Année Universitaire : 2014-2015

UNIVERSITE D'ANTANANARIVO

ECOLE SUPERIEURE POLYTECHNIQUE

MENTION ELECTRONIQUE

MEMOIRE DE FIN D'ETUDES POUR L'OBTENTION DU DIPLOME

Domaine : SCIENCES DE L'INGENIEUR

Mention: ELECTRONIQUE

Parcours : A VISEE DE RECHERCHE : TELECOMMUNICATION, AUTOMATIQUE, SIGNAL ET IMAGES

SECURISATION DE LA TRANSMISSION OPTIQUE PAR CRYPTOGRAPHIE QUANTIQUE QKD

Etudiant:

DIEU DONNE Richard Jean Noel

UNIVERSITE D'ANTANANARIVO

ECOLE SUPERIEURE POLYTECHNIQUE D'ANTANANARIVO

MENTION ELECTRONIQUE

MEMOIRE DE FIN D'ETUDES EN VUE DE L'OBTENTION DU DIPLOME

Domaine : SCIENCES DE L'INGENIEUR
Mention ELECTRONIQUE
Parcours : A Visée de Recherche : Télécommunication, Automatique, Signal et Images

SECURISATION DE LA TRANSMISSION OPTIQUE PAR CRYPTOGRAPHIE QUANTIQUE QKD

Présenté par :

DIEU DONNE Richard Jean Noel

Devant les membres du jury :

Président Monsieur RANDRIAMITANTSOA Paul Auguste, Professeur Titulaire
Examinateur Madame RAMAFIARISONA Malalatiana, Maitre de Conférence
Examinateur Monsieur HERINANTENAINA Edmond Fils, Maitre de Conférence
Examinateur Monsieur RAJAONARISON Tianandrasana Roméo, Docteur en Télécommunication

Rapporteur :
Monsieur RASTEFANO Elisée, Professeur

Soutenu, le 15 Décembre 2016

Année Universitaire 2014-2015

N° d'ordre /EN/TASI/16

REMERCIEMENTS

Nous manifestons nos profondes reconnaissances à Dieu Tout Puissant pour toute sa bonté et sa générosité, nous ayant permis de garder force et santé tout au long du parcours dans la préparation de ce mémoire.

La réalisation de ce travail a été possible grâce au concours de nombreuses personnes.

Nous ne saurons constituer une liste exhaustive de toutes ces personnes, cependant nos premiers remerciements iront tout de même :
A Monsieur ANDRIANAHARISON Yvon, Professeur Titulaire, Directeur de l'Ecole Polytechnique d'Antananarivo.

A Monsieur ANDRIAMANANTSOA Guy Danielson Chef de la Mention Electronique

A Monsieur RASTEFANO Elisée, Professeur, Directeur de ce mémoire, pour son encadrement et ses conseils fort judicieux.

A Monsieur RANDRIAMITANTSOA Paul Auguste, Professeur Titulaire, qui, malgré ses lourdes responsabilités, me fait l'honneur de présider le jury de ce mémoire.

A Madame et Messieurs les membres du jury pour avoir pris soin d'examiner et d'évaluer notre travail malgré leurs obligations :

Madame RAMAFIARISONA Malalatiana, Maitre de Conférences
Monsieur HERINANTENAINA Edmond Fils, Maitre de Conférences
Monsieur RAJAONARISON Tianandrasana Roméo, Docteur en Télécommunication

A tous nos Professeurs de l'Ecole Supérieure Polytechnique d'Antananarivo, qui nous ont transmis leurs savoirs.
A tout le Personnel Administratif et Technique, en particulier celui de la Mention Electronique,

A nos familles respectives, pour tout le soutien, l'aide et l'affection qu'elles nous ont prodigués tout au long de nos études et recherches.

A nos amis, qui nous ont apporté leurs aides et leurs conseils.

RESUME

La fibre optique est un support de transmission privilégiée pour le transport de divers type de données publiques, privées et confidentielles. La cryptographie quantique est utilisée pour sécuriser ces divers données grâce au « Quantum Key Distribution » et au protocole BB84 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 permis d'implémenter un comportement équivalent d'une liaison optique illustrant le principe de base du QKD et l'analyse des taux QBER nous permettant de conclure l'existence d'intrus sur le canal de communication.

ABSTRACT

Fiber optic is a preferred transmission medium for transporting various types of public, private and confidential data. Quantum cryptography is used to secure these various data thanks to the quantum key distribution and the BB84 protocol for the sharing of encryption keys making information: inviolable, impossible to clone and especially offers the possibility of detection of intrusion. Our simulation on the Optisystem software enabled to implement an equivalent behavior of an optical link illustrating the basic principle of the QKD and the analysis of the QBER rates allows us to conclude the existence of intruders on the communication channel.

TABLE DES MATIERES

LISTE DES NOTATIONS

α	: Atténuation linéique
C	: Vitesse de la lumière dans le vide
D	: Dispersion chromatique
e	: Charge de l'électron
ε	: Permitivité du milieu
ε_0	: Permitivité du vide
λ	: Longueur d'onde
$\propto$	: Perméabilité du milieu
$\propto_0$	: Perméabilité du vide
n_1	: Indice de réfraction du cœur
n_2	: Indice de réfraction de la gaine
nm	: Nanomètre
µm	: Micromètre
ON	: Ouverture Numérique
Λ	: Opérateur nabla
rin(f)	: Bruit relatif d'intensit

LES CONSTANTES FONDAMENTALES

Constante de Planck $h = 6,6261\ 10^{-34}$ J s

Vitesse de la lumière $c = 299\,792\,458$ m s^{-1}

$hc = 197,327$ MeV fm

Perméabilité du vide $\mu_0 = 4\pi 10^{-7}$ Hm^{-1},

Constante de Boltzmann $k_B = 1,38066\ 10^{-23}$ J K^{-1} $= 8,6174\ 10^{-5}$ eV K^{-1}

Nombre d'Avogadro $N_A = 6,0221\ 10^{23}$

Charge de l'électron $q_e = -q = -1,60218\ 10^{-19}$ C et $e^2 = q^2/(4\pi\ \ 0)$

Masse de l'électron $m_e = 9,1094\ 10^{-31}$ kg, $m_e c^2 = 0,51100$ MeV

Masse du proton $m_p = 1,67262\ 10^{-27}$ kg, $m_p c^2 = 938,27$ MeV

Masse du neutron $m_n = 1,67493\ 10^{-27}$ kg, $m_n c^2 = 939,57$ MeV

Constante de structure fine $\alpha = e^2/\ \ hc) = 1/137,036$

Longueur d'onde de compton de l'électron $\lambda c = h/(mec) = 2,426\ 10^{-12}$ m

Energie d'ionisation de l'hydrog`ene $E_I = m_e e^4/(2^{-2}) = \alpha^2 m_e c^2/2 = 13,6057$ eV

Constante de Rydberg $R_\infty = E_I/(hc) = 1,09737\ 10^7$ m^{-1}

Magnéton de Bohr $\mu_B = q_e h/(2m_e) = -9,2740\ 10^{-24}$ J T^{-1}

Magnéton nucléaire $\mu_N = qh/(2mp) = 5,0508\ 10^{-27}$ J T^{-1}

LISTE DES ABREVIATIONS

AES	Advanced Encryption Standard
AK	Authorisation Key
AP	Access Point
APD	Silicon Avalanche Photodiode
B92	QKD protocol intrusloped by C. H. Bennett in 1992
BB84	QKD protocol intrusloped by Bennett and Brassard 1984
CA	Certificate Authority
CR	Cognitive Radio
CTS	Clear to Send
CWDM	Coarse Wavelength Division Multiplexing
DWDM	Dense Wavelength Division Multiplexing
DES	Data Encryption Standard
DoS	Denial of Service
DEL	Diodes Electroluminescentes
DL	Diode Laser
DS	Distribution System
EAPOL	Extensible Authentication Protocol over LAN
ECC	Elliptic Curve Cryptography
ESS	Extended Service Set
EDFA	Erbium-Doped Fiber Amplifier
FPGA	Field Programmable Gate Array
FSO	Free Space Optics
FTTC	Fiber To The Curb
FTTCab	Fiber To The Cabinet
FTTB	Fiber To The Building
FTTH	Fiber To The Home
FTTO	Fiber To The Office
IOE	Interface Optique d'Emission
IBSS	Independent Basic Service Set
IE	Information Element
IEEE	Institute of Electrical and Electronics Engineers
IPsec	Internet Protocol Security
HWDM	Wavelength Division Multiplexing
KCK	Key Confirmation Key
KEK	Key Encryption Key
PBS	Polarisation Beam Splitter
L2TP	Layer 2 Tunnelling Protocol
LEAP	Lightweight Extensible Authentication Protocol
LASER	Light Amplification by Stimulated Emission of Radiation
MAC	Media Access Control
MAS	Multi Agent System
MEMS	Micro-Electro-Mechanical Systems
MMDM	Micromachined membrane deformable mirrors
MZI	Mach-Zehnder Interferometer

MIC Message Integrity Check
MIMO Multiple-Input Multiple-Output
MLME MAC Sublayer Management Entity
MMZ Modulateur Mach Zender
NAT Network Address Translation
NIC Network Interface Controller
NRZ Non Return to Zero
ON Ouverture Numérique
OCDMA Optical Code Division Multiple Access
OFDM Orthogonal Frequency Division Multiplexing
OSNR Optical Signal to Noise Ratio.
OXC Optical Cross Connector
PAPR Peak to Average Power Ratio
PDL Polarization Dependent Loss**.**
PMD Polarization Mode Dispersion
PON Passive Optical Network
PDA PhotoDiode à Avalanche
PRBS Pseudorandom Binary Sequence
P2P Peer to Peer
PHY Physical layer
PKC Public Key Cryptography
PKI Public Key Infrastructure
PKM Privacy Key Management
PMK Pairwise Master Key
PPTP Point-to-Point Tunnelling Protocol
PRF Pseudo Random Function
PTK Pairwise Transient Key
PM Phase Modulation
QBER Quantum Bit Error Rate
QKD Quantum Key Distribution
Q-Key Quantum Key
QM Quantum Mecanic
Qubit Quantum Bit
RIN Relative Nose Intensity
RSA Rivest-Shamin-Adleman
RSN Robust Security Networks
RSNA Robust Security Network Association
RTS Request to Send
SAID Security Association IDs
SNonce random or pseudo-random value generated by the Station
SS Subscriber Station
SSID Service Set Identifier
SDH Synchronous Data Hierarchy
SSL Secure Sockets Layer protocol
SMF Single Mode Fiber.
SONET Synchronous Optical Network.

SPM	Self Phase Modulation.
SSB	Single-Side Band.
TEB	Taux d'Erreur Binaire
TEK	Traffic Encryption Keys
TK	Temporal Key
TKIP	Temporal Key Integrity Protocol
TSN	Transition Security Network
VoIP	Voice over IP
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Networks
WMAN	Wireless Metropolitan area networks
WDM	Wavelength Division Multiplexing
WPA	Wi-Fi Protected Access
WPAN	Wireless Personal Area Networks

LISTE DES FIGURES

LISTE DES TABLEAUX

INTRODUCTION

Nous vivons actuellement dans l'ère du numérique. Nos données privées, professionnelles, gouvernementales, industrielles et confidentielles véhiculent à travers le monde sur des supports comme la fibre optique. La sécurité de l'information est l'élément fondamental et indispensable de toute transmission. Or, de nos jours, avec l'émergence des puissants ordinateurs et de la performance des nouveaux algorithmes de calcul, les cryptographies à base des théories mathématiques et logiques algorithmiques sont devenues vulnérables. Parallèlement à ce problème, une nouvelle forme de protection d'information est mise en place à travers des procédés physiques basés sur les lois de la mécanique quantique. Ainsi, la physique quantique est utilisée par la cryptographie destinée à rendre inviolable notre information. C'est la base même de notre actuel travail de mémoire. Notre objectif consiste à étudier les bases, les principes, les caractéristiques de cette cryptographie quantique sur les réseaux à fibres optiques. Toutefois, cette technologie de sécurisation comporte plusieurs défis technologiques pour pouvoir être bien intégrée de façon standard et homogène dans les équipements déployés dans les réseaux de télécommunications à grande échelle. A travers une implémentation via le simulateur Optisystem, nous allons décrire les réseaux optiques à base de cryptographie quantique, le mécanisme permettant le transport de données et l'analyse d'erreur quantique (QBER) permettant la détection d'intrusion sur un canal de transmission. Pour mieux aborder le thème, nous allons repartir le travail en quatre grands chapitres :

En premier lieu, nous allons étudier le fondement de la transmission par fibre optique.
Ensuite, nous parlerons longuement des systèmes de sécurisation en réseaux fibres optiques.
Puis, nous entamerons plus de détail sur le chapitre « cryptographie quantique ».
Et au finale, le chapitre sur les simulations des systèmes de transmission à cryptographie quantique suivi d'analyse et interprétations des résultats.

CHAPITRE 1
GENERALITE SUR LA TRANSMISSION OPTIQUE

1.1 Notion d'optoélectronique

a) Introduction

La fibre optique est un fil en verre ou en plastique très fin qui a la propriété d'être un conducteur de la lumière et sert dans la transmission de données et de lumière. Elle offre un débit d'information nettement supérieur à celui des câbles coaxiaux et peut servir de support à un réseau « large bande » par lequel transitent aussi bien la télévision, le téléphone, la visioconférence ou les données informatiques.

Elle est un guide d'onde qui exploite les propriétés réfractrices de la lumière. Elle est habituellement constituée d'un cœur entouré d'une gaine. Le cœur de la fibre a un indice de réfraction légèrement plus élevé que la gaine et peut donc confiner la lumière qui se trouve entièrement réfléchie de multiples fois à l'interface entre les deux matériaux.

Tout système de transmission d'information possède un émetteur et un récepteur. Pour un lien optique, deux fibres sont nécessaires. L'une gère l'émission, l'autre la réception. Il est aussi possible de gérer l'émission et la réception sur un seul brin mais cette technologie est plus rarement utilisée car l'équipement de transmission est plus onéreux.

b) Une liaison point à point par fibres optiques comprend :

- Les fibres optiques (en tant que support)
- L'interface optique d'émission
- L'interface optique de réception
- Lorsque la longueur de la liaison le nécessite, on y insère un ou plusieurs répéteurs, utilisés pour amplifier le signal.

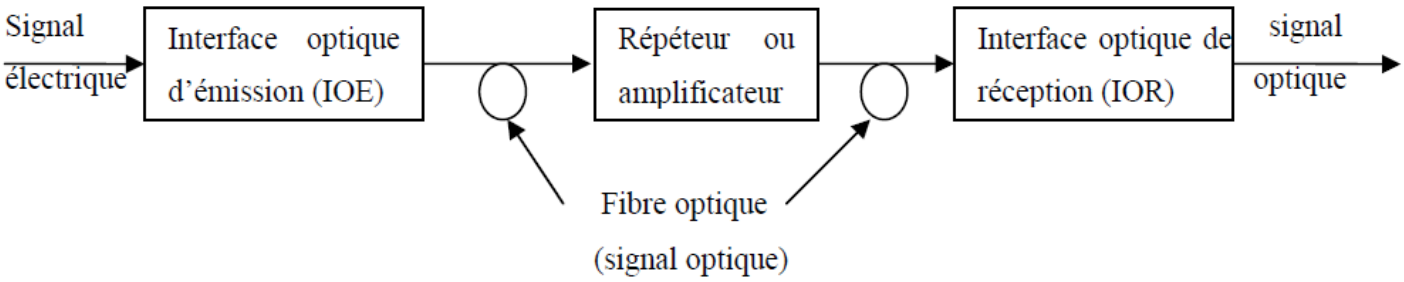


Figure 1.1 : Liaison point à point par fibre optique

Les modes sont l'expression des différents chemins optiques que peut suivre le signal dans la fibre. Suivant le nombre de modes N des ondes lumineuses qui peuvent se propager dans la fibre, la fibre est dite:
- Multimode quand N1>1
- Monomode quand N1=1.

i. Fibre multimode

La fibre multimode a un diamètre de cœur de l'ordre de 50 à 200µm. Plusieurs chemins de propagation y sont possibles. Suivant le type de profil d'indice, il y a la fibre à saut d'indice et la fibre à gradient d'indice [1]

- **La fibre multimode à saut d'indice**

Dans cette fibre, le cœur est homogène et d'indice n_1. Il est entouré d'une gaine optique d'indice n_2 inférieur à n_1. Le faisceau lumineux injecté à l'entrée de la fibre va atteindre la sortie en empruntant des chemins optiques différents. Ce qui se traduit par de temps de propagation. Les fibres à saut d'indice présentent un cœur transparent d'indice constant, et une gaine sombre, il y a alors réflexion du rayon lumineux à la frontière entre les deux matériaux. Cependant, le chemin optique varie, ce qui est gênant puisqu'un même signal se retrouve étendu à la sortie [1].

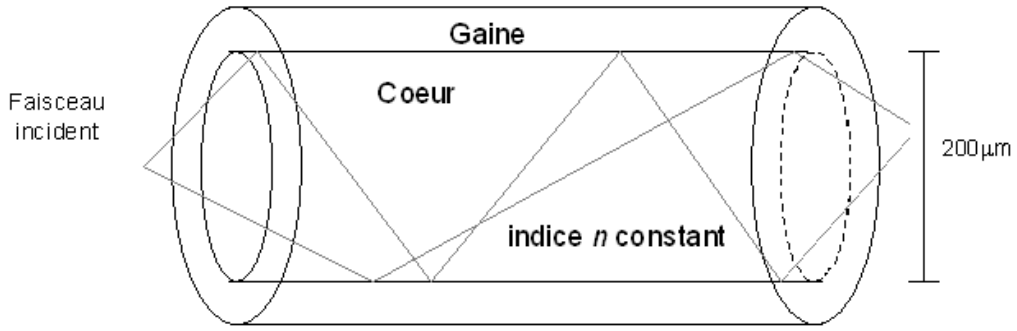


Figure 1.2 : Fibre multimode à saut d'indice

On définit le paramètre V appelé fréquence réduite donnée par la formule [1]:

$$\mathbf{V = \frac{2\pi a}{\lambda_0}\sqrt{{n_1}^2 - {n_2}^2}} \qquad (1.01)$$

Avec λ_0 : longueur d'onde dans le vide [m]
a : diamètre du cœur de la fibre [µm]
Le nombre de modes N dans ce type de fibre est égal à :

$$\mathbf{N = \frac{V^2}{2}} \qquad (1.02)$$

- **La fibre multimode à saut d'indice**

Ici l'indice varie peu à peu du centre à la gaine, la forme de la trajectoire est plus sinusoïdale car le rayon est dévié au fur et à mesure qu'il s'éloigne du centre. La variation du chemin optique est ici plus faible car le cœur à un diamètre moindre. L'étalement du signal est moins important grâce à la variation de l'indice [1].

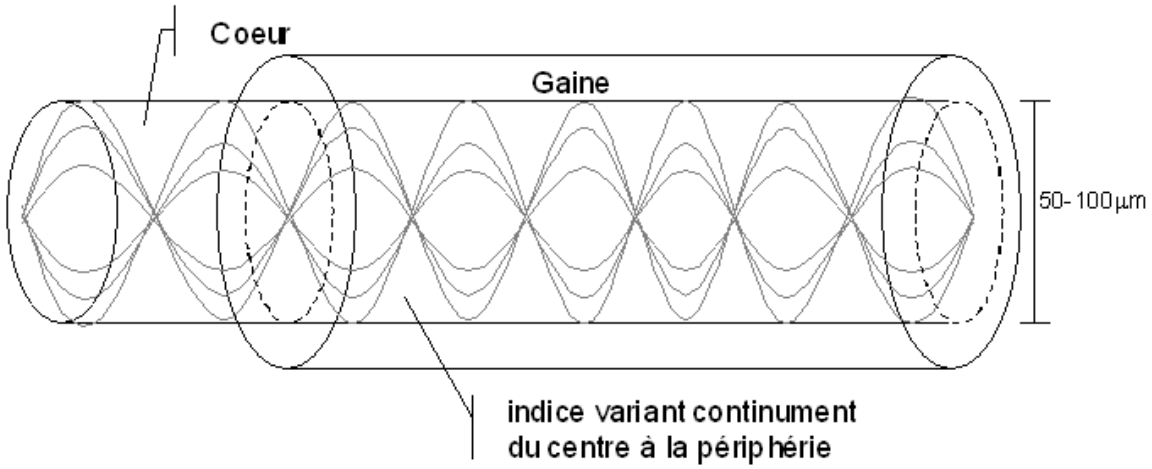


Figure 1.3 : Fibre à gradient d'indice

Le cœur n'est plus homogène : la valeur de l'indice décroît progressivement depuis l'axe du cœur jusqu'à l'interface cœur-gaine, suivant la loi :

$$\mathbf{n(r) = n_1\sqrt{1 - 2\Delta(r/a)^{\alpha}}} \tag{1.1}$$

Avec r : distance à l'axe, n(r) paramètre de profil d'indice relativement différent

$$\Delta = \frac{n_1{}^2 - n_2{}^2}{2n_1{}^2} \approx \frac{n_1 - n_2}{n_1} \quad \text{si } (n_1 - n_2 \ll n_1) \tag{1.2}$$

Les rayons lumineux vont aussi emprunter des chemins différents, mais un choix judicieux du profil d'indice du cœur permet de tendre vers des temps de parcours voisins et donc de réduire l'étalement du signal [1] [2]. La trajectoire des rayons lumineux est incurvée quand on se rapproche de la gaine.
Le nombre de modes N dans cette fibre est donné par :

$$\mathbf{N = \frac{\alpha}{\alpha + 2}\frac{V^2}{2}} \tag{1.3}$$

ii. La fibre monomode

Dans une fibre monomode, on obtient un seul mode grâce à la très faible dimension du cœur (diamètre de 10 µm et moins). Ainsi le chemin de la lumière est imposé, il n'y en a qu'un seul : celui du cœur. A l'entrée de la fibre, il est nécessaire d'avoir une grande puissance d'émission pour ce diamètre de cœur très petit. La déformation du signal dans ce type de fibres est quasi inexistante [1] [2].

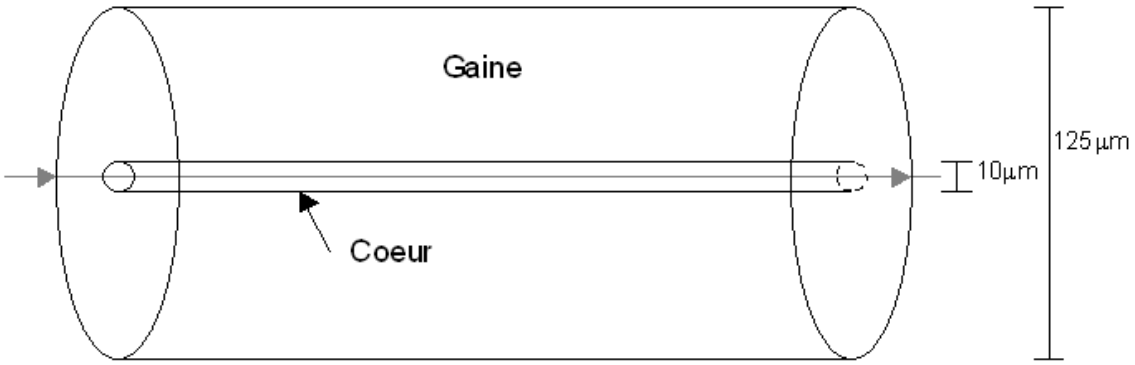


Figure 1.4 : Fibre monomode

La fibre monomode classique est une fibre à saut d'indice, avec la condition sur la fréquence réduite V :

$$\mathbf{V = \frac{2\pi a}{\lambda_0}\sqrt{n_1{}^2 - n_2{}^2} < 2,405} \qquad (1.4)$$

La fibre monomode présente deux avantages considérables qui sont :
- une grande bande passante ;
- une faible atténuation.

Le fait qu'un seul mode se propage à la limite de la dispersion chromatique qui se traduit par une variation de l'indice en fonction de la longueur d'onde. La propagation d'un seul mode limite également l'atténuation en fonction de la longueur d'onde ce qui permet d'augmenter la distance entre les répéteurs de lignes. En ajustant les paramètres optoélectroniques des guides diélectriques qui constituent la fibre, il est possible de les optimiser pour une longueur d'onde donnée. Mais cela se traduit généralement par l'obtention d'un diamètre de cœur très faible générant des problèmes de raccordement.

c) Propagation d'ondes lumineuse

Lorsqu'un faisceau lumineux heurte obliquement la surface qui sépare deux milieux plus ou moins transparents, il se divise en deux : une partie est réfléchie tandis que l'autre est réfractée c'est à dire transmise dans le second milieu en changeant de direction [2].

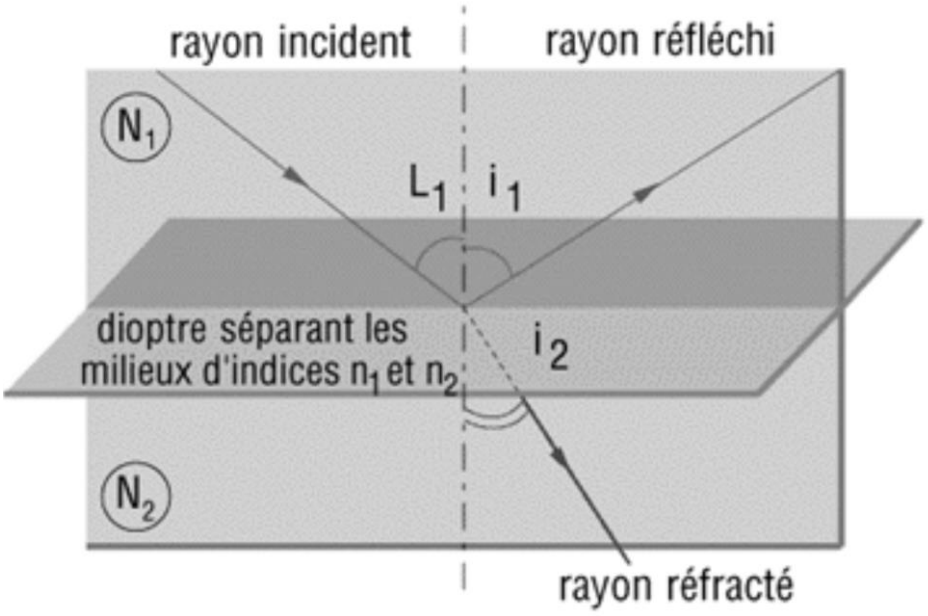


Figure 1.5 : Principe de propagation d'onde lumineuse

La vitesse de la lumière dans un matériau d'indice n est donnée par la formule :

$$\boldsymbol{v = \frac{c}{n}} \quad [\text{m /s}] \tag{1.5}$$

Pour guider la lumière, la fibre utilise le phénomène de réflexion totale qui se produit à l'interface de deux milieux d'indices différents. Ces deux milieux sont définis par le cœur et la gaine. L'indice de réfraction de la gaine doit être inférieur à celui du cœur.

i. Loi de Descartes

Un faisceau lumineux qui heurte la surface séparant deux milieux transparents et d'indice de réfraction différent, n_1 et n_2 se divise en deux rayons [3] [2] :

- un rayon réfléchi formant un angle i_1 par rapport à la normale à l'interface des deux milieux
- un rayon réfracté avec un angle i_2 par rapport à la même normale.

