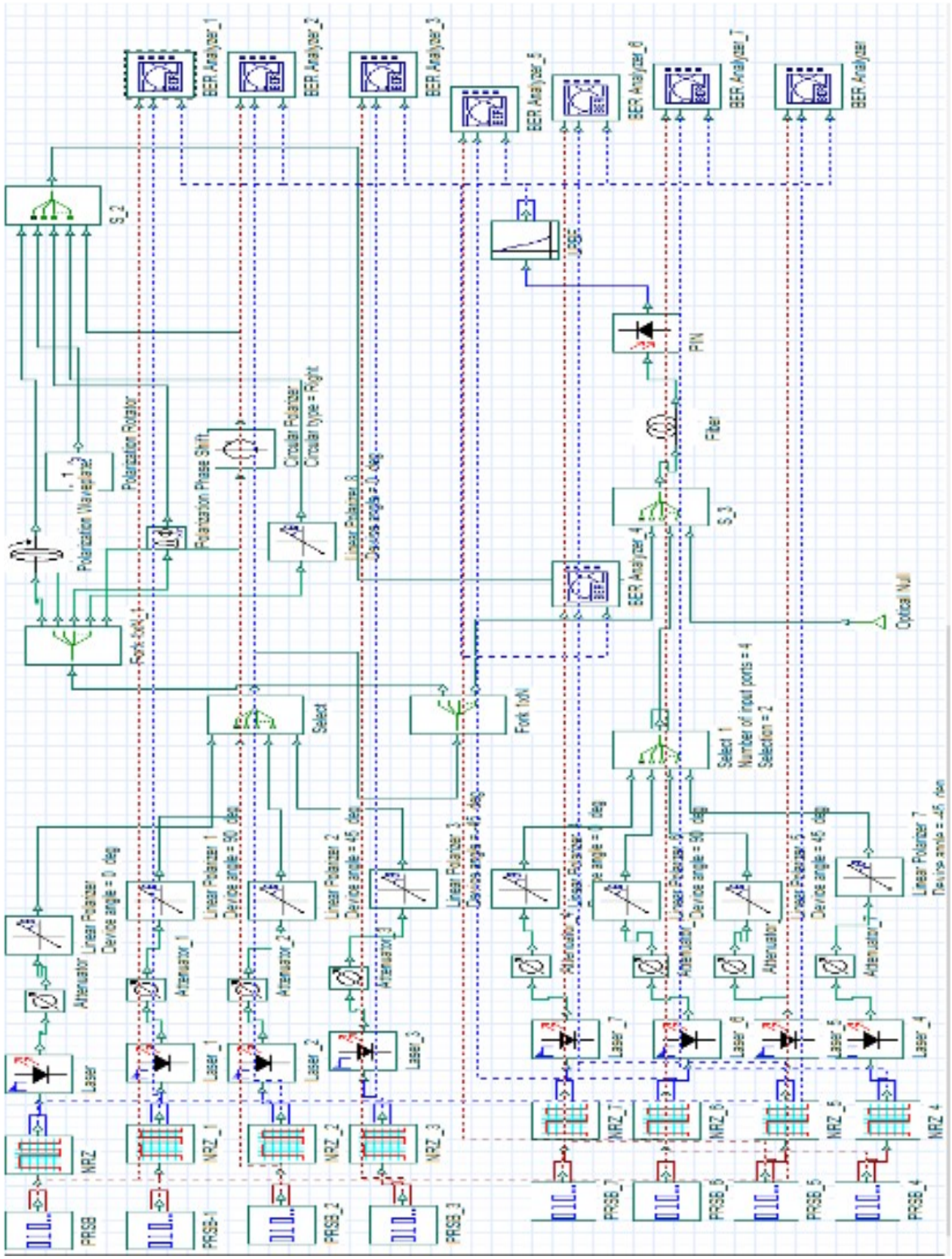

Figure III.25 : Synoptique d'une chaine de transmission avec le protocole BB84 en présence d'espion [28].

Les résultats obtenus sont représentés dans le tableau suivant :

Facteur de qualité :	38,452
BER :	1,81569 e^{-306}

Tableau III.5 : Les résultats du BER et facteur de qualité dans une chaine optique avec BB84 en présence d'espion.

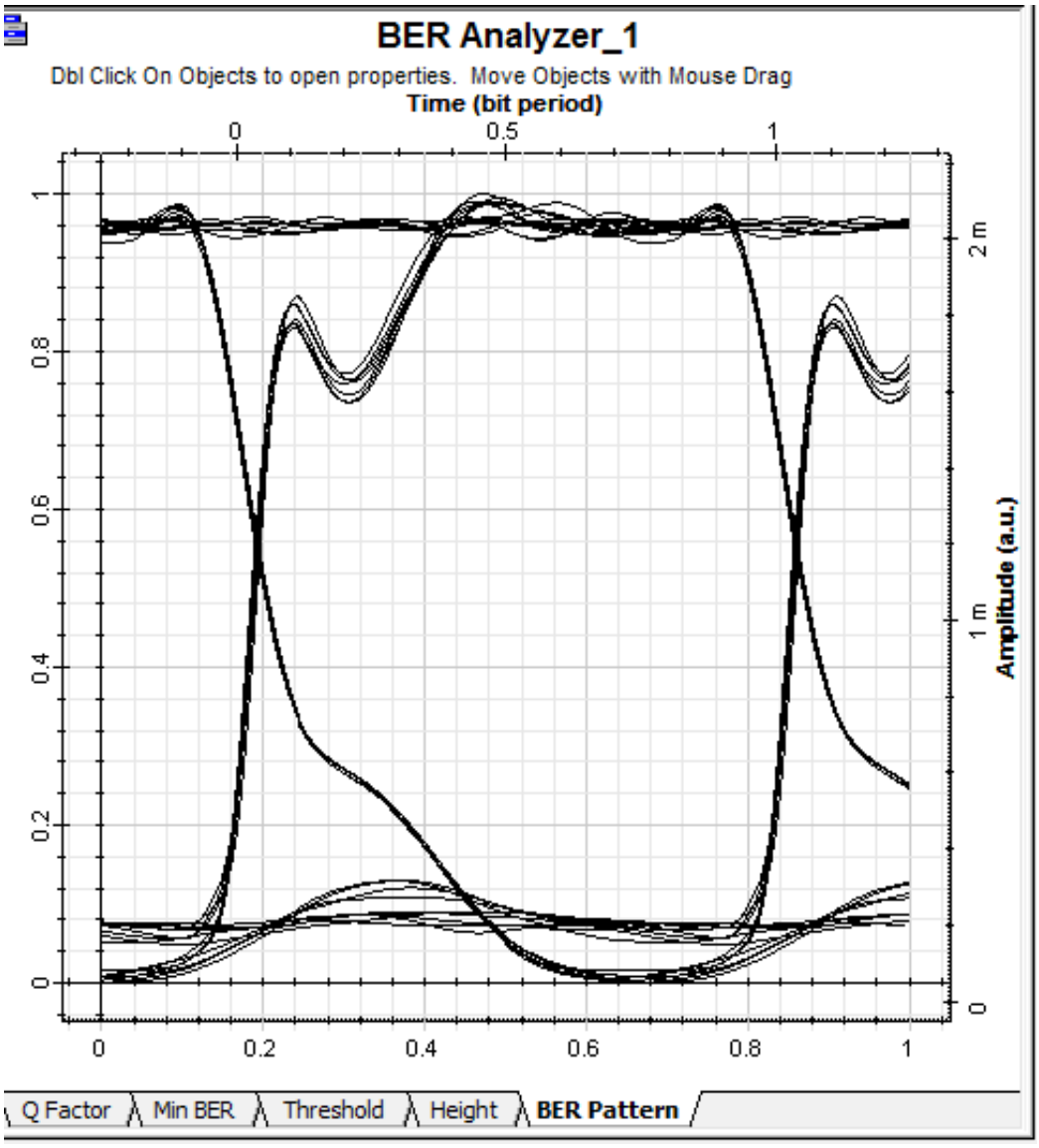

Figure III.26 : Diagramme d'œil pour une distance 17 Km en présence d'espion.

➢ **Commentaire :**

D'après les résultats, on a obtenus un taux d'erreur de1, 81569 e^{-306} et un facteur de qualité de 38, 452 pour un débit de 2.5Gbit/s et une distance de 17Km, ce qui montre l'influence de la présence d'espion sur la chaine de transmission avec BB84 d'où la qualité de transmission diminue.

III.9.3.1 Influence de la distance en présence de l'espion :

Dans cette partie, nous avons fait varier la distance de propagation de 1 à 50Km en utilisant un débit de 2.5Gbit/s et une longueur d'onde de 1550nm afin de faire une comparaison avec les résultats obtenus en absence d'espion. Les résultats obtenus sont représentés dans le tableau suivant :

Distance :	**BER :**	**Facteur de qualité :**
1 Km	0	51,5653
5 Km	0	49,551
10 Km	0	44,3251
15 Km	0	41,162
20 Km	$6{,}80987\ e^{-293}$	37,5543
25 Km	$1{,}92076\ e^{-275}$	35,2462
30 Km	$3{,}76958\ e^{-266}$	34,8305
35 Km	$4{,}67802\ e^{-245}$	32,6259
40 Km	$2{,}0244\ e^{-221}$	31,7306
45 Km	$1{,}33165\ e^{-190}$	29,4218
50 Km	$2{,}27056\ e^{-151}$	26,1744

Tableau III.6 : Les résultats du BER et facteur de qualité en fonction de la distance avec espion.

Avec les résultats obtenus, nous avons tracé les courbes ci –dessous :

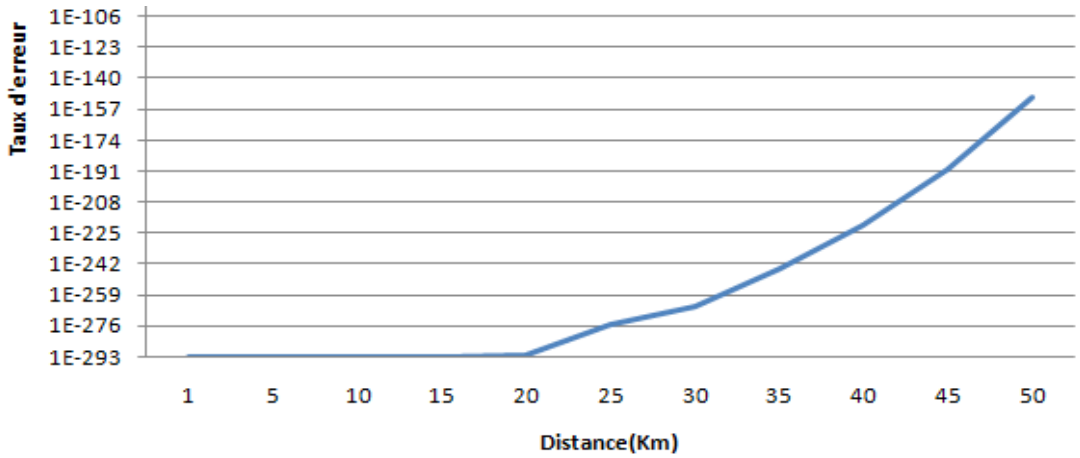

Figure III.27 : Taux d'erreur en fonction de la distance en présence d'espion.

