République Algérienne Démocratique et Populaire

Ministère de l'enseignement Supérieur et de la Recherche Scientifique

Université ABDERRAHMANE MIRA Bejaia

جامعة بجاية
Tasdawit n'Bgayet
Université de Béjaïa

Faculté de Technologie

Département de Génie Electrique

Mémoire de fin d'études pour l'obtention de :

DIPLOME MASTER RECHERCHE EN ELECTRONIQUE

Spécialité : Télécommunication

Thème

Etude et simulation de la Cryptographie Quantique

Présenté par :

BENBOUYA Fahem

Encadré par :

BERRAH Smail

SELLAMI Mohammed

Membre du jury:

Mr. ROUHA Mustapha

Mr. MOKRANI Karim

Année : 2012/2013

REMERCIEMENTS

Nous tenons à remercier tout d'abord DIEU le tout puissant Qui nous a donné durant toutes ces années la santé, le courage Et la foi.

Nous ne saurions, réellement, trouver les expressions éloquentes que méritent nos encadreurs « Mr BERRAH Smail et SELLAMI Mohammed », a fin de les remercier pour leur sympathie, encouragements, aides, dévouement pour le travail et leur présence totale.

Nous adressons nos remerciements à messieurs, le président et les membres de jury qui nous ont fait l'honneur d'évaluer et d'examiner notre travail.

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

Enfin, nous exprimons nos remerciements à tous ceux qui ont contribué de près ou de loin à l'élaboration de ce travail.

Dédicaces

A mon cher père

Et ma chère mère

A mes chers frères

Et mes chères sœurs

A toutes mes proches

Et tous mes amis (es)

Je dédie ce travail.

Table de matières

Abréviations

Alice : Pour designer l'émetteur du message.

Bob : Pour designer le récepteur final.

Eve : Pour designer l'intrus qui va essayer d'intercepter le message.

QC : Cryptographie quantique.

QKD : Distribution quantique de clé.

B92 : Protocole de Bennett, présenté en 1992.

BB84 : Protocole de Bennett et Brassard, présenté en 1984.

XOR : Exclusive OR.

QBER : Taux d'erreur binaire quantique.

I-R : Interception-renvoi.

SNP : Séparation du nombre de photons.

Listes des figures

Liste des tableaux

Introduction générale

Introduction générale

Le besoin d'assurer la sécurité des communications entre les personnes se faisait toujours sentir. Ainsi, être sûr que les messages échangés n'ont pas étés modifiés en cours de route ou encore intercepter par une tierce personne était un souci permanent qui ne s'est dissipé que par l'apparition des procédés de sécurisation avancées. L'un des outils les plus efficaces adoptés dans nos jours est la cryptographie.

La cryptographie est traditionnellement utilisée pour dissimuler des messages aux yeux de certains utilisateurs et garantir que seuls les destinataires légitimes auront la possibilité de les consulter. La cryptographie sert, non seulement, à préserver la confidentialité des données, mais aussi à garantir leur intégrité et leur authenticité.

De ce fait, la cryptographie a pris une grande ampleur et est devenue une discipline scientifique à part entière qui utilise des concepts mathématiques et informatiques pour prouver ca sécurité. Cependant, des attaques viennent périodiquement pour nuire la confiance des utilisateurs. En cryptographie, il est nécessaire de représenter les buts de l'adversaire et ses moyens, c'est-à-dire ce qu'il cherche à faire et la manière dont il agit avec le système. C'est ici que la cryptographie montre ses limites face à la réalité.

Face aux divers problèmes et exigences de sécurité de la communication, il s'est développé depuis quelques années un nouveau champ d'investigation dans ce domaine connu sur l'appellation « Cryptographie Quantique », cette technique est structuré sur une belle combinaison des concepts de la physique quantique et la théorie de l'information 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.

C'est dans ce cadre que s'inscrit notre travail. Notre but est d'étudier la cryptographie quantique. Par la suite, nous nous proposons d'étudier en détail le protocole BB84.

Ce rapport est organisé en trois chapitres :

Le premier chapitre, présente un aperçu général sur des notions de cryptographie classique telles que, les divers types de cryptographie existant et les problèmes liés à la distribution des clés.

Le chapitre 2, passe en revue les principes et les fondements sur lesquels se base la cryptographie quantique.

Le chapitre 3 porte en première partie, une description détaillée des différentes phases constituant le protocole BB84. Ainsi, que les différentes techniques possibles d'attaques et leurs influences sur la sécurité de ce protocole. Dans une seconde partie, l'analyse de

protocole, dans le cas ou le canal de communication est non idéale tout en donnant les différents paramètres physiques qui sont à l’ origine de cette faiblesse.

Le rapport est clôturé par une conclusion et des perspectives.

Chapitre 1

Généralités sur la cryptographie

1. Introduction

Avant d'aborder le vif sujet, un bref historique sur l'évolution de cryptographie est 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.

2. Histoire :

Les communications ont de tout temps constitué un aspect important dans l'acquisition de nouvelles connaissances et l'essor de l'humanité. Le besoin d'être en mesure d'envoyer un message de manière sécurisé est probablement aussi ancien que les communications elles-mêmes. D'un point de vue historique, c'est lors des conflits entre nations que ce besoin a été le plus vif, pour assurer la confidentialité d'une partie de leur portée.

L'histoire retient Jules César comme précurseur et utilisateur régulier de la cryptographie pour envoyer des messages confidentiels s'ont de tout temps protégé d'éventuels messagers malhonnêtes.

Et, bien avant, entre le Xe et VIIe siècle av. J.-C. Les Grecs utilisaient déjà une technique de chiffrement par transposition qui permettait de modifier la disposition des lettres dans un message. Ils se servaient d'une scytale [W1]. Le scytale était un ruban (un cylindre) sur lequel on enroulait une bandelette de papier, le texte était alors écrit en lignes droites successives, le ruban qui constitue le texte chiffré était ensuite déroulé et expédié au destinataire qui devait le ré-enrouler sur un axe de même diamètre, le texte apparait donc en clair, sans la connaissance du diamètre du ruban qui jouait le rôle de la clé, il était impossible de déchiffrer le message.

Puis, au cours du $19^{iéme}$ siècle, on assista au développement plus au moins ingénieux de techniques de chiffrement expérimentales. Kirchhoff posa les principes de la cryptographie moderne, l'un des principaux, pose que la sécurité d'un système de chiffrement ne résidait que dans la clé et non dans le procédé de chiffrement [1]. Une dernière innovation, plus récente, fût l'utilisation de la machine "Enigma" par l'armée Allemande, durant la Seconde

Guerre Mondiale [W1]. Cette machine permettait de chiffrer toutes les communications radio ou télégraphiques. Le système était simple mais efficace. Chaque lettre est substituée par une autre, avec des résultats qui changent à chaque fois. La machine est alimentée par une pile électrique. Elle contient un mécanisme de rotors qui modifie le circuit électrique à chaque frappe. Lorsqu'un utilisateur appuie sur une touche du clavier, un circuit électrique se ferme et une lampe s'allume en indiquant le caractère à utiliser.

A partir de 1970 La cryptographie, à connu une réelle explosion avec le développement des systèmes informatiques. Elle a connu un plus large progrès avec l'arrivé des systèmes d'informations modernes où il y a une nécessité de protéger les données.

3. Généralité sur la cryptographie

3.1. Quelques définitions

Le chiffrement : consiste à rendre le message incompréhensible pour quiconque n'est pas doté de clé de déchiffrement.

Le déchiffrement : c'est l'opération inverse du chiffrement.

Clé : moyen permettant d'obtenir ou d'empêcher l'accès.

Cryptogramme : message chiffré.

La cryptologie : est une science mathématique qui englobe la cryptographie et la cryptanalyse.

La cryptographie : c'est l'ensemble des techniques permettant de rendre les messages incompréhensibles et de transmettre les données de manière confidentielle.

La cryptanalyse : est l'étude des procédés cryptographiques dans le but de trouver des faiblesses et en particulier, de pouvoir décrypter des textes.

Algorithmes cryptographiques : ensemble de règles mathématiques (logiques) utilisées au cours des processus de cryptage et de décryptage.

3.2. Objectifs de la sécurité informatique

L'objectif de la sécurité d'un système informatique c'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 : c'est de garder les informations secrètes de tous sauf les personnes autorisées.
- L'authentification : permet de prouver l'authenticité par la confirmation de l'identité d'une entité.
- L'intégrité des informations : garantie selon laquelle les données ne sont pas modifiées (par des utilisateurs non autorisés) lors du stockage ou du transfert.
- Non répudiation : cela consiste à garantir qu'aucun des partenaires ne puisse nier la transaction effectué.
- La disponibilité : garantir l'accès à un service ou une donnée.
- Contrôle d'accès : limiter l'accès aux ressources aux personnes privilégiées.
- Message d'authentification : la confirmation de la source de l'information.
- Signature : le moyen de lier l'information à une entité.

3.3. Le modèle simplifié de la cryptographie

Par convention on utilise les noms d'Alice, Bob et Eve pour designer respectivement l'émetteur du message, le récepteur final et l'intrus qui va essayer d'intercepter le message.

Un système de cryptographie est constitué d'un texte en clair et d'un texte chiffré, algorithme de chiffrement et de déchiffrement, ainsi que de toutes les clés, comme le montre la figure suivante :

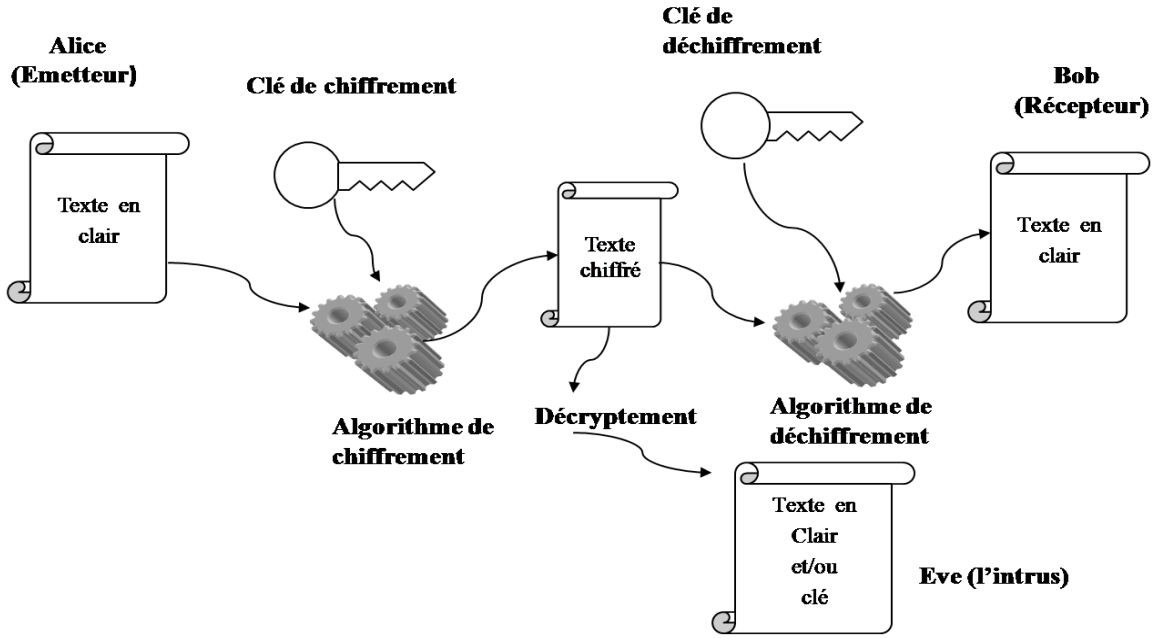

Figure 1.1 .modèle simplifie de la cryptographie

3.4. Les différents types de cryptographie

Nous présentons dans cette section deux techniques de cryptographie.

3.4.1. Cryptographie symétrique ou à clé secrète :

Dans le chiffrement symétrique une même clé secrète est partagée entre les correspondants, comme le montre la figure 1.2, 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.