D'après la loi de Descartes, les trois rayons (incident, réfléchi et réfracté) sont dans le même plan et sont liés par les relations :

$$\boldsymbol{n_1 sin(L_1) = n_1 sin(i_1)} \tag{1.6}$$

Soit L_1 i_1, L_1 étant l'angle d'incidence.

$$\boldsymbol{n_1 sin(L_1) = n_2 sin(i_2)} \tag{1.7}$$

$$\boldsymbol{n_1 sin(i_1) = n_2 sin(i_2)} \tag{1.8}$$

ii. Angle limite et condition de guidage

Si $n_2 > n_1$, il est théoriquement possible d'avoir $i_2 = \frac{\pi}{2}$. Dans ce cas il n'y a pas réfraction. On notera i_{iL} l'angle du rayon incident correspondant à $i_2 = \frac{\pi}{2}$

La loi de Descartes [2] [3] devient alors :

$$\boldsymbol{n_1\, sin(i_{iL}) = n_2\, sin(\frac{\pi}{2}) = n_2}$$

D'où

$$i_{iL} = arcsin(\frac{n_2}{n_1}) \tag{1.9}$$

i_{iL} est appelé angle limite

La condition de guidage dans le cœur est donnée par la relation :

$$\boldsymbol{i_1 \geq arcsin(\frac{n_2}{n_1})} \tag{1.10}$$

Si cette condition n'est pas vérifiée alors le rayon est réfracté dans la gaine de la fibre optique.

iii. Ouverture numérique (ON)

Pour qu'un rayon lumineux arrive à la sortie de la fibre, il doit subir plusieurs réflexions tout au long de la fibre. A chaque réflexion une partie de la lumière est réfractée et donc absorbée par la gaine. Le rayon finit alors par être complètement atténué. Cependant il est possible de choisir l'angle d'incidence pour qu'il n'y ait pas de réfraction, soit $i_1 > i_{iL}$. Par conséquent, le rayon injecté à l'entrée arrivera à la sortie sans aucune atténuation. On définit alors l'ouverture numérique d'une fibre optique, en fonction de l'angle d'incidence limite i_{iL} , qui permet d'assurer une transmission sans pertes théoriques[2] [3].

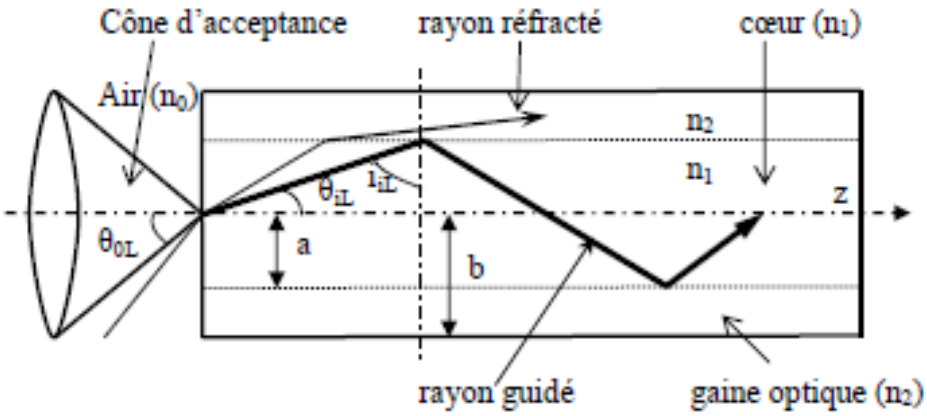


Figure 1.6 : Propagation de l'onde

Soit n_1 l'indice de réfraction du cœur, n_2 celui de la gaine et n_0 celui de l'air (n_1). On cherche l'angle incident θ_{0L} à l'entrée de la fibre correspondant à l'angle limite i_{iL} .

D'après la loi de Descartes on a :

$$\boldsymbol{n_0\, sin(\theta_0\ )n_1\, sin(\theta_1\ )} \tag{1.11}$$

Avec $\theta_1 = \frac{\pi}{2} - i_1$ et $n_0 = 1$

Soit $sin(\theta_{oL}) = n_1 \, sin\left(\frac{\pi}{2} - i_{iL}\right) = n_1 \, cos(i_{iL}) = n_1\sqrt{1 - sin^2(i_{iL})}$

Or

$$i_{iL} = arcsin(\frac{n_2}{n_1})$$

D'où

$$\boldsymbol{sin(\theta_{oL}) = n_1\sqrt{1 - (\frac{n_2}{n_1})^2}} \tag{1.12}$$

L'ouverture numérique (ON) est ainsi défini par :

$$\boldsymbol{ON = sin(\alpha_{max}) = n_1 \, sin\left(\frac{\pi}{2} - \theta_{1lim}\right) = \sqrt{{n_1}^2 - {n_2}^2}}$$

Afin de faciliter l'injection de la lumière dans la fibre à l'entrée, on a intérêt à avoir l'angle limite θ_{oL} le plus grand possible. Ceci s'obtient pratiquement en choisissant des indices n_1 et n_2 très proches [3].

1.2 Interface optique d'émission

Le rôle d'un émetteur optique est de transformer un signal électrique en signal lumineux pour l'envoyer dans la fibre optique qui sert de canal de transmission. Dans les systèmes de transmission par fibres optiques, on utilise comme source optique des composants semi-conducteurs. Les émetteurs peuvent être de deux types :

- Les diodes électroluminescentes (DEL) ;
- Les diodes laser (DL).

a) Principe de l'émission de lumière dans un semi-conducteur

Dans un semi-conducteur, les électrons peuvent transiter entre la bande de valence et la bande de conduction : soit si la bande interdite n'est pas trop importante ; soit en présence d'impuretés créant des niveaux intermédiaires dans cette bande interdite [3]. L'énergie nécessaire à ces électrons pour passer d'un niveau à un autre est au minimum égale à l'énergie de cette bande interdite :

$$\boldsymbol{E_C - E_V = E_g} \tag{1.13}$$

Ces transitions correspondent à une recombinaison des niveaux tendant à combler les trous de la bande de valence par la transition des électrons en provenance de la bande de conduction. Une méthode, pour générer ces transitions, consiste à créer artificiellement des trous dans la bande de valence (dopage). La transition de la bande de conduction à la bande de valence est alors assurée par un apport d'énergie extérieur (polarisation externe). C'est le cas des semi-conducteurs [3] [4].

Ce type de transition peut être soit non radiatif, auquel cas il n'y a pas émission de lumière, soit radiatif : il y a alors émission de rayonnement et c'est le cas des diodes électroluminescentes. Les transitions radiatives peuvent être naturelles ou stimulées.

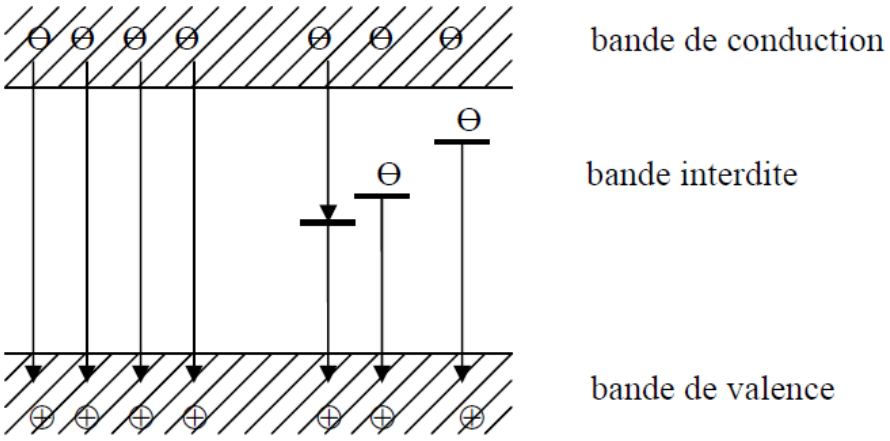


Figure 1.7 : Transition dans un semi-conducteur

b) Principe des diodes DEL

La base des diodes DEL est la jonction pn qui est constituée d'un semi- conducteur ayant en contact une zone dopée n et une zone dopée p. Lorsque la jonction pn est traversée par un courant direct, une émission spontanée de photon, due à la recombinaison de paires électron- trou, se produit [3] [4].

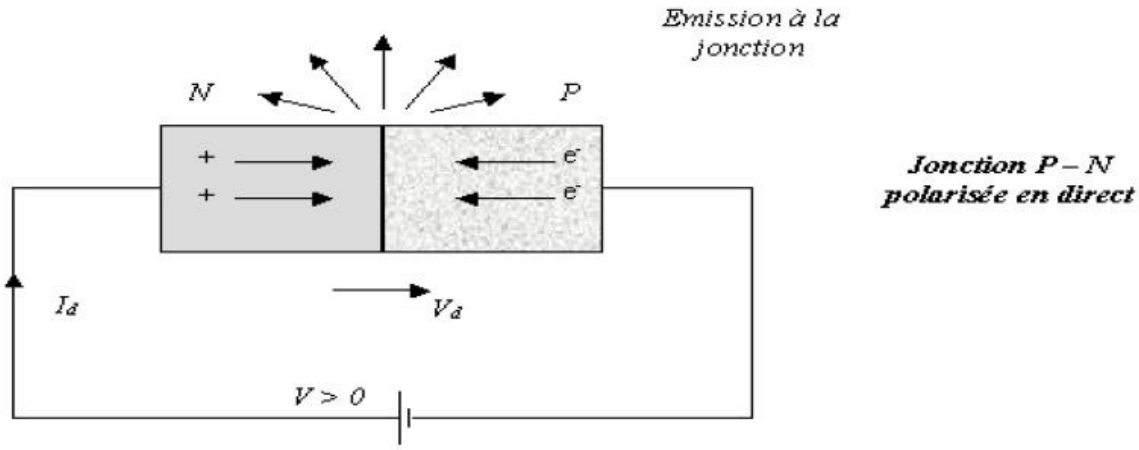


Figure 1.8 : Jonction PN polarisé en direct

c) Principe du laser

Le principe du laser ou Light Amplification by Stimulated Emission of Radiation est la combinaison de deux éléments essentiels :

- Un amplificateur d'ondes lumineuses ;
- Une boucle de réaction formant un résonateur.

L’amplificateur utilise les propriétés de l’émission stimulée d’un photon par une particule excitée. L’exploitation de cette émission stimulée nécessite une modification importante du milieu : l’inversion la plus importante possible de ses populations actives. L’émission stimulée s’accompagne de la création d’un photon. Si on s’arrange pour que la durée de vie des électrons soit suffisamment longue pour ne pas perturber le phénomène, on aura une émission induite plus forte que l’absorption : c’est l’effet laser. Ce photon ainsi créé a même direction, même phase, même polarisation et même fréquence que le photon incident. Le résonateur est une cavité optique dans laquelle l’onde lumineuse se réfléchit et s’amplifie. Le plus utilisé est le résonateur de Fabry-Pérot constitué de deux miroirs plans dont l’un est semi-transparent [4] [5].

Les diodes laser sont des semi-conducteurs dans lesquels on a recréé un milieu amplificateur avec sa cavité résonnante et dont l’inversion de la population est réalisée par un courant. Tant que l’on reste en dessous d’une valeur seuil de ce courant, la diode laser se comporte comme une diode électroluminescente classique ; dès que le seuil est atteint, l’inversion de population est réalisée et l’effet laser est déclenché.

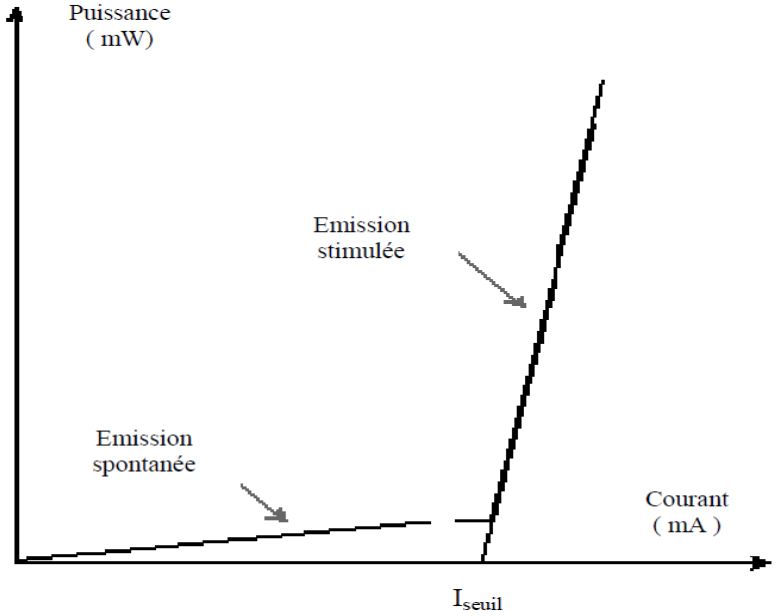


Figure 1.9 : Puissance émise par une diode laser

d) Techniques de modulation

Afin de transmettre des informations dans les systèmes numériques optiques, il faut les imprimer sur le signal à envoyer dans la fibre, c'est ce que l'on appelle une modulation. Pour cela, il est nécessaire de réaliser une conversion des données électriques en données optiques. Il existe principalement deux techniques : la modulation directe et la modulation externe [5] [6].

i. La modulation directe

Un des principaux avantages de l'utilisation des lasers à semi-conducteur pour les systèmes de télécommunications par fibres optiques réside dans le fait qu'il est possible de les moduler facilement : la modulation du courant qui les traverse entraîne directement la modulation en intensité de la lumière émise. Cette technique est appelée modulation directe. Ainsi, il suffit d'inscrire les données sur l'alimentation du laser.

Cette solution de modulation directe requiert assez peu de composants. En dehors de la source optique, le laser, seul un générateur de courant et un « driver » sont nécessaires. Le premier va émettre à un débit donné une séquence de données, expression de l'information à transmettre.
Le second a pour rôle de commander la source optique au niveau des puissances émises (en fixant les valeurs du courant d'alimentation). Pour cela, il modifie et transforme les niveaux du courant issu du générateur [5] [6].

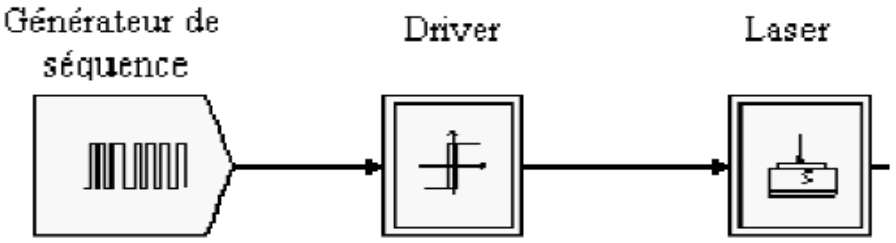


Figure 1.10 : Synoptique de la modulation directe

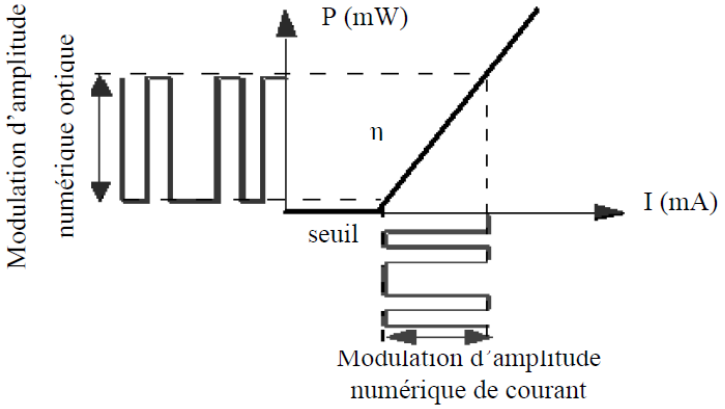


Figure 1.11 : Modulation directe d'une diode laser

La modulation directe connaît beaucoup d'avantages, en particulier le faible coût de mise en œuvre. Mais elle comporte aussi des limites. Les lasers en sont souvent la cause. Leur temps de réaction, les oscillations, le bruit créé font que la modulation directe engendre, pour les hauts et très hauts débits, certaines dégradations sur le signal optique modulé. A cela, la modulation externe constitue une solution plus pratique.

ii. La modulation externe

La modulation externe consiste à écrire les données électriques sur un signal optique continu. Elle est obtenue en modulant directement le faisceau lumineux en sortie du laser et non plus le courant d'alimentation à l'entrée du laser. Ainsi les défauts de la modulation directe qui incombent au laser ne seront plus présents sur le signal optique.
La modulation est effectuée sur une onde pure et constante et par un composant indispensable : le modulateur externe. Celui-ci est commandé par une tension externe v(t), modulée et représentative de l'information à transmettre. Cette tension appliquée au modulateur a pour propriété de modifier le facteur de transmission en intensité à la sortie.

Le signal optique continu émis par le laser alimenté par un courant constant est donc peu dégradé. En traversant le modulateur, il subit les modifications du facteur de transmission et le signal de sortie se trouve modulé selon v(t). Un driver est souvent présent entre les données et le modulateur afin de fixer les niveaux de v(t) et de choisir les modifications du facteur de transmission.

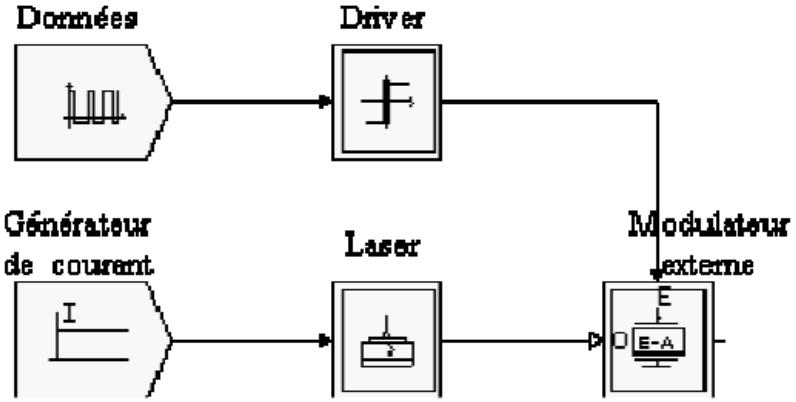


Figure 1.12 : Synoptique de la modulation externe.

La modulation directe, plus simple et moins coûteuse est encore très utilisée si les données sont transmises à un débit de quelques gigabits/s, selon la qualité du laser. Mais au-delà de 5 Gbits/s, la modulation externe est indispensable pour maintenir une qualité de transmission correcte. Cependant, les modulateurs ne sont pas parfaits et peuvent engendrer des défauts mais leurs impacts sont moins importants [7].

1.3 Interface optique de réception

Le rôle du récepteur optique est de convertir le signal optique en signal électrique d'origine et de retrouver les données transmises à travers la fibre [7].
Son principal constituant est un photodétecteur. Deux variantes de photodétecteur sont fréquemment utilisées dans une liaison par fibre optique :

- La photodiode PIN ;
- La photodiode à avalanche (PDA).

a) La photodiode PIN

La photodiode PIN est une photodiode classique dans laquelle on a inséré, entre les deux zones de porteurs, une région à forte résistivité (zone intrinsèque I). Dans cette zone, on appauvrit la quantité de porteurs libres en la faisant travailler sous tensions.
Lorsque la jonction est polarisée en inverse, la zone déplétée augmente et les porteurs majoritaires sont incapables de la traverser : le seul courant (Is), dit de seuil, qui subsiste est dû à la traversée des porteurs initialement minoritaires [7]

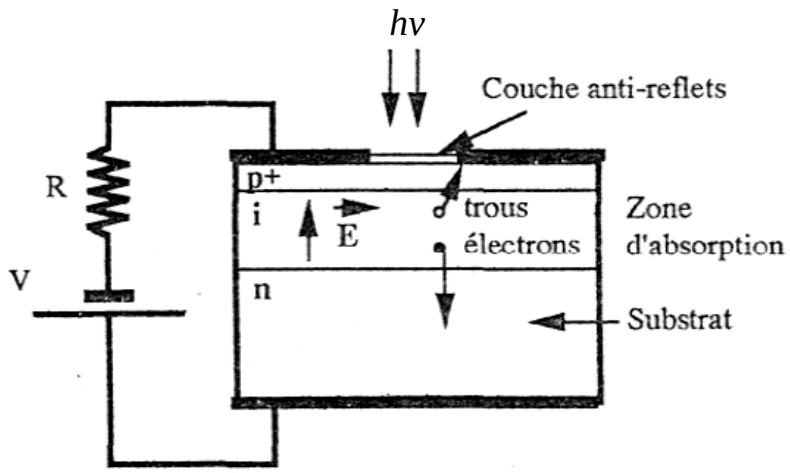


Figure 1.13 : Photodiode PIN

b) La photodiode à avalanche (PDA).

Le signal reçu étant souvent très faible, il est nécessaire d'amplifier le photocourant. On fait suivre la photodiode d'un amplificateur, mais le bruit de celui-ci est souvent prépondérant. Aussi a-t-on parfois intérêt à utiliser un composant à gain interne, la photodiode à avalanche ou PDA. Son principe est l'ionisation en chaîne, par impact, des porteurs, sous l'effet d'un champ électrique très intense. C'est l'effet d'avalanche qui, s'il n'est pas contrôlé, aboutit au claquage de la jonction [7] [8] [9].

1.4 Les photons

La lumière est un rayonnement électromagnétique ou un transfert d'énergie sous la forme d'ondes électromagnétiques. Elle est constituée, comme son nom l'indique, d'un champ électrique (champ E) ainsi que d'un champ magnétique (champ M). Les champs $\vec{E}$ et $\overrightarrow{M}$ sont perpendiculaires entre eux et sont contenus dans un plan perpendiculaire à la direction de propagation de l'onde EM.

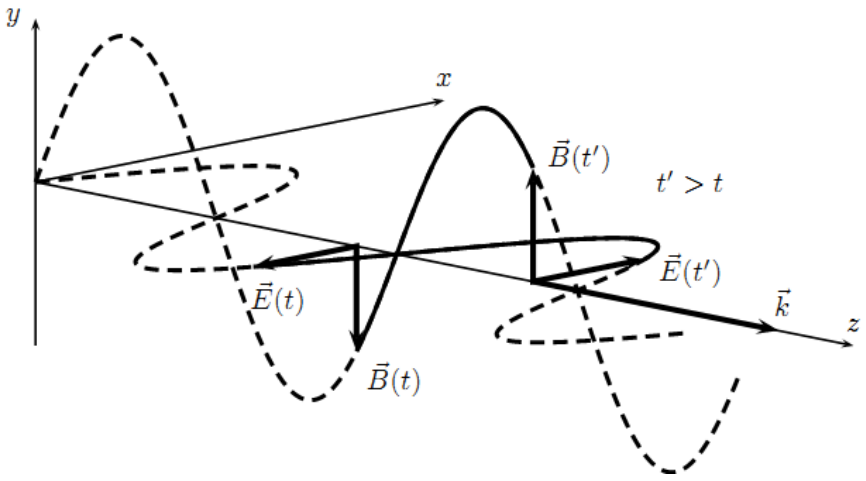


Figure 1.14: Structure de l'onde électromagnétique polarisée rectilignement selon Ox

La direction du champ $\vec{E}$ est la direction de polarisation de l'onde lumineuse. Ainsi la formule suivante exprime sa variation en fonction de t et z :

$$\overrightarrow{E} = E_0 \vec{e}_x cos(xt - kz) \quad (1.14)$$

Où w = kc avec c= $3x10^8$ $m.s^{-1}$ la célérité de la lumière dans le vide

Dans le cas présent ci-dessus, l'onde est polarisée rectilignement sur l'axe Ox. Les plans d'équation z = Constante sont des plans d'onde car le champ électrique y est le même en tout point à t donné [10]. Le photon est la particule élémentaire qui constitue le rayonnement électromagnétique. Il est un « paquet » d'énergie élémentaire ou quanta de rayonnement électromagnétique créé par l'échange entre deux particules. L'état quantique dans ce contexte est un ensemble des caractéristiques qui aident à décrire le photon: sa position, son énergie, sa polarisation. En communication quantique, le travail consiste à jongler avec des paires de photons dans des fibres optiques.

1.5 La polarisation de la lumière

La polarisation de la lumière correspond à la direction et à l'amplitude du champ électrique $\vec{E}$. Pour une lumière non polarisée ou naturelle, $\vec{E}$ tourne autour de son axe de façon aléatoire et imprévisible au cours du temps. La polarisation d'une lumière correspond à donner une trajectoire définie au champ $\vec{E}$. Si la lumière a une polarisation constante, on dit qu'elle est polarisée. Ce phénomène peut être appliqué à un photon individuel, c'est à dire la polarisation du photon définie par la direction de l'oscillation du champ électrique. Comme la lumière, le photon peut être polarisé par n'importe quel angle W dans le plan perpendiculaire à la direction de propagation du photon [11] [12].

1.6 La notion de mesure quantique

Un photon est une particule quantique donc il observe les lois de mécanique quantique. Telle qu'une théorie physique fondamentale de matière, la mécanique quantique a beaucoup de caractéristiques compteur-intuitifs. Parmi celles-ci, le principe de l'incertitude de Heisenberg est le plus approprié pour la cryptographie. Ce dernier a déclaré que la mesure de la valeur d'un état quantique implique une incertitude intrinsèque au sujet des valeurs de quelques autres états [13].

La mesure de l'état d'un système quantique n'est pas une fonction réelle comme dans la mécanique classique. Elle est représentée par un opérateur Hermitien sur l'espace spatiale linéaire de Hilbert H. Si l'état interne d'un système quantique comme la polarisation d'un photon est présenté par un vecteur normé |Y>=1 dans H, alors chaque mesure physique qui pourrait être réalisée sur le système correspond à la résolution de ce vecteur dans l'ensemble des vecteurs normés orthogonaux mutuels :

$$|Y> = |P_i|b_i> \quad (1.15)$$

Où P_i sont les grandeurs physiques des vecteurs de projection orthogonales correspondantes. Après la mesure, le système est dans l'état $|b_i>$ avec la probabilité $\|P_i|Y>\|$. [13] Ceci signifie que la mesure dépend du choix de l'ensemble de vecteurs de projection et elle est de nature probabiliste.

Grâce au principe d'incertitude de Heisenberg, on peut avoir deux déductions suivantes :

- La mesure en mécanique quantique : l'obtention d'information sur un système inconnu de quantum cause généralement une perturbation à l'état de quantum de ce système.
- Le théorème de non-clonage : il est impossible de dupliquer ou cloner un état quantique arbitraire.

1.7 Les réseaux par fibre optique

La technologie WDM est à la base des liaisons par fibres optiques. La WDM ou Wavelength Division Multiplexing ou « multiplexage en longueur d'onde » est une technique de multiplexage révolutionnaire qui, en succédant à deux autres modes de modulation, a marqué l'univers des réseaux hauts débits aussi bien au niveau des débits qu'au niveau des équipements de transmission.

a) Le principe de WDM

La fibre optique possède un vaste potentiel et surtout un avantage non exploité. Pour cela, sur une fibre optique, il est possible d'utiliser plusieurs longueurs d'onde simultanément. C'est justement sur ce principe qu'une technique de modulation a été mise en place avec de nombreux avantages mais tout de même quelques limites. L'idée est de reprendre le multiplexage fréquentiel utilisé dans les réseaux électriques pour l'appliquer dans le domaine optique.
Le principe de base du multiplexage en longueur d'onde est l'injection simultanée dans une fibre optique de plusieurs trains de signaux numériques sur des longueurs d'ondes distinctes. La fibre optique se prête d'autant plus à cela que sa bande passante est très importante. La norme ITU-T G692 définit la plage de longueurs d'ondes dans la fenêtre de transmission de 1530 à 1565 nm et un espacement normalisé entre deux longueurs d'ondes de 1,6 ou 0,8 nm. Ainsi le multiplexage de longueur d'onde se fait exclusivement sur fibre monomode [10] [13].

