République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieure et de la Recherche Scientifique

Université Abderrahmane Mira

Faculté de Technologie

Département d'Automatique, Télécommunication et d'Electronique

Projet de Fin d'études

Pour l'obtention du diplôme de Master

Filière : Télécommunication

Spécialité : Réseaux et Télécommunications

Thème

Implémentation du protocole B92 dans une liaison optique

Préparé par :

M^lle^ CHILA Sarah

M^lle^ DJEBARA Kahina

Dirigé par :

***Mr** BERRAH Smail*

Examiné par :

***Mr** ALLICHE* Abdenour

***Mme** BOUNCER Samira*

Année universitaire : **2020/2021**

À mes très chers parents : Tahar, Farida

A ma deuxième mère Houri

A mes grands parents

Que Dieu les gardes

A Mes sœurs : Nadjette, Amina, Imene

A mes amis : Nesrine, Narimane, Meriem , Manel, Fatima,

Sarah, Manel

A

Ma chérie avec qui j'ai Réalisé ce Travail : Kahina

À tous ceux qui sont proches à mon cœur

SARAH !

À mes très chers parents : Mahdi, Aicha

A ma deuxième mère Fatima

Que Dieu les gardes

A mon grand-père Hachemi ellah irehmou

A Mes frères : Lamine, Bilal

A mes amis : Lilia, Sabrina, Fouzia, Salwa, Meriem ,

Fatima, Sarah, Manel

A

Ma chérie avec qui j'ai Réalisé ce Travail : Sarah

À tous ceux qui sont proches à mon cœur

KAHINA !

REMERCIEMENTS

Tous d'bord nous remercions le BON DIEU de nous avoir aidés à accomplir ce modeste travail

Nous ne saurions réellement, trouver les expressions éloquentes que mérite notre encadreur « Mr : BERRAH », à fin de le remercier pour son sympathies, encouragements, aides, dévouements pour son travail et sa présence total.

Nous tenons à remercier vivement «Mr : ALLICHE » et «Mme : BOUNCER» de l'université de Bejaia d'avoir pour l'intérêt qu'ils ont porté en acceptant d'examiner notre travail et l'enrichir par leurs propositions.

Nous tenons également remercier Mme : BOUCHOUCHA»

Pour son aide précieux

Enfin, Un énorme merci à nos familles et amis pour leurs éternel soutien et confiance qu'ils ont en nos capacités.

Table des matières

Chapitre I: Généralités sur la cryptographie

Chapitre II: Implémentation du protocole B92 sur OPTISYSTEM sans et avec espion

Chapitre III : Etude des performances du protocole B92 dans une liaison optique

Liste des figures

Liste des tableaux

Liste des abréviations

AES Advanced Encryption Standard

B92 Bennett 1992

BB84 Charles Bennett et Gilles Brassard 1984

BER Bit-Error Rate

CW Continus Wave

DES Data Encryption Standard

EDFA Erbium-Doped Fiber Amplifier

NIST National Institute Of Standards and Technology

NRZ Non Return to Zero

NSA National Security Agency

RSA Ron Rivest, Adi Shamir et leonard Adelman

Q Facteur de Qualité

QKD Quntum Key Distribution

Qubit Quantum + bit

Introduction

Introduction générale

Depuis l'Antiquité, l'homme a ressenti toujours un besoin pressant de communiquer et d'échanger des informations de manière sure. Ce dernier a utilisé au fur et à mesure de différents moyens qui ont évolué au cours du temps afin de sécuriser l'information qu'il voulait transmettre. La sécurité de l'information est l'un des piliers majeurs de tout système d'information quelle que soit sa nature. Pour protéger une information, rien de plus simple que de l'écrire de sorte que seul le destinataire légitime puisse la comprendre, c'est exactement ce que fait la cryptographie.

La cryptographie, ou encore la science du secret, se définit comme étant la transformation d'une information sous une autre forme en utilisant un algorithme et une information supplémentaire dite clé de cryptage. Actuellement, les techniques de cryptographie se classent en deux grandes familles en se basant sur le nombre de clés utilisées. On parlera de cryptographie symétrique, comme DES, AES,…. Et asymétrique tel que le RSA.

Aujourd'hui, ce besoin de communiquer est toujours plus important non seulement parce que la masse d'informations qui circule est conséquente, mais aussi pour son importance qui requiert un certain niveau de sécurité. Le e-commerce, e-health, visioconférence, militaire…sont toutes des applications où l'information requiert justement un niveau élevé de sécurité. En 2020 le e-commerce a enregistré un chiffre de 112 milliards d'euros [1].

Avec les progrès mathématiques et technologiques, la sécurité des méthodes de cryptage les plus répandues est menacée. A titre d'exemple, le RSA-768 (232 chiffres décimaux) a été cassé après 2 ans et demi de calcul [2].Ce qui revient à dire que la résolution de tel problème mathématique n'est difficile que pour une capacité de calcul actuelle et que si un calculateur puissant existait, il serait facilement possible de retrouver les clés de chiffrement/déchiffrement, tel est le cas du calculateur quantique qui marque un nouveau record en factorisant le nombre 56,153 avec seulement 4-qubits[3]

La cryptographie quantique permet de remédier à cet inconvénient. Cette technique est structurée sur des concepts de la physique quantique et la théorie de l'information dans le sens qu'elle applique la mécanique quantique, elle montre comment les photons peuvent être utilisés pour transmettre de l'information

Introduction générale

L'objectif de notre travail c'est d'étudier et de simuler le protocole B92 dans une liaison optique en présence et en absence d'un espion, afin de voir son efficacité.

Le présent manuscrit est organisé en trois chapitres :

Le premier chapitre présente un aperçu général sur des notions de cryptographie classique, et les diverses classes de cryptographie existantes. Ensuite il traite les principes et les fondements sur lesquels se base la cryptographie quantique.

Le deuxième chapitre présente les différentes phases constituantes un protocole quantique et une description détaillée du protocole B92.Ensuite, se termine par la simulation du protocole quantique B92 sur OPTISYSTEM. Où nous implémenterons le protocole sur une liaison optique pour évaluer la polarisation du photon et le phénomène d'espionnage.

Le troisième chapitre sera consacré à la simulation d'une chaine de transmission avec le protocole quantique B92 sur OPTISYSTEM. Où nous étudierons la qualité de transmission de ce dernier.

Nous terminerons le présent mémoire par une conclusion et perspectives.

Chapitre I

Généralités sur la cryptographie

I.1 Introduction

La cryptographie a pris une grande dimension et est devenue une discipline scientifique à part entière. Elle utilise des concepts mathématiques et informatiques pour crypter les données.

Dans ce premier chapitre, nous présenterons quelques généralités sur la cryptographie. Un aperçu sur le principe et les algorithmes de la cryptographie classique et moderne sera donné. En mettant l'accent sur les limites de cette dernière. De ce fait, nous nous intéresserons à la cryptographie quantique. Ensuite nous introduirons quelques notions de base du monde quantique nécessaires et utiles pour la cryptographie quantique.

I.2 Généralités sur la cryptographie

I.2.1 Définition

L'origine du mot cryptographie est grec, il est devisé en deux partie kruptos et graphein qui signifient respectivement cacher et écrire [4].

La cryptographie est une science qui utilise les mathématiques pour le cryptage et le décryptage, permettant ainsi de convertir des informations "en clair" en informations codées ou chiffrées, c'est à dire non compréhensible, puis, à partir de ces informations codées, de restituer les informations originales en utilisant une clé de chiffrement. Elle regroupe un ensemble de techniques afin d'assurer la sécurité des communications et des données stockées et les transmettre sur des réseaux non sécurisés.

Un système de cryptographie est représenté sur la figure I.1, il est constitué comme suit :

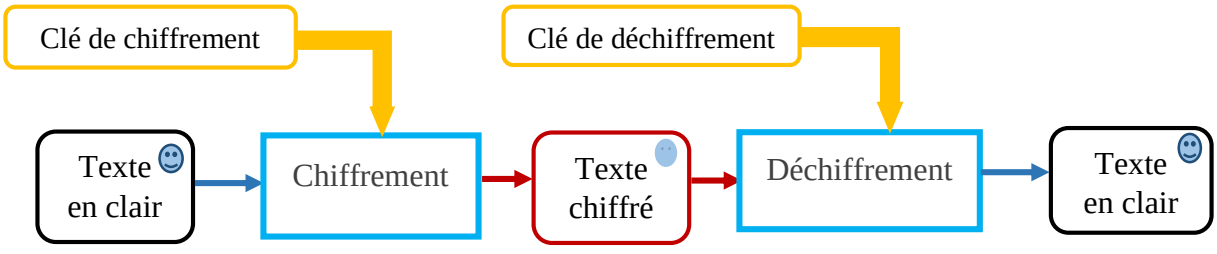


Figure I.1 Modèle simple de la cryptographie.

- **Texte en clair :** C'est le message à protéger.
- **Texte chiffré :** Le texte chiffré est le résultat de l'application d'un chiffrement à un texte clair.

- **Chiffrement :** C'est la méthode utilisée pour transformer un texte en clair en texte chiffré.
- **Déchiffrement :** C'est l'opération permettant de retrouver le texte clair à partir du texte chiffré.
- **Clé :** C'est le secret partagé utilisé pour chiffrer le texte en clair en texte chiffré et pour déchiffrer le texte chiffré en texte en clair.
- **Algorithme :** C'est la définition des fonctions mathématiques utilisées pour le chiffrement et le déchiffrement.

I.2.2 Objectif de la cryptographie

L'objectif de la sécurité d'un système informatique est la protection des informations et des ressources contre toute dévaluation, modification ou destruction.

Le but de la cryptographie est de respecter adéquatement les objectifs suivants.

- **La confidentialité :** Il s'agit de rendre la lecture du message inintelligible à des tiers non autorisés.
- **L'intégrité** : Qui assure que l'information n'a pas été modifiée entre son envoi et sa réception.
- **L'authentification :** L'authentification est un mécanisme permettant d'identifier des personnes ou des entités et de certifier leur identité.
- **Non Répudiation :** signifie que l'expéditeur peut vérifier qu'un certain destinataire a reçu un message particulier. [5]

I.3 Les classes de la cryptographie

On peut regrouper les systèmes de chiffrement en trois classes comme nous le montre la figure I.2.

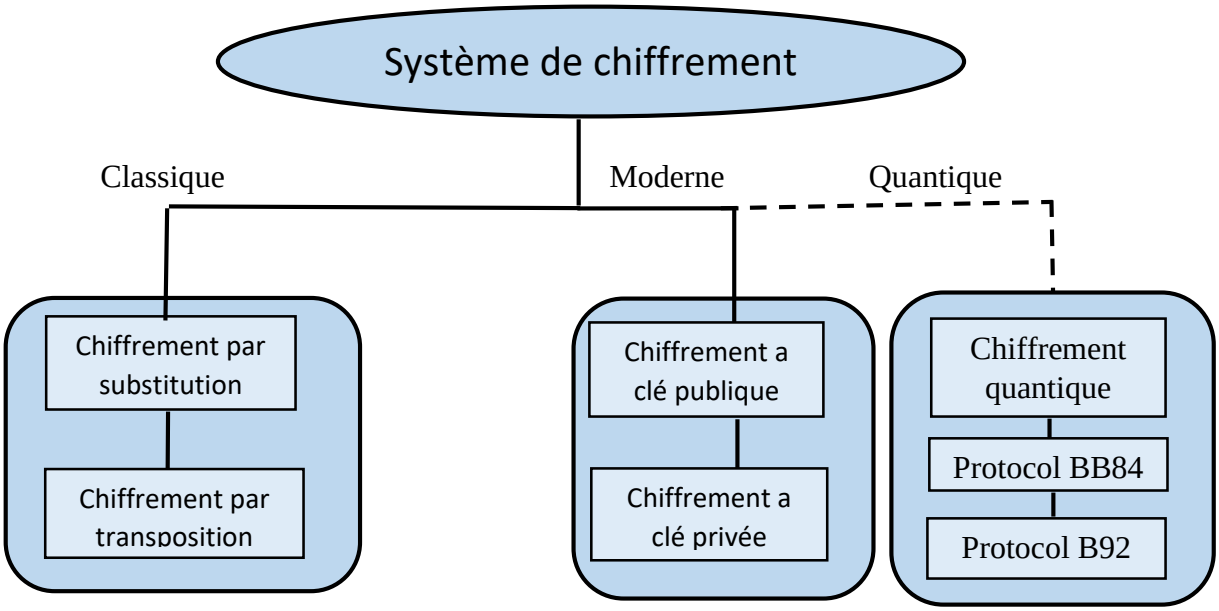


Figure I.2 Système de chiffrement.

I.3.1 La cryptographie classique

La cryptographie classique décrit la période avant les ordinateurs durant laquelle, les principaux outils utilisés consistent à remplacer des caractères par d'autres et ou les transposer dans des ordres différents tout en gardant secrètes les procédures de chiffrement ou de déchiffrement.

La plupart des méthodes de cryptographie classique reposent sur deux principes essentiels : la substitution et la transposition [6].

I.3.1.1 La cryptographie par substitution

Le chiffrement par substitution, historiquement est le premier type de chiffrement utilisé. Il consiste à remplacer certaines entités (généralement des lettres) par d'autres ou par des symboles dans un message [6].

- **Exemple**

Dans le message clair, on remplace chaque lettre par une lettre différente. Tel qu'il est illustré dans le tableau I.1.

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

Tableau I.1 Exemple de la substitution.

Texte clair : cryptographie

Texte chiffré : FWAIVRKWDIL

I.3.1.2 Chiffrement par transposition ou chiffrement par permutation

Les méthodes de chiffrement par transposition consistent à réarranger les données à crypter de telle façon à les rendre incompréhensibles [4]. Avec le principe de la transposition toutes les lettres du message sont présentées, mais dans un ordre différent.

- **Exemple**

On cherche à chiffrer le message secret

Lettre	S	E	C	R	E	t
Position	1	2	3	4	5	6
Permutation	5	3	1	4	6	2
Texte chiffré	E	C	S	R	T	E

Tableau I.2 Principe de la transposition.

Le message chiffré est : ECSRTE

I.3.2 La Cryptographie moderne

Au fil du temps, des calculateurs puissants sont apparue et les techniques de cryptographie classique sont devenues inefficaces. Par conséquent de nouvelles techniques ont été amenées et une nouvelle classe a été introduite il s'agit de la cryptographie moderne.

On trouve principalement deux grandes familles :

- La cryptographie symétrique ou à clé secrète.
- La cryptographie asymétrique ou à clé publique.

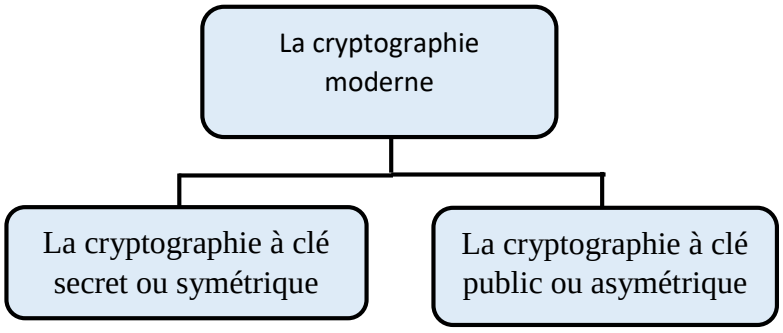


Figure I.3 Les méthodes de la cryptographie moderne.

Ils ont tous les deux leurs avantages et leurs inconvénients. La différence qui existe entre ces deux types se situe au niveau de la clé.

I.3.2.1 Le chiffrement symétrique

Le chiffrement symétrique (aussi appelé chiffrement à clé privée ou chiffrement à clé secrète) consiste à utiliser la même clé pour le chiffrement et le déchiffrement entre deux utilisateurs, comme le représente la figure I.4

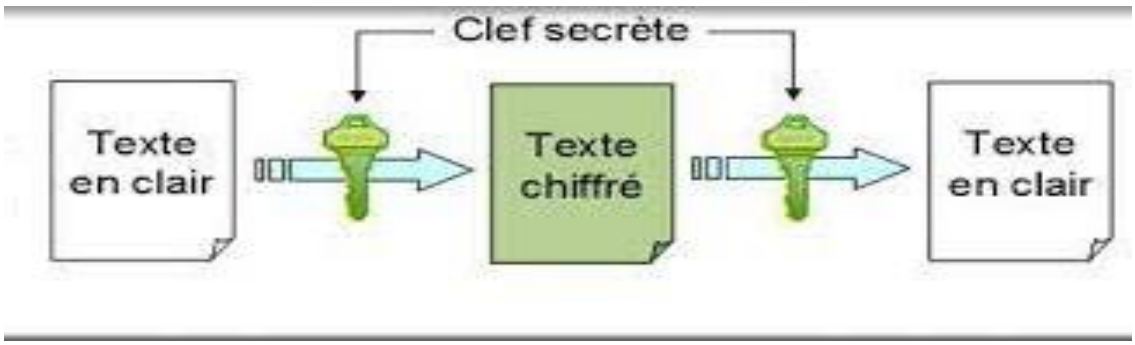


Figure I.4 Chiffrement symétrique.

Plus précisément, pour transmettre un message l'émetteur réalise au préalable le chiffrement en utilisant une clé secrète. A la réception, le destinataire reçoit le message crypté et applique un algorithme de déchiffrement avec la même utilisée clé que l'émetteur utilise pour le message en clair.

Les algorithmes de chiffrements symétriques les plus utilisés sont le DES et l'AES.

- **DES (Data Encryption Standard)**

La norme DES est adoptée par NSA en 1967 [7]. C'est un algorithme de chiffrement par bloc qui agit sur des blocs de 64 bits. La longueur de la clé est de 56 bits.

- **AES (Advanced Encryption Standard)**

AES est le nouveau standard de chiffrement à clé secrète et le successeur de DES, il a été choisi parmi une vingtaine d'algorithmes qui ont participé à un concours lancé par NIST (National Institute Of Standards and Technology).Il Utilise des clés de tailles 128, 192 et 256 bits. [8]

I.3.2.2 Le chiffrement asymétrique

En 1976, Whitfield Diffie et Martin E. Hellman décrit la possibilité de développer un algorithme de chiffrement basé sur deux clés différentes [5].

La cryptographie à clé publique (asymétrique) consiste en l'existence d'une paire de clés de chaque côté (émetteur et récepteur) liées mathématiquement. Chaque paire est composée d'une clé privée et d'une clé publique.

