République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A.MIRA-BEJAIA

Faculté de Technologie

Département de Génie Électrique

Projet de Fin d'étude

Pour l'obtention du diplôme de Master en Télécommunications

Spécialité : Réseaux et Télécommunication

Thème

La distribution quantique de clés à variables continues

Préparé par :

AZZAR Kenza

BELHADDAD Menoune

Encadré par :

M. BERRAH Smail

Mme. BOUCHOUCHA Lydia

Membres du jury :

M. BENAMIROUCHE

Mme. ACHOUR

Année Universitaire : 2017/2018

Remerciements

Avant tout, remercions dieu tout puissant de nous avoir donné le courage et la patience de mener ce travail à fond.

Nous exprimons nos remerciements à nos parents pour leur soutien moral, leurs encouragements et leurs aisés financiers.

Nos remerciements les plus distingués sont à l'égard de notre promoteur Mr BERRAH.

Nous tenons à remercier et exprimer notre profonde gratitude et vif remerciements à notre co-promotrice Melle Bouchoucha pour ses encouragements, ses conseils et ses efforts afin de terminer ce travail.

Nous remercions aussi les membres de jury qui ont bien voulu nous faire l'honneur d'évaluer et d'examiner notre travail.

Tous les mots restent faibles pour exprimer notre profonde reconnaissance à tous ceux qui nous ont aidés de près ou de loin à réaliser ce travail.

Dédicaces

Je dédie ce travail :

A mes très chers parents, pour tous leurs sacrifices,

leur amour, leur tendresse, leur soutien et leurs prières

tout au long de mes études ;

A mes chers frères (Karim et Fares), pour leurs encouragements

permanents, et leur soutien moral ;

A ma chère belle-sœur (Sabrina);

A mes chères nièces (Leyna et Nelya) que j'aime beaucoup ;

A mon binôme Menoune pour sa patience ;

A tous mes camarades de la promo ;

A mes très chères amies ;

A toutes ma famille

Merci d'être toujours là pour moi.

A. Kenza

Dédicaces

Je dédie ce travail:

A mes chers parents ;

Et mon cher mari ;

A mes frères ;

Et mes sœurs ainsi que leurs

Maris et leurs enfants ;

A ma belle-famille ;

Et toutes mes amies.

B. Menoune

Table des matières

Chapitre II : Protocoles de distribution quantique de clé.

Liste des abréviations

BB84	**B**rassard, **B**ennett 19**84**.
B92	**B**ennett 19**92.**
CV-QKD	**C**ontinuous **V**ariable-**Q**uantum **K**ey **D**istribution.
DES	**D**ata **E**ncryption **S**tandard.
EPR	**E**instein, **P**odolsk and **R**osen.
E91	**E**kert 19**91**.
QBER	**Q**uantum **B**it **E**rror **R**ate.
QKD	**Q**uantum **K**ey **D**istribution.
RSA	**R**ivest, **S**hamir and **A**delman.

Liste des figures

Liste des tableaux

Introduction générale

Introduction générale

La communication a toujours été indispensable pour les individus ; qui échangent des informations qui doivent rester secrètes et confidentielles.

En effet, avec le développement technologique et l'ouverture des réseaux de communication, la sécurité d'information est devenue un besoin primordial dans tous les domaines vu que l'espionnage touche une très grande gamme d'informations telles que les mots de passe, les codes de cartes bancaires, les messages électroniques… etc. Cependant, le seul moyen pour assurer la sécurité est la cryptographie.

La cryptographie est l'une des disciplines de la cryptologie qui a pour but d'assurer la sécurité des communications et des données stockées en présence d'une tiers personne. Elle offre un ensemble de techniques et des méthodes assurant la confidentialité, l'authentification et l'intégrité, en développant souvent des clés secrètes qui sont basées sur des codes et des algorithmes.

Au début, les militaires grecs codaient leurs messages sur des bâtons de bois (scytales), puis ils sont passés au téléphone rouge entre le Kremlin et la Maison Blanche, la cryptographie a été un outil très puissant autant en temps de guerre qu'en temps de paix.

D'une manière générale, la sécurité des données tend à s'améliorer vers des techniques dite à clé symétrique et asymétrique qui posent encore des problèmes et des exigences de sécurité. On se tourne alors vers un nouveau domaine de cryptographie ; c'est la cryptographie quantique.

Au début des années 80 la cryptographie quantique appelée aussi distribution quantique de clés, a été émergée comme une technique qui est fondée sur une combinaison des concepts de la mécanique quantique et de la théorie de l'information.

L'encodage de l'information se fait soit en utilisant les photons uniques, dans ce cas on parle des variables discrètes. Ou bien via les états cohérents qui sont définit par des variables continues.

