République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieure et de la Recherche Scientifique

Université Abderrahmane Mira

Faculté de Technologie

Département Automatique, Télécommunication et Electronique

Projet de Fin d'étude

Pour l'obtention du diplôme de Master

Filière : Télécommunications

Spécialité : Réseaux et Télécommunications

Thème :

Etude comparative des protocoles de la cryptographie quantique

BB84 et à six états

Réalisé par :

M^elle BENSAADA Fatima & M^elle DJOUADI Sarah

Devant le jury composé de :

- **Promoteur** : Mr BERRAH Smail
- **Président :** Mr BELLAHSENE Hocine
- **Examinatrice :** Mme ACHOUR Lyakout

Promotion : 2020-2021

Remerciements

Ce travail est l'aboutissement d'un dur labeur et de beaucoup de sacrifices, nos remerciements vont d'abord au créateur de l'univers Allah le tout puissant de nous avoir donné la volonté et le courage pour l'achèvement de ce travail.

*Nos remerciements sont aussi adressés à notre encadreur le professeur **Mr Berrah** qui nous a proposé le thème de ce mémoire pour ses orientations, ses conseils, ses remarques judicieuses et sa disponibilité, nous tenons à lui exprimer notre profonde graduation en vue du bon déroulement du travail durant l'élaboration de ce mémoire.*

*Nous remercions également **Mme Bouchoucha** pour ses conseils et ses encouragements*

Nous adressons nos sincères remerciements à l'ensemble des membres du jury, qui nous ont fait l'honneur de bien vouloir étudier avec attention notre travail :

***Mr Bellahsene** et **Mme Achour** pour l'intérêt qu'ils ont porté en acceptant d'examiner notre travail et l'enrichir par leurs propositions. Nos remerciements s'étendent également à tous nos enseignants durant les années des études*

- Fatima & Sarah-

Dédicace

Je dédie ce modeste travail à :

A ma chère mère : *quoi que je fasse ou que je dise, je ne saurai te remercier comme il se doit. Ton affection me couvre, ta bienveillance me guide et ta présence à mes côtés a toujours été ma source de force pour affronter les différents obstacles.*

A mon cher père : *tu as toujours été pour moi un exemple du père respectueux et honnête, grâce à toi j'ai appris le sens du travail et de la responsabilité, ton soutien fut une lumière dans tout mon parcours. Ce modeste travail est le fruit de tous les sacrifices que tu as déployé pour mon éducation et ma formation.*

A ma belle-mère : *cette âme flamboyante d'amour et de tendresse*

A mes chers frères et mes sœurs.

A mon âme sœur, ma confidente Assia : *je ne saurais te remercier pour ton soutien moral, ton encouragement, tes conseils, ta confiance en moi.*

A frère et à sa femme : *je tiens à témoigner ma reconnaissance à mon très cher frère* **Ghani** *et à sa femme* **Ahlem** *qui ont toujours cru en moi et qui m'ont soutenu dans ce projet et tout au long de ces nombreuses années d'étude.*

A mes chers grands-parents paternels et A ma grand-mère maternelle.

A la mémoire de mon grand-père maternelle.

A mes chers tantes et oncles.

A ma chère tata fakia : *qui a toujours été comme une deuxième maman a moi.*

A mes chers cousins et cousines : *Nabila, Rahma, Sabrina, Radia, Amina, Hafsa, Meriem, Hadjer, Nassima, Rahim. Bassem, Youcef.*

A mes chères copines : *Yasmine, Houda, Zohra, Nesrine, Kahina, Ines, Sarah, Manel, Bothaina, Maissa, Samah.*

A mon cher binôme Sarah : *je souhaite personnellement remercier ma deuxième sœur et mon binôme et copine qui a été mon binôme durant tout notre cursus, avec laquelle j'ai pris beaucoup de plaisir à travailler. Nous avons formé une belle équipe, je te remercie donc pour tout ce que tu m'as apporté au cours de ces cinq années partagées.*

- Fatima -

Dédicace

Je dédie ce modeste travail à :

A ma chère mère : *quoi que je fasse ou que je dise, je ne saurai te remercier comme il se doit. Ton affection me couvre, ta bienveillance me guide et ta présence à mes côtés a toujours été ma source de force pour affronter les différents obstacles.* ***je t'aime mama.***

A mon cher père : *tu as toujours été pour moi un exemple du père respectueux et honnête, grâce à toi j'ai appris le sens du travail et de la responsabilité, ton soutien fut une lumière dans tout mon parcours. Ce modeste travail est le fruit de tous les sacrifices que tu as déployé pour mon éducation et ma formation.*

A ma chère sœur Aya *: que dieu te protège et te garde pour moi. Mon ange t'avoir dans ma vie est une chance.*

A mon chère frère Abdou : *tu m'as toujours encouragé et soutenu*
A mon âme tente, ma confidente tata Samira : *je ne saurais te remercier pour ton soutien moral, ton encouragement, tes conseils, ta confiance en moi.*

A mon cher grand-père maternel et A ma chère grand-mère paternelle.

A la mémoire de ma grand-mère maternelle et mon grand-père paternelle.

A mes chers tantes et oncles.

A mes chers cousins et cousines : *Samia, Sophie, Wissem, Zouina, Aida, Ryma, Kahina, Nissa, Massi, Mamou, Billel, Ramzi.*

A mes chères copines *: Assia, Manel, Kahina, Sarah, Bouthaina*

A mon cher binôme Fatima : *je souhaite personnellement remercier ma deuxième sœur et mon binôme et copine qui a été mon binôme durant tout notre cursus, avec laquelle j'ai pris beaucoup de plaisir à travailler. Nous avons formé une belle équipe, je te remercie donc pour tout ce que tu m'as apporté au cours de ces cinq années partagées.*

Sarah -

Sommaire

Sommaire

Remerciements

Dédicace

Sommaire

Liste d'abréviation

Liste des tableaux

Liste des figures

Introduction Générale 1

Cadre théorique

Chapitre I

Généralités sur la cryptographie

Introduction 7

I. 1 Concepts de base **..... 7**

1.1. Cryptologie 7

1.2. Définition de la cryptographie 7

1.2.1. La terminologie 8

1.2.2. L'usage de la cryptographie 8

I. 2 Les types de chiffrement **..... ……..9**

2.1. Chiffrement classique 10

2.1.1. Le chiffrement par substitution 10

2.1.2. Le chiffrement par transposition 11

2.2. Chiffrement moderne 11

2.2.1. Cryptographie symétrique ou à clé secrète 11

2.2.2. Cryptographie asymétrique ou à clé publique : 13

I. 3 Comment on a passé du classique au quantique ? **..... 15**

Conclusion 15

Sommaire

Chapitre II

Cryptographie quantique

Introduction 17

II. 1.Notion de la mécanique quantique **17**

1.1. Les systèmes quantiques 17

1.2. État quantique 18

II. 2.Principe générale de distribution quantique de clé **18**

2.1. Principe d'incertitude de Heisenberg 18

2.2. Théorème de non-clonage 18

II. 3.La cryptographie quantique : **19**

3.1. Photon 19

3.2. Polarisation 20

3.3. Bit quantique (qubit) 20

3.4. Transmission de la clé 20

3.5. Propriétés des qubits 21

3.5.1. La superposition 21

3.5.2. L'intrication : 21

II. 4.Principe de la cryptographie quantique **21**

4.1. Le canal quantique 22

4.2. Le canal classique 22

II. 5 Les protocoles de la cryptographie quantiques **22**

5.1. Le protocole bb84 22

5.1.1. Les sources à photon unique 24

5.2. Protocole à six états 25

5.3. Protocole B92 (à deux états) : 26

Conclusion 27

Sommaire

Cadre pratique

Chapitre III

Implémentation des protocoles BB84 et à six états sur OptiSystem sans attaque

Introduction 30

III. 1.Logiciel OPTISYSTEM **30**

III. 2.Les paramètres de l'OptiSystem **30**

2.1. Les paramètres de Stockes 31

2.2. La sphère de Bloch 31

III. 3.Le protocole BB84et le protocole à six états sans attaque **32**

3.1. Le protocole BB84 32

3.1.1. La simulation avec une seule polarisation 32

3.1.2. La simulation avec deux polarisations 35

3.1.3. Simulation avec quatre polarisations 38

3.2. Le protocole à six états 41

3.2.1. Simulation avec une polarisation 41

3.2.2. Simulation avec deux polarisations circulaire (gauche et droite) : 43

3.2.3. Simulation avec six polarisations 45

Conclusion 48

Chapitre IV

Implémentation des protocoles BB84 et à six états sur OptiSystem avec attaqu

Introduction 50

IV. 1.Le protocole bb84 et le protocole à six états avec attaque **50**

1.1. Le protocole BB84 52

1.2. Le protocole à six états 55

IV. 2.Exemple d'une séquence binaire dans le protocole BB84 et à six états **59**

2.1. Le protocole BB84 59

2.2. Le protocole à six états 63

Sommaire

IV. 3.Comparaison entre le protocole BB84 et le protocole à six état **..... 66**

Conclusion 66

Conclusion Générale 67

Références bibliographiques 70

Liste d’abréviation

A : Anti-diagonal.

AES : Advanced Encryption Standard.

Alice : Pour designer l'émetteur du message.

Bob : Pour désigner le récepteur.

D : Diagonal.

DES : Data Encryption Standard.

Dr : Circulaire droite.

EM : Electromagnétique.

Eve : Eavesdropper.

G : Circulaire gauche.

H: Horizontale.

MIT: Massachusetts Institute of Technology.

QKD: Quantum Key Distribution.

RSA: Rivest, Shamir and Adleman.

Sop*:* Observable Polarizarion Sphere.

SSP: *six-state protocols.*

V : vertical

Liste des tableaux

Numéro	Titre	Page
01	*Une séquence binaire sans espion du protocole BB84.*	**59**
02	*Une séquence binaire avec espion du protocole BB84.*	**60**
03	*Une séquence binaire sans espion du protocole à six états.*	**63**
04	*Une séquence binaire avec espion du protocole à six états*	**63**

Liste des figures

Numéro	Titre	page
01	*Principaux objectifs de la sécurité.*	**9**
02	*Types de chiffrement.*	**10**
03	*Les méthodes de la cryptographie moderne.*	**11**
04	*Principe de la cryptographie symétrique.*	**12**
05	*Le principe de la cryptographie asymétrique.*	**13**
06	*un système de distribution de clé quantique.*	**19**
07	*Le bit classique et le bit quantique.*	**20**
08	*Les systèmes de communication quantique.*	**22**
09	*Le protocole BB84.*	**24**
10	*Source Laser atténué.*	**25**
11	*Trois paires de bases utilisées dans le protocole à six états.*	**26**
12	*Les bases de polarisation du protocole B92.*	**27**
13	*Simulation de BB84 pour une seule polarisation.*	**32**
14	*Paramètre de Stockes obtenus de l'émetteur.*	**33**
15	*Paramètre de Stockes obtenus du récepteur*	**34**
16	*Paramètre de Stockes de la sphère Poincaré*	**34**
17	*Simulation de BB84 pour deux polarisations*	**35**
18	*Les paramètres de Stockes du récepteur*	**36**
19	*La sphère de Bloche*	**37**
20	*Simulation de BB84 pour quatre polarisations*	**38**

Liste des figures

21	*Les paramètres de Stockes au niveau du récepteur*	**39**
22	*La sphère de Bloche*	**40**
23	*Le protocole à six états avec une seule polarisation*	**41**
24	*Les paramètres de Stockes*	**41**
25	*La sphère de Bloche du récepteur*	**42**
26	*Simulation du protocole à six états avec deux polarisations*	**43**
27	*La sphère de Bloch du récepteur*	**43**
28	*La sphère de Bloch du récepteur*	**44**
29	*Protocole à six états*	**45**
30	*Les paramètres de Stockes*	**46**
31	*La sphère de Bloche*	**47**
32	*Le protocole BB84 avec une attaque*	**52**
33	*Les paramètres de Stockes de Bob*	**53**
34	*Les paramètres de Stockes d'Eve*	**53**
35	*La sphère de Bloche*	**54**
36	*Le protocole à six états avec un espion*	**55**
37	*Les paramètres de Stockes du récepteur*	**56**
38	*Les paramètres de Stockes de l'espion*	**57**
39	*La sphère du Bloche du récepteur*	**58**
40	*Les paramètres de Stockes entre Alice(a) et Eve(b)*	**61**
41	*Les paramètres de Stockes entre Eve (a) et Bob(b)*	**61**
42	*Les paramètres de Stockes entre Alice(a) et Eve(b)*	**62**

Liste des figures

43	*Les paramètres de Stockes entre Eve (a) et Bob(b)*	**62**
45	*Les paramètres de Stockes entre Alice(a) et Eve(b)*	**64**
46	*Les paramètres de Stockes entre Eve (a) et Bob(b)*	**65**

Introduction Générale

L'humanité depuis son existence exprima le besoin de transmettre les messages de manière sécurisée en les rendant invisible pour une tierce personne étrangère. Ils se servaient donc d'outils permettant de garder leurs confidences hors d'atteinte des yeux indiscrètes. La progression de ces outils primitifs à travers le temps, a permet de concevoir des règles de sécurité plus efficaces et plus logique qui ont donné naissance à la cryptographie.

Avec l'avènement des réseaux, et tout en particulièrement Internet, la cryptographie a pris une nouvelle dimension, économique cette fois. C'est en effet toute la sécurité du commerce électronique qui dépend maintenant de l'inviolabilité des codes cryptés.

La cryptographie classique traite des systèmes reposant sur les lettres et les caractères d'une langue naturelle, de nos jour les méthodes utilisées sont plus complexe, cependant la philosophie reste la même mais la différence fondamentale est que la cryptographie moderne manipule des bits contrairement aux anciennes méthodes.

La sécurisation des transactions utilisée dans le commerce électronique, à titre d'exemple en 2020 le bilan e-commerce a enregistré un chiffre de 112milliard d'euro concernant unique les ventes en ligne [21]. Regardant ce chiffre, la sécurité et la confidentialité des données s'avère plus qu'une priorité.

L'algorithme le plus répandu est le RSA (Rivest, Shamir and Adleman) .son utilisation intervient pour le cryptage avec beaucoup d'efficacité, le but de tel système est de sécuriser plus particulièrement la transmission des numéros de cartes utilisées pour le paiement des commerçants et d'assurer leurs vérifications.

Avec L'apparition de l'ordinateur quantique, a rendu capable de casser les algorithmes cryptographique existant (RSA), mettant à mal la sécurisation des données, cependant il est temps de chercher d'autre outils du cryptage afin d'y remédier à ces défaillances.

La cryptographie quantique apparue à la fin du siècle précèdent se présente comme un moyen puissant pour la sécurisation de données. Elle a été réalisée pour la première fois, lors des élections suisses en 2007 [10], où une connexion quantique a été utilisée pour sécuriser la transmission des données d'un point d'entrée jusqu'au dépôt de données central du gouvernement.

Le 29 septembre 2017 est une date majeure de l'histoire des télécommunications [9]. Ce vendredi matin à 9.30, pendant une quinzaine de minute le physicien Anton Zeilinger, président de l'académie des sciences en Autriche, et son homologue chinois, Chunli Bai, ont pu se parler au moyen d'une vidéocommunication qui est réputée être inviolable, entre Vienne et Pékin la vidéo a été chiffrée au moyen de ce que les experts appellent «une clé quantique » qui rend la communication protégée contre toute tentative d'espionnage. Par ailleurs, Toshiba a réalisé une percée avec la cryptographie quantique au sein de son laboratoire de recherche de Cambridge en créant le périphérique quantum Key.

Son réalisation est limitée actuellement par son coût relativement élevé. Il est probable qu'il faut attendre encore quelques années pour que cette technologie soit largement utilisée avec une prévision d'un marché mondial estimé à 948.82 millions de dollars d'ici 2025 [22], l'informatique quantique promet aux pays qui s'imposeront dans cette compétition technologique mondiale.

Bien évidemment, la cryptographie quantique a toujours été une nécessité militaire. La Darpa (agence américaine sur la recherche militaire avancée) utilise ainsi depuis 2004 un réseau de distribution quantique de clefs pour transmettre des messages confidentiels qui s'ils étaient pris par l'ennemi, ne devaient pas pouvoir être compris [10].

En effet, la cryptographie a pris un grand développement et devenue une discipline qui utilise des concepts mathématique et informatique pour prouver sa sécurité [18].

C'est dans ce contexte que s'inscrit notre thème .l'objectif de ce travail est de réaliser une étude comparatif entre deux protocoles quantiques le BB84 et celui à six états afin de tester leurs robustesses.

Ce mémoire est organisé en quatre chapitres :

Le premier chapitre, présente un aperçu général sur des notions et les concepts de base de la cryptographie classique et son usage, et d'autre part la cryptographie moderne qui se partage en deux types : le chiffrement symétrique (ou à clé secrète) et le chiffrement asymétrique (ou à clé publique) plus précisément RSA qu'est l'algorithme de chiffrement asymétrique le plus utilisé au monde mais nous savons que nous pourrons le casser une fois que les obstacles techniques à la construction d'ordinateurs quantique de grande taille auront été surmontés. Dans la derrière partie nous allons intéresser à une nouvelle classe de la

cryptographie qui est la cryptographie quantique plus correctement nommée distribution quantique de clés qui est basée sur les principes de la physique et la mécanique quantique utilisant le photon comme porteur d'information.

Dans le deuxième chapitre ,nous détaillerons une nouvelle approche qui est la distribution quantique de clé qui résout l'un des problèmes dans les communications sécurisées en exploitant les lois de la mécanique quantique afin de parvenir à une distribution de clés certifiées sécurisée entre deux participants, Mais en premier lieu ,nous nous intéressons au concept de la mécanique quantique qui est souvent considérée avec la théorie de la relativité comme une des plus grandes avancées scientifiques du XXe siècle. Dans la deuxième partie de ce chapitre, nous montrons quelques caractéristiques et mesure quantique. Dans la troisième partie, nous expliquerons les différents protocoles de distribution quantiques.

Le troisième chapitre, porte en première partie le logiciel OPTISYSTEM et quelques paramètres utilisés. Dans la seconde partie, l'analyse des protocoles à savoir : bb84 et six état et leurs simulation à une, deux, quatre polarisation sans attaque.

Dans le quatrième chapitre, Apres l'analyse effectuer d'échange quantique de clé du protocole BB84 et à six états. Nous allons voir maintenant d'autres expériences significatives qui montrent le fonctionnement de ses protocoles avec une attaque qui essaye de déborder des informations. Dans la dernière partie nous allons comparer entre ses deux protocoles.

Au finale une comparaison entre ces deux spéciaux protocoles dans la cryptographie quantique.

Le rapport est clôturé par une conclusion et des perspectives.

Cadre théorique

Chapitre I

Généralités sur la cryptographie

Introduction

Avec l'accélération indéniable de l'adoption de la digitalisation, une augmentation vertigineuse des échanges de données a été observée. En effet, nous assistons à une compétition sans précédent des géants d'Internet dans l'installation de la 5ème génération, par conséquent, la 4ème révolution industrielle arrive. Cependant, cette nouvelle ère de communication de données dans laquelle nous entrons plus vite que prévu est très vulnérable en matière de sécurité. En réalité, nous avons déjà atteint les centaines de millions d'objets connectés, voire même atteindre quelques dizaines milliards d'objets connectés d'ici quelques années.

Avant d'aborder le vif sujet, un bref historique sur l'évolution de cryptographie est utile voire même indispensable. Ainsi, une connaissance sur ses des différents types, suivie d'une énumération de ses divers avantages et inconvénients, sera faite dans ce chapitre. La dernière partie est consacrée à la présentation d'une nouvelle technique qui vient palier à un sérieux problème de cryptographie moderne à savoir le problème de distribution des clés.

I. 1 Concepts de base

1.1. Cryptologie

La cryptologie est un art ancien et une science nouvelle : un art ancien car Jules César l'utilisait déjà et il fit son apparition dans l'ancien testament sous la forme du code Atbash ; une science nouvelle parce que ce n'est que depuis les années 1970 qu'elle est devenue un thème de recherche scientifique, aussi est un mot composé qui tire son origine du grec : cryptos qui signifie secret et logique qui signifie science, et a été utilisé depuis des milliers d'années pour assurer les communications militaires et diplomatiques.

La cryptologie, étymologiquement <<la science du secret>>, ne peut être vraiment considérer comme une science que depuis peu de temps, cette science englobe la cryptographie [1].

1.2. Définition de la cryptographie

La cryptographie est l'art de chiffrer, coder les messages est devenue aujourd'hui une science à part entière. Au croisement des mathématiques, de l'informatique, et parfois même de la physique, elle permet ce dont les civilisations ont besoin depuis qu'elles existent le

maintien du secret. Pour éviter une guerre, protéger un peuple, il est parfois nécessaire de cacher des choses.

1.2.1. La terminologie

- ***Texte en claire*** *:* c'est le message à protéger.
- ***Texte chiffré :*** c'est le résultat du chiffrement du texte en claire.
- ***Clé:*** représente une valeur utilisée dans un algorithme cryptographique dans le but de chiffrer une donnée.
- ***Chiffrement :*** c'est la méthode ou l'algorithme utilisé pour transformer le texte clair en texte chiffré.
- ***Déchiffrement :*** c'est la méthode ou l'algorithme utilisé pour transformer le texte chiffré en texte clair [2].

1.2.2. L'usage de la cryptographie

La cryptographie est traditionnellement utilisée pour dissimuler des messages aux yeux de certains utilisateurs. Cette utilisation a aujourd'hui un intérêt d'autant plus grand que les communications via internet circulent dans des infrastructures dont on ne peut garantir la fiabilité et la confidentialité. Désormais, la cryptographie sert non seulement à préserver la confidentialité des données mais aussi à garantir leur intégrité et leur authenticité.

- ***La confidentialité*** *:* consiste à rendre l'information intelligible à d'autres personnes que les acteurs de la transaction.
- ***L'intégrité :*** vérifier l'intégrité des données consiste à déterminer si les données n'ont pas été altérées durant la communication.
- ***L'authentification :*** consiste à assurer l'identité d'un utilisateur, c.-à-d. de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être un contrôle d'accès peut permettre (par exemple par le moyen d'un mot de passe qui devra être crypté) l'accès à des ressources uniquement aux personnes autorisées.
- **Le non répudiation de l'information :** est la garantie qu'aucun des correspondants ne pourra nier la transaction.

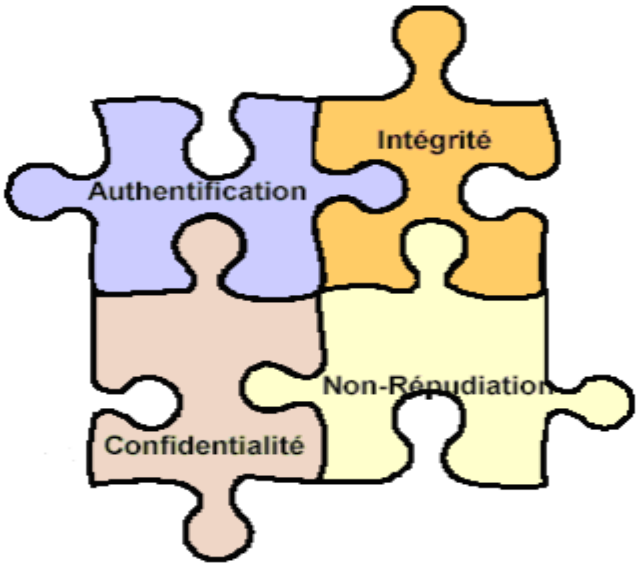


Figure 1.1 : Principaux objectifs de la sécurité.