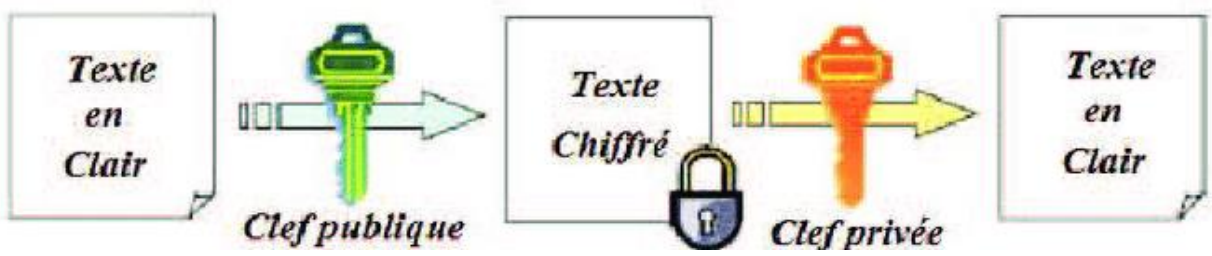


Figure I.5 Chiffrement asymétrique.

L'algorithme de chiffrement asymétrique le plus connus est le RSA.

- **RSA (Ron Rivest, Adi Shamir et leonard Adelman)**

Le RSA est l'un des algorithmes à clé publique les plus utilisés. Sa sécurité réside dans la difficulté à factoriser le produit de deux grands nombres premiers [9]. Les clés sont générées selon le processus suivant :

- Choisir deux grands nombres premiers p et q
- Calculer n le produit de ces 2 nombres (il est difficile de retrouver p et q à partir de n)
- Calculer le nombre d'Euler de n $\Phi(n) = (p-1)(q-1)$ Choisir un nombre aléatoire $e < \Phi(n)$ et premier avec $\Phi(n)$
- Déterminer le nombre d tel que $e.d \equiv 1 \bmod \Phi(n)$
- Généralement e représente la clé publique et d représente la clé secrète
- Ainsi les quantités publiques sont : n et e les quantités secrètes sont : d et $\Phi(n)$

I.3.2.3 Les avantages et les inconvénients de cryptographies symétrique et asymétrique

Cryptographie	Avantages	Inconvénients
Symétrique	-Adapté au grand flux de données à chiffrer. -Rapidité du système de chiffrement et de déchiffrement du message. -simplicité et facilité de l'implémentation. -Nécessite moins de ressources de calcul.	-Moins sécurisé. - Problème de communication de clés entre émetteur et récepteur. - Toute personne interceptant la clé lors d'un transfert peut ensuite lire ou même modifier ou falsifier toutes les informations cryptées.
Asymétrique	-Très sécurisée à cause de l'utilisation de deux clés distinctes, l'une ne permettant pas de retrouver l'autre. -L'expéditeur et le destinataire n'ont plus besoin de partager des clés secrètes via une voie de transmission sécurisée. -Les communications impliquent uniquement l'utilisation de clés publiques et aucune clé privée n'est transmise ou partagée.	-Le traitement de données est lent et demande beaucoup plus de calculs. -Problèmes de gestion de clés publiques.

TableauI.3Les avantages et les inconvénients de cryptographies symétrique et asymétrique.

I.3.3 Les limites de la cryptographie classique et moderne

Pour répondre aux besoins croissants des utilisateurs, la puissance de calcul ne cesse d'augmenter de manière exceptionnelle, ce qui a mis en danger la sécurité des données. En effet, en 1994 Peter Shor a découvert un algorithme qui permet la factorisation d'un grand nombre premier qui utilise un calcul polynômial [10]. En outre, l'apparition des calculateurs quantiques possédant des calculs géants, a mis en péril les algorithmes classique et moderne. D'où la recherche de nouvelles techniques de cryptage.

Pour ces raisons, une nouvelle solution est apparue. Elle ne se base plus sur l'aspect mathématique, mais sur les principes de la mécanique et de la physique quantique assurant ainsi une clé totalement sûre. Il s'agit de la cryptographie quantique appelée distribution quantique des clés.

I.4 La cryptographie quantique

La cryptographie quantique n'est pas fondée sur la théorie classique de l'électronique (bit), mais sur la physique quantique dont le comportement des photons (les particules élémentaires de lumière) est régi par les lois de la mécanique quantique. Le photon représente un qubit.

La cryptographie quantique n'est pas en soi un nouveau procédé de cryptographie. En effet, elle permet de distribuer une clé de chiffrement secrète entre deux interlocuteurs distants, tout en assurant la sécurité de la transmission. Cette méthode permet de détecter et d'empêcher toute tentative d'espionnage grâce aux lois de la mécanique quantique à savoir le théorème de non-clonage et le principe d'incertitude d'Heisenberg.

I.4.1 Quelques notions de la mécanique quantique

La mécanique quantique est reconnue comme étant la science qui permet de décrire le monde de l'infiniment petit c'est-à-dire qu'elle permet de décrire les systèmes à l'échelle atomique. Elle est apparue au début du 20ème siècle [10] [11]. Dans cette partie nous allons citer quelques notions de base sur la mécanique quantique.

Les différentes représentations utilisées en mécanique quantique pour la description des états d'une particule ou d'un système de particules utilisent les espaces d'Hilbert.

- **Le qubit**

En électronique, un bit est une unité de base de l'information informatique. Elle correspond à une tension ou un courant. Elle ne peut avoir que deux valeurs possibles : 0 ou 1.

En informatique quantique, on parle de photon et chaque photon est considéré comme un qubit (quantum + bit). Il correspond un état quantique qui représente la plus petite unité de stockage d'information quantique.

L'expression du qubit est donnée par :

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \qquad (I.1)$$

Où α et β sont des coefficients complexes, ils représentent les amplitudes de probabilité d'obtenir l'état 1 et l'état 0 respectivement lors d'une mesure de l'état ψ. Ces deux états constituent une base orthogonale de l'espace de Hilbert du système. Ces coefficients satisfont la condition de normalisation suivante :

$$\|\alpha\|^2 + \|\beta\|^2 = 1 \qquad \text{(I.2)}$$

α^2 : représente la probabilité d'avoir le bit 0.

β^2 : représente la probabilité d'avoir le bit 1.

1 Et 0 : représente deux états orthogonaux dans le système quantique.

I.4.2 Polarisation d'un photon

Un photon peut être considéré comme étant un minuscule champ électrique oscillatoire. La direction de l'oscillation définit alors la polarisation du photon.

Lorsque l'on fait passer la lumière à travers un filtre polarisant, les photons seront absorbés ou transmis selon leur polarisation [12] :

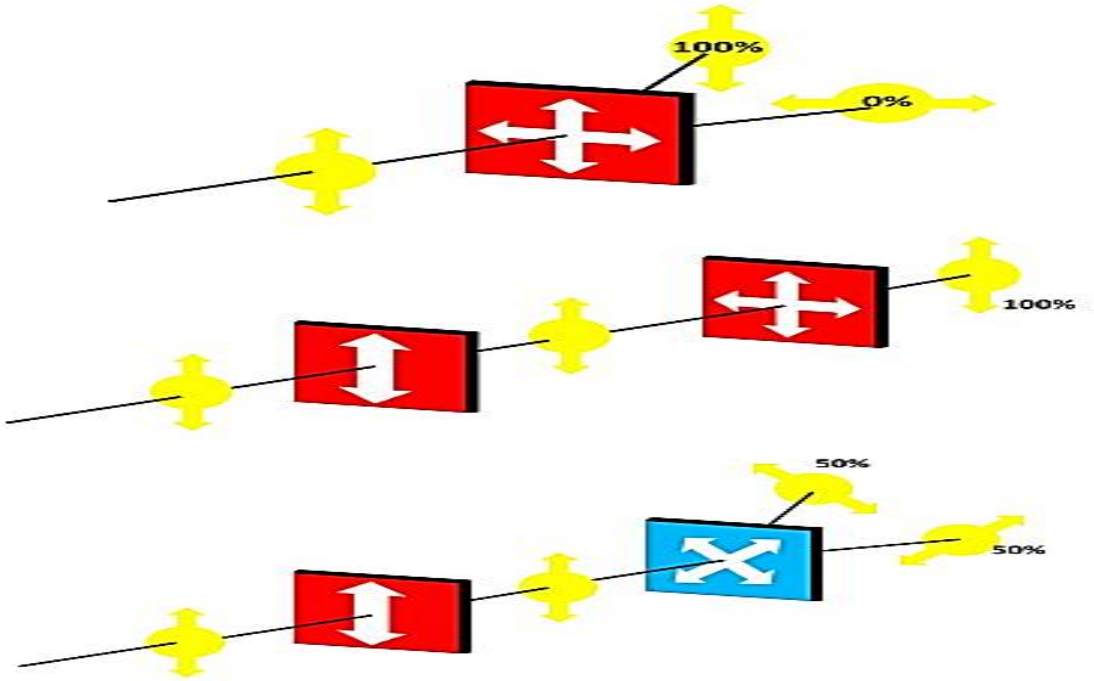


Figure I.6 Polarisation du photon

- Si le photon est polarisé parallèlement à l'angle d'orientation du filtre. Alors la probabilité que ce photon traverse le filtre est égale à 1 (100%), c'est-à-dire qu'il traverse le filtre.

- Si le photon est polarisé perpendiculairement à l'angle d'orientation du filtre, alors la probabilité que ce photon traverse le filtre est égale à 0 (0%), c'est-à-dire qu'il est absorbé.
- Si le photon est polarisé selon une direction intermédiaire, alors ce photon sera transmis avec une probabilité $\cos^2(\alpha)$, ou $\alpha = \gamma - \beta$. Tel que γ est l'angle de polarisation du photon et β est l'angle d'orientation du filtre, α alors est l'angle de polarisation du photon mesuré par rapport à l'angle d'orientation du filtre. Si le photon est transmis, alors sa nouvelle polarisation correspondra à l'angle d'orientation du filtre.

- Pour un système de photons polarisés, on peut par exemple associer le symbole $|0\rangle$ à une polarisation horizontale et $|1\rangle$ à une polarisation verticale.

I.4.3 Quelques lois de la mécanique quantique

Dans cette partie, nous allons présenter quelques lois de la mécanique quantique qui sont la base de la cryptographie quantique.

I.4.3.1 Le principe d'incertitude de Heisenberg

Élaboré en 1927 par Heisenberg (1901-1979) [13], ce principe montre qu'il est impossible d'attribuer à un corpuscule la position ***p*** et la vitesse ***q*** avec précision, car la mesure perturbe système.

I.4.3.2 Théorème de non-clonage

Il est tout à fait facile de réaliser une copie d'un bit classique. En mécanique quantique, il est difficile de réaliser une telle opération aussi simple qu'elle puisse paraître sur un qubit, en effet cloner un état enduit à la perte de son état initial. Le théorème de non-clonage s'énonce alors : il n'est pas possible de produire des copies parfaites d'un état quantique inconnu. En 1982, W. K. Wooters et W.H. Zurek ont démontré qu'il est impossible de cloner un état quantique arbitraire et inconnu [14].

I.5 Conclusion

Nous avons essayé à travers ce chapitre de mettre le point sur quelques généralités de la cryptographie, son objectif et nous avons présenté les différentes classes de la cryptographie : le cas de la cryptographie classique, cryptographie moderne où nous avons cité ces deux types et avons cité en particulier les algorithmes les plus connus, qui sont devenus des standards comme DES, AES, RSA. Et la cryptographie quantique qui est la dernière classe introduite pour assurer la confidentialité des clés. Ensuite nous avons fourni un bref aperçu sur les notions de la mécanique quantique. Où nous avons abordé la polarisation du photon et quelques lois de la mécanique quantique qui sont à la base de la cryptographie quantique, notamment le principe d'incertitude d'Heisenberg et le théorème de non-clonage.

Chapitre II

Implémentation du protocole B92 sur OPTISYSTEM sans et avec espion

II.1 Introduction

Le protocole de distribution quantique de clé (QKD) a été introduit pour la première fois par Bennett en 1992(B92) [15].Il permet à deux personnes séparées de construire une clé secrète qu'ils seront les seuls supposés à la connaitre, par l'envoi de l'un vers l'autre des photons uniques qui proviennent d'une source de lumière cohérente avec une polarisation, le long d'un canal de transmission quantique (fibre optique, espace libre).

Dans ce chapitre, nous allons voir en premier lieu les sources de lumière (photon) utilisées dans la distribution quantique de clé, et plus particulièrement les sources à photons uniques. Ensuite, nous présenterons les protocoles de distribution de clé quantique les plus fonctionnelles dans le domaine de la cryptographie et expliquer chaque protocole ainsi que les fonctionnalités qui ont été utilisées dans chacun d'eux ainsi que l'espionnage dans la cryptographie quantique. Dans la dernière partie nous allons simuler le protocole B92 sans et avec présence d'un espion, en utilisant une source laser à l'aide du logiciel OPTYSYSTEM. Afin d'évaluer la polarisation du photon lors de la transmission via une fibre optique.

II.2 Sources de photon unique

La source de photon unique représente tous dispositif capable d'émettre des impulsions lumineuses contenant un seul photon par impulsion. Dans la distribution quantique de clé, on utilise ces sources pour émettre des photons uniques au lieu de paquets de photons, de cette façon un intrus ne pourra pas simplement détourner les photons qui sont envoyés d'une personne à une autre. Tel que les sources d'impulsions cohérentes atténuées

- **Sources lasers atténués**

Les sources lasers atténués sont les premières sources utilisées dans les protocoles de distribution quantique de clé [10]. Elles sont réalisées en ajoutant un atténuateur optique à la source laser. On aurait donc une source qui émet des impulsions fortement atténuées contenant en moyenne un photon par impulsion, on obtient alors une source cohérente atténué. Dans ce cas, la distribution de photon dans chaque impulsion suit une loi de Poisson, en fonction du nombre de photons (n) et du nombre moyen de photon μ par impulsion [16]

$$\boldsymbol{P(n,\mu)} = \left(\frac{\boldsymbol{\mu^n}}{\boldsymbol{n!}}\right) e^{-\mu} \qquad \text{(II.1)}$$

II.3 Protocole de distribution quantique de clés

Comme pour tous les domaines des communications quantiques, les systèmes QKD exploitent le codage de l'information quantique dans certaines propriétés des signaux photoniques. Les deux parties qui communiquent, échangent un grand nombre de signaux par un canal physique (fibre optique ou espace libre), et des informations supplémentaires envoyées sur un canal classique public mais authentifié. Ils suivent ainsi un protocole qui aboutit à la génération d'une chaîne de qubits qui constitue la clé secrète avec un niveau de sécurité voulu au prix d'une réduction de la taille de chaîne initiale.

II.3.1 Principe de la distribution de clés quantiques

Généralement, on appelle Alice et Bob les deux utilisateurs souhaitant établir une clé secrète commune. L'objectif du protocole est de s'assurer que l'adversaire ou espion appelé Eve ne puisse pas obtenir d'information sur la clé partagée par Alice et Bob [17].

Bien sûr, si on simule ce scénario avec une machine quantique pour chacun, il apparaît qu'il y'a deux canaux entre Bob et Alice :

- **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
- **Canal quantique :** Il s'agit d'un câble de fibre optique permettant la transmission des photons.

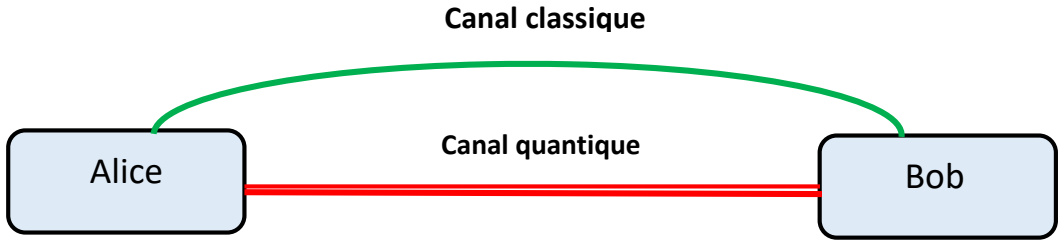


Figure II.1Schéma du principe du protocole quantique.

II.3.2 Etapes d'un protocole de distribution quantique de clés

II.3.2.1 Communication quantique

Alice et Bob échangent des états quantiques à travers le canal quantique et effectuent des mesures sur ces états.

II.3.2.2 Phases tamisage

Alice et Bob annoncent publiquement leurs choix de base. Ils choisissent alors de ne conserver que les bits pour lesquels leurs choix de base coïncident. En moyenne ces chaînes sont donc deux fois plus courtes que les chaînes de départ. La clé obtenue dans cette étape est appelée la clé tamisée [17].

II.3.2.3 Estimation de paramètre (discussion)

Alice et Bob dévoilent publiquement une petite partie (choisie aléatoirement) de leurs résultats de mesures pour estimer le taux d'erreur entre leurs chaînes de bits respectives. Si ce taux d'erreur est trop élevé, ils peuvent choisir d'interrompre le protocole ici. En effet, un taux d'erreur supérieur à 25% peut être le signe de la présence d'un espion sur le canal [17].

II.3.2.4 Correction d'erreur

Alice et Bob modifient les informations publiques sur une chaine classique authentifiée et se mettent d'accord sur une chaine de bits commune. Cette étape augmente la quantité d'information de l'écoute clandestine. Alice et Bob peuvent abandonner le protocole à ce stade, si la quantité totale d'informations de l'écoute clandestine après toutes les étapes précédentes est supérieure à la taille de la chaine de bits commune [17].

II.4 Exemple de protocoles de distribution quantique de clés

II.4.1 Le protocole BB84

Le protocole de distribution quantique de clef, élaboré en 1984 par Charles Bennett et Gilles Brassard [18], permet à deux correspondants d'échanger une clef de chiffrement. De nombreuses réalisations expérimentales utilisant des variables physiques à valeurs discrètes, codées sur des photons uniques, reposent sur l'utilisation de ce protocole.

Le but du protocole est de permettre à deux utilisateurs, Alice et Bob, d'échanger une clé aléatoire et secrète pouvant être utilisée ensuite pour chiffrer un message. Le codage est effectué sur quatre états correspondant aux axes de deux bases perpendiculaires appelées base rectiligne et base diagonale, tel qu'il est illustré sur le tableau II.1.

Mode de polarisation	Symbole	Etat de polarisation	Qubit
Base rectiligne	+	Horizontale0° →	Qubit 0
		Verticale90° ↑	Qubit 1
Base diagonale	×	Diagonale 45° ↗	Qubit 0
		Anti-diagonale –45° ↖	Qubit 1

Tableau II.1 Etat de polarisation associée à chaque qubit

II.4.2 Le protocole B92

En 1992, selon Bennett, quatre états sont trop pour une cryptographie quantique et seulement deux états non-orthogonaux sont suffisants.

Le protocole Bennett 1992 ou B92 [15] est un protocole de distribution quantique de clés fondamentalement la plus simple version du protocole BB84. L'idée principale de ce protocole est d'utiliser deux bases non orthogonaux au lieu de quatre comme le montre la figure II.2 Alice prépare une séquence binaire de système quantique représentant 0 et 1. Comme Bob ne peut pas deviner à chaque fois la base utilisée, il effectuera par des mesures des tests lui permettant d'obtenir la bonne réponse, puis Bob déclare publiquement à Alice quelle mesure lui a fourni un résultat positif.