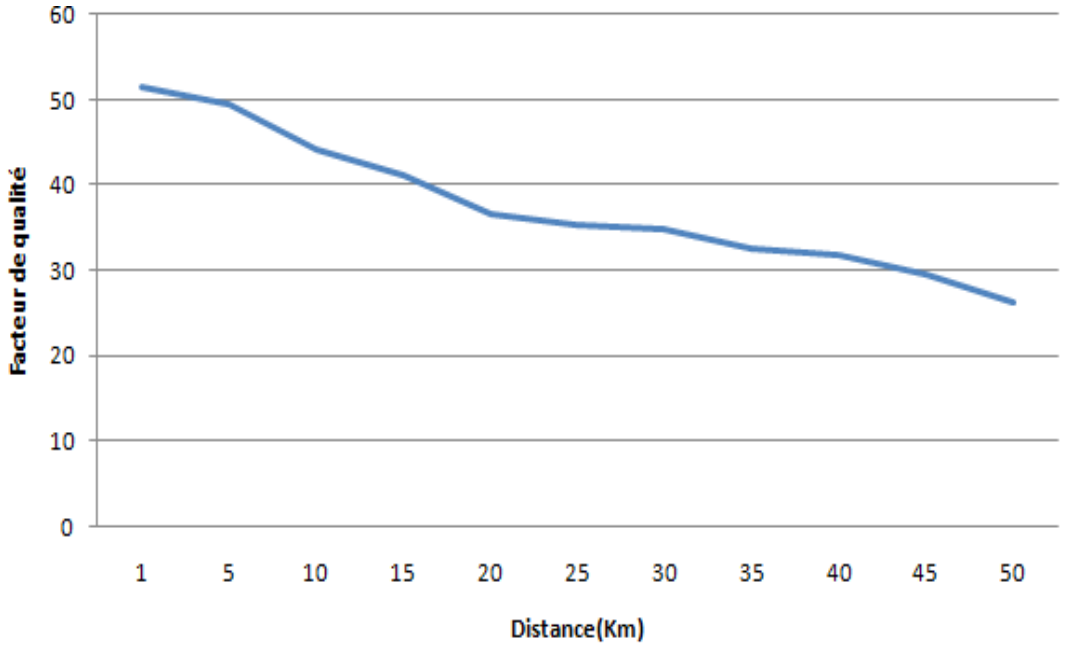

Figure III.28 : facteur de qualité en fonction de la distance en présence d'espion.

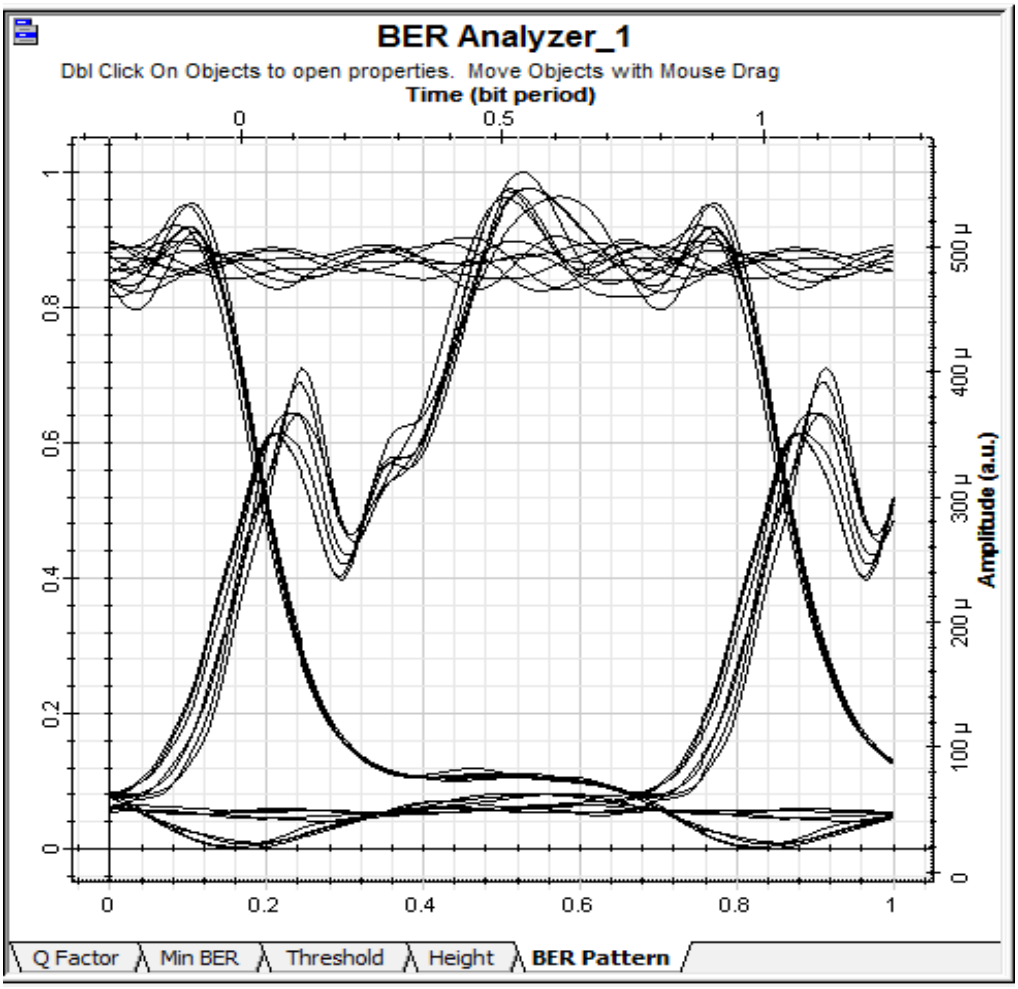

Figure III.29 : Diagramme de l'œil pour une distance de 50Km avec attaque.

Afin de bien voir la différence entre la présence d'espion et son absence, nous avons tracé les courbes suivantes :

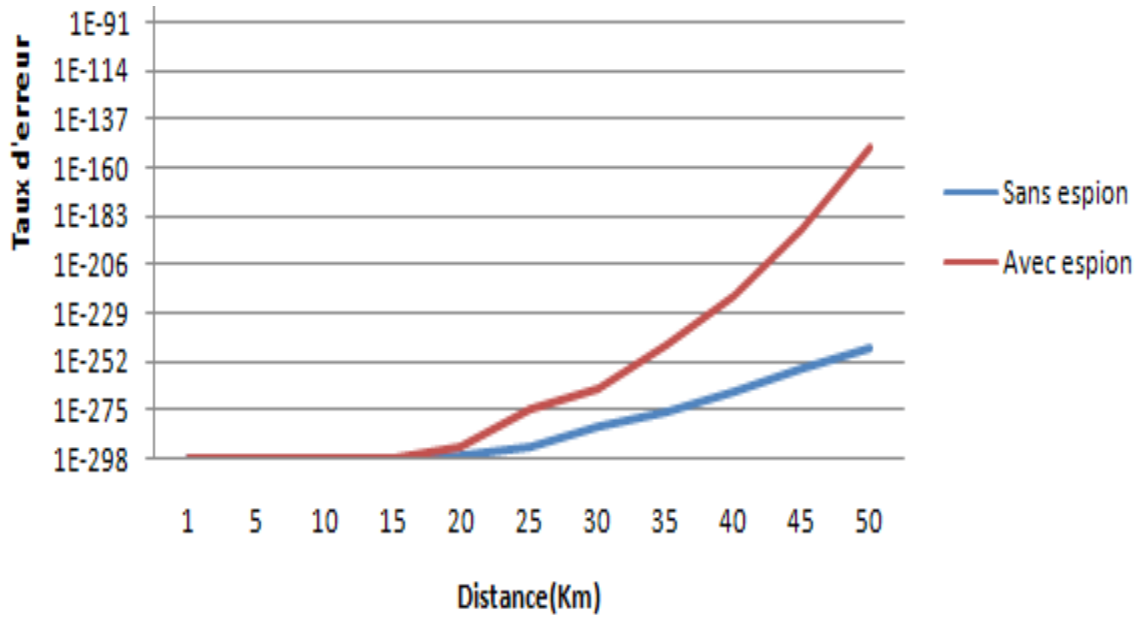

Figure III.30 : Taux D'erreur en fonction de la distance en présence et en absence d'espion.

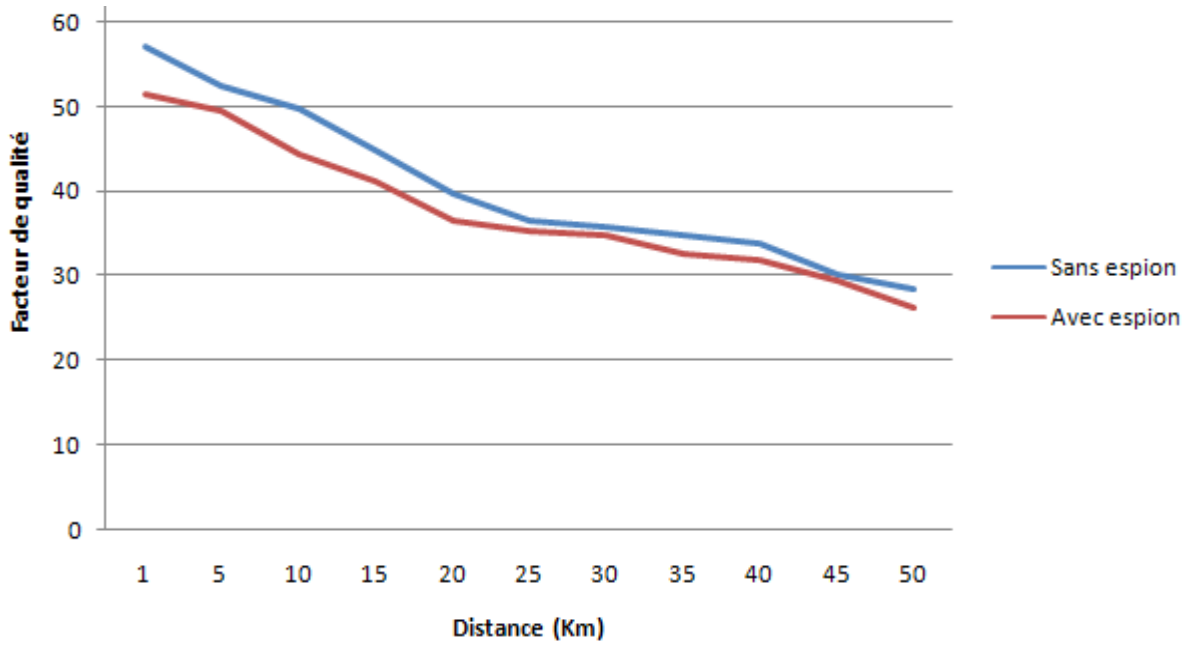

Figure III.31 : Facteur de qualité en fonction de la distance en présence et en absence d'espion.

- **Commentaire :**

D'après les résultats obtenus, nous voyons bien que le taux d'erreur croit avec l'augmentation de la longueur de la fibre ce qui entraine une diminution du facteur de qualité,

mais en comparant nos résultats aux valeurs obtenus en absence d'espion, on remarque que le BER augmente plus qu'en présence d'espion d'où il peut arriver à des valeurs inacceptable à cause des capacités de l'espion d'intercepter l'information transmise entre Alice et Bob ce qui veut dire : perturbation, perte et retard…etc.

III.9.3.2 L'influence des variations de la longueur d'onde sur la transmission :

Dans cette simulation, nous avons fait varier la longueur d'onde en fixant les mêmes paramètres utilisés en absence d'espion afin de faire une comparaison entre eux.

Nous avons obtenus les résultats représentés dans le tableau ci-dessous :

Longueur d'onde :	BER :	Facteur de qualité :
900 nm	1	0
1300 nm	5,20204 e^{-191}	29,4558
1450 nm	5,64106 e^{-282}	35,856
1550 nm	1,81569 e^{-306}	38,452
1650 nm	7,50511 e^{-311}	39,6684

Tableau III.7 : Les résultats du BER et facteur de qualité en fonction de la longueur d'onde avec espion.