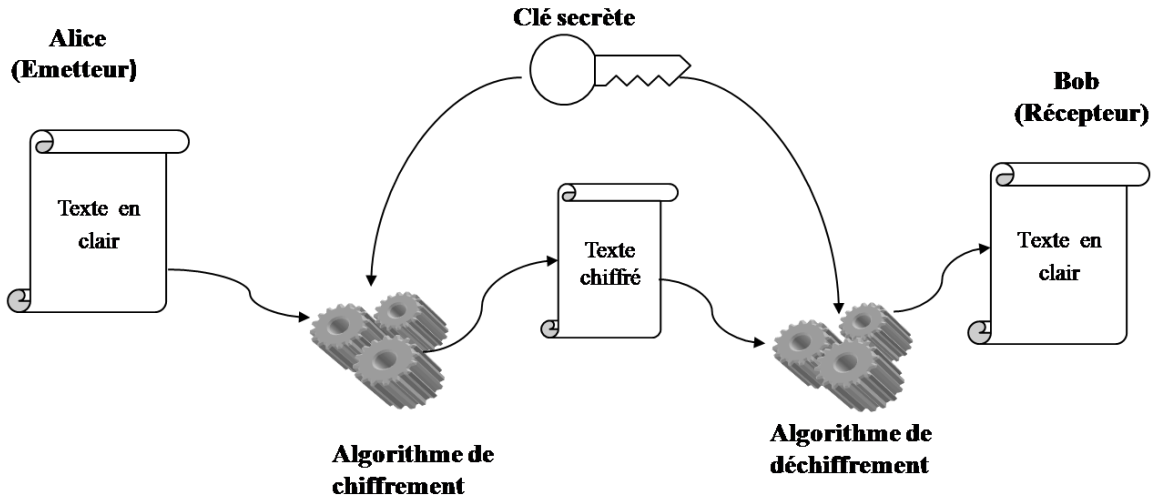

Figure 1.2. Principe de la cryptographie symétrique.

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:

1. 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 un bloc à la fois.
   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.
2. Le chiffrement de flux : ces algorithmes chiffrent les messages bit par bit quelque soit la longueur du message à coder sans besoin de les découper.

Avantage

- Adapté au grand flux de données à chiffrer.
- Simple et facile à implémenter.

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.

3.4.2. Cryptographie asymétrique ou à clé publique

Chaque correspondant possède deux clés, une est publique et donc connue par tous le monde, et elle ne permet que de chiffrer un message, pas de le déchiffrer, par contre la seconde clé est privée et ne permet que le déchiffrage, comme le montre la figure 1.3.

Pour envoyer un message qu'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 [2].

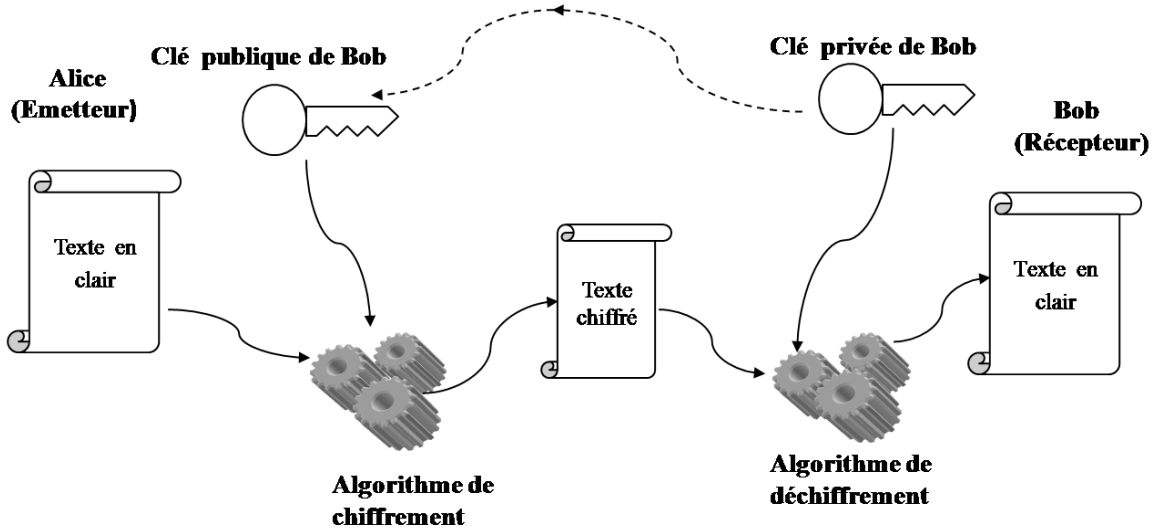

Figure 1.3. Le principe de la cryptographie asymétrique

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 : Diffie Hellman, RAS (Rivest, Shamir, Adelman), El Gamal.

3.5. Clé de cryptage

Les algorithmes de cryptages se basent sur une clé, dans ce paragraphe nous présentons les aspects relatifs à la longueur, à la gestion et les problèmes de distribution des clés :

3.5.1. Longueur de la clé

La sécurité d'un cryptosystème à clé secrète dépend de deux paramètres :

- La longueur de la clé.
- La solidité de l'algorithme.

On parle de solidité parfaite s'il n'existe pas de meilleurs moyens pour casser le cryptosystéme que d'essayer toutes les clés possibles, on parle d'attaque exhaustive.

Une attaque exhaustive sur une clé de 56 bits nécessite la vérification de 2^{56} (2^{56}=7.2 10^{16}) combinaisons possibles, avec un ordinateur puissant possédant un microprocesseur traitant 10 milliard de clés par seconde**,** il faut 83 jours pour trouver la bonne clé.

3.5.2. Gestion des clés

La gestion des clés est le problème de sécurité le plus difficile. Concevoir des algorithmes et des protocoles sûrs n'est pas chose facile mais être sûr que les clés restent secrètes est encore plus délicat.

3.5.3. Problème de distribution des clés

La cryptographie à clé secrète ne permet pas une sécurité complète puisque la divulgation de la clé doit se faire par un moyen traditionnel comme la poste ou le téléphone. Pour ce qui est de la cryptographie à clés publiques, les utilisateurs doivent pouvoir obtenir leur clé privée de manière tout à fait sûre et toutes les clés publiques doivent être accessibles pour appeler le gestionnaire de clés. Le gestionnaire peut être par exemple un serveur grâce auquel les clés publiques peuvent être consultées. [3]

Un des problèmes principaux en matière de cryptographie est la distribution des clés c'est-a-dire comment faire pour qu'une clé ne soit pas connue que par les personnes concernées ?

4. Evolution vers la cryptographie quantique

La cryptographie quantique, plus correctement nommée distribution quantique de clés, désigne un ensemble des protocoles permettant de distribuer une clé de chiffrement secrète entre deux interlocuteurs distants, tout en assurant la sécurité de la transmission grâce aux lois de la physique quantique et de la théorie de l'information. Cette clé secrète peut ensuite être utilisée dans un algorithme de chiffrement symétrique, afin de chiffrer et déchiffrer des données confidentielles.

En effet, cette méthode permet non seulement de démasquer toute tentative d'espionnage grâce aux propriétés de la mécanique quantique, mais également de réduire la quantité d'information détenue par un éventuel espion à un niveau arbitrairement bas [4]. La cryptographie quantique constitue donc un outil précieux pour des systèmes de cryptographie symétrique où les deux interlocuteurs doivent impérativement posséder la même clé.

Le système de cryptographie quantique est utilisé essentiellement pour communiquer une clé, et non le message en lui-même par ce que les bits d'informations communiqués par les dispositifs de la cryptographie quantique ne peuvent être qu'aléatoires. Ceci ne convient pas pour un message, mais convient parfaitement bien à une clé. Les fondements de la cryptographie quantique ont été établis, entre autre, par les travaux de Charles H. Bennet et Gilles Brassard en 1984 et les premières idées ont été posées par Stephen Wiesner dans les années 1970.

5. Conclusion

L'étude des principes de bases de cryptographie classique nous à permis de cerner les atouts et les limites des divers schémas cryptographies.

Afin de remédier à ces limites et particulièrement le problème des distributions des clés, des nouvelles techniques ont vu le jour à savoir la cryptographie quantique, c'est l'objet principal de la section suivante.

Chapitre 2

La cryptographie quantique

1. Introduction

La cryptographie quantique est apparue comme une solution fiable pour assurer un transfert sécurisé des clés. Son apparition à vu le jour voici une trentaine d'année quand deux chercheurs, Charles Bennett et Gilles Brassard, ont eu l'idée d'utiliser les principes de la physique quantique pour transmettre des messages de façon confidentielle. La transmission se fait au moyen d'impulsion de photon individuel « quanta » de lumière envoyées d'un émetteur (Alice) à un récepteur (Bob) et voyageant à travers une fibre optique.

Dans ce chapitre, nous décrivons brièvement quelques concepts de base de la théorie de l'information et de l'information quantique. Par la suite, nous décrivons les principes de la distribution de clés quantiques. Ainsi, que certains protocoles proposés dans ce sens.

2. Théorie de l'information :

La théorie de l'information à été fondée par Claude Shannon peu après la seconde guerre mondiale. Et explique comment compresser au maximum l'information (1^{ere} théorème de Shannon) et la transmettre de façon à réduire au maximum le taux d'erreur sur un canal bruité (2^{eme} théorème de Shannon) [5].

2.1. Entropie de Shannon H(x)

L'entropie de Shannon a diverses significations :

- L'entropie de Shannon est la moyenne de la longueur d'un message, c'est-à-dire qu'une augmentation de la moyenne de la longueur d'un message augmentera l'entropie de Shannon.
- Plus l'entropie de Shannon est grande sur une variable, plus cette variable a un contenu aléatoire, c'est-à-dire qu'une augmentation de la variabilité du contenu de la variable augmentera l'entropie de Shannon.
- Symétriquement, plus l'entropie de Shannon est grande sur une variable, plus on a de l'information nouvelle, et moins elle a de chances d'apparaitre. Inversement, une information connue n'apportera aucune information nouvelle. Son contenu ne sera pas aléatoire. Son entropie sera nulle.

Certains messages (tel que des mots, des nombres,…) peuvent avoir une probabilité d'apparition différente. Ainsi, les messages avec une forte probabilité devront être codés sur un nombre petit de bit, alors que ceux qui ont une faible probabilité pourront être codés sur un nombre de bits plus conséquent. Grace à cela, on réduit le nombre de bits envoyés d'un lieu à un autre, ce qui implique une augmentation de la vitesse de transmission de l'information.

L'entropie d'une variable aléatoire peuvent valoir un ensemble de message différents se trouvant dans l'ensemble χ vaut [6] :

$$H(\chi) = -\sum_{x\in\chi} \mathrm{p(x)} * log_2(p(x)) \qquad (2.1)$$

Ou p(x) représente la probabilité d'avoir la valeur x

2.2. Entropie conditionnelle de Shannon H(X|Y)

Représentons (X, Y) comme une paire de variable aléatoires dont la distribution de probabilité vaut $p(x, y)$ [6].

$$H(X, Y) = H(X) + H(X|\mathrm{Y}) \qquad (2.2)$$

$$H(X, Y) = \mathrm{H(Y)} + \mathrm{H(Y|X)} \qquad (2.3)$$

$H(X)$ Est l'incertitude moyenne des entrées du canal. $H(Y)$ Est l'incertitude moyenne des sorties du canal.

L'entropie conditionnelle $H(X|\mathrm{Y})$ est une mesure d'incertitude moyenne du canal qui reste au sujet des entrées du canal.

L'entropie conditionnel $\mathrm{H(Y|X)}$ est une mesure d'incertitude moyenne des sorties du canal étant donné la transmission de X.

L'entropie conjointe $H(X, Y)$ est l'incertitude moyenne du canal de communication

2.3. Information mutuelle

L'information émise par la source est représentée par X et l'information reçues par le destinataire est représentée par Y.