Notre étude est portée sur les protocoles de distribution quantique de clés à variables continues, où nous simulerons ces protocoles en utilisant la détection homodyne puis la détection hétérodyne afin de savoir quelle est la meilleur détection qui assure plus de sécurité.

Pour cela, nous avons subdivisé notre travail en trois chapitres suivants :

Premier chapitre, présente un aperçu général sur les notions de la cryptographie classique et les problèmes liés à la distribution de clés. Puis nous introduirons les principes fondamentaux sur lesquels se base la cryptographie quantique.

Le deuxième chapitre porte en premier lieu, quelques protocoles de distribution quantique de clé à variables discrètes, et en second lieu, nous donnerons une description détaillée sur les protocoles à variables continues.

Le dernier chapitre est consacré à la simulation des protocoles à variable continues en utilisant la réconciliation directe et inverse pour les deux détections homodyne et hétérodyne dans le cas générale. Puis, nous discuterons l'influence des attaques individuelles et collectives sur ces protocoles.

Enfin, nous terminerons notre travail par une conclusion et perspectives.

Chapitre I :
Convergence de la cryptographie classique vers la cryptographie quantique

I.1. Introduction

Depuis l'antiquité, l'homme n'a cessé de développer des techniques et des méthodes qui lui permettent de cacher ses messages qu'il ne souhaitait pas voir interceptés par autrui. C'est l'objectif de la cryptographie.

Dans ce chapitre, nous définirons la cryptographie classique avec ses deux types, et ses limites. Ensuite, nous décrirons les notions de la mécanique quantique et de la théorie d'information qui constituent la base de la cryptographie quantique.

I.2. La cryptographie classique

La cryptographie est l'étude des techniques permettant la transmission confidentielle d'informations entre deux participants légitimes, par convention on utilise les noms Alice et Bob pour designer respectivement l'émetteur et le récepteur. Pour protéger un message, on lui applique une transformation dépendante d'un paramètre, appelé clé, afin de le rendre incompréhensible par un intrus appelé Eve « chiffrement ». Le déchiffrement est l'action inverse qui permet de reconstruire le texte en clair à partir du texte chiffré.

La cryptographie est donc l'art de la science de garder le secret message. Elle se réparti en deux grandes catégories.

I.2.1. Cryptographie à clé privée (symétrique)

La cryptographie est dite à clé privée, quand la clé de chiffrement *e* est égale à la clé de déchiffrement *d* comme le montre la figure I.1, ou quand *d* peut être calculée facilement à partir de *e*.

Pour envoyer un message chiffré à Bob, Alice utilise la clé de chiffrement *e*. Pour retrouver le message, Bob utilise la clé de déchiffrement *d* qui correspond à *e* [1].

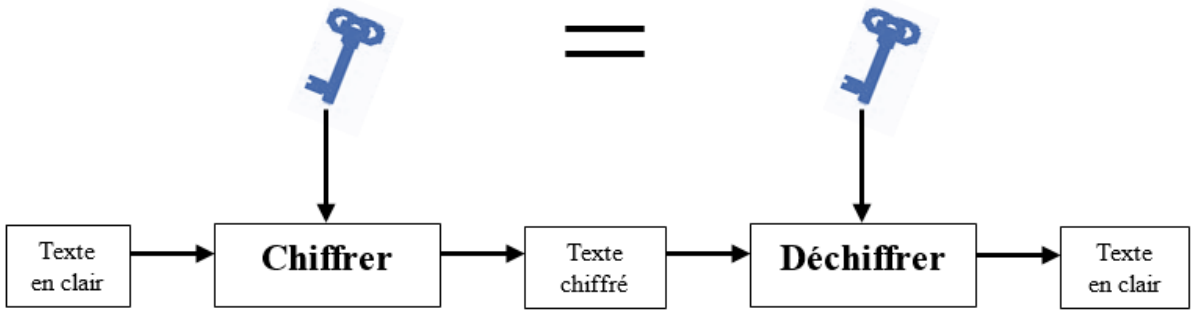

Figure I.1 : Principe de la cryptographie symétrique.

De nombreux algorithmes de chiffrement symétrique sont apparus, comme l'algorithme DES.

L'algorithme DES

Le DES (*Data Encryption Standard*) est un standard mondial depuis la fin des années 1970. C'est un cryptosystème agissant par blocs ; cela signifie qu'il ne chiffre pas les données à la fois quand les caractères arrivent, mais il découpe virtuellement le texte clair en blocs de 64 bits qu'il les code séparément, puis il les concatène. Un bloc de 64 bits du texte clair entre par un côté de l'algorithme et un bloc de 64 bits du texte chiffré sort de l'autre côté. Cet algorithme est assez simple puisqu'il ne combine en fait que des permutations et des substitutions [2].