A travers les résultats obtenus, nous avons tracé les courbes suivantes :

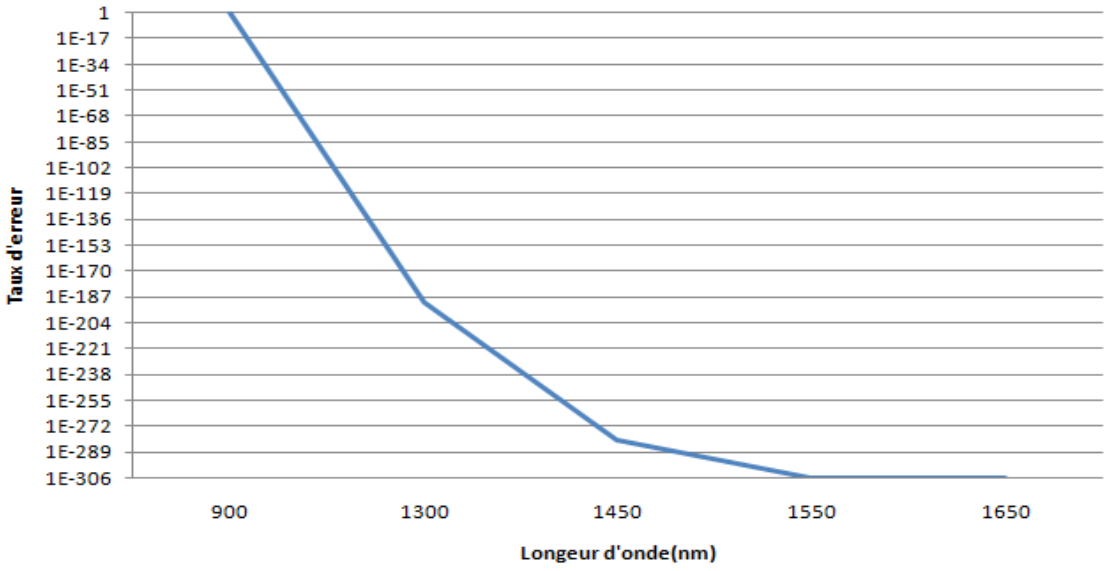

Figure II.32 : Taux d'erreur en fonction de la longueur d'onde en présence d'espion.

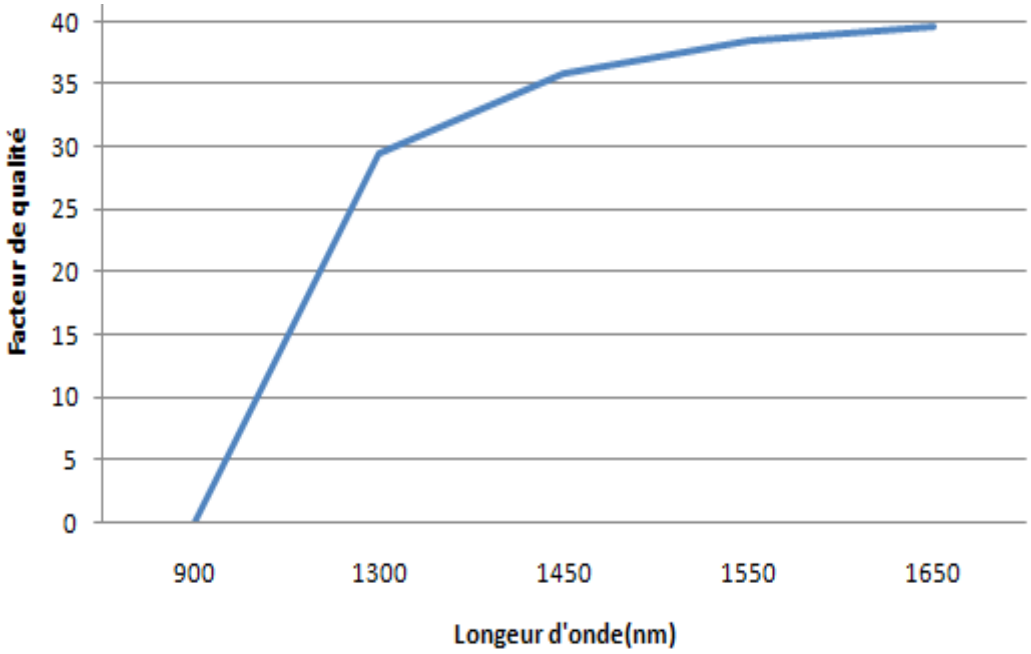

Figure III.33 : facteur de qualité en fonction de la longueur d'onde en présence d'espion.

Afin de comparer les résultats obtenus en présence d'espion et son absence, nous avons tracé les courbes suivantes :

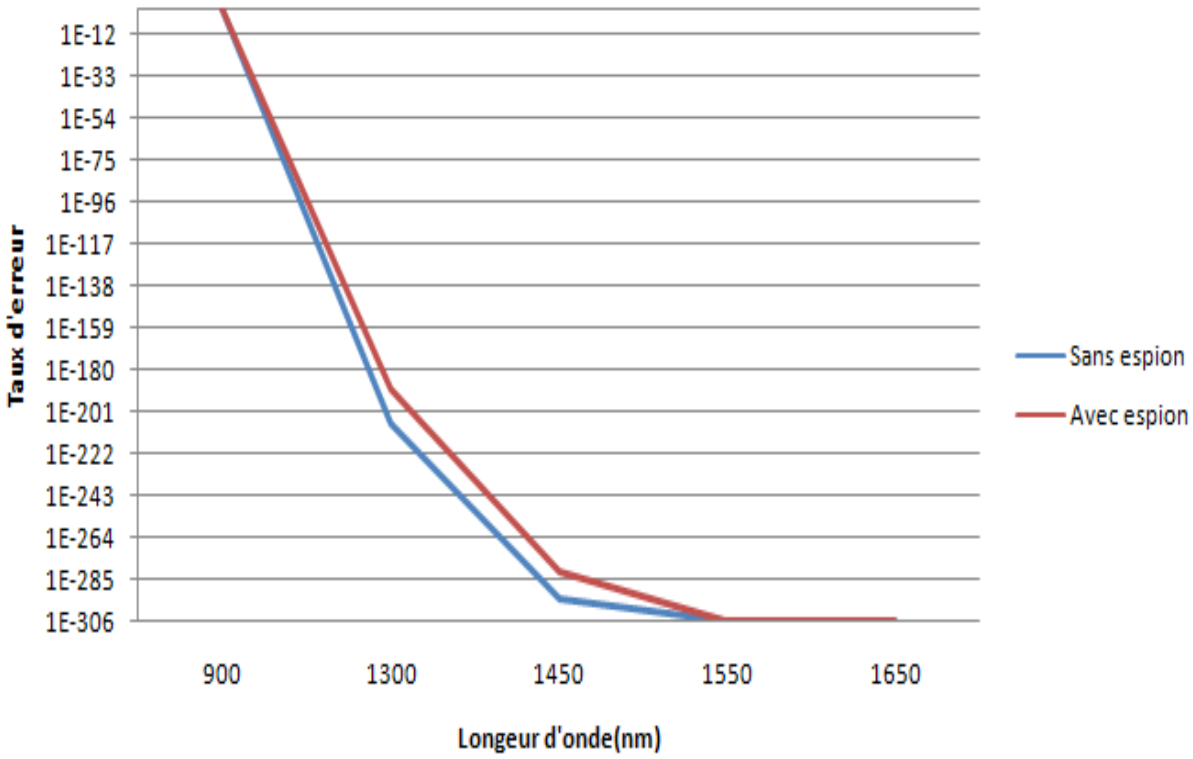

Figure III.34 : Taux d'erreur en fonction de la longueur d'onde en présence et en absence d'espion.

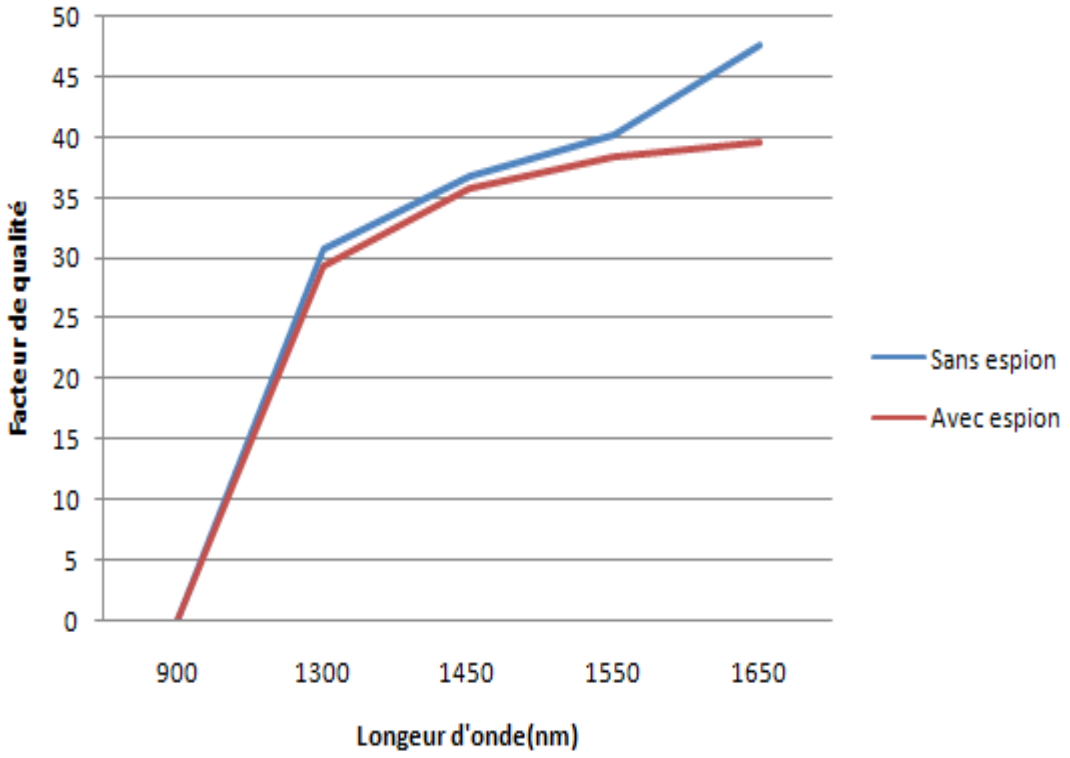

Figure III.35 : Facteur de qualité en fonction de la longueur d'onde en présence et en absence d'espion.

➢ **Commentaire :**

D'après les résultats obtenus de la simulation, nous remarquons que le taux d'erreur diminue avec la croissance de la longueur d'onde ce qui engendre l'augmentation de qualité de signal.

En comparant les résultats obtenus en présence et en absence d'espion, on déduit que la troisième fenêtre est le meilleur choix même si en présence d'espion, mais il est clair que le BER est plus grand en présence d'espion et le facteur de qualité est plus petit.

III.10 Etude de l'effet du protocole B92 sur une liaison optique :

Afin d'évaluer la qualité de transmission, nous avons implémenté le protocole B92 dans une chaine de transmission optique. Nous avons simulé cette dernière en effectuant des mesures sur le taux d'erreur binaire (TEB) et le facteur de qualité (Q) en fonction de la variation des paramètres physique de la fibre optique tels que la distance et la longueur d'onde dans les deux cas suivantes : en présence et en absence d'espion.