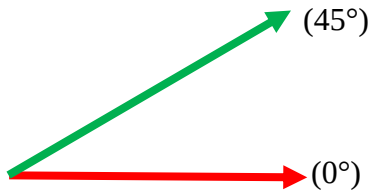


Figure II.2 Etats de polarisation du protocole B92.

Plus formellement, soit — 0° (horizontal) et / 45° (diagonal) les deux polarisations utilisées par Alice représentent respectivement les valeurs binaire 0 et 1. Celles de Bob sont

| 90° (vertical) et \ -45° (anti-diagonal) traduisant respectivement les valeurs 1 et 0.

II.4.2.1 Déroulement du protocole B92

Le principe du protocole B92 [15] est identique à celui du protocole BB84. Il se déroule en plusieurs étapes, et permet à deux participants d'établir une clé secrète.

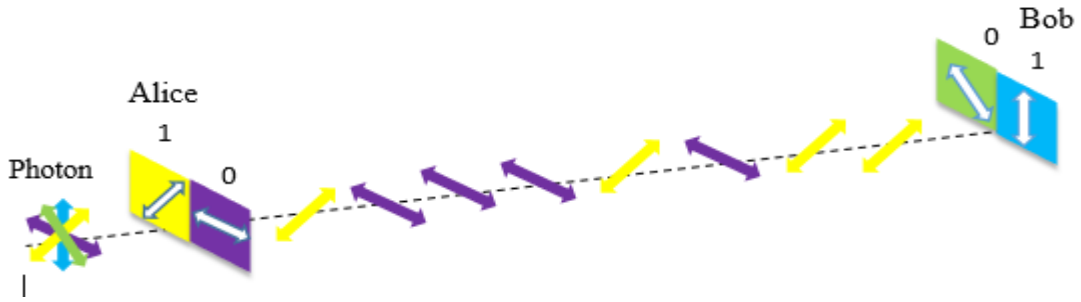


Figure II.3 Principe du protocole B92.

- Alice choisit les filtres selon le qubit qu'elle veut envoyer. Elle effectue de même pour tous les qubits. Elle garde en mémoire tous les choix qu'elle a faits.
- Bob reçoit chaque qubit. Pour en effectuant une mesure, il choisit également un filtre au hasard pour chaque qubit avec une probabilité de ½ de choisir le bon filtre qu'Alice. Bob garde également en mémoire les choix qu'il fait, ainsi que les valeurs des mesures obtenues.
- Alice et Bob annoncent sur le canal classique les choix de filtres qui ont été faits. Puis comparent leurs résultats et ne gardent alors que les valeurs des qubits pour lesquels leurs choix ont coïncidés, et rejettent les autres.
- Alice et Bob appliquent des algorithmes sur la clé obtenue de manière à détecter d'éventuelles erreurs, et à amoindrir l'information volée par un éventuel tiers Ève.

II.4.2.2 Actions d'Eve (espionnage)

Parmi les stratégies qu'un espion peut suivre pour tenter d'intercepter la clé nous avons la stratégie d'intercepter-renvoyer.

Afin d'illustrer cette tentative d'espionnage sur le protocole B92 [15], nous allons émettre l'hypothèse que Eve écoute le canal quantique entre Alice et Bob pour intercepter la clé.

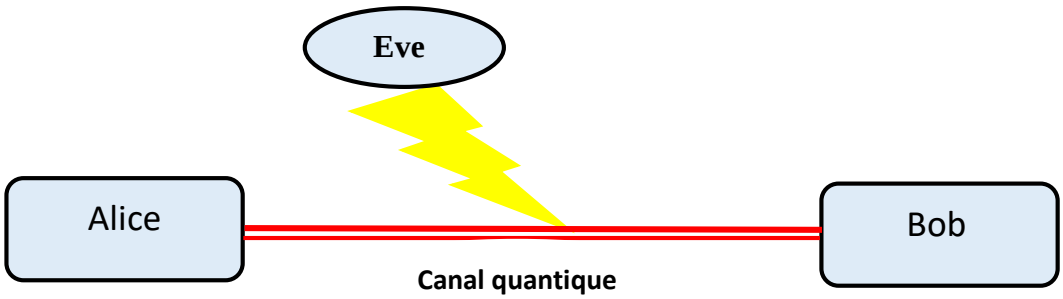


Figure II.4 Communication en présence d'un espion.

- L'émission des photons par Alice ne change pas, elle reste identique à une communication simple, car Alice ne sait pas qu'il y a un espion sur le canal quantique.

- Cette fois-ci Eve (l'espion) va utiliser des filtres polarisants et faire comme Bob dans une communication simple afin de mesurer et comprendre les qubits envoyés par Alice.
- Pour ne pas être repérée, Eve essayera de renvoyer le même photon qu'Alice dans le canal quantique en fonction du résultat trouvé.
- Comme pour l'échange simple, Bob va utiliser les filtres polarisants afin de trouver la clé envoyée par Alice, mais cette fois-ci Bob a une chance sur deux pour utiliser un mauvais filtre et tomber sur un résultat erroné dû à l'envoi du photon par Eve, ce qui ne peut pas arriver s'il n'y a pas d'espion sur le canal quantique.
- Alice et Bob vont ensuite réaliser la phase de tamisage à l'aide du canal classique pour avoir la clé finale reconstituée.
- Afin de vérifier qu'ils ne se sont pas faits espionnés et interceptés, Bob et Alice vont réaliser la phase «Estimation de paramètre» de leur clé commune. où parmi tous les qubits qu'ils sont censés avoir en commun (hors qubits sans sens qui sont éliminés), ils vont choisir d'en dévoiler et les comparer publiquement sur le canal de communication. Si sur les qubits comparés, il y'a des qubits différents, la clé n'est plus identique, ils ont une preuve qu'ils ont été écoutés. Ils vont abandonner et ne pas utiliser cette clé.

II.5 Implémentation du protocole B92 sur OPTISYSTEM

Dans ce qui suit, nous proposons une modélisation et une simulation du protocole B92 sur le simulateur OPTISYSTEM.

II.5.1 Présentation du logiciel

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

Dans notre travail, nous avons opté pour un logiciel d'OPTISYSTEM 7.0, qui est un simulateur basé sur la modélisation réaliste des systèmes de communication par fibre optique. Il est conçu pour la conception, le test et l'optimisation, pratiquement de tous types de liaison optique. Il dispose d'un environnement de simulation proche de la réalité. Ses capacités peuvent être facilement étendues grâce à l'ajout de composants utilisateurs et d'interfaces transparentes à une gamme d'outils largement utilisés.

II.5.2 Simulation

Afin de simuler le protocole B92. Nous utilisons une source fortement atténuée et cela en utilisant deux diodes laser ayant une longueur d'onde de 1550 nm, d'une atténuation plus faible avec une puissance de 5 dbm. Chacune est reliée à un atténuateur optique réglé à 0.1 dB, qui permet de créer un photon unique par impulsion. Par la suite, chaque photon dont sa polarisation est orienté à l'aide d'un polariseur (0 ˚, 45˚). Ensuite l'un des états sera choisi aléatoirement par un sélectionneur et l'envoie sur la fibre optique de 20 km. A la réception, nous utiliserons un analyseur de polarisation pour visualiser l'état du photon reçu sur l'une des deux bases choisies aléatoirement.

Pour la réalisation de ce travail, nous l'avons devisé en deux parties sans et avec espionnage afin de bien comprendre le choix de base et les états de polarisation.

Nous présenterons ci-dessous les différents composants présents et nécessaires pour notre simulation. Ces composants sont choisis en fonction des objectifs de simulation.

- **Source laser continue (CW)**

Une telle diode génère un signal optique à onde continue (CW).Son modèle de simulation est représenté dans la figure II.5.

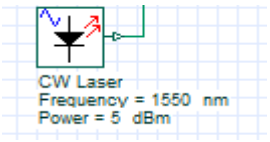


Figure II.5 Modèle de simulation de CW Laser.

- **Atténuateur optique**

L'atténuateur optique est également appelé l'atténuateur à fibre optique qui est utilisé pour réduire le niveau de puissance du signal optique. Son modèle de simulation est représenté dans la figureII.6.

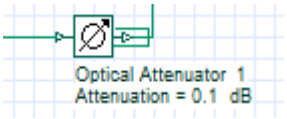


Figure II.6 Modèle de simulation d'un atténuateur optique.

- **Le polariseur linéaire**

Le polariseur linéaire conçut pour polariser linéairement la lumière entrante selon un angle**.** Son modèle de simulation est représenté dans la figure II.7.

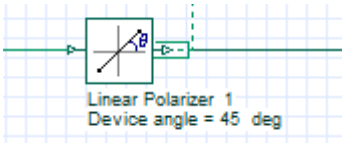


Figure II.7 Modèle de simulation du polariseur linéaire.

- **Le select**

Le select est un composant de sélection aléatoire, l'un des signaux entrant dans les ports d'entrée sera envoyé au port de sortie. Son modèle de simulation est représenté dans la figure II.8.

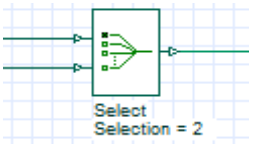


Figure II.8 Modèle de simulation d'un select.

- **La fibre optique**

Pour la transmission, Nous utilisons la fibre optique. Son modèle de simulation est représenté dans la figure II.9

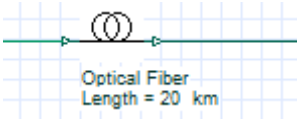


Figure II.9 Modèle de simulation d'une fibre optique.

- **Analyseur de polarisation**

Analyseur de polarisation permet de calculer et d'afficher différentes propriétés de la polarisation du signal. Son modèle de simulation est représenté dans la figure II.10.

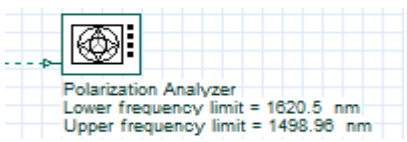


Figure II.10 Modèle de simulation d'un analyseur de polarisation.

Les paramètres de Stokes affichent quatre valeurs dérivant l'état de polarisation du photon où chaque paramètre correspond à une différence de puissance [19] :

- S0 représente la puissance totale transportée.
- S1 est la différence de puissance entre les polarisations verticale et horizontale.
- S2 représente la différence de puissance entre la polarisation linéaire orientée à +45˚et -45˚ de la polarisation verticale.
- S3 représente la différence de puissance entre la polarisation circulaire gauche et droite.

II.5.2.1 Simulation du protocole B92 sans espionnage

- **A un seule état**

Afin de comprendre le principe du protocole en question nous allons entamer la simulation pour un seul état. Nous avons choisi un canal avec une polarisation de 0° comme est présenté dans la figure II.11.

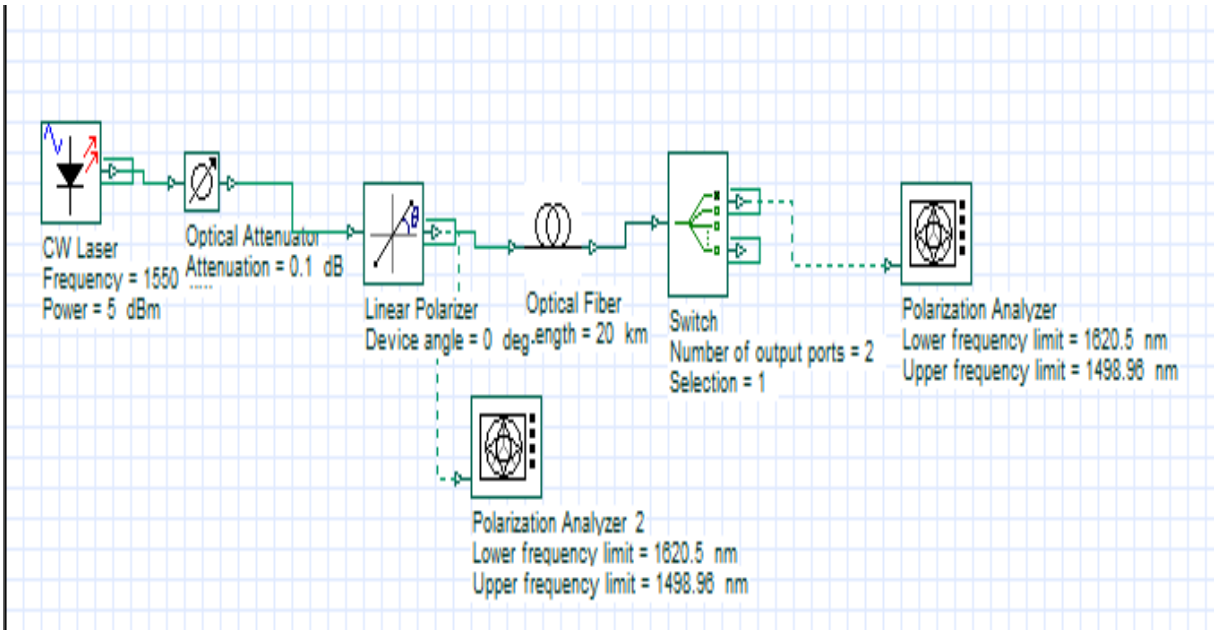


Figure II.11 Simulation du B92 sur un seul canal.

Dans cette simulation, nous avons obtenu les paramètres de Stockes suivants S1= 1, S2= 0, S3=0, et qui caractérisent l'angle 0°.Comme le montre la figure II.12.

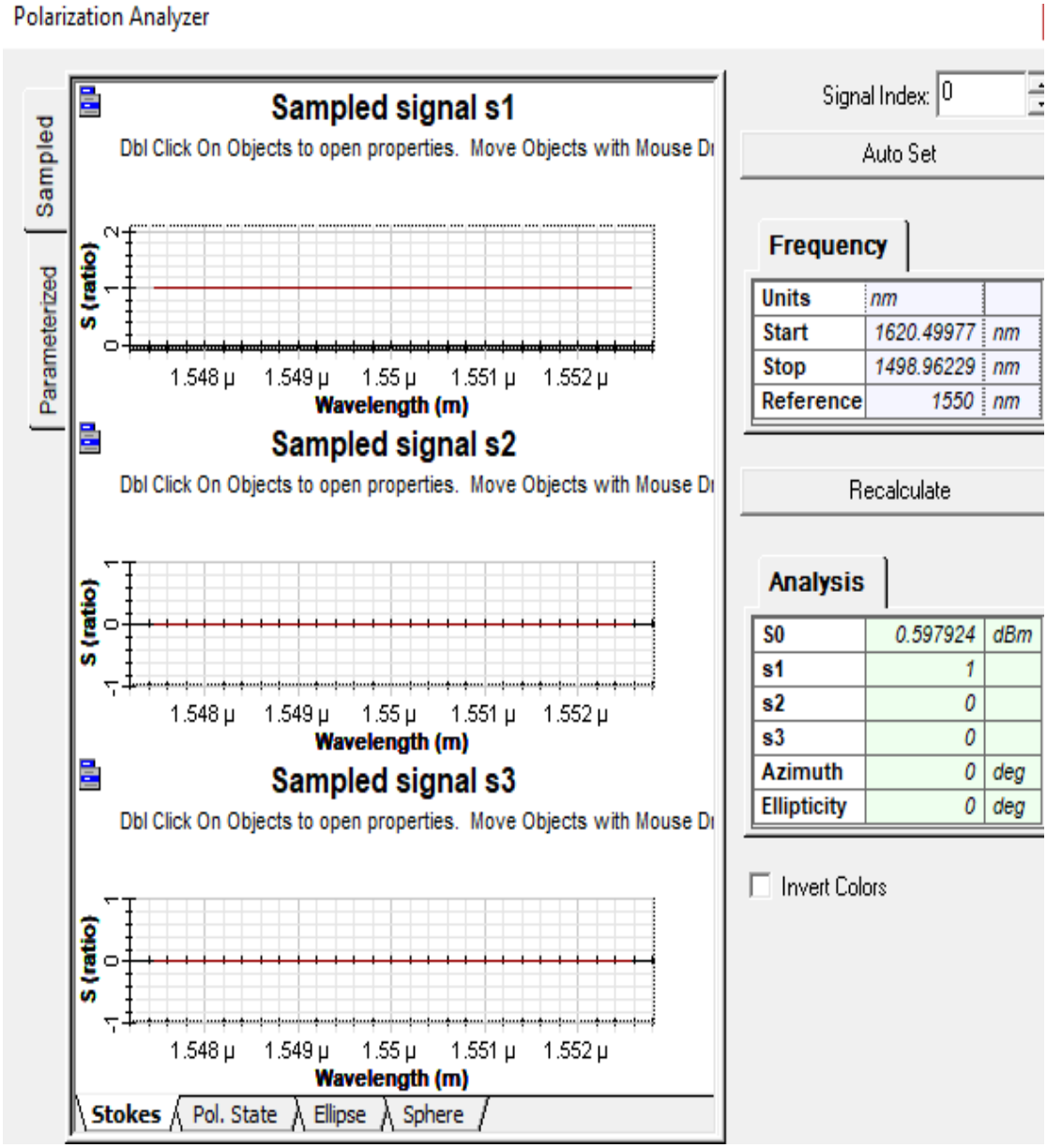
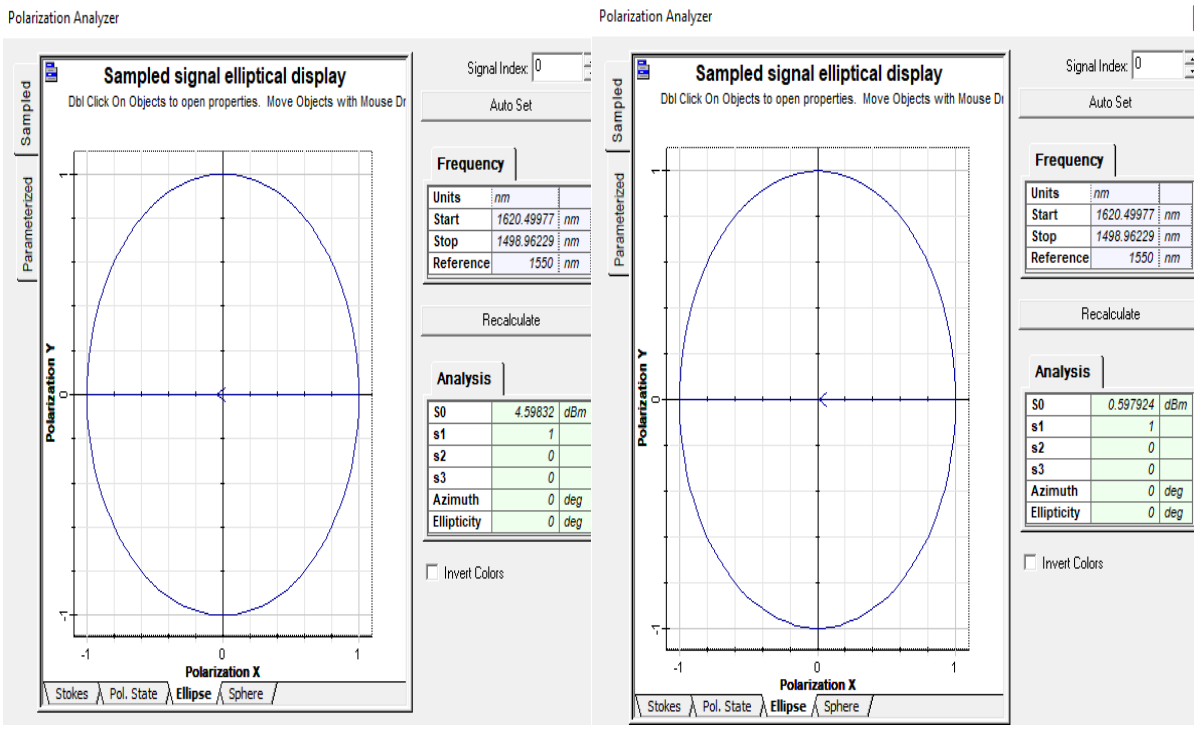


Figure II.12 Les résultats des Paramètres de Stockes obtenus.