$P\ (y|x)$ Est la probabilité d'avoir « y » sachant qu'on a émis«x ». L'information mutuelle (ou l'entropie mutuelle) est définie par [6] :

$$I(X;Y) = H(X) + H(Y) - H(X,Y) = I(Y;X) \qquad (2.4)$$

Ce qui peut ramener à :

$$I(X;Y) = H(X) - H(X|Y) \qquad (2.5)$$

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

2.4. Correction d'erreurs

La correction d'erreurs est également gérée par la théorie de l'information [7]. Cette méthode permet de coder l'information pour qu'elle puisse résister à un certain taux d'erreurs causées par le canal sur lequel l'information passe.

3. Introduction à l'information quantique

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

3.1. Polarisation de la lumière

La lumière est une onde électromagnétique et en même temps elle est un flux de particules appelées photons [8]. Sa nature ondulatoire révèle qu'elle est composée d'un champ électrique $\vec{E} = \overrightarrow{E_0}\cos(\omega t - kz)$ et d'un champ magnétique $\vec{H} = \overrightarrow{H_0}\cos(\omega t - kz)$ perpendiculaires entre eux et contenus dans un plan perpendiculaire à la direction de propagation $\overrightarrow{n}$. Ce plan est appelé le plan d'onde. Pour une lumière non polarisée, ou naturelle, E tourne autour de son axe de façon aléatoire et imprévisible au cours du temps. La Polarisation d'une lumière correspond à donner une trajectoire bien définie au champ E.

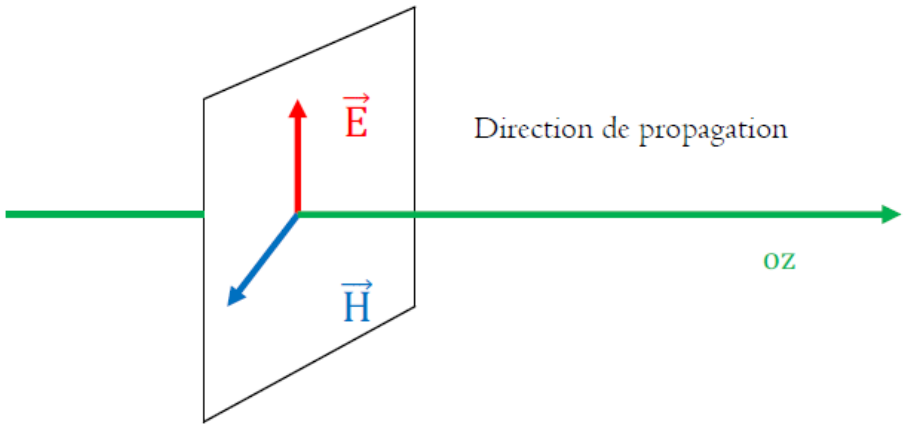

Figure 2.1 : Orientation des champs électrique et magnétique de l'onde lumineuse

Lorsque l'onde lumineuse est filtrée par un polaroïd, la polarisation est un vecteur du plan xoy, à travers la direction de propagation.

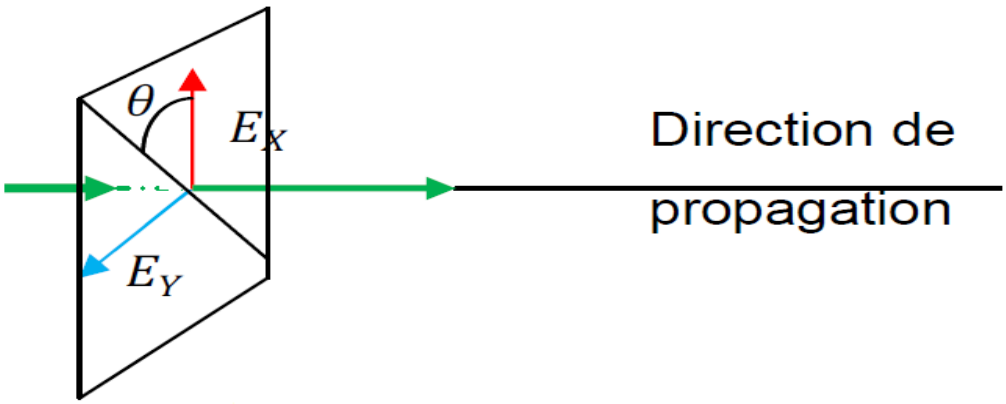

Figure 2.2 : polarisation de la lumière par un polaroïd

Remarque : une lame biréfringente permet de séparer deux états de polarisation orthogonaux, tandis qu'un polaroïd absorbe une des deux polarisations en laissant passer la polarisation orthogonale.

L'équation du champ électrique [8] :

$$\vec{E} = \overrightarrow{E_0}\cos(\omega t - kz) \qquad (2.6)$$

Où ω est la fréquence de vibration $\omega = ck$.

Dans le plan $z = 0$: $\vec{E}(z = 0, t) = \overrightarrow{E_0}\cos\omega t$ (2.7)

$$\vec{E} = \begin{cases} E_0 \cos\theta \cos\omega t \\ E_0 \sin\theta \cos\omega t \end{cases} \qquad (2.8)$$

D'où θ est l'angle d'inclinaison du polaroid sur la direction de propagation oz .

L'intensité de la lumière mesurée à l'aide d'une cellule photoélectrique est proportionnelle au carré du champ électrique $I \propto E_0^2$. Le vecteur unitaire $\vec{P}$ du plan xoy, tel que $\overrightarrow{P}(\cos\theta, \sin\theta)$.

$\vec{E} = \vec{P}E_0 \cos\omega t$ Caractérise la polarisation de l'onde (linéaire) lumineuse.

- Si $\theta = \pi/2$, la lumière est polarisée suivant oy $(Ey = 0)$.
- Si $\theta = 0, Ey = 0$, la lumière est polarisée suivant $ox, (E = Ex)$.

Pour étudier de façon quantitative la polarisation de la lumière, nous allons servir d'un ensemble polariseur-analyseur.

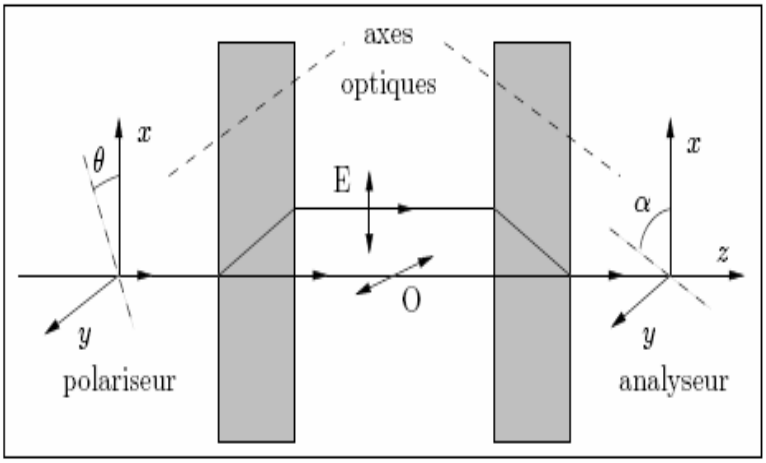

Figure 2.3. Décomposition et recombinaison de la lumière par un ensemble polariseur-analyseur.

Le rayon extraordinaire E est polarisé verticalement et le rayon ordinaire O est polarisé horizontalement.

La lumière passe dans un polariseur dont l'axe est orienté d'un angle θ par rapport à l'axe ox, puis dans un second polariseur appelé analyseur, dont l'axe fait un angle α avec l'axe ox. A la sortie de l'analyseur, le champ électrique $\vec{E}$ de l'onde projeté sur la normale $\vec{n}$ est [7] :

$$\vec{E} = (\vec{E}.\vec{n})\vec{n} = E_0 \cos\omega t\,.(\vec{P}.\vec{n})\vec{n}$$

$$= E_0 \cos\omega t\,(\cos\theta\cos\alpha + \sin\theta\sin\alpha)\vec{n} \quad (2.9)$$

$$= E_0 \cos\omega t\,(\cos\theta - \alpha)\vec{n}$$

On en déduit la loi de Malus pour l'intensité $I' = Icos^2(\theta - \alpha)$

3.2. Le Photon

3.2.1. Nature et propriétés du photon

Les photons ont été originellement appelés par Albert Einstein « quanta de lumière ». Leur existence a été prédite par ce dernier mais c'est Arthur Compton qui fit leur découverte en 1923. En physique des particules, le photon est souvent symbolisé par la lettre γ (gamma). C'est une particule élémentaire de masse nulle et de spin 1. Du fait de son spin, le photon transporte également un moment cinétique intrinsèque dont la projection sur l'axe de propagation est $-\hbar$ ou $+\hbar$.

Dans le premier cas on parle de polarisation circulaire gauche, dans le second cas on parle de polarisation circulaire droite. Il est possible de produire des photons grâce aux processus suivants :

- Transition électronique
- Transition nucléaire
- Annihilation des paires particules antiparticule. Ils sont absorbés par les processus inverses. La polarisation d'un photon est liée à l'orientation de son spin.

Il peut être polarisé linéairement, circulairement ou elliptiquement.

3.2.2. Polarisation d'un photon

En réduisant considérablement l'intensité lumineuse, on peut étudier individuellement la polarisation des photons qu'on détecte à l'aide de photomultiplicateurs.

On peut appliquer ce phénomène à un photon individuel, c'est-à-dire la polarisation du photon [9]. Le photon peut être polarisé par n'importe quel angle dans les plans perpendiculaires à la direction de propagation du photon.

Dans la figure ci-dessous : une lame biréfringente sépare un faisceau lumineux dont la polarisation fait un angle θ avec Ox en un faisceau polarisé suivant Ox et un faisceau polarisé suivant Oy, les intensités étant respectivement $I\ cos^2\ \theta\ \ et\ I\ sin^2\ \theta$. Réduisons l'intensité de telle sorte que les photons arrivent un à un, et plaçons deux photo-détecteurs $Dx\ et\ Dy$ derrière la lame

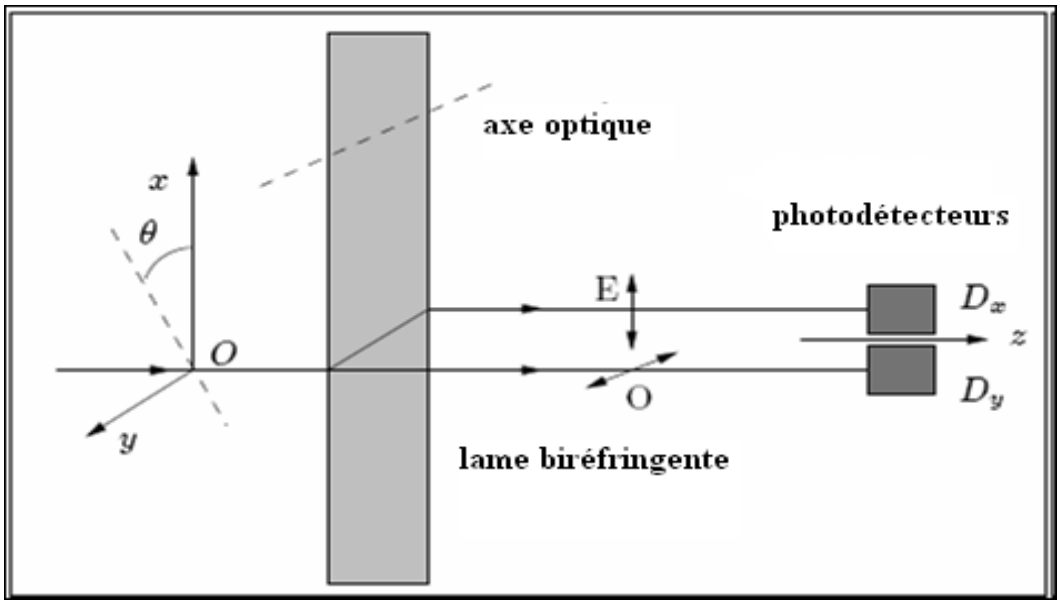

Figure 2.4. Décomposition de la polarisation par une lame biréfringente.

L'expérience montre qu'un photon ne clique jamais simultanément sur $Dx\ et\ Dy$: un seul photon arrive soit sur Dx (si le rayon extraordinaire E est polarisé verticalement), soit sur Dy (si le rayon ordinaire O est polarisé horizontalement).