Dans cette section, nous allons simuler cette chaine en absence d'espion, tel qu'on l'a effectué précédemment, en utilisant seulement deux états comme est indiqué dans la figure III.36 :

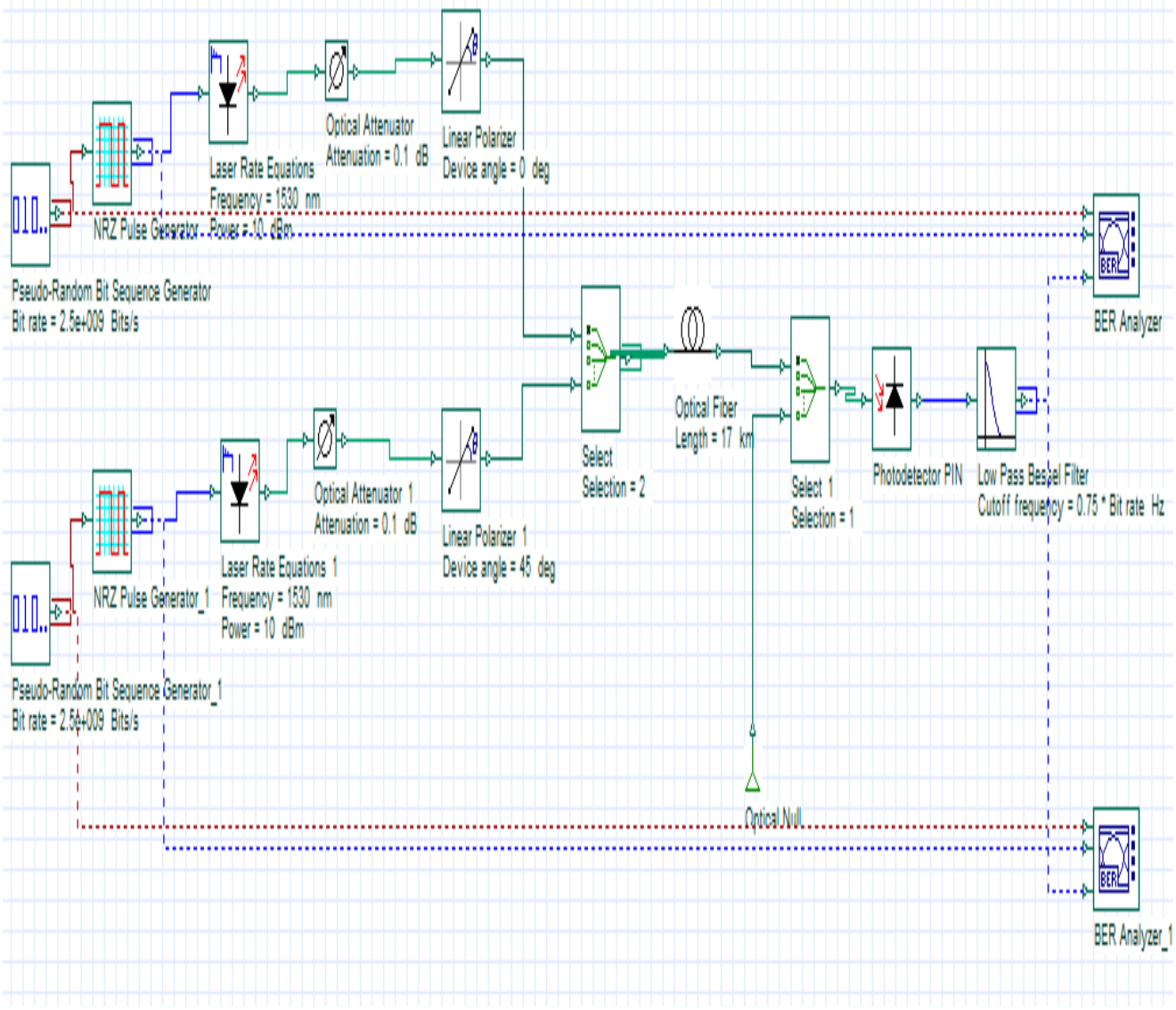

Figure III.36 : Synoptique d'une chaine de transmission avec le protocole B92 [28].

La simulation de ce synoptique d'une chaine de transmission du protocole B92 dans une liaison optique avec les mêmes paramètres (débit de 2.5Gbit/s et une distance de 17km) a donné les résultats suivants :

Facteur de qualité :	39,5042
BER :	4 ,10004e^{-312}

Tableau III .8: Les résultats du taux d'erreur et du facteur de qualité d'une chaine avec B92.

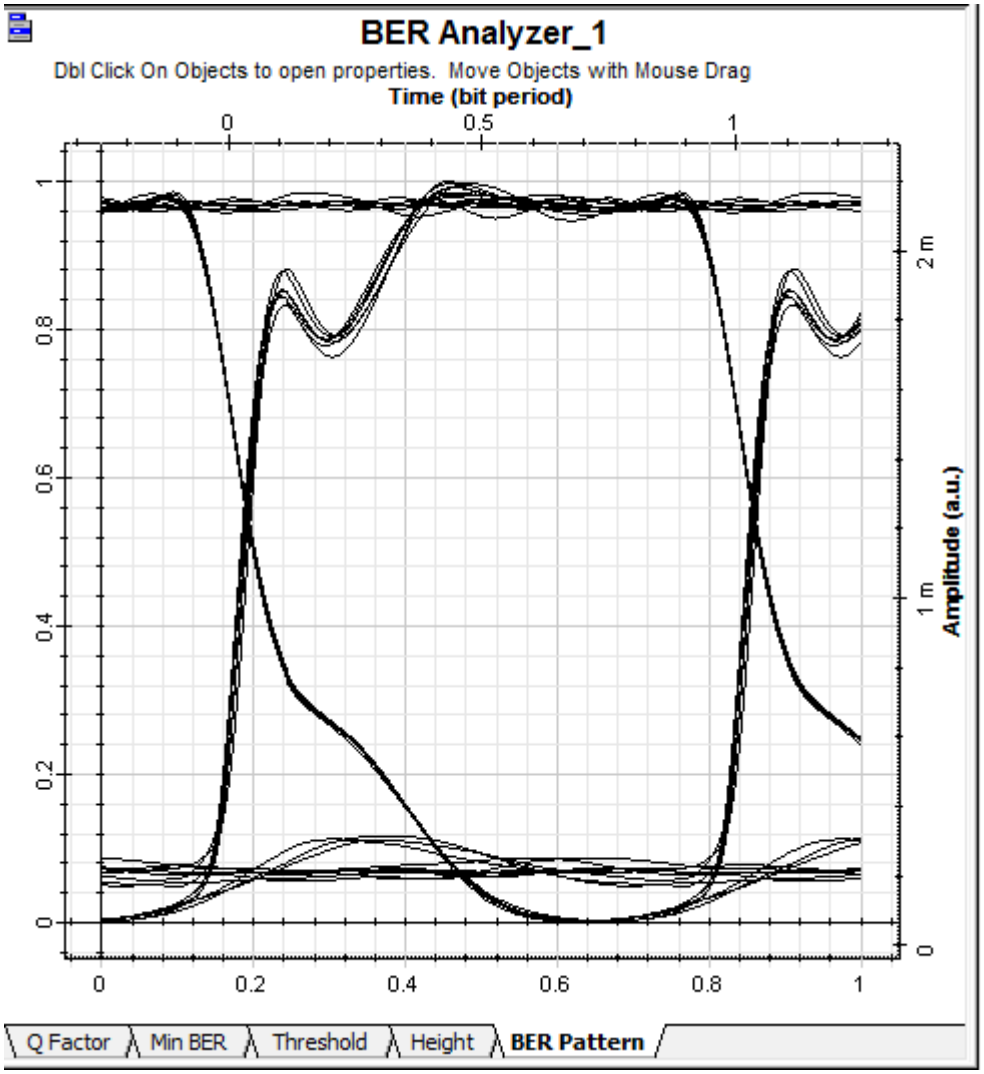

Figure III.37 : Diagramme de l'œil pour une distance de 17Km.

➢ **Commentaire :**

La simulation de la chaine de transmission avec le protocole B92 pour un débit de 2,5Gbit/s et une distance de 17Km a permis d'obtenir les valeurs suivantes : 38,5042 comme facteur de qualité et 4,1000 e^{-312} comme taux d'erreur ,ce qui montre la qualité de transmission du protocole B92 sur la chaine de transmission .

III.10.1 L'influence de la distance de propagation sur la transmission :

Dans cette partie, nous avons fait varier la distance de 1 à 50km pour un débit de 2.5Gbit/s et une longueur d'onde égale 1550nm, Les résultats obtenus sont représentés dans le tableau ci-dessous :

Distance :	***BER :***	***Facteur de qualité :***

1 Km	0	51,3042
5 Km	0	47,0991
10 Km	0	44,4844
15 Km	0	41 ,0623
20 Km	$1{,}62184e^{-288}$	38,2778
25 Km	$5{,}63518\ e^{-275}$	35,9977
30 Km	$1{,}72821\ e^{-259}$	34,8929
35 Km	$1{,}99054e^{-238}$	33,8444
40 Km	$1{,}08434e^{-218}$	31,3096
45 Km	$2,\ 26546\ e^{-202}$	28,0815
50 Km	$3{,}11582\ e^{-187}$	26,5961

Tableau III.9 : Résultats de BER et facteur de qualité en fonction de la distance.

Les résultats du taux d'erreur (BER) et facteur de qualité obtenus en fonction de la distance sont tracés sur les figures suivantes :

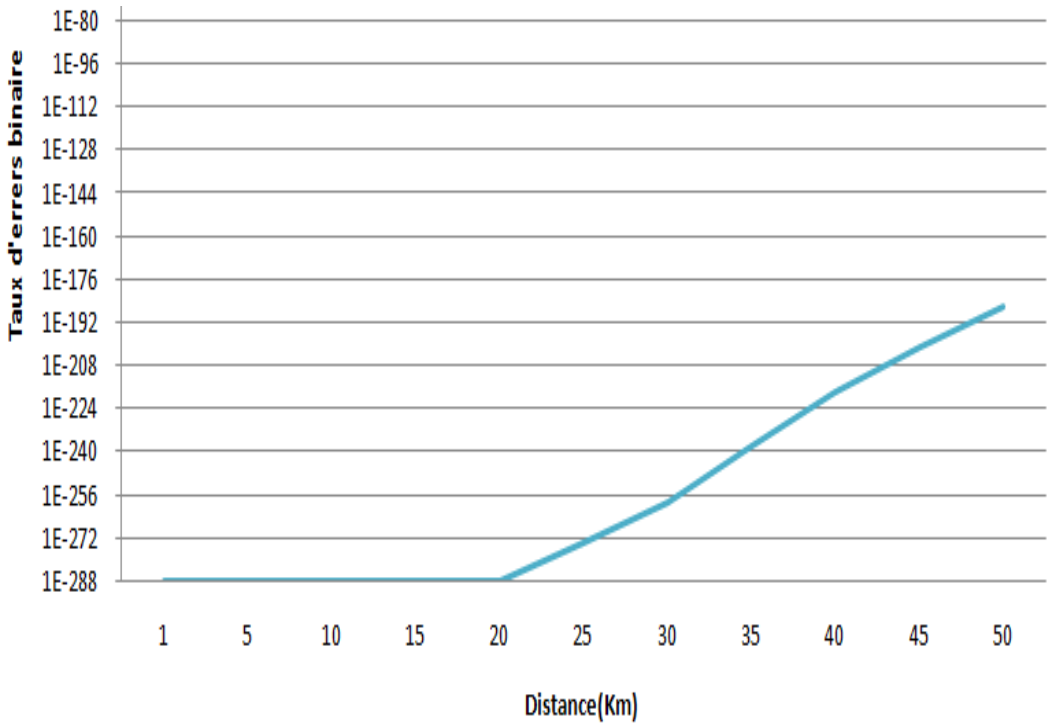

Figure III.38 : Taux d'erreur en fonction de la distance.

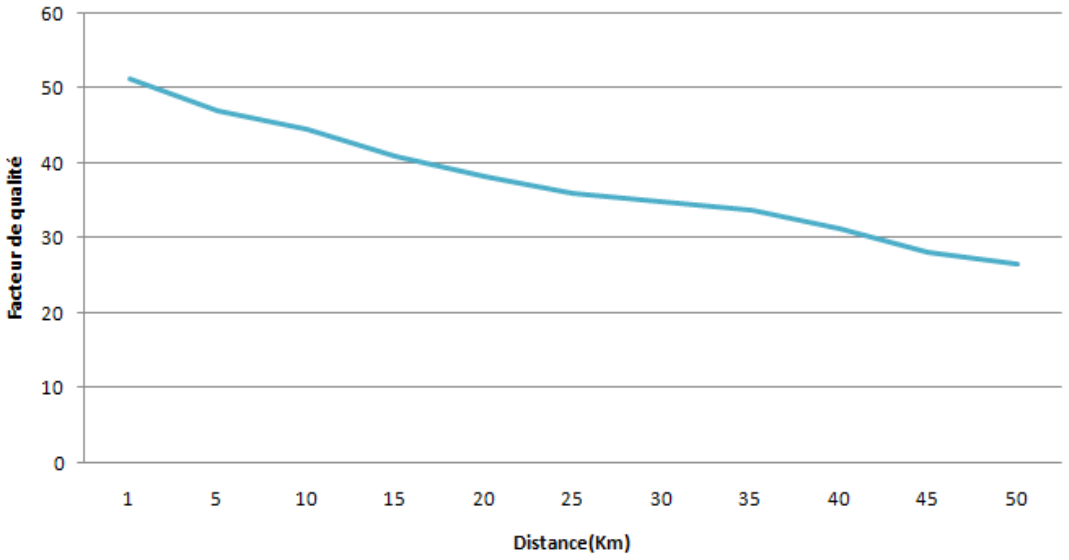

Figure III.39 : Facteur de qualité en fonction de la distance.