La confidentialité est assurée par le chiffrement, par contre l'authentification, l'intégrité et la non répudiation sont vérifiées par une signature numérique ; qui est considérée comme étant une version électronique d'une signature manuscrite. Nous pouvons décrire cette signature comme un code rattaché aux données qui sert de preuve que le message n'a été trafiqué d'aucune sorte entre l'expéditeur et le destinataire. De ce fait, nous distinguons deux classes principales de cryptographies, à savoir : la cryptographie classique et la cryptographie moderne ainsi que la cryptographie quantique introduite récemment.

I. 2 Les types de chiffrement

On peut classer ces méthodes en trois grandes classes, comme nous le montre le schéma qui suit :

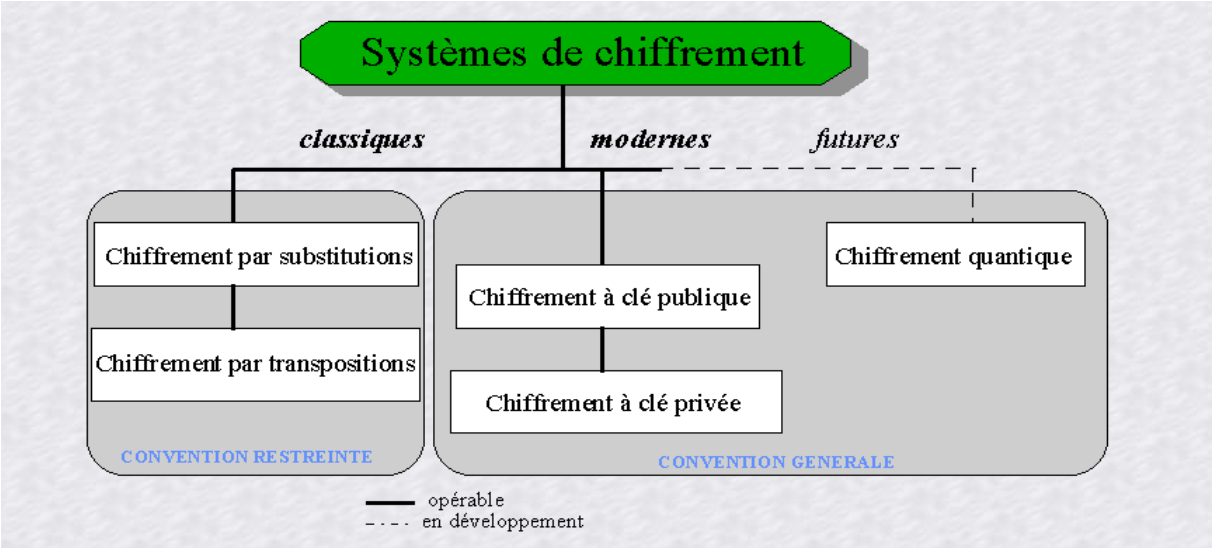


Figure 1.2 : Types de chiffrement.

1.3. Chiffrement classique

L'origine de la cryptographie classique remonte à l'antiquité jusqu'à l'apparition des ordinateurs, elle traite les systèmes qui reposent sur les lettres et les caractères d'une langue, son principe est de remplacer des caractères par des autres. La plupart des méthodes de la cryptographie classique s'appuient sur deux principes : la substitution et la transposition [3].

1.3.1. Le chiffrement par substitution

Est une technique de chiffrement très ancienne, nous identifions quatre types différents:

a) Substitution mono alphabétique : dans ce type de chiffrement, chaque caractère du texte clair est remplacé par un autre caractère dans le texte chiffré.

b) Substitution poly alphabétique dite aussi alphabets multiples : signifie qu'une même lettre du message peut être remplacée par plusieurs lettres.

c) Substitution par poly gramme : il opère sur les blocs de caractères, c'est-à-dire ; les caractères du texte clair sont chiffrés par bloc.

1.3.2. Le chiffrement par transposition

Les méthodes de cryptographie par transposition sont celles, pour lesquelles le chiffrement du message clair, se fait en permutant l'ordre de ses lettres suivant des règles bien définies de façon à les rendre inintelligibles.

1.4. Chiffrement moderne

La plupart des chiffrements classiques peuvent être calculés et résolus manuellement, contrairement aux chiffrements modernes qui s'intéressent généralement aux problèmes de sécurité. Dans cette section, nous allons présenter les principaux fondements de la cryptographie moderne à savoir le chiffrement symétrique et le chiffrement asymétrique.

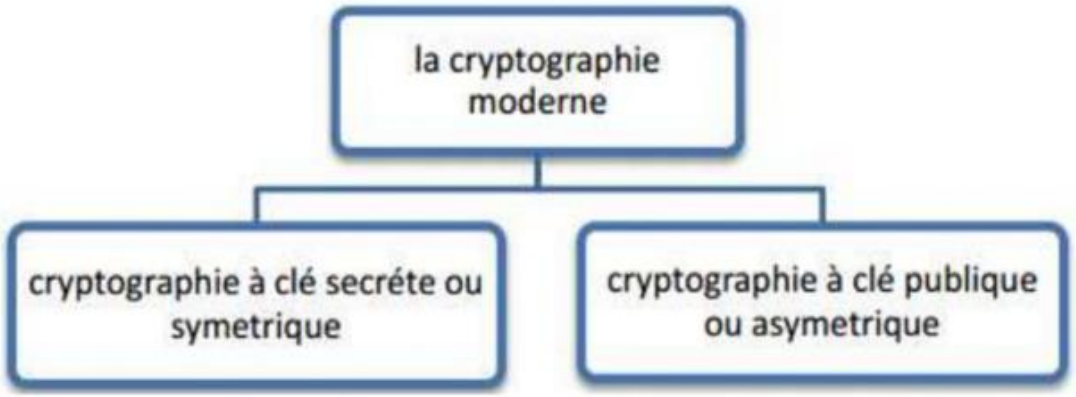


Figure 1.3 : les méthodes de la cryptographie moderne.

1.4.1. Cryptographie symétrique ou à clé secrète

Dans le chiffrement symétrique une même clé secrète est partagée entre les correspondants, comme le montre la figure 1.4, cette clé sert à chiffrer et à déchiffrer le message. Il est donc nécessaire que les deux interlocuteurs se soient mis d'accord sur une clé privée auparavant, ou ils doivent utiliser un canal sécurisé pour échanger la clé [4].

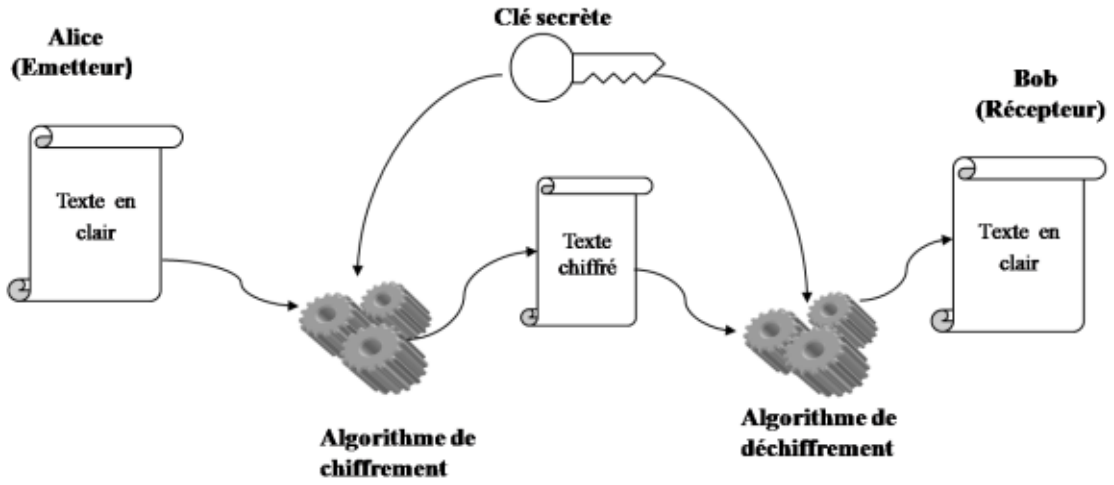


Figure 1.4 : Principe de la cryptographie symétrique.

A chaque fois que l'expéditeur veut transmettre un message au destinataire, il utilise la clé secrète pour chiffrer et il envoie le résultat de ce chiffrement. Le destinataire utilise à son tour la même clé secrète et le même algorithme pour déchiffrer le message. On distingue deux types de chiffrement:

a. ***Le chiffrement par bloc :*** dans ce chiffrement, il y a une séparation du texte clair en blocs d'une longueur fixe et un algorithme chiffre chaque bloc. La taille de ces blocs est essentielle pour la sécurité des communications, c'est-à-dire les grands blocs sont plus sécuritaires mais aussi plus lourds à transférer [5].

b. ***Le chiffrement par flux :*** ces algorithmes chiffrent les messages bit par bit quel que soit la longueur du message à coder sans besoin de les découper [6].

Avantage :

- Adapté au grand flux de données à chiffrer.
- Simple et facile à implémenter.
- La rapidité du système.
- Nécessite moins de bande passante.

Inconvénients :

- Nécessite la connaissance de la clé par l'émetteur et par le destinataire.
- Toute personne interceptant la clé lors d'un transfert peut ensuite lire ou même modifier ou falsifier toutes les informations cryptées.

➢ **Les exemples d'algorithmes symétriques :**

- DES (Data Encryption Standard) : utilise une clé secrète de 56 bits, la taille des blocs est de 64 bits. 3DES (Triple DES) : utilise une clé de taille comprise entre 128 et 192 bits. La taille des blocs est de 8 octets (64 bits).
- AES (Advanced Encryption Standard) : il travaille avec des blocs de 128 bits et il utilise des clés de 56 bits seulement.

1.4.2. Cryptographie asymétrique ou à clé publique :

Chaque correspondant possède deux clés, une est publique, et elle ne permet que de chiffrer un message et non pas de le déchiffrer, par contre la seconde clé est privée et ne permet que le déchiffrage, comme le montre la figure 1.5. Pour envoyer un message d'Alice à Bob, la procédure est la suivante : Alice se procure la clé publique de Bob, ensuite Alice utilise la clé publique de bob pour chiffrer le message confidentiel et envoie l'information à Bob, ce dernier utilise la clé privée pour déchiffrer le message [7].

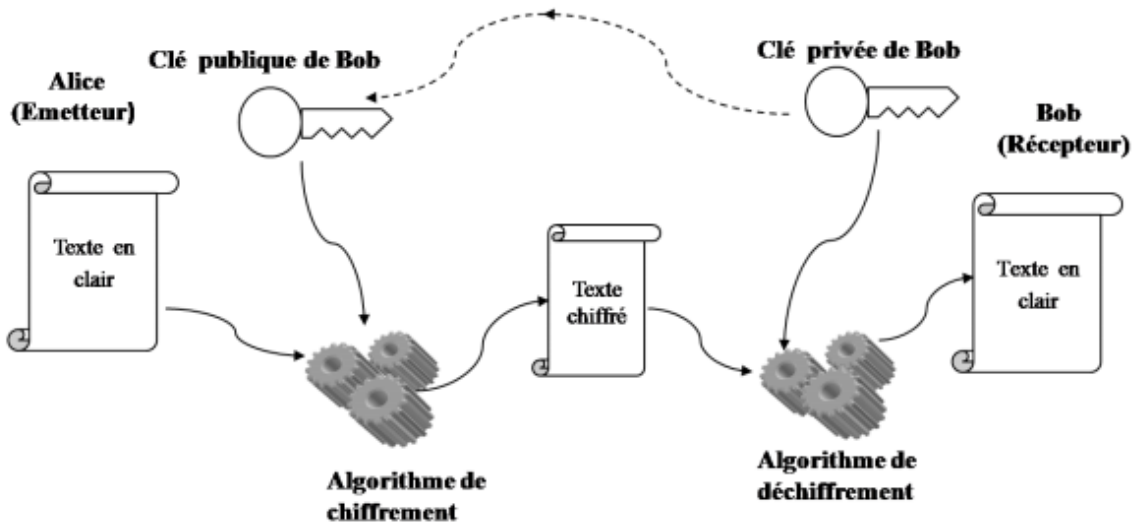


Figure 1.5 : Le principe de la cryptographie asymétrique.

Avantage :

- L'échange des messages de manière sécurisé.
- L'expéditeur et le destinataire n'ont plus besoin de partager des clefs secrètes via une voie de transmission sécurisée.
- Les communications impliquent uniquement l'utilisation de clefs publique et aucune clef privée n'est transmise ou partagée.

Inconvénients :

- Le traitement de données est lent et demande beaucoup de calculs.
- Assurance que la clé publique appartient bien à la personne à qui l'on souhaite communiquer les données chiffrées.

➢ ***Les exemples d'algorithmes asymétriques :***

RSA : l'acronyme RSA provient de Ron Rivest [8], Adi Shamir et Léonard Adleman, qui sont les inventeurs de cet algorithme. C'est les premiers systèmes cryptographie asymétrique fut inventé en aout 1977 couramment utilisé pour sécuriser les données sensibles, en particulier lors de leurs transmission via un réseau non sécurisé. Le RSA est basé sur la théorie des nombres premiers, sa robustesse tient du fait qu'il n'existe aucun algorithme de décomposition d'un grand nombre en facteurs premiers. Alors qu'il est facile de multiplier deux nombres premiers, il est très difficile de retrouver ces deux entiers si l'on en connait le produit, c'est le principe de fonction à sens unique c'est-à-dire que la multiplication de deux entiers est facile, mais l'opération réciproque, à savoir la factorisation d'un produit de deux entiers est difficile. La sécurité du R.S.A repose principalement sur l'incapacité à l'heure actuelle de reconstituer en un temps raisonnable la clé secrète en connaissant la clé publique.

➢ ***RSA et factorisation :***

En général, les attaques contre la cryptographie asymétrique peuvent être partagées en deux catégories : les attaques de nature mathématique, qui exploitent des relations mathématiques sous-jacentes, et les attaques d'implémentation, par exemple le fait d'exploiter les processus physique sous-jacents.

Dans le cas de RSA, il repose sur un problème mathématique difficile à résoudre pour un ordinateur classique. Ce problème est la factorisation des nombres, un ordinateur peut assez facilement calculer deux très grands nombres premiers et les multiplier .En revanche, essayer de retrouver les facteurs d'origine (la décomposition en facteurs premiers) du résultat est impossible à faire en pratique, il faudrait tout simplement des siècles (on parle ici de nombres extrêmement grands de l'ordre de 600 chiffres) [9,10].

I. 3 Comment on a passé du classique au quantique ?

En 1994, le mathématicien Peter Shor, travaillant au Massachusetts Institute of Technology (MIT), démontra que les ordinateurs quantiques sont capables de factoriser de grands nombres plus efficacement que les ordinateurs classique .En un mot, son algorithme se sert de la superposition quantique pour tester tous les nombres premiers en un seul cycle de calcul (un ordinateur classique le faisant l'un après l'autre).

Résultat, les algorithmes actuels mettraient des millions de millions d'années pour factoriser un nombre de 600 chiffres .un ordinateur quantique entièrement fonctionnel pourrait effectuer cette opération en quelques minutes. Donc les algorithmes modernes sont devenus vulnérables aux attaques. Aujourd'hui la recherche d'autres stratégies de cryptage est indispensable, La cryptographie quantique est une solution pour la sécurité de l'information dans l'avenir.

Elle résout donc, en se basant sur les règles de la mécanique quantique, l'une des plus importantes problématiques de la cryptographie classique, à savoir la distribution de clé. En effet, en cryptographie quantique, on utilise la polarisation du photon pour représenter l'information il s'agit du qubit au lieu du bit dans la cryptographie moderne [9] [10].

Conclusion

Ce chapitre est consacré pour la présentation des principes de la cryptographie et les techniques utilisées pour assurer la sécurité des systèmes de transmission. La cryptographie classique a été introduite depuis des siècles, elle est très limitée. La cryptographie moderne qui subdivise en deux types : celle à chiffrement symétrique et asymétrique qui sont longuement utilisées d'une manière efficace jusqu'à l'apparition des ordinateurs quantiques.

Enfin, nous terminerons par une introduction à la cryptographie quantique.

Chapitre II

Cryptographie quantique

Introduction

La mécanique quantique, est cette branche de la physique qui décrit la manière dont ce comportent les objets microscopiques. Dans le chapitre précèdent nous avons mentionné les faiblesses de la cryptographie classique, ce qui nous a mené vers la cryptographie quantique.

Cette nouvelle technologie est utilisée essentiellement pour communiquer une clé, et non le message car les bits d'informations communiqués par les dispositifs de la cryptographie quantique ne peuvent être qu'aléatoires.

L'objectif de ce chapitre est de discuter brièvement sur quelques concepts de la mécanique quantique. Nous nous intéressons ensuite au principe et quelques notion de la cryptographie quantique. Enfin Nous allons voir les protocoles de distribution de clé quantique les plus fonctionnels dans le domaine de la cryptographie en expliquant leurs fonctionnalités.

II. 1 Notion de la mécanique quantique

La mécanique classique a connu un large succès dans l'étude des phénomènes macroscopiques. Pour étudier certain phénomènes spécifique, relatifs à la structure de la matière microscopique: les molécules, les atomes, les électrons ou les particules en générale de la nano physique. La mécanique classique est incapable de les décrire, on fait donc appel à une nouvelle théorie c'est la mécanique quantique.

Cette dernière est apparue en XXème siècle, elle n'est pas une science intuitive, basée sur un formalisme mathématique dans l'espace d'Hilbert.

Au cours de cette section, nous énonçons quelques définitions de base de la physique quantique utiles en cryptographie quantique. [11]

1.5. Les systèmes quantiques

En mécanique quantique, un système physique donné est décrit par sa fonction d'onde ou son vecteur d'état $|\psi>$ qui une grandeur dans l'espace de Hilbert mené d'un produit scalaire hermitien positif.

Soit deux fonctions d'onde φ et ψ dans l'espace de Hilbert.

✓ ***Propriétés :***

$|\psi>$ Est appelé Ket, Et $<\varphi|$ appelé Bras.

L'action d'un bras $<\varphi|$ sur un Ket, $|\psi>$est donnée par le produit scalaire suivant :

- $$<\varphi|\psi>=\int \varphi*.\psi.dV \quad (1.1)$$

- $$(<\psi|\varphi>)^* = <\varphi|\psi> \quad (1.2)$$

- $$<\psi|\psi> = 1 \quad (1.3)$$

- Le module d'un état est défini par :

$$\|\psi\| = \sqrt{<\psi|\varphi>} \quad (1.4)$$

1.6. État quantique

L'état $|\psi>$ d'un qubit isolé est défini par l'observable associée à l'énergie du système, selon l'équation de Schrödinger :

$$i\hbar \frac{d|\psi(t)>}{dt} = H^{1}(t)\,|\psi(t)> \quad (1.5)$$

Avec H est un opérateur hamiltonien, et $\hbar$ la constante de Planck réduite qui est égale à h/2π. h=6.62.10^{-34} J/S.

II. 2 Principe générale de distribution quantique de clé

2.1 Principe d'incertitude de Heisenberg

Dans le monde de la mécanique quantique, une particule ne pourra jamais avoir une position et une vitesse avec précision au même temps.

2.2 Théorème de non-clonage

En 1982, Wooters et Zurek démontrèrent qu'il est impossible de concevoir un cloneur quantique qui puisse copier et cloner parfaitement et librement l'information quantique d'un système à un autre, c.-à-d. qu'il n'est pas possible de copier un photon de manière à obtenir deux photons identiques. En contrepartie, cette opération est réalisable en monde de l'information classique.

II. 3 La cryptographie quantique

La cryptographie quantique ou la distribution de clé quantique permet l'échange d'une clé secrète entre un émetteur habituellement appelé Alice et un récepteur nommée Bob, en utilisant deux canaux tel qu'il est présenté sur la figure2.1, un canal quantique qui peut être la fibre optique ou l'air libre. Le second est un canal classique.

Les protocoles de distribution de clé quantique utilisent les photons comme porteurs d'information constituant la clé secrète selon deux types d'encodage. Le premier type est défini par l'encodage à base des variables discrètes qui utilise deux types de transmission de qubit, une transmission directe par des photons uniques ou une transmission intriquée par des paires de photons intriqués. Par contre le second type d'encodage est l'application des variables continues.

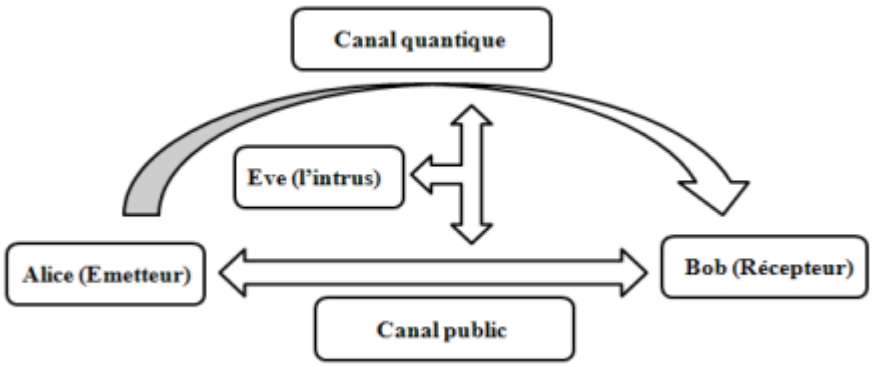


Figure 2.1 : un système de distribution de clé quantique.

3.1 Photon

La théorie quantique décrit la lumière comme une particule appelée Photon, sachant que la lumière est un rayonnement électromagnétique ou un transfert d'énergie sous la forme d'onde électromagnétique .cette onde se déplace dans l'espace selon une direction donnée comme son nom l'indique .d'un champ électrique ainsi magnétique qui sont perpendiculaires entre eux et leurs contenus dans un plan perpendiculaire à la direction de propagation de l'onde EM .En 1992, Nobel a proposé que la lumière soit constitué de quanta appelés photon qui ont une énergie et une quantité de mouvement bien définies.

Jusqu'au 20 e siècle, on a cru que la lumière était une onde mais les théories et les expériences ont montré qu'on pouvait aussi la traiter comme une particule dénuée de masse.

3.2 Polarisation

La polarisation de la lumière découle de la théorie ondulatoire de la lumière qui correspond à la direction et à l'amplitude du champ électrique. Cette polarisation correspond à donner une trajectoire définie au champ, si la lumière a une polarisation constante donc on dit qu'elle est polarisée.

Ce phénomène peut être appliqué à un photon individuel puisque 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 dans le plan perpendiculaire à la direction de propagation du photon.

3.3 Bit quantique (qubit)

En informatique classique, le terme bit est une contraction des mots binary digit il désigne l'unité la plus simple utilisée dans système de numération, on encode l'information grâce à des bits pouvant être soit des 0, soit des 1. En informatique quantique, on va utiliser des qubits ou un bit quantique qui représente la plus petite unité de stockage de l'information quantique. Il représente soit un 0 ou 1, soit une combinaison de 0 et 1 en même temps. Ces qubits sont représentés par des particules gouvernées par les lois de la mécanique quantique.

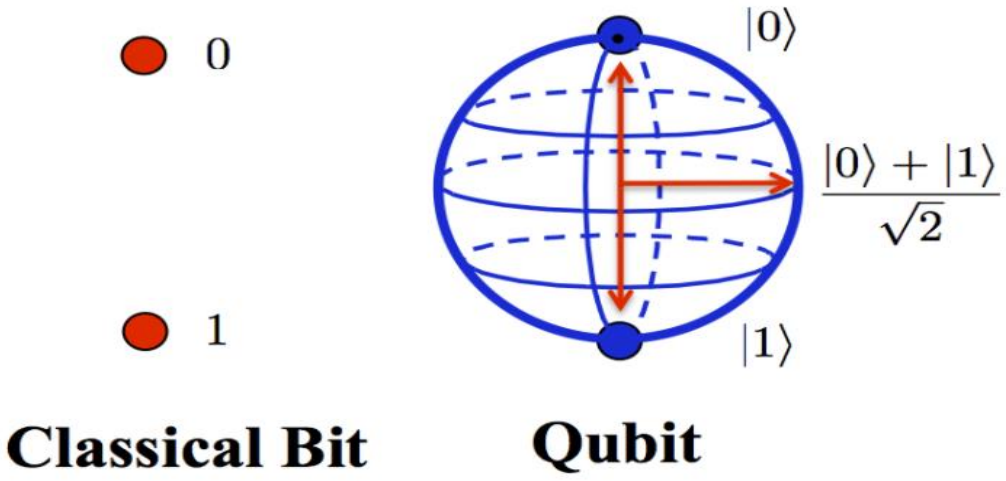


Figure2.2 : Le bit classique et le bit quantique.