D'autre part un photon peut choisir le trajet X avec une probabilité de $cos^2\ \theta$, et le trajet Y avec une probabilité de$sin^2\theta$. Il a ensuite la probabilité $cos^2\ \alpha(\ sin^2\ \alpha)$ pour le trajet X et $sin^2\ \alpha$ pour le trajet Y de traverser l'analyseur.

La probabilité totale s'obtient en additionnant les probabilités des deux trajets possibles :

$$P_{tot} = cos^2\ \theta\ \ sin^2\alpha + sin^2\ \theta\ \ sin^2\ \alpha \qquad (2.10)$$

Ce résultat s'avère être faux expérimentalement. En effet l'optique classique nous apprend que l'intensité est : $Icos^2\,(\theta - \alpha)$

Alors le résultat correct confirmé par l'expérience est : $P_{tot} = cos^2\,(\theta - \alpha)$ (2.11)

En fait, pour retrouver les résultats de l'optique ondulatoire, il faut introduire en physique quantique la notion fondamentale d'amplitude de probabilité, dont le module carré donne la probabilité :

$$a(\theta \to x) = \cos\theta \qquad a(x \to \alpha) = \cos\alpha$$

$$a(\theta \to y) = \sin\theta \qquad a(y \to \alpha) = \sin\alpha$$

On doit additionner les amplitudes pour des trajets indiscernables :

$$a_{tot} = \cos\theta\cos\alpha + \sin\theta\sin\alpha = \cos(\theta - \alpha) \qquad (2.12)$$

Ce qui donne : $P_{tot} = |a_{tot}|^2 = cos^2(\theta - \alpha)$ (2.13)

En résumé, c'est impossibilité de répondre à la question quel trajet le photon choisira et les résultats que nous venons de décrire nous plonge au cœur de la physique quantique.

On peut utiliser la polarisation des photons pour transmettre de l'information. Par exemple on décide, tout à fait arbitrairement, d'attribuer la valeur 1 bit à un photon polarisé suivant Ox et la valeur 0 à un photon polarisé suivant Oy. Alors, Alice envoie à Bob une suite de photons polarisés suivant $yyxyxyyyx$ …. Ensuite, Bob analyse la polarisation de ces photons à l'aide d'une lame biréfringente et en déduit le message d'Alice 001010001 ...

C'est de cette façon d'échanger l'information qui est à la base de la communication quantique [10]. Cependant la question véritable est de savoir : quelle est la valeur du bit que l'on peut attribuer par exemple à un photon polarisé à $45°$?

Un photon polarisé à $45°$ est une superposition linéaire d'un photon polarisé suivant Ox et d'un photon polarisé suivant Oy. Cette superposition linéaire de polarisations suivant ox et oy correspond au qubit. Un qubit est donc entité beaucoup plus riche qu'un bit ordinaire, qui ne peut prendre que les valeurs 0 et 1. En un sens, un qubit peut prendre toutes les valeurs intermédiaires entre 0 et 1 et contiendrait donc une quantité infinie d'information. Cependant cet énoncé optimiste est immédiatement démenti lorsque l'on se rend compte que la mesure

du qubit ne peut donner que le résultat 0 ou 1, quelle que soit la base choisie. Malgré tout on peut se poser la question de cette « information cachée » dans la superposition linéaire.

Afin de décrire mathématiquement ces combinaisons linéaires, nous allons considérer que les états de polarisation engendrent un espace vectoriel $\mathcal{H}$, dont les bases sont les vecteurs $|x\rangle\ et\ |y\rangle$ correspondant aux polarisations linéaires suivant $Ox\ et\ Oy$ [10]. Tout état de polarisation pourra se décomposer suivant cette base :

$$|\phi\rangle = \lambda|x\rangle + \mu|y\rangle \qquad (2.14)$$

Les coefficients $\lambda\ et\ \mu$ réels pour une polarisation linéaire, mais ils sont complexes pour les polarisations circulaire et elliptiques : l'espace $\mathcal{H}$est donc un espace vectoriel complexe.

Les amplitudes de probabilité vont correspondre à un produit scalaire sur cet espace.

Soit deux vecteurs $|\phi\rangle\ et\ |\psi\rangle$ deux vecteurs de $\mathcal{H}$.

Avec $|\psi\rangle = \nu|x\rangle + \delta|y\rangle\ et\ |\phi\rangle = \lambda|x\rangle + \mu|y\rangle$.

Alors le produit scalaire de ces deux vecteurs sera noté $\langle\Psi|\Phi\rangle$ est par définition :

$$\langle\psi|\Phi\rangle = \lambda^*\nu + \mu^*\delta = \langle\psi|\Phi\rangle^* \qquad (2.15)$$

Ou $\lambda^*\ et\ \mu^*$ sont respectivement les conjuguées de λ et μ.

Il est à noter que les vecteurs $|x\rangle\ et\ |y\rangle$ sont orthogonaux et normés

$$\langle x|x\rangle = \langle y|y\rangle = 1 \qquad \langle x|y\rangle = 0 \qquad (2.16)$$

La base $\{|x\rangle, |y\rangle\}$ est donc une base orthonormée de $\mathcal{H}$.

Alors on a :

$$||\phi||^2 = |\lambda|^2 + |\mu|^2 = 1 \qquad (2.17)$$

Les états de polarisation seront donc représentés mathématiquement par des vecteurs unitaires de l'espace $\mathcal{H}$ [9]. Un espace vectoriel muni d'un produit scalaire défini positif est appelé un espace de Hilbert, et $\mathcal{H}$ est l'espace de Hilbert des états de polarisation.

Un état de polarisation linéaire (figure 2.4) suivant θ est noté $|\theta\rangle$ et on a :

$$|\theta\rangle = \cos\ \theta\ |x\rangle + \sin\theta\ |y\rangle \qquad (2.18)$$

L'amplitude de probabilité pour qu'un photon polarisé suivant θ traverse un analyseur orienté suivant α est donnée par :

$$\alpha(\theta \to \alpha) = \langle\alpha|\theta\rangle = \cos(\theta - \alpha) \qquad (2.19)$$

Elle est donc donnée par le produit scalaire des vecteurs |α⟩ et |θ⟩, et la probabilité de traverser l'analyseur est donné par le module carré de cette amplitude

$$P(\theta \to \alpha) = \langle\alpha|\theta\rangle^2 = cos^2(\theta - \alpha) \qquad (2.20)$$

De façon générale, on définit les amplitudes « l'amplitude de probabilité de trouver $|\phi\rangle$ dans $|\psi\rangle$ », où $|\phi\rangle$ et $|\psi\rangle$ représente les états de polarisation par : $a(|\phi\rangle \to |\psi\rangle) = \langle\psi|\phi\rangle$

Et la probabilité correspondante sera :

$$P(|\phi\rangle \to |\psi\rangle) = |a(|\phi\rangle \to |\psi\rangle)|^2 = |\langle\psi|\Phi\rangle|^2 \qquad (2.21)$$

3.3. Qubit

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

L'expression du qubit est donnée par : $\psi = \alpha|0\rangle + \beta|1\rangle \qquad (2.22)$

Ou α et β sont des coefficients complexes, ils représentent les amplitudes de probabilité d'obtenir l'état $|1\rangle$ et l'état $|0\rangle$ respectivement lors d'une mesure de l'état $|\psi\rangle$. Ces deux états constituent une base orthogonale de l'espace de Hilbert du système. Ces coefficients satisfont la condition de normalisation suivante : $|\alpha|^2 + |\beta|^2 = 1 \qquad (2.23)$

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

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

$|1\rangle$ Et $|0\rangle$: représente deux états orthogonaux dans le système quantique.

En général, la représentation géométrique du qubit est donnée par la sphère de Bloch (figure 2.4). L'état $|\psi\rangle$ qubit est un point de la surface de la sphère, la superposition des états $|1\rangle$ et $|0\rangle$ permet de représenter une infinité de quantité d'information [12].

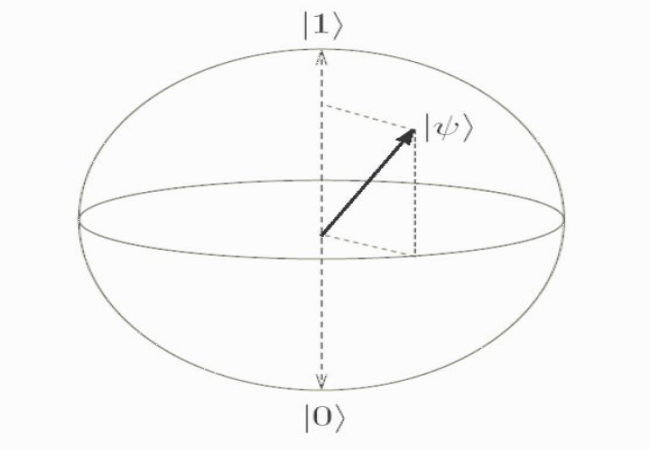

Fig.2.5 : représentation de qubit sur la sphère de Bloch

Une autre particularité du qubit par rapport à un bit classique est qu'il ne peut être dupliqué. En effet, pour le dupliquer, il faudrait pouvoir mesurer α et β d'une qubit (tout en préservant l'état du qubit), de sorte à préparer un autre qubit dans le même état $\alpha|0\rangle + \beta|1\rangle$.

Ceci est doublement impossible :

- Il est impossible de lire un qubit sans détruire définitivement son état (puisque après mesure le qubit est dans l'état mesurée)
- Une mesure d'un qubit ne donne aucune information sur $\alpha\ et\ \beta$ puisque le résultat est soit $|0\rangle\ soit\ |1\rangle$ ce qui équivaut à $(\alpha, \beta) = (1,0)$ ou (0,1) ce qui ne correspond pas aux valeurs initiales de α et β.

3.4. Le problème de la mesure en physique quantique

La mesure de l'état d'un système quantique n'est pas une fonction réelle comme dans la mécanique classique [9]. La notion de mesure en physique quantique repose sur celle de la préparation d'un état quantique et celle du test.

Supposons un polariseur qui prépare le photon dans l'état :

$$|\theta\rangle = \cos\ \theta\ |x\rangle + \sin\theta\ |y\rangle$$

Après le passage dans l'analyseur, l'état de polarisation du photon n'est plus $|\theta\rangle$ mais $|x\rangle$ si l'analyseur est orienté suivant ox. L'analyseur vient d'effectuer un test (de polarisation).

Ce test permet donc de connaitre la polarisation du photon. La mesure modifie donc l'état de polarisation du photon. Le test est réussi avec une probabilité de $cos^2\theta$. Le test ne permet pas de déterminer la polarisation du photon de façon non ambiguë. Seuls les cas où la probabilité du test vaut 0 ou 1 nous renseignent sur l'état de polarisation initiale. Il n'existe pas de test permettant de déterminer de manière sûre l'état de polarisation d'un photon. On constate donc une différence de principe entre une mesure en physique classique et la mesure en physique quantique : en physique classique, la quantité à mesurer préexiste à la mesure. Dans l'expérience du test de polarisation, le fait que le test donne une polarisation suivant ox ne permet pas de conclure que le photon test avait au préalable sa polarisation suivant ox.

La mesure quantique permet de détecter l'espionnage du canal quantique. Si un espion, intercalé entre Alice et Bob, tente de mesurer l'état de polarisation des photons envoyés par Alice, il utilisera avec probabilité $\frac{1}{2}$ la mauvaise base de polarisation. Ce faisant, il projettera l'état quantique sur l'état propre correspondant à la valeur de sa mesure. Si les choix de base d'émetteur (Alice) sont adaptés, cet état n'est plus un état propre de la base initialement choisie par Alice, et la valeur du bit envoyé aura une certaine probabilité d'erreur à son arrivée chez le récepteur (Bob) [14].

3.5. Principe fondamentaux de la distribution à clé quantique

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

3.5.1. Principe d'incertitude de Heisenberg

3.5.1.1. Enoncé du principe

Ce principe a été énoncé par Werner Heisenberg en 1926, il stipule que :

Plus la position d'une particule est déterminer avec précision moins son impulsion peut l'être.