Aujourd'hui, il est possible d'atteindre des débits pouvant aller de 10 à 200 Gbits/s. En effet, il existe des systèmes proposant de 4 à 80 canaux optiques à 2,5 Gbit/s par canal.

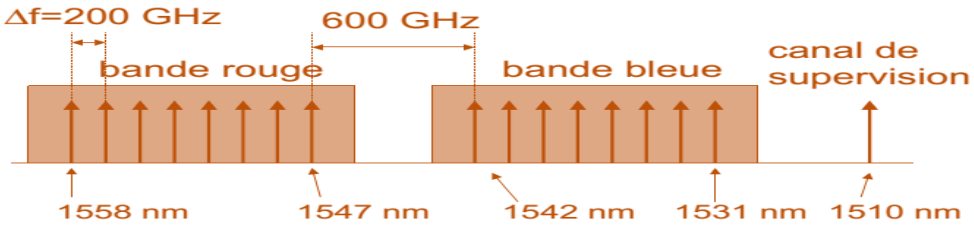


Figure 1.15 : Fenêtre des diverses longueurs d'ondes

b) La technologie DWDM ou multiplexage en fréquence

Le DWDM est une technique de multiplexage en fréquence. Supposons que nous pouvons utiliser les 12,5 Tbit/s de la fibre optique. Aucun appareil électronique n'est capable de travailler et de transmettre à un tel débit. L'idée est alors de diviser la bande de 12,5 THz en sous bandes.
Comme il s'agit de bande de transmission dans le domaine optique on appelle communément ces sous-bandes des « couleurs ». On peut ainsi pour une capacité de 12,5 Tbit/s utiliser 5000 couleurs de 2,5 Gbit/s, 1250 de 10 Gbit/s ou 312 de 40 Gbit/s.De plus, la technologie DWDM permet une économie notable sur les équipements : un équipement de 40Gbit/s coûte environ 2,5 fois plus qu'un équipement traitant à 10 Gbit/s. [13]

Technologie	Caractéristiques	Application, distance
DWDM	Stabilisation, Température laser 80λ	Longue distance,$> 100\ Km$
CWDM	Canaux de 20 nm Température laser non stabilisée, 18λ	MAN,$< 70\ Km$
WWDM	10GBase-LX4, 4λ, 1360 nm	Campus LAN, 40Km mono, 300m multimode
HDWDM	Plusieurs Centaines de λ	A l'étude

Tableau 1.1: Les technologies de la WDM

c) Réseau optique terrestre ou Backbone National

La conception de système de transmission à très grande capacité est désormais possible grâce à la technologie optique qui a pris place pour venir en renfort aux anciens systèmes de transmission FH ou faisceau hertzien et satellite. De plus, les échanges à travers ces systèmes vont être de plus en plus nombreux et la demande de services de plus en plus élevée.

Les différentes étendues de réseaux sont :

Du point de vue global, dans le monde de l'informatique et des transmissions, on distingue 3 capacité principales, ou types de réseaux s'organisant comme suit:

i. Les WAN ou Wide Area Network

Un vaste réseau déployé à l'échelle d'un pays, voire d'un continent pour cela, les nœuds sont de très grands centres urbains. La transmission de ces informations se fait sur fibre optique à une longueur d'onde de 1,55µm et à un débit élevé permettant de gagner en débit et en espacement entre les répéteurs par rapport aux systèmes existants, à savoir le câble coaxial dont la distance passe typiquement de 2 à 100 km [13] [16].

ii. Les MAN ou Metropolitan Area Network

Ce sont les réseaux mis en œuvre dans une grande ville ou une agglomération et permettant ainsi de relier entre eux par exemple des différents arrondissements. Déployés entre le dernier autocommutateur à autonomie d'acheminement du réseau longue distance et une zone plus précise, il possède un environnement souvent très complexe et divers.

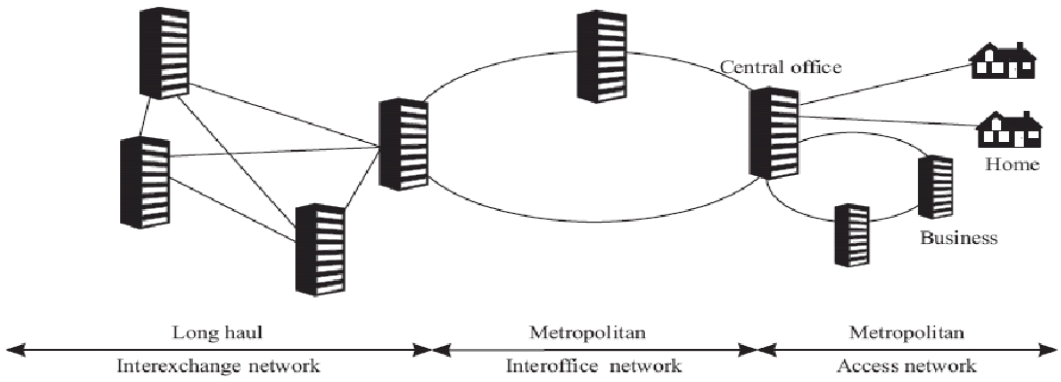


Figure 1.16 : Architecture globale d'un réseau

iii. Les LAN ou Local Area Network

Ce sont des réseaux de distribution qui représentent le dernier maillon et finissent d'acheminer les informations à l'abonné. Ils sont donc plus courts et moins gourmands en termes de capacité. Sa longueur varie de 2 à 50 km et sa capacité est, au plus, du même ordre de grandeur que celle du réseau métropolitain [13].

Mais des liaisons optiques commencent à prendre de l'ampleur au niveau local. Selon la localisation de la terminaison optique, différentes configurations sont envisageables:

- FTTH/FTTO (Fiber To The Home / Fiber To The Office):

C'est une terminaison de réseau optique, qui est propre à un abonné donné et implantée dans ses locaux. La fibre va donc jusqu'à son domicile ou son bureau, et la partie terminale en cuivre est très courte.

- FTTB (Fiber To The Building):

Cette terminaison de réseau optique est localisée soit au pied de l'immeuble, soit dans un local technique généralement situé en sous-sol, soit dans une armoire ou un conduit de palier

- FTTC/FTTCab (Fiber To The Curb / Fiber To The Cabinet):

C'est une terminaison localisée soit dans une chambre souterraine, soit dans une armoire sur la voie publique, soit dans un centre de télécommunications, soit sur un poteau.

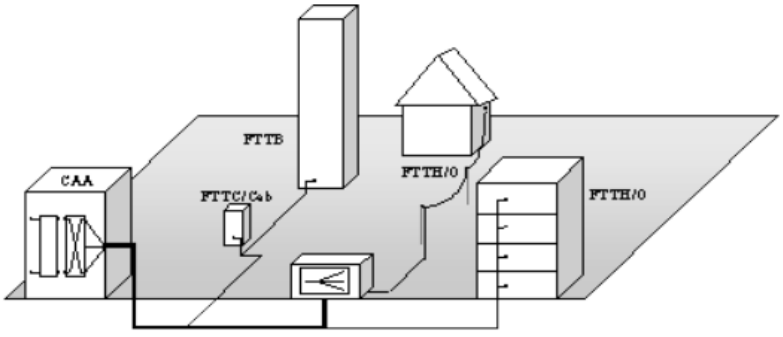


Figure 1.17 : Structure d'un réseau local

1.8 La sécurité des systèmes d'information

Un système d'information se présente sous trois formes : les données, les connaissances et les messages. C'est l'ensemble des moyens techniques et humains qui permettent de stocker, de traiter ou de transmettre l'information. Le concept de sécurité des systèmes d'information recouvre un ensemble de méthodes, techniques et outils chargés de protéger les ressources d'un système d'information afin d'assurer [14] :
– **La disponibilité des services** : les services et les informations doivent être accessibles aux personnes autorisées quand elles en ont besoin ;

– **La confidentialité des informations :** les informations n'appartiennent pas à tout le monde ; seuls ceux qui en ont le droit peuvent y accéder ;

– **L'intégrité des systèmes :** les services et les informations ne peuvent être modifiés que par les personnes autorisées. Elle indique l'ensemble des mesures à prendre, des structures à définir et l'organisation à mettre en place afin :

– D'empêcher la détérioration, l'utilisation anormale ou la pénétration des systèmes et réseaux ;
– de détecter toute atteinte, malveillante ou non, à l'intégrité, la disponibilité et la confidentialité des informations ;

– D'intervenir afin d'en limiter les conséquences et, le cas échéant, poursuivre l'auteur du délit.

1.9 La valeur et les propriétés d'une information

L'informatique et les réseaux de communication sont des composantes indispensables de la vie personnelle et professionnelle d'un nombre croissant de personnes. Leur bon fonctionnement est donc vital. La notion de bon fonctionnement des réseaux de communication se situe à deux niveaux du point de vue de la sécurité. Elle comprend :

• Les obligations légales : la protection des données à caractère personnel
• Les obligations professionnelles : fiabilité, disponibilité, performances, protection des données (intégrité et confidentialité), protection des accès (authentification), assurance sur l'interlocuteur (authentification, signature), il faut donc définir des politiques de sécurité.

Les algorithmes de chiffrement actuels qu'ils soient à clé symétrique ou asymétrique tels que RSA, DES, ECC, RC4, ont déjà été cassés et sont donc sans garantie. En effet, plus les ordinateurs sont puissants, plus la méthode brute force est efficace et plus les algorithmes de chiffrement sont vulnérables. La cryptographie chaotique, en contrepartie, répond aux exigences de sécurité et aux contraintes, à savoir une résistance très grande à la cryptanalyse combinée au maintien de tous les attributs nécessaires aux algorithmes de chiffrement.

1.10 Les failles système de transmission

Les solutions de défense sont nombreuses mais on peut distinguer :

- La sécurité des informations
- La sûreté des systèmes
- La gestion du risque qui se compose de:

- L'identification, authentification

- Les politiques d'autorisations et privilèges
- La gestion des droits et des privilèges
- Les contrôles d'accès logiques et physiques
- Les profils de protection, classes de fonctionnalités
- L'évaluation, certification, accréditation, agrément
- La journalisation ("audit") des événements liés à la sécurité

1.11 Protection physiques et logiques

La sécurisation des données transportées par longueur d'onde est donc une nécessité primordiale. Les méthodes classiques de chiffrement par des algorithmes mathématiques (AES, DES, DSA, RSA) demeurent inadaptés pour le haut débit. D'une part, ces derniers deviennent de plus en plus fragiles face à la montée en puissance des calculateurs, et d'autre part ils sont très longs pour fonctionner dans le domaine optique. Plus récemment, d'autres techniques de chiffrement matériel ont été introduits, telles que la cryptographie quantique et la cryptographie chaotique [14].

Valorisation de l'information et de la quantité de flux d'informations en transit au niveau international:

Ce dernier peut se décrire comme un système où l'information source est suffisamment protégée, de façon qu'une interception non autorisée soit difficile à réaliser de la part des adversaires potentiels. Par contre il n'est pas suffisamment sécurisé pour supporter une attaque sophistiquée, de la part d'un adversaire résolu et surtout disposant de gros moyens financiers, tel un gouvernement ou une grande société. Au contraire, un système est sécurisé si l'information transmise est bien protégée contre l'intrusion non autorisée des adversaires très sophistiqués et avec une grande puissance de calcul. La sécurité est échelonné suivant cette pyramide suivant selon moins sécurisé au plus sensible voir très sécurisé :

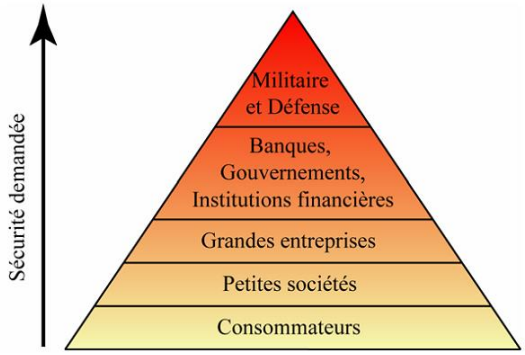


Figure 1.18: Classification système d'information

D'autre part, dans le cadre de transmission par fibre optique, mis à part la capacité de garantir la confidentialité des données, les critères les plus critiques à prendre en compte sont :

- La transparence par rapport à l'équipement déployé existant [14] [15].
- La capacité de transmission (le débit).
- L'impact sur la qualité de la transmission (QoT).

1.12 Conclusion

Ce chapitre nous a permis de savoir les principes de fonctionnement et les caractéristiques de la transmission par fibre optique. Nous avons aussi abordé la notion de sécurité de l'information. Dans le chapitre suivant nous allons voir la sécurisation en réseaux de communication par fibre optique.

CHAPITRE 2
SECURISATION EN TRANSMISSION OPTIQUE

2.1 Introduction

Les fibres optiques constituent, à l'heure actuelle, l'épine dorsale du réseau des télécommunications. La montée en débit réalisée ces dernières années a conduit au déploiement des réseaux SDH et WDM faisant office de réseaux de transport national, continental et intercontinental. Les données confidentielles : économiques, militaires ou diplomatiques ne doivent pas être captées simplement en interceptant le signal optique.

2.2 Vulnérabilité des fibres optiques

Généralement on pense que la fibre optique est un milieu de transmission sécurisée par sa nature, c'est-à-dire que qu'il n'est pas possible de pénétrer la fibre et de se brancher sur elle pour « écouter » sans l'endommager et/ou sans interrompre le flux transmis. Mais en réalité, la vulnérabilité des fibres est assez grande, à tel point que les dispositifs de libre commercialisation quotidiennement utilisés dans le monde entier pour entretenir les réseaux peuvent être adaptés pour être branchés sur le canal de transmission, avec une faible probabilité de détecter que le réseau a été pénétré. C'est pourquoi, les opérateurs des réseaux ne garantissent pas la protection de l'information. La (figure 2.1) montre la représentation schématique des deux façons simples d'agir pour récupérer l'information qui est transmise par la fibre. Il suffit de couder et/ou presser légèrement la fibre pour accroître la diffusion de la lumière, détecter et décoder la lumière diffusée et ainsi remonter aux données transférées par la fibre optique.

Par exemple, pour une « écoute » basique, seulement 0,1 dB (∼2%) de puissance fuite est nécessaire pour déterminer la présence et la direction du signal. Il existe des méthodes d'écoute plus sophistiquées qui profitent de la lumière naturellement diffusée par la diffusion Rayleigh. Donc, il est évident que les données transférées par une fibre optique sont absolument sensibles à l'espionnage et sûrement l'émetteur et/ou récepteur n'auront aucune chance de s'apercevoir [16] [17].

2.3 Équipement de capture ou d'intrusion pour fibre optique

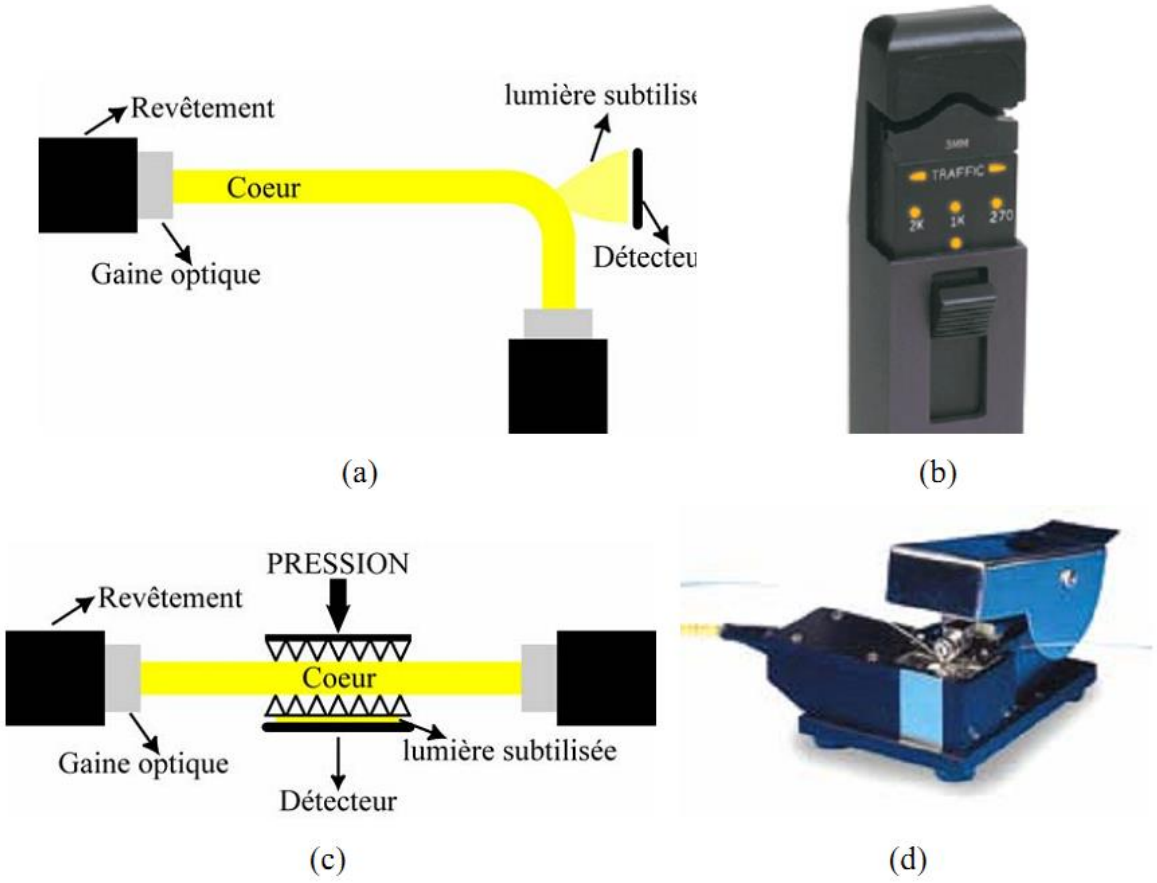


Figure 2.1: Détecteur optique, (a, b) la courbure de la fibre et (e, d) sur de micro courbure plus une pression.

La première solution qui vient à l'esprit est d'isoler les câbles. On pourrait les rendre inaccessibles si on les met à l'intérieur d'une structure de béton, ou similaire. Mais de cette façon on empêcherait tout accès, et il faut permettre toujours l'accès du service technique. D'autre part, il n'est pas viable de faire cela avec les câbles déjà déployés. Donc, comme les fibres seront toujours en «libre accès » il est difficile de détecter les attaques ; on est forcé de rendre illisible l'information auprès de l'intrus ou de lui rendre difficile la tâche de récupérer les données.

Il existe plusieurs façons d'approcher cette problématique de confidentialité ; par exemple, une approche au niveau software et/ou hardware par cryptographie algorithmique (au niveau de la couche d'application) et des approches au niveau de la couche physique, telles que la cryptographie quantique, la cryptographie par chaos et le brouillage [17] [18].

2.4 Protection physique

Les diverses techniques de cryptage sont acceptables ou non selon leur scénarios d'application. Notamment le niveau de sécurité requis dans les réseaux d'une société de développement d'armement et défense n'est pas le même que celui requis par la société qui distribue la télévision par fibre optique.

a) Cryptographie par algorithme

On fait référence dans ce cas aux approches qu'exploitent les divers champs des mathématiques, théorie de codes, probabilité, mathématiques discrètes, les architectures algorithmiques, les sciences de l'informatique et l'électronique.
Ces méthodes algorithmiques reposent normalement sur la capacité de calcul informatique. Ils sont exécutés sur la couche d'application avant la modulation de la porteuse optique et avec l'aide de l'électronique ou des ordinateurs.

Les systèmes cryptographiques basés sur ces méthodes sont groupés dans trois catégories de chiffrage : les symétriques, les cryptosystèmes à clé publique et les fonctions de hachage. On peut remarquer le DES (Data Encryption Standard) et l'AES (Advanced Encryption Standard) pour les systèmes symétriques et le RSA (Rivest Shamir Adelman) pour les systèmes asymétriques ou à clé publique [17] [18].

Dans les cryptosystèmes à clé publique, la clé de cryptage est connue ouvertement par les utilisateurs sans aucune contrainte. Par exemple, si on publie via internet la clé publique, quelqu'un peut crypter et envoyer un message sans aucun arrangement préliminaire par rapport à la clé. Cela est en contraste avec un algorithme de chiffrement symétrique, où les participants doivent se mettre d'accord sur une clé partagée et qui n'est pas connue de façon publique. Malgré ce gros avantage, la cryptographie symétrique est quelques ordres de grandeur plus rapide que les cryptosystèmes à clé publique. Pour cette raison, les systèmes de cryptographie symétrique sont utilisés dans la plus part des applications. Ces algorithmes sont implantés avec les technologies existantes en utilisant des ordinateurs ou circuits électroniques spécialisés.

La confidentialité des données transmises par fibre optique, et si on prend en compte que la tendance des réseaux optiques est d'intégrer de nouvelles technologies, par exemple DWDM pour rendre possible la transmission de grandes quantités de données, les cryptosystèmes électroniques ou par software tombent dans l'impossibilité de crypter les données à tel débit.

En bref, actuellement, la RSA de 1024 bits voir 2048 bits sont cassé ; les cryptographies asymétriques comme SSL et TLS sont déjà cassées ; les systèmes de cryptographie à base de factorisation, logarithme discret sont vulnérables [17] [18]. .

b) Approches physiques

La cryptographie ou la sécurisation de l'information au niveau physique peut être interprétée de deux façons. D'une part, quand la méthode et le système font reposer la confidentialité sur des propriétés physiques et d'autre part, quand le système de cryptage agit directement sur l'information physique à transmettre. D'ailleurs les deux sens d'interprétation ne sont pas exclusifs, par exemple, la cryptographie optique par chaos se base sur les propriétés de porteuses chaotiques pour cacher les données et en même temps elle agit entièrement sur les données dans son état physique.

Le but des approches physiques est de résoudre les principaux inconvénients des méthodes algorithmiques. Par exemple, la vitesse de cryptage et de décryptage. Baser la confidentialité sur des propriétés physiques donne aussi l'avantage de décorreler la capacité de résistance aux attaques des facultés informatiques et de calcul des intrus. On remarque qu'à la base, la cryptographie physique est tout à fait complémentaire des méthodes algorithmiques exécutées sur la couche d'application.

De cette façon la sécurité peut dépendre simultanément des deux approches : de la complexité informatique et des propriétés physiques [17] [18].

i. Cryptographie quantique

La cryptographie quantique a été proposée en 1983 par Stephen Wiesner, et en 1984 par Charles Bennett et Gilles Brassard. Cette méthode se base sur l'énoncé de la physique quantique qui affirme qu'il n'est pas possible de faire une mesure sans perturber le système.

Pour assurer la validité de cet axiome, il faut coder l'information en états non orthogonaux. Par exemple sur des photons individuels, les états de polarisation verticale et horizontale peuvent coder les valeurs de bit 1 ou 0, respectivement. Une autre base peut être constituée par les états de polarisation linéaire à ±45°.

Donc, si l'émetteur et le récepteur partagent l'information en utilisant un système quantique, par exemple des photons individuels, ils auront l'occasion de savoir quand un intrus a essayé de détecter leur information. Par conséquent, l'intrus ne pourrait pas obtenir l'information sans introduire des perturbations qui révèlent sa présence [18].

L'émetteur et le récepteur vont découvrir la présence d'un intrus mais après avoir échangé le message. De cette façon, il est possible de partager théoriquement, avec une parfaite sécurité, des clés secrètes pour crypter/décrypter des messages. Cette méthode est connue comme la distribution quantique de clé.

La distribution quantique de clé est le complément parfait des méthodes symétriques de cryptage, car elle « résoudrait » la problématique autour du partage des clés entre l'émetteur et le récepteur sans que l'intrus ait l'occasion de « pirater » les clés. Des récents résultats montrent qu'il est possible de partager une clé de 192 bits tous les 10 secondes sur une portée de 50 km [18] [19].

ii. Cryptographie par Chaos

Le terme chaos définit un état particulier d'un système dont le comportement ne se répète jamais qui est très sensible aux conditions initiales, et imprédictible à long terme. Le chaos a ainsi trouvé des nombreuses applications dans les domaines tant physiques que biologique, chimique ou économique. Ainsi, nous nous intéresserons principalement dans ce chapitre aux systèmes dynamiques chaotiques basés sur les espaces de phases, les attracteurs étranges et les scénarios de transition vers le chaos appelés aussi bifurcations, lesquels nous permettront de mieux comprendre la nature du chaos. Le chaos est le comportement qu'on observe dans certains systèmes dynamiques non-linéaires. Le caractère chaotique fait référence à l'évolution d'une ou plusieurs variables dans le temps et/ou dans l'espace.

Les systèmes chaotiques sont sensibles aux conditions initiales, en générant un comportement déterministe et apparemment aléatoire (pseudo aléatoire). L'évolution des variables chaotiques est contrôlée par des principes physiques bien définis, en permettant la définition des équations de mouvement du système en question. Ainsi on peut toujours obtenir les mêmes valeurs, à condition d'avoir la même fonction chaotique et les valeurs initiales.

Le comportement pseudo aléatoire confère aux signaux chaotiques des propriétés qualitatives proches de celles du bruit, tel que la périodicité non mesurable, la présence de fluctuations à différentes échelles du temps, le désordre apparent et le non prévisibilité de l'évolution [18].

Ces propriétés du chaos ont des applications en cryptographie à cause de la difficulté de faire des prédictions sur le système chaotique. Le caractère « bruité » est un élément d'importance qui peut apporter la sécurité aux communications, car l'émetteur peut masquer les messages dans le signal chaotique, et prévenir de cette façon la détection non désirée du message secret.

D'autre part, à cause de la sensibilité aux conditions initiales des fonctions chaotiques, une légère différence dans la valeur initiale employée pour crypter par le chaos va donner des différences très importantes dans les données cryptées. Cette propriété peut être l'interprétée comme une bonne résistance aux attaques du type force brute. Soit un schéma synoptique d'un système de communication par chaos suivant :

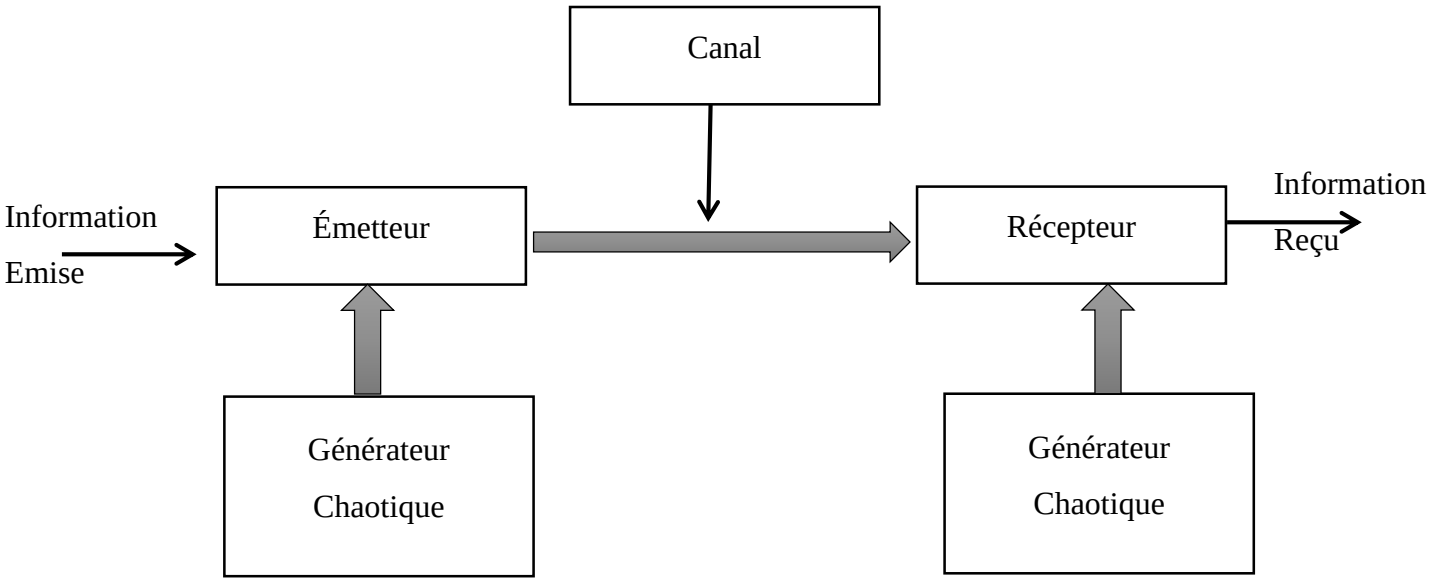


Figure 2.2 : Principe d'une communication sécurisée par chaos

La communication entre deux systèmes chaotiques peut s'établir grâce à la synchronisation. Brièvement, la synchronisation signifie que l'évolution irrégulière dans le temps, par exemple, de la puissance optique d'émission d'un laser chez l'émetteur, peut être reproduite par le laser du récepteur. Avec la capacité de synchronisation, le récepteur est capable de filtrer la porteuse chaotique et d'extraire le message depuis le signal transmis. La clé de cryptage dans un système de cryptographie par chaos est basée sur les paramètres de réglage du système chaotique.