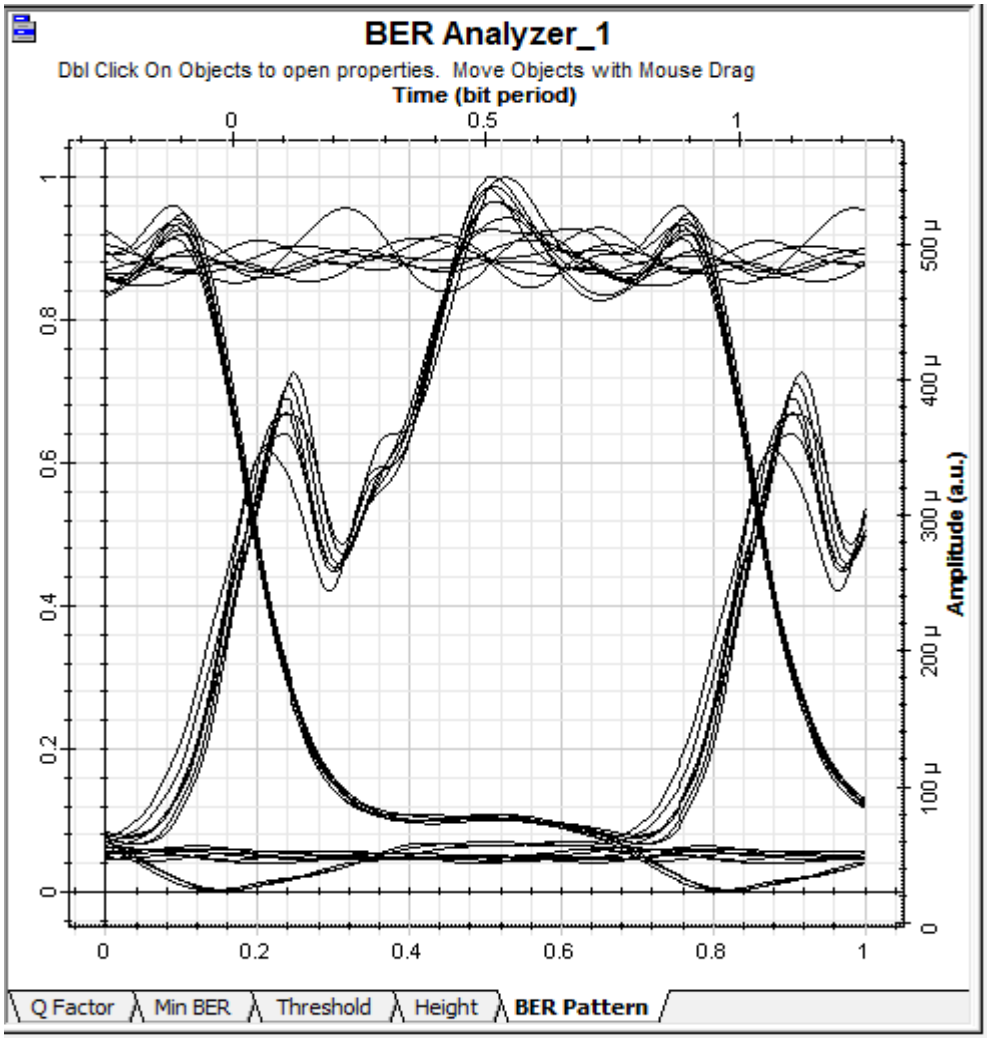

Figure III.40 : Diagramme de l'œil pour une distance de 50Km.

➢ **Commentaire :**

Selon les courbes obtenues, il est clair que le taux d'erreur augmente en augmentant la distance de propagation (longueur de la fibre optique), ce qui engendre une diminution de la puissance et la qualité du signal, d'où la sécurité du système est menacée.

Bien que cette dégradation reste acceptable pour des valeurs de BER inferieurs à 10^{-9} et le facture de qualité (Q) supérieur à 6, selon les normes internationales, mais si la distance de propagation augmente plus y'aura plus de pertes d'où la sécurité sera violée.

III.10.2 L'influence de la longueur d'onde sur la transmission :

Dans cette simulation, nous avons fait varier la longueur d'onde de la fibre avec un débit de 2,5Gbit/s et une distance de 17km. Nous avons obtenu les résultats présentés dans le tableau suivant :

Longueur d'onde :	**BER :**	**Facteur de qualité :**
900 nm	1	0
1300 nm	$9{,}21887e^{-140}$	25,1389
1450 nm	$1{,}30869\ e^{-283}$	35,9639
1550 nm	$4\ {,}10004e^{-312}$	39,5042
1650 nm	0	40 ,563

Tableau III.10 : Résultats de BER et facteur de qualité en fonction de la longueur d'onde.

A partir des résultats obtenus, nous avons tracé les courbes ci-dessous :

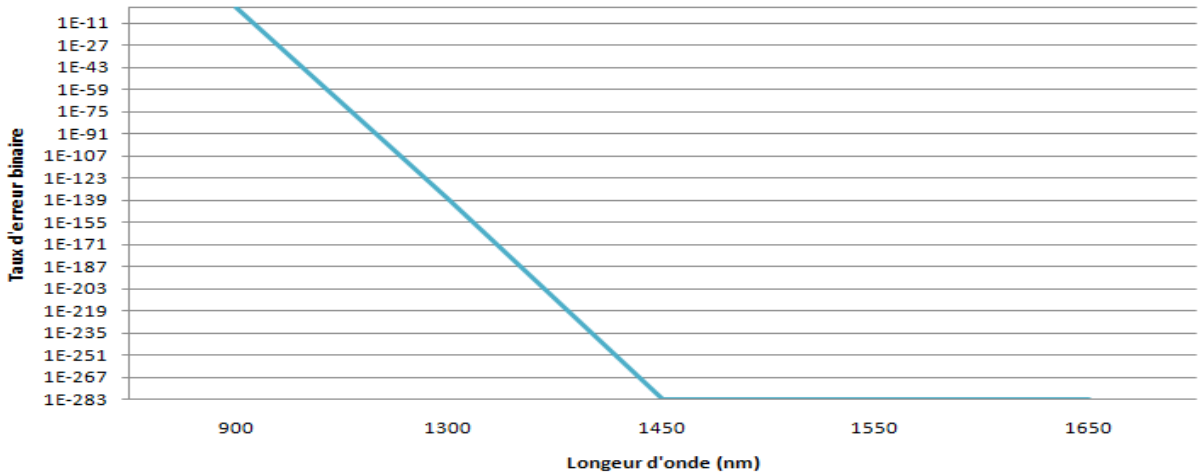

Figure III.41 : Taux d'erreur binaire en fonction de la longueur d'onde.

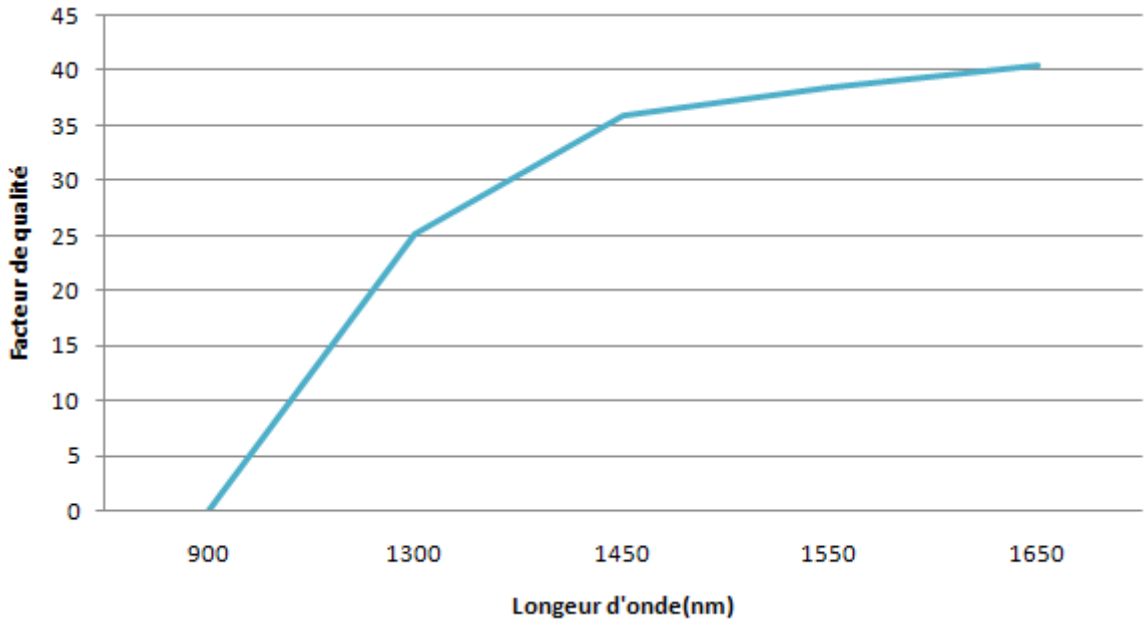

Figure III.42 : Facteur de qualité en fonction de la longueur d'onde.

➢ **Commentaire :**

D'après la courbe, nous remarquons que le BER diminue en augmentant la longueur d'onde d'où le facteur de qualité augmente.

On distingue pour les trois fenêtres :

- La première fenêtre (900nm) n'est pas acceptable car le taux d'erreur égale à 1 et supérieur à 10^{-9}, ce qui veut dire que le nombre de bit envoyer égale au nombre de bit erronée et la qualité de signal est trop faible.
- La deuxième fenêtre (1300nm) est acceptable car le taux d'erreur binaire est inférieur à 10^{-9} et le facteur de qualité supérieur à 6.
- La troisième fenêtre (1450 à150nm) est la meilleure fenêtre car elle présente moins d'atténuation et un taux d'erreur plus faible.

III.10.3 L'effet d'un espion sur la transmission :

Afin de voir l'influence d'une attaque, nous allons simuler une chaine de transmission avec le protocole B92 en présence d'espion pour un débit de 2,5Gbit/s et une distance de 17km, dans lequel l'espion Eve dispose d'une infrastructure qui lui permet d'intercepter-Renvoyer les qubits entre Alice et Bob tel que représente la figure suivante :