Si on détermine la position d'une particule suivante x de l'impulsion p_x avec une incertitude Δp_x, on ne peut déterminer en même temps sa position x avec une incertitude Δx inférieure à $\frac{\hbar}{2\Delta p_x}$

Les inégalités de Heisenberg sont données par [15] :

$$\Delta x\ \Delta p_x\ \geq \frac{\hbar}{2} \qquad \Delta y\ \Delta p_y\ \geq \frac{\hbar}{2} \qquad \Delta z\ \Delta p_z\ \geq \frac{\hbar}{2} \qquad (2.24)$$

Désignons par $\Delta x\ \Delta y\ \Delta z$ et $\Delta p_x\ \Delta p_y \Delta p_z$ les « erreurs » (incertitudes) sur la position et l'impulsion.

Où $\hbar$ est la constante de Dirac (du nom du physicien Paul Dirac) est dérivée de la constante de Planck h. Elle est également appelé constante de Planck réduite [16].

Cela signifie que l'incertitude sur la position multipliée par l'incertitude sur l'impulsion est supérieure ou égale à une constante. Ce qui implique que le comportement de la matière à l'échelle atomique n'est pas déterminé ou prévisible.

3.5.1.2. Application du principe à la cryptographie quantique

Le principe d'incertitude d'Heisenberg repose sur le fait qu'en mécanique quantique il est impossible de mesurer une de deux propriétés d'une paire de propriétés complémentaires sans perturber l'autre. Ainsi, pour établir un protocole quantique de distribution des clés secrètes, il faut choisir une paire de bases conjuguées et utiliser les photons non pas pour garder de l'information mais bien pour transmettre de l'information.

3.5.2. Théorème de non Clonage

3.5.2.1. Enoncé du théorème

Il n'existe pas de transformation unitaire U qui permette de cloner parfaitement l'état $|\psi\rangle$

Tel que [17] : $$U(|\psi\rangle|\mu\rangle) = |\psi\rangle|\psi\rangle \qquad (2.25)$$

Pour démontrer le théorème, supposons qu'on veuille dupliquer un état quantique inconnu $|X_1\rangle$. Le système sur lequel on veut imprimer la copie est noté φ : c'est l'équivalent

de la feuille blanche. L'évolution du vecteur d'état dans le processus de clonage doit être de la forme $|X_1 \otimes \varphi\rangle \rightarrow |X_1 \otimes X_1\rangle$

Cette évolution est régie par un opérateur unitaire U tel que :

$$|U(X_1 \otimes \varphi)\rangle = |X_1 \otimes X_1\rangle$$

L'opérateur U doit être universel (l'opération de photocopie ne doit pas dépendre de l'état à photocopier) et donc indépendant de $|X_1\rangle$, qui est inconnu par hypothèse. Si on veut cloner un second original $|X_2\rangle$, on doit avoir : $|U(X_2 \otimes \varphi)\rangle = |X_2 \otimes X_2\rangle$

Evaluons maintenant le produit scalaire :

1. $Y = \langle X_1 \otimes \varphi | X_2 \otimes \varphi\rangle = \langle X_1 | X_2\rangle$
2. $Y = \langle X_1 \otimes X_1 | X_2 \otimes X_2\rangle = (\langle X_1 | X_2\rangle)^2$

De (1) et (2), il résulte que $|X_1\rangle \equiv |X_2\rangle$; soit $\langle X_1 | X_2\rangle = 0$

En conclusion il est possible de cloner un état $|X_1\rangle$ ou un état orthogonal, mais pas une superposition linéaire des deux.

3.5.2.2. Application du théorème

Basé sur le principe d'incertitude, il n'existe aucune façon de connaitre sûrement un état. Et c'est impossible de cloner un état inconnu. C'est à dire que l'on ne peut pas obtenir une copie identique d'un état aléatoire de qubit.

3.6. Quelques types de protocoles de distribution de clé quantique

Plusieurs protocoles sont proposés afin de discipliner la cryptographie quantique. Nous récapitulons certains d'entre eux dans la suite de cette section.

3.6.1. Protocole BB84

BB84 est un protocole de distribution de clé le plus connu. Il utilise quatre états différents qui font une paire des états de base. BB84 est un protocole non déterministe. Cela signifie qu'il distribue une suite aléatoire des bits [18].

Le but est de générer une clé partagée entre Alice et Bob n'autorisant aucun tiers à acquérir une information pertinente sur cette clé. Cette clé doit pouvoir servir à un chiffre de Vernam, et conduire ainsi à une transmission d'informations inconditionnellement sûres [19].

Avec le schéma ci-dessous représentant les quatre états non orthogonaux utilisés dans le protocole BB84. Telle que le bit classique est codé par des états quantiques. Chaque état quantique peut représenter les deux bits classique, le 1 ou le 0, et inversement, chaque 0 ou 1 correspond à un mélange de deux états quantiques égaux probablement non orthogonaux.

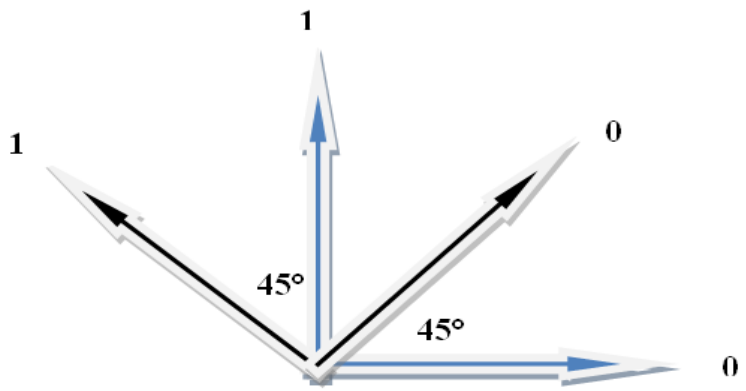

Figure 2.6. Quatre états Non-orthogonaux utilisés dans le protocole BB84

L'information transmise dans le canal quantique est souvent sous la forme de photons polarisés. Le codage des bits classiques est fait en utilisant la direction de la polarisation. Dans le schéma de codage de BB84, le bit classique 0 est représenté par un photon polarisé à 0° et 45° de l'axe horizontal, et les deux directions orthogonales correspondants, 90° et 135°, sont employées pour le bit 1 [17].

Deux mesures sont employées pour distinguer les différents états de qubit :

- La mesure permettant d'identifier clairement entre deux états $|0\rangle$ et $|1\rangle$. Cette mesure s'appelle également la mesure dans la base rectiligne.
- La mesure permettant d'identifier clairement entre deux états $|0'\rangle$ et $|1'\rangle$. Cette mesure s'appelle également la mesure dans la base diagonale.

3.6.2. Protocole à deux états : Protocole B92

En 1992, selon Bennett, quatre états sont trop pour une CQ et seulement deux non-orthogonaux sont suffisants [20].

Le protocole B92 peu être décrit dans un système quantique par la représentation à deux dimension de l'espace d'Hilbert.

Comme le montre le tableau 2.1. Le protocole B92 utilise une base non orthogonale pour coder des bits. On choisit la base de codage suivante : $|\theta\rangle \; et \; |\bar{\theta}\rangle$

Telle que $|\theta\rangle \; et \; |\bar{\theta}\rangle$ représentent la polarisation à l'angle $\theta \; et \; \bar{\theta}$ correspondant, ou $0 < \theta < \frac{\pi}{4}$.

Le protocole BB84 utilise deux bases conjuguées pour coder les bits, par contre le protocole B92 utilise seulement une base non orthogonale. C'est-à-dire on utilise un alphabet quantique non orthogonal. On choisit l'alphabet quantique non-orthogonal A_θ, et de coder les bits comme suivant [21] :

Symbole	Bit
$\|\theta\rangle$	1
$\|\bar{\theta}\rangle$	0

Tableau 2.1. Représentation de la polarisation linaire de l'alphabet quantique A_θ

La sécurité des bases de cryptographie quantique repose sur l'incapacité d'un espion de distinguer sûrement et sans perturbation les états différents qu'Alice envoi à Bob ; par conséquent deux états sont suffisants s'ils sont incompatibles (c'est-à-dire, non mutuellement orthogonaux). Toutefois en pratique, ce protocole n'est pas vraiment efficace. En effet, pour que deux états non-orthogonaux ne puissent pas être distingués clairement sans perturbation, on peut les distinguer clairement au coût d'une certaine perte.

3.6.3. Protocole à trois états

Ce protocole est l'amélioration de BB84. Le protocole BB84 est symétrique dans son utilisation de polarisation. Après la génération de la clé, il est nécessaire d'échanger d'autres

informations pour le secret de la clé. Le protocole à trois-états propose d'employer trois états, au lieu de quatre dans BB84. Ceci réduit la probabilité d'espionnage pour obtenir de bons états ainsi qu'il minimise la quantité de l'information utile envoyée par Alice [22].

3.6.4. Protocole à six états

Tandis que deux états sont suffisants et quatre états sont standard, un protocole à six-états figure 2.6 respecte plus la symétrie de l'espace d'état de qubit. Les six états constituent trois bases, par conséquent, la probabilité qu'Alice et Bob choisissent pour base est seulement 1/3, mais la symétrie de ce protocole simplifie considérablement l'analyse de sécurité et réduit le gain optimal de l'information de l'espion pour un taux donné d'erreurs. Si l'espion mesure tous les photons, il induira une erreur de 33%, en comparaison à 25% dans le cas du protocole BB84 [19].

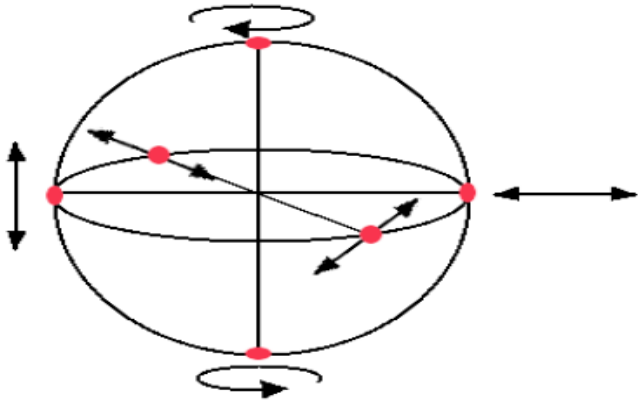

Figure 2.7. Trois paires de bases utilisées dans le protocole à six états

4. Conclusion

L'introduction de l'information quantique et de la théorie de l'information dans ce chapitre nous a permis de définir les différents outils nécessaires à la compréhension des principes fondamentaux du protocole de distribution de clé quantique. Nous avons ensuite donné quelques protocoles de cryptographie quantique. Nous détaillons dans le chapitre suivant le protocole BB84.

Chapitre 3

Description et simulation du protocole BB84

1. Introduction

Le premier protocole de distribution quantique de clé (QKD) a été inventé par Bennett et Brassard en 1984 (BB84). Il permet à deux personnes séparées de construire une clé secrète qu'ils seront les seuls à connaitre, par l'envoi de l'un vers l'autre de photons unique qui provienne d'une source de lumière cohérente, à traverse un canal de transmission quantique (fibre optique, espace libre) et d'un canal publique (radio, internet).

En première partie, nous présenterons le principe du protocole BB84, ainsi ces différentes phases pour distiller une clé secrète entre l'émetteur et le récepteur. Puis nous définirons la sécurité de ce protocole dans les cas ou l'intrus peut influencer sur la sécurité du protocole ou bien lorsque le canal quantique lui même présente des faiblesses et en termine avec une simulation.

2. Schéma de codage quantique du protocole BB84

Avec ce schéma, le bit classique est codé par des états quantiques. Chaque état quantique peut représenter les deux bit classique, le 0 ou le 1, et inversement, chaque 0 ou 1 corresponde à un mélange de deux états quantique égaux probablement non-orthogonaux.