La cryptographie par chaos basée sur une architecture optoélectronique avec contre-réaction a été démontrée expérimentalement pour crypter des PRBS (Pseudorandom Binary Sequence) messages NRZ (Non Return to Zero) à 3 Gb/s et avec TEB de 7x10-9 pour une configuration « back-to-back ». La figure ci-dessus montre le schéma de l'architecture du l'émetteur chaotique de ce système [19] [20].

Il existe plusieurs techniques de chiffrement par chaos qui peuvent servir comme moyen de masquage de l'information dans le chaos, nous décrivons ici quelques-uns :

- **Chiffrement par addition**

Dans cette méthode appelée, masquage chaotique, l'émetteur est un système chaotique autonome dont le signal de sortie y(t) est ajouté au signal du message m(t). La somme de deux signaux est transmise au récepteur à travers le canal de transmission, qui est un canal public. Le récepteur est constitué d'un système chaotique identique à l'émetteur et un simple soustracteur. Ainsi, après la synchronisation des deux systèmes chaotiques (émetteur et récepteur), le message est extrait à l'aide d'une opération de soustraction.(Figure 2.3)

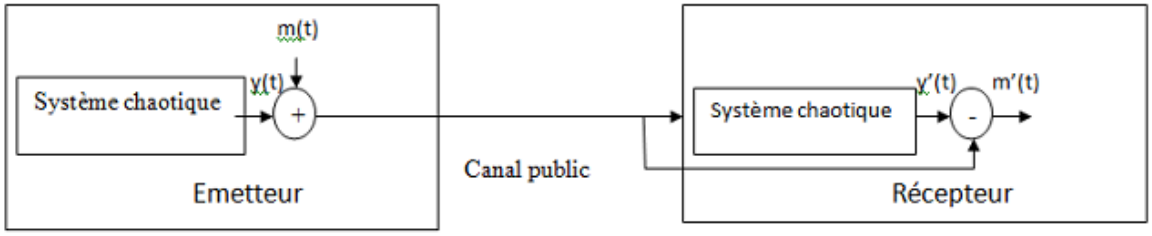


Figure 2.3 : Principe du chiffrement chaotique par addition

- **Chiffrement par commutation**

Cette méthode Chaos Shift Keying, est utilisée pour transmettre un message binaire. L'émetteur est composé de deux systèmes chaotiques et pour chaque niveau de message m(t) (0 ou 1), l'un des systèmes envoi sa sortie sur la ligne de transmission. Ainsi, le signal transmis commute entre deux attracteurs étranges [19] [20]. Le récepteur est constitué de deux systèmes chaotiques identiques à ceux de l'émetteur et un bloc de comparaison permet de relever la valeur du message noté m'(t).

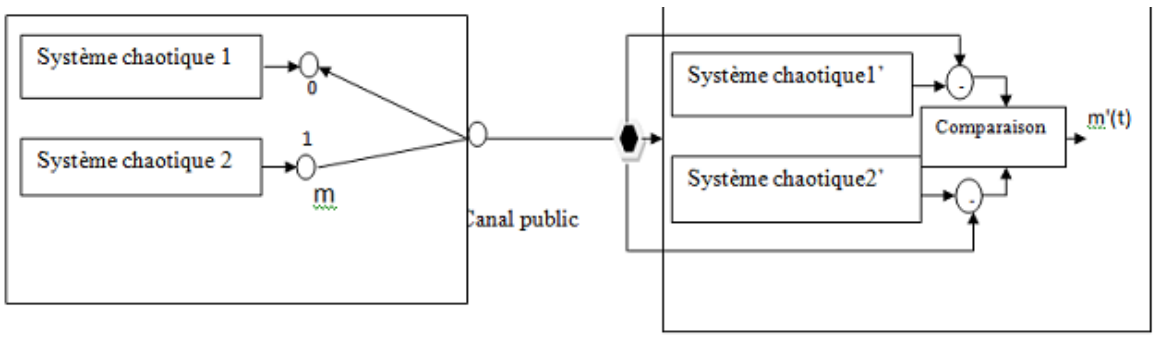


Figure 2.4 : Principe du chiffrement chaotique par commutation

- **Chiffrement par modulation**

Cette technique utilise le message contenant l'information pour moduler un paramètre de l'émetteur chaotique. Un contrôleur adaptatif est chargé de maintenir la synchronisation au niveau du récepteur, tout en suivant les changements du paramètre modulé. Le schéma correspondant est présenté à la figure. Au niveau de l'émetteur, le fait de moduler un (ou plusieurs) paramètre(s) impose à la trajectoire de changer continûment d'attracteur, et de ce fait, le signal transmis est plus complexe qu'un signal chaotique normal. Cependant, la façon d'injecter le message et

donc la fonction de modulation des paramètres ne doit pas supprimer le caractère chaotique du signal envoyé au récepteur. Il est important de souligner que cette technique exploite pleinement les qualités des systèmes chaotiques.

Elle n'a pas d'équivalent parmi les systèmes de communication classique. Cependant, le cryptage par modulation s'est avéré sensibles à certaines attaques [19] [20].

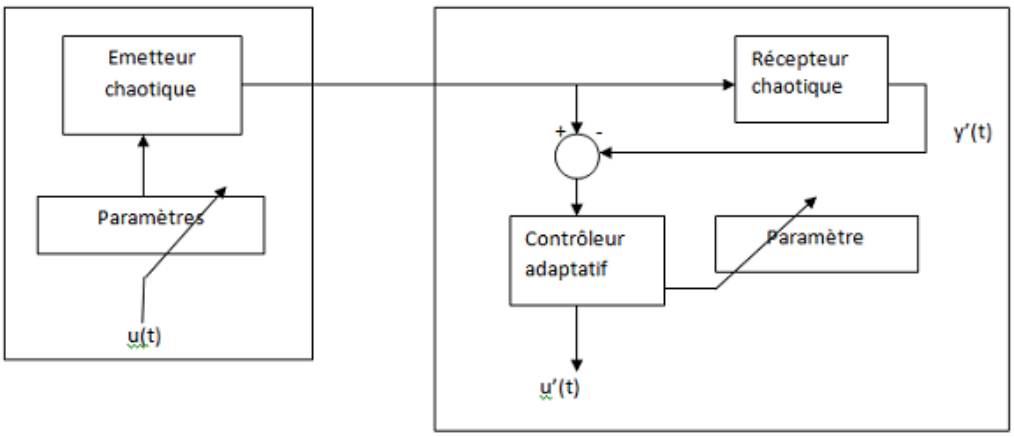


Figure 2.5 : Principe du chiffrement chaotique par modulation

Le schéma synoptique ci-dessous nous montre un émetteur chaotique optoélectronique à base de modulateur MZI.

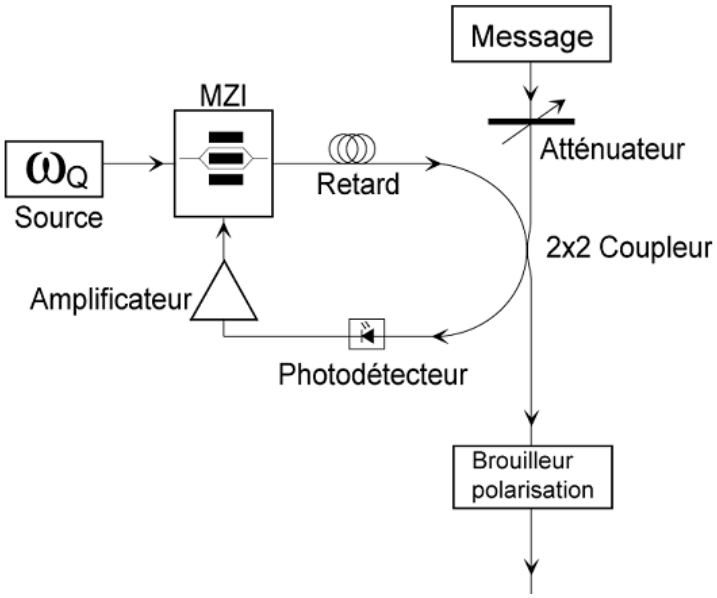


Figure 2.6 : Schéma synoptique d'une émettrice chaotique optoélectronique

iii. Brouillage Optique

Le brouillage est une opération de « filtrage » qu'on réalise sur les signaux analogiques avec le but rendre difficile la détection directe de l'information que l'émetteur envoie au récepteur. À la réception, pour débrouiller le signal, le récepteur applique la transformation inverse. Généralement, le brouillage est réalisé en utilisant un système qui permute le signal dans l'espace temporel ou qui déforme le signal dans l'espace fréquentiel grâce à l'utilisation des filtres ou des convertisseurs de fréquence.

Bien que le niveau de confidentialité des systèmes de brouillage soit indéterminé, comme pour la cryptographie par chaos, on peut le qualifier peut fiable. Par conséquence, ces systèmes ne peuvent pas être utilisés pour crypter information de haute sensibilité ou « top-secret ».
Autrement dit, le brouillage n'est pas sécurisé mais « faiblement sécurisé ». En faisant attention à la classification précédemment présentée dans la figure 1.18, on peut dire que le brouillage s'adapte bien aux applications des deux premiers niveaux de la pyramide.

La principale qualité des systèmes de brouillage optique est leur capacité de crypter et décrypter rapidement, de façon à pouvoir traiter un vaste volume de données à haut débit [19] [20]. On va montrer aussi qu'ils sont non invasifs ; ainsi ces systèmes ont la possibilité de s'intégrer dans les réseaux optiques WDM actuels, parce que les effets induis par la transmission dans les fibres optiques sont bien tolérés et la QoT peut se préserver sans problème pour des applications de portées équivalentes aux réseaux métropolitains (de 200 km à 300 km).

iv. Les systèmes de cryptage quantique dédiés aux réseaux optiques

Dans les systèmes de cryptage quantique dédié à la sécurisation des données en transmission sur fibre optique, les grandeurs polarisation, phase, fréquence, temps sont utilisés pour le codage. Ainsi on distingue :

- Codage en polarisation
- Codage en phase dans le domaine temporel
- Codage en phase dans le domaine fréquentiel

- Codage par polarisation

Ce type de codage consiste à manipuler les bases de l'unité (bit/qubit) de l'information suivant la propriété de polarisation. Nous allons le détailler dans le prochain chapitre. Il est schématiquement représenté comme ci-dessous :

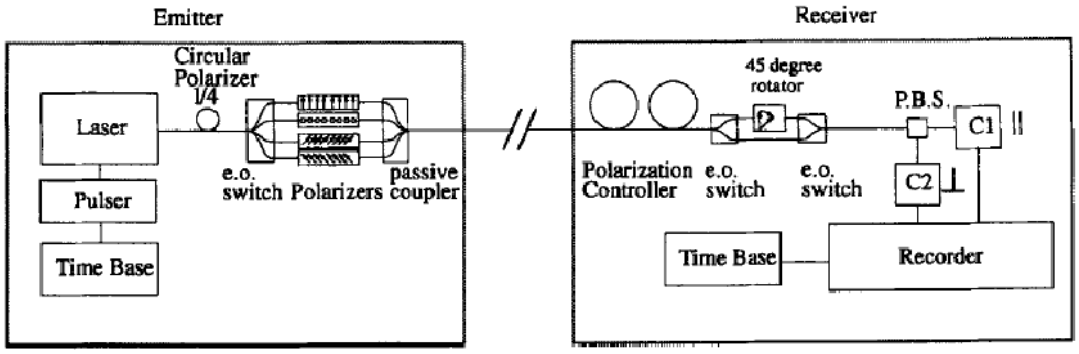


Figure 2.7 : Synoptique du principe de codage suivant la polarisation

- Codage en phase dans le domaine temporel

Cette technique consiste à faire variée la phase d'un signal lumineux par rapport à une base temporelle transcrivant l'information à transmettre. Le schéma ci-dessous montre les différents processus pour cette méthode :

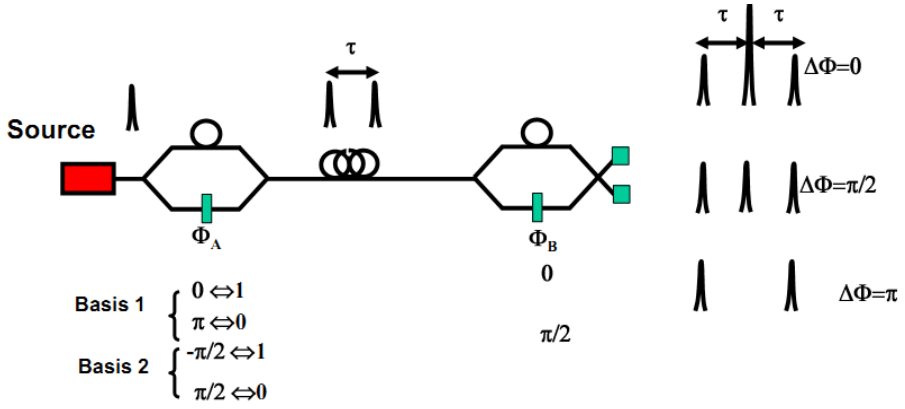


Figure 2.8 : Synoptique du principe de codage dans le domaine temporel

- **Codage en phase dans le domaine fréquentiel**

Toutes les opérations permettant de modifier les différentes composantes spectrales d'un état quantique, et donc de coder l'information en utilisant explicitement des modes du champ à différentes fréquences. Nous ne décrirons ici que les opérations aisément réalisables expérimentalement, plus particulièrement avec des composants optiques utilisés dans les télécommunications optiques comme : les modulateurs Mach Zender (MZ), les sources laser, les filtres optiques, et les détecteurs. Le schéma ci-dessous montre le synoptique pour la réalisation d'un système de cryptographie par codage en fréquence.

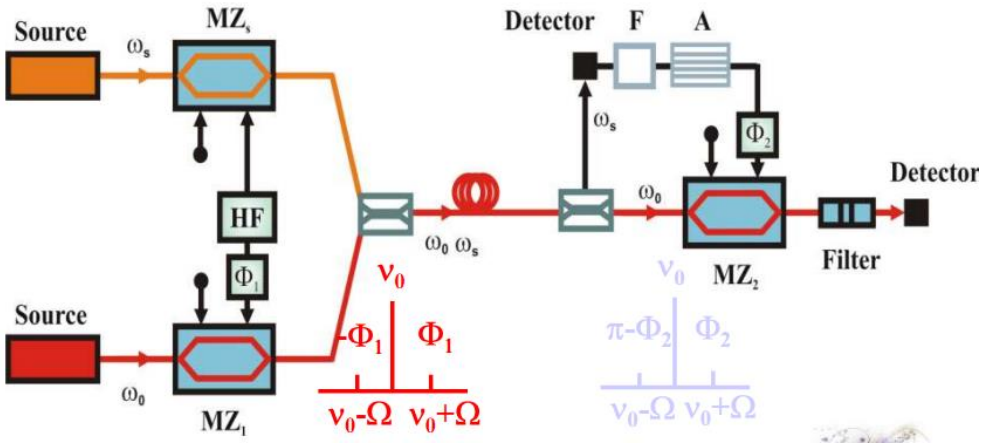


Figure 2.9 : Synoptique du principe de codage dans le domaine fréquentiel

2.5 Conclusion

La fibre optique est un support le plus utilisé pour les transports de données de type différent. Toutefois elle est vulnérable aux attaques ou intrusion extérieur. Plusieurs techniques sont utilisées pour la sécurisation de l'information notamment de méthode algorithmique et des méthodes physique. Certains d'entre eux sont moins efficaces que d'autre mais la cryptographie quantique est plus intéressante en matière de sécurisation. Le chapitre suivant nous en dira plus.

CHAPITRE 3 CRYPTOGRAPHIE QUANTIQUE

3.1 Introduction et définition

Depuis l'antiquité et dans la plupart des civilisations, la cryptographie est utilisée pour protéger les messages de façon à assurer leur intégrité, confidentialité et authenticité, et aussi pour leur stockage ou pour leur transmission. Au fil du temps, les techniques sont devenues complexes, passant des algorithmes de chiffrement rudimentaires comme le chiffre de César, chiffre de Vigenere à des algorithmes de cryptographie symétrique comme la RSA, DSA.
La cryptographie classique, qui est celle qui n'utilise pas la mécanique quantique, se base sur des propriétés mathématiques. Cette technique est limitée, et ne s'adapte pas à la technologie contemporaine. Une découverte mathématique permettant d'accélérer le calcul d'une opération particulière peut détruire un protocole de cryptographie classique. La cryptographie quantique se base sur les principes physiques de la mécanique quantique.

Aucune découverte technologique ne peut contredire les principes physiques, ce qui nous donne un protocole sûr à long terme. La sécurité assurée par les fondements de la physique quantique, de plus grâce à la mécanique quantique, nous serons capables, dans un futur proche, de réaliser un ordinateur quantique se basant sur les propriétés de la mécanique quantique pour son fonctionnement. Une vue générale de la cryptographie quantique est donné ci-dessous :

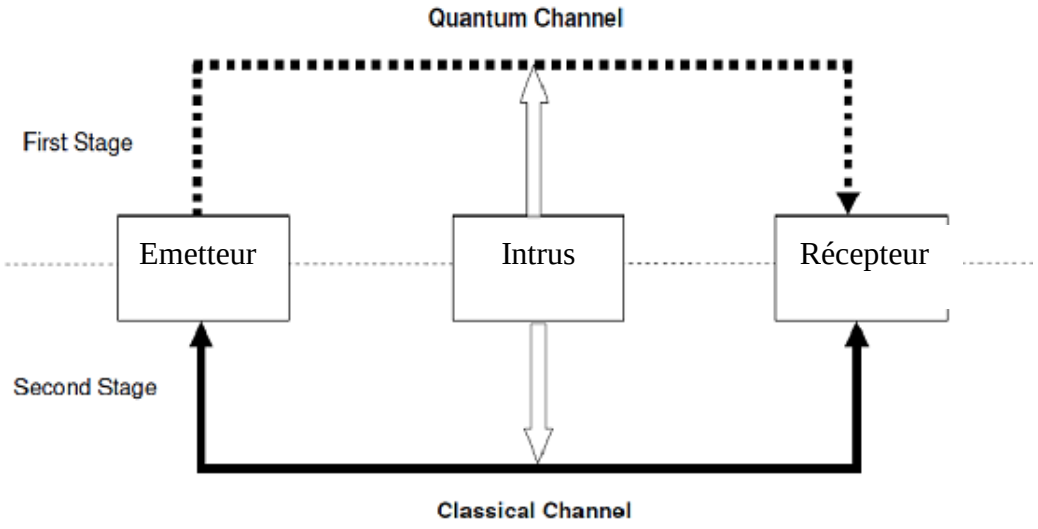


Figure 3.1 : Les systèmes de communication quantique

- **Le canal quantique**

Il s'agit d'un câble de fibre optique permettant la transmission des photons. C'est ce canal qui est hautement sécurisé pour le partage des clés.

- **Le canal classique**

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

3.2 La détection quantique

Le principe de la photo-détection quantique est extrêmement simple : il s'agit, à l'aide d'un photon, de faire transiter l'électron entre un niveau de base, où il ne conduit pas l'électricité, et un niveau excité où il va la conduire. Le semi-conducteur pur peut par exemple faire office de photodétecteur quantique (fig. 3.2): à l'état de base, il ne conduit pas le courant, mais un photon peut créer, par effet photoélectrique, une paire électron-trou et placer un électron dans la bande de conduction, permettant le transport du courant. Le schéma ci-dessous décrit le principe :

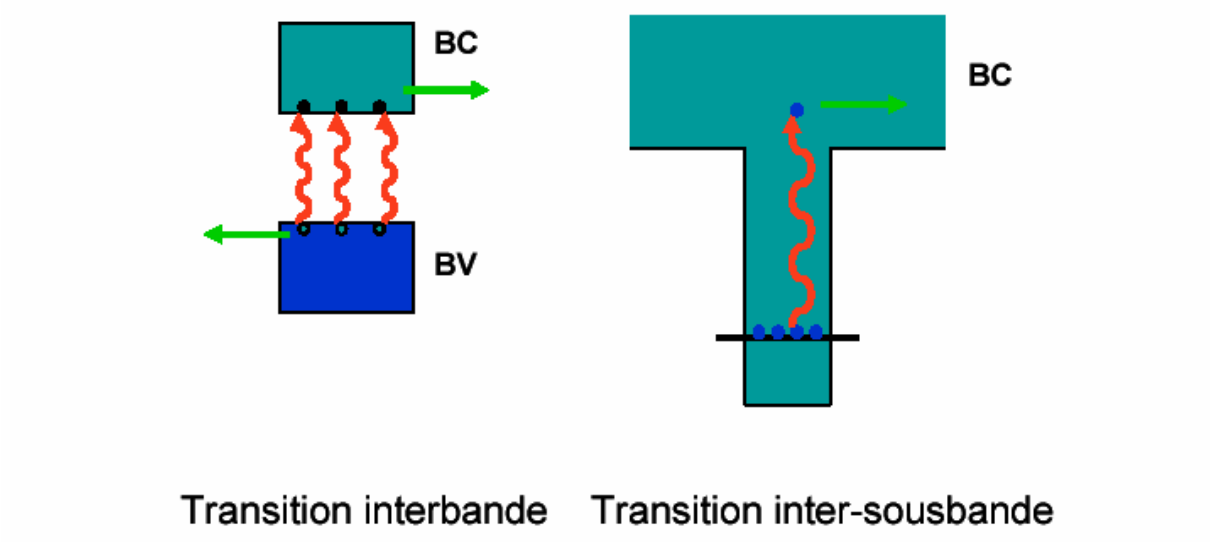


Figure 3.2: Deux mécanismes de détection quantique. A gauche, on utilise la structure de bande d'un semi-conducteur. A droite, un puits quantique

La physique des particules est gouvernée par les lois de la mécanique qui a été découverte au 20 ème siècle, une nouvelle discipline a vu le jour, » la théorie de l'information », qui définit le concept de l'information et sa description mathématique. De ce fait, il est désormais possible de connaitre de manière quantitative une information, ainsi que les dégradations qu'elle peut subir. Claude Elwood Shannon a démontré que, pour avoir une sécurité parfaite mathématiquement, on doit avoir une clé unique aussi longue que le message, et ce pour chaque message échangé. Cette trouvaille a comme faiblesse de devoir transmettre une clé aussi longue que le message de façon sécurisée.

En utilisant la théorie de la mécanique quantique, la théorie de l'information ainsi que le code de Vernam, Bennett et Brassard ont proposé un protocole en 1984 appelé cryptographie quantique(BB84). Le but est la transmission d'une clé de façon sécurisée. En effet, la plupart des protocoles de sécurité sont connus et utilisés n'est pas une faille en soi. C'est ainsi que, par la suite, cette clé pourra être utilisée par n'importe quel protocole de cryptographie classique. Néanmoins, le code de Vernam assure une sécurité absolue. De plus, la distribution de la clé aléatoire doit être unique et secrète, les transmissions erronées doivent être corrigées, qu'elles soient causées par un espion ou par les imperfections du système physique.

Enfin puisque l'espion ne doit rien connaitre initialement sur la clé, on doit réduire sa connaissance éventuelle de celle-ci.

3.3 Cryptographie quantique :

- Principe de la communication quantique selon le schéma ci-dessous :

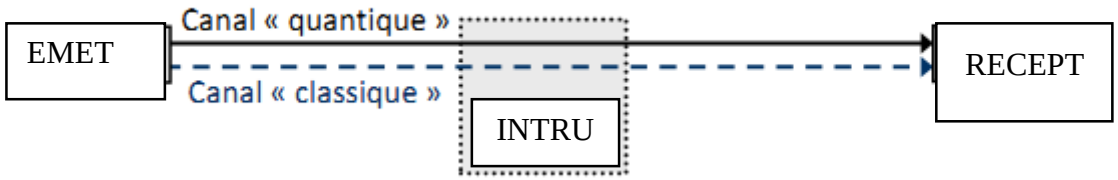


Figure 3.3 : Synoptique communication Quantique

Pour espionner un "canal de communication quantique", l'intrus doit effectuer des mesures sur des quantas individuels. Comme par exemple: impulsions à un photon [21] [22]

• Mais la physique quantique nous dit que "toute mesure effectuée sur un système quantique le perturbe".
• Donc "lire" le signal quantique diminue la corrélation entre les données partagées par l'émetteur et le récepteur.
• L'émetteur et le récepteur peuvent détecter l'intervention de l'intrus en comparant via un canal de communication classique un échantillon des données obtenues avec le signal quantique

Remarques
Le canal quantique n'est pas utilisé pour transmettre un message, c'est-à-dire une information existante. Seule une "clé" est transmise.
• S'il s'avère que la clé est corrompue, l'émetteur et le récepteur la jettent donc pas de perte d'information. Par contre, si la clé passe le test avec succès, alors l'émetteur et le récepteur peuvent l'utiliser en toute confiance.
• La confidentialité de la clé doit être contrôlée avant que le message ne soit envoyé par l'émetteur au récepteur.