3.4 Transmission de la clé

La transmission ou le partage de la clé consiste à transmettre une sérié de bits aléatoires (0 ou 1) .Alice transmit a Bob chaque bit en choisissant aléatoirement une des deux polarisations possible :

Base rectiligne : consiste à envoyer un photon polarisé à 0° pour un qubit 0 et à 90° pour le qubit 1.

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

3.5 Propriétés des qubits

Les deux propriétés les plus importantes qui sont utilisées :

3.5.1 La superposition

Le qubit peut se trouver dans l'un des deux états de base |0> ou |1> cette notation est appelée <<notation de Dirac>> .Dans la base rectiligne l'état |0> sera associe à l'état de polarisation horizontale et l'état |1> à l'état de polarisation verticale.

Le bit quantique peut se trouver dans n'importe quel état intermédiaire, qui est exprimé par une superposition de ces deux états.

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \quad (1.6)$$

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

3.5.2 L'intrication

Dans un système quantique, elle permet de relier les qubits entre eux pour les synchroniser et notamment ce qui permet d'en faire des copies mais sans pouvoir en lire leur contenue ni les modifier de manière indépendante.

II. 4 Principe de la cryptographie quantique

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

La cryptographie quantique repose sur l'utilisation de deux canaux. L'un est obligatoirement quantique. Capable de transmettre des objets régis par les lois de la mécanique quantique (par exemple un photon transmis par fibre optique), le second est un canal classique qui peut être écouté par Eve, mais qu'elle ne peut modifier. Il est impossible d'empêcher Eve d'écouter discrètement le canal quantique, mais il est possible de le savoir.

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

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

4.1 Le canal quantique

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

4.2 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.

Figure 2.3 : les systèmes de communication quantique.

II. 5 Les protocoles de la cryptographie quantiques

5.1 Le protocole bb84

C'est le premier protocole pour la cryptographie de quantum, présenté par Bennet et Brassard en 1984 [12,13].le but de ce protocole est de permettre à l'expéditeur nommé Alice et au destinataire nommé Bob d'échanger une clef aléatoire .Lorsque l'information digitale est encodée par les systèmes primitifs il s'agit d'une méthode standard qui consiste à coder une information via la polarisation de photons simples, il est en principe possible de créer un canal de communication sur lequel un espion quelconque ne peut pas gagner l'information sans perturber la transmission de façon aléatoire et incontrôlable .

Dans ce protocole, on utilise un photon single pour présenter un bit d'information 0 et 1 .les état de polarisation de photon appartiennent à deux bases conjuguées, qui sont la base rectilinéaire B+= {|0+>, |1+>}, et la base diagonale ou circulaire Bx= {|0+>, |1+>} pour fournir les bases conjuguées.

On utilise dans ce cas les deux bases linéaires :

- La base rectiligne :{0 :|H>, π/2 :|V>}, H : Horizontale, V : Verticale
- La base diagonale :{ π/4 :|A> ,3 π/4 :|D>}, A : anti-diagonal, D : diagonal.

En outre, la mise en œuvre du protocole nécessite deux canaux, un canal de transmission quantique et un canal public (radio, internet). Les détails du protocole sont donnés comme suit :

1. Alice génère des états de polarisation ou qubits de façon aléatoire, puis il envoie une suite de photons polarisées à Bob par un canal quantique.
2. Bob reçoit les photons et chacun décide, indépendamment de l'autre, d'effectuer une mesurer sur les polarisations avec une probabilité 1/2, suivant la base B+ ou B×.
3. Alice et Bob comparent leurs bases en utilisant un canal de communication classique, puis ils rejettent tous les cas où Bob n'a pas fait le bon choix comme Alice. Cette opération est connue sous le nom de la réconciliation des bases.
4. Alice et Bob vérifient la présence d'un espion, en comparant et en sacrifiant quelques résultats publiquement, aussi les résultats sont choisis au hasard parmi toutes les données de l'étape 3.
5. Si le test de comparaison montre qu'il y a eu la présence évidente de l'espion, ils rejettent les données échangées et reviennent à la première étape. Sinon, ils conservent les données de l'étape 4. Ces données construisent la clé secrète qui n'est connue que par Alice et Bob.
6. En fin de communication, il y a toujours des erreurs qui sont introduites par le canal quantique et peut être par Eve. Ainsi, Alice et Bob utilisent des techniques classiques pour augmenter la sécurité et corriger ces erreurs.

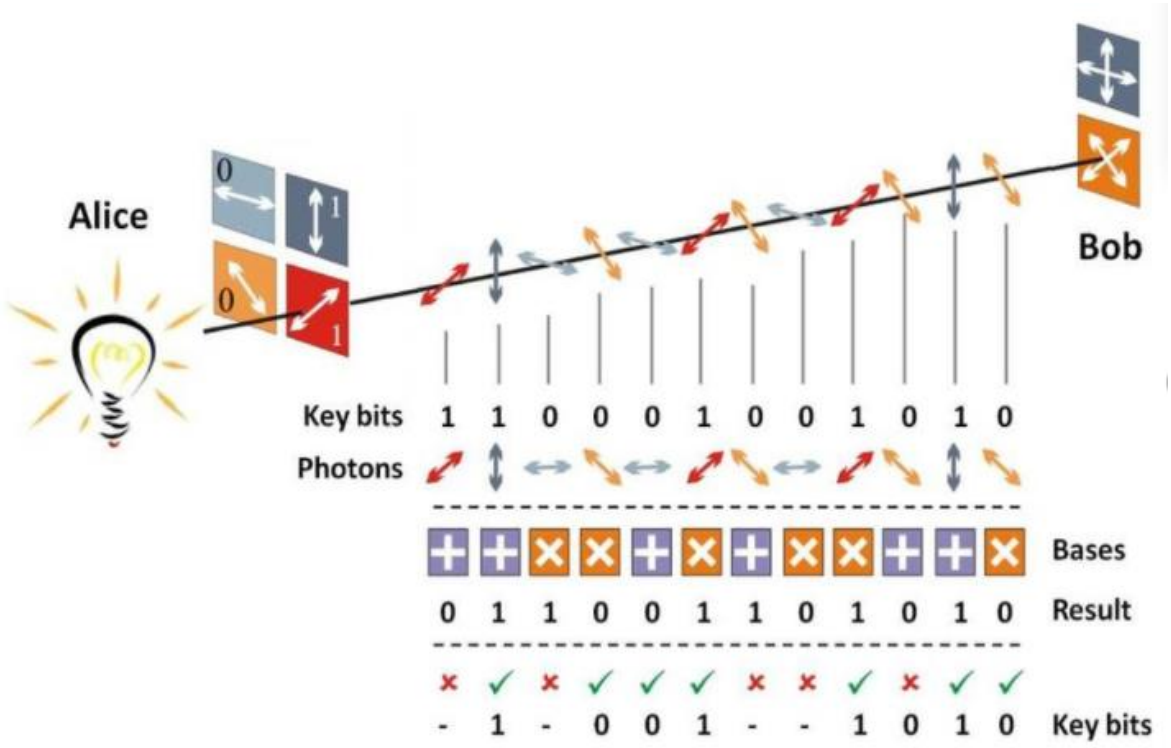


Figure 2.4 : Le protocole BB84.

5.1.1 Les sources à photon unique

On définit par une source de photon unique tous dispositif capable d'émettre des impulsions lumineuses contenant un et un unique photon. Ces sources se différent de l'une par rapport à l'autre selon l'application visé. Alors le choix de la source est fondé sur des critères d'évaluation importantes de sorte à avoir un photon unique à la demande et de garantir la sensibilité du canal quantique à toutes tentative d'écoute de l'espion Eve, en exploitant les impulsions vide ou bien les impulsions multi photoniques qui constituent une véritable fuite d'information.

On obtient alors une source cohérente atténué émettant des impulsions très fortement atténué ne contenant en moyen qu'un photon par impulsion .Dans ce cas, la distribution de photon dans chaque impulsion suit une loi de poisson, en fonction du nombre de photon (n) et du nombre moyen de photon μ par impulsion.

$$p(n,\mu) = \frac{\mu^n . e^{-\mu}}{n!} \quad (1.7)$$

En réduisant le nombre moyen de photon par impulsion à μ=0,1.

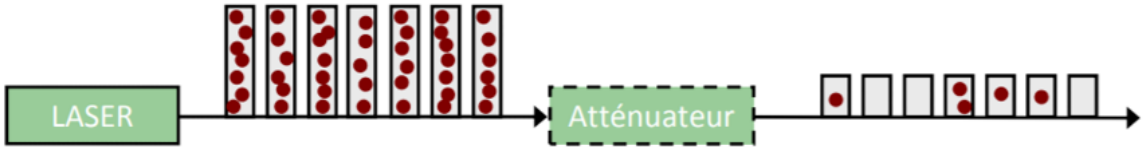


Figure 2.5 : Source Laser atténué.

5.2 Protocole à six états

Ce protocole est proposé par Brub [7].En 1999 Pasquinucci et Gisin proposèrent dans leur article « *Incoherent and coherenteavesdropping in the six-state protocol of quantum cryptography* », un protocole qui est considéré comme une amélioration du protocole BB84 à quatre états, avec deux états de polarisation supplémentaire représenté sur une base circulaire ($|\circlearrowright>, |\circlearrowleft>$), leurs expressions sont données par (1.7). Ce protocole est nommé le protocole à six états (SSP).

Lors de la représentation du protocole à six états sur la sphère de Poincaré, les deux états supplémentaires correspondent à l'axe ± Z, de ce fait les six états sont selon les trois axes suivant ±x, ± y et ± z comme est représenté sur la figure2.6.

$$|\circlearrowright>= \frac{1}{2}\,(|0> +|1>)$$

$$|\circlearrowleft> = \tfrac{1}{2}\,(|0> -|1>) \quad (1.7)$$

On utilise dans ce cas les deux du protocole BB84 linéaires plus la base circulaire:

- La base rectiligne :{0 :|H>, π/2 :|V>}, H : Horizontale, V : Verticale
- La base diagonale :{ π/4 :|A> ,3 π/4 :|D>}, A : anti-diagonal, D : diagonal.
- La base circulaire : Emetteur : {0 :|R>,1 :|L>}, R : droite, L : gauche.
- Récepteur : {1 :|R>,0 :|L>}, R : droite, L : gauche [14].

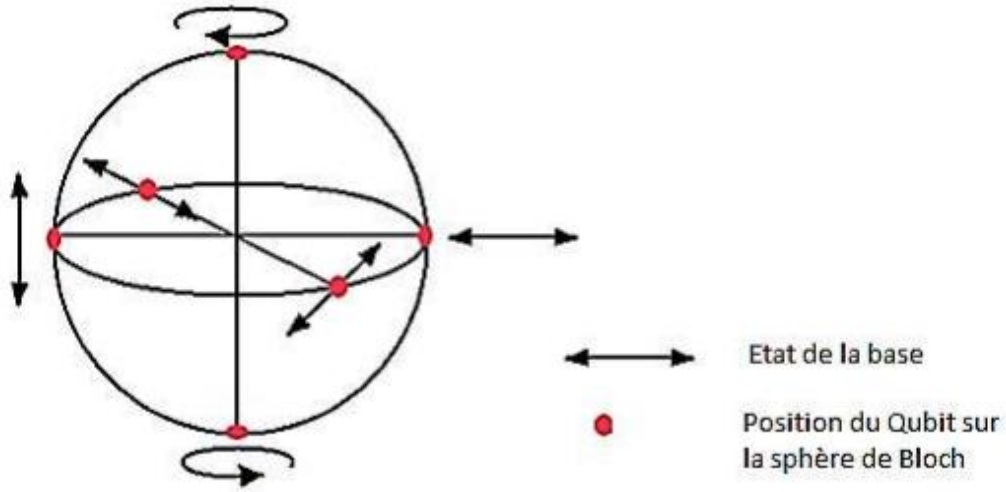


Figure 2.6 : Trois paires de bases utilisées dans le protocole à six états.

5.3 Protocole B92 (à deux états) :

Après la publication du premier protocole de distribution de clé quantique, Bennett réalisa qu'il fut possible d'encoder les états du BB84 sur la phase relative de la lumière. En 1992, il présenta une version simplifiée du Protocole BB84 dans son article « *Quantum cryptography using two non-orthogonal states* », il le nomma le protocole B92.

Le protocole B92 peut être décrit dans un système d'Hilbert à deux dimensions. Il utilise la phase des photons pour coder les bits 0 et 1 sur deux états non orthogonaux de deux bases conjuguées. Le bit 0 est codé dans la base rectilinéaire à 0˚ et le bit 1 est encodé sur 45˚ dans la base diagonale, comme il est illustré sur la figure 2.7.

Le principe et la procédure du protocole B92 est identique à celui du protocole BB84. A l'émission, Alice choisit une séquence binaire aléatoire qu'elle code sur la phase du photon. Présentant une différence par rapport au BB84, où Alice annonce à Bob qu'elles sont les bases de mesure à utiliser. Néanmoins, à la réception des qubits, Bob les mesure dans des bases au hasard qui en résulte deux cas : Si le choix est différent, aucune mesure ne sera effectuée et le qubit sera ignoré. Mais si le choix coïncide et les données d'Alice et Bob sont corrélées, alors le qubit sera conservé et contribuera à construction de la clé secrète.

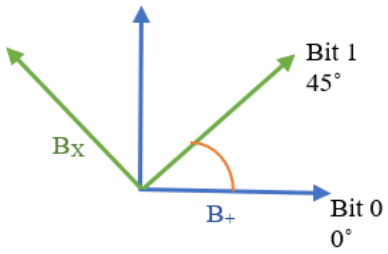


Figure 2.7 : Les bases de polarisation du protocole B92.

Conclusion

La cryptographie quantique est un sujet d'actualité qui recouvre un très large choix de compétences. Elle est introduite pour résoudre le problème d'échange de clef dans le système de clef secrète. Cette technique est structurée sur une belle combinaison des concepts de la physique quantique dans le sens qu'elle applique la mécanique quantique sans autre moyen technologique, elle montre comment les photons peuvent être utilisés pour transmettre de l'information.

Notre objectif dans ce chapitre de présenté les protocoles de distribution le plus connu qui ont été développés. Donc la distribution quantique de clés est l'avenir du monde de la cryptographie.

Cadre pratique

Chapitre III

Implémentation des protocoles BB84 et à six états sur OptiSystem sans attaque.

Introduction

La distribution quantique des clés est une méthode permettant de produire une clé secrète partagée par deux utilisateurs distants. L'avantage des protocoles de distribution quantique de clés est qu'il est possible de prouver la sécurité inconditionnelle des clés produites.

Dans ce chapitre nous allons présenter en premier le logiciel OPTYSYSTEM et quelques paramètres utilisés pour notre étude. Puis nous allons simuler les protocoles de distribution de clé à savoir : le protocole BB84 et le protocole à six états les plus fonctionnels dans le domaine de la cryptographie.

III. 1 Logiciel OPTISYSTEM :

Le logiciel OptiSystem développé par une société canadienne Optiwave (Optical Communication System Design Software) [15], il permet aux ingénieurs et aux chercheurs de concevoir, de simuler et d'analyser des systèmes de transmission optique. La diversité des systèmes simulés peut être étendue par la possibilité d'insérer des fonctions réalisées par l'utilisateur et qui peuvent être ajoutées au système simulé. En plus sa vaste bibliothèque de composants permet introduire les différents paramètres de simulation. Il comporte également les outils de mesure et de visualisation. Le logiciel OPTISYSTEM permet de tester et optimiser pratiquement n'importe quel type de liaison optique réel.

III. Les paramètres de l'OptiSystem :

Le logiciel OptiSystem comporte plusieurs sources optiques, dont on va citer juste ce qu'on a utilisé:

- ***Le laser (CW):***

La source laser à semi-conducteurs (CW) doit fournir une lumière continue dans une bande passante étroite et spécifique qui transporte des données numériques modulées par un signal analogique.

- ***Atténuateur optique (Optical attenuator)***

L'atténuation est un mécanisme de QKD pour obtenir un niveau de photon unique d'impulsion**,** A pour rôle de laisser un seul et unique photon passeras.

- ***le polariseur linéaire (Linear polarizer) :***

Est un compteur de photon pour visualiser l'état du photon reçu sue l'une des deux bases choisies aléatoirement.

- ***Switch (Select) :***

L'un des 4 états de polarisation sera choisi aléatoirement par un sélectionneur et l'envoie sur une fibre optique.

- ***Fibre optique :***

OptiSystem dispose d'un ensemble de fibres optiques dans lesquels on peut changer la longueur, la dispersion et l'atténuation ainsi que le type de la fibre.

2.1 Les paramètres de Stocks

Les paramètres de stockes affichent quatre valeurs dérivant l'état de polarisation du photon, leurs valeurs sont présentées sous forme normalisée comme S1, S2, S3 tandis que S0 est présenté dans unité [dbm] où chaque paramètre correspond à une différence de puissance.

S0 : représente la puissance totale transportée.

S1 : est la différence de puissance 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.

2.2 La sphère Poincarré

Le principe de cartographie sur la sphère de Poincaré est basé sur la projection du vecteur de stockes éléments aux axes des systèmes de coordonnées cartésiennes (X, Y, Z), plus elle offre un large éventail de capacités .Le SOP (Observable Polarizarion Sphere) particulier est projeté sur la surface de la sphère de Poincaré, il correspond aux angles particuliers d'ellipticité et d'azimut d'ellipse de polarisation, ces entités représente les amplitudes non observables du champ optique [16] [17].

III. 3 Le protocole BB84et le protocole à six états sans attaque

Dans cette partie du travail, on présentera l'implémentation du protocole BB84 et le protocole à six états sur OptiSystem.

Durant l'implémentation de ces deux protocoles, plusieurs paramètres doivent être pris en considération. On utilise quatre diodes laser à une longueur d'onde de 1550nm chacune est reliée à un atténuateur optique réglé à 0.1dB (loi du poisson) .par la suite, chaque photon est polarisé par un polariseur (0°,90°,45°,-45°) dans le protocole BB84 et le photon dans le protocole à six états est polarisé par un polariseur (0°,90°,45°,-45°, circulaire à gauche et circulaire à 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 (10km) vers le coté du récepteur. Au niveau du récepteur, nous implémentons le switch qui va choisir aléatoirement la polarisation linéaire ou de la polarisation diagonale et le résultat qui sera affiché sur l'analyseur de polarisation.

3.1 Le protocole BB84

3.1.1 La simulation avec une seule polarisation

Dans cette partie, nous avons choisi un seul canal qui émet une seule polarisation à (90°) comme est présenté dans la figure3.1.

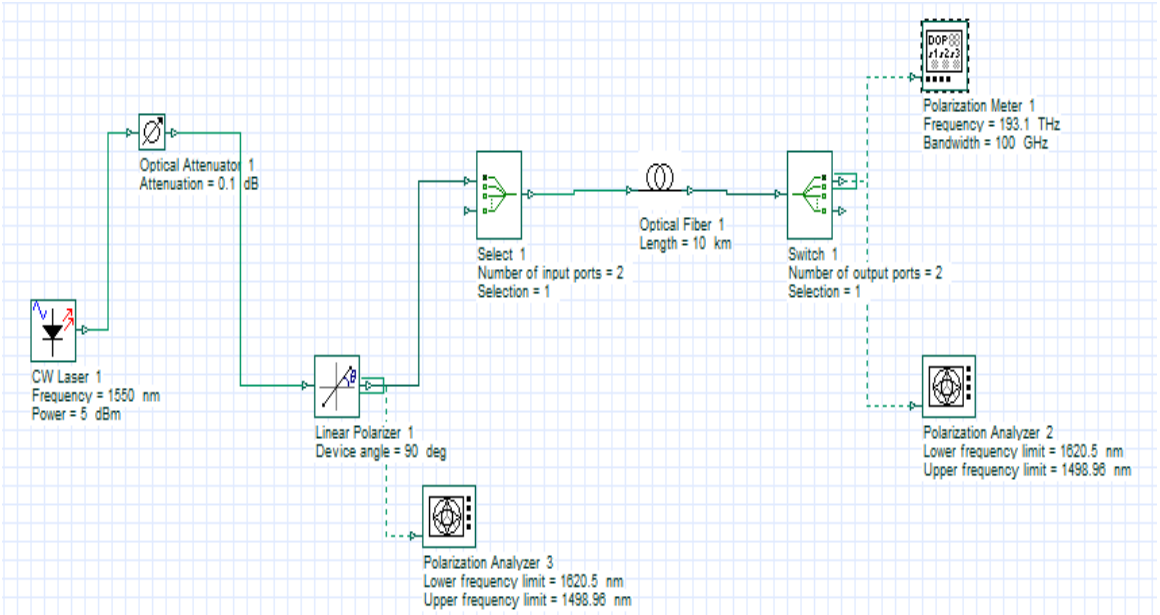


Figure 3.1 : simulation de BB84 pour une seule polarisation.

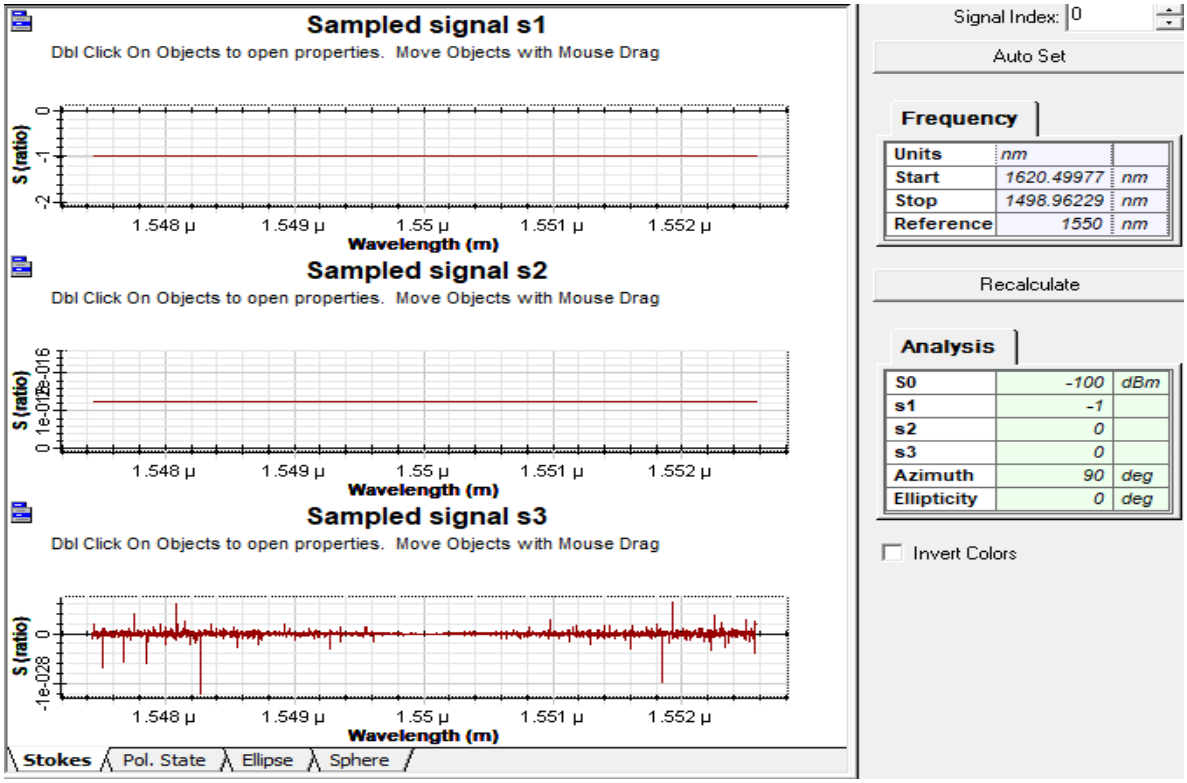


Figure3.2 : paramètre de Stockes obtenus de l'émetteur.