En comparant les formes des ellipses au niveau de l'émetteur et du récepteur tel qu'il est représenté dans la figure II.13.a et II.13.b respectivement, nous constatons une similitude des différentes polarisations, ce qui montre la conservation de la polarisation lors de la transmission des qubits.



(a) (b)

Figure II.13 Résultat des ellipses a) l'émission, b) à la réception.

- **A deux états**

Dans cette partie, nous allons simuler le protocole B92 à 2 états de polarisation (0°,45°) tel qu'il est représenté sur la figure II.14.Du côté du récepteur nous rajoutons un sélectionneur d'états « select », le récepteur choisira aléatoirement l'un des polariseurs. Ici, nous avons utilisé « optical null» comme différenciation du polariseur. Le zéro optique correspond à une mauvaise polarisation [20].Le sélect est relié à un analyseur de polarisation, sur lequel le résultat s'affichera.

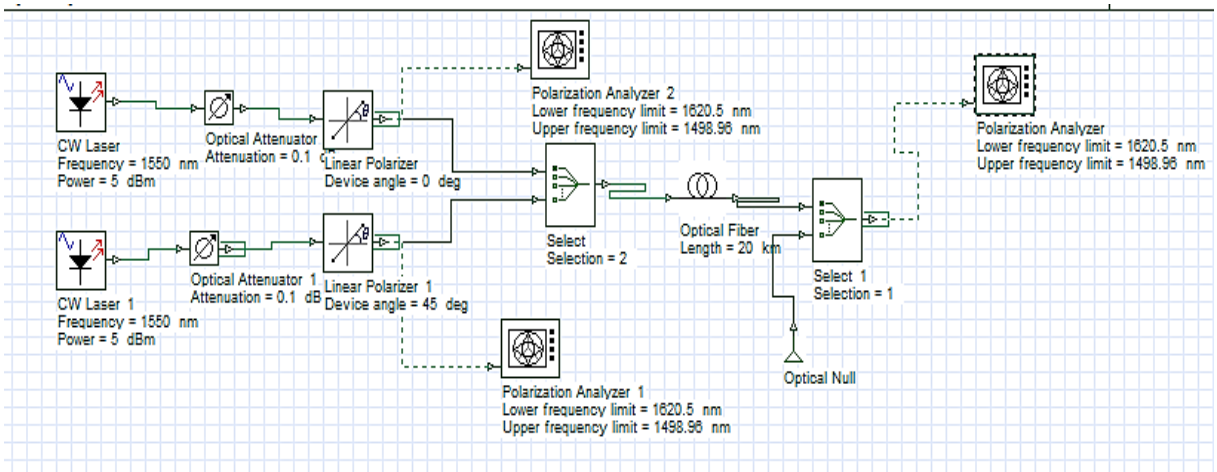


Figure II.14 Simulation du protocole B92.

A partir de l'analyseur de polarisation, nous avons obtenu les paramètres de Stokes suivants S1= 0, S2= 1, S3=0, et qui caractérisent l'angle 45°, correspondant ainsi au qubit 1 tel qu'indiqué sur la figure II.15.

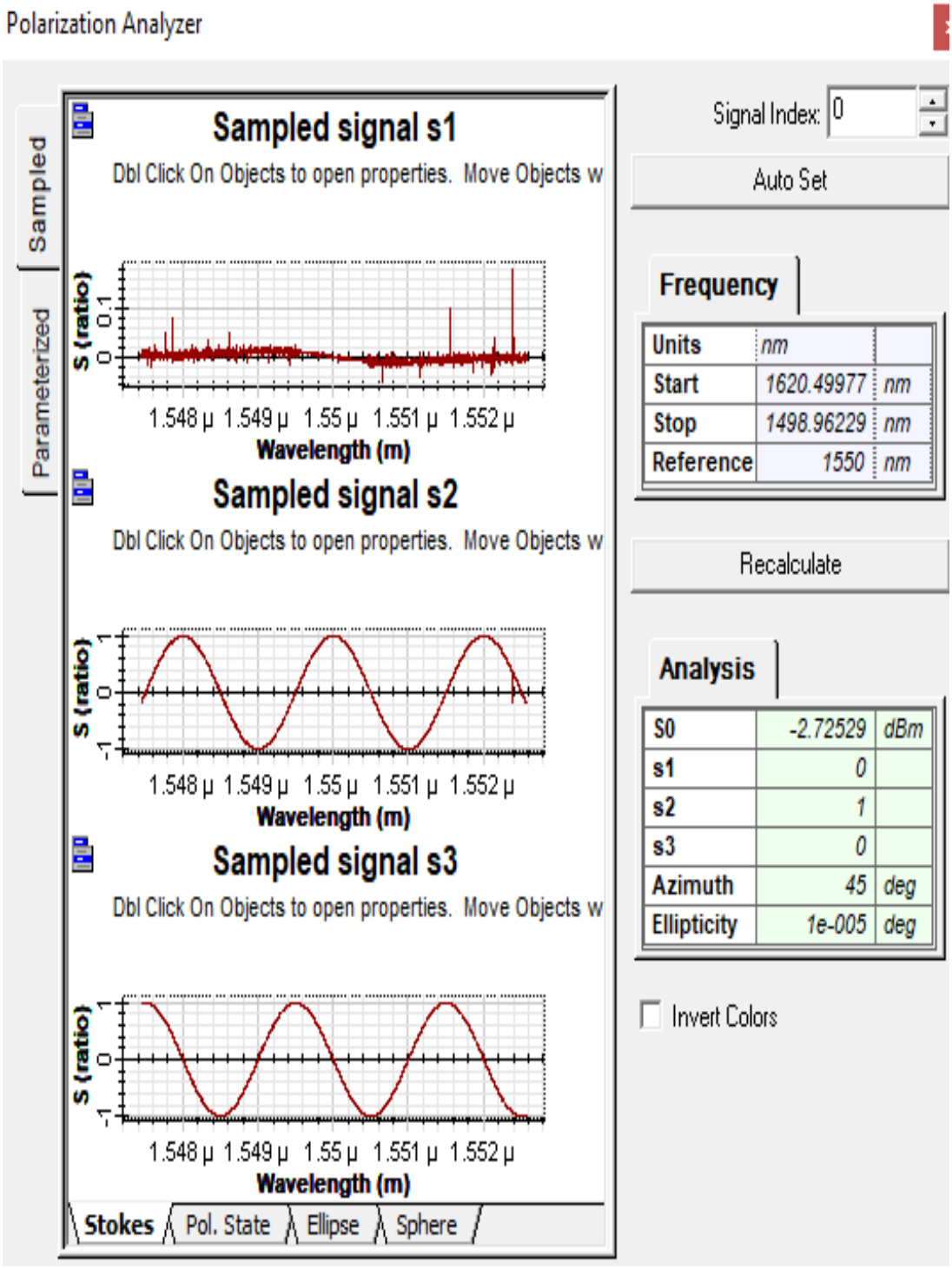


Figure II.15 Paramètres de Stockes obtenus.

II.5.2.2 Simulation du protocole B92 en présence d'un espion

Dans cette partie, nous allons simuler le protocole B92 en présence d'un espion (Eve).En supposant qu'Eve n'a absolument aucune limite technologique, c'est-à-dire qu'elle peut faire tout ce que la physique quantique ne fait pas interdire.

Dans notre simulation illustrée sur la figure II.16, nous avons utilisé un simple modèle de démonstration des attaques. Pour notre expérience, nous généralisons que L'attaque d'Eve est principalement basée sur la stratégie d'attaque Intercept-Resend [21]. Eve est connectée entre Alice et Bob, elle peut effectuer diverses actions afin d'obtenir la clé. Eve peut intercepter les qubits entrants et les mesurer avec les polariseurs rectilignes, déphasages ou rotateurs de photons. Elle peut envoyer un nouveau qubit, ou bien envoyer le qubit d'Alice à Bob [22].

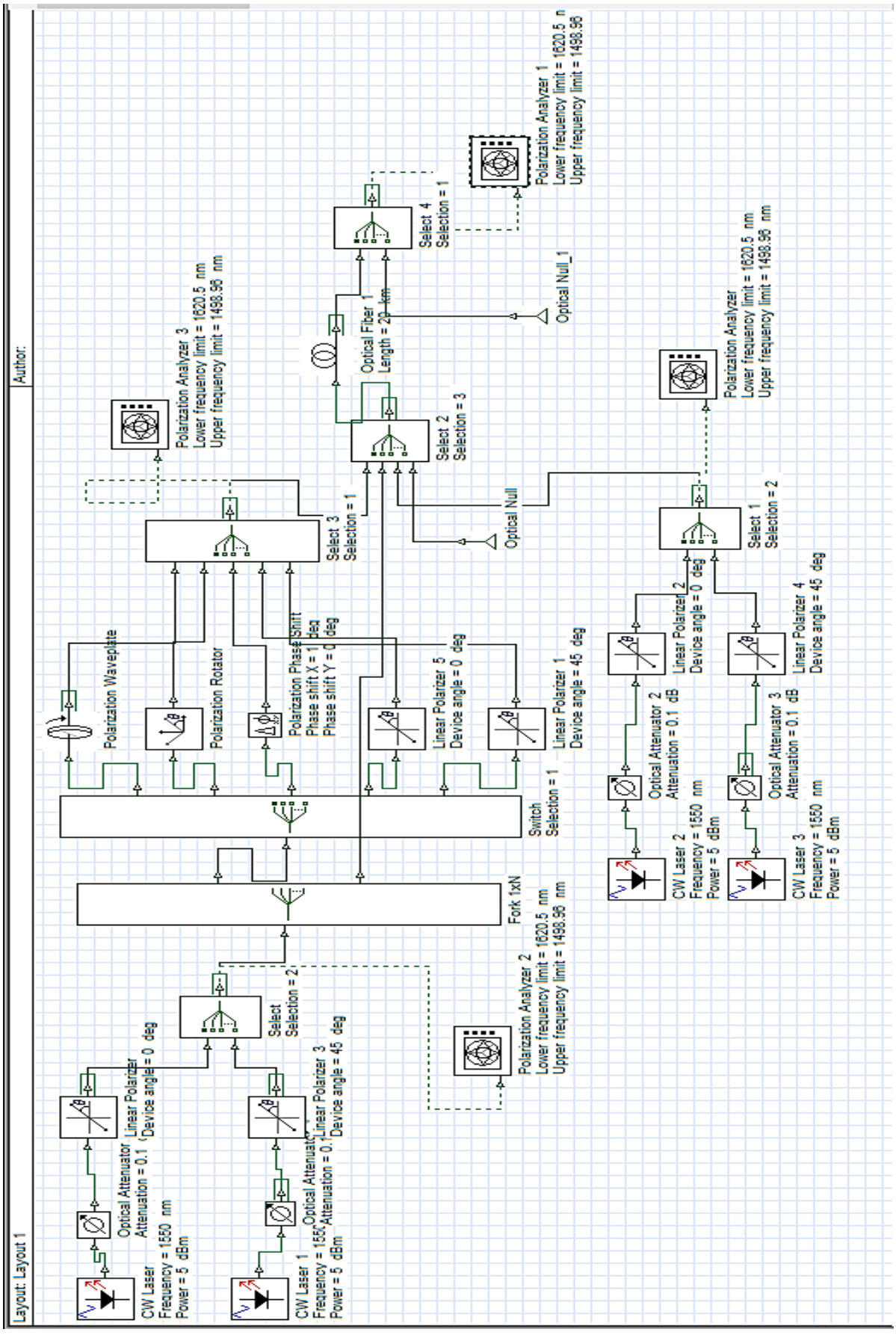


Figure II.16 Simulation du protocole B92 en présence d'Eve.

➢ **Analyse des résultats**

Nous remarquons que l'analyseur de polarisation au niveau du récepteur a choisis aléatoirement la polarisation horizontal (qubit 0) avec les paramètres de Stockes suivants : S1=1, S2=0, ET S3=0 comme c'est représenté dans la figure II.17.

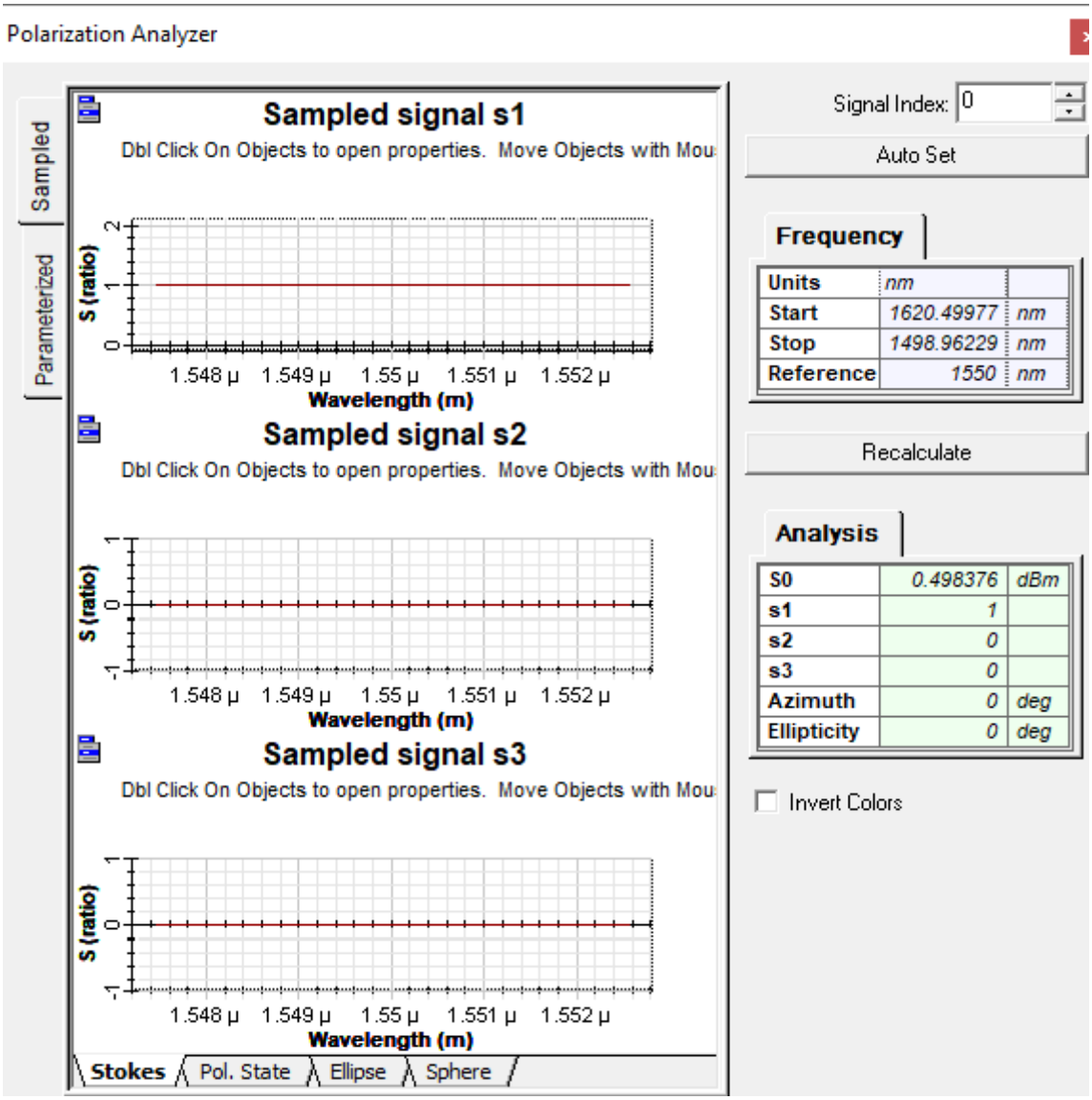


Figure II.17 Les résultats des Paramètres de Stockes obtenus.

II.5.2.3 Exemple d'envoi d'une clé

Dans cette simulation, nous donnons un exemple d'envoi de la séquence 101100111 entre Alice et Bob en absence et en présence d'un espion.