- La cryptographie quantique sur les fibres optiques:

Qu'est-ce qui est vraiment quantique dans la cryptographie quantique et comment elle est mise en œuvre en pratique sur la fibre optique. C'est le fait de transmettre des flux de signal, optique à travers un support fibre. On a comme exemple de caractéristique d'un canal optique suivant :
λ=1550 nm ou 1300 nm
$T= 10^{-\alpha l}$ avec α= 0.25 dB/Km
Portée de la transmission : 50 à 100 km
QKD et interférométrie (équipement fibres optiques) [23]

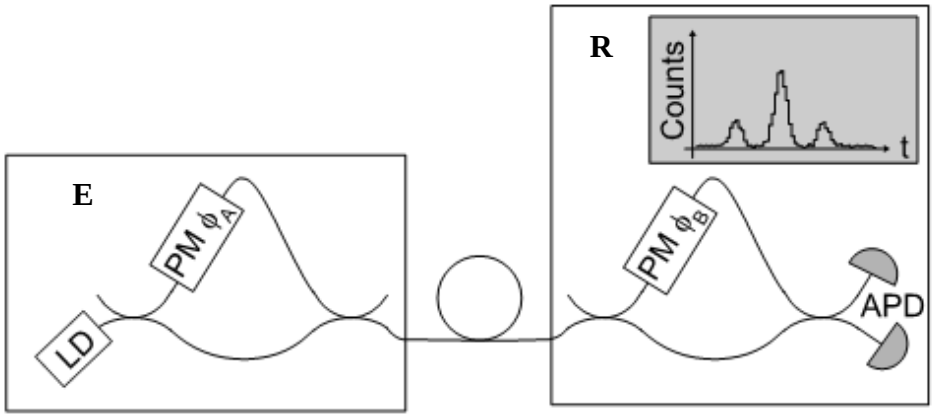


Figure 3.4 : Schéma de mise en œuvre sur support optique

3.4 Bruit des détecteurs

La détection au niveau du récepteur consiste à détecter les photons au niveau des états de polarisation de façon aléatoire et en même base que l'émetteur. La probabilité de détection est donnée par la formule suivante :

$$P = \mu T \eta \qquad (3.1)$$

Probabilité de fausse détection est $\mathbf{p_{dark}}$ et :

$$QBER = p_{dark}/\mu T\eta$$

$$T= 10^{-\alpha l/10} = p_{dark}/\mu\eta QBER$$

$$l = \frac{10}{\propto}\log_{10}\frac{\mu\eta QBER}{p_{dark}} \qquad (3.2)$$

Avec l la longueur de la fibre de transmission, α la constante d'atténuation
Le tableau suivant présent quelques valeurs de p_{dark}, α, η, l_{max}, en fonction de la longueur d'onde utilisée pour la transmission [25].

Λ	p_{dark}	A	H	l_{max}	
800 nm	10^{-8}	2 dB/km	50%	28 km	(μ = 0,1)
1300 nm	10^{-5}	0,35 dB/km	20%	65 km	
1550 nm	10^{-5}	0,25 dB/km	10%	80 km	

Tableau 3.1 : Exemple de valeurs résultantes de la longueur d'onde

- La confidentialité de la transmission des données se base sur deux étapes :

- La distribution de la clé quantique

- L'algorithme de cryptage

Si l'une de ces étapes est corrompue, la transmission de l'information des données de manière confidentielle n'est plus assurée. Mais comment réaliser la distribution de la clé de manière confidentielle. La mécanique quantique a des propriétés qui permettent de savoir si un espion a tenté d'obtenir des informations sur la clé que deux personnes voulaient s'échanger (le récepteur et l'émetteur) à travers un canal quantique [24] [25].

3.5 La théorie de l'information

La théorie de l'information est essentielle dans la cryptographie quantique. Avec le langage de la théorie de l'information [24].

$$I_{AB} > \max\{I_{AE}, I_{BE}\} \quad (3.3)$$

Avec :

I_{AB}: L'information mutuelle entre l'émetteur (A) et le récepteur (B)

I_{AE}: L'information mutuelle entre l'émetteur (A) et l'intrus (E) (respectivement I_{EB})

Ainsi donc on décide de garder la clé secrète ou de le renvoyer car l'intrus l'a intercepté. On peut visualiser cette notion de quantité d'information intercepté par la courbe ci-dessous :

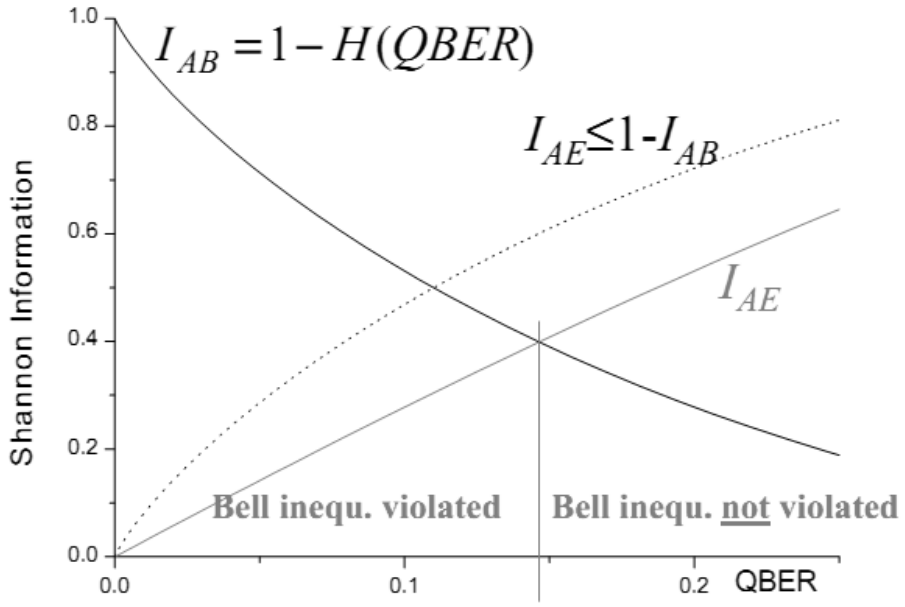


Figure 3.5 : rapport d'analyse entre QBER et quantité d'information

a) Entropie de Shannon H (X)

L'entropie de Shannon a diverses significations :

-L'entropie de Shannon est la moyenne de la longueur d'un message, c'est-à-dire qu'une augmentation de la moyenne de la longueur d'un message augmentera l'entropie de Shannon.

-Plus l'entropie de Shannon est grande sur une variable, plus cette variable a un contenu aléatoire de la variable augmentera l'entropie de Shannon.

-Symétriquement, plus l'entropie de Shannon est grande sur une variable plus on a de l'information nouvelle, et moins elle a de chance d'apparaitre. Inversement, une information connue n'apportera aucune information nouvelle. Son contenu ne sera pas aléatoire. Son entropie sera nulle.

Certains messages peuvent avoir une probabilité d'apparition différente. Ainsi les messages avec forte probabilité devront être codés sur un nombre petit de bits, alors que ceux qui ont une faible probabilité pourront être codés sur un nombre de bits envoyés d'un lieu à autre, ce qui implique une augmentation de la vitesse de transmission de l'information.

L'entropie d'une variable aléatoire pouvant valoir un ensemble de messages différents se trouvant dans l'ensemble χ vaut :

$$H(\chi) = -\sum_{x \in \chi} p(x) * \log\big(p(x)\big) \text{ bits} \qquad (3.4)$$

Où p(x) représente la probabilité d'avoir la valeur de x. L'entropie sera toujours supérieure ou égale à zéro [25] [26].

b) L'information mutuelle

L'information mutuelle émise par la source est représentée par X et l'information reçue par le destinataire est représentée par Y. Soit p (y|x) est la probabilité d'avoir « y » sachant qu'on a émis « x ». L'information mutuelle (ou entropie mutuelle) est définie par :

$$I(X ; Y) = H(X) + H(Y) - H(X, Y) = I(Y ; X) \qquad (3.5)$$

Shannon a démontré que le taux de transmission ne pouvait pas dépasser I(X ; Y).

3.6 Réalisation physique d'un qubit

a) Etats internes d'un atome

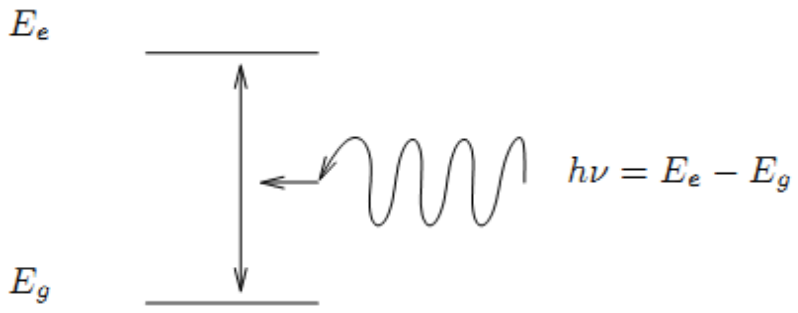


Figure 3.6 : Atome à deux niveaux

b) Polarisation d'un photon

Une onde électromagnétique, la lumière par exemple, peut représenter mathématiquement par un champ vectoriel transverse, i.e orthogonal à la direction de propagation [27].

Dans un référentiel $(0,\hat{e_x},\hat{e_y},\hat{e_z})$, de coordonnés (x,y,z) **,** choisi tel que l'onde se propage selon l'axe des z, le champ électrique est décrit par :

$$\bar{\mathbf{E}}(\mathbf{t},\mathbf{z}) = \bar{\mathbf{E}}_{\mathbf{0}}\mathbf{e}^{\mathbf{i(wt-kz)}} \qquad \textbf{(3.6)}$$

Où $\bar{E}_0 = \bar{E}_{0x}\hat{e_x} + \bar{E}_{0y}\hat{e_y}$.

Le vecteur $\bar{E}_0$, vu comme un nombre complexe, définit la polarisation de l'onde. L'intensité de l'onde est proportionnelle au module au carré de $\bar{E}_0$: $\|\bar{E}_0\|^2$

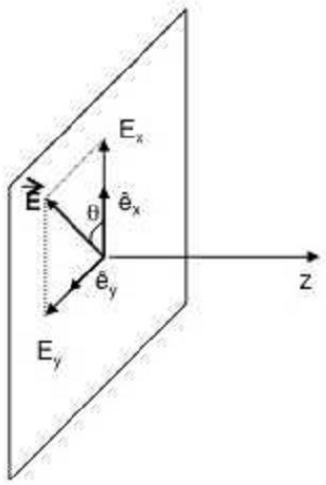


Figure 3.7 : Plan de polarisation d'une onde lumineuse

La polarisation peut être mise en évidence à l'aide de cristaux ayant une propriété optique particulière : la biréfringence. Si nous envoyons sur une biréfringente un faisceau d'intensité I, polarisé linéairement suivant une direction qui fait un angle θ avec l'axe ordinaire du cristal qu'on prend comme Ox : le faisceau est séparé en un faisceau est séparé en un faisceau polarisé suivant Ox d'intensité I $\cos^2\theta$ et un autre faisceau polarisé suivant Oy d'intensité I $\sin^2\theta$. [27] [28]

c) La détection et mesure de la polarisation

On utilise deux filtres polarisants de façon à détecter les polarisations. Le premier, appelé "polariseur", polarise la lumière. Le second, appelé "analyseur", ne laisse passer que les composantes de la lumière polarisée, qui sont le long de sa direction de polarisation. Ainsi, l'intensité obtenue dépend des orientations relatives de ces deux filtres. C'est pourquoi on a besoin des deux filtres pour observer la polarisation. Supposons que le polariseur laisse passer une lumière dont le champ électrique à une amplitude E_0, et que l'angle entre les directions de l'analyseur et du polariseur est égal. Le champ électrique transmis par les deux filtres aura une amplitude

$$E = E_0\cos\theta \qquad (3.7)$$

,

L'intensité étant proportionnelle au carré du champ électrique, elle varie donc comme $\cos^2\theta$.

La loi de Malus affirme que: $I=I_0\cos^2\theta$

A $\theta = 90°$ il n'y a pas de lumière transmise. On trouve plus facilement cette orientation associée à l'intensité maximum transmise. Donc, pour trouver le plan de polarisation, trouvez la position pour laquelle aucune lumière n'est transmise, et prenez le plan de polarisation comme étant à 90° par rapport à cette direction.

i. Polarisation par réflexion

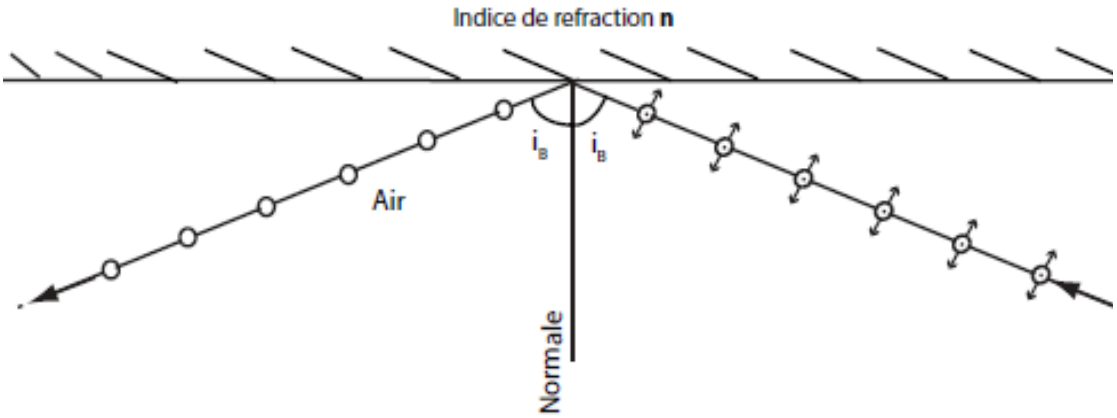


Figure 3.8 : Cas d'une polarisation par réflexion

Si la lumière ordinaire à partir d'un milieu d'indice de réflexion n, la lumière réfléchie est alors partiellement polarisée linéairement. Le vecteur champ électrique (plan de polarisation) est perpendiculaire au plan de réflexion. Le dégrée de polarisation dépend de l'angle d'incidence et à l'angle donné par l'expression suivant :

$$\mathrm{tg}(i_B) = n \qquad (3.8)$$

Où i_B est appelé l'angle Brewster, la polarisation de la lumière réfléchie est totale [27]

ii. Polarisation par polaroid

Certains matériaux plastiques ont une structure moléculaire particulière, alignée dans une direction. Ils ne transmettent ainsi que la lumière polarisée dans cette direction. Ces matériaux sont disponibles sous la forme de fines feuilles. Ils semblent transparents car la lumière ordinaire est composée de toutes les polarisations. Il y a donc toujours une composante transmise.

d) Source de photon :

En communication quantique on utilise des sources de photons à l'entrée des canaux à fibres optiques. Souvent des sources à photon unique ou par pair de photon.

Ce denier est le plus utilise et compatible pour les réseaux télécoms optique standard. Le schéma ci-dessous montre les sources de paires de photons :

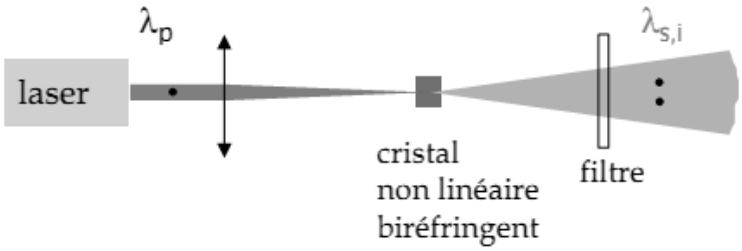


Figure 3.9: Source de photon par paires

La conservation de l'énergie et de l'impulsion est donnée par la formule suivante :

$$w_p = w_s + w_i \; k_p = k_s + k_i \tag{3.9}$$

Où w_p est l'énergie du photon, w_s énergie de la source, w_i l'énergie de l'impulsion. L'accord de phase détermine les longueurs d'ondes et directions de propagations. Le schéma ci-dessous montre la réalisation physique pour un équipement de transmission optique.

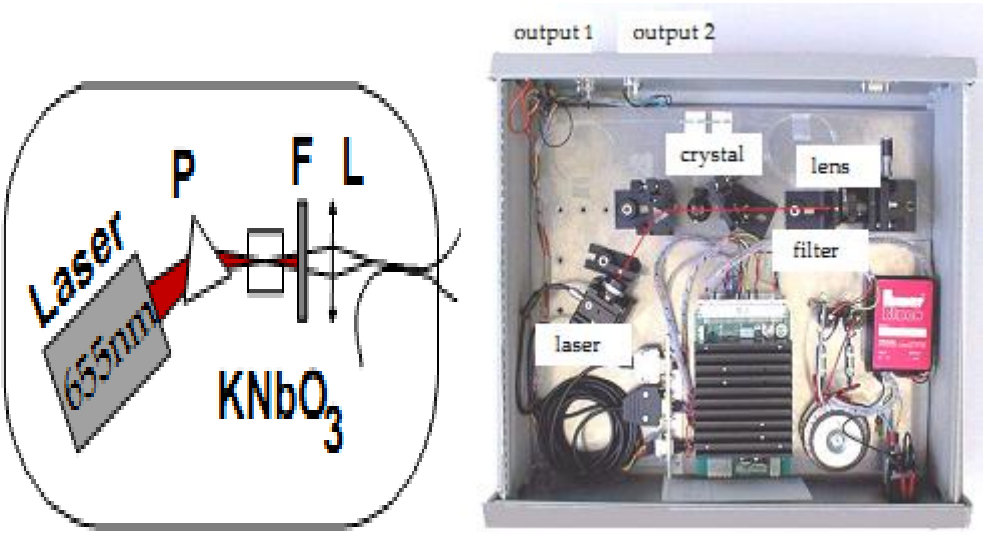


Figure 3.10: Système électronique d'une source de photon

Les caractéristiques de la source ci-dessous sont :

- Intrication énergie-temps $\lambda_p = 655$ nm; $\bar{\lambda}_{S,i} = 1310$ nm
- Intégré sur diode laser, simple, petit, pratique (40 x 45 x 15 cm3)
- I_{pump} = 8 mW avec guide dans LiNbO3 avec quasi accord phase, $I_{pump} \approx 8$ µ W

De manière schématique, après une excitation appropriée, un système atomique luminescent unique se désexcite en émettant un quantum d'énergie $\Delta E = E_e - E_g$ correspondant à un photon unique de fréquence Δ_E/h. La méthode ici consiste à isoler spatialement un émetteur unique : atome, molécule, atome artificiel en utilisant par exemple des techniques de microscopie

confocale. Idéalement l'émetteur possède une structure à 3 niveaux d'énergie (figure 3.11).

Un laser de pompe porte le système dans le niveau supérieur qui se désexcite très rapidement vers le niveau intermédiaire |e> de manière nonradiative.
Dans un second temps le système relaxe vers le niveau fondamental |g> en émettant un photon.
Cette configuration à trois niveaux permet décaler spectralement l'excitation par rapport au signal de luminescence et donc de filtrer aisément les photons uniques. Pour obtenir une source de photons uniques déclenchée, il faut utiliser des impulsions de pompe de durée δt plus courte que la durée de vie τ_v ($\delta t \ll \tau_v$) du niveau intermédiaire et de période T_R telle que $T_R > \tau_v$.
La puissance utilisée doit être suffisante pour saturer l'absorption du système. Enfin des techniques particulières de collection de la luminescence doivent être mises enœuvre pour collecter efficacement le signal de luminescence isotrope : objectif de microscope de grande ouverture numérique, couplage de l'émetteur à un microrésonateur. Le débitd'une telle source est inférieur à $1/\tau_v$ et en réalité souvent limité par l'efficacité de collection.

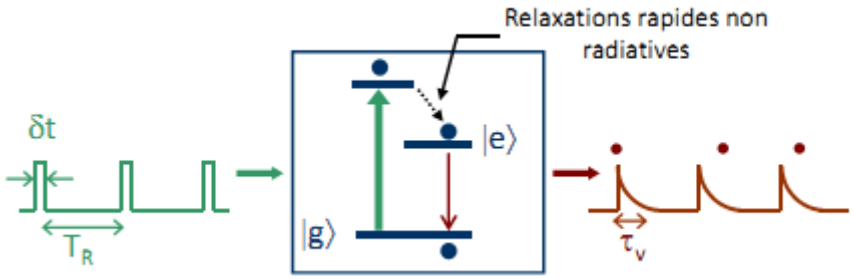


Figure3.11: Système atomique isolé utilisé comme émetteur individuel pour l'émission de photons unique.

L'utilisation d'un champ pompe impulsionnel permet d'obtenir une source déclenchée de photons uni ques. Un champ de pompe continu conduit à une émission asynchrone de photons uniques.

3.7 Mécanique quantique

La physique des particules est gouvernée par les lois de la mécanique quantique, qui ont étés découvertes au début du 20 ème siècle. L'ensemble des objets de la mécanique quantique se trouve dans un espace : l'espace d'Hilbert complexe [23] [28].

i. Espace d'Hilbert complexe

En mécanique quantique, le système physique est décrit par un espace d'Hilbert complexe noté ´H. Cette description se fait au moyen de la notation d'onde de Dirac. Les éléments de cet espace sont appelés des fonctions d'onde.

ii. Notation de Dirac

La notation de Dirac permet de montrer l'aspect vectoriel de l'objet représentant l'état quantique dans l'espace des états. Elle utilise un symbole mis entre une barre verticale et un signe « plus grand que ». Certain symbole sont utilisées comme des bases orthonormales. Ces bases orthonormales peuvent être combinées pour former un Ket :

$$|Y> = \sum C_i * |x> \qquad (3.10)$$

Où C_i appartient à l'ensemble des complexes [28]
Le C_i est une valeur de |x> et |x> est un vecteur propre. La somme de toutes les valeurs absolues au carré des valeurs propres vaut 1. Cette somme est utilisée quand on travaille avec un nombre de dimension finie ou avec un nombre fini de vecteurs propres.
Elle est remplacée par une intégrale quand on se trouve avec un nombre de dimension infini. Cette combinaison linéaire est appelée une superposition d'état lorsqu'il existe un ensemble composé d'au moins deux valeurs propres non égales à zéro. Dans le cas contraire, on a affaire à un état propre (état pur).

iii. Le Quantum bit ou qubit

En informatique classique, on encode l'information grâce à des bits pouvant être soit des 1, soit des 0. En informatique quantique, on va utiliser les qubits. Un quantum bit (qubit) est l'unité de stockage de l'information quantique. Il représente soit un 1, soit un 0, soit une combinaison de 1 et de 0 en même temps. Ces qubits sont représentés par des particules gouvernées par les lois de la mécanique quantique.

iv. Représentation du qubit par une particule élémentaire

Une particule élémentaire permet de décrire une information quantique. Supposons qu'on détient un photon. Ce photon peut être polarisé horizontalement, verticalement, diagonalement, ou anti-diagonale. Chaque état polarisé représente une valeur binaire. Par convention, on appliquera la valeur 0 à la polarisation horizontale et diagonale alors que la valeur 1 sera appliquée à la polarisation verticale et anti-diagonale. L'état de ces particules peut être décrit par la notation de Dirac.

v. Notation de Dirac appliquée à un qubit

Un qubit peut donc être décrit par la notation de Dirac dans un espace d'Hilbert complexe bidimensionnel. Pour le décrire, nous utilisons deux nombres complexes appartenant à l'ensemble :

$$\alpha\,|0> + \beta\,|1> : |\alpha|^2+|\beta|^2 = 1,\ \alpha \wedge \beta \in \mathbb{C} \qquad (3.11)$$

Avec |0 > et |1 > référençant deux qubits, correspondant à deux états orthogonaux dans le système quantique. Les qubits |0 > (α=1, β=0) et |1 > (α=0, β=1) sont les équivalents quantiques des bits 0 et 1 respectivement. En d'autres termes, lors de la mesure d'un qubit, $|\alpha|^2$ représente la probabilité d'avoir le bit 0 et $|\beta|^2$ représente la probabilité d'avoir le bit 1. De ce fait, il paraît logique que $|\alpha|^2+|\beta|^2 = 1$ puisqu'il est certain d'avoir l'un ou l'autre [28].

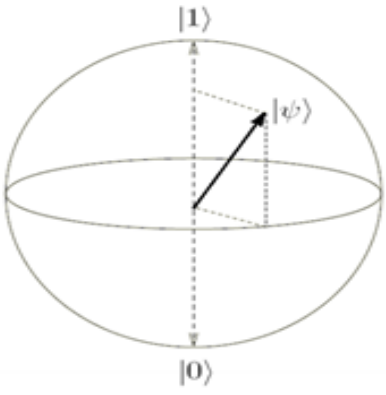


Figure 3.12 : Représentation des différentes qubit dans une sphère

Lorsqu'un qubit n'est pas en superposition d'état, sa mesure donne un résultat déterministe. Ce qubit est représenté par la notation de Dirac :

- $|0>$ pour le bit 0
- $|1>$ pour le bit 1

Lorsqu'un qubit est en superposition d'état, sa mesure donne un résultat aléatoire. Ce qubit est représentable par les notations de Dirac :

- $|+> = 2^{-1/2} |0> + 2^{-1/2} |1>$
- $|-> = 2^{-1/2} |0> - 2^{-1/2} |1>$

vi. La mesure en mécanique quantique

Dans la mécanique classique, il est facile de calculer la position et la vitesse de tout objet à tout instant. Ce calcul n'influence pas l'objet mesuré.
En mécanique quantique, ce calcul influence les particules mesurées. Il y a donc une perturbation du système lors de sa mesure. Pour lire les qubits, il faut pouvoir les mesurer. Cette mesure se fait grâce à un polarisateur et un photodétecteur. Le polarisateur ne laisse passer que des photons polarisés verticalement (ou horizontalement) dans le cas où on travaille dans base H-V (Horizontale-verticale), ou diagonalement (ou anti-diagonalement) dans le cas où on travaille dans une base D-A (Diagonale-Anti-diagonale). En utilisant un photon polarisé avec une base H-V, un polarisateur qui ne laisse passer que des photons polarisés dans une base D-A, laissera passer une fois sur deux le photon. Inversement, en utilisant un photon polarisé avec une base D-A, un polarisateur qui ne laisse passer que des photon avec une base D-A, un polarisateur qui ne laisse passer que des photons polarisés dans une base D-A, un polarisateur qui ne laisse passer que des photons polarisés dans une base H-V, laissera passer une fois sur deux le photons. Lors de ce passage, le photon deviendra soit polarisé horizontalement soit verticalement. Le système est donc perturbé suite à la mesure.
C'est pour cette raison qu'on dit qu'un qubit polarisé D-A est une superposition d'état du qubit polarisé verticalement et du qubit polarisé horizontalement. Le photo-détecteur permet de détecter un photon qui le percute.

b. Envois d'information à travers un canal quantique

E	Elément à coder	0	0	1	0	1	1	0	1
	Paire utilisée	{|0>,|1>}	{|0>,|1>}	{|+>,|->}	{|+>,|->}	{|0>,|1>}	{|+>,|->}	{|+>,|->}	{|+>,|->}
R	Paire utilisée	{|0>,|1>}	{|+>,|->}	{|0>,|1>}	{|+>,|->}	{|0>,|1>}	{|+>,|->}	{|0>,|1>}	{|+>,|->}
	Résultat	0	0	0	0	1	1	1	1

Tableau 3.2 : Elément d'information transmis

Dans cet exemple, l'émetteur envoie un octet au récepteur. L'émetteur utilise une paire H-V

({|0 >, |1 >}) pour polariser les photons horizontalement ou verticalement, soit une paire D-A ({|+ >, |- >})
Pour les photons diagonalement ou anti-diagonalement.
Le récepteur utilise également une paire H-V ou D-A pour lire l'information. Dans le cas où ils utiliseront la même paire, l'information reçue est l'information envoyée. Dans le cas contraire, l'information reçue a une chance sur deux d'être l'information envoyée [28].