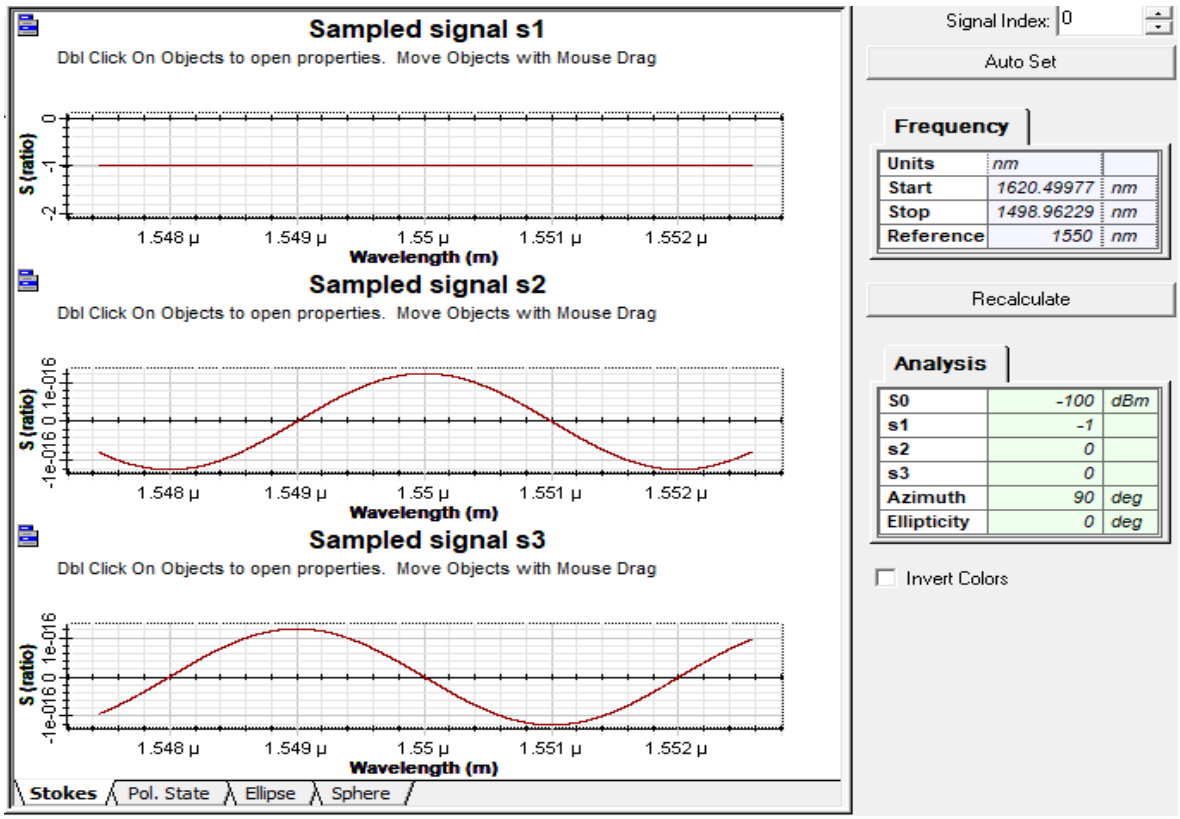


Figure 3.3 : paramètre de Stockes obtenus du récepteur.

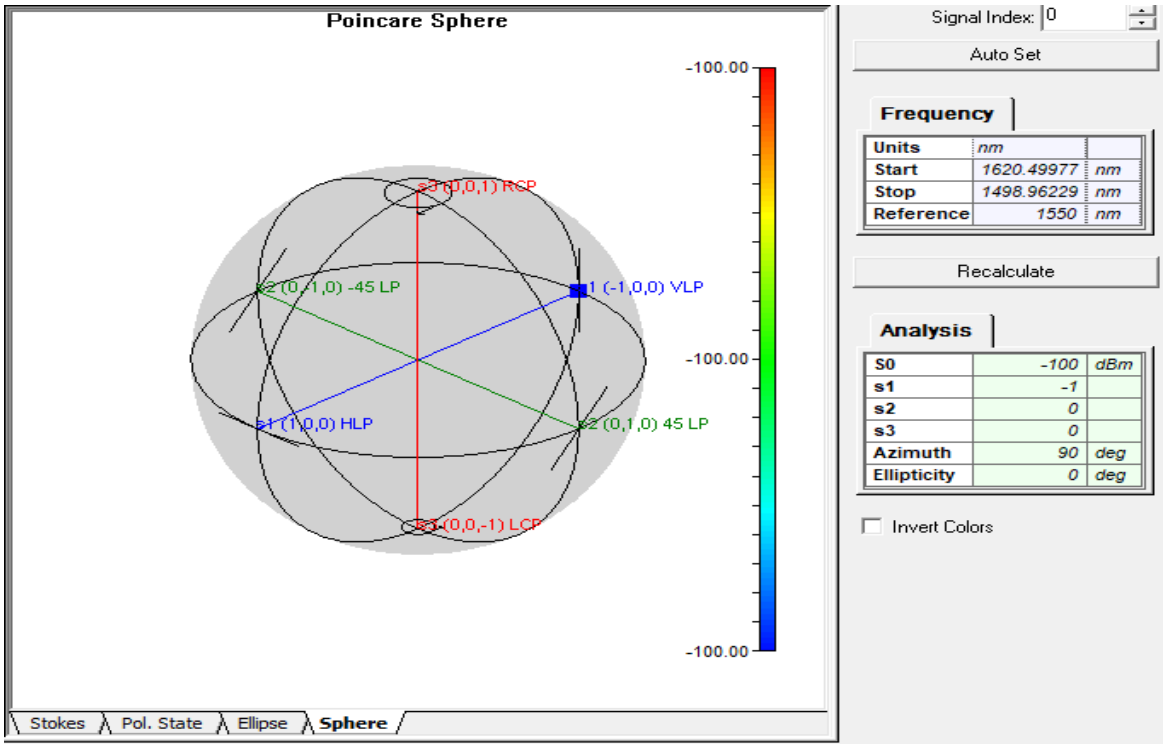


Figure 3.4 : les paramètres de Stockes de la sphère Poincaré.

➢ ***Commentaire***

Dans cette simulation nous avons obtenu S1=-1 ; S2=0; S3=0. Ces paramètres caractérisent l'angle 90°.

En comparant les résultats au niveau de l'émetteur tel qu'il est représenté dans la figure3.1 et au niveau du récepteur tel qu'il est illustré sur la figure 3.3, nous constatons que les polarisations sont identiques.

3.1.2 La simulation avec deux polarisations

La figure ci-dessous montre une simulation a deux polarisions diagonale et anti diagonale :

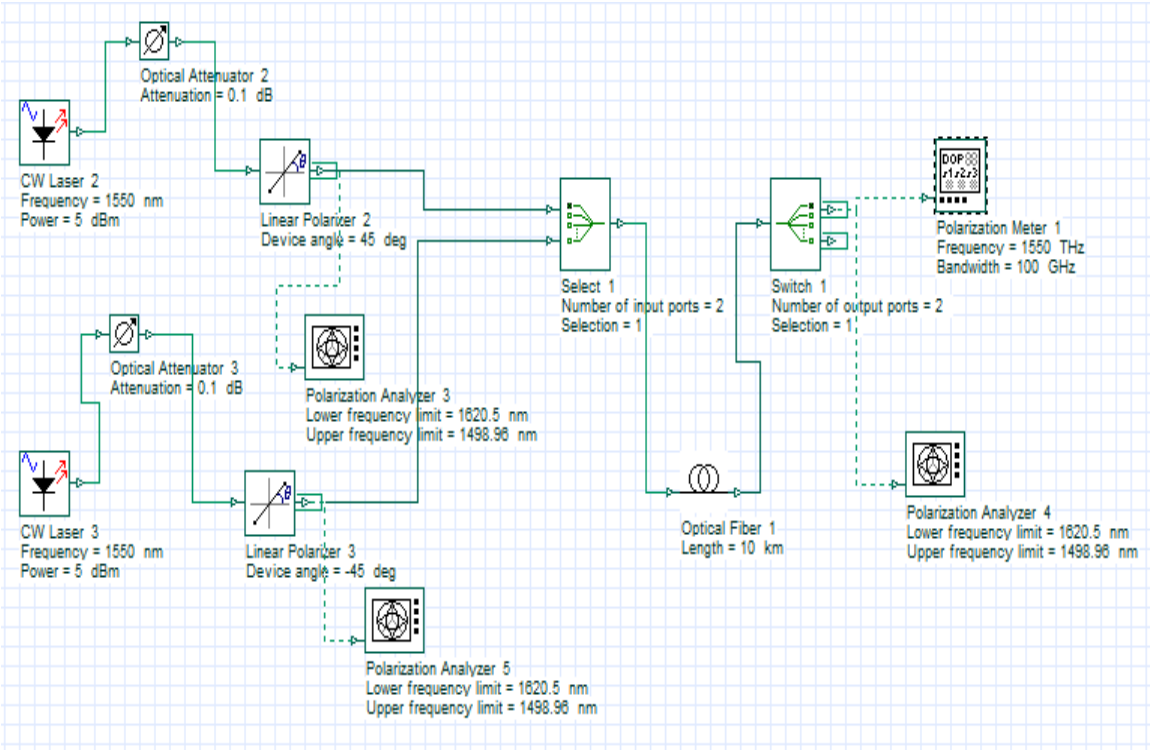


Figure 3.5 : Simulation de BB84 pour deux polarisations.

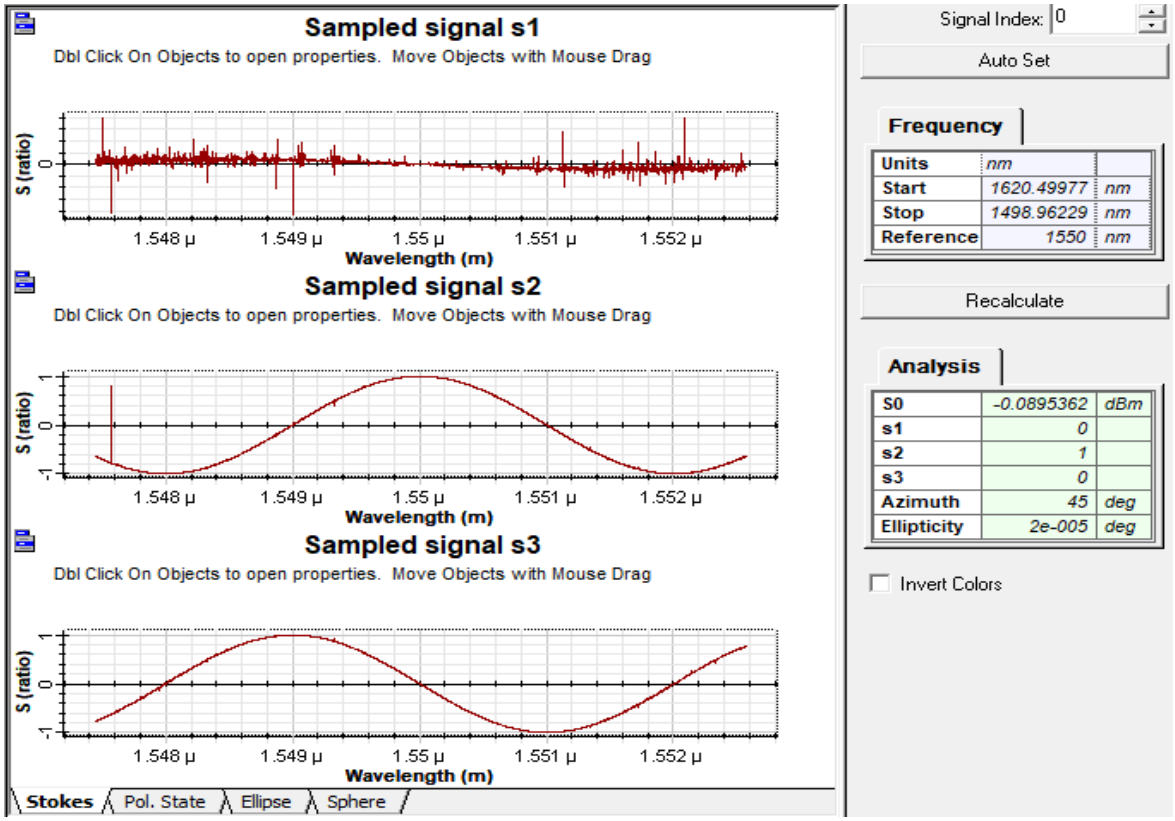


Figure 3.6 : les paramètres de Stockes du récepteur.

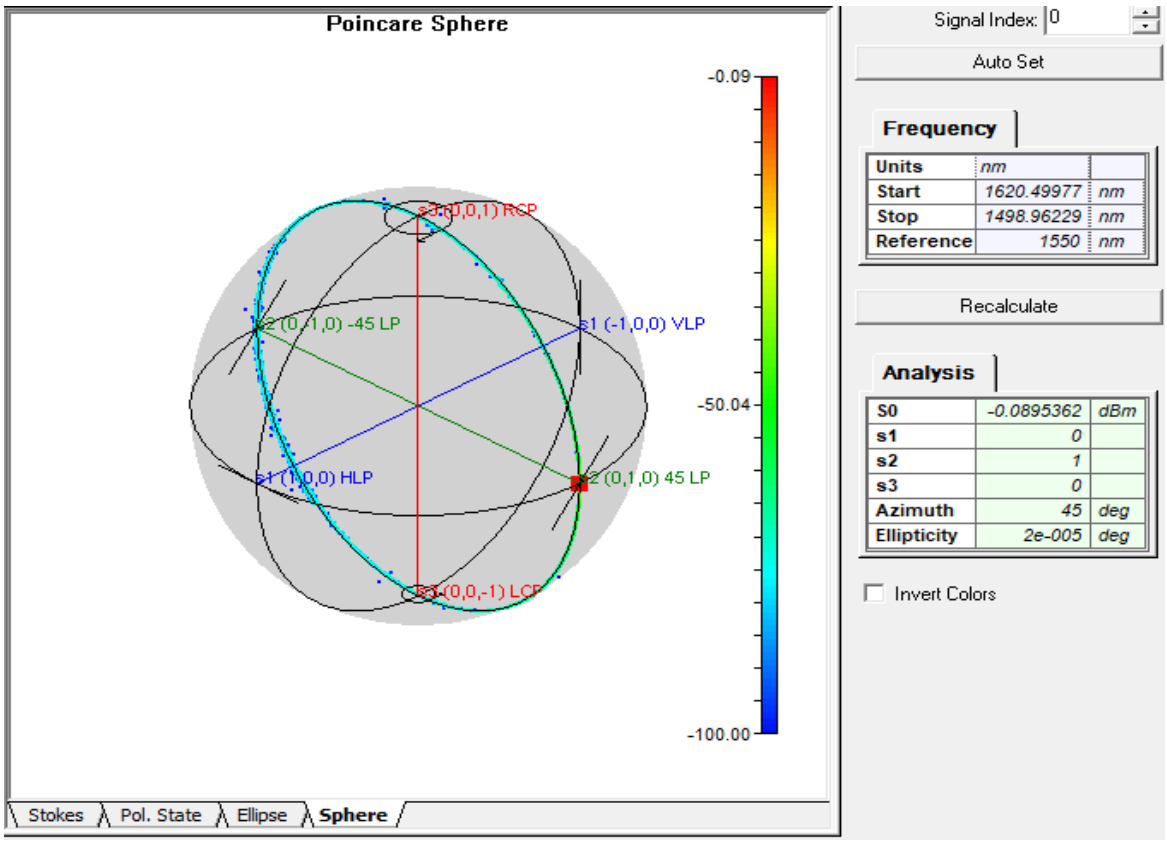


Figure 3.7 : la sphère de Bloche.

- ***Commentaire***

Dans cette partie nous avons utilisé à l'émission deux polarisation 45° et -45° tel qu'il est représenté sur la figure 3.5, on a obtenu S1=0 ; S2=1 ; S3=0. Ces paramètres caractérisent l'angle 45°.

En comparant les résultats au niveau de l'émetteur et du récepteur. Au niveau du destinataire on a obtenu le résultat d'une seule polarisation choisie aléatoirement qui est identique à celle de 45°.

3.1.3 Simulation avec quatre polarisations

Dans la figure ci-dessous, nous avons implémenté le protocole à quatre états :

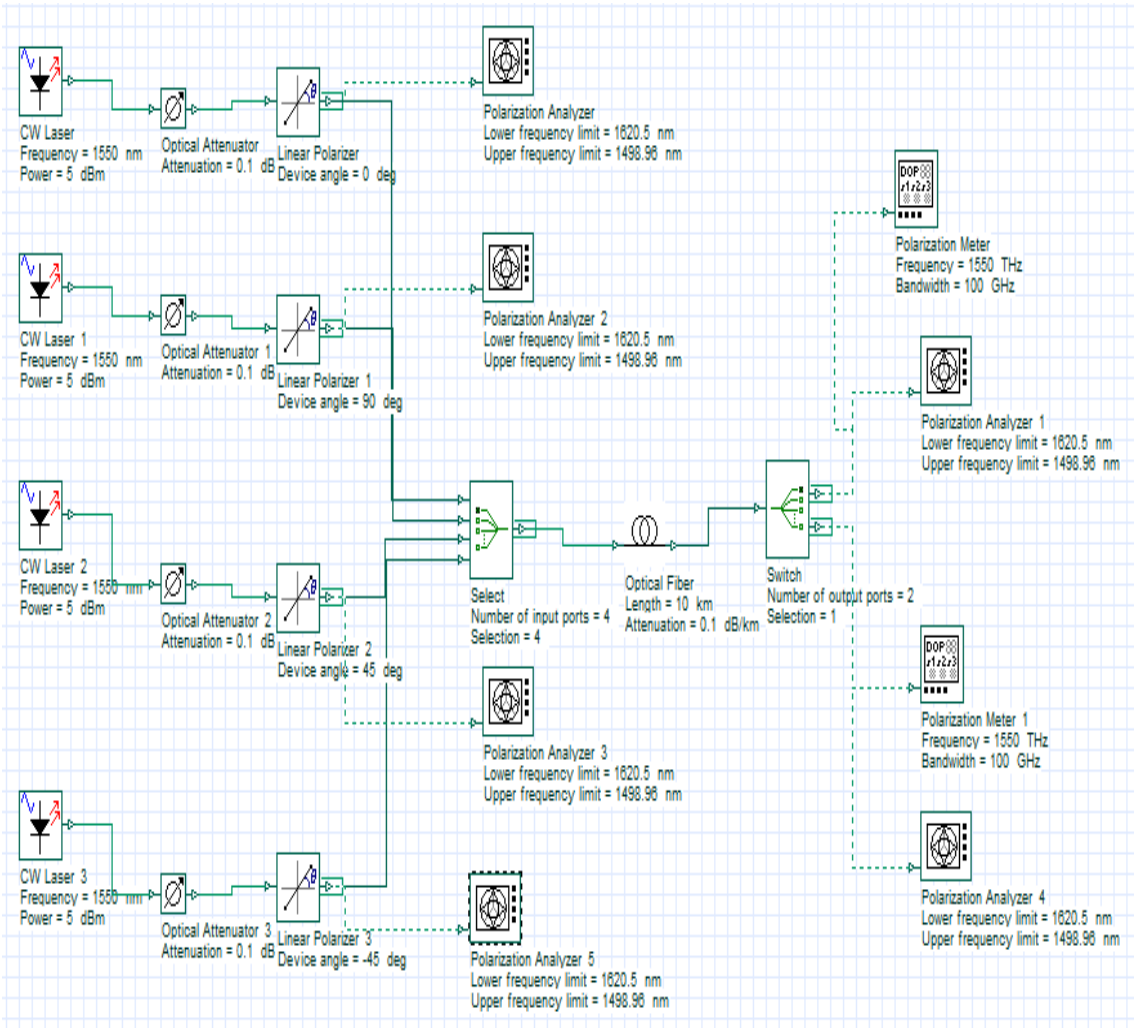


Figure 3.8 : Simulation de BB84 pour quatre polarisations

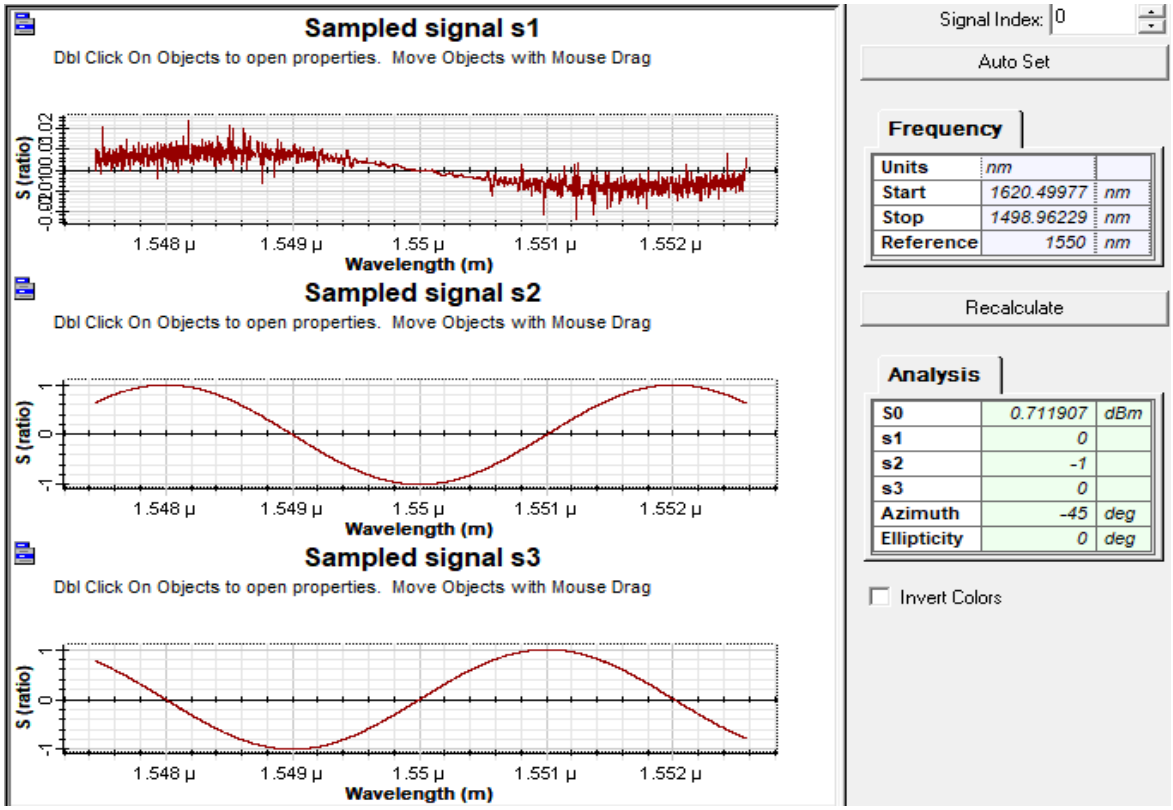


Figure 3.9 : les paramètres de Stockes au niveau du récepteur.