➢ **En absence d'un espion**

La configuration d'un tel système est représentée dans le tableau II.1 suivant :

Alice émet les photons :	**1** ↗	**0** →	**1** ↗	**0** →	**0** →	**1** ↗	**1** ↗	**1** ↗
Bob choisi les filtres :	↑	↖	↖	↖	↑	↑	↖	↑
Bob comprend la valeur :	1	0	rien	0	rien	1	rien	1
Clé finale :	1	0	-	0	-	1	-	1

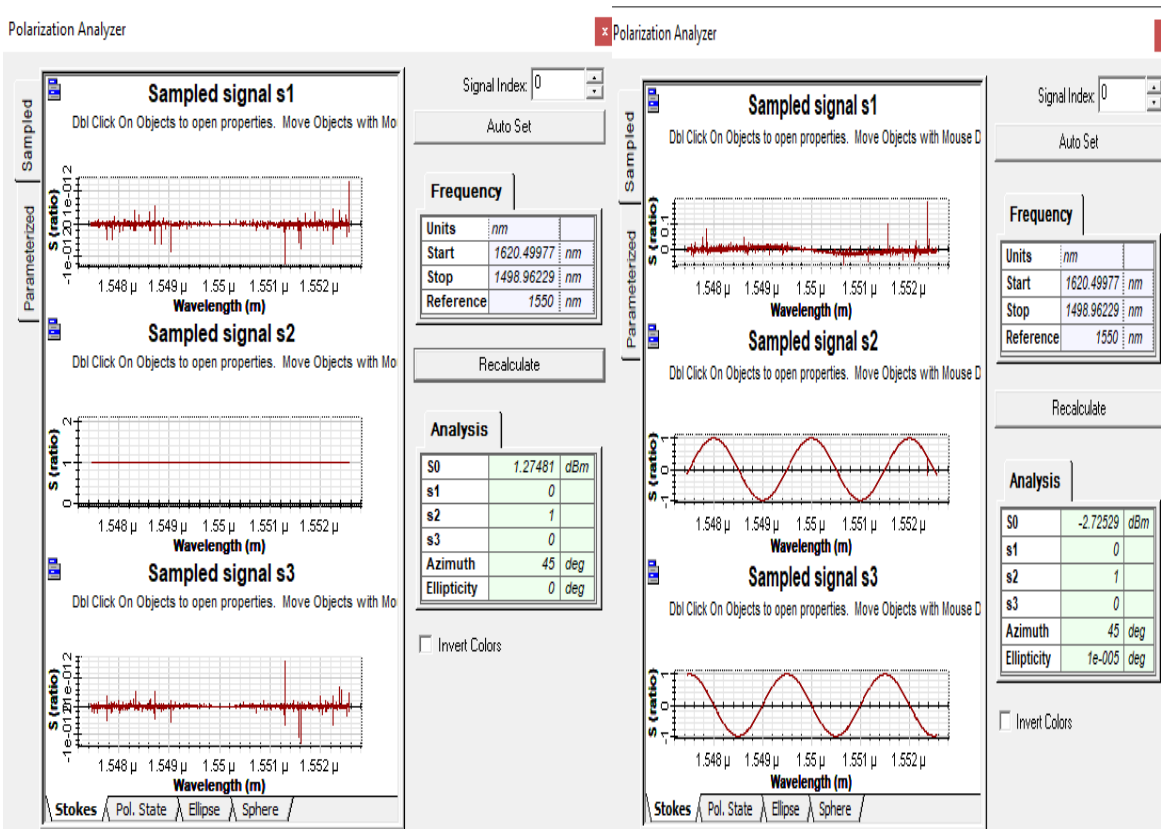
Tableau II.2 Exemple d'envoi d'une clé en absence d'un espion.

La clé résultante est : 10011

- **Analyse des résultats**

Comme exemple nous nous allons intéresser au premier qubit de la séquence

Alice envoie un qubit 1 polarisé avec l'angle 45°à Bob, ce dernier reçoit ce photon.



(a) (b)

Figure II.18 Résultats des analyseurs a) envoi d'Alice b) réception de Bob.

✓ **Commentaire**

Nous remarquons que l'analyseur de polarisation au niveau Bob a choisi aléatoirement la polarisation diagonale (qubit 1) avec les paramètres de Stockes suivants : S1=1, S2=0 et S3=0 envoyé par Alice

➢ **En présence d'un espion**

La même séquence est envoyée,

Alice émet les photons :	**1** 	**0** 	**1** 	**0** 	**0** 	**1** 	**1** 	**1** 
Eve choisi les filtres :								
Eve comprend :	rien	0	1	0	rien	1	1	rien
Eve envoi à bob :	-	0	0	1 	-	0	0	-
Bob choisi les filtres :								
Bob comprend la valeur :	1	0	rien	1	rien	rien	0	1
Clé finale	1	0	-	1	-	-	0	1

Tableau II.3 Exemple d'envoi d'une clé en présence d'un espion.

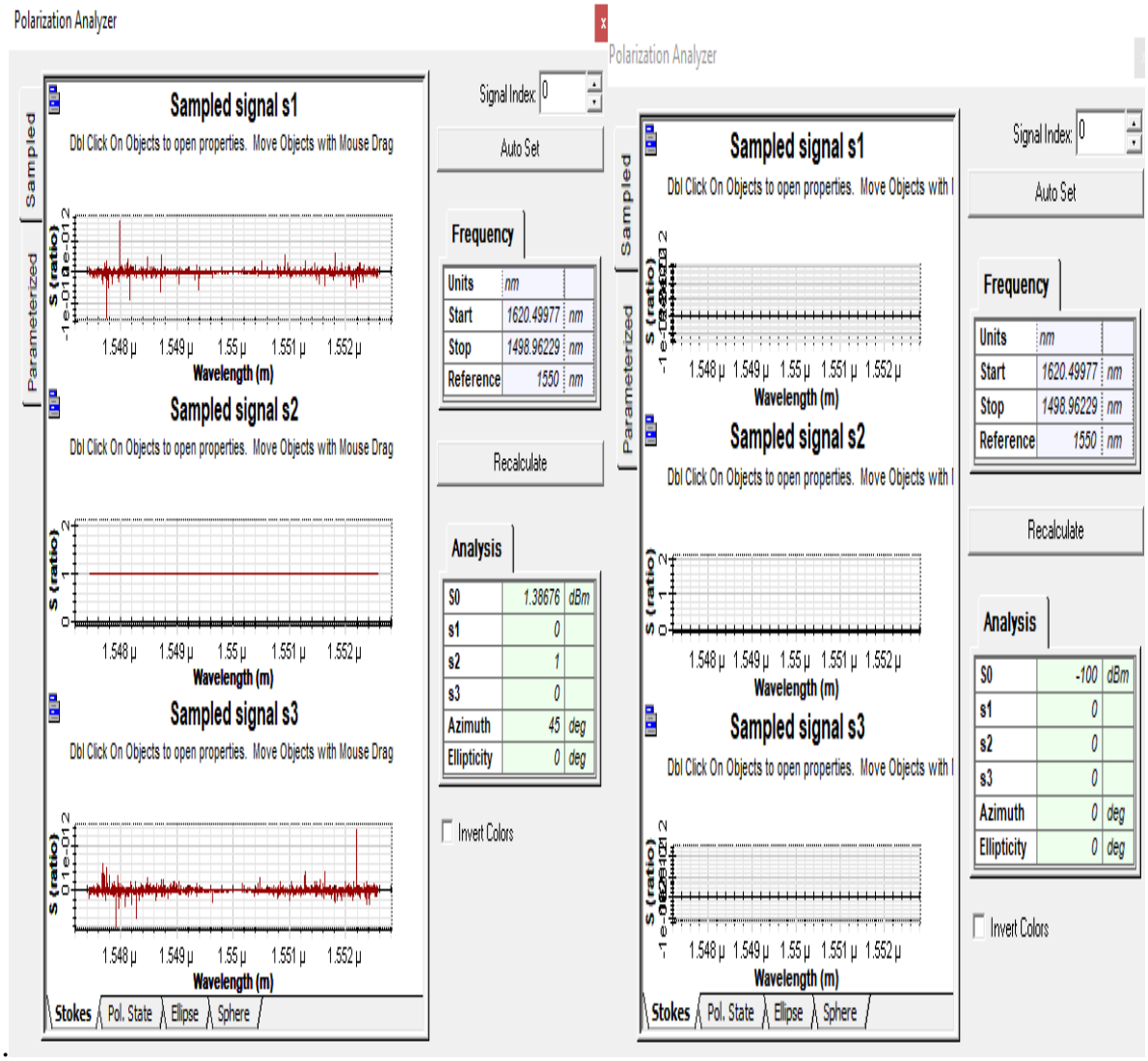
La clé résultante est 10101

➢ **Analyse des résultats**

Nous allons nous intéresser aux quatre premiers qubits de la séquence

1er qubit :

Alice envoie un qubit 1 polarisé avec l'angle 45°, Eve n'intercepte pas le photon et Bob reçoit le photon d'Alice.



(a) (b)

Figure II.19 Résultats des analyseurs a) envoi d'Alice b) réception d'Eve.

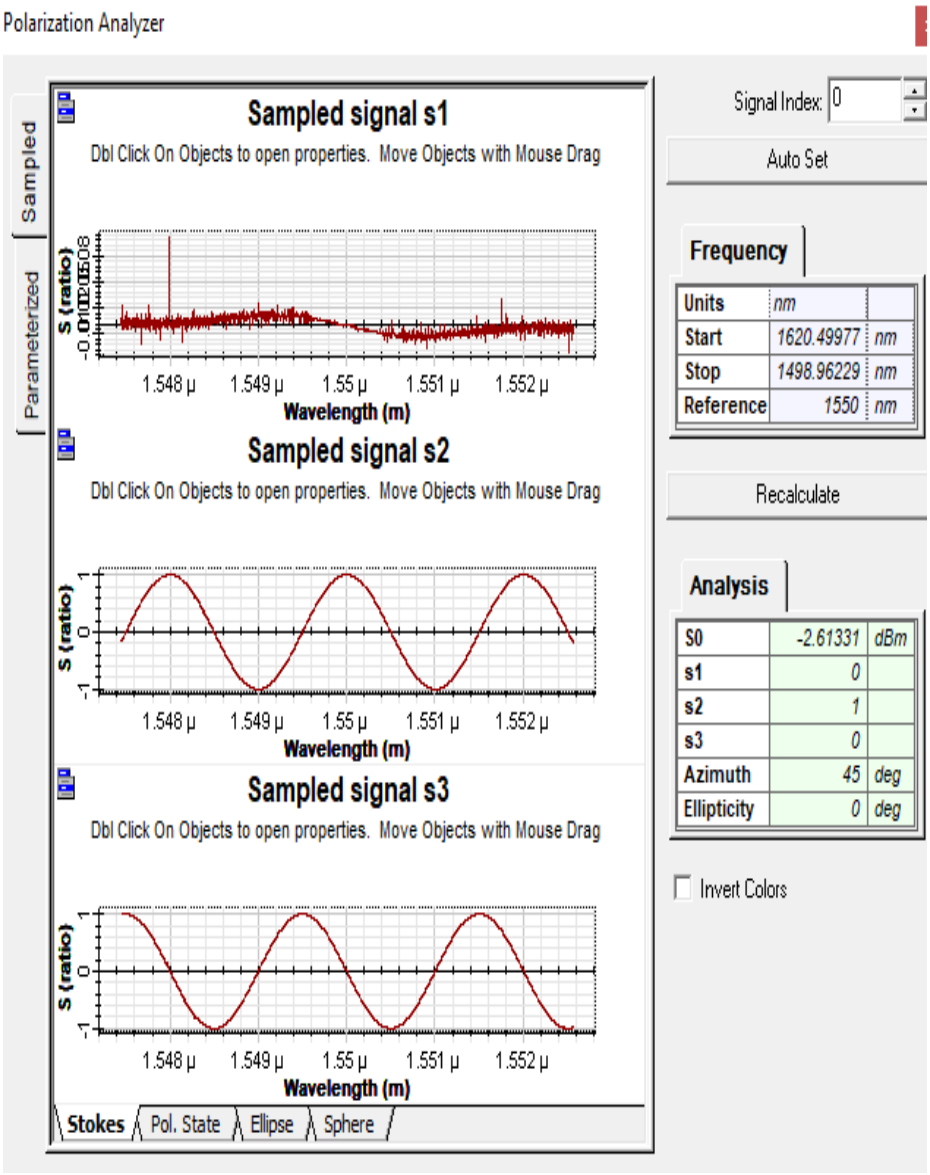
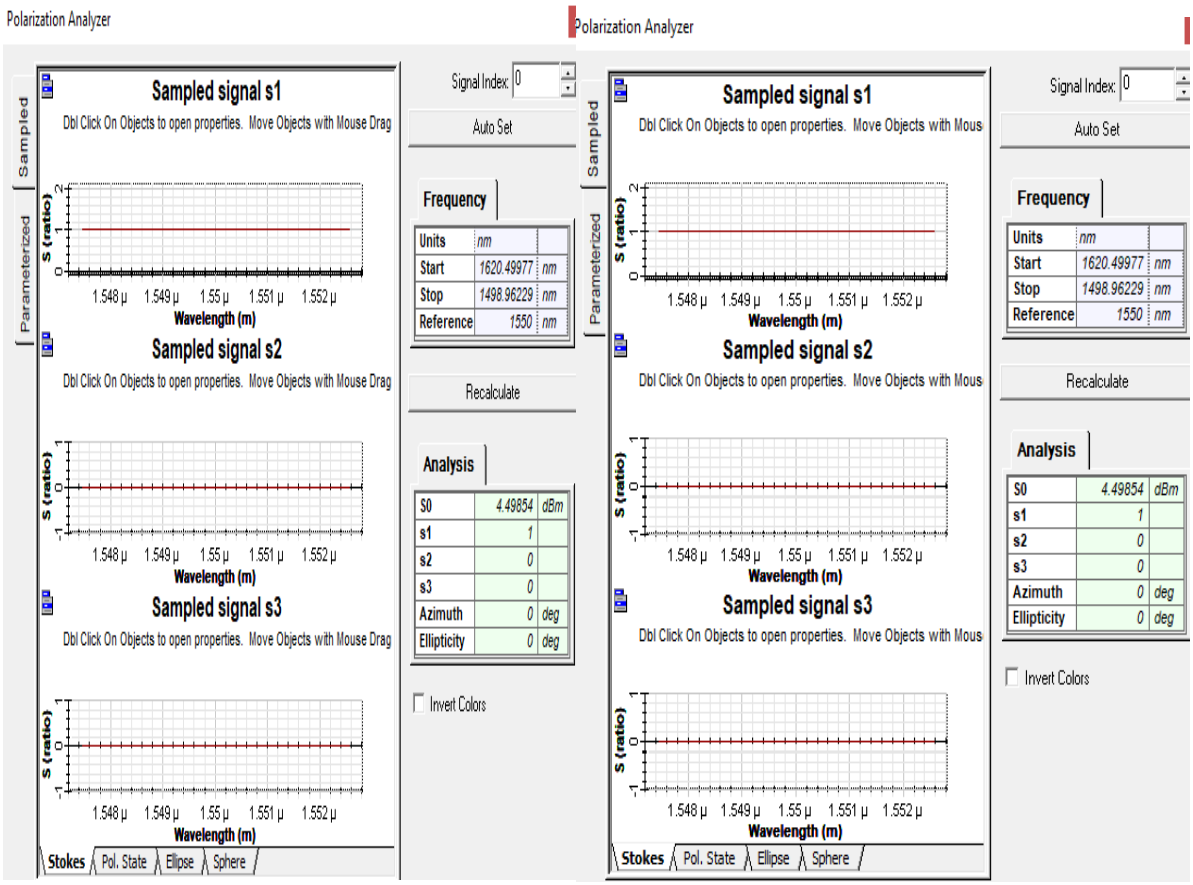


Figure II.20 Les résultats des paramètres de Stockes obtenus par Bob.

2éme qubit :

Alice envoie un qubit 0 polarisé avec l'angle 0°, Eve intercepte le photon polarisé à 0° et envoie un photon polarisé avec l'angle 0° à Bob.



(a) (b)

Figure II.21 Résultats des analyseurs a) envoi d'Alice b) réception d'Eve.

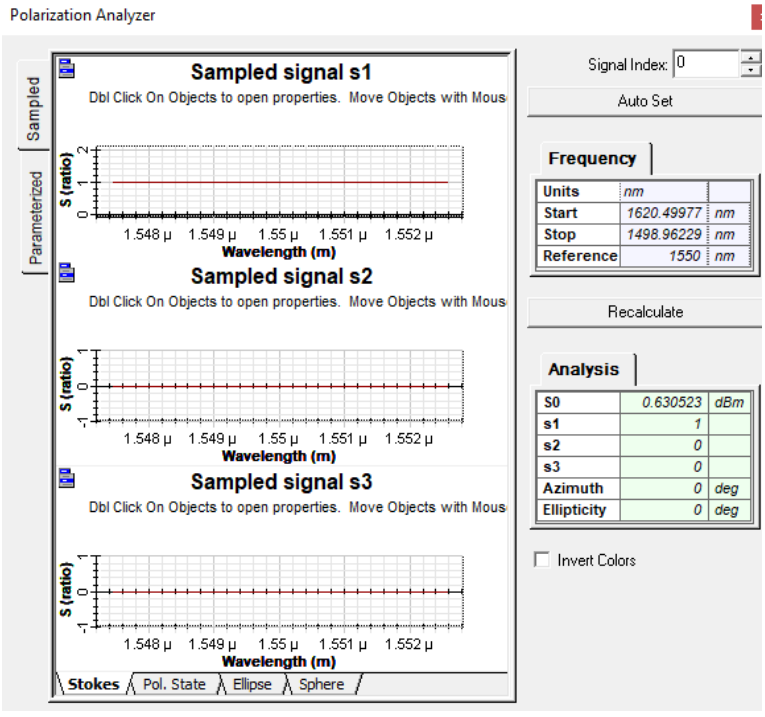
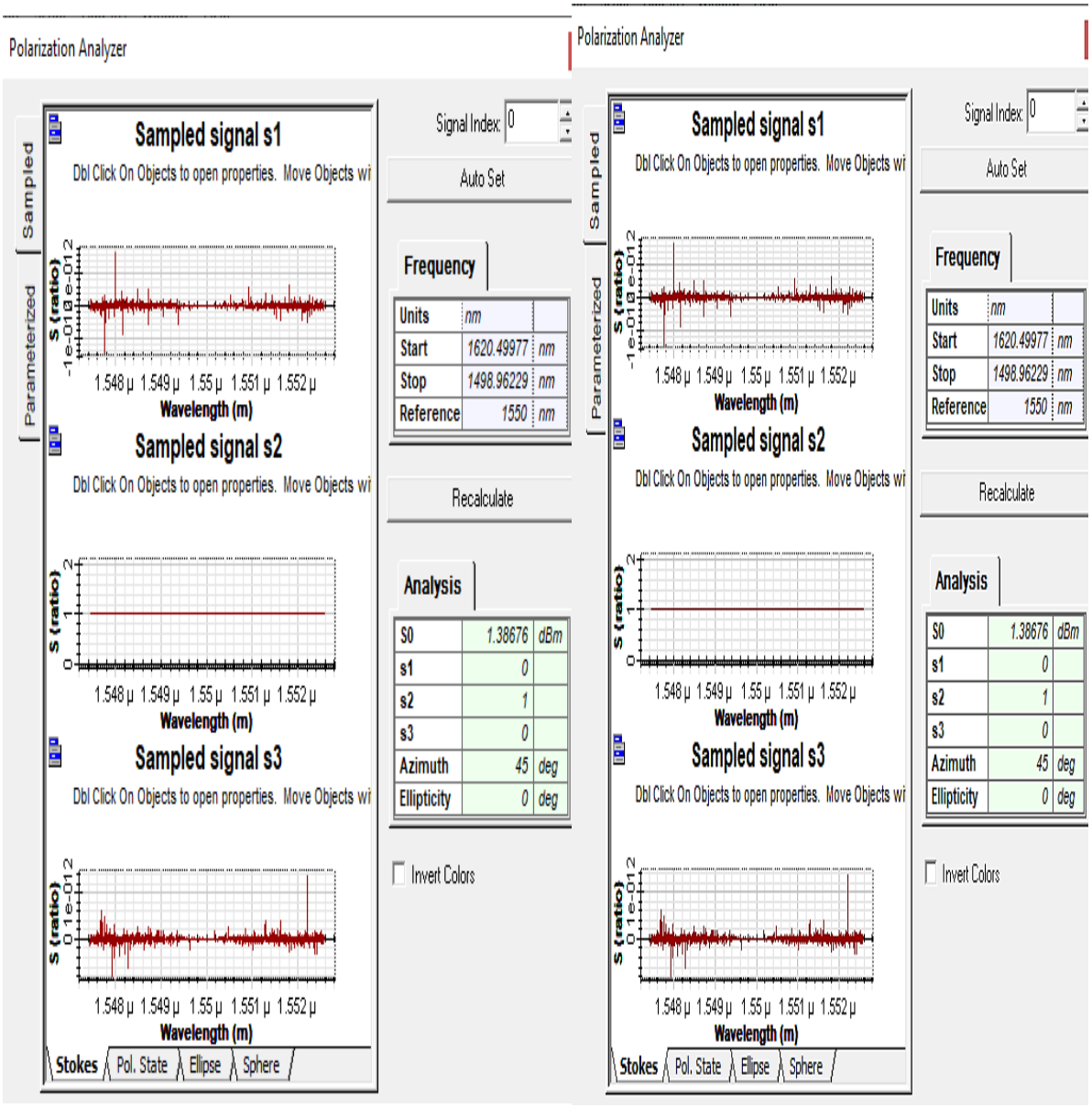