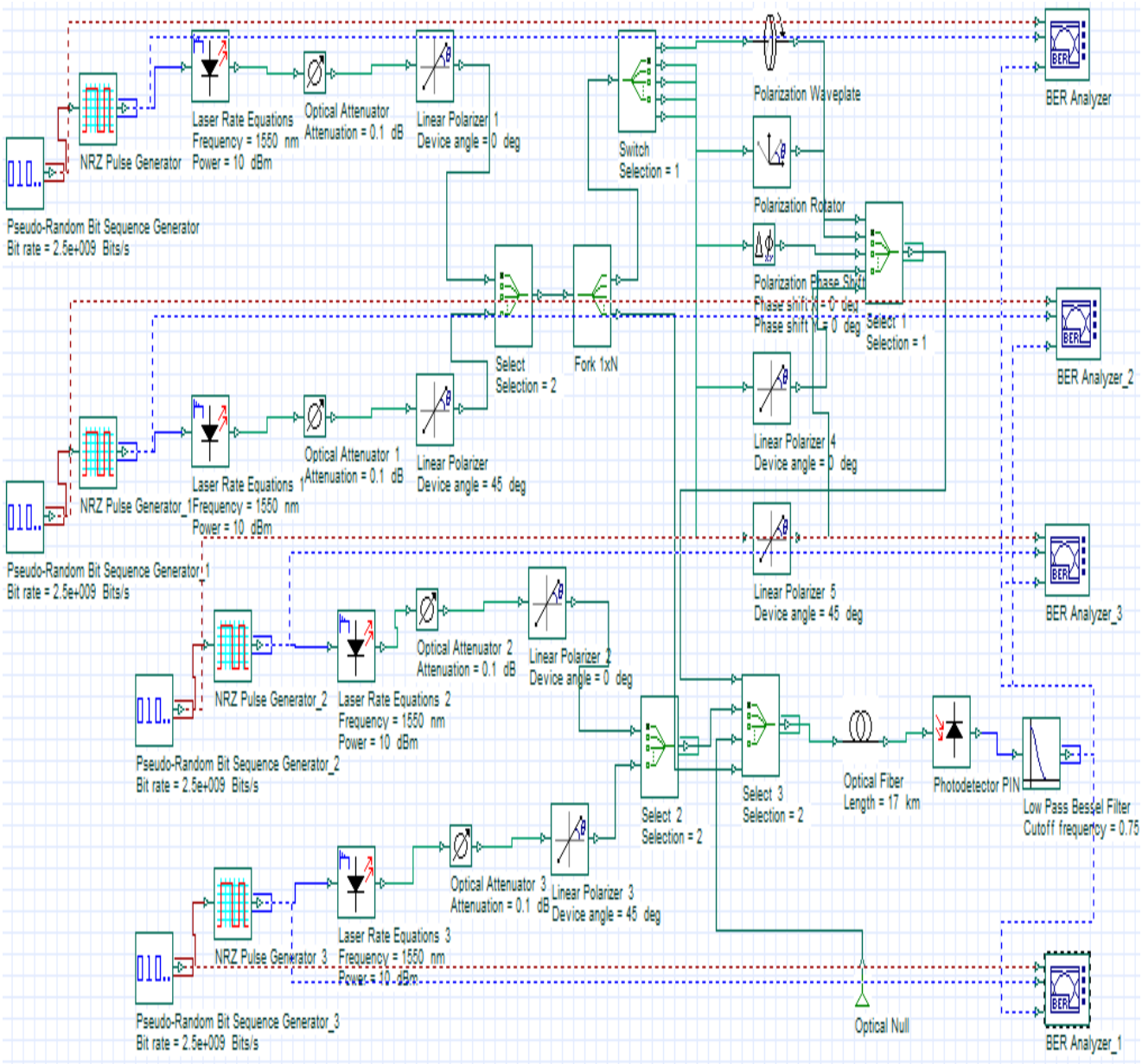

Figure III.43 : Synoptique d'une chaine de transmission avec le protocole B92 en présence d'espion [28].

Les résultats de la simulation sont représenté dans le tableau suivant :

Facteur de qualité :	37 ,1898
BER :	4,76435 e^{-303}

Tableau III.11 : Les résultats du BER et facteur de qualité dans une chaine optique avec le protocole B92 en présence d'espion.

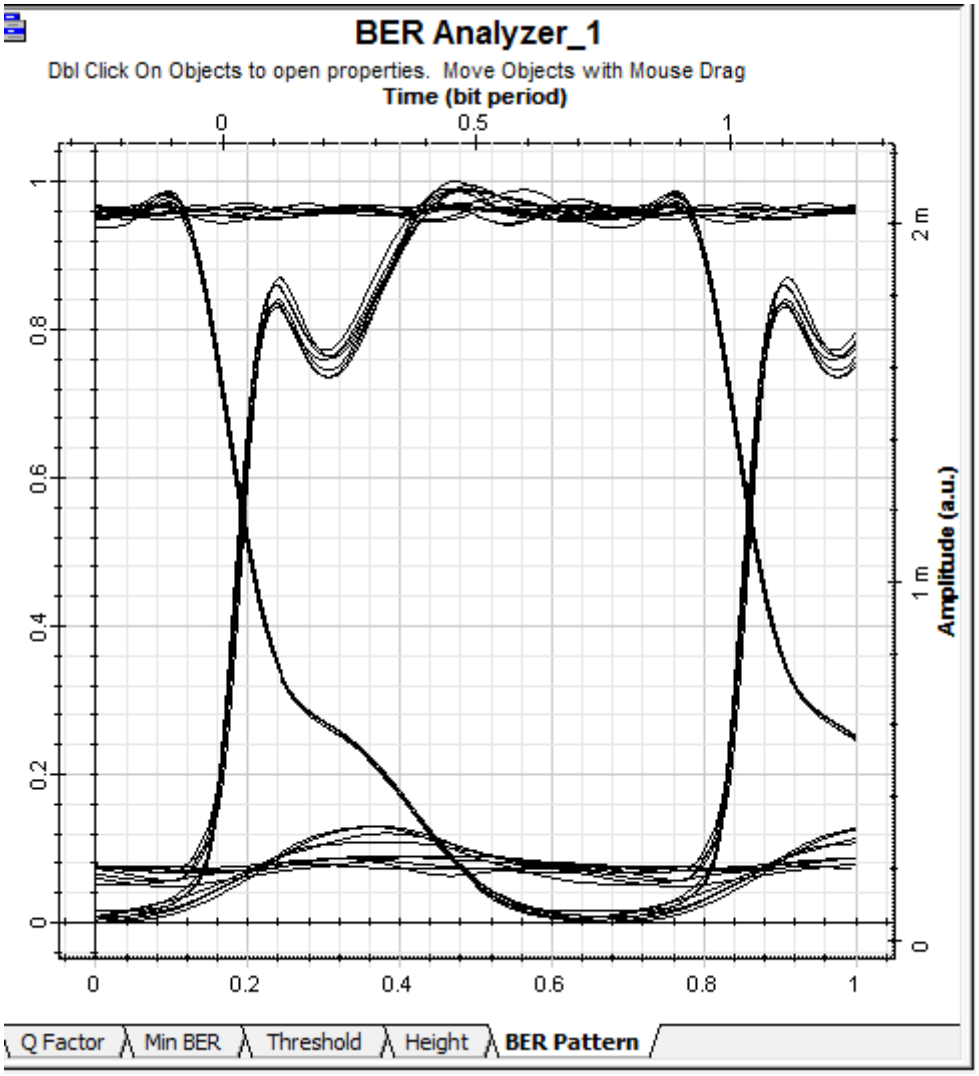

Figure III.44 : Diagramme de l'œil pour une distance de 17Km en présence d'espion.

III.10.3.1Influence de la distance en présence de l'espion :

Dans cette étape, nous avons fait varier la distance de 1à 50 km avec les mêmes conditions utilisées dans une chaine de transmission optique avec le protocole B92 en absence d'espion afin de faire une comparaison entre eux.

Nous avons obtenu les résultats représentés dans le tableau suivant :

Distance :	**BER :**	**Facteur de qualité :**
1 Km	0	46,224
5 Km	0	44,6767
10 Km	0	42,1535
15 Km	0	39,7134
20 Km	$9{,}15359\ e^{-280}$	36,9912
25 Km	$1{,}5843\ e^{-264}$	34,7228
30 Km	$2{,}08511\ e^{-241}$	33,1571
35 Km	$3{,}528\ e^{-223}$	31,866
40 Km	$6{,}61356\ e^{-190}$	29,3643
45 Km	$5{,}54705\ e^{-153}$	27,3197
50 Km	$7{,}72306\ e^{-130}$	25,5033

Tableau III.12 : Les résultats du BER et facteur de qualité en fonction de la distance avec espion.

Sur la figure III.45, on a relevé le diagramme de l'œil pour une distance de 50 Km en présence de l'espion.

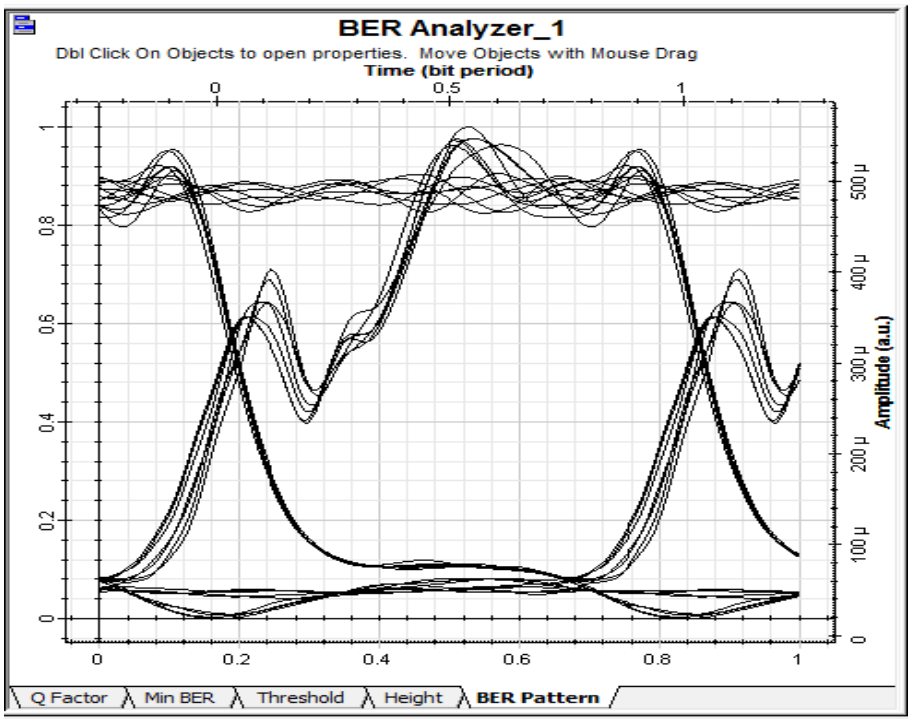

Figure III.45 : Diagramme de l'œil pour une distance de 50Km avec espion.

Pour faire une comparaison entre les résultats obtenus de taux d'erreur et facteur de qualité en présence et en absence d'espion, nous avons tracé les courbes suivantes :

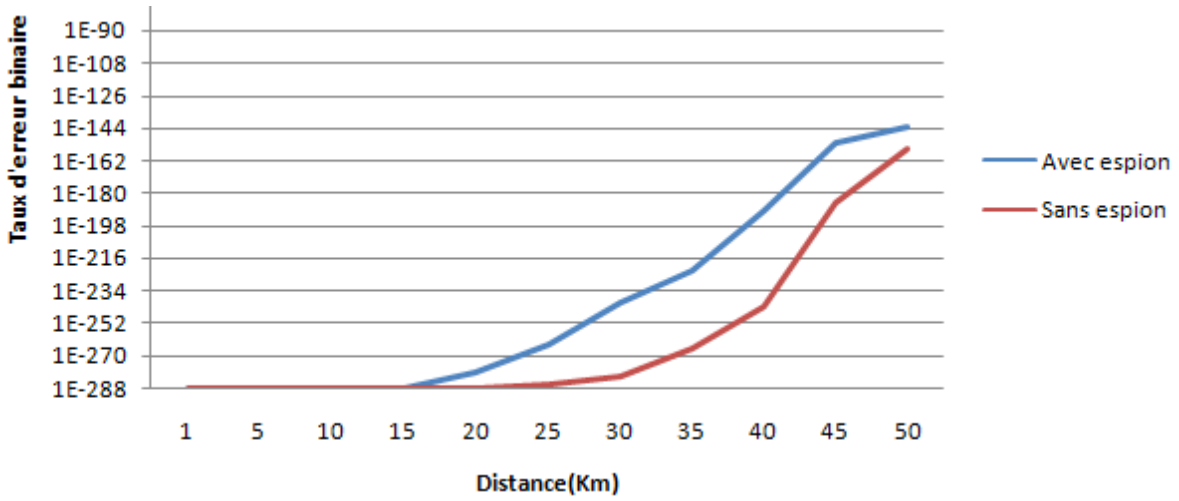

Figure III.46 : Taux d'erreur en fonction de la distance avec et sans espion.