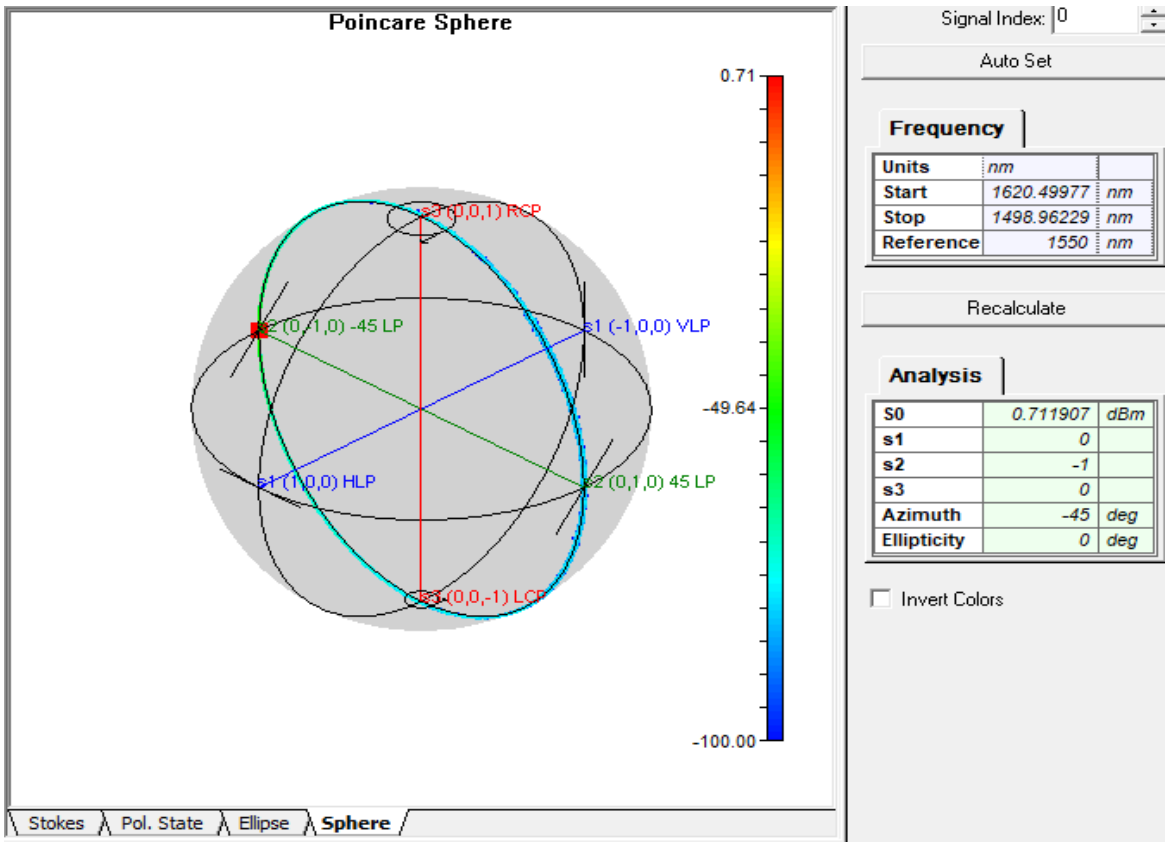


Figure 3.10 : La sphère de bloche.

- ***Commentaire :***

Dans cette partie on a simulé le protocole BB84 à quatre états de polarisation (0° ; 90° ; 45° ; -45°) tel qu'il est représenté sur la figure 3.8, on a rajouté un sélectionneur d'états. Et au niveau du récepteur, on a utilisé un switch avec deux ports. Chaque port est relié à un compteur et un analyseur de polarisation, le résultat s'affichera d'une façon aléatoire sur l'un des analyseurs.

Nous remarquons que le premier analyseur de polarisation au niveau du récepteur choisit aléatoirement la polarisation anti diagonal avec les paramètres de Stockes suivant : S1=0; S2=-1 ; S3=0, comme est représenté dans les deux figures (figure 3.9 et figure 3.10).Alors le deuxième analyseur n'affiche aucun résultat.

.

3.2 Le protocole à six états

3.2.1 Simulation avec une polarisation

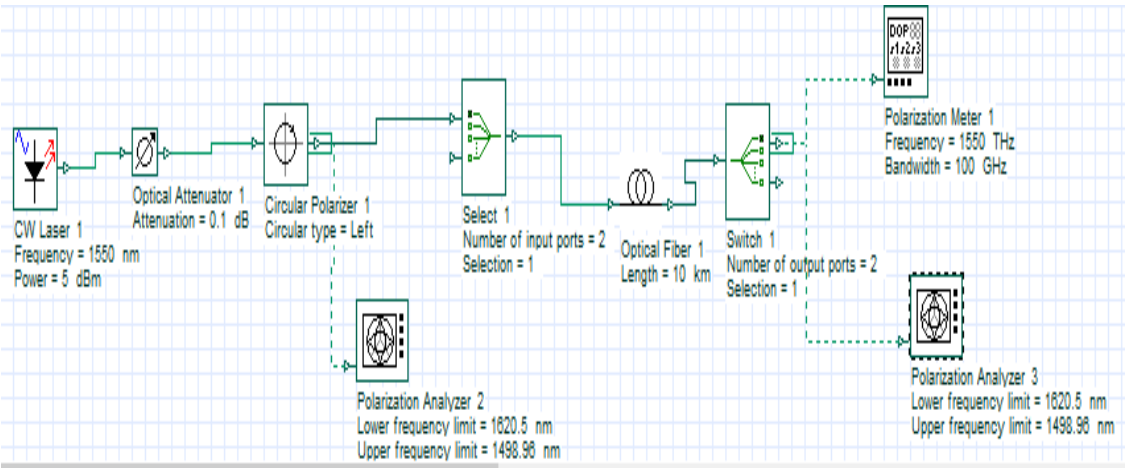


Figure 3.11 : le protocole à six états avec une seule polarisation.

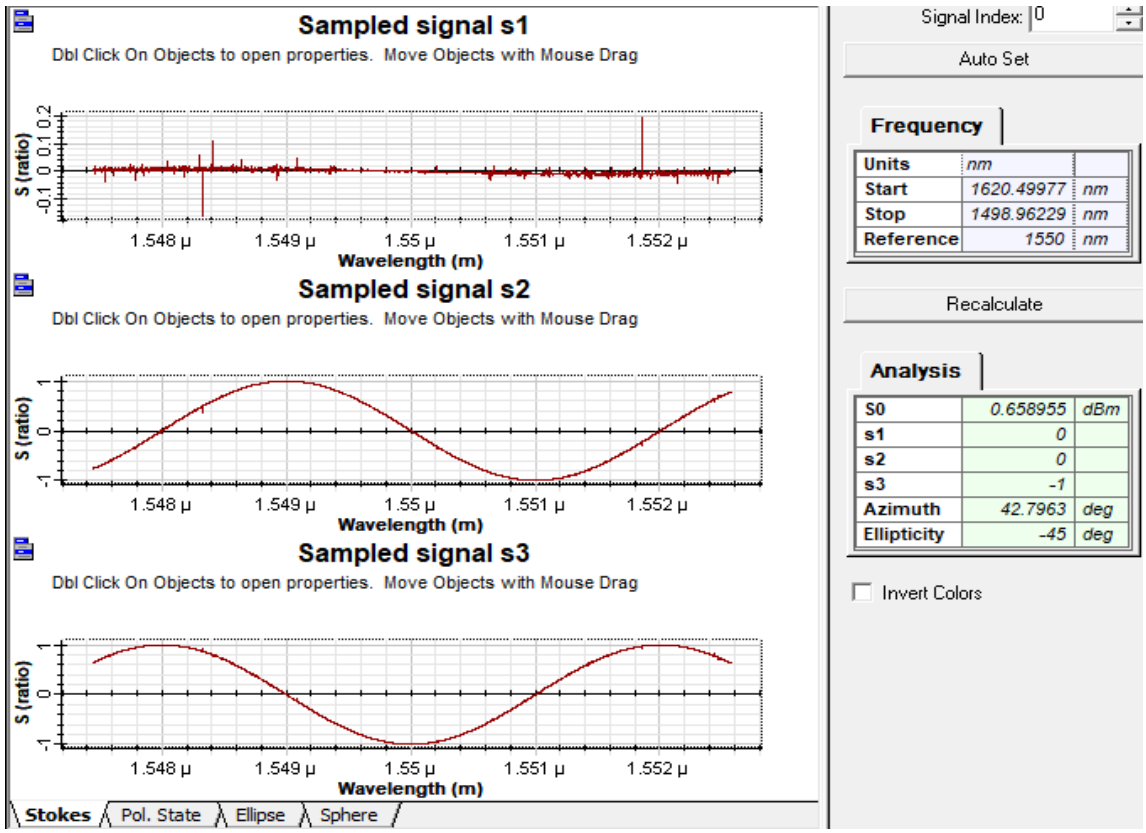


Figure 3.12 : les paramètres de Stockes.

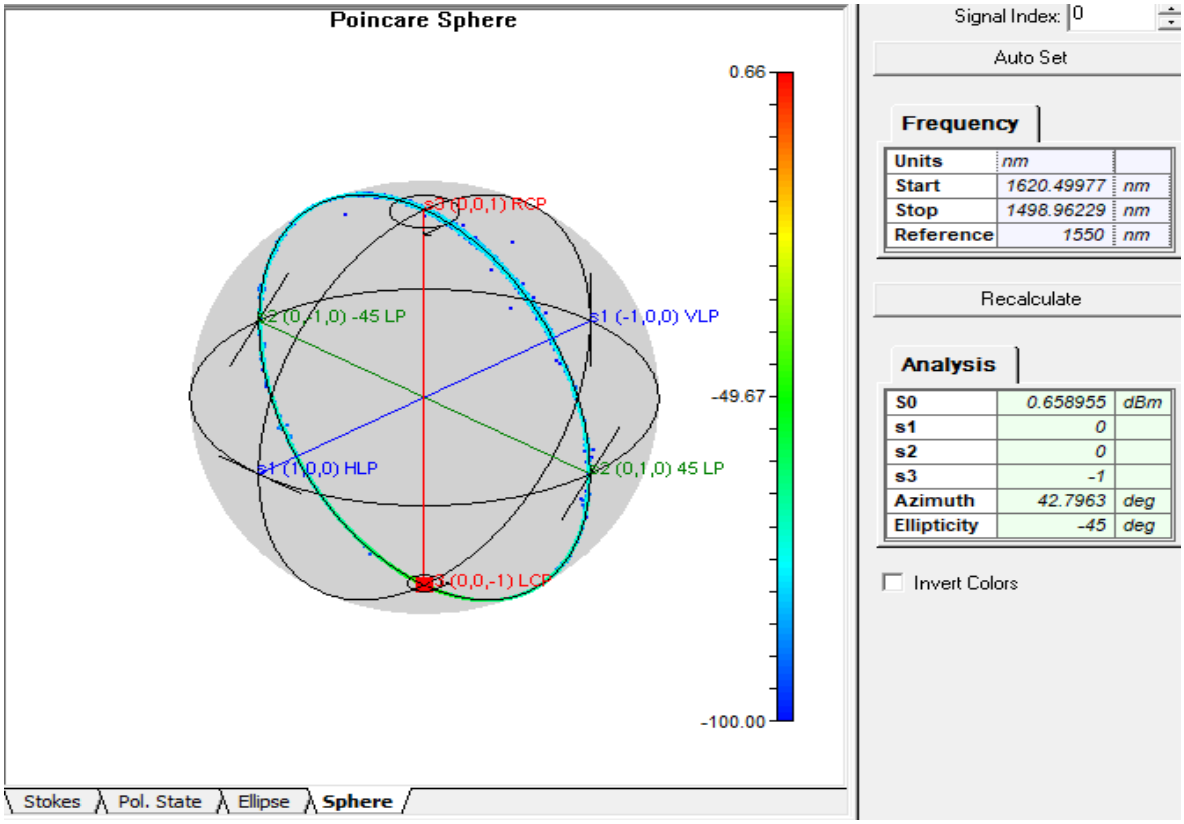


Figure 3.13 : la sphère de Bloch du récepteur.

- ***Commentaire :***

Suite à la simulation réalisée, nous sommes aboutis au résultat suivant : S1=0 ; S2=0 ; S3=-1. Ces valeurs déterminent la polarisation circulaire à gauche.

En comparant les résultats au niveau de l'émetteur et les résultats au niveau du récepteur, nous constatons une absence de changement de polarisation entre l'état émis et celui reçu, ce qui traduit des polarisations semblables.

3.2.2 Simulation avec deux polarisations circulaire (gauche et droite)

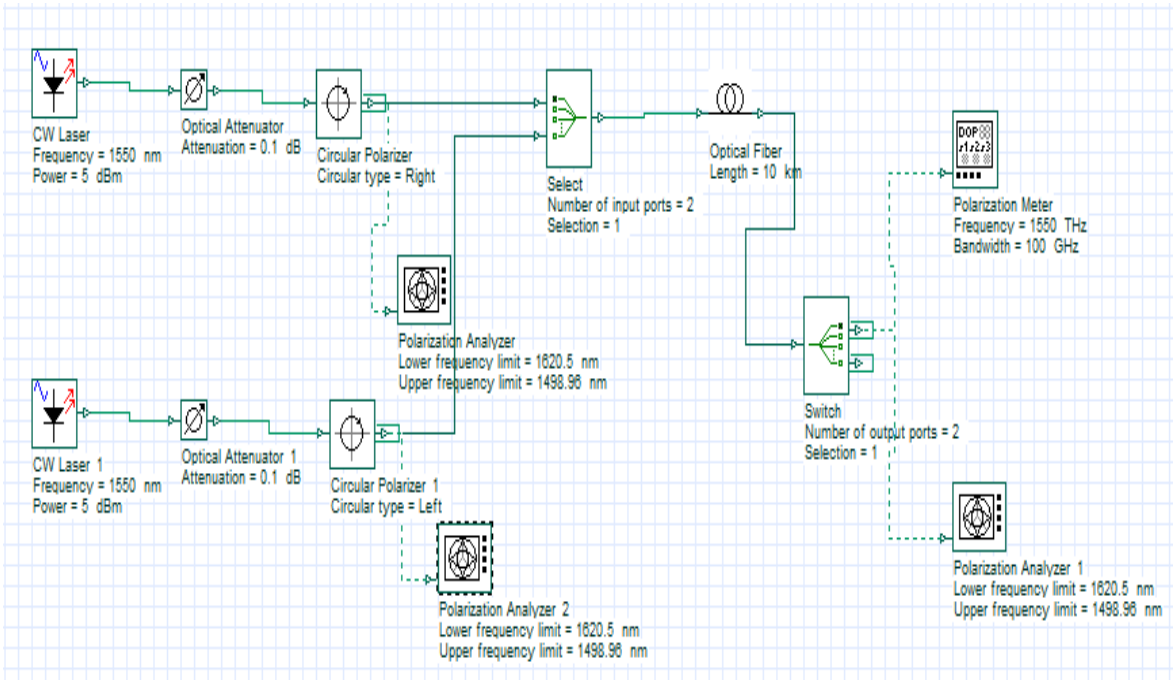


Figure 3.14 : simulation du protocole a six états avec deux polarisations.

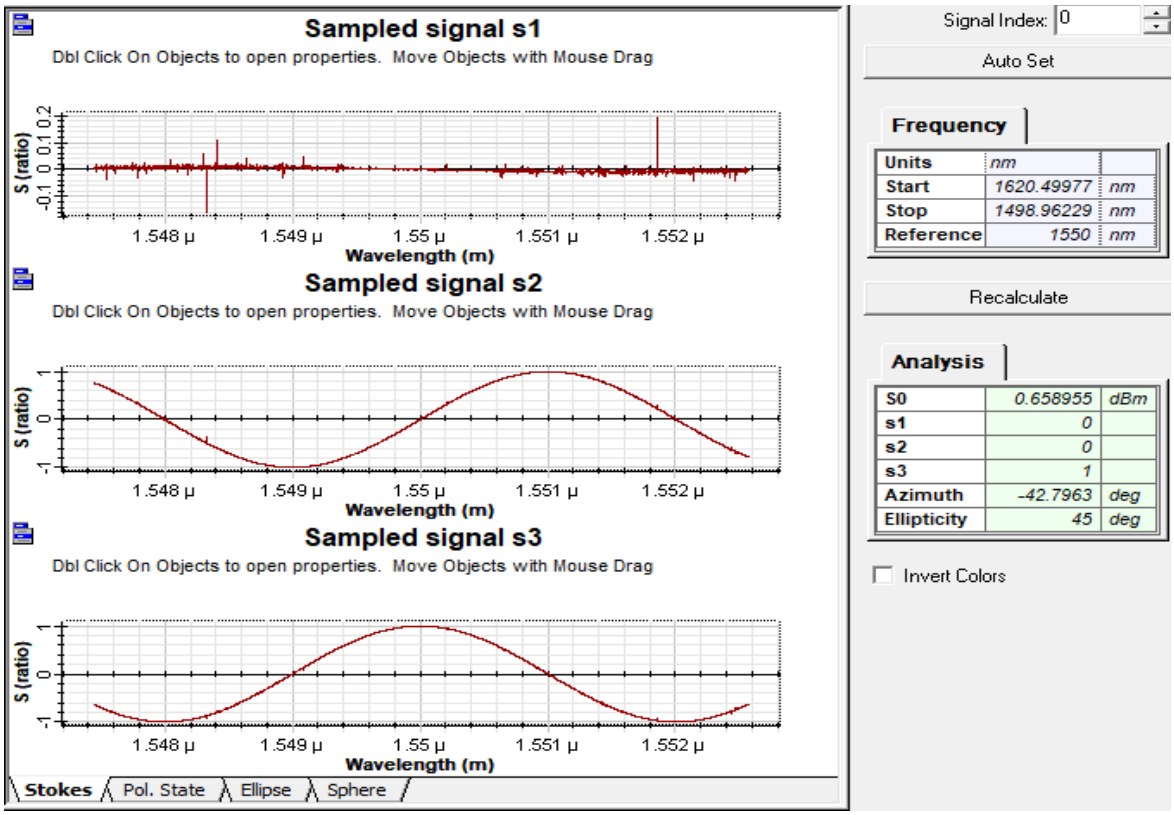


Figure 3.15 : les paramètres de Stockes du récepteur.

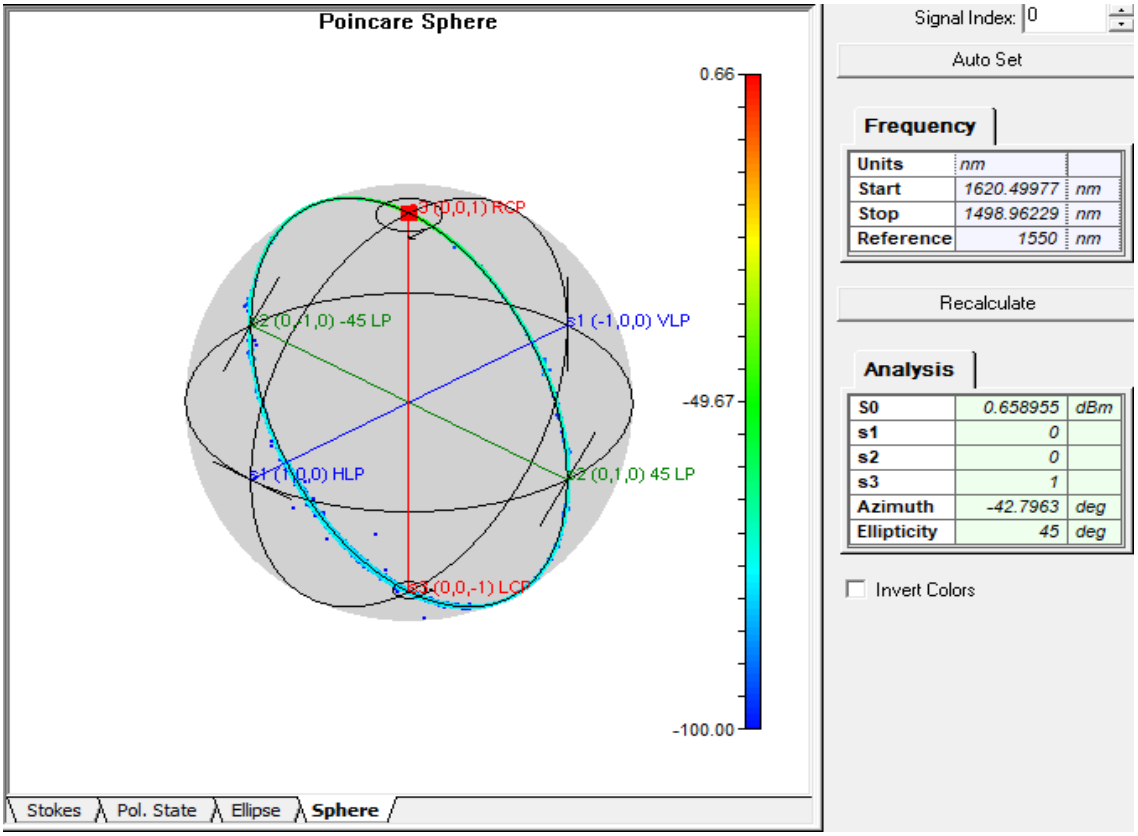


Figure 3.16 : La sphère de Bloch du récepteur.

- ***Commentaire :***

A l'issue de cette séquence et en utilisant à l'émission deux polarisations circulaires à droite et circulaires à gauche comme ils sont montrés sur les figures3.15 et 3.16, le résultat obtenus sont : S1=0 ; S2=0 ; S3=1.ces valeurs caractérisent la polarisation circulaire à gauche.

3.2.3 Simulation avec six polarisations:

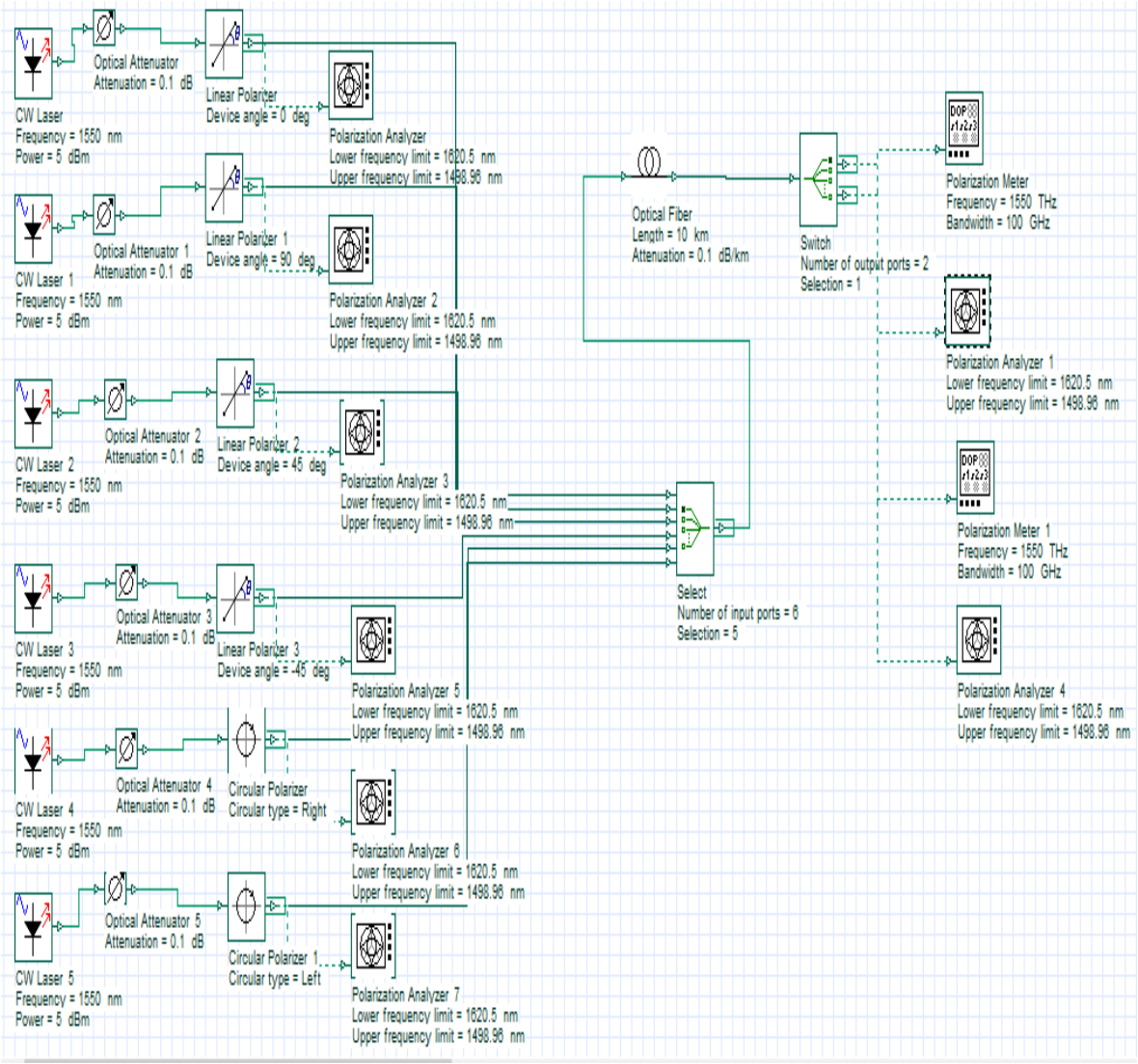


Figure 3.17: protocole à six états.