Figure II.22 Les résultats des paramètres de Stockes obtenus par Bob

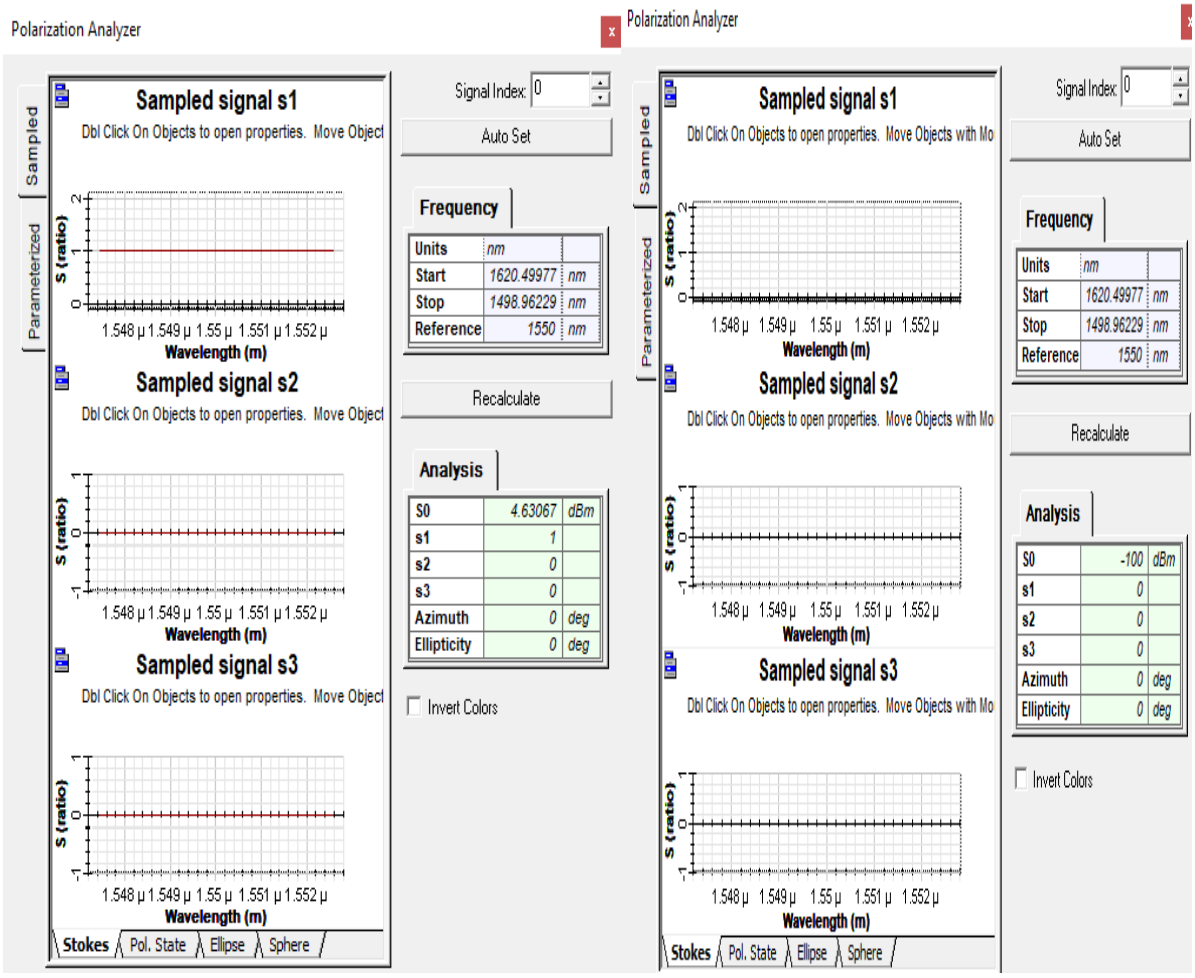
3éme qubit :

Alice envoie un qubit 1 polarisé avec l'angle 45°, Eve intercepte ce photon et envoie un nouveau photon polarisé avec l'angle 0° à Bob, ce dernier n'intercepte pas le photon.



(a) (b)

Figure II.23 Résultats des analyseurs a) envoi d'Alice b) réception d'Eve

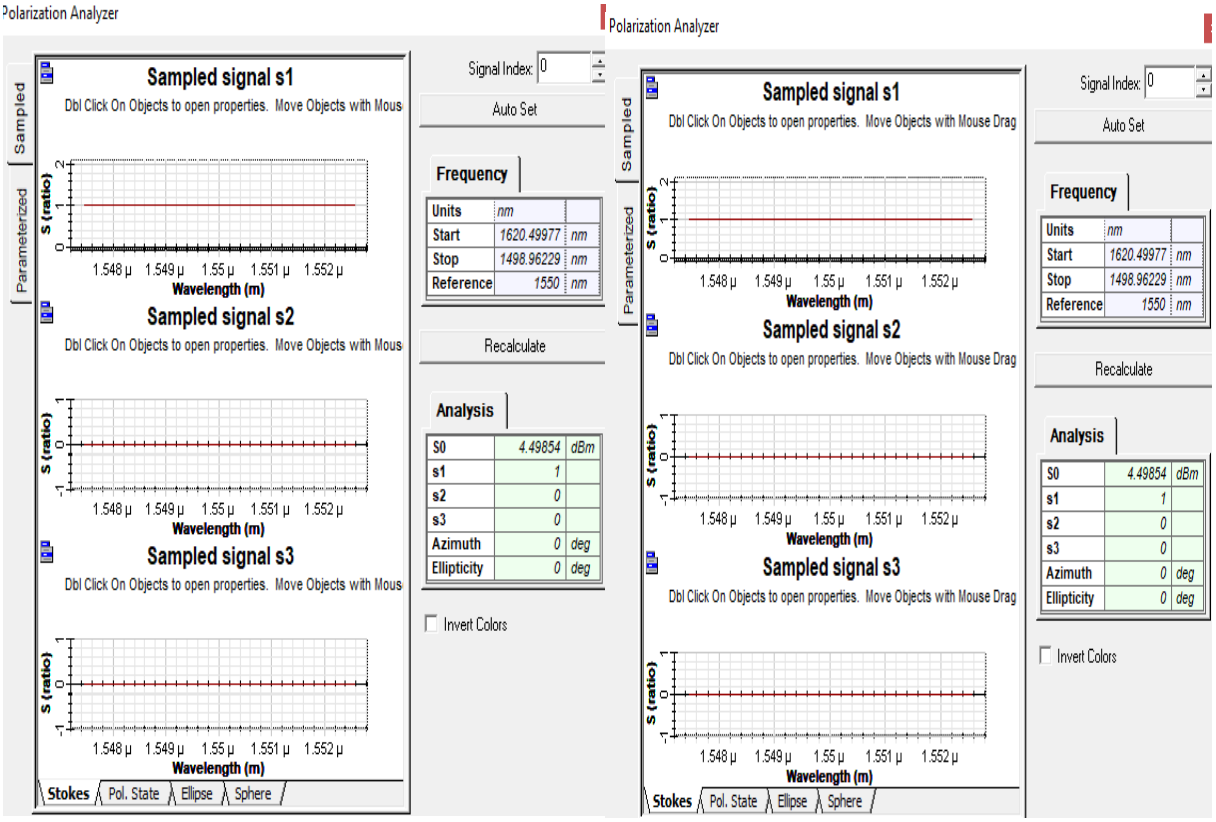


(a) (b)

Figure II.24 Résultats des analyseurs a) envoi d'Eve b) réception de Bob.

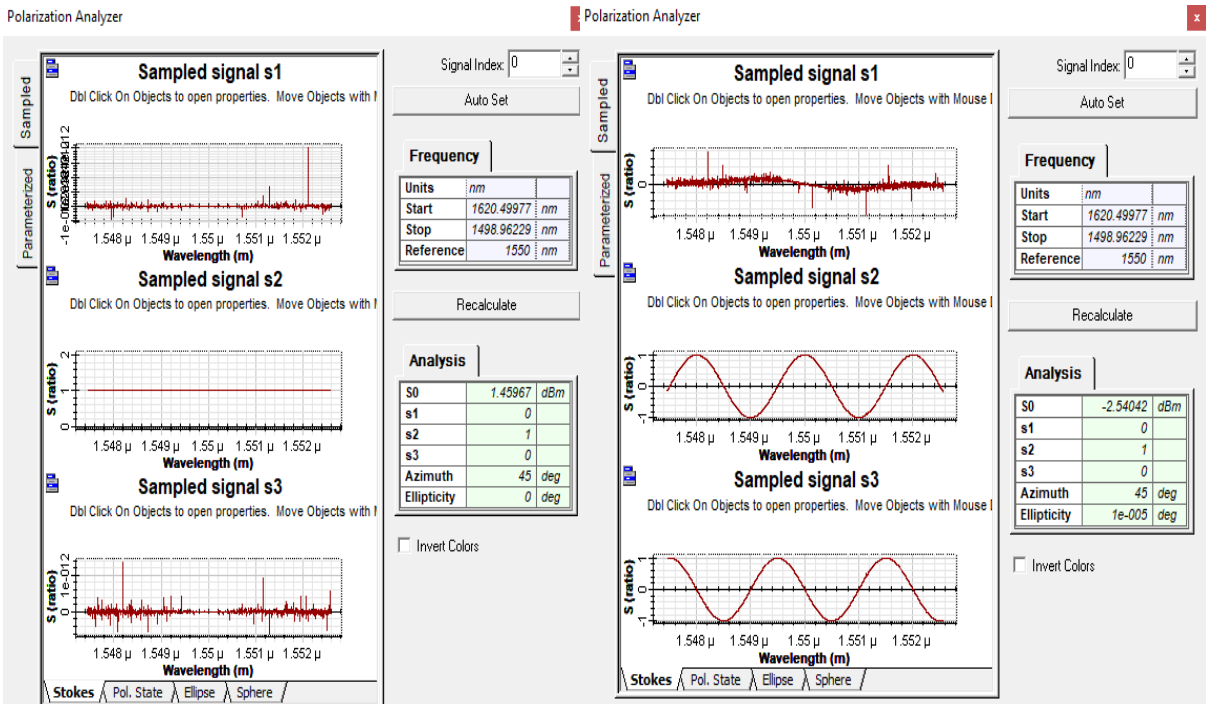
4eme qubit :

Alice envoie un qubit 0 polarisé avec l'angle 0°, Eve intercepte ce photon et envoie un nouveau photon polarisé avec l'angle 45° à bob, ce dernier reçoit le photon.



(a) (b)

Figure II.25 Résultats des analyseurs a) envoi d'Alice b) réception d'Eve.



(a) (b)

Figure II.26 Résultats des analyseurs a) envoi d'Eve b) réception de Bob.

✓ **Commentaire**

Nous remarquons d'après les résultats obtenus, que les clés transmises en absence et en présence d'espion (Eve) ne sont pas identiques. Quand Alice et Bob effectuent la phase de discussion, où ils vont sacrifier une partie de leurs clés sur le canal public. Ils sauront une si une personne avait tenté d'intercepter la clé.

Nous pouvons aussi remarquer, que même si Eve n'avait pas été découverte, elle n'aurait pas eu la bonne clé de chiffrement.

II.6 Conclusion

Nous venons de voir dans ce chapitre que la distribution quantique de clé utilise des sources qui émettent des photons uniques. Ensuite nous avons défini le principe de la QKD ainsi que les étapes d'un protocole quantique. Puis nous avons présenté le protocole de distribution le plus connu qui est BB84 publié par Bennett et Brassard en 1984, et nous avons mis l'accent sur le protocole B92.Dans la dernière partie de ce chapitre, nous avons réalisé avec succès la simulation du protocole B92 à l'aide d'OPTISYSTEM 7.0. La simulation s'est concentrée sur le montage expérimental en utilisant les composants disponibles dans ce dernier. Cela donne une image réelle de QKD qui est une combinaison de matériel et de protocoles utilisés pour obtenir une sécurité inconditionnelle dans la distribution des clés, nous avons pu mettre en œuvre une liaison sur un canal quantique, ainsi qu'une simulation du phénomène d'espionnage entre émetteur et récepteur. La présence d'Eve engendre des erreurs sur le résultat ainsi qu'Alice et Bob ont constaté la présence d'un espion.

Chapitre III

Etude des performances du protocole B92 dans une liaison optique

III.1 Introduction

Afin de prélever les performances du protocole B92 dans une liaison à fibre optique, nous allons procéder à la simulation de ce protocole sous OPTISYSTEM. Des mesures qualitatives seront effectuées à travers des mesures sur le facteur de qualité (Q) et le taux d'erreur binaire (BER) en absence et en présence d'un espion.

III.2 Principe de base d'une transmission optique

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

La figure III.1 illustre le principe de base d'une transmission de données par une fibre optique.

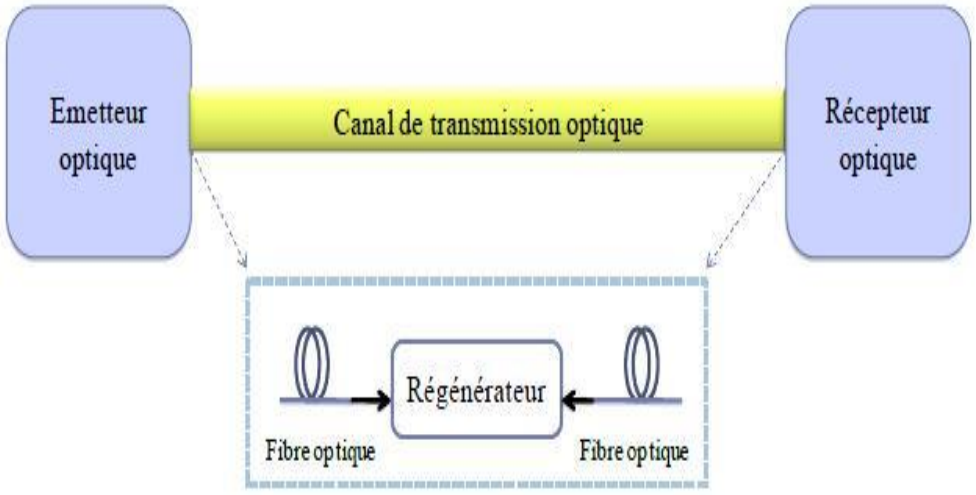


Figure III.1 Principe de base d'une transmission optique.

III.2.1 Fibre optique

La fibre optique est un support de transmission en verre ou en plastique très fin qui a la propriété d'être un conducteur de lumière de forme cylindrique constituée des éléments suivants :

- **Le cœur :** C'est la région centrale de la fibre qui permet le guidage des ondes lumineuses, d'indice de réfraction n1.
- **La gaine :** Représente une couche entourant le cœur de la fibre avec un indice de réfraction légèrement inférieur à celui du cœur, ce qui permet par conséquent, la réflexion totale et perpétuelle des modes à l'interface cœur-gaine.
- **Le revêtement** : Le revêtement assure la protection, voir la figure III.2 suivante :

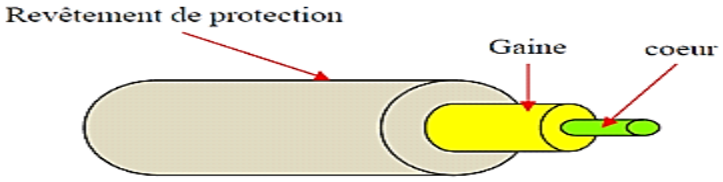


Figure III.2 Composants d'une fibre optique.

III.2.1.1 Les type de la fibre optique

Il y'a deux types de fibre optique :

- **Fibre monomode**

Dans ce type de fibre un seul mode est autorisé c'est le mode fondamental, elle est utilisée pour les systèmes de télécommunications à très longues distances à grands débits. Elle possède un diamètre de cœur de l'ordre de 8 à 10 µm.

Figure III.3 Fibre monomode.

- **Fibre multimode**

Les fibres multimodes ont été les premières sur le marché, elles permettent la propagation de plusieurs modes. Elles sont employées dans les systèmes à courtes distances notamment les réseaux locaux [23].

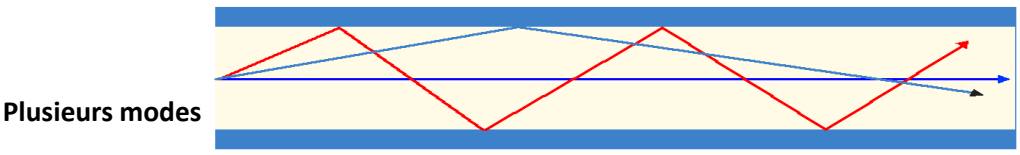


Figure III.4 Fibre multimode.

III.2.1.2 Propriétés de la fibre optique

- **Atténuation**

L'atténuation ou affaiblissement correspond à une diminution de la puissance d'un signal au cours de sa transmission. En effet ; le niveau de puissance d'un signal qui se propage dans une fibre optique, s'affaiblit exponentiellement en fonction de la distance de propagation [24].