3.8 Le protocole BB84

Le protocole BB84 ou Charles Bennett et Gilles Brassard 1984 est l'un des protocoles utilisant les propriétés de la mécanique quantique à travers le code de Vernam le plus utilisés.

a) Description du protocole

Le protocole BB84 est divisé en 05 parties :

- Envoi de la clé à travers le canal quantique
- Réduction de la différence entre la clé de l'émetteur et du récepteur : causée uniquement par des choix de filtres différents. Lorsque ceci est réalisé, on réduit les différences entre les deux clés causées par la présence de l'intrus ou par d'autre sorte de perturbation. Cette différence permet d'estimer le taux maximum des connaissances de l'intrus sur la clé potentielle.
  - Si ce taux est supérieur à un certain seuil la clé est rejetée ; car l'espion détient trop d'informations [29]
  - Si non on réduira les connaissances de l'intrus à zéro en appliquant un algorithme sur la clé, ainsi qu'en s'échangeant une nouvelle clé cryptée au moyen de la clé détenue par l'émetteur et le récepteur. Comme l'intrus n'a pas l'entièreté de la clé, elle ne pourra pas déchiffrer le message comportant la clé cryptée.
- Au final, on crypte le message grâce à la clé finale pour l'envoyer sur un canal public [29].

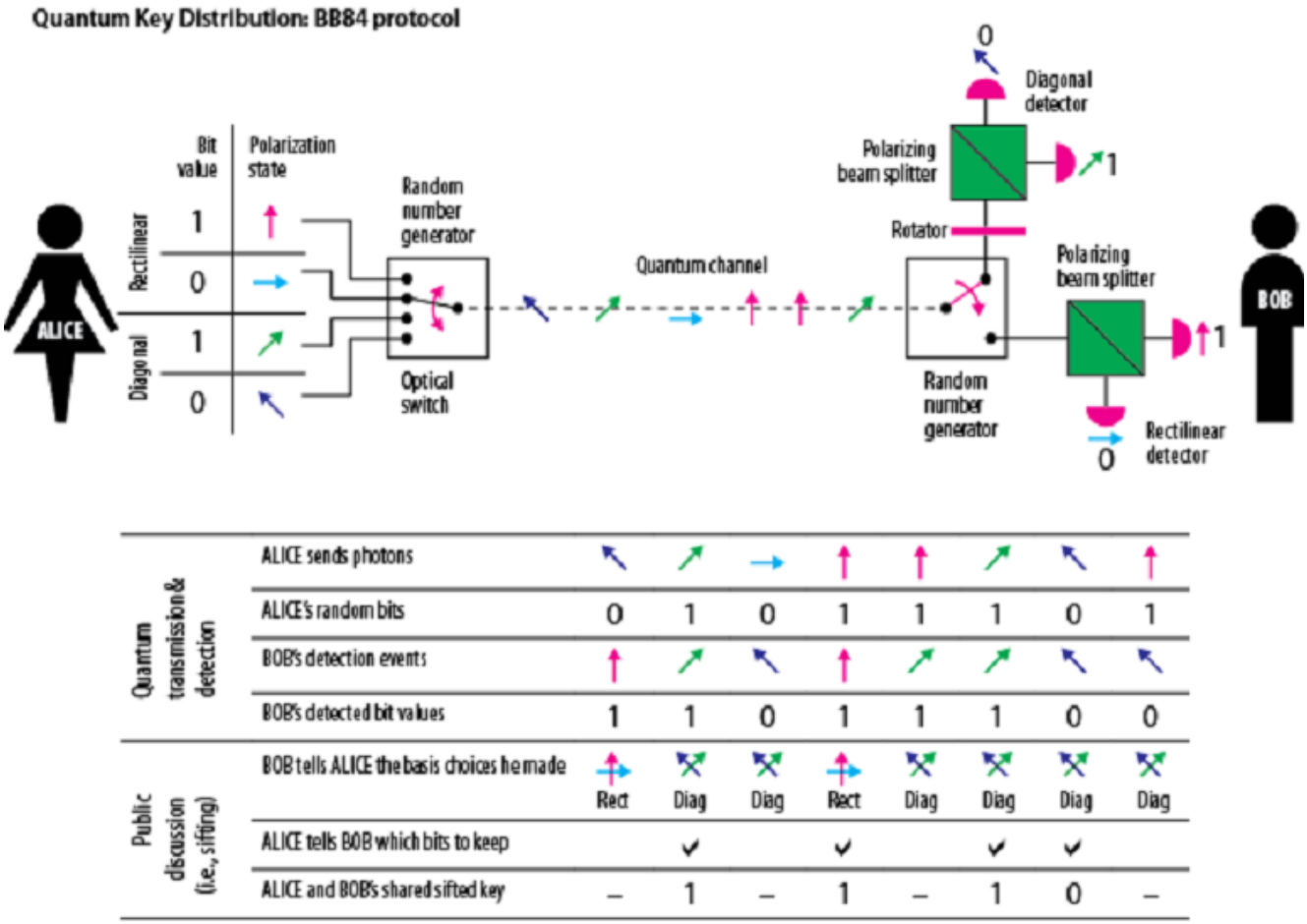


Figure 3.13 : Comparaison des différentes bases entre l'émetteur et le récepteur

L'espionnage peut être détecté grâce à l'analyse des taux d'erreur reçu à la réception. A l'issue de la phase quantique, l'émetteur et le récepteur disposent d'informations corrélées mais

• Entachées d'erreurs (expérimentales et / ou dues à l'espion)

• Partiellement connues de l'espion [29].

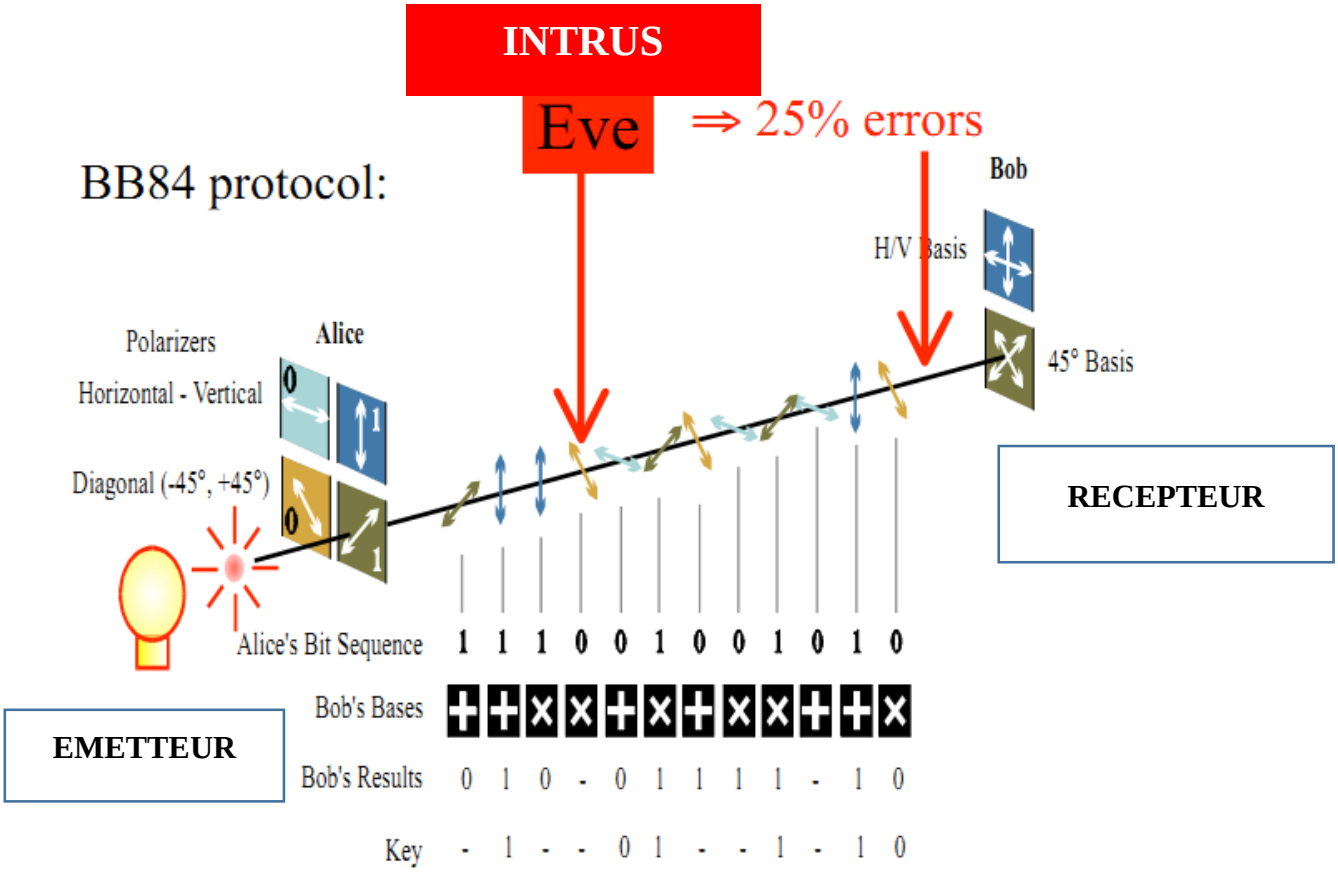


Figure 3.14 : Mise en Œuvre du protocole de communication BB84

b) 2 étapes de post-processing

La correction d'erreur codes correcteurs d'erreurs classiques

- Réconciliation : se fait sur canal classique (public)
- But : travailler près de la borne de Shannon
- Augmente l'information d'un espion potentiel

Amplification de confidentialité d'où => clé totalement secrète

i. Amplifier la confidentialité de la clé : principe

Soit la figure ci-dessous :

Figure 3.15 : Communication entre émetteur et récepteur

Comme situation initiale on a d'abord : I (X_A=X_B ; U_E) > 0

X_A =0100110001010 X_B =0100110001010

$X'_A = X'_B$ I(X'_A=X'_B ; U_E) > 0

Ainsi au bilan : la génération d'une clé secrète est donnée selon un processus en 3 étapes. Données initiales contiennent des erreurs : la présence de l'intrus détecté. Donc il faut corriger les erreurs. Il faut annihiler l'information de l'intrus.

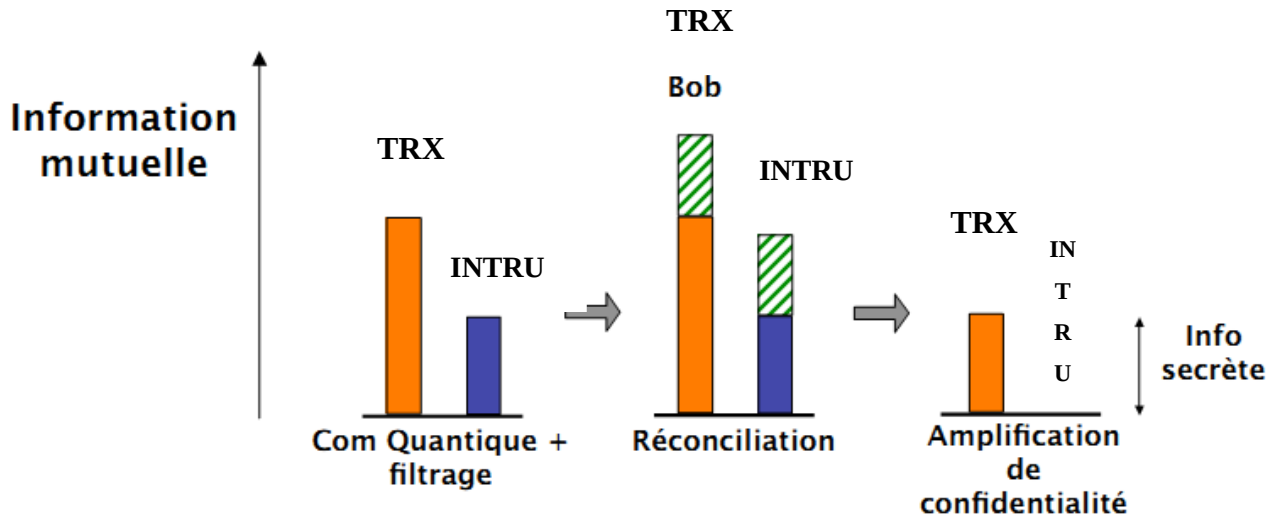


Figure 3.16 : Rapport entre les taux d'information mutuel

ii. Amplification de niveau de sécurité

Pour permettre la réduction de l'information que l'intrus a de la clé, on peut appliquer une fonction sur l'ensemble des bits que l'émetteur et le récepteur ont. Ainsi, comme l'intrus n'a pas l'entière des bits, il ne connaitra pas le résultat de la fonction. Il suffit que l'émetteur communique au récepteur le numéro d'un bit qu'il désire combiner. Si l'intrus n'a qu'une partie de la paire, elle ne connaitra pas le résultat de cette opération et perdra une information sur la clé. Cette opération réduit la connaissance de l'intrus ainsi que la taille de la clé. La taille de la clé dans le cas d'une technique de réconciliation parfait vaut :

$$\max\big(\mathrm{I}(\mathrm{X};\mathrm{Y})\big) - \mathrm{I}(\mathrm{X},\mathrm{Z}), \mathrm{I}(\mathrm{X};\mathrm{Y}) - \mathrm{I}(\mathrm{Y};\mathrm{Z})) \qquad (3.11)$$

Où X= L'émetteur, Y= Le récepteur et Z= L'intrus

iii. Bruit sur un canal

Un canal peut causer du bruit sur tout élément qui le traverse. Certain phénomène peuvent perturber la polarisation d'un photon à travers la transmission par fibre optique, d'autre part l'air contient des photons qu'il faut distinguer des photons émis par la source. Une solution à ce problème est l'augmentation de la puissance d'émission. L'autre est l'ajout d'information supplémentaire pour que ces bruits n'altèrent pas trop l'information vitale. Ces solutions ne sont pas toujours applicables, c'est pourquoi on utilise un code correcteur permettant de résoudre certaines erreurs dues au bruit. Dans le cas où le contenu est détérioré, le message est retransmis. Néanmoins, la retransmission n'est pas toujours réalisable, et elle ne l'est évidemment pas dans notre cas [29].

3.9 Les grands défis de l'implémentation de la cryptographie quantique

Ces défis constituent l'un des préoccupations majeur des chercheurs et laboratoires de notre époque. Parmi ces défis :
- La possibilité de créer des photons uniques avec laquelle la probabilité d'avoir deux est extrêmement très faible.
-Au niveau de la distance entre émetteur et récepteur pour une liaison quantique reste très faible par rapport au réseau déployé actuellement.
-L'efficacité des détecteurs quantique au niveau du récepteur car actuellement on arrive à une efficacité de 20% à 80% de cohérence.
- Les contraintes de la dispersion, dépolarisation causant la décohérence à la réception.
- La difficulté d'implémenté les canaux quantiques à la technologie optique haut débit (Multiplexage longueur d'onde, fréquentielle, temporelle…) car cela reste impossible avec les photons.

3.10 Les acteurs de la cryptographie quantique

Ce sont les institutions requérant de forts niveaux de sécurité pour leur communication : les gouvernements pour les communications nationales et internationales, l'armé, les services secrets et surtout les plus gros utilisateurs restent les banques pour la sécurisation des transactions lourdes ainsi que pour le transfert d'information intersites et extrasites).

3.11 Conclusion

La cryptographie quantique exploite la loi de la mécanique quantique pour la sécurisation de l'information. C'est une distribution quantique des clés de cryptage entre un émetteur et un récepteur communiquant sur la fibre optique. Dans le prochain chapitre, nous allons implémenter et simuler les bases de la cryptographie quantique, la simulation du protocole BB84. Au final, nous analysons les résultats et interprétations.

CHAPITRE 4
SIMULATION DU CONCEPT CRYPTOGRAPHIE QUANTIQUE

4.1 L'objectifs des cryptosystèmes

Les cryptosystèmes assurent et garantissent : la confidentialité, l'authenticité, l'intégrité et la non-répudiation.

• La confidentialité signifie qu'une personne non autorisée n'ait accès aux informations.

• L'authenticité fait référence pour la validation de la source du message pour assurer que l'expéditeur est correctement identifié.

• L'intégrité fournit l'assurance que le message n'a pas été modifié pendant la transmission, accidentellement ou intentionnellement.

• La non-répudiation veut dire qu'un expéditeur ne peut pas nier d'avoir envoyé le message et le récepteur ne peut pas nier sa réception.

Si une personne envoie un message, puis plus tard, il prétend qu'il n'a pas envoyé le message, il s'agit d'un acte de répudiation. Quand un mécanisme de cryptage prévoit la non-répudiation, cela signifie que l'expéditeur ne peut pas nier d'avoir envoyé le message et le récepteur ne peut pas nier sa réception. Ainsi donc, le cadre de notre mémoire d'étude se focalise sur les concepts ci-dessus. Notre travail dans ce chapitre consiste à effectuer des simulations sur les points suivant:

-Simulation montrant une liaison (classique) par fibre optique.
-Implémentation d'une liaison QKD sur Optisystem-optiwave.
-La simulation d'une liaison optique à base de protocole BB84.
-Rapport entre : quantité d'information, taux d'intrusion d'information et QBER
-Interprétations des résultats obtenus selon les courbes de données de transmission.

4.2 Simulation d'une liaison par fibre optique pour un canal classique sur Optisystem

Pour une liaison de base en communication par fibre optique les éléments sont : du côté émetteur (générateur pseudo aléatoire de bit, modulateur MZ, un driver de modulateur, source laser), du côté canal (fibre optique, amplificateur, multiplexeur) et au niveau de la réception (Photodiode PIN, Filtre, Analyser). Ci-dessous un schéma synoptique de base :

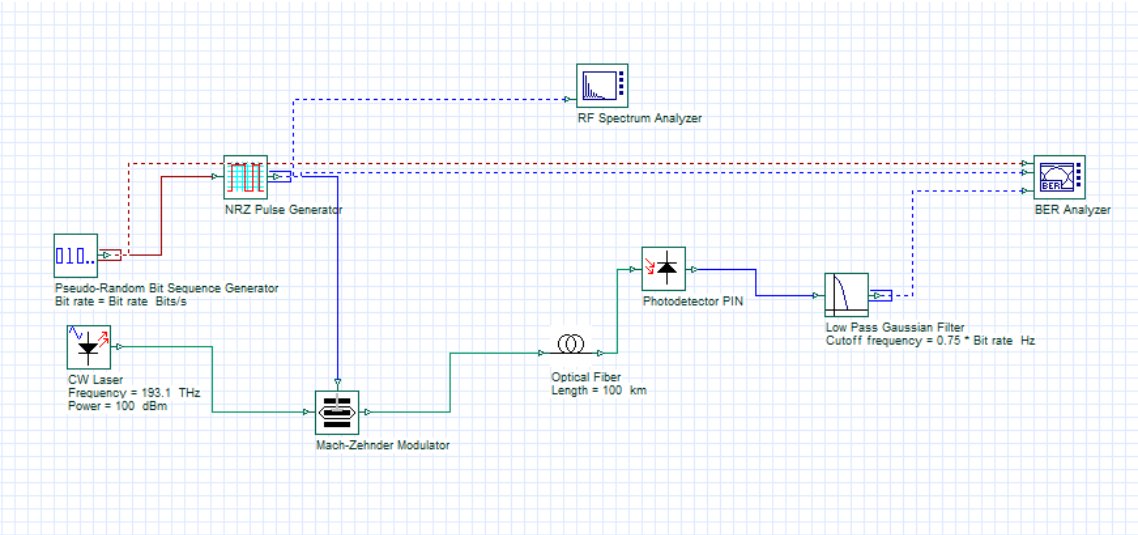


Figure 4.1: Communication classique via fibre optique

Les résultats de notre simulation donnent les caractéristiques de la liaison (BER, les facteurs de qualité,…) précédente :

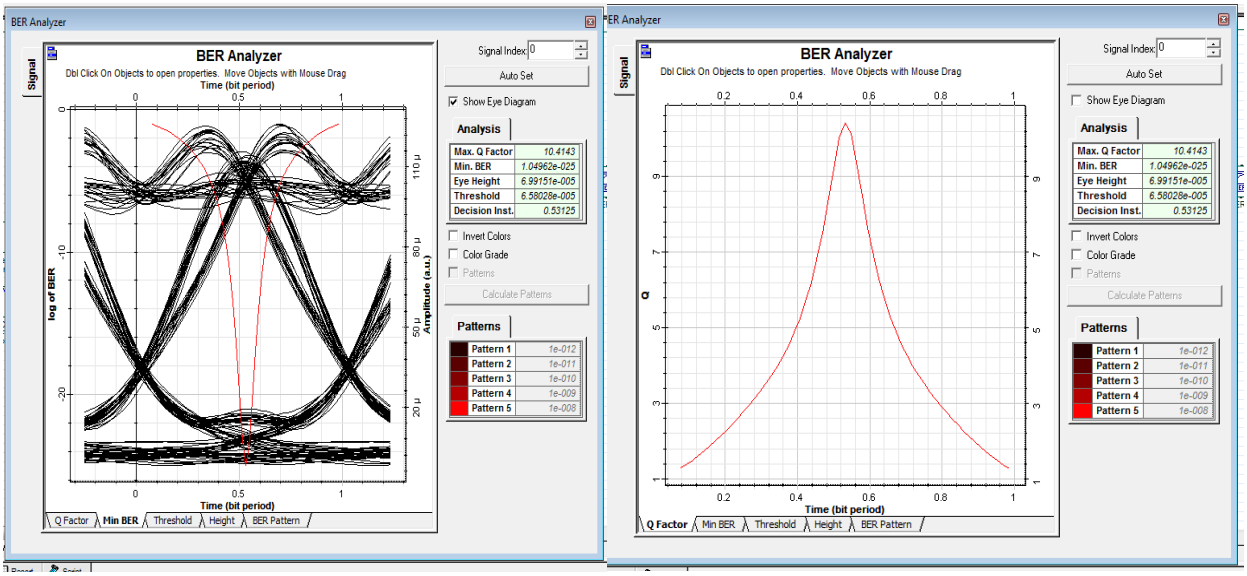


Figure 4.2 : Visualisation du résultat de la simulation

Ces résultats conclus une qualité de transmission satisfaisante à travers l'analyse du diagramme de l'œil et du graphe de facteur de qualité. On constate l'ouverture nette de l'œil et suivant la courbe de facteur de qualité on remarque un pic atteignant Q=9 à Q=10. Cependant, cela concerne le canal classique, l'objet de notre mémoire c'est l'étude du canal quantique, nous allons le voir plus loin.

4.3 Simulation du protocole BB84 et du taux d'erreur sur Quantum Key Distribution Protocol suivant une approche optoélectronique

Nous proposons une modélisation et une simulation pour les protocoles de distribution de clé quantique en utilisant des simulateurs photoniques comme OptiSystem-optiwave. Ce cadre de simulation met l'accent sur les composantes expérimentales de la clé de distribution quantique.

Nous simulons l'opération BB84 et distribution de la clé quantique : le caractère aléatoire et l'équivalence approximative. En outre, le cadre de notre configuration fournit un outil d'étude pour analyser l'impact des composants de photons expérimentaux lors du processus de distribution des clés quantiques.

La cryptographie numérique est une solution basée sur la sécurité informatique. Avec la rapidité de la croissance technologique d'aujourd'hui, de plus en plus d'ordinateur sont capable de briser la sécurité, la technique la plus simple est appelée « attaque par force brute ». En outre, le produit imminent du quantum avec le principe de la mécanique (MQ) est l'ordinateur quantique et ses algorithmes qui sont capables de résoudre le problème non polynomial (NP) en temps polynomial.

D'autre part, le quantum cryptographie de la MQ offre une sécurité inconditionnelle grâce au principe d'incertitude, au théorème de non-clonage et l'enchevêtrement. Le protocole de distribution des clés quantiques (QKD) est déjà disponible sur le marché. Le QKD est une combinaison de matériel (c'est-à-dire photonique et télécommunications optiques) et logiciels (protocoles et messages méthodes quantiques) pour accomplir la clé inconditionnelle de distribution. La propriété intrinsèque de QKD est la détection de l'écoute électronique ; cela en fait une application lourde.
Dans la présente section, nous analysons des travaux et nous nous concentrons sur la simulation du QKD [30] [31].

4.4 Quelques brefs aperçus de l'opération QKD dans le tableau suivant :

QKD CHANNEL OPERATIONS		
NIVEAU	OPERATIONS	CANNAL
1	Qubits exchange	Quantum
2	QBER/Sift	Public
3	Error Correction	Public
4	Privacy amplification	Public

Tableau 4.1 : Opération sur le canal QKD

À partir du tableau ci-dessus sauf échange des qubits, toutes les autres opérations sont effectuées dans le canal public. Il s'agit d'un système biparti appelé conventionnellement l'émetteur et le récepteur qui sont les utilisateurs légitimes. D'autre part, l'intrus est considéré comme un utilisateur illégitime. Il faut préciser que notre proposition de simulation se concentre sur la première étape.
D'autres étapes qui ne sont autres que le tamisage, la correction d'erreurs et l'amplification du niveau de sécurité sont également appelés « action post-quantique ou processus de distillation de clé ». Cela est nécessaire pour établir une clé sécurisée où l'intrus a un pouvoir totalement négligeable sur la clé secrète.

4.5 Modélisation proposée et configuration de la simulation

Pour la simulation appelée « visualiseurs » sous cette bibliothèque, nous pouvons utiliser des analyseurs de polarisation et des compteurs pour le comptage des photons et les détecteurs.

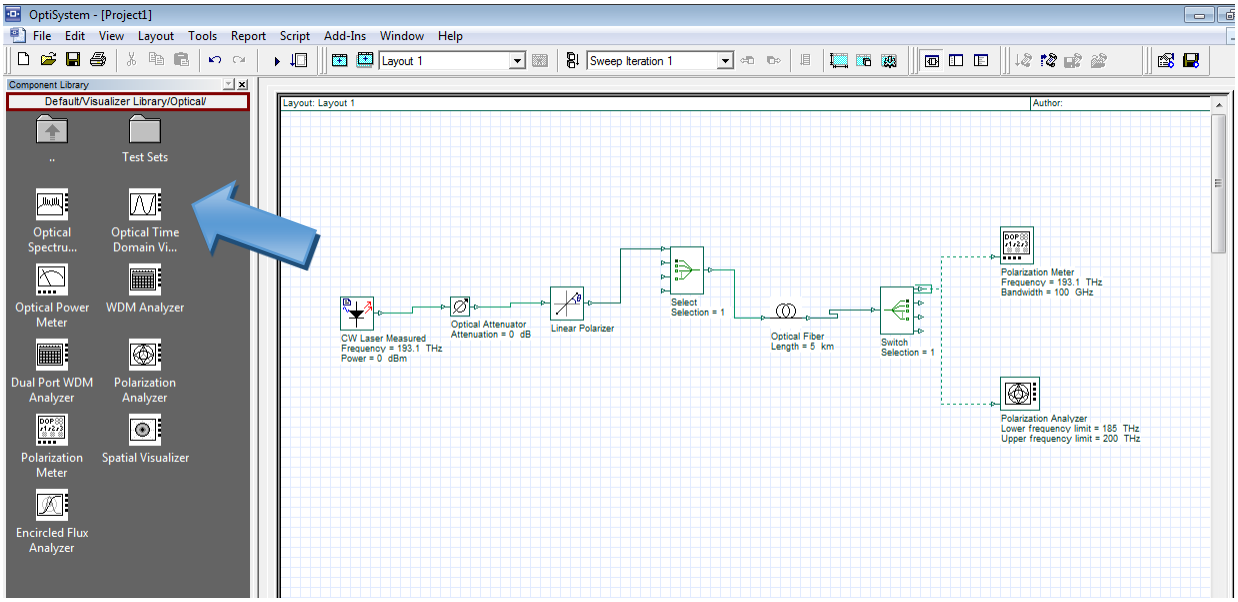


Figure 4.3 : Visualisation des composants du simulateur Optisystem

Dans le scénario expérimental des télécommunications, trois classifications principales, nommément émetteur, canal et récepteur seront utilisés. Nous pouvons relier ce paradigme aux protocoles QKD. Dans le bloc émetteur, la source de photons est un composant important et l'Optisystem offre la grande variété de sources optiques avec de nombreuses propriétés. L'atténuation est un mécanisme de QKD pour obtenir un niveau de photon unique d'impulsion. Le polariseur est un autre élément composant passif pour polariser le photon dans l'angle désiré. Pour la classification des canaux, la fibre optique est la composante standard et le support complet par le logiciel de simulation.