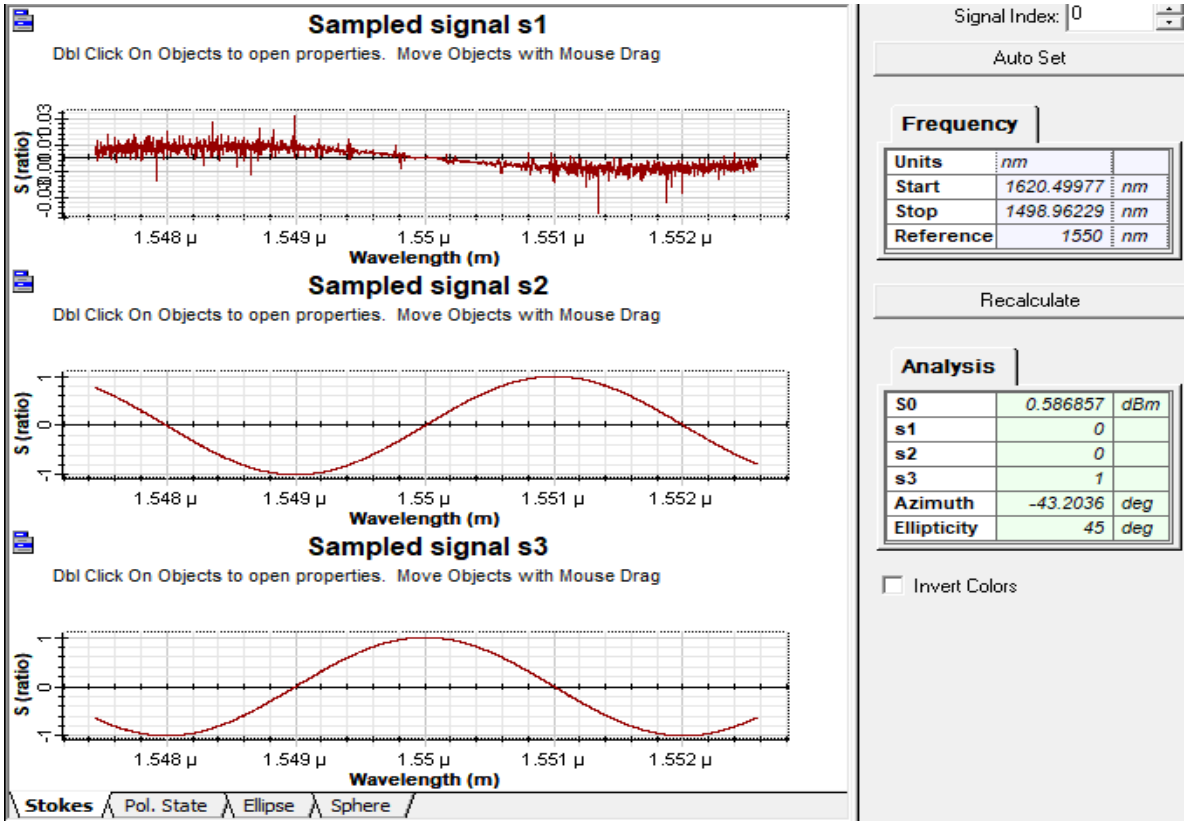


Figure 3.18: les paramètres de Stockes.

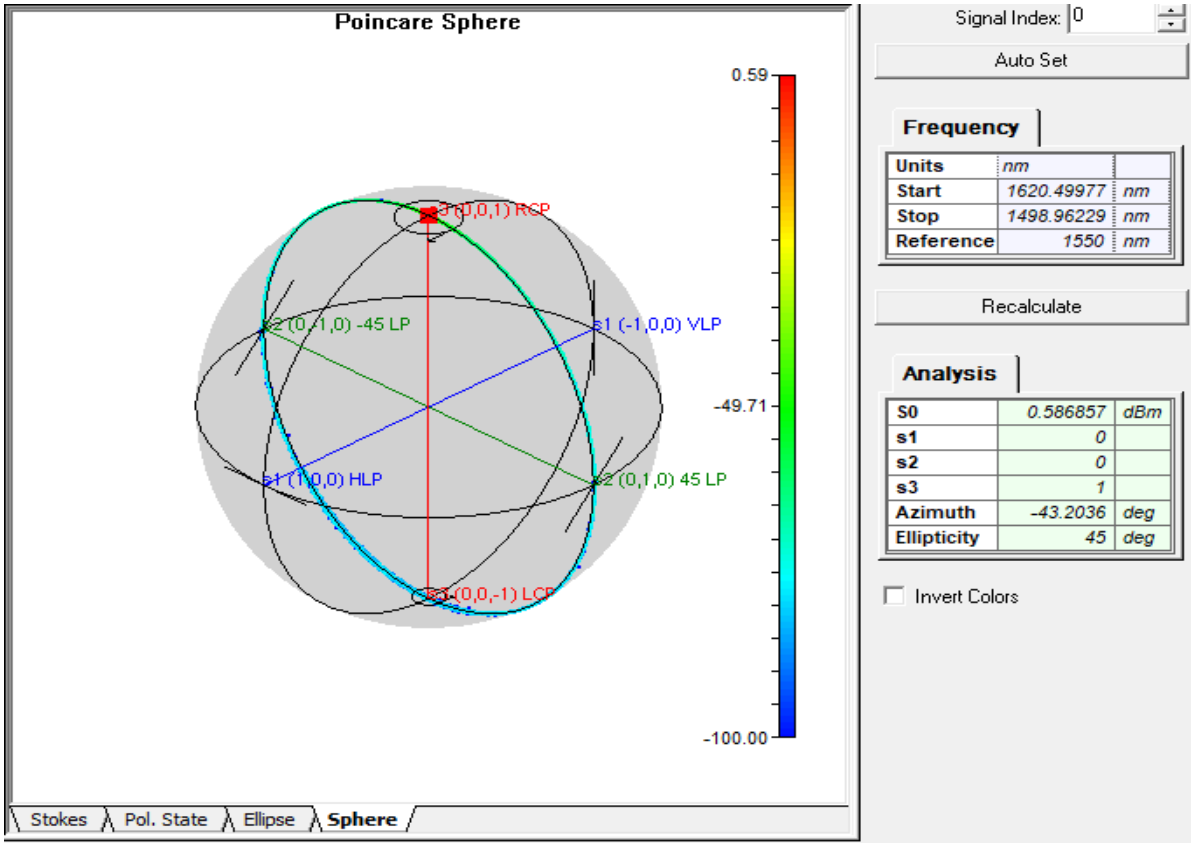


Figure 3.19: La sphère de Bloch.

- ***Commentaire :***

Dans cette partie nous avons simulé le protocole à six états de polarisation (0° ; 90° ; 45° ; -45° ; circulaire à droite et circulaire à gauche) tel qu'il est représenté sur la figure 3.17, nous rajoutons un sélectionneur d'états. Et au niveau du récepteur, nous utilisons un switch avec deux ports. Chaque port est relié à un compteur et un analyseur de polarisation, le résultat s'affichera d'une façon aléatoire sur l'un des analyseurs.

Suite à cette analyse de polarisation au niveau du récepteur nous avons aperçu qu'il a choisi aléatoirement la polarisation circulaire à gauche avec les paramètres de Stockes suivants S1=0 ; S2=0 ; S3=-1.

Conclusion

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

Dans ce chapitre, nous avons vu en revu les divers composants utilisés dans les deux protocoles à l'aide de logiciel OptiSystem en utilisant les protocoles de distribution les plus connus qui sont le bb84 et à six état. En dernier lieu nous avons implémenté les deux protocoles sur une liaison optique en utilisant une source à photon unique pour enfin aboutir à des résultats similaires à la théorie.

Chapitre IV

Implémentation des protocoles BB84 et à six états sur OptiSystem avec attaque

Introduction

Apres le premier succès convainquant d'échange quantique de clé du protocole BB84 et à six états. Nous allons voir maintenant d'autres expériences significatives qui montrent le fonctionnement de ses protocoles avec attaque. Dans la dernière partie nous allons comparer entre ses deux protocoles.

IV. 1 Le protocole bb84 et le protocole à six états avec attaque

Dans la description du protocole, on emploie le prénom classique pour les différents éléments du protocole .Le prénom Alice est employé pour l'initiateur du protocole et le prénom Bob est employé pour le destinataire.

Pendant la communication entre Alice et Bob un espion essaye d'écouter l'information. Cet espion est habituellement appelé Eve, c'est l'abréviation du mot Eavesdropper en anglais.

Maintenant, nous expliquerons dans la partie comment ça fonctionne cette type t'attaque :

- ***Émetteur***

Alice est l'expéditeur du message chiffré. Elle doit communiquer avec Bob pour produire une clé aléatoire, autrement dit, ils se communiquent à travers le canal quantique afin d'échanger la clé. Alice doit préparer cette clé sous la forme d'une chaine de qubits aléatoires, elle doit informer Bob du début et de la fin du message et de chaque impulsion. Elle est également capable d'écouter le canal pour le savoir quand Bob finira sa détection signal .une fois toutes les qubits ont été envoyés et reçus, Alice communiquera avec Bob les bases pour coder les bits envoyés qui sont identiques.

- ***L'espion***

Eve se place au milieu entre Alice et Bob .Elle joue leurs deux rôles en même temps et elle partage avec eux plusieurs fonctions communes afin d'exploiter BB84 .son rôle principale est de rassembler autant que possible les informations sur la clef partagée entre Alice et Bob sans être découverte.

Sa puissance réside dans la possibilité de pouvoir en même temps de recevoir et envoyer des impulsions à travers le canal de quantique dans la stratégie, mais ceci est limité par la configuration du canal.

Au final, elle essaie de présenter ses résultats pour que Bob les utilise.

- ***Récepteur***

Bob est le partenaire d'Alice dans ce protocole, il est la destination de son message .certaines de ses fonctions sont les mêmes avec les siens, pour répondre à l'impulsion d'Alice il doit accuser la réception.

C'est l'émission de toutes les bases aléatoirement choisies par son détecteur de photons pour mesurer les impulsions d'Alice. Une autre différence entre Alice et Bob est la décision de la polarisation du photon, du côté de Bob il est fait par lui mais le point commun ici est que les deux choix sont aléatoires.

Pour avoir une simulation d'échange de clef quantique la plus efficace, il faut également faire attention à l'interaction entre Bob et Eve. En conclusion, Bob doit afficher son résultat comme Alice

1.1 Le protocole BB84

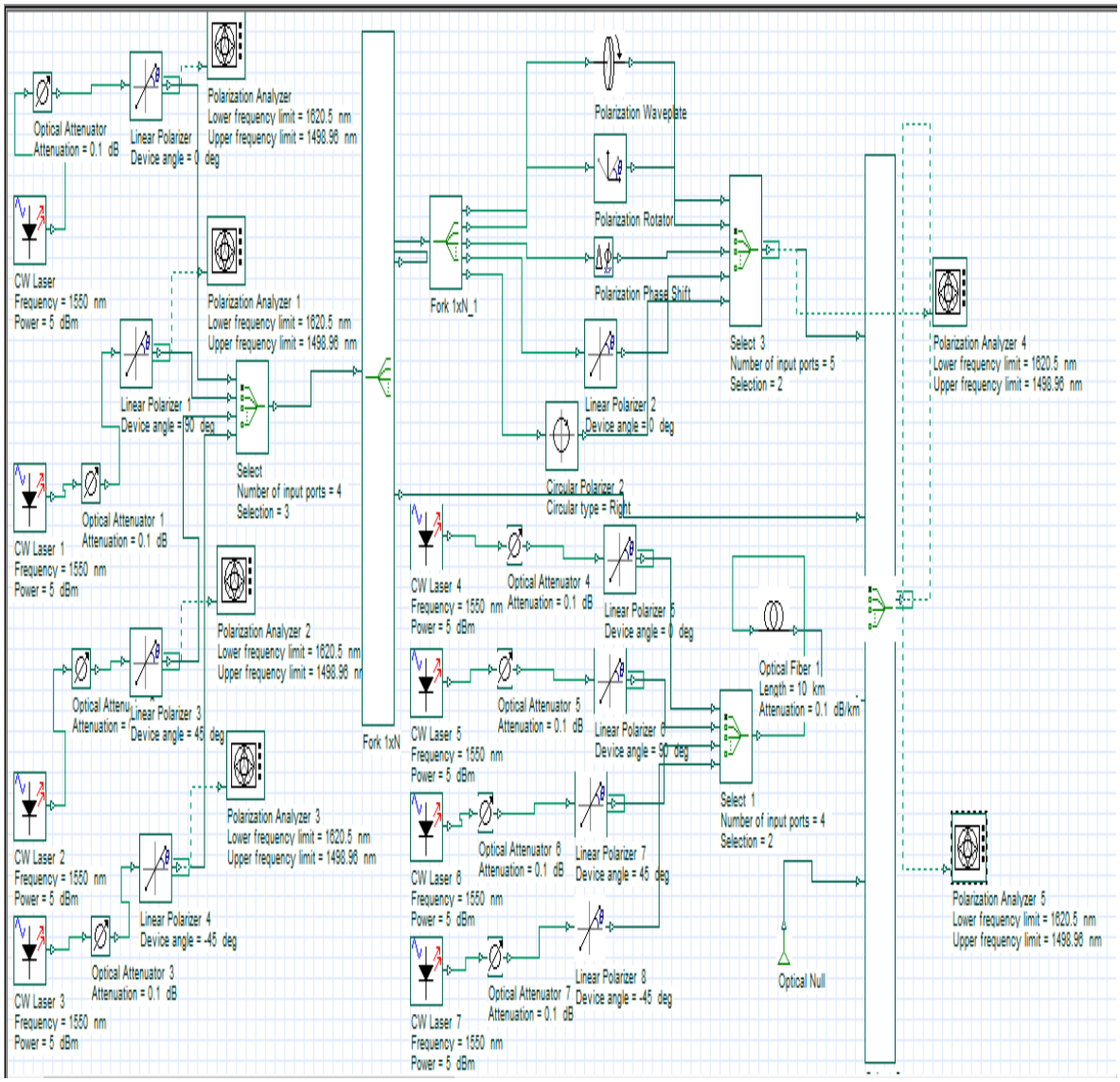


Figure 4.1 : Le protocole BB84 avec une attaque.

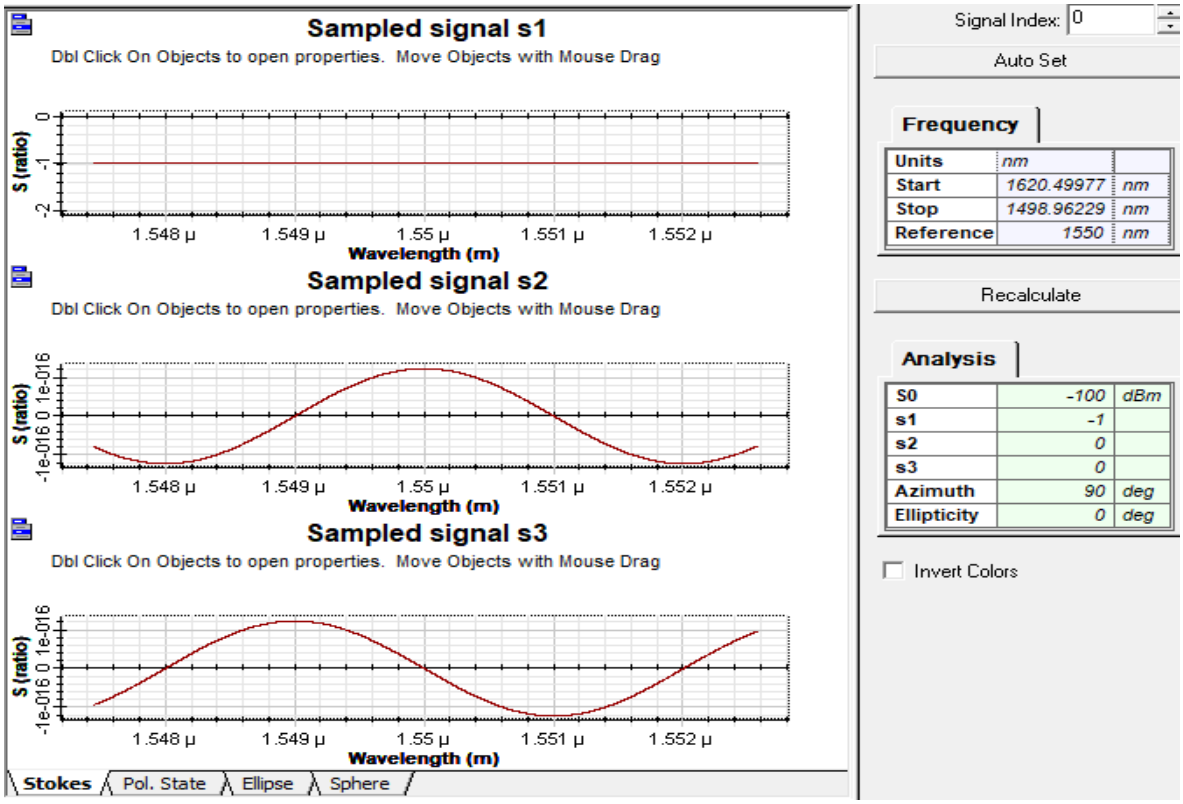


Figure 4.2 : Les paramètres de Stockes de Bob.

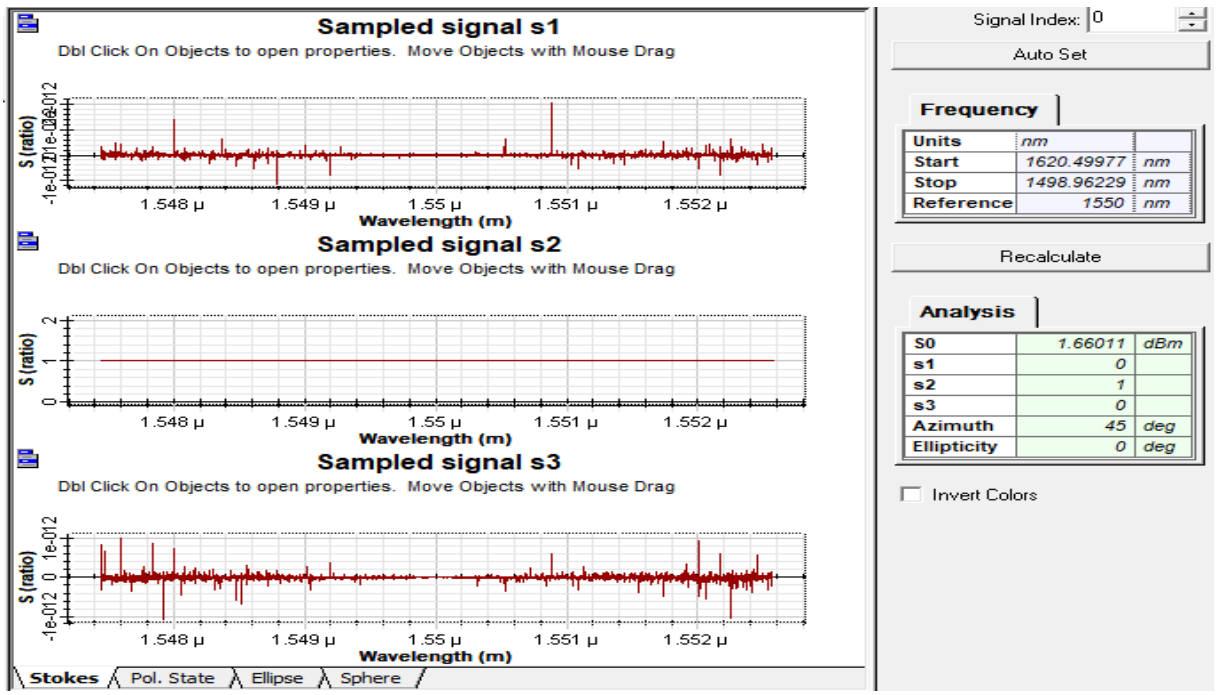


Figure 4.3 : Les paramètres de Stockes d'Eve.

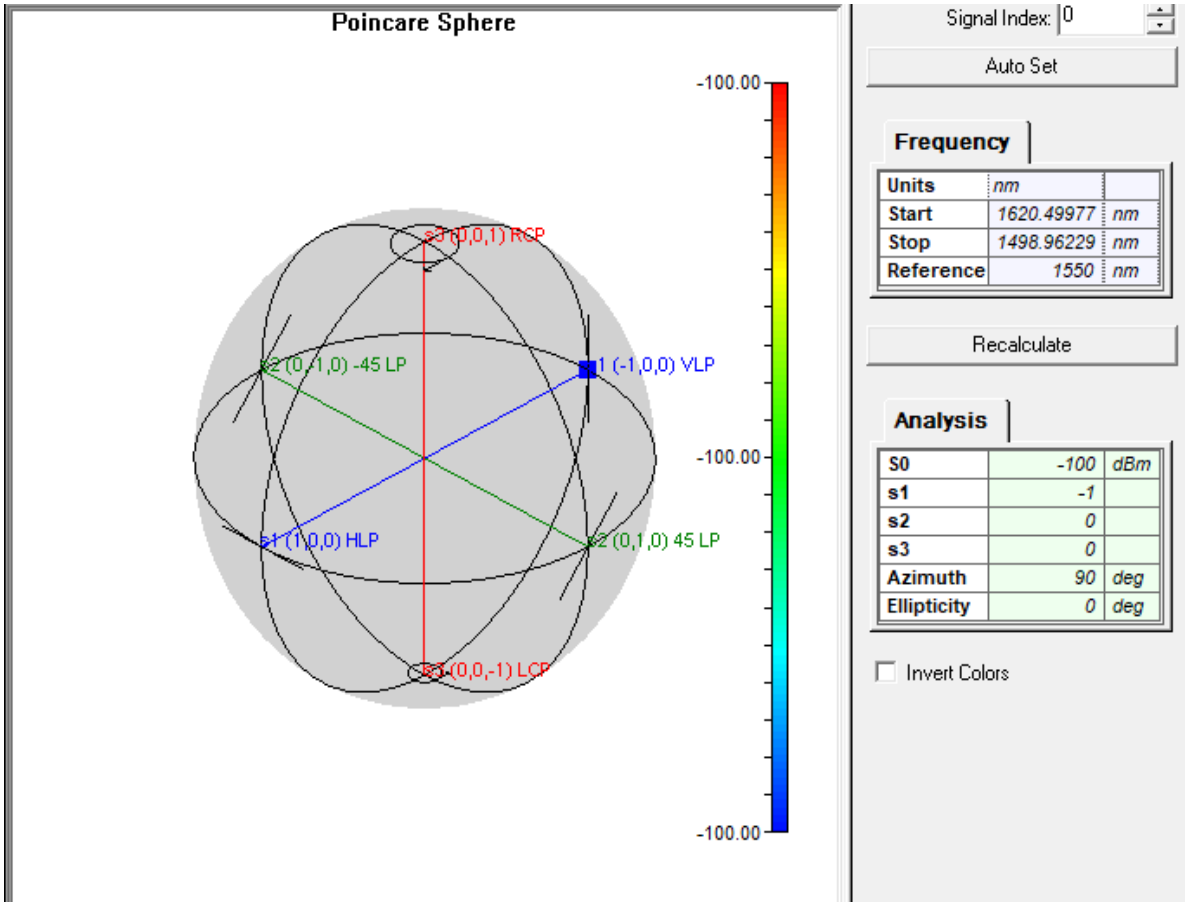


Figure 4.4 : la sphère de bloche.