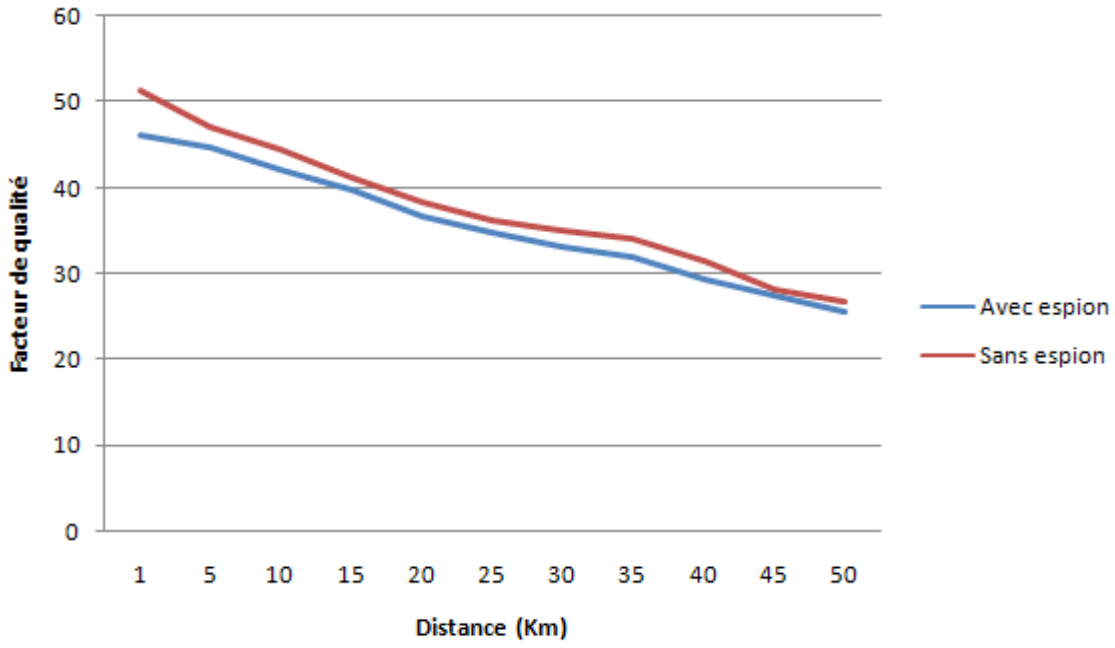

Figure III.47 : Facteur de qualité en fonction de la distance avec et sans espion.

➢ **Commentaire :**

A travers les résultats obtenus, nous constatons une dégradation du signal à travers le taux d'erreur qui croit lorsque la longueur de la fibre augmente et le facteur de qualité qui diminue.

D'après la comparaison entre les valeurs obtenues dans le cas d'absence et de présence d'espion, nous remarquons clairement que le taux d'erreur augmente plus en présence d'attaque.

La présence d'espion peut engendrer une perte d'information, d'où sa présence entraine plus d'atténuation et plus de perturbations sur la transmission.

III.10.3.2 Influence de la longueur d'onde en présence de l'espion :

Dans cette partie, nous avons fait varier la longueur d'onde pour un débit de 2.5Gbit/s et une distance de 17Km, afin de mesurer le taux d'erreur binaire et le facteur de qualité pour faire une comparaison avec les valeurs obtenues en absence de l'espion.

Les résultats obtenus sont représentés dans le tableau suivant :

Longueur d'onde :	BER :	Facteur de qualité :
900 nm	1	0
1300 nm	$1,8978e^{-130}$	22,2728
1450 nm	$4,81827\ e^{-274}$	32,3641
1550 nm	$4,76435\ e^{-303}$	37 ,1898
1650 nm	$5,44836\ e^{-305}$	38 ,1874

Tableau III.13 : Les résultats du BER et facteur de qualité en fonction de la longueur d'onde avec espion.

Afin de faire une comparaison entre les résultats obtenus précédemment en présence et en absence d'espion, nous avons tracé les courbes suivantes :

Figure III.48 : Taux d'erreur en fonction de la longueur d'onde avec et sans espion.

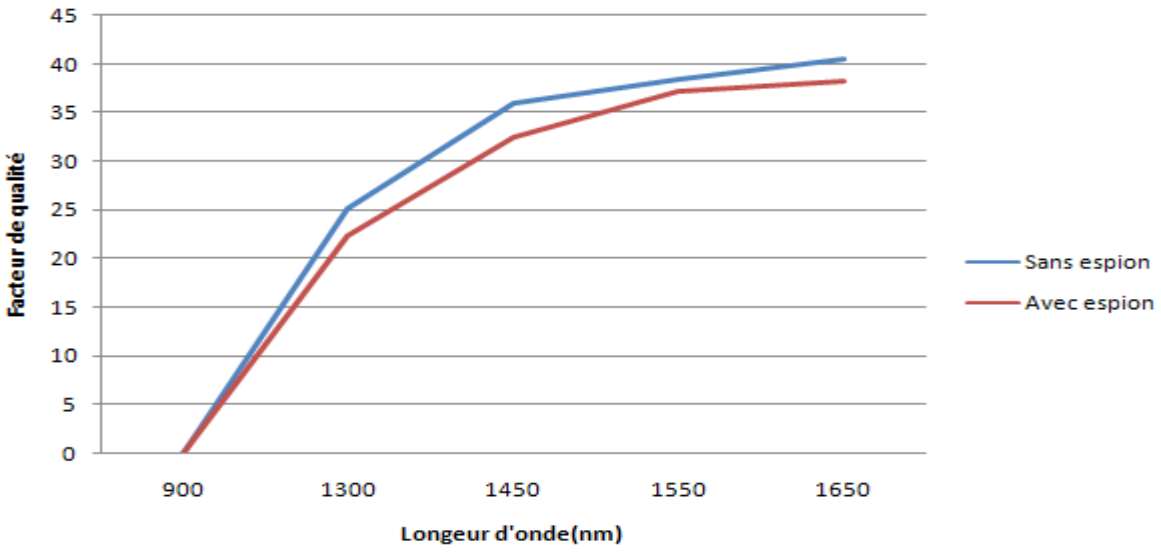

Figure III.49 : Facteur de qualité en fonction de la longueur d'onde avec et sans espion.

➢ **Commentaire :**

D'après les résultats obtenus, on voit bien que le taux d'erreur (BER) diminue avec l'augmentation de la longueur d'onde ce qui entraine une augmentation de la qualité de signal, il est claire que la troisième fenêtre reste la meilleure même si en présence d'un espion.

En comparant les deux cas d'absence et de présence d'une attaque, on déduit que le BER est plus grand en présence d'espion d'où le facteur de qualité est plus petit en comparaison avec son absence car l'espion dispose des outils et de moyen qui lui permettant d'émettre et de recevoir le signal donc sa présence dans une liaison optique peut entrainer des perturbations à travers ses effets.

III.11 Comparaison entre le protocole BB84 et B92 :

Le protocole B92 est un développement de protocole BB84 qui n'utilise que deux états de polarisation, au lieu de quatre dans le BB84.Chaque état est dans une base différente, ce qui rend le protocole plus facile à mettre en œuvre expérimentalement, bien que la sécurité soit plus faible, ce qui entraine une baisse des taux de clés sécurisées, c'est que ce qu'est montrer dans les figures suivantes :

- Variation de taux d'erreur binaire en fonction de la distance :

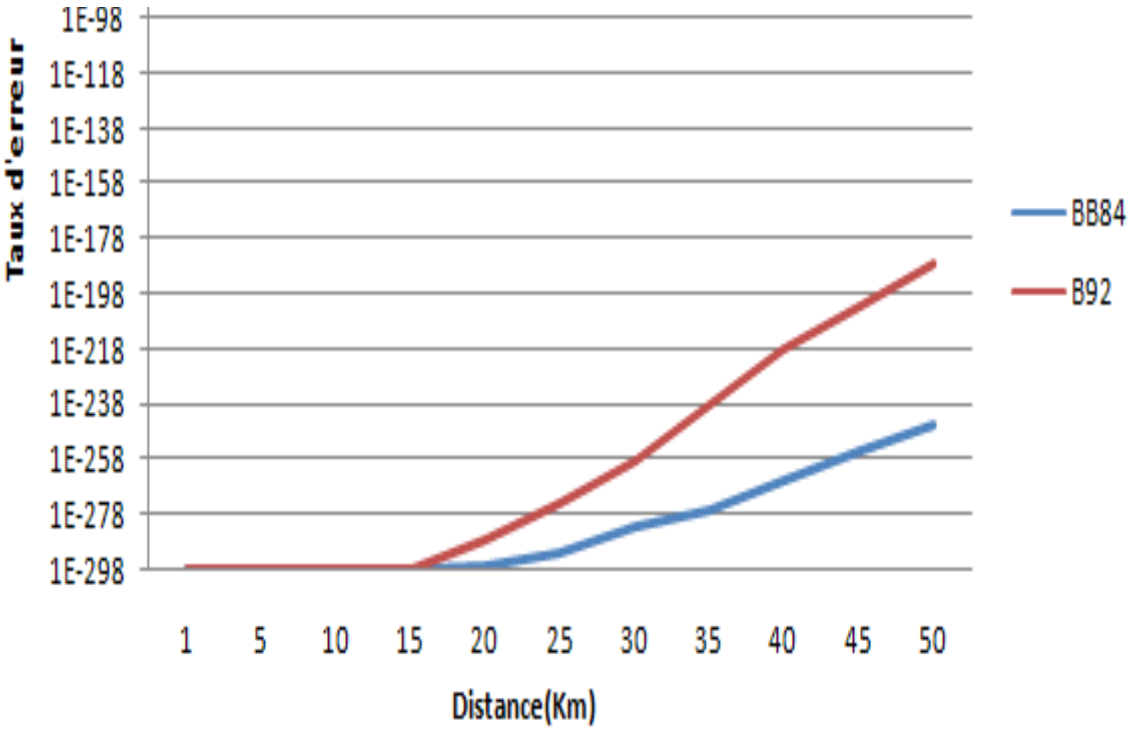

Figure III.50 : taux d'erreur en fonction de la distance sans espion avec BB84 et B92.

- Variation de facteur de qualité en fonction de la longueur d'onde en présence d'espion :

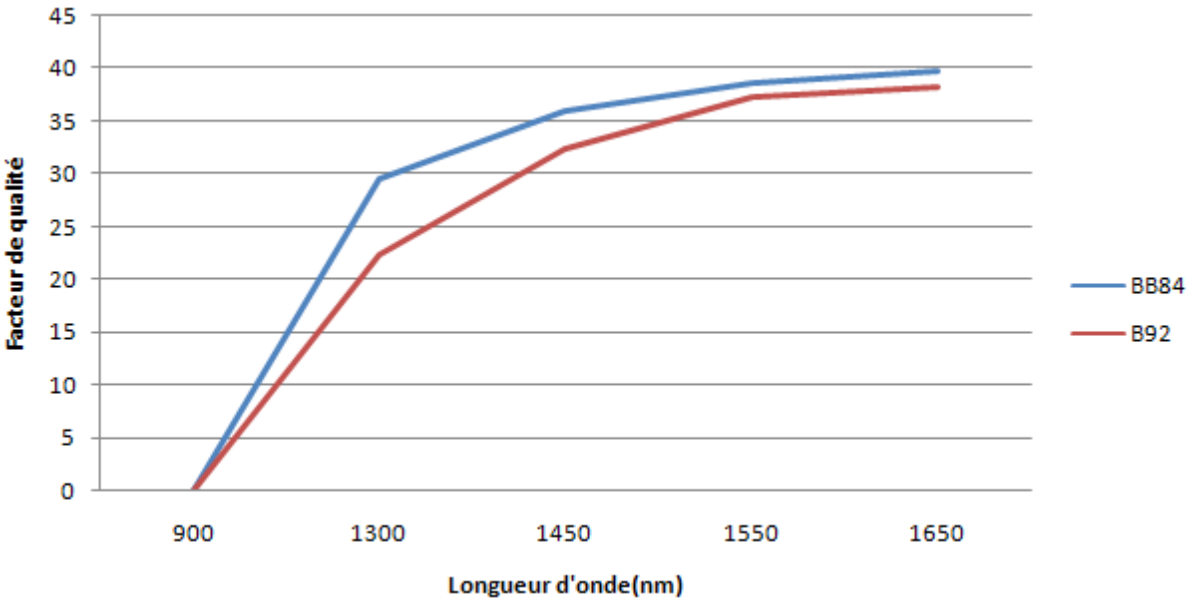

Figure III.51 : facteur de qualité en fonction de la longueur d'onde en présence d'espion avec BB84 et B92.