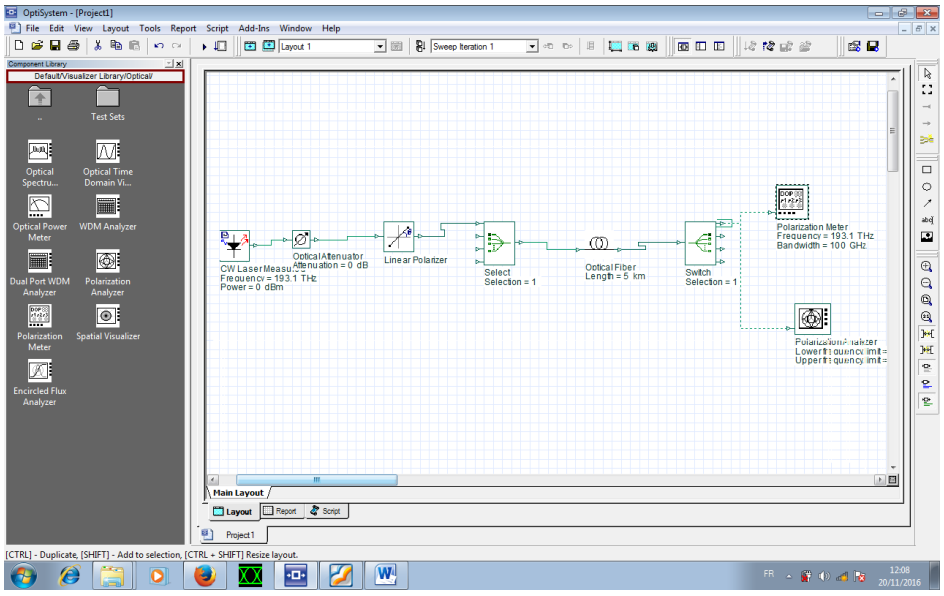


Figure 4.4 : Schéma synoptique d'une liaison de base à cryptographie quantique

Le composant appelé «select» peut être utilisé comme un PBS est pour la sélection aléatoire des photons entrants. Habituellement, dans l'expérience de QKD, l'émetteur choisit au hasard la polarisation des photons envoyé au récepteur. Le récepteur nécessite des pics de polarisation aléatoire pour

la mesure du photon entrant. Ce mécanisme est mis à part par le composant de sélection même. Finalement basé sur la polarisation, les détecteurs se déclencheront. L'émetteur et le récepteur enregistrent tous les photons discutant dans la chaîne publique. La figure 4.4 suivante explique le fonctionnement de base du scénario QKD.

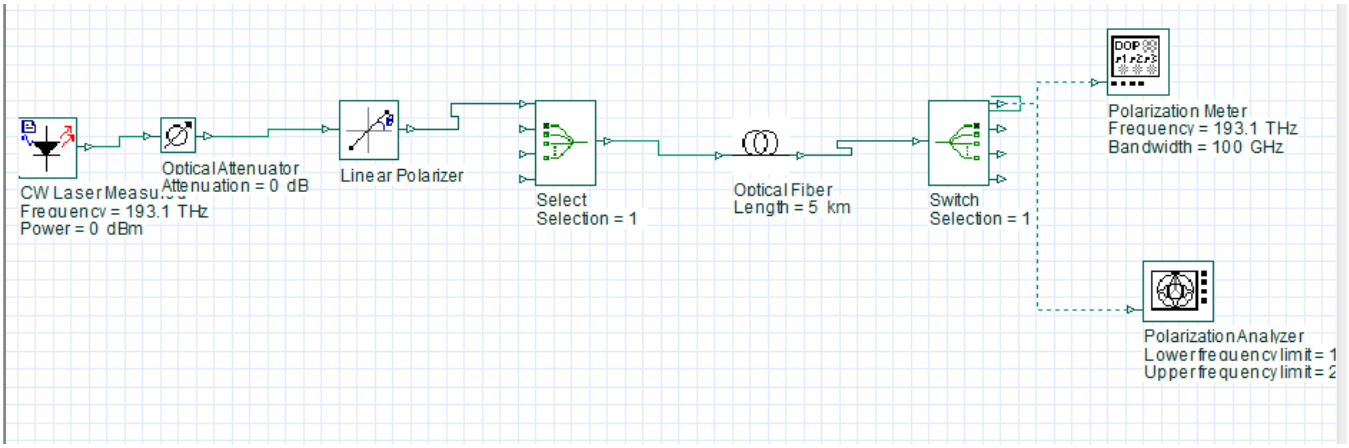


Figure 4.5 : Synoptique d'un système QKD

Dans cette figure ci-dessus, au lieu d'un APD (Avalanche Photo Diode) comme détecteur, nous utilisons les autres composants appelés « analyseur de polarisation », qui montre la valeur de polarisation (azimut et elliptique). Aussi, la polarisation-mètre est un composant facultatif pour mesurer la puissance. À ce point, le détecteur n'est pas implémenté dans notre simulation. Une autre préoccupation vitale concerne le caractère aléatoire. Dans notre modèle de simulation, seul le composant 'select' est aléatoire. La plupart des composants du système Optisystem à propriété construite est appelée « calcul de balayage ». Ce dernier permet la simulation pour effectuer de nombreuses itérations avec un ensemble différent de valeur. Pour l'aléatoire, nous utilisons la fonction discrète « random indice » de valeur minimale et maximale. En choisissant soigneusement les bonnes valeurs pour ces paramètres, un bon caractère aléatoire peut être atteint.

4.6 Simulation de protocole BB84

Dans la figure suivante, nous illustrons l'opération complète du protocole BB84. Ce modèle expérimental est légèrement modifié à partir de la configuration pratique QKD d'origine.

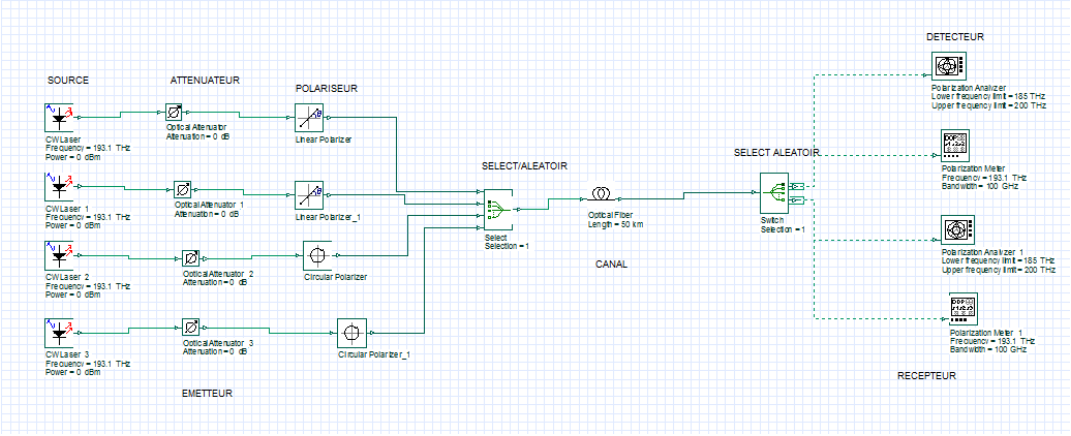
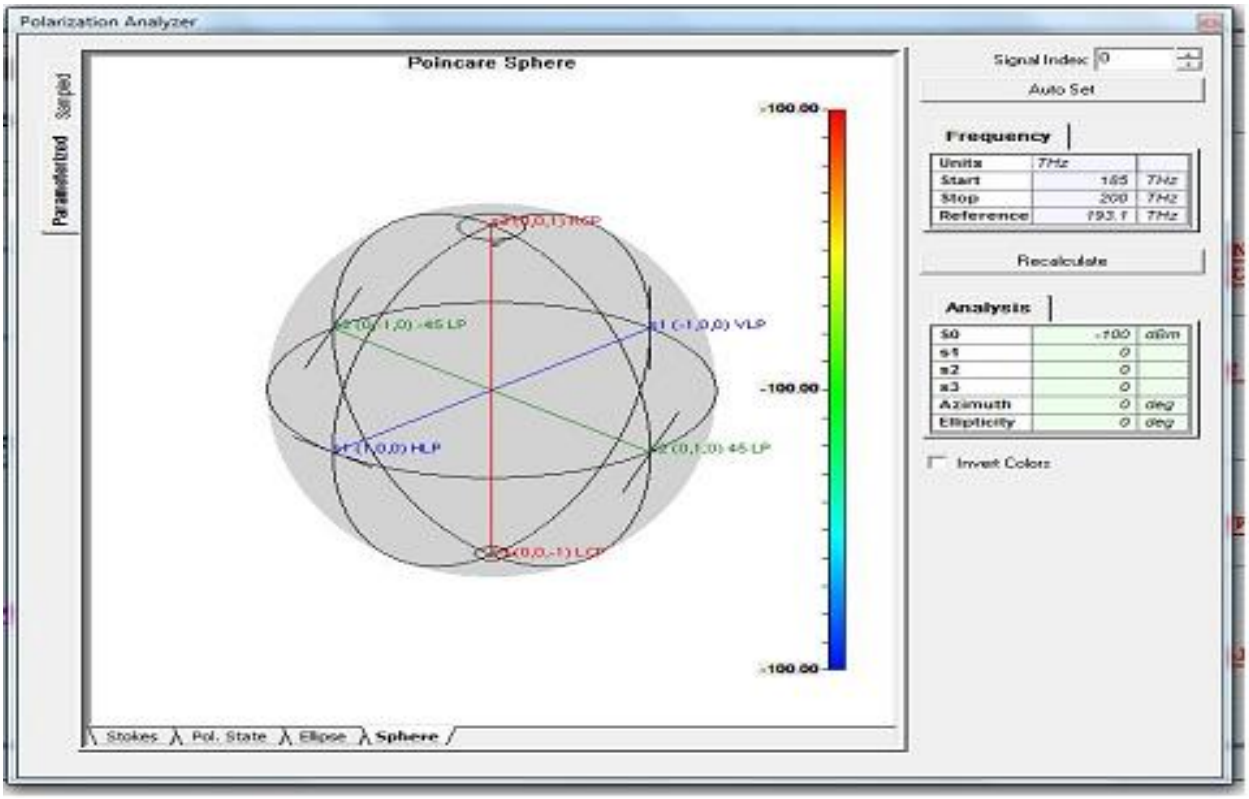


Figure 4.6 : Implémentation du protocole BB84 sur Optisystem

Dans la figure, nous mettons en œuvre quatre ondes optiques cohérentes de sources laser avec atténuateur optique variable. La valeur d'atténuation est de 0,1 dB pour avoir le photon unique. Nous avons également mis en place quatre types de polariseurs: horizontal, vertical, gauche diagonale et diagonale droite.
Nous lançons au moins 10000 itérations; pour chaque itération, le composant « select » choisit un qubit aléatoirement sur les quatre angles de polarisation et traversent la fibre optique vers le côté du récepteur. Au niveau du récepteur, nous implémentons le composant « select » pour simuler l'aléatoire de la sélection de la polarisation linéaire ou de la polarisation diagonale et la détection sera effectuée par l'analyseur de polarisation.
Il s'agit de la configuration simple pour le fonctionnement de base du protocole BB84. L'Optisystem est livré avec une grande option pour exporter les données vers les fichiers Excel et Matlab. Notre simulation consiste également en un petit script visuel de base pour extraire du récepteur des valeurs de l'analyseur de polarisation.

Enfin, un calcul est nécessaire pour obtenir un taux d'erreur binaire quantique QBER. Les sorties du visualiseur sont représentées à la figure ci-dessous :



.

Figure 4.7: Polarisation au niveau du détecteur, suivant la sphère

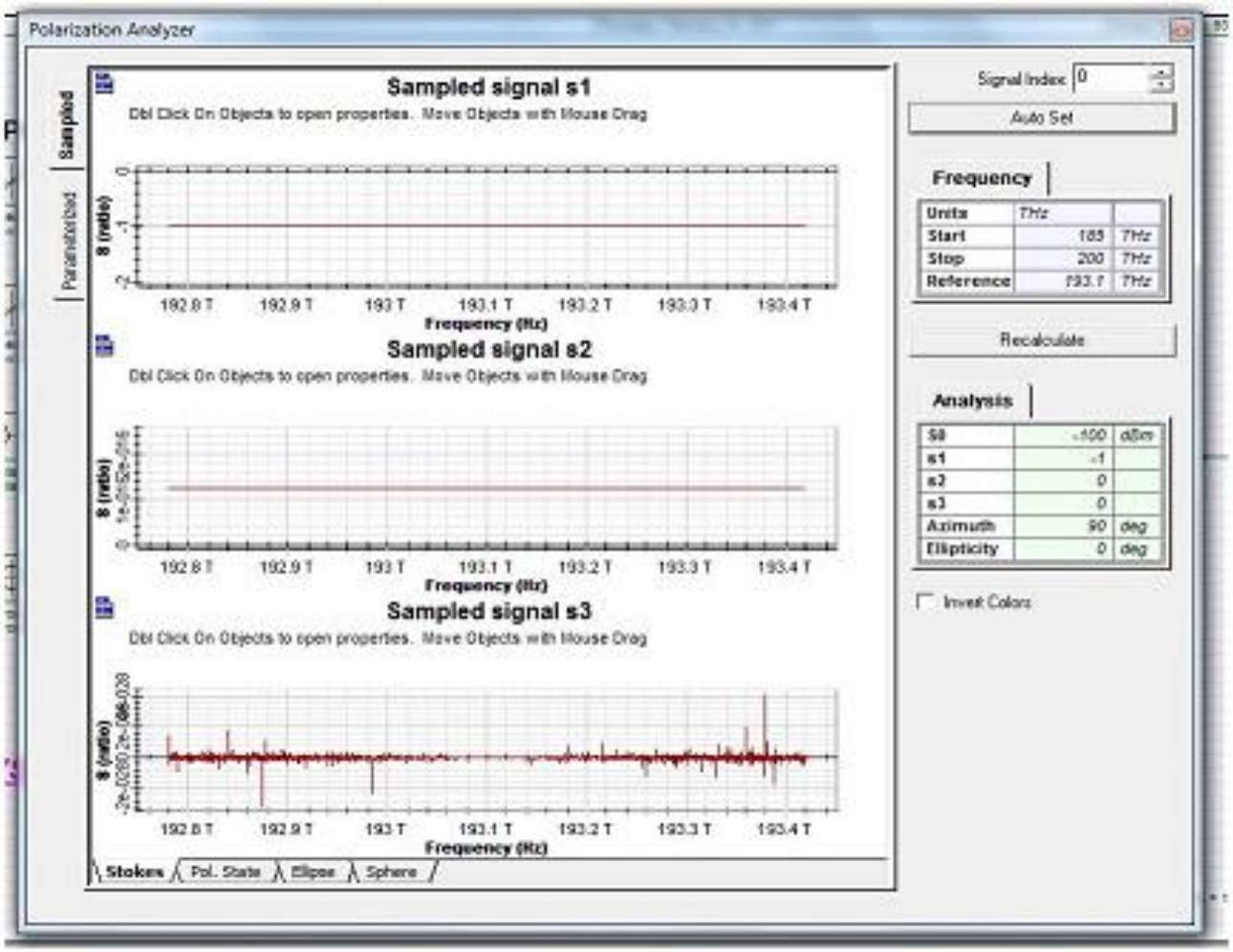


Figure 4.8 : Propriété du signal reçu au niveau du détecteur et analyse fréquentiel

4.7 Simulation du protocole BB84 et de l'opération d'attaques de l'intrus

L'intrus ne pourrait jamais fonctionner contre le canal quantique. En supposant que l'intrus n'a absolument aucune limite technologique, c'est-à-dire qu'elle peut faire tout ce que la physique quantique ne fait pas explicitement.
Cependant, les attaques de l'intrus ne se limitent pas à un canal de communication quantique. Par exemple, l'intrus pourrait avoir le même appareil comme l'émetteur ou du récepteur, ou elle pourrait exploiter les faiblesses dans la mise en œuvre réelle du QKD.

Principalement, les attaques de l'intrus sont classées comme « attaque individuelles cohérentes » et les « attaques incohérentes ». Pour notre expérience, nous généralisons l'attaque de l'intrus qui est basée sur la stratégie d'attaque Intercept-Resend et d'attaque man-in-middle. De plus, le déni de service (DoS) est effectué dans notre simulation. Nous avons assumé le DoS effectué par l'intrus par une interruption de la ligne de transmission entre l'émetteur et le récepteur. Ce scénario convient particulièrement au canal à fibre optique. Dans notre scénario expérimental, l'intrus est la Hub de connexion entre l'émetteur et le récepteur. Elle peut faire divers actions pour obtenir la clé, ou simplement refuser la transmission.

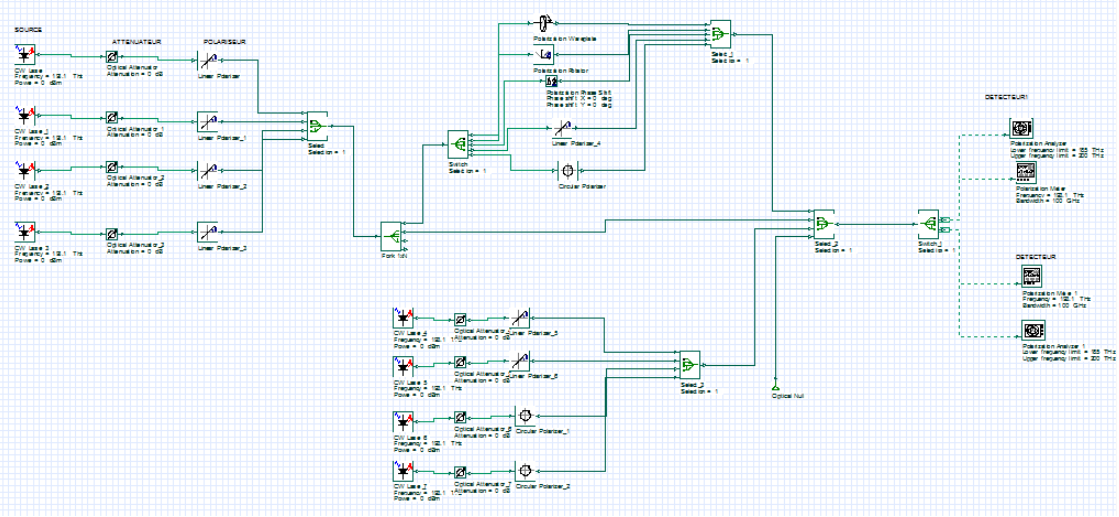


Figure 4.9: Simulation du model d'attaque de l'intrus sur un canal à BB84

L'attaque de sécurité de l'intrus sur le protocole BB84 est illustrée à la figure 4.9 L'intrus peut intercepter des qubits entrants et mesurer avec les polariseurs diagonaux rectilignes, déphasage, rotateur de photons.

Elle peut envoyer un nouveau qubit au récepteur. Autrement dit, elle peut également envoyer null qubit ou le qubit de l'émetteur au récepteur. Nous utilisons le composant «select» pour les attaques aléatoires de l'intrus. Enfin, nous le calculons sur les mesures de l'émetteur, l'intrus et le récepteur. Le nombre total de l'itération de balayage est de 10000.

Le tableau 4.2 représente les actions de simulation des attaques sur BB84 et les notations de tête de table, c'est-à-dire PZ polarisation, H, V et D correspondent à l'horizontale, à la verticale et au polariseur diagonal. La colonne 'Action' indique la décision réalisé par l'émetteur et le récepteur après des qubits d'échange.

Envoi		Reçu		Intrus		Décision
PZ	Bit	PZ	Bit	Attaque	Bit	
H	0	H/V	0	NLL	-	Sift Key
V	1	H/V	1	NLL	-	Sift Key
D	0	D	0	NLL	-	Sift Key
D	0	D	1	NLL	-	Sift Key
H/V	0/1	D	|?>	NLL	-	Discard
D	0/1	H/V	0/1	NLL	-	Discard
D	0/1	H/V	0/1	INTERCEPT RESEND (H/V)	0/1	Sift Key
H/V	0/1	H/V	|?>	INTERCEPT RESEND (D)	|?>	QBER

H/V	0/1	D	|?>	INTERCEPT RESEND (H/V)	0/1	IGNORE
D	0/1	D	|?>	INTERCEPT RESEND (H/V)	|?>	QBER
H/V-	0/1	H/V	|0/1> |?>	INTERCEPT RESEND (H/V)/D	|0/1> |?>	Sift Key/ QBER
D	0/1	D	-	DOS	-	NO ACTION
(H/V)D	0/1	(H/H)D	|/0/1>	DOS	-	REC/DET
			|?>			DARK

Tableau 4.2 : Simulation Action BB84 d'intrusion du model QKD

Le récepteur a envoyé un photon rectiligne à l'émetteur. L'émetteur passe en entrant un qubit au rotateur de Faraday et à l'issu de ce dernier, le photon sera reçu par le récepteur. L'émetteur a envoyé un photon non polarisé au récepteur. Les informations sur le photon sont calculées par la base de polarisation et du délai entre photons. La propriété du rotator de Faraday est donnée par la propriété suivante :
$H_{in} \rightarrow$ Rotor de Faraday $\rightarrow V_{out}$
$V_{in} \rightarrow$ Faraday Rotator $\rightarrow H_{out}$

Ici H et V se réfèrent à la base horizontale et verticale. Dans notre simulation, nous utilisons un rotateur de polarisation qui est intégré à OptiSystem. La simulation de QKD anti-bruit est représentée sur la figure 4.13 et les propriétés de la fibre optique de la figure 4.12. La propriété du rotateur de polarisation est :

$0^\circ - 90^\circ = -90^\circ$
$90^\circ - 90 = \quad 0^\circ$

Ici 0° et 90° se réfèrent aux angles rectilignes. Nous utilisons deux «Time Delay» pour les différences de temps entre photons envoyés. Les deux composants génèrent du temps / Valeur du générateur de nombres pseudo-aléatoires. C'est l'implémentation par simple expression VbScript en balayage d'itération.

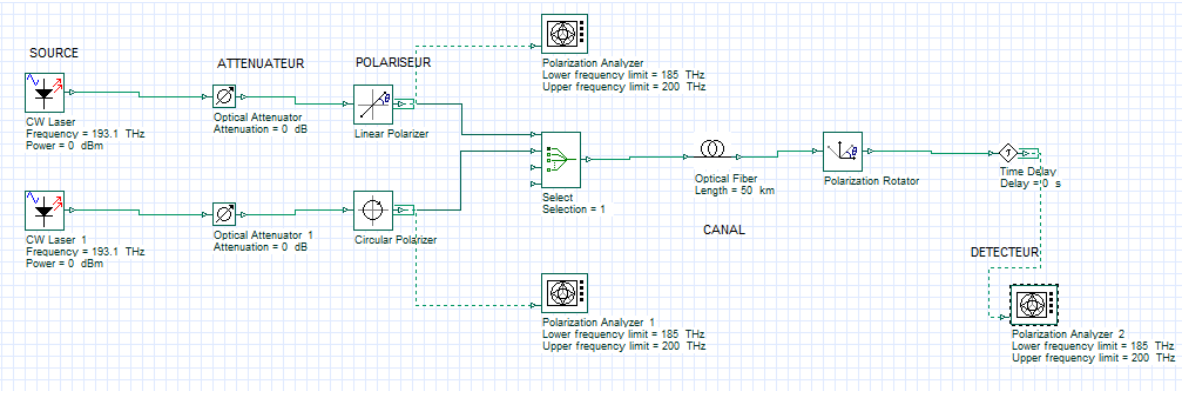


Figure 4.13: Implémentation de bruit sur canal à model QKD

Pour les détecteurs, nous avons utilisé l'analyseur de photons et toutes les données sont transférées vers une feuille Excel à l'aide de VbScript. La table élabore des actions de simulation. Le nombre total d'itération est de 10000.

SIMULATION DES EFFET DE BRUIT SUR CANAL QKD					
Paramètre d'envoi			Paramètre de réception	Résultats	
Envoi photon	Photon reçu				
	1er Photon	2nd Photon	Délais	Etat	Bit
H	V	non polarisé	Non	Accepté	0
V	H		Non	Accepté	0
H	Non polarisé	V	Oui	Accepté	1
V	Non polarisé	H	Oui	Accepté	1
H	H	Non polarisé	Non	Ignoré	-
V	V	Non polarisé	Non	Ignoré	-
H	V	-	Non	Ignoré	-
V	H	-	Non	Ignoré	-

Tableau 4.3 : Simulation de l'action du bruit sur un model QKD

4.8 Résultats et discussion

Dans cette section, nous soulignons certains résultats de configuration de la simulation. Les figures représentent les résultats de simulation du protocole BB84 et de la distribution de clés immunisées contre le bruit, le résultat est illustré dans la figure 4.10 à 4.13.

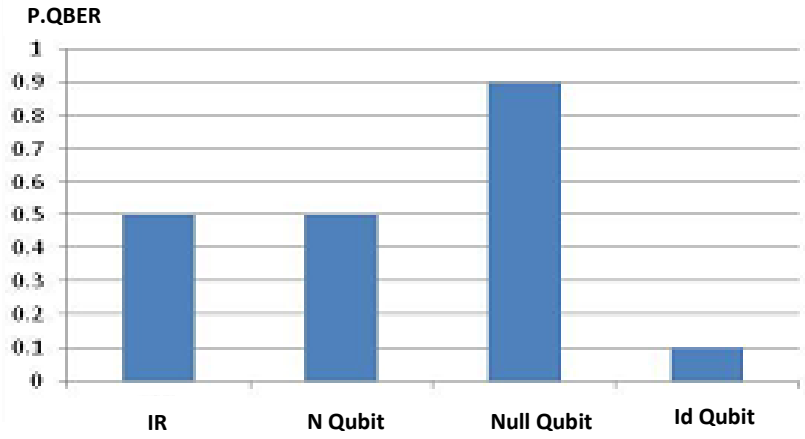


Figure 4.9 : La probabilité d'erreur quantique binaire suivant l'action de l'intrus

La figure 4.10 montre la probabilité de QBER par les attaques. L'attaque d'interception et de renvoi cause une probabilité QBER de 0,5. Cela est dû au hasard de la sélection de qubit par l'intrus. L'intrus peut causer 50% de chances de choisir un polariseur différent. La probabilité la plus élevée de QBER est faite par un qubit nul.

Dans notre simulation, il contribue 0.9 de probabilité pour QBER. Cette attaque peut facilement être détectée par des parties légitimes. Le qubit nul peut être une lumière non polarisée. Si l'intrus, permet le même qubit généré par l'émetteur et le récepteur choisit le correct, alors il contribue QBER plus bas. Dans notre simulation, 0,1 probabilité d'erreur est ajoutée pour l'inefficacité du détecteur.