1.2 Le protocole à six états

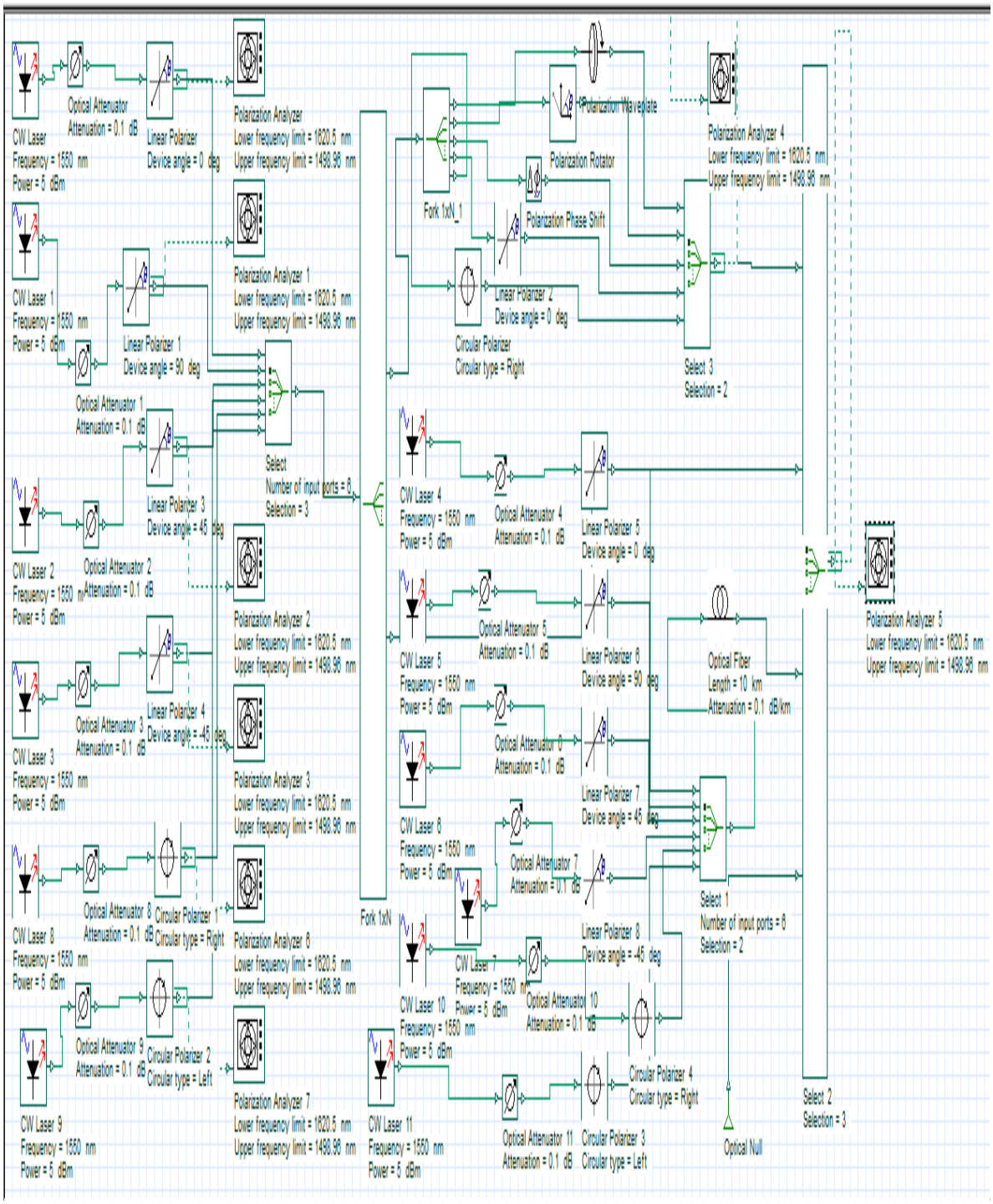


Figure 4.5 : le protocole à six états avec un espion.

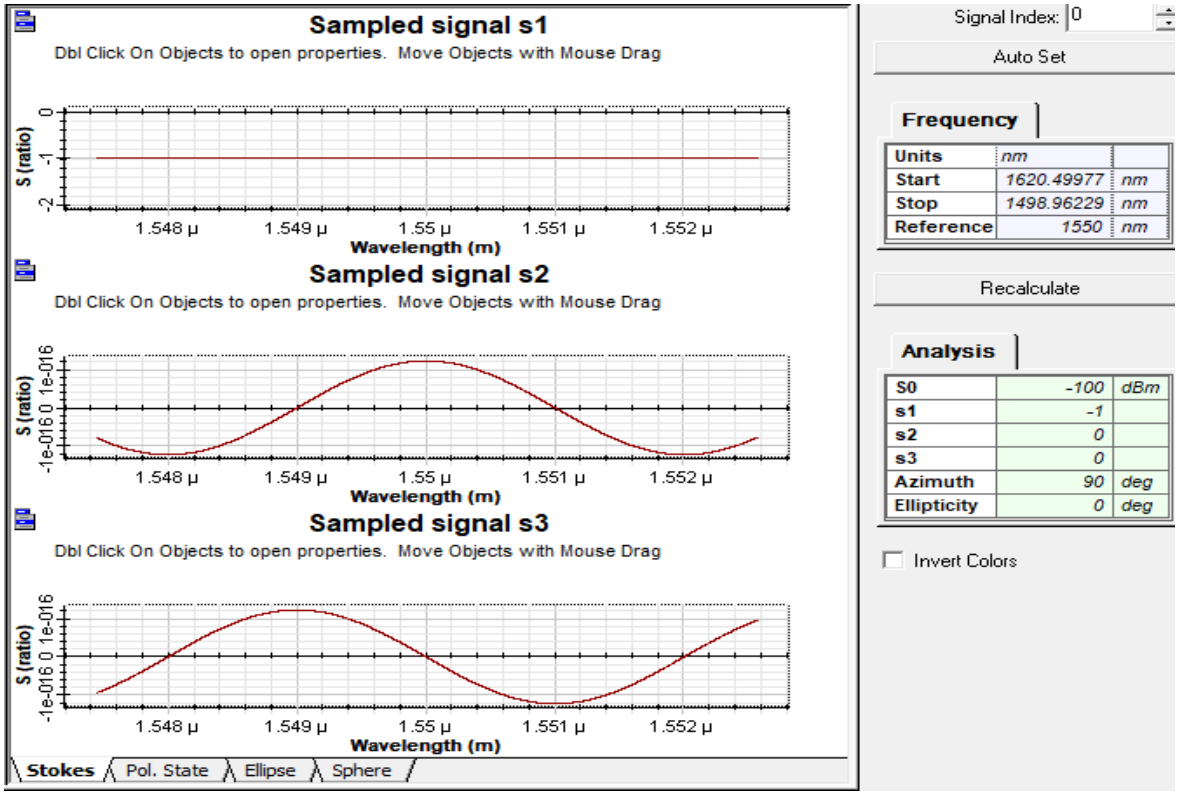


Figure 4.6 : les paramètres de Stockes du récepteur.

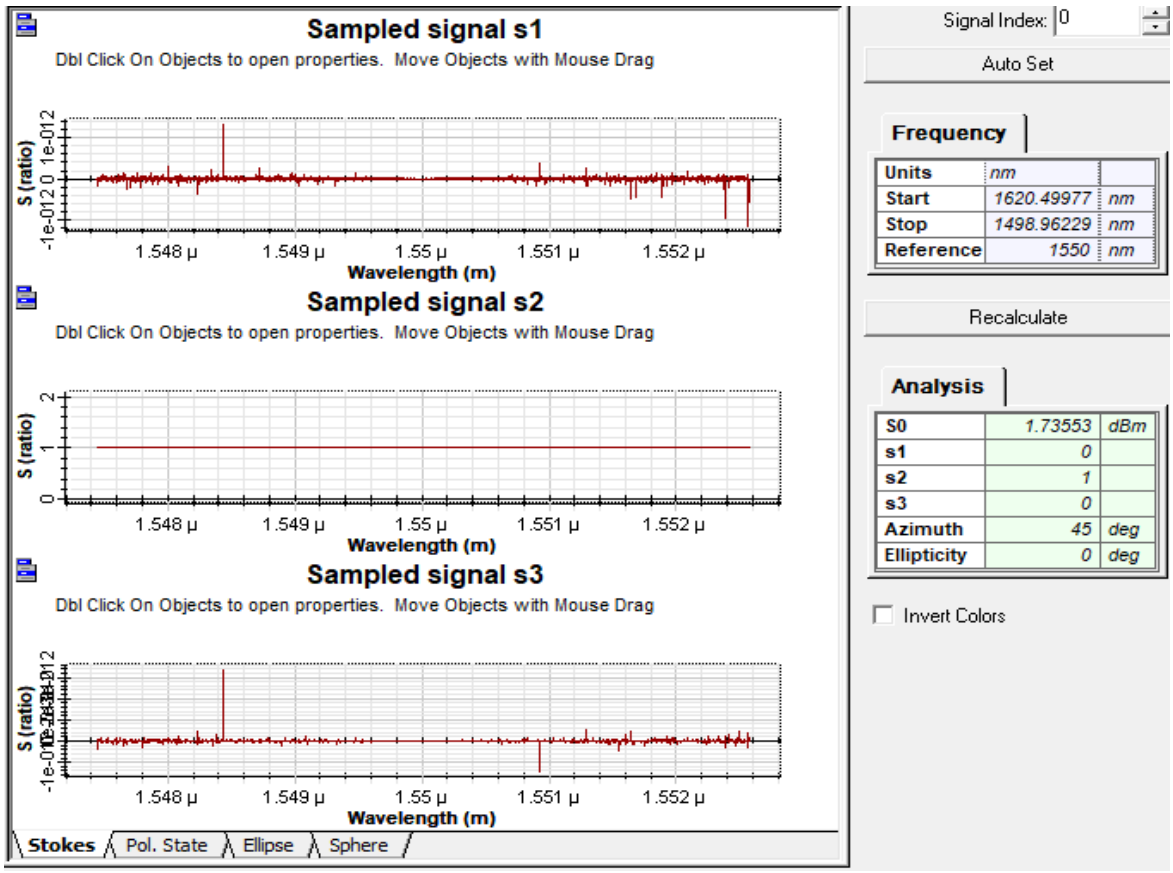


Figure 4.7 : les paramètres de Stockes de l'espion.

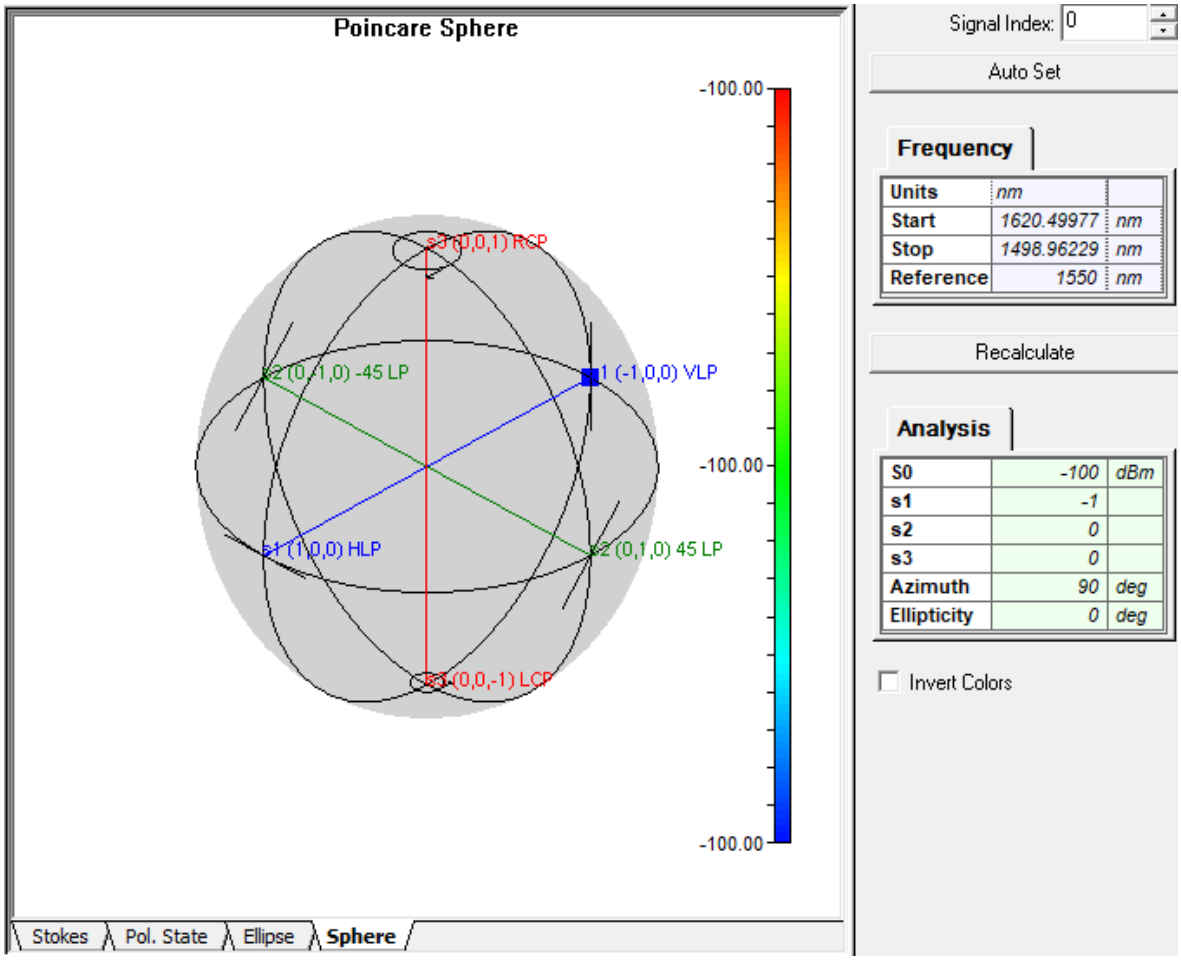


Figure 4.8 : la sphère de Bloch du récepteur.

- ***Commentaires***

Dans cette simulation Alice envoi quatre polarisations pour le protocole bb84 et six polarisation pour le protocole à six états, une parmi eux sera choisie aléatoirement par le switch (90°), Eve n'a aucun moyen de connaitre la base qu'Alice a utilisé, donc elle devra la deviner pour mesurer le photon et de renvoyer à Bob une nouvelle base pour l'espionner, alors qu'elle a choisi la polarisation 45°. Au niveau du récepteur le polariseur affiche la même polarisation d'Alice (90°). Au final, Eve n'a pas réussi à l'espionner et Bob a eu la même polarisation d'Alice.

Avec leurs paramètres de Stockes suivant : S1=-1, S2 =0, S3=0 comme est représenté dans les figures ci-dessus.

IV. 2 Exemple d'une séquence binaire dans le protocole BB84 et à six états

2.1 Le protocole BB84

- Un exemple d'une séquence binaire sans espion :

Bit d'Alice	1	0	0	1	1	0	1	0	0	1	1	1	0	1	0
Base d'Alice	✚	✖	✖	✖	✖	✚	✚	✚	✚	✚	✖	✚	✚	✚	✖
Polarisation d'Alice	V	D	D	G	A	H	V	H	H	V	A	V	H	H	A
Base de Bob	✚	✚	✖	✖	✚	✖	✚	✚	✚	✖	✖	✖	✚	✚	✚
Polarisation de Bob	H	H	A	V	V	D	H	H	V	A	D	D	V	H	V
La clé secrète	**1**	**1**	**0**	**1**	**0**	**1**	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**1**	**1**

Tableau 4.1 : une séquence binaire sans espion du protocole BB84.

Le protocole BB84 se déroule en plusieurs étapes, et permet à deux participants d'établir une clé secrète, comme c'est illustré dans le tableau ci-dessus :

- Alice émit une séquence de bits aléatoire à l'aide d'une source à photon unique, où chaque bit $\in \{0,1\}$ est codé sur un état de polarisation d'un photon, en utilisant deux polarisateurs optiques de base différentes (rectiligne ou diagonale) choisie au hasard. Bob de son coté, choisit une base de réception aléatoire pour chaque photon, avec une probabilité de ½ de choisir la bonne base qu'Alice.
- Bob reçoit et mesure l'état de polarisation de chaque photon reçu à l'aide de deux analyseurs, en sélectionnant au hasard la base de mesure, avec une probabilité de ½ de choisir la bonne base qu'Alice.

D'après les résultats obtenus on remarque que uniquement les qubits de même polarisation qui passent, donnant la clé suivante : 1 0 1 1 0 0 1 0 1.

- Un exemple d'une séquence binaire avec espion dans le protocole BB84 :

Bit d'Alice	1	0	0	1	1	0	1	0	0	1	1	1	0	1	0
Base d'Alice	+	×	×	+	×	+	+	+	+	+	×	+	+	+	×
Polarisation d'Alice	V	D	D	V	A	H	V	H	H	V	D	H	V	H	A
Base d'Eve	×	×	+	×	+	+	×	+	×	+	×	×	+	+	×
Mesure d'Eve	A	D	H	A	V	H	A	H	D	V	D	A	V	H	A
Bit d'Eve modifié	0	0	1	1	1	0	0	0	1	1	1	1	0	0	1
Nouvelle base d d'Eve	×	+	+	×	+	+	×	+	+	×	×	×	+	+	×
Polarisation d'Eve	D	H	V	A	V	H	D	H	V	A	D	A	V	H	A
Base de Bob	+	+	×	+	+	×	+	+	+	×	×	×	+	+	×
Mesure de Bob	H	H	A	V	V	D	H	H	V	A	D	A	V	H	A
La clé secrète	**1**	**0**	**0**	**0**	**1**	**1**	**1**	**0**	**1**	**1**	**1**	**1**	**0**	**0**	**1**

Tableau 4.2 : une séquence binaire avec espion du protocole BB84.

Dans le tableau ci-dessus Alice et Bob vont savoir qu'Eve à détecter le qubit dans les cas suivants:

- Eve réussi à déborder la séquence quand il n'utilisera pas la même polarisation du côté émetteur et récepteur.
- Eve réussi à espionner quand il utilise la même polarisation dans la mesure qui envoie à Bob et différente à celle d'Alice.
- Eve réussi à détruire le canal quantique quand il utilise la même polarisation que celle d'Alice et différente de celle de Bob.
- Le dernier cas où Eve utilise la même polarisation avec émetteur et dans sa nouvelle séquence utilisera la même polarisation avec récepteur.

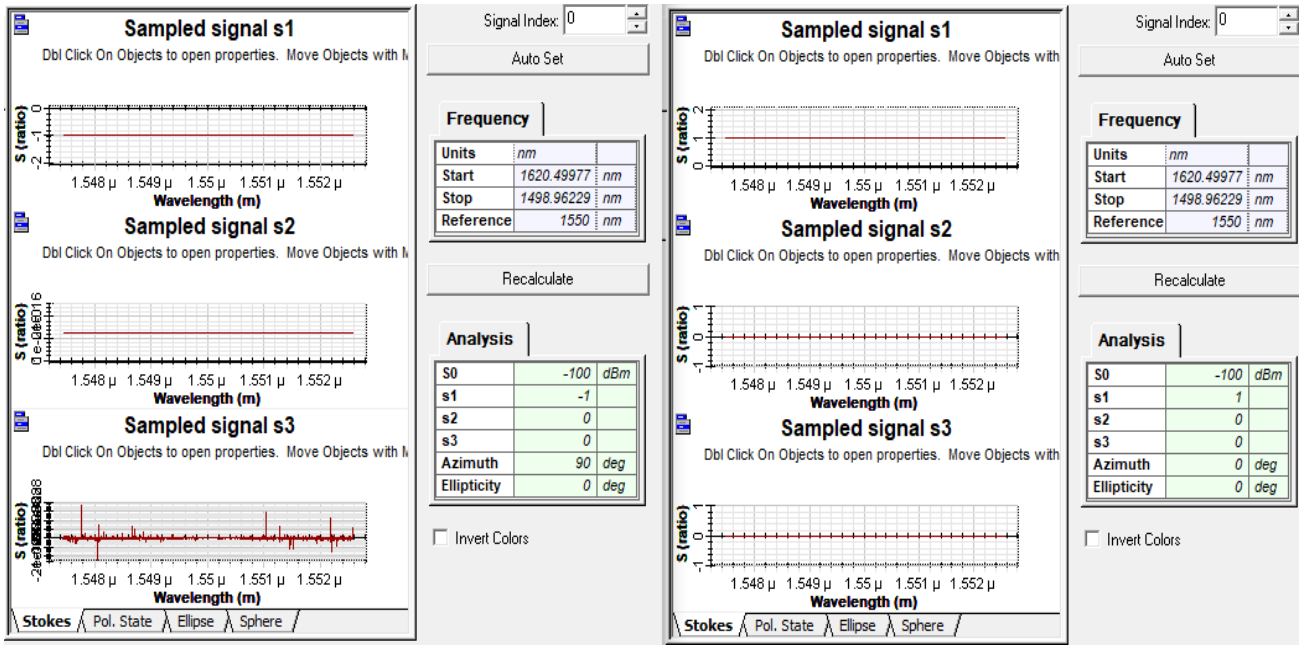
Par contre, Eve peut espionner l'information à l'insu d'Alice et Bob quand ces derniers partagent la même polarisation.