BB84 :	**B92 :**
BB84 est le premier protocole de distribution de clé quantique, développé par Charles Bennett et Gilles Brassard en 1984.	B92 est la version simplifie de BB84, il a été proposé par Charles Bennett en 1992.
Les performances des deux protocoles (BB84 et B92) basées sur la polarisation pulsée à photon unique contre les attaques individuelles pour les liaisons de communication optique quantique.	
A besoin de quatre état de polarisation (0°, 45°, 90°, -45°).	N'a besoin que de deux états de polarisation.
Le protocole BB84 présente de meilleures performances que B92dans la distribution de la clé de communication sécurisée sur une longue distance.	B92 est moins efficace que le protocole BB84 dans le taux de clé produit.

Tableau III.14 : Comparaison entre BB84 et B92.

Conclusion :

Durant ce chapitre, nous avons simulé une chaine de transmission optique avec les protocoles BB84 et B92 en présence et en absence d'espion afin d'étudier les performances de ces protocoles, et ça à travers l'analyse de taux d'erreur binaire et le facteur de qualité en fonction de la distance et la longueur d'onde de la fibre optique.

On constate que ces deux protocoles permettent de mieux sécuriser une chaine de transmission optique, la qualité de transmission diminue avec l'augmentation de la distance, et la fenêtre 1550nm présente une meilleure sécurité. Enfin, le protocole BB84 malgré sa complexité, reste plus performant et plus fiable par rapport au protocole B92.

Conclusion générale

Conclusion générale :

Durant ce mémoire, nous avons présenté la cryptographie quantique qui a pour objectif le partage de clé entre deux usagers, qui pourra être utilisée dans le chiffrement symétrique et cela grâce au principe d'incertitude d'Heisenberg et théorème de non clonage. Il existe plusieurs protocoles de distribution de clé quantique tels que : BB84 et B92 qui sont étudiés dans le cadre de notre travail.

Après une présentation des principes de base de la cryptographie ainsi que les différentes méthodes de chiffrement classique. A savoir, le chiffrement par transposition et le chiffrement par substitution, qui est très limitée, un aperçu a été jeté sur la cryptographie moderne pour ces deux types de chiffrement symétrique et asymétrique, elle a été largement utilisée avec beaucoup de robustesse jusqu'à l'apparition des ordinateurs quantiques.

Ces derniers à cause de leur capacité de calcul énorme, peuvent facilement casser n'importe quelle clé quel que soit sa dimension, ce qui rend le recours à d'autres techniques adéquates à ces ordinateurs, il s'agit de la distribution quantique de clé qui permet de palier les limites des méthodes de chiffrement modernes.

La distribution quantique de clé est une solution pour le partage de clé dans le chiffrement symétrique. C'est une technique qui se base sur la mécanique quantique et la théorie d'information, dans ce contexte nous avons présenté les notions et les principes de cet outil ainsi que le formalisme mathématique basé sur la mécanique quantique, un intérêt particulier a été donné aux protocoles BB84 et B92 avec leurs principes et déroulements en présence et en absence d'espion.

La suite du travail a été subdivisée en deux parties, la première est consacrée aux notions de base de la fibre optique ainsi que les critères de qualité d'une transmission optique. La deuxième partie présente la simulation sur le logiciel Optisystem qui a pour but d'étudier les performances des deux protocoles BB84 et B92 dans une liaison optique avec et sans attaque.

Cette étude est effectuée à travers la variation des paramètres physique tels que la longueur de la fibre, la longueur d'onde en absence et en présence d'un espion. La conclusion tirée à travers l'analyse du BER et du facteur de qualité indiquent que plus la distance augmente la qualité de transmission diminue et la troisième fenêtre 1550nm présente un

meilleur choix pour la qualité de transmission. Finalement, une comparaison entre les deux protocoles a été effectuée, d'après les résultats obtenus, dans lequel on déduit que le protocole le plus sécurisé est le protocole BB84 bien qu'il est plus ancien et l'avantage de protocole B92 est seulement simple et moins couteux.

Comme perspectives, il serait intéressant d'étendre cette étude pour d'autres canaux de transmission tels que le faisceau hertzien, et d'implémenter d'autre protocoles à variables discret et continue.

Bibliographies

Bibliographies :

[4]: *Ch.Tafeno Harizaka « Etude de protocole BB84 en cryptographie quantique », Mémoire de fin d'étude, Université d'Antanarivo, 2019.*

[5]: *A.Tekkouk « Etude et implémentation d'une méthode cryptanalyse pour le chiffrement continue», Mémoire de magister, université Mohamed Boudiaf Oran ,2010.*

[6]: *L.Rezkallah « De la cryptographie classique à la cryptographie moderne théorie et application » Mémoire de magister, université Houari Boumediene Alger, 2007.*

[10]: *Abderrahim EL A. Étude de cryptographie et de téléportation quantiques et proposition de quelques protocoles quantiques. Université Mohammed VAGDAL faculté des sciences. Thèse de Doctorat. Rabat, (2012).*

[11]: *Marcin Niemiec. (2011). « Design, construction and verification of a high-level SecurityProtocol allowing applying the quantum cryptography in communication networks ». Thèses de doctorat. Université des sciences ET de technologie. Portugal.*

[12]: *B. Hassene, « Protocols quantiques et relativistes de mise en gage », Mémoire pour Maîtrise en informatique, Université du Québec à Montréal, février 2009.*

[13]: *L.BOUCHOUCHA, "La distribution de clés quantiques dans une liaison optique", Thèse de Doctorat en électronique, Bejaia : Université A/Mira (Bejaia), 2020.*

[14] : *R.Djellab, « Cryptographie quantique, Nouvelle approches », Thèse de Doctorat en science informatique, université Batna2, 2017.*

[15]: *H.Makhlouf, A.mouhoub, « Distribution quantique de clé à variables continues par la modulation discrète », mémoire de fin d'étude, université de Bejaia, 2019.*

[16]*: NGUYEN Thanh Mai. (janvier 2005). « Etudier et implémenter une simulation du protocole d'échange de clef quantique BB84 ». Rapport de stage. Ecole nationale supérieure des télécommunications. Paris.*

[17]: *Gisin N. & Wolf S. (1999). « Quantum Cryptography on Noisy channels : quantum versus classical key-agreement protocols ». Thèses de doctorat. Département de Physique. Universités de Geneva. Switzer-land.*

[18]: *C. Bennett ET G. Brassard, « Quantum cryptography: Public-key distribution and coin tossing ». IEEE International Conference on Computers, Systems and Signal Processing. Bangalore, 1984, pp. 175-179.*

[19]: *NGUYEN Thanh Mai. (janvier 2005). « Etudier et implémenter une simulation du protocole d'échange de clef quantique BB84 ». Rapport de stage. Ecole nationale supérieure des télécommunications. Paris.*

[20]: *C. Bennet, « Quantum Cryptography Using Any Two Nonorthogonal States »,*

PHYSICAL REVIEW LETTERS, 1992, Vol 68, N°21, pp. 3121-31240.

[21]: *"Télécommunications optiques (sources, fibres et détecteurs)" Dr. SIDI ALI MEBAREK, office de publication universitaire, Ben Aknoun –Alger,2001*

[22]: *" Optimisation des paramètres d'une liaison à fibre optique" université Bejaia, présenté par : Itegarets Halim et Rezkellah Nadir,2015.*

[23]: *J. VERNEUIL, " Simulation de systèmes de télécommunications par fibre optique à 40Gbit/s", Thèse Doctorat en Télécommunication Hautes Fréquence et Optique : université 2003, 297p.*

[24]: *Nassima BOUDRIOUA "Etude et optimisation d'une chaîne de transmission numérique sur fibre optique : vers une compensation électronique de la PMD" de l'Université Paul Verlaine Soutenance le 25 octobre 2007.*

[25]: *W.BERROUNANE,'Etude de conception d'une chaine de transmission optique à très haut débit à base de semi-conducteur du type III. Nitrures', Thèse de Doctorat en réseaux Architecture et Multimedia, Sidi Bel Abbas : Université Djillali Liabes, 2018,163p*

[26]: *A.Benamare, W.Miloudi, «* Etude d'une liaison optique WDM Radio sur Fibre », Mémoire de fin d'étude, Université Aboubakr Belkaïd– Tlemcen –,2017.

[28]: *S.Chila,K.Djebarra, 'Implémentation du protocole B92 dans une liaison optique', Mémoire de fin d'étude, Université A/Mira Bejaia, 2021.*

Webographie :

[1]:[*https://www.blogdumoderateur.com/chiffres-cle-e-commerce2021*]

[2] :[*https://www.aps.dz/economie/134477-paiement-par-internet-plus-de-7-8-millions-d-operations-effectuees-en-2021*]

[3]: [*France 2030 | Stratégie quantique : lancement d'une plateforme nationale de calcul quantique | Gouvernement.fr*]

[7]: [*https://space.univ-lemcen.dzEtude-comparative-entre-la-cryptographie.pdf.*]

[8]: [*Ordinateur quantique : cinq questions pour (enfin) tout comprendre | Les Echos*]

[9]: [*https://www.riskinsight-wavestone.com/2018/08/cryptographie-post-quantique/*]

[27]:[*https://fr.scribd.com/document/464841549/optisystem-Chapitre-III-Simulation-et-resultats*].

ملخص

الأمن عنصر لا غنى عنه في مختلف مجالات الاتصالات السلكية واللاسلكية والشركات والمصارف..ـ إلخ، من أجل ضمان حماية البيانات السرية من جميع أنواع الهجمات، تم تطويرـ تقنيات التشفير. تعتمد هذه على تقنيات التشفير الكلاسيكية والحديثة. ولكن بعد تطويرـ مفهوم الكمبيوتر الكمي، فإن أمان هذه التقنيات محدود، والتي أصبحت غير فعالة، وولد نهج آخر للتشفير، وهو توزيع المفاتيح الكمومية «QKD».

يعتمد QKD على قوانين ميكانيكا الكم ونظرية المعلومات التي تسمح بمشاركة مفتاح بين المحاورين عن بعد، ويمكن استخدام هذا المفتاح في التشفير المتماثل. في هذا الملخص، قمنا بفحص بروتوكولات BB84 و B92، والتي قمنا بمحاكاتها باستخدام برنامج Optisystem لفحص ومقارنة أدائهم.

العلامات: التشفير الكمي، توزيع المفاتيح الكمومية، B92 ،BB84، التشفير، Qubit، الألياف البصرية.

Résumé

La sécurité est un élément indispensable dans les différents domaines des Télécommunications, entreprises, banques…etc., afin d'assurer la protection des données confidentielles contre toutes types d'attaques, des techniques de cryptage ont été développées. Ces dernières sont basées sur des techniques de chiffrement classique puis moderne. Mais suite au développement du concept de l'ordinateur quantique, la sécurité de ces techniques est limitée, dont laquelle sont devenues inefficaces, une autre approche de cryptage est née, c'est la distribution de clés quantique« QKD ».

La QKD est basée sur les lois de la mécanique quantique et la théorie d'information permettant le partage d'une clé entre deux interlocuteurs distants, cette clé pourra être utilisée dans le chiffrement symétrique. Durant ce mémoire, nous nous sommes intéressés aux deux protocoles BB84 et B92 dont lequel nous les avons simulé sur le logiciel Optisystem afin d'examiner leurs performances et de faire une comparaison entre eux.

Mots clés : Cryptographie quantique, distribution de clé quantique, BB84, B92, chiffrement, Qubit, fibre optique.

Abstract

Security is an essential element in the various fields of Telecommunications, companies, banks...etc., in order to ensure the protection of confidential data against all types of attacks, encryption techniques have been developed. These are based on classical and modern encryption techniques. But following the development of the quantum computer concept, the security of these techniques is limited, and some of them have become ineffective. Another approach to encryption was born, it is the quantum key distribution "QKD".

The QKD is based on the laws of quantum mechanics and information theory allowing the sharing of a key between two distant interlocutors, this key can be used in symmetric encryption. During this thesis, we are interested in the two protocols BB84 and B92 of which we simulated them on the Optisystem software in order to examine their performances and to make a comparison between them

Key words: Quantum cryptography, Quantum Key Distribution, BB84, B92, encryption, Qubit, optical fiber.