Le protocole BB84 utilise deux bases : la base rectangulaire B_+ (pour les angles 0° et 90°), et la base diagonale B_X (pour les angles 45° et 135°). Les états B_+ et B_X s'écrivent comme suit :

Bit	La base $\boldsymbol{B_+}$		La base $\boldsymbol{B_X}$	
0	Qubit	L'état de photon	Qubit	L'état de photon
	$\|0_+\rangle = \|0\rangle$	$\|\rightarrow\rangle$	$\|0_X\rangle = \frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$\|\nearrow\rangle$
1	$\|1_+\rangle = \|1\rangle$	$\|\uparrow\rangle$	$\|1_X\rangle = \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\|\nwarrow\rangle$

Tableau .3.1. Tableau du codage d'un bit en fonction du choix d'une base.

3. Description du protocole BB84

Dans la description du protocole, on emploie les prénoms classiques pour les différents éléments du protocole. Le prénom Alice employé pour l'émetteur, et le prénom Bob pour le

destinataire. Typiquement, Alice communique avec Bob tandis qu'un intrus essaye d'écouter ou de perturber la communication. Cet intrus est habituellement appelé Eve.

Le schéma général d'un système de distribution de clé quantique est représenté sur la figure 3.1. Alice et Bob disposent de deux canaux pour communiquer, un canal quantique, et un canal public. La distinction faite entre les deux canaux tient uniquement au type d'information véhiculé, états quantiques dans le premier cas et bits d'information classiques dans le second, mais non à leur nature physique.

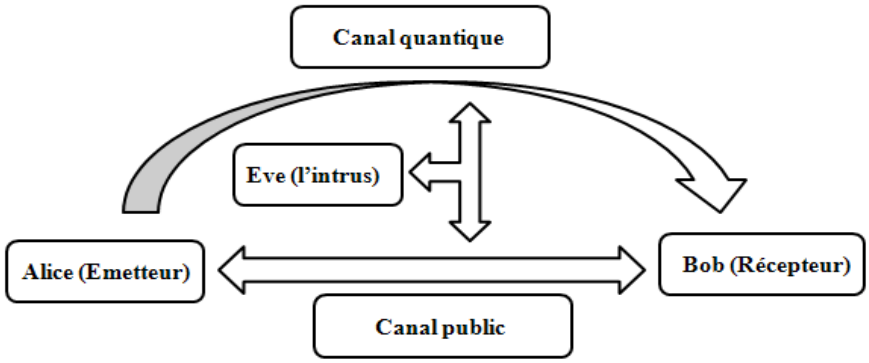

Figure 3.1. Déroulement du protocole BB84 sur les deux canaux public et quantique.

En générale, le protocole BB84 est procède en 5 étapes suivantes :

3.1. Transmission quantique :

Cette phase utilise un canal quantique pour l'échange d'information:

- Alice choisit aléatoirement une chaine de bite classique (0 ou1) et l'une des deux bases (B_+ et B_X) ensuit elle code ses choix sur la polarisation d'un photon et le transmet à Bob via un canal quantique sous forme d'un qubit.
- Bob reçoit les qubit et pour chacun choisit aléatoirement une base (B_+ et B_X) pour effectuer sa mesure. Quand la transmission quantique est finie, Bob obtiendra une chaine de bites classique, appelée clé crue.

3.2. Annonce de Bases

Dans cette phase, toutes les positions, où les mêmes bits sont partagés, seront conservées et le reste sera jeté à l'aide du canal public :

- Bob révèle à Alice son choix de base pour chaque photon reçu.
- Alice compare cet ordre des bases avec le sien et révèle toutes les bonnes à Bob.
- Alice et Bob comparent leurs résultats et rejettent tous les positions des bits où Bob n'a pas fait le bon choix et rejettent les positions des bits qui ne sont pas détectés par Bob. La clé obtenu dans cette étape est appelée la clé tamisé.

3.3. Estimation du taux d'erreur quantique (QBER)

Afin réduire la différence de la clé tamisé entre Alice et de Bob due à l'imperfection d'appareil où bien à une éventuelle intrusion, il est nécessaire de corriger les erreurs. C'est la phase où l'erreur de la clé tamisée est estimée. Ils choisissent alors de se révéler une fraction de la clé tamisé (~10%), ceci leur permet d'estimer le QBER de la transmission. l'émetteur et le récepteur doivent calculer le taux d'erreurs observées et gardent cette transmission si le taux d'erreur est moins a un seuil désiré, sinon la clé sera avortée.

3.4. Réconciliation des données

La réconciliation est un processus interactif, ayant lieu dans le canal public [18]. Le but de cette phase est réduire la quantité d'information qu'Eve a obtenue, et de supprimer tous les bruits dus au canal de communication, ainsi ceux causés par les appareils de mesure ou par Eve. L'algorithme de réconciliation est divisé en deux étapes :

1^{ere} partie :

Alice et Bob sont d'accord pour utiliser une permutation aléatoire et l'applique à la clé crue pour avoir la clé permutée. Ensuite de divisé cette dernier aux blocs dont la longueur est l. Pour comparer les blocs, Alice et Bob vérifient les parités bit de deux blocs correspondants. Après chaque comparaison, Alice et Bob doivent jeter le dernier bit du bloc. Si les parités bits ne sont pas d'accords, ils utilisent l'algorithme « recherche binaire » pour trouver l'erreur bit. Ils divisent chaque bloque à deux sous blocs et comparent les parités bit pour trouver le sous blocs qui contient le bit erreur. Il faut aussi jeter le dernier bit de chaque sous blocs après la comparaison. Cette étape est exécutée plusieurs fois.

2eme partie :

A fin de s'assurer qu'aucune erreur ne se trouve, Alice et Bob échangeront et compareront la parité des sous-ensembles aléatoires en appliquent l'algorithme de recherche binaire. En général, si est une comparaison à N fois. Si jamais après N fois ils ne trouvent pas d'erreurs, alors ils peuvent assurer que la clé est sans erreur avec une grande probabilité. En fin de cette phase, Alice et Bob ont la clé réconciliée.

3.5. Purification

En fin de communication, Alice et Bob ont la même clé réconciliée, ils vont essayer de réduire l'information que possède Eve [23]. Alors ils utilisent un algorithme dit « Purification du sécurité». Pour ce faire, Alice choisit à nouveau des paires de bits dont elle prend leur somme XOR, mais cette fois-ci, elle annonce seulement le numéro des bits. Alice et Bob remplacent simplement la valeur de chacun de ces deux bits par la valeur de leur somme XOR. Ainsi, Alice et Bob n'engendrent pas de nouvelles différences entre leur clé et déduisent l'information d'Eve au détriment bien sûr de la longueur de leur clé. En effet, si Eve ne connait que la valeur du premier bit mais pas du deuxième, elle n'a aucune information sur leur somme XOR. Finalement Alice et Bob disposent d'une clé secrète et sans erreur à propos de laquelle Eve n'a aucune information.

4. Etude du protocole BB84

4.1. Influence de l'espionnage

4.1.1. Attaque interception-renvoi (I-R)

Ce type d'attaque correspond à celles qui sont les plus immédiates à mettre en ouvre, elle consiste pour Eve, à mesure individuellement les impulsions lumineuse émises par Alice, puis à envoyer vers Bob un photon codé dans l'état correspondant au résultat de mesure qu'elle a obtenu [24]. Si Eve a choisi la même base qu'Alice, elle ne sera pas détectée car l'état de polarisation du photon ne sera pas perturbé et Bob mesurera la polarisation avec une probabilité d'erreur égale à 0. Par contre, si Eve choisira une base différente, elle aura une chance sur deux de se tromper. Quand Bob reçoit le photon, s'il a mal polarisé par Eve, il a une chance sur deux d'avoir un résultat différent avec le photon original, et finalement, pour chaque photon intercepté par Eve, il y a une

chance sur 4 que Bob reçoit une information erronée. Ainsi, dans le cas ou Eve intercepte toutes les impulsions à un photon, la probabilité d'erreur induite sera égale à 25%.

4.1.2. Attaque par séparation du nombre de photons (SNP)

L'une des attaques les plus puissantes d'une mise en œuvre expérimentale du protocole BB84 a été imaginée et étudiée par Norbert LUTKENHAUS [25]. Couramment désignée par l'acronyme d'attaque « PNS », elle a permis de définir ce qui est aujourd'hui considéré comme les limites « pratiques » de la cryptographie quantique avec des impulsions cohérentes atténuées.

Cette attaque consiste à séparer de façon déterministe un des photons de l'impulsion envoyé [26]. Pour ce faire, on suppose qu'Eve réalise une mesure quantique non destructive du nombre de photon. Si l'impulsion contient plus d'un photon, Eve en conserve un dans une mémoire quantique et transmet l'autre photon à Bob. Eve attend ensuite que Bob annonce sa base de mesure pour faire la mesure a posteriori, dans la même base. De cette façon, Eve peut acquérir, sans introduire aucune erreur, la totalité de l'information contenue sur l'impulsion à deux photons. Une telle attaque suppose qu'Eve est capable de réaliser une mesure non destructive du nombre de photons et qu'elle dispose d'une mémoire quantique.

4.1.3. Homme-au-milieu

Une imperfection évidente de BB84 est le manque d'authentification. En plus, avec la technologie de niveau élevé, Eve peut penser à une attaque appelée homme-au-milieu ou attaque intermédiaire, dans laquelle Eve devient un truqueur [18]. Elle intercepte le canal sécurisé (celui de quantum) et joue comme Bob avec Alice et inversement. En faisant ainsi, elle peut recueillir toute l'information échangée entre Alice et Bob sans leur doute. Donc, à la fin de casser ce genre d'attaque, l'authentification est le souci le plus grand pour le protocole BB84.

4.2. Influence du canal quantique

4.2.1. Les sources de bruits

Il y a plusieurs sources de bruit : la source lumineuse, les appareils de mesure et le canal de communication.

4.2.1.1. La source de lumière

Le protocole BB84 exige une source du photon unique. Cependant, dû à la limitation de technologie, la source parfaite de photon unique est encore loin de pratique. Dans l'expérience réelle, nous utilisons les sources laser fortement atténuées. Ceci veut dire que chaque impulsion lumineuse qu'elle envoie ne contient qu'un seul photon. En effet si l'impulsion contient plus d'un photon, il suffit à Eve (attaque par SNP) de prélever l'information sur un des photons et de laisser passer l'autre ou les autres photons. Dans ce cas, Alice et Bob ne s'apercevraient jamais qu'ils sont espionnés.

4.2.1.2. Les appareils de mesure

Les photo-détecteurs ne sont pas efficaces à 100%. IL peut arriver qu'ils ne détectent pas un photon ou en comptabilisent un alors qu'il n'existe pas. C'est ce qu'on appelle les coups d'obscurité (dark count). La probabilité d'avoir un coup d'obscurité par seconde n_{dark} est lié la fenêtre temporelle de détection Δ_τ (temps nécessaire à la réception pour détecter l'ensemble des photons incidents) :

$$P_{dark} = n_{dark}\,\Delta_r \qquad (3.1)$$

4.2.1.3. Le canal de communication

Il peut y avoir des interactions avec le milieu, le photon se propage dans la fibre optique. Ces interactions ont pour effet d'absorber les photons, de modifier ses propriétés (polarisation, phase, etc.).

4.2.2. Taux d'erreurs

Un canal réel est naturellement bruité. Le bruit est caractériser par la valeur moyenne du taux d'erreur par bit transmis QBER (quantum Bit Error Rate) [11].

$$QBER = \frac{N_{erreur}}{N_{total}} * 100\% \qquad (3.2)$$

Où :

N_{erreur} : Représente le nombre de bits non corrélatifs entre Alice et Bob, correspondants à un choix identique de bases.

N_{total} : Représente le nombre total de qubits reçues.

Une étude théorique du QBER définit qu'il est équivalent au rapport de la probabilité d'obtenir une fausse détection sur la probabilité totale de détection par impulsion :

$$QBER = \frac{P_{opt}P_{phot} + P_{dark}}{P_{phot} + 2P_{dark}} \approx P_{opt} + \frac{P_{dark}}{P_{phot}} \qquad (3.3)$$

L'expression de QBER se compose de deux termes, le QBER optique par:

$$QBER_{opt} = P_{opt} \qquad (3.4)$$

Et le QBER détecté donné par :

$$QBER_{det} = \frac{P_{dark}}{P_{phot}} \qquad (3.5)$$

Ainsi le QBER totale est donné par :

$$QBER_{tot} = QBER_{opt} + QBER_{det} \qquad (3.6)$$

Le P_{dark} , le P_{phot} , et le P_{opt} sont respectivement les probabilité pour obtenir un coup d'obscurité , pour détecter un photon, et la probabilité de commettre une erreur sur la phase ou la polarisation d'un photon reçu.