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

- **La dispersion**

Les impulsions lumineuses qui traversent la fibre ont tendance à s'étaler, principalement à cause des retards du temps de propagation des différents rayons.

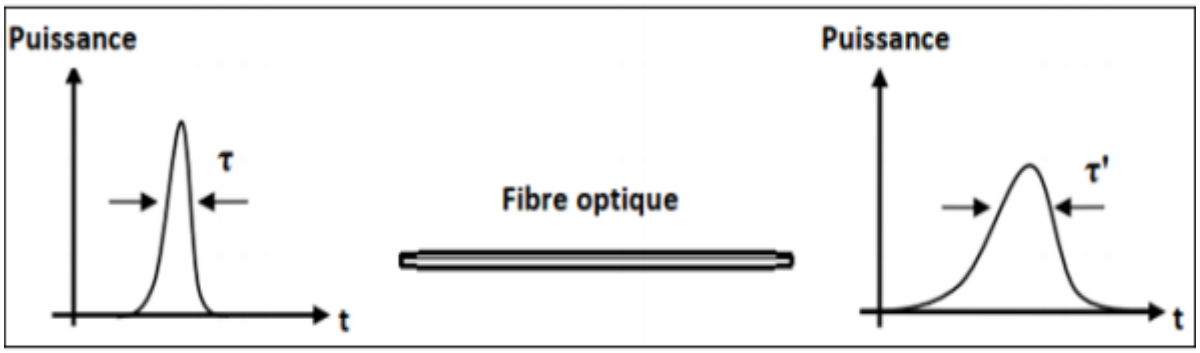


Figure III.6 La dispersion d'une fibre optique.

III.2.2 Les critères de qualité d'une transmission optique

Pour évaluer la qualité d'une transmission, différents critères existent. Les trois principaux critères de qualité d'un signal sont le diagramme de l'œil, le taux d'erreur binaire BER et le facteur de qualité Q.

III.2.2.1 Taux d'erreur binaire

Le signal transmis est un signal numérique binaire. La durée d'un symbole binaire est nommée 'temps bit' [25].L'évaluation de la qualité d'une transmission numérique binaire exige la comparaison de la séquence de symboles envoyés avec la séquence de symboles reçus grâce au calcul du nombre de bits erronés.

On définit alors le taux d'erreur binaire TEB ou Bit-Error Rate BER en anglais par le nombre de bits erronés sur le nombre de bits transmis**.**

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

III.2.2.2 Facteur de qualité (Q)

Le facteur de qualité est un paramètre qui permet l'estimation du taux d'erreur binaire sans avoir à compter les erreurs. Il représente le rapport signal sur bruit électrique en entrée du circuit de décision du récepteur. Sachant que le rapport signal sur bruit du récepteur d'un système de transmission par fibre optique a un impact direct sur les performances de ce système [24].

III.2.3 Chaine de transmission optique de base

Dans son synoptique le plus général et le plus simple possible, un système de télécommunications optique est donné par la chaîne de la figure III.7.

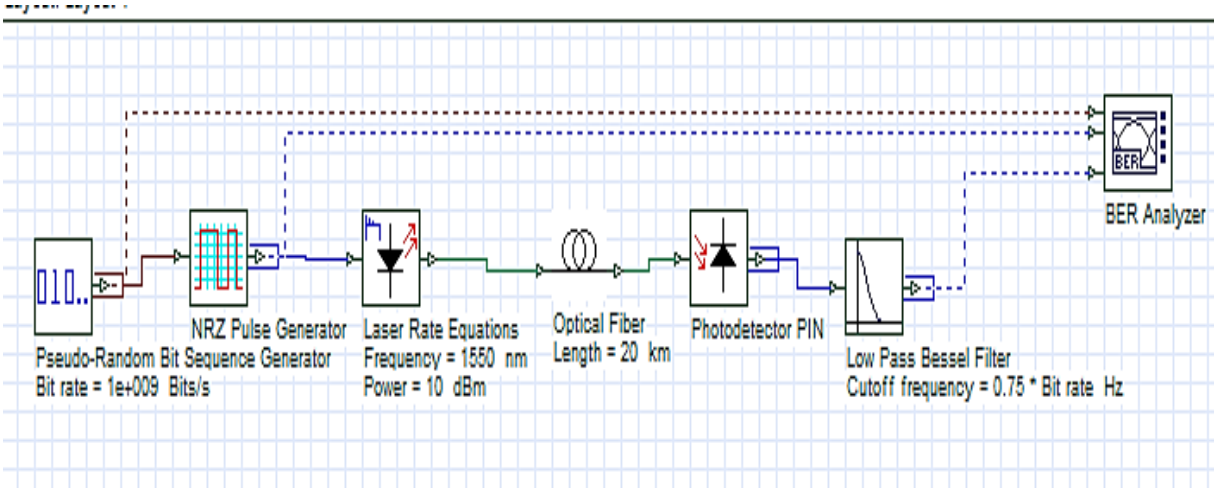


Figure III.7 Synoptique d'une chaine de transmission de base.

Les paragraphes suivants présentent les paramètres caractéristiques des composantes utilisées de la bibliothèque OPTIYSTEM pour construire les différents blocs de la chaine.

III.2.3.1 Bloc émission

Le rôle de l'émetteur consiste à délivrer à la fibre un signal optique continu et modulé, sur lequel sont inscrites les données électriques binaires.

- ✓ **Générateur de séquence binaire**

Il représente les données numériques qui vont servir pour la génération du courant électrique à l'entrée du laser. Son modèle de simulation est représenté dans la figure III.8.

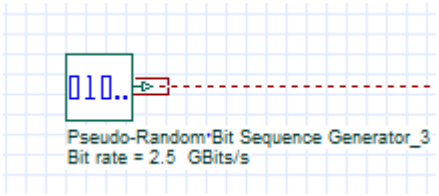


Figure III.8 Modèle de simulation de la séquence binaire.

- ✓ **Générateur NRZ**

Le générateur d'impulsions NRZ permet de créer une séquence d'impulsions codée par un signal numérique d'entrée, et prend uniquement deux valeurs ou le (0) est codé par un signal faible puissance et le (1) est codé par un signal fort puissance. Son modèle de simulation est représenté dans la figure III.9.

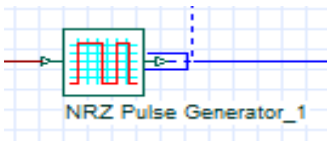


Figure III.9 Modèle de simulation du générateur NRZ.

- ✓ **Diode laser**

La diode laser sert comme source optique, son modelé de simulation est représenté dans la figure III.10.

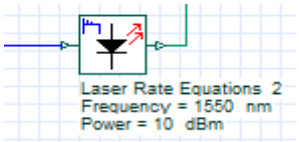


Figure III.10 Modèle de simulation de la diode laser.

III.2.3.2 Bloc réception

- ✓ **Photodiode PIN**

Le modèle utilisé en réception du signal optique comme le montre dans la figure III.11.

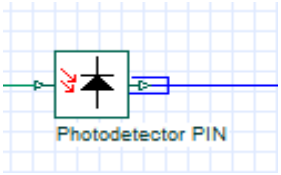


Figure III.11 Modèle de simulation d'une photodiode PIN.

- ✓ **Filtre passe bas**

Filtre passe bas utilisé pour filtrer le signal et pour limiter le signal en bande de base.Son modèle de simulation est représenté dans la figure III.12

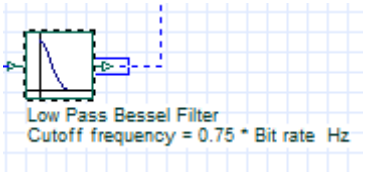


Figure III.12 Modèle de simulation filtre passe bas Bessel.

- ✓ **Analyseur de BER**

Pour visualiser on utilise BER. Son modèle de simulation est représenté dans la figure III.13.

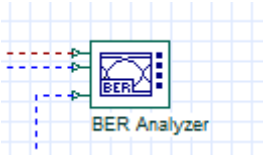


Figure III.13 Modèle de simulation d'un analyseur de BER.

III.2.3.3 Simulation de la chaine de base

Comme nous l'avons cité précédemment, nous choisissons d'évaluer les performances du système étudié avec le facteur Q (facteur de qualité) et le BER. Sachant que les normes fixées dans le domaine de télécommunications exigent, pour maintenir la qualité de transmission, un facteur supérieur à 6 et un taux d'erreur binaire BER inférieur à 10^{-9}.

La simulation de cette chaîne de référence pour un débit de 2.5Gbits/s et une distance de 20 Km donne le résultat ci-dessous :

Facteur de qualité	33.1145
BER	$8.50239e^{-241}$

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

✓ **Commentaire**

La simulation d'une chaine de transmission optique pour un débit de 2.5 Gbits/s a permis d'obtenir un facteur de qualité égale à 33.1145 et un taux d'erreur binaire égale $8.50239e^{-241}$, ce qui montre la bonne qualité de transmission.

III.3 Etude de la qualité de transmission du protocole B92 dans une liaison optique

Afin d'évaluer les performances du protocole B92 nous l'avons intégré dans une liaison de transmission optique où nous allons étudier l'influence des paramètres physiques de la fibre optique et de l'espionnage sur la transmission. L'analyse des différents résultats sera effectuée à travers les mesures du BER et du facteur de qualité.

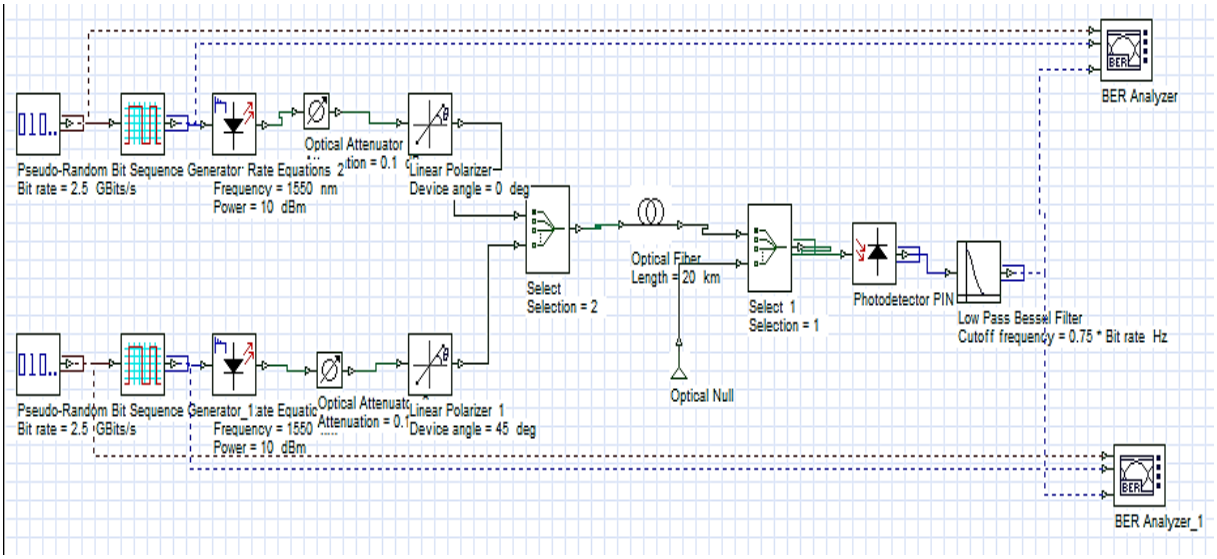


Figure III.14 Synoptique d'une chaine de transmission avec le protocole B92.

La simulation de cette chaine de transmission avec le même débit de 2.5Gbits/s a donné un facteur de qualité et le taux d'erreur binaire suivants :

Facteur de qualité	37.7277
BER	$8.09169e^{-312}$

Tableau III.2 Les résultats du facteur de qualité et du taux d'erreur binaire avec B92.

✓ **Commentaire**

La simulation d'une chaine de transmission optique pour un débit de 2.5 Gbits/s a permis d'obtenir un facteur de qualité 37.7277 et un taux d'erreur $8.09169e^{-312}$.Ces valeurs satisfont les normes fixées dans le domaine de télécommunications.

III.3.1 L'influence des variations de la distance de propagation sur la transmission

Dans cette simulation, nous avons varié la distance de propagation de 1 à 100 Km en utilisant une longueur d'onde égale à 1550 nm avec un débit de 2.5 Gbit/s. Nous avons obtenu les résultats présentés dans le tableau III.3 ci-dessous :

Longueur d'onde / Distance	λ=1550	
	Facteur de qualité	BER
1Km	77.3965	0
25Km	35.6982	$1.96919\ e^{-279}$
50Km	32.1188	$1.07282\ e^{-226}$
75Km	28.2282	$9.4545e^{-176}$
100Km	13.5825	$2.12947e^{-042}$

Tableau III.3 Résultats de la variation de la distance.

Avec les résultats du BER obtenus nous avons tracé la courbe pésentée sur la figure III.15

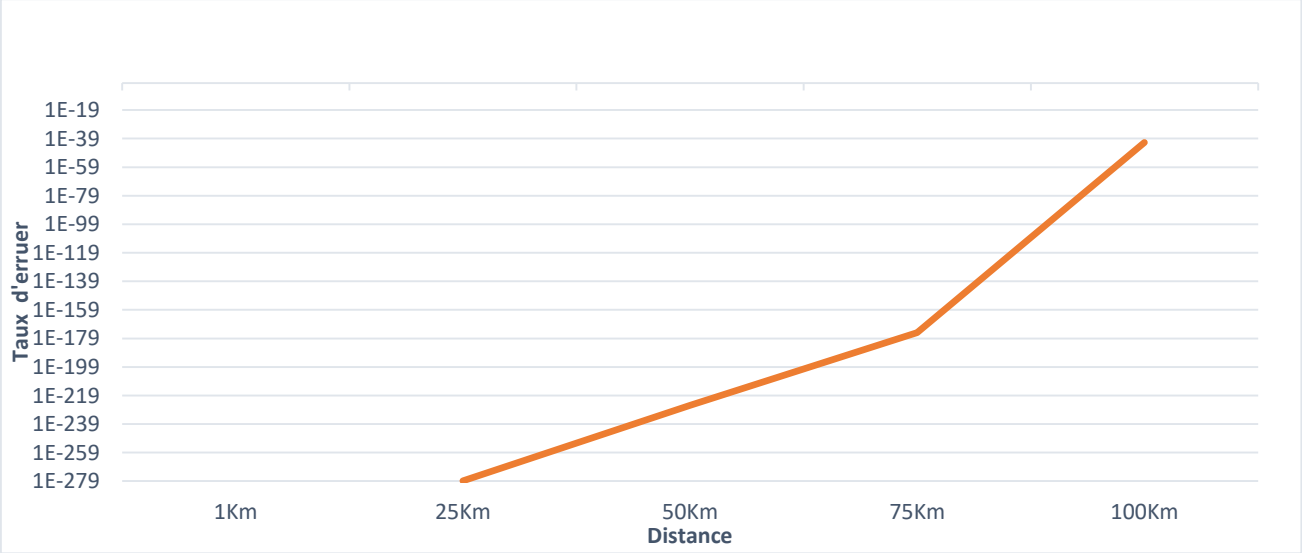


Figure III.15 BER en fonction de la distance.

✓ **Commentaire**

D'après la courbe obtenue, nous remarquons que le taux d'erreur augmente en augmentant la distance de propagation. Par conséquent la qualité du signal diminue.

Cette dégradation reste acceptable, pour des valeurs du BER inférieurs à 10^{-9}, selon les normes internationales,

Dans la pratique, actuellement la distance atteinte est inférieure à 60 km, ceci est dû au fait qu'à une certaine distance, le signal s'atténue, et l'implémentation d'un amplificateur optique EDFA devient plus qu'une nécessité, son fonctionnement peut violer le théorème de non clonage qui l'une des principales lois de la mécanique quantique.

III.3.2 Influence de la longueur d'onde sur la transmission

Pour cette étape, nous avons varié la longueur d'onde de la fibre pour un débit de 2.5 Gbit/s et une distance de 25 Km. Nous avons obtenu les résultats présentés dans le tableau III.4 ci-dessous

Longueur d'onde	Facteur de qualité	BER
850 nm	0	1
1300 nm	32.9697	$1.07518e^{-238}$
1550 nm	35.6982	$1.96919\ e^{-279}$

Tableau III.4 Résultats du BER et du facteur de qualité avec la variation de la longueur d'onde.

Avec les résultats du BER obtenus nous avons tracé la courbe pésentée sur la figure III.16

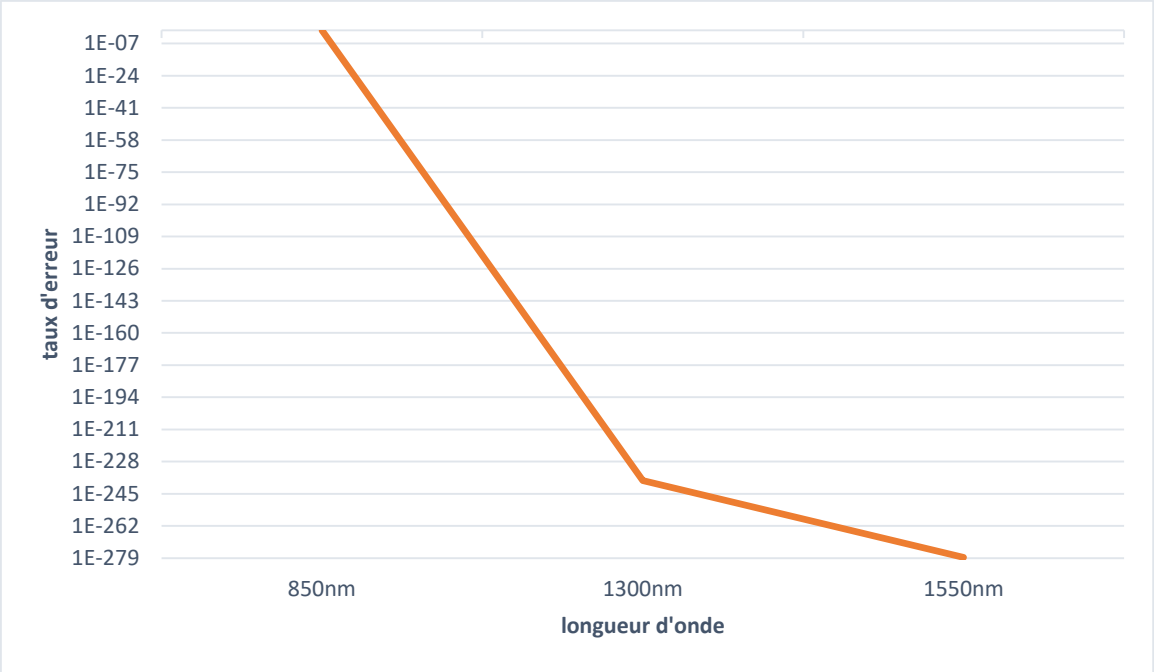


Figure III.16 Résultats du BER en fonction de la longueur d'onde.