La clé est : 0 1 0 0 1

Cas d'une séquence (exemple) :

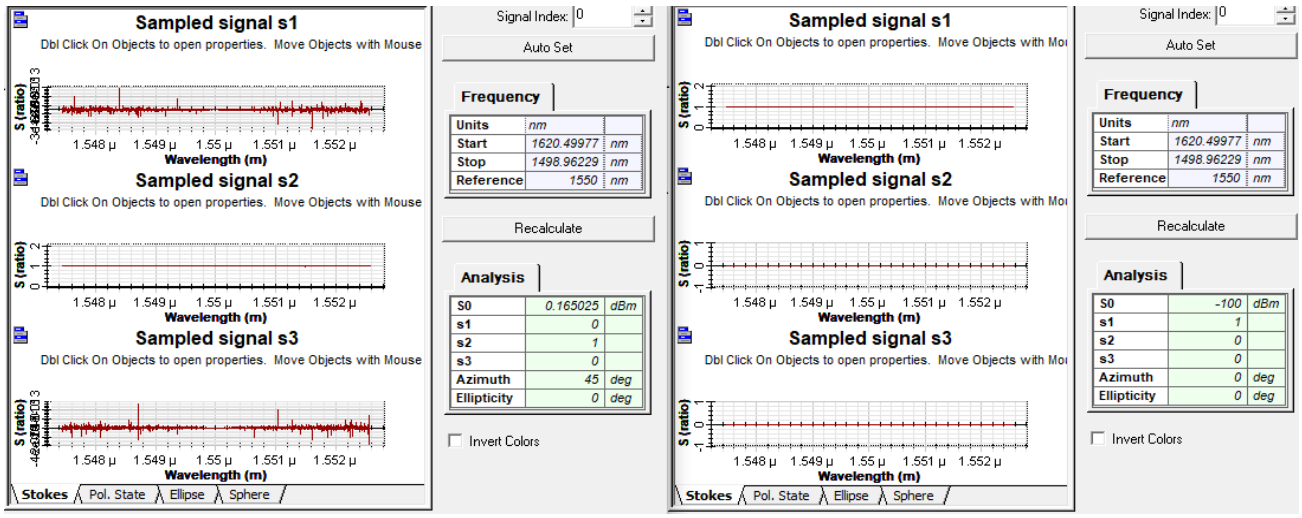
Sur les figures ci-dessous, on a simulé les deux premiers qubits de la séquence binaire d'avant (1 0 0 1 1 0 1 0 0 1 1 1 0 1 0) pour montrer l'espionnage :

- ***Premier bit :***



(a) (b)

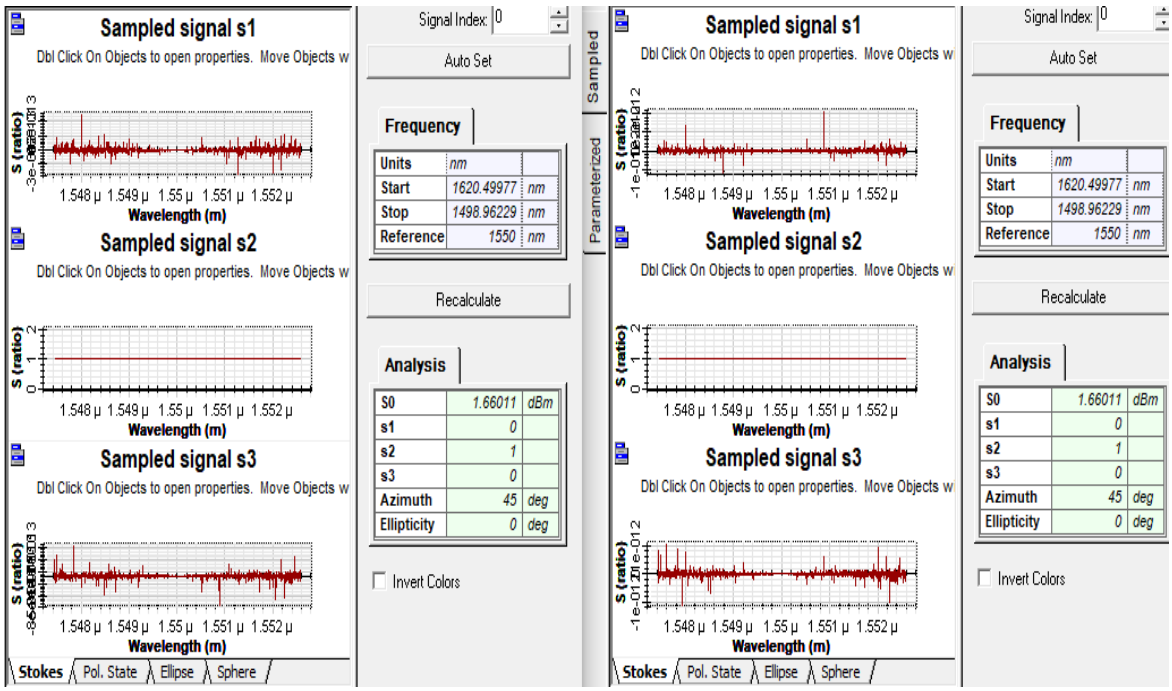
Figure 4.9 : les paramètres de Stockes entre Alice(a) et Eve(b)



(a) (b)

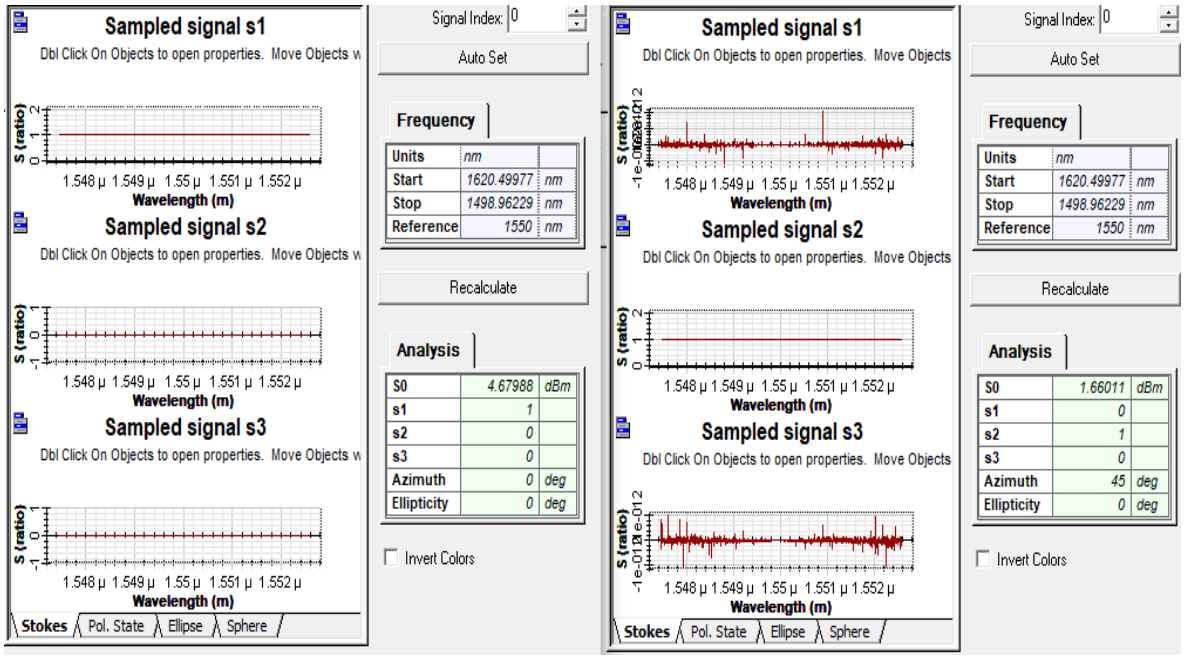
Figure 4.10 : les paramètres de Stockes entre Eve(a) et Bob(b).

- ***Deuxième bit :***



(a) (b)

Figure 4.11 : les paramètres de Stockes entre Alice(a) et Eve(b).



(a) (b)

Figure 4.12 : les paramètres de Stockes entre Eve(a) et Bob(b).

2.2 Le protocole à six états

- Un exemple d'une séquence binaire sans espion dans le protocole à six états :

Bit d'Alice	1	0	0	1	1	0	1	0	0	1	1	1	0	1	0
Base d'Alice	+	×	×	⟲	×	+	+	+	+	+	⟲	⟲	+	⟲	⟳
Polarisation d'Alice	V	D	D	G	A	H	V	H	H	V	G	G	H	G	Dr
Base de Bob	+	+	×	⟲	+	×	+	+	+	⟲	⟳	⟳	+	⟳	⟲
Polarisation de Bob	H	H	A	G	V	D	H	H	V	G	Dr	Dr	V	Dr	G
La clé secrète	**1**	1	**0**	**?**	0	1	**1**	**0**	**0**	?	1	1	**0**	1	0

Tableau 4.3: Une séquence binaire sans espion du protocole à six états.

Ce protocole a le même comportement que celui du protocole BB84 avec une polarisation circulaire de plus.

La clé est : 1 0 1 0 0 1 1 0 1 0

- Un exemple d'une séquence binaire avec espion dans le protocole à six états:

Bit d'Alice	1	0	0	1	1	0	1	0	0	1	1	1	0	1	0
Base d'Alice	+	×	×	+	×	+	+	↻	+	+	×	+	+	+	×
Polarisation d'Alice	V	D	D	V	A	H	V	Dr	H	V	D	H	V	H	A
Base d'Eve	×	×	↻	×	+	+	×	+	×	↺	×	×	+	+	×
Mesure d'Eve	A	D	Dr	A	V	H	A	H	D	G	D	A	V	H	A
Bit d'Eve Modifié	0	0	1	1	1	0	0	0	1	1	1	1	0	0	1
Nouvelle base d d'Eve	×	+	+	×	+	+	×	+	+	×	×	×	+	+	×
Polarisation d'Eve	D	H	V	A	V	H	D	H	V	A	D	A	V	H	A
Base de Bob	↻	+	×	↺	+	×	+	↺	+	×	×	↺	+	↺	↻
Mesure de Bob	Dr	H	A	G	V	D	H	G	V	A	D	A	V	G	Dr
La clé secrète	?	0	0	?	1	1	1	0	1	1	1	?	0	0	1

Tableau 4.4 : une séquence binaire avec espion du protocole à six états.

- L'attaque du protocole à six états a le même comportement que celui du protocole BB84.

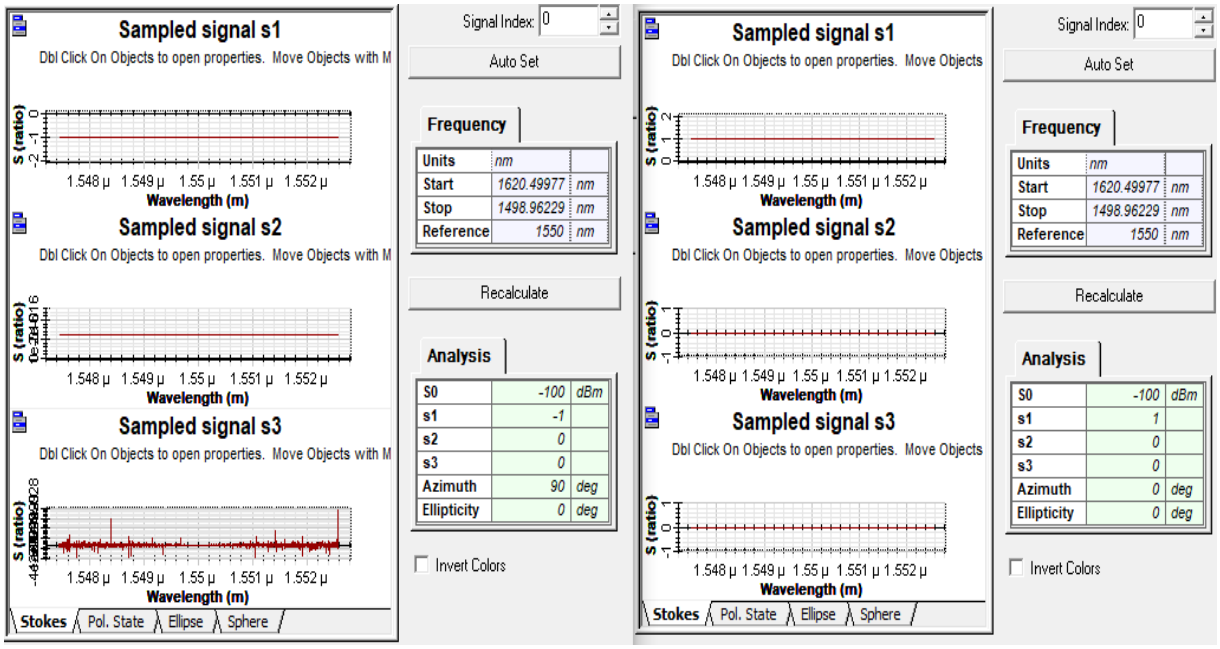
Ce protocole est plus difficile à espionné comme le montre le tableau ci-dessus.

La clé est : 1 0

Cas d'une séquence (exemple) :

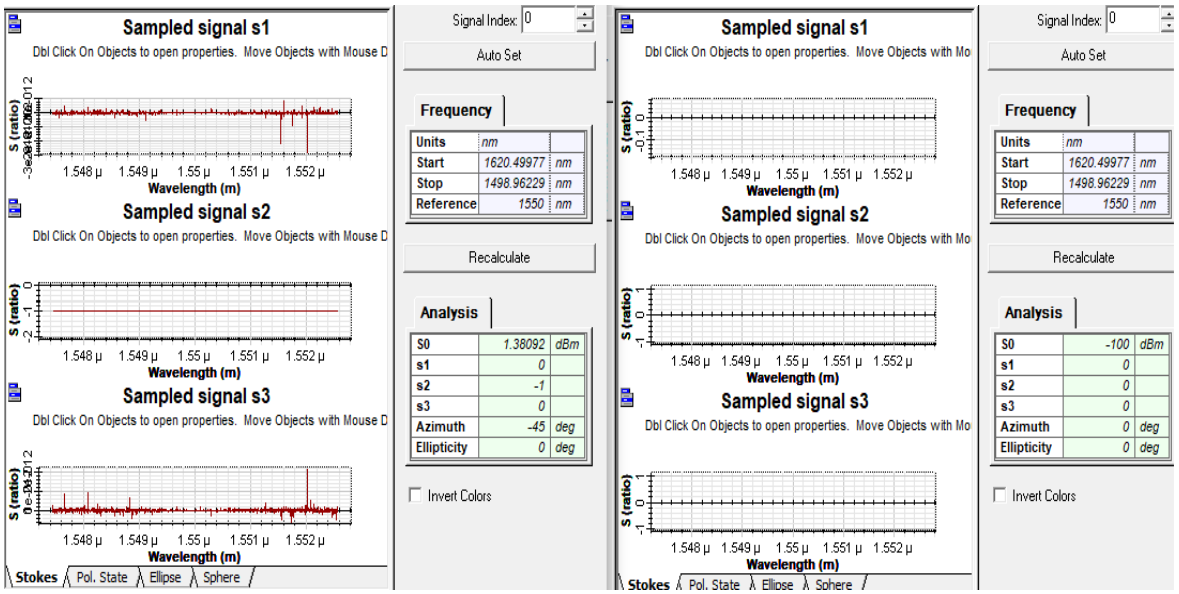
On a pris l'exemple du premier qubit de la séquence, on remarque que Bob reçoit un qubit erroné cela revient au principe de la polarisation circulaire.

Sur la figure ci-dessous, on a simulé le premier qubit de la séquence binaire (1 0 0 1 1 0 1 0 0 1 1 1 0 1 0) pour montrer l'espionnage :



(a) (b)

Figure 4.13 : les paramètres de Stockes entre Alice(a) et Eve (b).



(a) (b)

Figure 4.14 : les paramètres de Stockes entre Eve(a) et Bob(b).

Les deux figures 4.13 et 4.14 montrent que le message n'est pas transmis à Bob, du fait que les paramètres de Stockes sont nuls.

IV. 3 Comparaison entre le protocole BB84 et le protocole à six état

- Le protocole à six états est une génération de BB84 dans laquelle une troisième base d'encodage de la polarisation est ajoutée. L'ajout de cette troisième base rend l'étude de la sécurité de ce protocole plus efficace que pour BB84.
- Le protocole à six états est un protocole à variable discrète pour la distribution de clés quantiques qui permet de tolérer un canal plus bruiter que le protocole BB84. SSP(le protocole à six états) produit plus d'erreurs lors des tentatives d'écoute, ce qui facilite la reconnaissance de la présence d'un espion. par ailleurs, ce qui a été confirmé dans la littérature [2].
- Le protocole a six états rend la tâche de l'espion difficile par rapport au protocole BB84 qui est un peu plus facile à espionné. Mais l'inconvénient majeur de ce protocole est qu'Alice et Bob mesurent dans la même base seulement 1/3 du temps au lieu de la moitié du temps pour BB84. Toute chose étant égale par ailleurs, le taux de clé sera donc moins élevé.
- Enfin, comme inconvénients de ce protocole est que son implémentation nécessite des dispositifs supplémentaires par rapport à BB84 [23]. Par conséquence ce dernier est plus rapide que celui à six états.

Conclusion

Dans ce chapitre, nous avons montré l'importance de la sécurité d'information en évaluant ses performances. Dans la première partie nous avons effectué notre simulation en agissant sur la variation des polarisations afin de voir la déférence entre les deux protocoles avec attaque.

La dernière partie a été consacrée à la comparaison entre ces protocoles afin de montrer l'efficacité de chacun d'eux.

Conclusion Générale

La nécessité de sécuriser la transmission de données augmente chaque jour, et nécessite des dispositifs de chiffrement de données sécurisées pour préserver la confidentialité et l'authentification. Dans notre mémoire, nous nous sommes intéressées à la distribution quantique de clé dans les liaisons à fibre optique, cette dernière est devenue le support le plus utilisé pour les transmissions d'informations.

Ce travail a été organisé en quatre chapitres :

Le premier chapitre est consacré pour la présentation des principes de la cryptographie et les techniques utilisées pour assurer la sécurité des systèmes de transmission. La cryptographie classique a été introduite depuis une dizaine de siècle, elle est très limitée. La cryptographie moderne qui subdivise en deux types : celle à chiffrement symétrique et asymétrique qui sont longuement utilisées d'une manière efficace jusqu'à l'apparition des ordinateurs quantiques et la naissance de l'ère de la cryptographie quantique.

Le deuxième chapitre, montre que La cryptographie quantique est un sujet d'actualité qui recouvre un très large choix de compétences. Elle est introduite pour résoudre le problème d'échange de clef dans le système de clef secrète. Cette technique est structurée sur un ensemble de combinaison et des concepts de la physique quantique, dans le sens qu'elle applique la mécanique quantique, elle montre comment les photons peuvent être utilisés pour transmettre de l'information. Dans cette partie du travail, nous avons présenté les protocoles de distribution les plus connus qui ont été développés.

La partie suivante du travail a été dédié à la sécurité de l'information dans une liaison optique, afin de montrer son importance, nous avons procédé à l'évaluation de ses performances. Dans la première partie nous avons décrit les divers composants utilisés dans les deux protocoles à l'aide de logiciel OptiSystem. Dans la partie suivante nous avons effectué notre simulation en agissant sur la variation des polarisations afin de voir la différence entre les deux protocoles sans attaque.

Dans la dernière partie de ce mémoire, nous avons montré l'importance des protocoles à distribution de clé quantique dans la sécurité de l'information. En effet, nous avons effectué notre simulation en agissant sur la variation des polarisations afin de voir la différence entre les deux protocoles avec attaque.

Le résultat obtenu montre que le protocole à six états est plus efficace pour la sécurité des données, par ailleurs ce protocole présente une durée plus grande que celle du BB84.

Comme perspectives, plusieurs axes peuvent être ressortir :

- Etendre l'étude à d'autres protocoles à variables discrets tels que B92, SARG04, Protocole4+2, GV95, Protocole par codage temporelle.

- Etendre l'étude des protocoles à variables continues à modulation gaussienne.

-Réalisation pratique

Références bibliographiques

Références bibliographiques

[1] B.KADRI, << initiation à la cryptographie >>, cours 2017Cryptologie, une histoire des écritures secrètes des origines à nos jours de Gilbert Karpman, éditions Charles Lavauzelle 2006.

[2] RAMM-0000. Introduction à la cryptographie : https://ram0000.developpez.com/ Tutoriels/cryptographie/,2009

[3] M. Hamza, 'étude et comparaison des principaux systèmes de cryptage', Mémoire de fin d'étude, Université Mohamed Boudiaf M'sila, 2016

[4] N. Hassan, 'Conception et simulation des générateurs, crypto-systèmes et fonctions de hachage basés chaos performants', Thèse de doctorat, université de Nantes, 2015.

[5] C. Berbain, 'Analyse et conception d'algorithmes de chiffrement à flot', Mémoire de Master, Université de Paris, 2007.

[6] S. Hacini, I. Boumedyen, M. Inal, 'Implémentation d'algorithmes de Cryptographie', Mémoire de licence, université de Tlemcen, 2014.

[7] P. Navez et G. Van Assche. (2002). « Une transmission sécurisée : la cryptographie quantique ». Rev. Mod. Phys. 75, 145.

[8] R.Rivest, A. Shamir, and L. Adleman, 'A method for obtaining digital signatures and public-Key cryptosystems', Communications of the ACM, 1978.

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

[12] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. Review of Modern Physics, 2002.

[13] Philippe Grangier, John Rarity, and Anders Karlsson. The European Physical Journal D, February 2002.

[14] Jing Ma, Guangyu Zhang, Yiwen Rong, Liying Tan,'' Theoretical study of polarization tracking in satellite quantum key distribution", Quantum Physics, *11 Apr 2005.*

[16] E. Collett. Polarized light in fiber optics. Lincroft, New Jersey (USA), 2003.

[17] E. Collett, B. Schaefer. Visualization and calculation of polarized light. I. The polarization ellipse, the Poincare sphere and the hybrid polarization sphere. Applied optics, vol.47, no. 22, 2008.

[18] Jean-Louis Basdevant et Jean Dalibard. «Mécanique quantique, cours de l'Ecole polytechnique ». Février 2002.

[19] Futura, <<cryptographie quantique >> [archive], sur Futura (consulté le 3 octobre 2020).

[20] HAN Minh Phuong, <<discription du protocole BB84 en trois dimention >>, Paris, 1 avril 2005.

[23] Nicolas Cerf, Iordanis Kerenidis, '' Modèles de sécurité réalistes pour la distribution quantique de clés'', Thèse présentée pour obtenir le grade de docteur de Télécom ParisTech, 6 décembre 2011.

Webographie

[9] https://www.lefigaro.fr/sciences/2017/09/29/01008-20170929ARTFIG00241-premiere-communication-a-tres-longue-distance-par-cryptographie-quantique.php

[10]https://www.futura-sciences.com/sciences/definitions/physique-cryptographie-quantique-10172/#:~:text=La%20Darpa%20(agence%20am%C3%A9ricaine%20sur,l'origine%20du%20r%C3%A9seau%20Secoqc.

[15] https://fr.readkong.com/page/tp-n-1-initiation-a-l-utilisation-du-logiciel-optisystem-8033967

[21]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/

[22] https://www.inria.fr/fr/acteurs-informatique-quantique

Résume

Le but de la cryptographie est d'améliorée des techniques et des méthodes permettant une transmission sécurisé. Les premières techniques sont sous le nom de la cryptographie classique qui est composée de deux types de chiffrement : chiffrement à clé secrète où une seule clé suffit pour le cryptage, et chiffrement à clé publique consiste en l'existence d'une paire de clés de chaque côté, une clé publique pour chiffrer et une clé secrète pour déchiffrer. Mais la sécurité de cette technique repose sur les méthodes de calcul mathématique que les ordinateurs actuels non pas la puissance nécessaire pour l'assurer.

Pour faire face à ce problème, la cryptographie quantique intervient comme solution.la distribution quantique de clé permet à deux parties distantes de communiquer avec intimité absolue, même en présence d'un espion. En se basant sur les lois de la mécanique quantique. Dans ce travail, nous avons présenté les concepts de bases de la cryptographie quantique pour prouver son efficacité dans des transmissions sécurisées. Nous avons simulé deux protocoles les plus important dans le quantique puis comparé entre eux

Abstract

The goal of cryptographie is to improve techniques and methods for secure transmission. The first techniques appeared under the name of classical cryptography which is composed of two types of encryption: secret key encryption where a single key is sufficient for encryption, and public key encryption consists of the existence of a pair of keys. On each side, a public key to encrypt and a secret key to decrypt. But the security of this technique relies on mathematical calculation methods that current computers do not have the power to provide it. To face this problem, quantum cryptography comes in as solution.

Quantum key distribution allows two distant parties to communicate with absolute privacy, even in the presence of a spy. Based on the laws of quantum mechanics. In this work, we presented the basic concepts of quantum cryptography to prove its efficiency in secure transmission. We have simulated two most important protocols in quantum and then compared between them