L'expression du P_{phot} est donnée par :

$$P_{phot} = \mu\, \eta\, T_l + 4\, n_{dark} \qquad (3.7)$$

D'où :

$$T_l = 10^{-\alpha l/10}$$

Où μ , η et T_l représentent respectivement, le nombre moyen de photon par impulsion, l'efficacité quantique de photo-détecteur et l'efficacité du lien de transmission.

Généralement le P_{opt} en dessous de 1% peut être facilement réalisé avec n'importe quelle installation, $QBER_{opt}$ peut ainsi être négligé. Alors le $QBER_{tot}$ dépendra en majeure partie du $QBER_{det}$ et on peut écrire [26] :

$$QBER_{tot} = \frac{P_{dark}}{P_{phot}} \qquad (3.8)$$

4.3. Calcul de probabilité d'erreur limite

4.3.1. Information mutuelle entre Alice et Bob

Il est utile de comprendre l'effet de la correction d'erreur à l'aide de la théorie de l'information. Soient A et B les variables aléatoires associées aux bits de clé d'Alice et de Bob, lorsque la préparation et la mesure ont été faites dans la même base. Ces variables prennent les valeurs $a, b \in [0.1]$ et sont liée par la distribution de probabilité P_{AB}. Pour une clé tamisée avec un taux d'erreur E et avant d'effectuer la correction d'erreur, l'information mutuelle entre Alice et Bob est donnée par [24] :

$$I(A;B) = 1 + log_2 E + (1-E) log_2 (1-E) \qquad (3.9)$$

Après la correction d'erreur, on a $I(A;B) = 1$ avec une très grande probabilité.

4.3.2. Information moyenne obtenue par l'espion

Les Trois attaques présentées ne tiennent pas compte du bruit des détecteurs. En principe, le bruit aide l'espion, car il camoufle les erreurs qu'il introduit. Cependant, l'effet le plus néfaste du bruit est que les erreurs qu'il induit doivent être considérées comme des erreurs causées par l'espion, ce qui a pour effet de diminuer grandement le taux de génération de clé. En tenant compte de cela, nous allons considérer que pour un taux d'erreur moyen E, l'information moyenne par bit de clé tamisée obtenue par l'espion est donnée par [24] :

$$I = \frac{4\,E}{\sqrt{2}} + \frac{1}{f + \frac{\mu}{2}} \left(\frac{\mu}{2} + \frac{f}{\sqrt{2}} \right) \qquad (3.10)$$

5. Simulation du protocole BB84

La simulation du protocole BB84 offre la possibilité de mener une étude de l'influence des paramètres physiques de l'espion sur la sécurité du protocole. Dans cette étude nous essayons de faire des simulations avec les valeurs des paramètres physiques proches de ce qu'offre l'industrie des composants optiques actuelles. Ceci est dans le but de nous approcher le maximum possible de la réalité des choses et pour pouvoir démontrer la sécurité du protocole BB84 comme étant un protocole d'échange de clé quantique inviolable.

Les résultats obtenus sont sous forme de courbes, nous allons essayer de présenter les résultats les plus importants avec les commentaires nécessaires.

Les notations suivantes ont été utilisées dans touts les simulations:

μ : Le nombre moyen de photons par impulsion.

α : Affaiblissement de la fibre.

L : La longueur de la fibre.

η : Efficacités quantique.

n_{dark} : Taux de coups d'obscurité.

Δ_τ : Temps d'observation.

5.1. Influence de la longueur sur le taux d'erreur

Pour $\mu = 0.1, \alpha = 0.22\ dB/Km, n_{dark} = 50\ coups/s, \Delta_\tau = 3\ \mu s, \eta = 1$

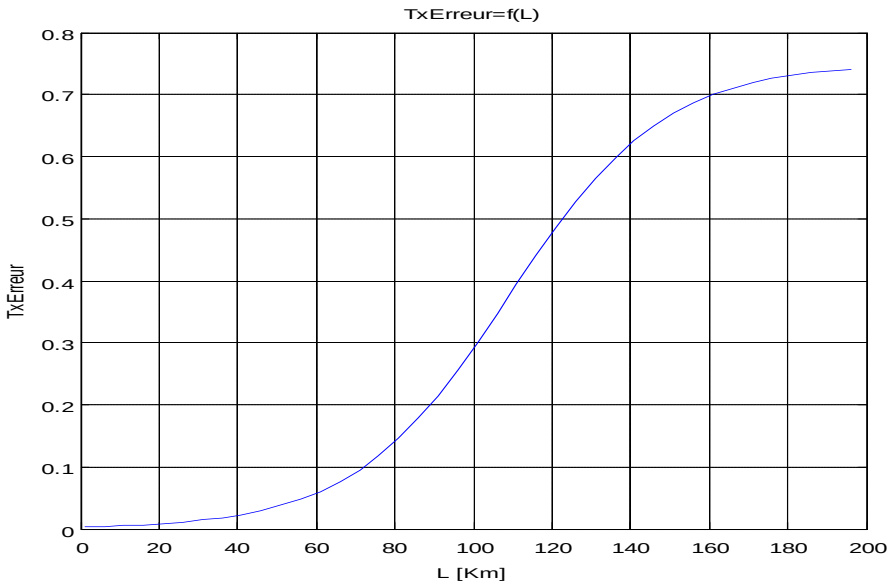

Figure 3.2. Influence de la longueur sur le taux d'erreur

Commentaire

La courbe a été obtenue pour une variation de la longueur de 0 à 200 Km. Il est bien clair que le taux d'erreur augmente avec la longueur puisque la qualité de la liaison se dégrade avec l'augmentation de la distance.

Avec les paramètres spécifiés, la distance maximale sécuritaire de cette liaison est de 80 Km parce qu'on ne doit pas dépasser un taux d'erreurs de 15 % vu qu'au dessous de ce seuil maximal, on est sûr que la quantité d'information que possède l'intrus sur la clé est négligeable même dans le cas ou elle optimise son taux d'intrusion.

5.2. Influence de l'efficacité quantique sur le taux d'erreur

Pour $\mu = 0.1, \alpha = 0.22\ dB/Km, n_{dark} = 10^{-5}\ coups/s, \Delta_\tau = 3\ \mu s, L = 30Km$

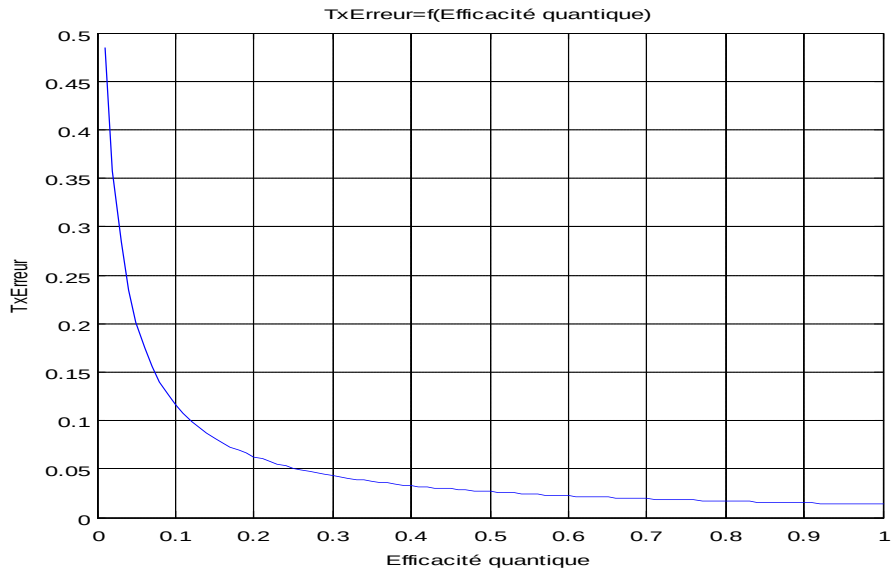

Figure 3.3. Influence de l'efficacité quantique sur taux d'erreur

Commentaire

La courbe a été obtenue pour une variation de η de 0.1 à 1. Il est bien clair que le taux d'erreur diminue avec η puisque la qualité de la liaison s'améliore avec l'augmentation de ce

dernière. On remarque aussi qu'une valeur de $\eta = 0.08$ avec les paramètres déjà spécifiés assure une liaison sécuritaire puisqu'à partir de cette valeur le taux d'erreur inférieur à 15 %

5.3. Influence du nombre moyen de photons par impulsion sur le taux d'erreur

Pour $\eta = 0.2, \alpha = 0.22\ dB/Km, n_{dark} = 10^{-5}\ coups/s, \Delta_\tau = 3\ \mu s\ , L = 30Km$

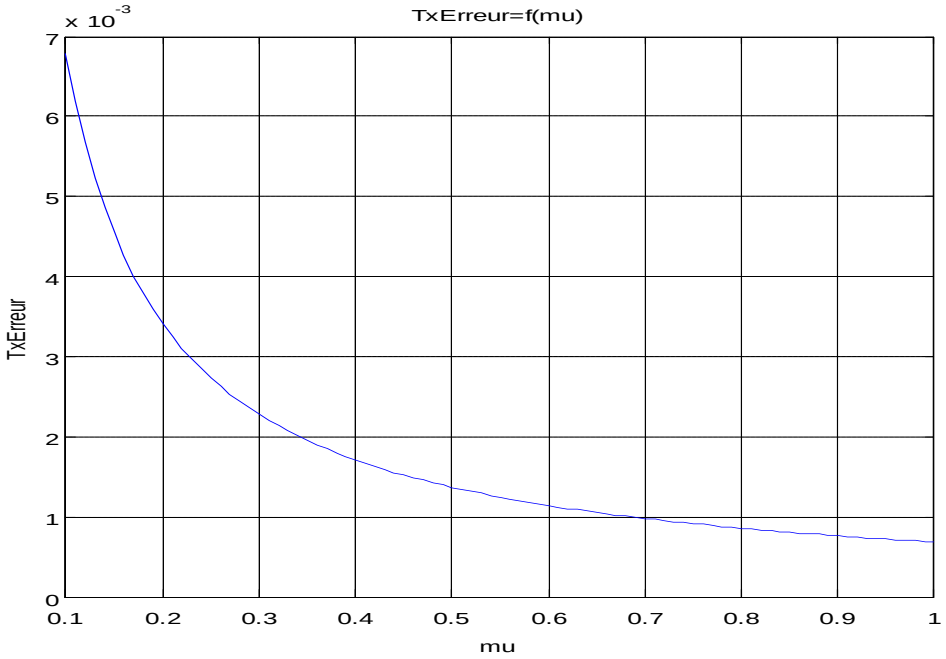

Figure 3.4. Influence du nombre moyen de photons par impulsion sur le taux d'erreur

Commentaire

La courbe a été obtenue pour une variation de μ de 0.1 à 1. Il est bien clair que le taux d'erreur diminue lorsque μ augmente puisque le QBER est décroissant avec la croissance de μ. Les valeurs élevées de μ permettent d'augmenter le débit de la transmission quantique et de diminuer le taux d'erreur. A l'inverse, ils vont permettre à l'espion d'acquérir une grande quantité d'information durant la phase de communication quantique.

5.4. L'information d'Eve et Bob en fonction de QBER

Comme l'information mutuelle entre Alice et Bob est donnée par l'équation 3.15 et celle d'Eve par l'équation 3.16, on peut trouver le taux d'erreur maximalement tolérable en posant

l'égalité des deux expressions. En particulier, on peut trouver une borne maximale en posant $f = 1$, signifiant qu'Eve renvoie toutes les impulsions à 1 photon qu'elle intercepte.