✓ **Commentaire**

Dans les systèmes de télécommunications à fibre optique, trois fenêtres (longueurs d'ondes) sont utilisées, d'après la littérature, .la fenêtre correspondant à 1550nm présente le minimum d'atténuation. D'après la courbe représentante la variation du taux d'erreur binaire en fonction de la longueur d'ondes pour les trois fenêtres, nous remarquons que la valeur du taux d'erreur binaire est meilleure et plus faible pour la longueur d'onde 1550nm (3éme fenêtre). Pour la 2éme fenêtre (1300nm) nous constatons que le taux d'erreur binaire est acceptable, alors pour la 3éme fenêtre (850nm), la valeur du BER est supérieure à 10^{-9}, et l'erreur est inacceptable.

III.3.3 Influence de l'espion sur la transmission

Dans cette partie nous allons simuler une chaine de transmission avec le protocole B92 en présence d'un espion, pour un débit de 2.5 Gbit/s et une distance de 20 Km.

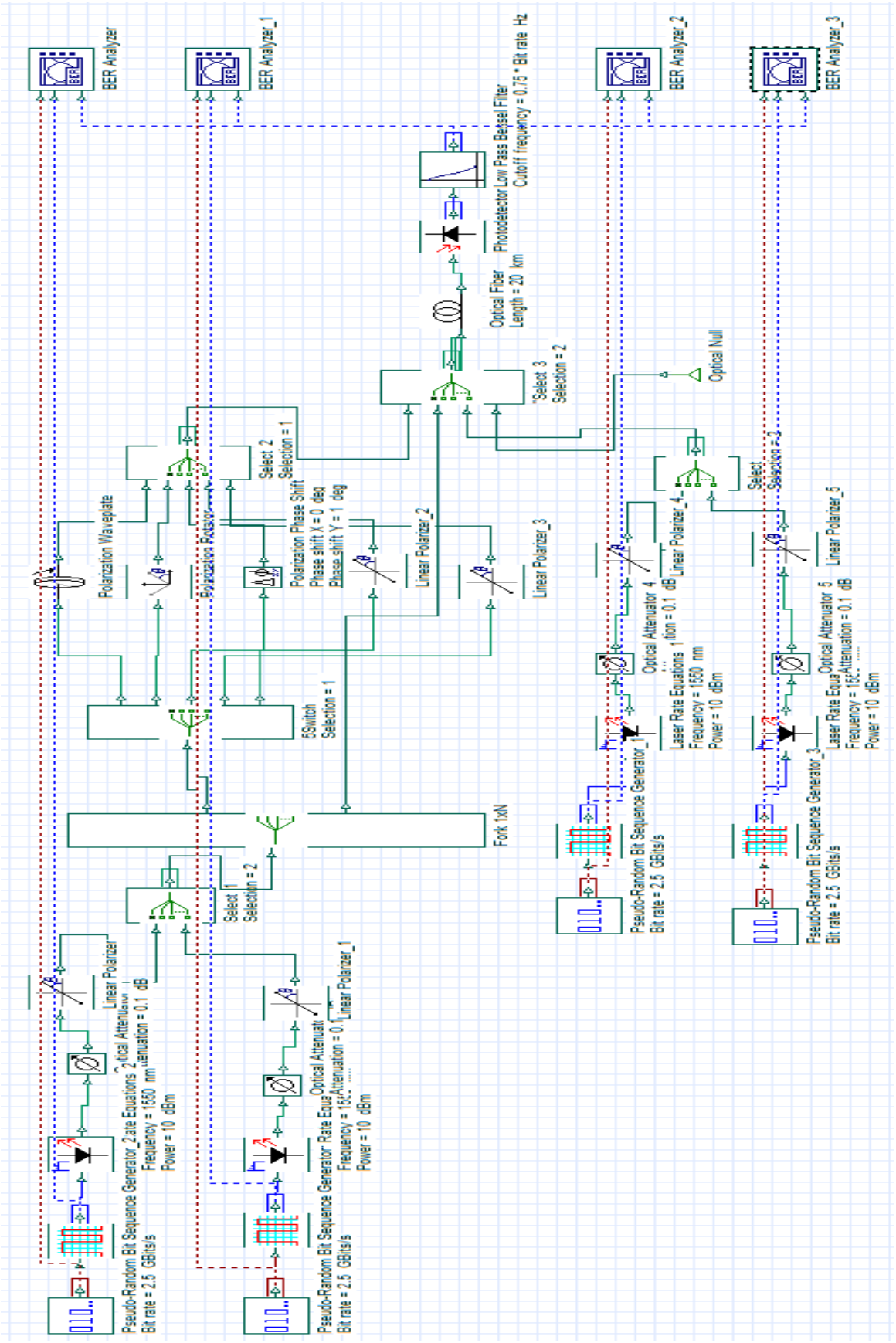


Figure III.17 Synoptique d'une chaine de transmission avec le protocole B92 en présence d'espion.

Les résultats de la simulation de cette chaine de transmission en présence d'un espion sont présentés dans le tableau III.5

	BER	**Facteur de qualité**
BER Analyzer	1	0
BER Analyzer_ 1	37.7277	$8.09169e^{-312}$
BER Analyzer_ 2	1	0
BER Analyzer _3	1	0

Tableau III.5 Les résultats du facteur de qualité et du BER.

- ✓ **Commentaire**

D'après les résultats obtenus Bob a reçu le photon (qubit) polarisé avec l'angle 45° envoyé par Alice.

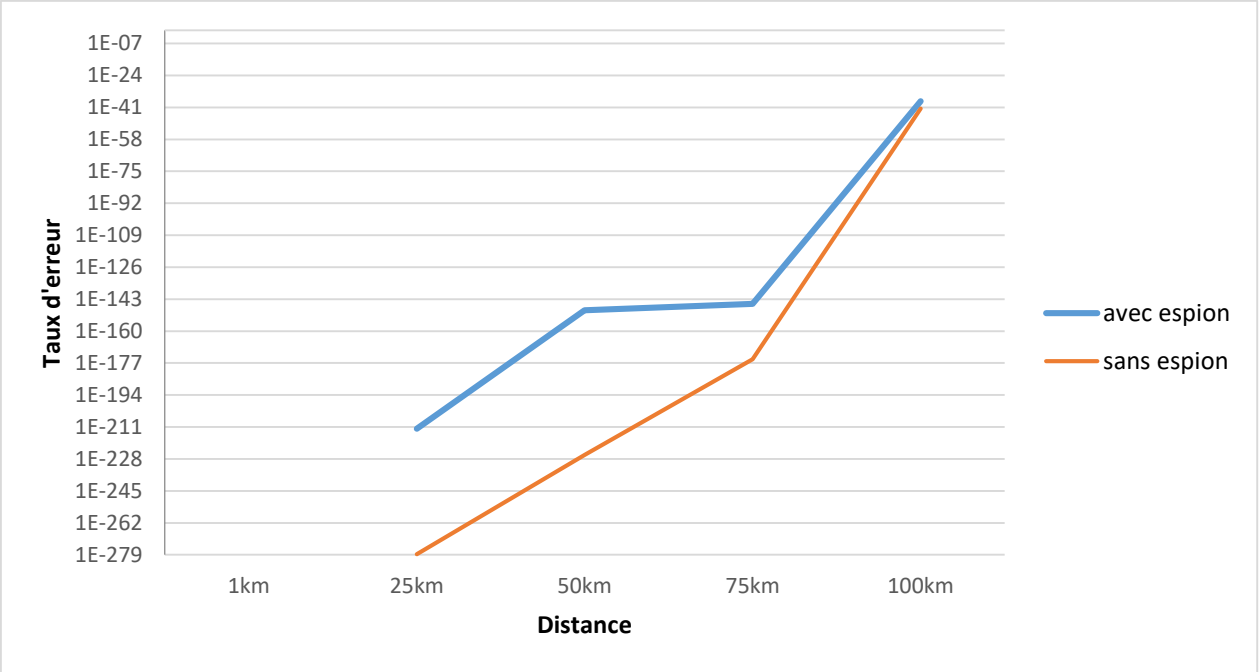
- ➢ **L'influence de la distance en présence d'un espion**

Pour cette étape, nous avons varié la distance de propagation de 1 à 100 Km pour un débit de 2.5 Gbit/s afin de faire une comparaison avec les résultats obtenus en absence d'un espion. Nous avons obtenu les résultats présentés dans le tableau III.6 ci-dessous :

Longueur d'onde / Distance	λ=1550	
	Facteur de qualité	BER
1Km	47.5462	0
25Km	31.1039	$1.06407e^{-212}$
50Km	26.0215	$1.37601e^{-149}$
75Km	25.7237	$2.60157\ e^{-146}$
100Km	12.9178	1.72726^{-038}

Tableau III.6 Résultats de la variation de la distance et de la longueur d'onde en présence d'un espion.

Avec les résultats du BER obtenus nous avons tracé la courbe pésentée sur la figure III.18



FigureIII.18 BER en fonction de la distance en présence d'un espion.

✓ **Commentaire**

En comparant les résultats obtenus en présence et en absence d'un espion. Nous remarquons que le taux d'erreur en présence d'un espion augmente plus en comparaison avec son absence. L'espion dispose de moyens et des outils qui lui permettent de recevoir et d'émettre le signal, sa présence sur la liaison peut entrainer des perturbations à travers ses actions, ce qui engendrera des pertes et du retard dans la transmission, cela se traduit par une valeur plus élevée du BER en sa présence, la transmission deviendra non acceptable pour des valeurs de BER supérieure à 10^{-9}.

III.4 Conclusion

Dans chapitre, nous avons défini les principes d'une liaison de transmission optique en citant les différents composants nécessaires, ensuite nous l'avons simulé avec l'OPTISYSTEM, suivit d'une implémentation du protocole B92. A travers l'analyse des facteurs de qualités et des taux d'erreur binaire obtenus, nous avons déduit que plus que la distance augmente la qualité de transmission diminue. Le choix de la fenêtre 1550nm est judicieux.

Conclusion générale

Conclusion générale

Dans ce mémoire, nous nous somme intéressées à la cryptographie quantique qui a pour objectif de rendre la communication entre deux usagers inviolables vis-à-vis d'intrusion extérieure. Cela est possible grâce aux principes de la mécanique quantique, le théorème de non-clonage et l'incertitude d'Heisenberg. Elle est utilisée pour remédier aux méthodes de cryptographie modernes qui sont de plus en plus vulnérables aux attaques des intrus. La cryptographie quantique tend actuellement à devenir un moyen d'apporter la confiance au cœur des affaires. L'un des protocoles de base de cette cryptographie est celui proposé par Charles Bennett en 1992.

Le premier chapitre, nous l'avons consacré à la présentation des principes de la cryptographie et les techniques utilisées pour assurer la sécurité, à savoir la cryptographie classique d'une part, et la cryptographie moderne d'autre part qui se subdivise en deux types, celles à chiffrement symétrique et asymétrique tout en définissant les algorithmes de chiffrement les plus connus. Ensuite, nous avons présenté une nouvelle classe de cryptographie qui est la cryptographie quantique .Cette dernière est apparue comme solution pour pallier aux insuffisances de la cryptographie classique. Ainsi que les notions et les principes de la mécanique quantique qui représente la base de la cryptographie quantique sont présentés.

Dans le deuxième chapitre, en première partie nous avons cité les phases constituantes un protocole quantique, qui utilise des sources à photon unique. Puis nous avons donnés les protocoles quantiques les plus performants ainsi qu'une description détaillée du protocole B92. Dans la dernière partie de ce chapitre, nous avons implémenté le protocole B92 sur OPTISYSTEM pour évaluer la polarisation du photon et le phénomène d'espionnage. Nous avons conclus que l'espion ne peut pas intercepter la clé sans qu'il soit repéré.

Dans la dernière partie du travail, nous avons implémenté le protocole B92 sur OPTISYSTEM, afin de voir la qualité de la transmission. La simulation consiste à déterminer le comportement du protocole lors de la variation d'un paramètre et la présence d'un espion. Par conséquent, nous avons déduit que plus la distance augmente la qualité de transmission diminue. Le choix de la fenêtre 1550nm est judicieux

Comme perspectives, il serait intéressant d'étendre l'étude à d'autres protocoles à variables discret et à variables continues et de penser de voir l'influence d'autres paramètres tel que le débit, la puissance….

Bibliographie

Bibliographie

[1] Fédération e-commerce et vente à distance. (2021) Bilan du e-commerce en 2020 : les ventes sur internet atteignent 112 milliards d'euros grâce à la digitalisation accélérée du commerce de détail. [En ligne]. https://www.fevad.com/bilan-du-e-commerce-en-2020-les-ventes-sur-internet-atteignent-112-milliards-deuros-grace-a-la-digitalisation-acceleree-du-commerce-de-detail/

[2] G. JEROME. (2010) Clé RSA de 768 bits cassée en deux ans et demi. [En ligne]. https://www.generation-nt.com/cle-rsa-768-bits-cassee-inria-actualite-939471.html

[3] L. ZYGA. (2014) New largest number factored on a quantum device is 56,153. [En ligne]. https://phys.org/news/2014-11-largest-factored-quantum-device.html

[4] Y. CONNAN, "Contribution à la cryptographie post-quantique basée sur les codes correcteurs d'erreurs en métrique rang : Hash Proof Systems et cryptographie à bas coût. Cryptographie et sécurité", Thèse de Doctorat en informatique, Limoges : Université de Limoges, 2020,125p.

[5] K. DICHOU, "Contribution à l'étude des cartes à puce avancées", Thèse de Doctorat, Génie Électrique, Boumerdes : Université M'HAMED BOGARA-BOUMERDES, 2016, 136p.

[6] F. OMARY, "Applications des algorithmes évolutionnistes à la cryptographie ", Thèse de Doctorat en informatique, RABAT : Université MOHAMMED V – AGDAL RABAT (MAROC), 2006, 127p.

[7] G. ZAIBI, "Sécurisation par dynamiques chaotiques des réseaux locaux sans fil au niveau de la couche MAC", Thèse de Doctorat, Tunisie : L'École Nationale d'Ingénieurs de Sfax, 2012, 137p

[8] Agence National de certification Electronique Tunisie (2005) Introduction à la Cryptographie [en ligne] https://www.calameo.com/books/0001212350f906e854112

[9] A. BERZATI "Analyse cryptographique des altérations d'algorithmes ", Thèse de Doctorat en informatique, Paris : Université de Versailles Saint-Quentin, 2010,159p.

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

[11] R.DJELLAB, "Cryptographie quantique, Nouvelles approches", Thèse de Doctorat en informatique, Batna : Université Batna 2, 2017,141p.

[12] M. LANGLOIS, "Cryptographie quantique solution au problème de distribution de clefs secrètes", Thèses de doctorat, Ottawa : Université d'Ottawa, 1999.

[13] S. GHOBBER, " Paires annihilantes en analyse harmonique", Thèse de Doctorat en Mathématique, Orléans: Université d'Orléans, 2011,164p.

[14] A. EL Allati, " Etude de cryptographie et de téléportation quantiques et proposition de quelques protocoles quantiques", Thèse Doctorat en physique théorique, Rabat : Université Mohammed V-Agdal, 2012, 139p

[15] C. Bennet, « Quantum Cryptography Using Any Two Nonorthogonal States », *PHYSICAL REVIEW LETTERS*, 1992, Vol 68, N°21, pp. 3121-31240

[16] R., ALLEAUME, "Réalisation expérimentale de source de photons uniques, caractérisation et application à la cryptographie quantique", Thèse Doctorat en physique quantique, France : Université Pierre et Marie Curie, 2004, 192p.

[17] A. Bocquet, "Modèles de sécurité réalistes pour la distribution quantique de clés", thèse de doctorat en Informatique et Réseaux, paris : École Doctorale d'Informatique, Télécommunications et Électronique de Paris, 2011, 137p.

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

[19] "Polarization Measurements of Signals and Components", Product Note 8509-1, Agilent Technologies

[20] Lawal Muhammad Aminu, « Performance Evaluation of Secure Key Distribution Based on Quantum Mechanics Principles Over Free Space », *International Journal Of Engineering And Computer Science,* 2014, Vol. 3, No.8460-8468

[21] N. Hafizah Mohamed Halip, M. Mokhtar, A. Buhari, « Simulation of Bennet and Brassard 84 Protocol with Eve's Attacks », Proc. *Of 2014 IEEE 5th International Conference on Photonics*, 2014, pp. 19-31.

[22] A. BUHARI, ZURIATI. AHMAD ZUKARNAI, SHAMALA. K.SUBRAMANIAM, HISHAM. ZAINUDDIN and SUHAIRI. SAHARUDIN, « An Efficient Modeling and Simulation of Quantum Key Distribution Protocols Using OptiSystem », *(IJCSIS) International Journal of Computer Science and Information Security*, Vol. 10, No. 12, 2012, pp .8-14.

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

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

[25] L.GRAINI, "Application des similaritons dans les systèmes de télécommunications par fibre optique à très haut débit", Thèse de Doctorat en Télécommunication, Annaba : Université Badji Mokhtar, 2017, 190p.

Résumé

Quelque soit l'environnement dans lequel se déroule une communication, la sécurité reste nécessaire pour le bon déroulement de cette communication. Afin d'assurer un certain niveau de sécurité, la confidentialité est un élément essentiel à assurer. Ce sont les techniques de cryptographie qui l'assurent. Plusieurs protocoles ont été proposés pour assurer une bonne gestion de clé, mais leur sécurité se base sur la complexité computationnelle. La distribution de clé quantique, dite cryptographie quantique se base sur les lois de la mécanique quantique, permettant d'établir une clé secrète commune entre les traditionnels correspondants Alice et Bob. Dans ce mémoire, nous nous intéressons à la distribution de clé quantique et plus précisément le protocole Bennet 1992 où nous allons l'implémenter dans une liaison optique sue le logiciel OPTISYSTEM.

Mots clé : Cryptographie, Cryptographie quantique, BB84, B92, Distribution de clé quantique, Quantique, Sécurité.

Abstract

Whatever the environment in which a communication takes place, security remains necessary for the smooth running of this communication. In order to ensure a certain level of security, confidentiality is an essential element to ensure. This is ensured by Cryptography techniques. Several protocols have been proposed to ensure good key management, but their security is based on computational complexity. Quantum key distribution, called quantum cryptography, is based on the laws of quantum mechanics, allowing to establish a common secret key between the traditional correspondents Alice and Bob. In this thesis, we are interested in quantum key distribution and more precisely the Bennet 1992 protocol where we will implement it in an optical link on the OPTISYSTEM software.

Key words : Cryptography, Quantum cryptography, BB84, B92, Quantum key distribution, Quantum, Security.