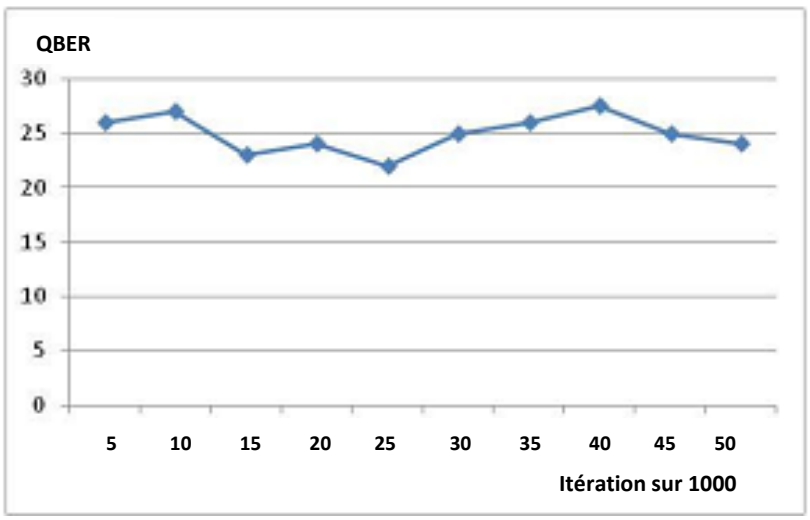


Figure 4.10 : Résultat de simulation d'attaque de l'intrus suivant le protocole BB84

La figure 4.11 montre globalement le QBER à chaque itération. La moyenne est de 25% de QBER. Cela indique la présence de l'intrus est fort et explicite.

Comme nous l'avons mentionné plus tôt, le caractère aléatoire est passé par le test de fréquence. Ainsi, chaque itération diffère les uns des autres. La fourchette globale de QBER de 22% à 38%.

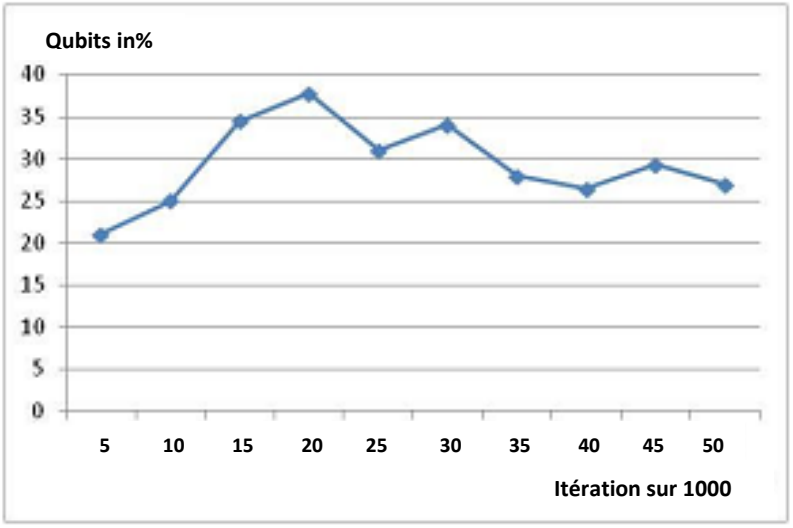


Figure 4.11 : Résultat de simulation QKD pour immunisions au bruit

La figure 4.12 illustre le pourcentage des qubits rejetés dans la configuration de la simulation. Dans cette expérience, aucun module de l'intrus est inclus et supposons que le canal et le récepteur sont idéal. Les résultats de notre simulation montrent l'intervalle de 20-38% des qubits rejetés dans la simulation. Le graphique présente de nombreuses fluctuations et met l'accent sur la mise en place aléatoire de la simulation. Implicitement, le résultat montre un taux directeur plus élevé que le montage expérimental. Plus de 65% des qubits peuvent être utilisés pour la génération de clés. Dans le cas expérimental, environ 25% des qubits soutiennent la génération des clés.
Le protocole BB84 exige de l'émetteur et du récepteur d'éliminer leurs données dès qu'ils identifient une erreur (remise au début du protocole BB84), donc ils ne réussiront jamais à échanger une clé secrète en suivant ce protocole. Pour cela l'émetteur et le récepteur utilisent le protocole et avec la méthode pour la correction d'erreur tout en suivant les mêmes conditions.

4.9 Conclusion de la simulation

Notre étude se concentre sur la configuration matérielle basée sur OptiSystem. Comme nous l'avons mentionné précédemment, QKD est une combinatoire et le paradigme des protocoles pour la sécurité inconditionnelle dans la distribution des clés. Les deux paradigmes devraient être évalués correctement pour comprendre les performances des protocoles QKD efficacement. Notre simulation met en relief les expériences pratiques légèrement modifiées. Le paramètre des composants modifié est une propriété intrinsèque du simulateur et aide à trouver la valeur optimale pour les paramètres expérimentaux. Ainsi, ce cadre de simulation réduit la mise en œuvre en choisissant la propriété des composants appropriés.

CONCLUSION

Pour conclure notre travail, la cryptographie quantique a pour objet de rendre notre communication inviolable vis à vis d'intrusion extérieure. Cela est possible grâce aux principes de la mécanique quantique sur la mesure, le théorème de non-clonage et de l'incertitude d'Heisenberg. Elle est utilisée pour secourir les méthodes de cryptographie mathématiques et algorithmiques qui sont de plus en plus vulnérable aux attaques des intrus. Pour la transmission par fibre optique, c'est l'élément clé pour la sécurisation de l'information. La QC est une méthode de cryptographie basée sur des procédés physiques et sur le code de Vernam à laquelle est adopté le protocole BB84. Ce dernier offre un canal de transmission inviolable, l'impossibilité de clonage et surtout un moyen efficace pour la détection d'intrusion. Grâce à notre simulation sur Opisystem, nous avons pu mettre en œuvre d'une part une liaison classique à base de fibre optique et d'autre part une liaison sur un canal quantique, ainsi qu'une simulation du phénomène d'intrusion entre émetteur et récepteur. A travers l'analyse des Taux d'Erreur sur des Bits Quantique ou QBER, nous serons en mesure de détecter l'existence d'interception sur le canal donc de pouvoir renforcer la sécurité de la communication. La solution par cryptographie quantique est déjà largement développée car il est disponible commercialement. Toutefois, l'implémentation de la Cryptographie quantique sur les réseaux optiques à très haut débit reste un défi technologique important car il est difficile voire impossible d'amplifier les photons pour une transmission de longue distance. Actuellement, de nombreux laboratoires de recherche se penchent sur la mise en place d'une solution standard pour pouvoir déployer la technique de cryptographie quantique sur nos réseaux optiques.

ANNEXE 1 : HISTORIQUE SUR L'EVOLUTION DU DOMAINE QUANTIQUE

1970 : Wiesner : Billets de banques infalsifiables et canaux multiplexeurs
1979 : Bennett et Brassard Prennent : connaissance des idées de Wiesner
1982 : Bennett, Brassard, Breidbart et Wiesner : Jetons de métro infalsifiables
Bennett, Brassard et Breidbart : Réutilisation sécuritaire d'une clef pour un code de Vernam
1984 : Bennett et Brassard BB84 : Protocole quantique de distribution de clefs secrètes basé sur le principe d'Heisenberg et tirage à pile ou face quantique
1989 : Bennett et Brassard : Expérimentation du premier prototype opérationnel basé sur le protocole BB84
1990 : Brassard et Crépeau : « Tirage à pile ou face quantique et "bit committement protocol"
1991 : Ekert : Protocole quantique de distribution de clefs secrètes basé sur le principe de EPR et le théorème de Bell Bennett, Brassard, Crépeau et Skubiszewska "Practical quantum oblivious transfert"

1992 : Bennett : Protocole quantique de distribution de clefs secrètes basé sur le principe de vecteurs d'états non-orthogonaux. Bennett, Brassard et Mermin Cryptographie quantique sans le théorème de Bell Ekert, Rarity, Tapster et Palma : Cryptographie quantique basée sur la corrélation de paires de photons
1993 : Muller, Breguet et Gisin : Réalisation à Genève, sur 1km des fibres optiques, du protocole BB84.
1994 : Shor Factorisation des grands nombres en temps polynomial
1995 : Yao : Démonstration de la sécurité des protocoles quantiques par rapport aux attaques basées sur le principe des mesures cohérentes
1996 : Mayers : démonstration qu'il n'existe pas de "bit commitement protocol" inconditionnel sécuritaire Deutsh et Ekert

ANNEXE 2 : PRINCIPES DE LA MECANIQUE QUANTIQUE

La mécanique quantique est la branche de la physique qui a pour objet d'étudier et de décrire les phénomènes fondamentaux à l'œuvre dans les systèmes physiques, plus particulièrement à l'échelle atomique et subatomique [33].

La mécanique quantique comporte de profondes difficultés conceptuelles, et son interprétation physique ne fait pas l'unanimité dans la communauté scientifique[1]. Parmi ces concepts, on peut citer la dualité onde corpuscule, la superposition quantique, l'intrication quantique ou encore la non-localité.
Le photon est également pourvu d'une impulsion :

$$\boldsymbol{p} = \hbar \boldsymbol{k} \qquad |\boldsymbol{k}| = 2\pi/\lambda \tag{A2.1}$$

Ou k est le vecteur d'onde de l'onde électromagnétique

Bohr postule que les énergies des édifices atomiques et moléculaires n'adoptent que des valeurs discrètes, et que l'émission ou l'absorption de lumière par ces édifices ne se fait que pour certaines fréquences lumineuses bien précises :

$$\nu_{if} = |E_i - E_f|/h \tag{A2.2}$$

Où E_i et E_f sont les énergies du système avant et après l'émission ou l'absorption de même que la lumière présente un comportement corpusculaire, de même, suppose Louis de Broglie, les particules, par exemple l'électron, peuvent présenter un comportement ondulatoire. A toute particule de vitesse v et d'impulsion p = mv, de Broglie « associe » une onde, de longueur d'onde :

$$\lambda = h/p \tag{A2.3}$$

-Les phénomènes quantiques sont de nature aléatoire. On ne peut prévoir le résultat d'une expérience que sous forme statistique ou probabiliste (un seul évènement).
-L'analyse des phénomènes d'interférences et de difractions montre qu'en mécanique quantique, on ne peut se contenter de travailler avec des lois de probabilité, comme dans les phénomènes aléatoires usuels. Il faut introduire des amplitudes de probabilité dont le module carré donne la probabilité recherchée.
-Les particules ont un comportement ondulatoire à l'échelle microscopique.
-Certaines grandeurs physiques, qui classiquement peuvent prendre un ensemble continu de valeurs, n'adoptent en mécanique quantique que des valeurs discrètes. C'est par exemple le cas pour l'énergie interne des atomes et des molécules.
- En général, le fait de mesurer une grandeur physique affecte le système considère.

ANNEXE 3 : PRINCIPE D'INCERTITUDE D'HEISENBERG

Le principe d'incertitude ou principe d'indétermination, aussi connu sous le nom de principe d'incertitude de Heisenberg, désigne l'inégalité mathématique affirmant qu'il existe une limite fondamentale à la précision avec laquelle il est possible de connaître simultanément deux propriétés physiques d'une même particule ; ces deux variables dites complémentaires peuvent être sa position et sa quantité de mouvement [33] [34].

Présenté pour la première fois en 1927, par le physicien allemand Werner Heisenberg, il énonce que toute amélioration de la précision de mesure de la position d'une particule se traduit par une moindre précision de mesure de sa vitesse et vice-versa. L'inégalité formelle reliant l'écart type de la position σ_x et l'écart type de la quantité de mouvement σ_p a été établi par Earle Hesse Kennard plus tard la même année et par Hermann Weyl en 1928 :

$$\sigma_x \sigma_p \geq \frac{h}{2} \qquad \text{(A3.1)}$$

Où ħ est la constante de Planck réduite, égale à h/2π. La quantité de mouvement étant le produit de la masse m et les vitesses v, cette relation peut aussi être écrite

$$\sigma_x \sigma_v \geq \frac{h}{2m} \qquad \text{(A3.2)}$$

Cette forme met en évidence que le produit des deux écarts types est important surtout pour les particules microscopiques qui ont de petites masses. Pour les objets macroscopiques de masse grande, ce produit est négligeable de sorte que leur mouvement est bien décrit par la mécanique newtonienne.

ANNEXE 4 : LES INEGALITES DE BELL

On se place dans la situation du paradoxe EPR. Il s'agit d'une expérience de pensée. On a un système qui émet des paires de particules dans l'état particulier. On a disposé deux détecteurs de part et d'autre de l'émetteur et à égale distance de celui-ci. Cette fois-ci on peut mesurer trois grandeurs A, B ou C. Les résultats possibles sont (A+) et (A-) si on mesure A, (B+) et (B-) si on mesure B... Si on mesure la même grandeur pour les deux particules d'un même couple les résultats sont opposés. On aura par exemple (B+, B-) ou (C-,C+).

Comment les particules d'une même paire peuvent-elles donner simultanément le même résultat alors qu'elles n'ont pas eu le temps de communiquer? On ne va pas croire à la MQ et ses explications fumeuses, on va faire des variables cachées. Nous allons donc dire que les particules ont décidé de la réponse qu'elles vont donner avant d'avoir atteint le détecteur, par exemple au moment de se quitter. Si on fait une théorie totalement déterministe, cette date est même reportée à t=-infini. Comme on peut mesurer trois grandeurs sur ces particules, elles ont dû décider des réponses à donner à chacune des trois mesures. Ainsi, les particules émises peuvent se classer en 8 classes : (A+B+C+), (A+B+C-), ... (A-B-C-). Les deux particules d'une même paire sont toujours dans des classes opposées. Voilà comment on explique de façon naturelle et intuitive le fait que deux particules d'une même paire donnent toujours des réponses opposées.

Malheureusement on ne peut pas déterminer dans laquelle de ces 8 classes se trouve une particule donnée. On sait que lorsqu'on fait une mesure sur une particule on modifie son état, c'est bien vérifié expérimentalement. Donc une deuxième mesure sur la même particule ne me renseigne en rien sur l'état de la particule avant la première mesure. Pourtant il y a une ruse qui nous permet d'avoir accès à deux des variables associées à une particule. Puisque les deux particules d'une paire sont dans des états opposés, si je mesure (A+) pour l'une, je sais que l'autre est (A-). Disons que je mesure A sur l'une et B sur l'autre. Si j'obtiens (A+)&(B+), je sais que mes particules étaient (A+B-)&(A-B+).

On constate que les résultats des différentes mesures sont aléatoires. Comme on croit au déterminisme on est porté à croire que l'origine de cet aléatoire est le chaos déterministe, mais ce n'est pas un hypothèse nécessaire. Livrons nous à un petit calcul de probabilités. Une particule (A+B+) doit être nécessairement soit (A+B+C+), soit (A+B+C-). Si on note P(état) la probabilité d'être dans un certain état, on peut écrire trivialement [34] :

$$P(A+B+) = P(A+B+C+) + P(A+B+C-) \qquad (A4.1)$$

Pour la même raison on a :

$$P(A+B+C+) <= P(A+C+) \qquad (A4.2)$$

$$P(A+B+C-) <= P(B+C-) \qquad (A4.3)$$

Si on reporte (2) et (3) dans (1) on obtient : l'INÉGALITÉ DE BELL.

$$P(A+B+) <= P(A+C+) + P(B+C-) \qquad (A4.5)$$

ANNEXE 5 : DUALITE ONDE CORPUSCULE

Soit les expériences de la mise en évidence de la dualité suivant :

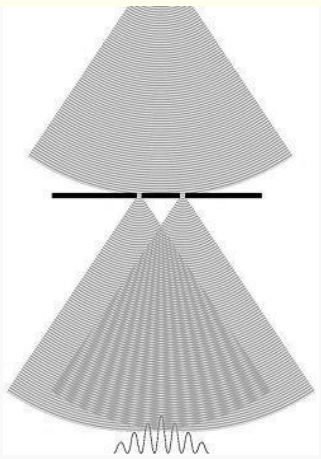


Figure A5.1 : Schéma de l'expérience.

Une des manières les plus claires de mettre en évidence la dualité onde-particule est l'expérience des fentes de Yong. Cette expérience est connue depuis le XIXe siècle, où elle a d'abord mis clairement en évidence l'aspect purement ondulatoire de la lumière. Modifiée de manière adéquate, elle peut démontrer de manière spectaculaire la dualité onde-corpuscule non seulement de la lumière, mais aussi de tout autre objet quantique. Dans la description qui suit, il sera question de lumière et de photons mais il ne faut pas perdre de vue qu'elle est également applicable - du moins en principe - à toute autre particule (par exemple des électrons), et même à des atomes et à des molécules.

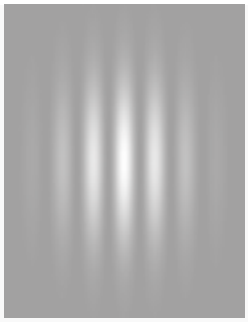


Figure A5.2 : Figure d'interférence observée.

L'expérience consiste à éclairer par une source lumineuse un écran percé de deux fentes très fines et très rapprochées. Ces deux fentes se comportent comme deux sources secondaires d'émission lumineuse. Une plaque photographique est placée derrière l'écran enregistre la lumière issue des deux fentes. Ces deux sources interfèrent et forment sur la plaque photographique ce que l'on appelle une figure d'interférence. Cette figure est caractéristique d'un comportement ondulatoire de la lumière. Si l'expérience en reste à ce niveau, l'aspect corpusculaire n'apparait pas.

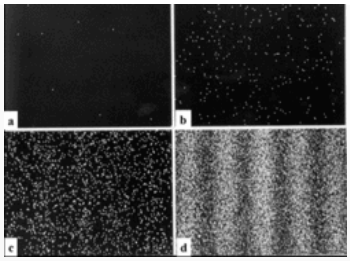


Figure A5.3 : Figure d'interférence constituée petit à petit

En fait, il est possible de diminuer l'intensité lumineuse de la source primaire de manière à ce que la lumière soit émise photon par photon. Le comportement de la lumière devient alors inexplicable sans faire appel à la dualité onde-corpuscule.

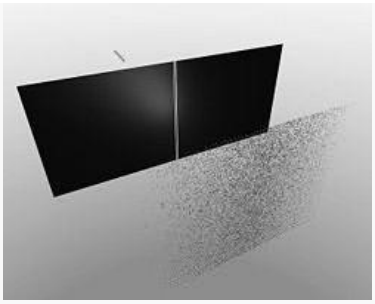


Figure A5.4 : Expérience avec de "vraies" particules, par exemple des micro-billes.

En effet, si on remplace la source lumineuse par un canon qui tire des micro-billes à travers les deux fentes (par exemple), donc de "vraies" particules, on n'obtient aucune figure d'interférence, mais simplement une zone plus dense, en face des fentes. Or, dans le cas des photons, on retrouve la figure d'interférence reconstituée petit à petit, à mesure que les photons apparaissent sur la plaque photographique. On retrouve donc une figure d'interférence, caractéristique des ondes, en même temps qu'un aspect corpusculaire des impacts sur la plaque photographique.

L'interprétation de cette expérience est difficile, car si on considère la lumière comme une onde, alors les points d'impacts sur la plaque photographique sont inexplicables; on devrait voir dans ce cas très faiblement, dès les premiers instants, la figure d'interférence de la figure A5.2, puis de plus en plus intense. Au contraire, si on considère la lumière comme étant exclusivement composée de particules, alors les impacts sur la plaque photographique s'expliquent aisément, mais la figure d'interférence ne s'explique pas : comment et pourquoi certaines zones seraient privilégiées et d'autres interdites à ces particules

ANNEXE 6 OPTISYSTEM

Le logiciel OPTISYSTEM ou" Optical Communication System Design Software" est un outil professionnel de simulation et planification de systèmes de communication par fibre optique FO et FSO (Optique en espace Libre). Il permet une large possibilité pour des ingénieurs, des chercheurs en laboratoire et des experts dans le domaine photonique, optoélectroniques. Optisystem offre de resultat precise et une performance excellent.

Figure A6.1 : Visuel du logiciel Optisystem-Optiwave

Optisystem est composé de plusieurs composants dédié au réseau optique et une possibilité d'exporter des données ou résultat vers Excel, Matlab et VBscrip pour l'analyse des résultats.

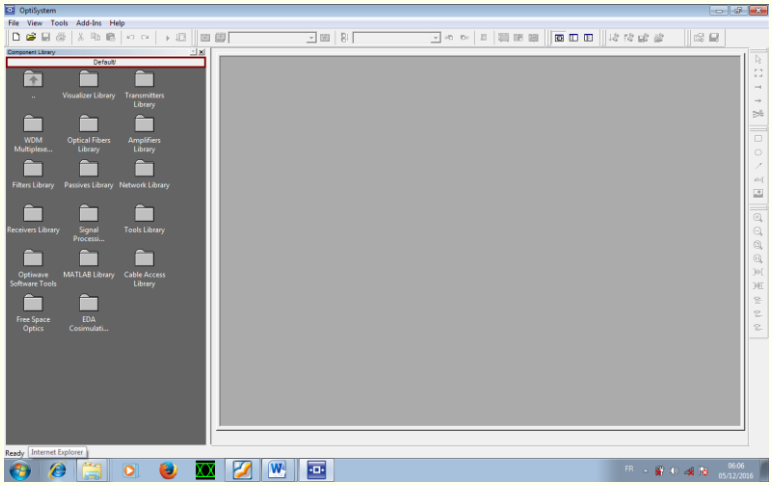


Figure A6.2 : Interface d'Optisystem 7.0

ANNEXE 7 : POTENTIEL INDUSTRIEL ET SOLUTION COMMERCIAL

Figure A7.1 : MagiQ **,** Boston, USA www.magiqtech.com

Figure A7.2 : IdQuantique, Genève, Suisse, www.idquantique.com

Figure A7.3 : SmartQuantum, Lannion, Metz, France, www.smartquantum.com

La cryptographie quantique progresse régulièrement et des systèmes sont disponibles commercialement. Le défi actuel c'est la mise en œuvre et évaluation en réseau.

REFERENCES

[1] P. Lecoy, « *Télécommunications optiques* », Hermes, Paris, 1992

[2] S. Ungar , « *Fibres optiques, Théorie et applications* », Dunod, Paris, 1989

[3] Y. Suematsu, K-I. Iga, « *Transmission sur fibres optiques* », Masson, Paris, 1996

[4] C. Vassalo: « *Fibres optiques pour les Télécommunications* », Techniques de l'Ingénieur, Traité Electronique, E 7 370, 1990

[5] I. Joindot , M. Joindot , « *Les Télécommunications par Fibre Optique* », Collection Technique et Scientifique des Télécommunication, Dunod, Paris, 1996

[6] P.G. Fontolliet, « *Systèmes de Télécommunications volume XVIII* », Presse Polytechniques, 2010

[7] T. Anfray, «*Étude et simulation des potentialités du dual electro absorption modulated Laser pour la montée en débit dans les futurs réseaux d'accès optique* », Thèse Pour obtenir le grade de Docteur de l'université de Limoges, 2013

[8] J .L . Verneuil, «*Simulation de systèmes de télécommunications par fibre optique à 40 Gbits/s* », Thèse pour obtenir le grade de Docteur de l'université de Limoges, 2003

[9] C .C. Cordat, « la fibre optique», 2003.

[10] M. Molnár, B. Cousin, « *Les réseaux tout optique* », IRISA, Cours Master 2,2006

[11] M. Bloch, « *Algorithme de réconciliation et méthodes de distribution quantique de clés adaptées au domaine fréquentiel* », Université de Franche-Comté, 2006.

[12] S. Fossier, « *Mise en œuvre et évaluation de dispositifs de cryptographie quantique à longueur d'onde télécom* », Université Paris Sud - Paris XI, 2009.

[13] CESIRE Plate-forme Optique, » *Polarisation et biréfringence* », Université Joseph Fourier, 2008-2009

[14] Cours Cryptologie « *Sécurité des systèmes d'information* », Vuibert – Paris, 2012-2013

[15] J. Marion, « *Sécurité des systèmes d'information* », Université de Nancy, 2007

[16] K. Banaszek, R. D. Dobrzanski, » *Quantum information ½* », Canada, 2012

[17] J. Merolla, « *Optical homodyne detection and applications in quantum cryptography*", Telecom ParisTech,2009

[18] P. Jorrand, « *Cryptographie quantique* », Laboratoire Leibniz, Grenoble, France, 2006

[19] Dalibor, "*Security aspects and simulations of practical QKD*", Platforms, 2005.

[20] Y. Leroyer et G. S, « *Introduction à l'information quantique* », 2015.

[21] H. Amellal, » *Étude de cryptographie et analyse des stratégies d'attaques quantiques* », université Mohammed V faculté des sciences, Rabat, 2016.

[22] Y. Dumeige, « *Source de photons uniques et applications-Introduction à l'optique quantique* », Université de Rennes 1 / IUT de Lannion,2016-2017.

[23] D.Feyel, » *Espaces de Hilbert* », Université d'Evry M52, 2008-09

[24] G. Messin, » *Photons uniques et cryptographie quantique* »Laboratoire Charles Fabry de l'Institut d'Optique, CNRS/Institut d'Optique / F. Treussart, Laboratoire de photonique quantique et moléculaire, CNRS/ENS Cachan, 2002

[25] S. Aybar, R. Harrison, I. Sairitupa, J. Thomas, R. Frank," *Developing a quantum Key distribution simulator* », May 2013

[26] R. C. Bialczak, » *Development of the fundamental components of a superconducting qubit Quantum Computer*", university of California Santa Barbara, 2011

[27] Y. Zhao, B. Qi, X. Ma, H. Lo, L. Qian, "*Experimental decoy state quantum key distribution over 15km*", Department of Physics and Department of Electrical and Computer Engineering, Canada, 2005

[28] J. Bas, J. Dalibard, », *Mécanique quantique* », cours de l'´école polytechnique, Février 2002

[29] Bocquet, » *Modèles de sécurité réalistes pour la distribution quantique de clés* », Télécom Paris Tech, 2011.

[30] M. Niemiec, « *Design, construction and verification of high-level security protocol allowing to apply the quantum cryptography un communication network*", AGH University, 2011.

[31] E. Meyer-Scott, » *Experimental quantum communication in demanding regimes* », University of Waterloo Canada, 2011.

[32] C. J Ware, » *Modeling and analysis of quantum cryptographic protocols*", University of Victoria 2005.

[33] E. Simonsen, » *Security of quantum key distribution source* », Norwegian University of Science and Technology, June 11, 2010

[34] A Buhari, Zuriati. A. Zukarnai, Shamala. K.Subramaniam, Hisham. Zainuddin, S. Saharudin, » *BB84 and noise immune quantum key distribution protocols simulation: an approach using photonic simulator* », Instrumentation and Biomedical Engineering Bangkok, 2012

Auteurs : DIEU DONNE Richard Jean Noel

Titre :
« SECURISATION DE LA TRANSMISSION OPTIQUE PAR CRYPTOGRAPHIE QUANTIQUE QKD»

Nombre de pages : 85
Nombre de figures : 61
Nombre de tableaux : 05

RESUME

La fibre optique est un support de transmission privilégiée pour le transport de divers type de données public, privée et confidentiel. La cryptographie quantique est utilisé pour sécuriser ces divers données grâce au quantum Key Distribution et le protocole BB84 pour la 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 permis d'implémenter un comportement équivalent d'une liaison optique illustrant le principe de base du QKD et l'analyse des Taux QBER nous permet de conclure l'existence d'intrus sur le canal de communication.

Mots-clés : fibre optique, cryptographie quantique, QKD, BB84, QBER

.

Rapporteur : Monsieur RASTEFANO Elisée
Adresse: A3J Ambohimiandra, Antananarivo – 101
Contact : +26134 99 846 70
E-mail : richar7djean@yahoo.fr