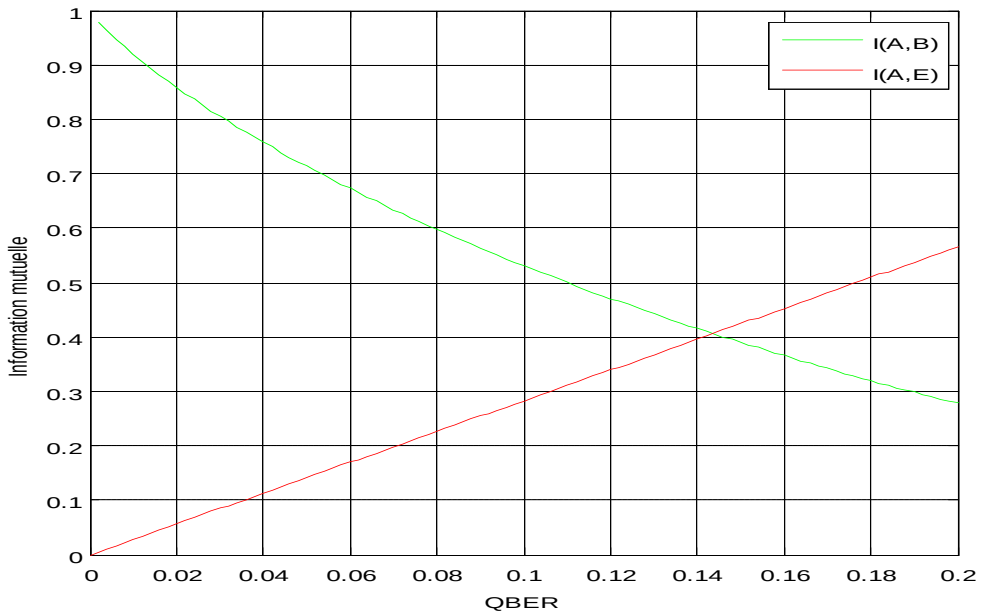

Figure 3.5. L'information d'Eve et Bob en fonction de QBER

Commentaire

Cette figure nous montre que si Eve n'intercepte pas tous les photons, alors l'information mutuelle entre Alice et Bob est supérieur à celle entre Alice et Eve $I(A,B) > I(A,E)$. Par conséquent, Alice et bob sont en mesure d'élaborer une clé. Si Eve intercepte tous les photons, Eve a autant de connaissance que Bob sur la clé brute $I(A,E) > I(A,B)$. Alice et bob sont obligés d'abandonner leur clé. Le taux d'erreur représente la perturbation due à l'intervention d'Eve.

6. Conclusion

Dans ce chapitre nous avons présenté les différentes phases nécessaires pour distiller une clé secrète en utilisant le protocole BB84. Le protocole BB84 utilise la mécanique quantique ainsi que la théorie de l'information pour vérifier la présence d'un espion. On a vu qu'il existe diverses techniques d'espionnage. Néanmoins, ces techniques ne permettant pas à un espion de rester indétectable. De plus, et contrairement à la cryptographie classique, la probabilité de déchiffrer un message ne varie pas dans le temps.

Tenant compte des résultats obtenus, dés que le QBER du canal quantique est inférieur à 15 %, Eve n'a aucun moyen d'intercepter la clé sans que son intervention soit détectable. Si ce bruit dépasse 15 %, elle pourra prendre de l'information en simulant le bruit du canal et passer inaperçue. Donc QBER < 15 % assure la sécurisation totale de la communication.

Conclusion générale

Conclusion générale

La cryptographie quantique est un sujet d'actualité qui recouvre un très large choix de compétences, allant de la physique fondamentale jusqu'aux applications industrielles. Le résultat de ces recherches devrait aboutir à augmenter la sécurité de nos transmissions confidentielles, toujours plus nombreuses pour ce qui concerne le commerce en ligne et les transactions financières.

L'objet de ce travail était de trouver une solution permettant de construire des protocoles de communication sans aucune faille pour la sécurité. Pour cela, nous avons commencé avec une étude d'état d'art de la cryptographie classique et quantique. Nous avons ensuite passé en revue le protocole BB84 en donnant son principe, aussi l'étude de l'influence des paramètres physiques sur la sécurité de ce protocole.

La simulation du protocole BB84 consiste à déterminer le comportement du protocole quand un paramètre est varie. Des courbes sont alors générées et analysées. Par conséquent, nous avons déduit l'intérêt d'optimiser les paramètres physiques constituant le canal quantique pour minimiser le taux d'erreur sans avoir recours à l'annuler.

La confidentialité ne se base plus sur les complexités computationnelles mais sur des impossibilités imposées par la physique quantique.

Annexes

Annexe A:

Le modèle du chiffre de Vernam (à clé jetable)

Le chiffrement par la méthode à clé jetable consiste à combiner le message en clair avec une clé présentant les caractéristiques très particulières suivantes :

- La clé doit être une suite de caractères au moins aussi longue que le message à chiffrer.
- Les caractères composant doivent être choisis de façon totalement aléatoire.
- Chaque clé, ou « masque », ne doit être utilisée qu'une seule foi.

La méthode est simple :

On pose :

M : le message chiffré.

K : la clé (qui doit être de la même longueur que M

C : le message clair.

Et pour obtenir le message codé C on applique simplement la fonction **XOR** et on a :

$$C=M \text{ XOR } K$$

Etant donné les propriétés de XOR, le message initial s'obtient facilement :

$$M=C \text{ XOR } K$$

Le gros défaut de cette méthode est que la clé s'obtient également facilement par :

$$K=M \text{ XOR } C$$

Le risque de réutilisation d'une clé :

Soit un message $\mathbf{M_1}$ masqué grâce à la clé K, nous obtenons le message chiffré $\mathbf{C_1}$. Supposons qu'un autre message $\mathbf{M_2}$ soit chiffré avec le même masque **K**, fournissant le chiffré $\mathbf{C_2}$

$$C_1=M_1 \text{ XOR } K$$

$$C_2=M_2 \text{ XOR } K$$

Supposons qu'un adversaire appliqué l'opération **XOR** aux deux chiffrés $\mathbf{C_1}$ et $\mathbf{C_2}$

$$\mathbf{C_1 \text{ XOR } C_2 = (M_1 \text{ XOR } K) \text{ XOR } (M_2 \text{ XOR } K)}$$

$$\mathbf{= (M_1 \text{ XOR } M_2) \text{ XOR } (K \text{ XOR } K) = M_1 \text{ XOR } M_2}$$

La clé a disparu.

Si par exemple un adversaire connait les deux messages chiffrés et l'un des messages en clair, il peut trouver instantanément le deuxième message en clair par le calcule suivant :

$$\mathbf{C_1 \text{ XOR } C_2 \text{ XOR } M_1 = M_2}$$

Références bibliographiques

Bibliographie

[1] : Bruce Schneier. (2001). « Cryptographie appliqué, algorithmes, protocoles et codes sources en c », 2eme édition. Vuibert, Paris.

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

[3] : Laurent Bloch, Christophe Wolfhugel. (2006). « Sécurité informatique, principe et méthode ». Editions Eyrolles. Paris

[4]: Gilles Van Assche. (2006). « Quantum cryptography and secret key distillation ». Cambridge University Press.

[5]: Shannon C.E. (1948). « A Mathematical Theory of Communication. Bell System Technical Journal », Vol. 27, pp. 379–423, 623–656.

[6]: Hwei Hsu, Francis Gottet. (2004). « Signaux et communication », 2eme édition. Dunod, Paris.

[7]: Bruno Martin. (1990). « codage, cryptologie et applications ». 1ere édition, Presses polytechniques et universitaires romandes.

[8]: Michel Le Bellac. (Octobre 2003). « Introduction a l'information quantique », Cours donnée a l'Ecole Supérieure de Sciences Informatiques (ESSI). Valbonne.

[9]: Patrick Bellot, DANG Minh Dung. (2005). «Description du protocole BB84 en trios démentions ». Rapport de stage. Ecole national supérieure de télécommunication. Paris.

[10]: BUI Tuan Nghia. (2005). « cryptographie quantique ». Rapport de stage. Institut de la francophonie pour l'informatique. Paris.

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

[12]: Abderrahim EL ALLATI. (Janvier 2012). « Etude de cryptographie et de téléportation quantique et proposition de quelques protocoles quantiques ». Thèses de doctorat. Université Mohammed V-AGDAL. Rabat.

[13]: Mélanie Langlois. (Décembre 1999). « Cryptographie quantique solution au problème de distribution de clefs secrètes ». Thèses de doctorat. Université d'Ottawa.

[14]: Jérôme Lodewyck. (décembre 2006). « Dispositif de distribution quantique de clé avec des états cohérents à longueur d'onde télécom ». Thèses de doctorat. Université Paris XI, UFR Scientifique D'Orsay.

[15]: Jean Hladik, Michel Chrysos. (2000). «Introduction à la mécanique quantique, cours et exercices corrigés». Dunod, Paris.

[16]: David J.Griffiths. (1995). « Introduction to quantum Mechanics». Prentice Hall. Inc. Upper Saddle River, NJ 07458. USA.

[17]: Dramix Florence, van den Broek Didier, Wens Vincent. (2003). « La cryptographie quantique », Printemps des sciences.

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

[19]: Manuel Sabban. (Avril 2009). « Sécurité en cryptographie quantique utilisant la détection homodyne d'états cohérents à faible énergie ». Thèses de doctorat. Ecole dctorale d'informatique télécommunication et électronique de Paris. Paris.

[20]: Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel et Hugo Zbinden. (2001). « Quantum cryptography ». Rapport technique. Groupe de physique appliquée. Université de Geneva.

[21]: Samuel J. Lomonaco. (November 1998). « A quick glance at quantum cryptography ». Thèses de doctorat. Université de Maryland, Baltimore.

[22]: Ho Thi Phuong. (Juillet 2008). « Amélioration d'une implémentation du protocole de cryptographie quantique BB84 ». Rapport de stage. Institut de la francophonie pour l'informatique. Hanoi.

[23]: Gisin N. & Wolf S. (1999). « Quantum cryptography on noisy channels: quantum versus classical key-agreement protocols ». Thèses de doctorat. Department de Physique. Universities de Geneva. Switzerland.

[24]: Olivier L. & Guerreau Lambert. (December 2005). « Multidimentional quantum key distrubution with single side pulse and single side band modulation multiplexing ». Thèses de doctorat. Institut de Géorgie de l'ingénieur de Technologie.

[25]: Norbert Lütkenhaus. (Jul 1996). « Security against eavesdropping in quantum cryptography ». New journal of Physics.

[26]: Félix Bussiére. (Octobre 2003). « Cryptographie quantique à plusieurs participants par multiplexage en longueur d'onde». Thèses de doctorat. Université de Montréal.

[W1] Un point sur la cryptologie: http://www.xmco.fr/article-crypto.html.

.

Résumé

La gestion des clés, est une tache qui doit être réalisé par tous systèmes cryptographiques, selon les différences types de ces clés. La cryptographie à clé secrète, exige le partage d'une même clé entre tous les interlocuteurs. Mais on a le problème de distribution des clés. En contrepartie, les systèmes à clé publique, assurant une clé publique et une clé privée pour chaque utilisateur, une clé publique pour chiffrer, et une clé privée pour déchiffrer. Mais la sécurité de cette méthode repose sur le postulat que les ordinateurs actuels ne proposent pas la puissance de calcul nécessaire pour casser cette protection.

Alors, La cryptographie quantique intervient à ce niveau comme solution permettant d'assurer un transfert sécurisé des clés et par la suite garantir la confidentialité et l'intégrité des messages échanges.

Dans ce travail, nous avons présenté la cryptographie quantique, explicité ses concepts de base pour arriver à prouvée son efficacité dans le monde des transmissions sécurisées. Nous avons également étudié le premier protocole de cryptographie quantique à savoir le BB84. Enfin nous avons simulée le protocole BB84 afin de dégager l'influence des différents paramètres physiques sur l'efficacité et la fiabilité du protocole.

Mot clés

Cryptographie, protocole, intrus, quantique, qubit, paramètre physiques, canal quantique.