I.2.2. Cryptographie à clé publique (asymétrique)

Avec un cryptosystème à clé publique, les clés *d* et *e* sont distinctes, comme le montre la figure I.2 et le calcul de *d* à partir de *e* est infaisable. Dans un tel système, la clé de chiffrement peut être rendue publique.

Si Bob veut recevoir un message chiffré, il publie une clé de chiffrement *e* et il garde la clé de déchiffrement *d* secrète. N'importe qui peut utiliser *e* pour chiffré des messages destinés à Bob, c'est pourquoi on dit que *e* est une clé publique. On dit que *d* est une clé privée parce que Bob est le seul à pouvoir déchiffrer ces messages [1].

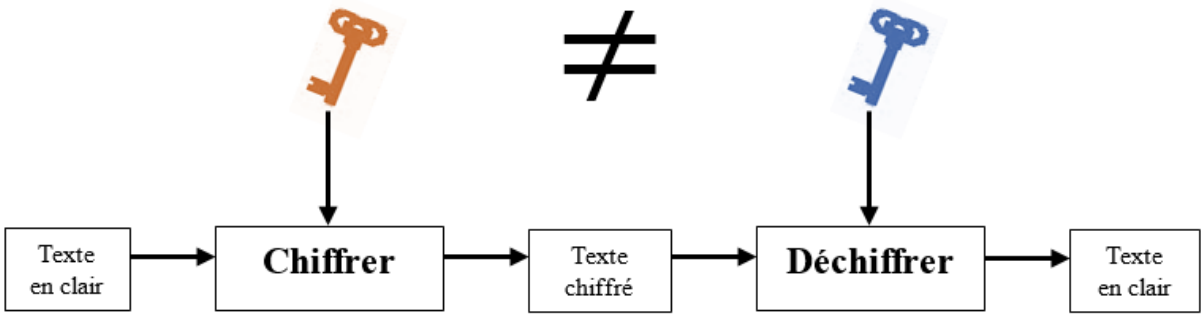

Figure I.2 : Principe de la cryptographie asymétrique.

Le cryptage asymétrique nécessite des clés beaucoup plus longues que celles du cryptage symétrique. Parmi ses algorithmes, prenons l'exemple de l'algorithme RSA.

L'algorithme RSA

Cet algorithme a été mis au point en 1977 par Rivest, Shamir et Adleman. D'où vient sa nomination RSA. Le chiffrement RSA est basé sur la difficulté de la factorisation d'un entier en produit *n* de deux grand nombre premiers [3].

Ce cryptosystème utilise une clé publique *e* et une clé privée *d*. Le chiffrement d'un

message *M* se fait selon :

$$C = M^e mod\ n \qquad \text{(I. 1)}$$

Et pour récupérer le message *M* à partir du message chiffré *C* :

$$M = C^d mod\ n \qquad \text{(I. 2)}$$

I.3. Limites de la cryptographie classique et évolution vers la cryptographie quantique

En cryptographie classique, une clé secrète ne peut être utilisée qu'une seule fois, et ne peut pas être authentifiée si elle est connue par plusieurs personnes. De plus, l'utilisation d'une même clé pour le chiffrement et le déchiffrement limite la confidentialité.

Pour ce qui est de la cryptographie à clé publique, les algorithmes de chiffrement et de déchiffrement sont lents et nécessitent un nombre important de calculs.

Afin de remédier à ces limites et particulièrement le problème de distribution de clé secrète, qui doit être aussi longue que le message et changée à chaque nouvelle transmission, des nouvelles techniques sont apparus à savoir la cryptographie quantique.

La cryptographie quantique est l'ensemble des techniques de distribution de clé secrète à distance, qui est basé sur les lois de la mécanique quantique et de la théorie de l'information pour les démonstrations de sécurité. Elle est dénommé *quantum key distribution* QKD.

Ce type de cryptographie utilise les photons comme porteur d'information, pour leur facilité de production, leur simplicité de manipulation et enfin leur rapidité de propagation à travers les fibres optiques.

I.4. Notions de base de la Mécanique quantique

La mécanique quantique est née au début du XXème siècle, c'est une branche de la physique qui a pour but d'étudier et de décrire la manière dont se comportent les particules.

L'état quantique de ces dernières est caractérisé par un vecteur d'état appartenant à un espace des états appelé espace de Hilbert complexe noté $\mathcal{H}$. Cette description se fait au moyen de la notation de Dirac, où un état est décrit par le Ket $|\psi\rangle$, dont la transposée est le Bra $\langle\psi|$. Le produit scalaire entre vecteurs d'état $|\psi\rangle$ et $|\phi\rangle$ est noté $\langle\psi|\phi\rangle$.

I.4.1. Mesure d'un état quantique

Soit un observable $\mathcal{A}$ auquel est associé l'opérateur *A* de valeurs propres $\{a_n\}$ et d'états propres $\{\phi_n\}$. Quand un système initialement dans un état $|\psi\rangle$ est soumis à la mesure de

l'observable $\mathcal{A}$; les seuls résultats possibles sont les $\{a_n\}$, et la probabilité d'obtenir la valeur a_n est donnée par l'équation (I.3) :

$$P(a_n) = |\langle \phi_n | \psi \rangle|^2 \qquad \text{(I. 3)}$$

Après la mesure si le résultat est a_n, le système se trouve projeté dans l'état $|\phi_n\rangle$. Mais si le système est déjà dans un état propre $|\phi_n\rangle$ tel qu'il est défini par l'équation (I.4), la mesure de $\mathcal{A}$ donnera a_n avec certitude. C'est donc le système de mesure qui fixera la base des états dans $\mathcal{H}$; où ces états sont les états propres de l'observable mesuré [4].

$$|\psi\rangle = |\phi_n\rangle \qquad \text{(I. 4)}$$

I.4.2. Equation de Schrödinger

En mécanique quantique, une particule est décrite par une fonction d'onde complexe $\psi(r,t)$, son évolution est donnée par l'équation de Schrödinger.

$$i\hbar \frac{d|\psi(r,t)\rangle}{dt} = \hat{H}|\psi(r,t)\rangle \qquad \text{(I. 5)}$$

- $\hbar$ est la constante réduite de Planck ; $\hbar = \frac{h}{2\pi}$
- $\hat{H}$ un opérateur hermitien du système isolé, appelé Hamiltonien du système [5].

I.4.3. Polarisation de la lumière

La lumière est un rayonnement électromagnétique (onde EM) constituée de deux champs ; un champ électrique $\vec{E}$ et un champ magnétique $\vec{B}$ qui sont perpendiculaires entre eux et sont contenus dans un plan perpendiculaire à la direction de propagation de l'onde EM comme illustré sur la figure I.3. Avec :

$$\vec{E} = \overrightarrow{E_0} \cos(\omega t - kz) \qquad \text{(I. 6)}$$

$$\vec{B} = \overrightarrow{B_0} \cos(\omega t - kz) \qquad \text{(I. 7)}$$

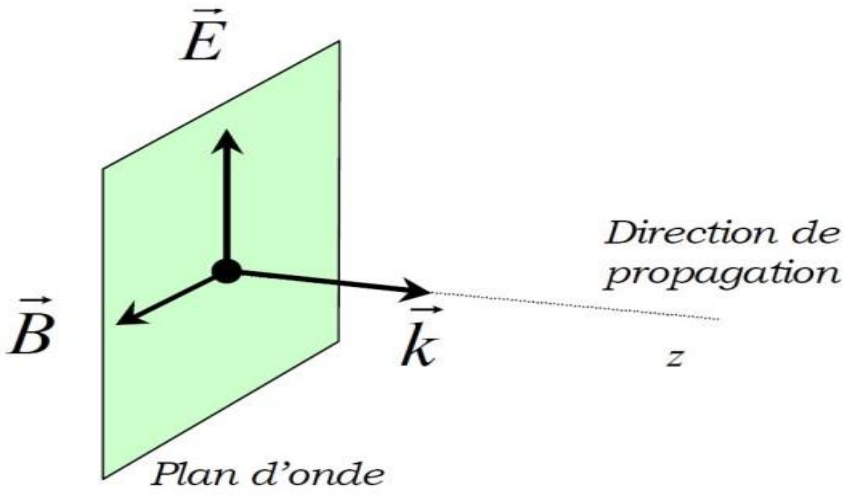

Figure I.3 : Direction de propagation d'une onde électromagnétique.

Pour une lumière non polarisée, ou naturelle, le champ $\vec{E}$ tourne autour de son axe de façon aléatoire et imprévisible au cours du temps. Tandis que, la polarisation de la lumière correspond à donner une trajectoire bien définie au champ électrique $\vec{E}$ [6].

Il existe des dispositifs qui polarisent la lumière ; dans ce cas, le vecteur lumineux n'a qu'une seule direction. Ces dispositifs sont appelés polariseurs ou polaroïds. Ces derniers sont constitués par une mince lame transparente de matière plastique, enrobant des petits cristaux tous orientés de la même façon. La lame est caractérisée par sa direction de polarisation.

Lorsqu'une lumière naturelle traverse un polariseur, elle se polarise selon une direction déterminée par le polariseur ; celle de son axe de polarisation [7].

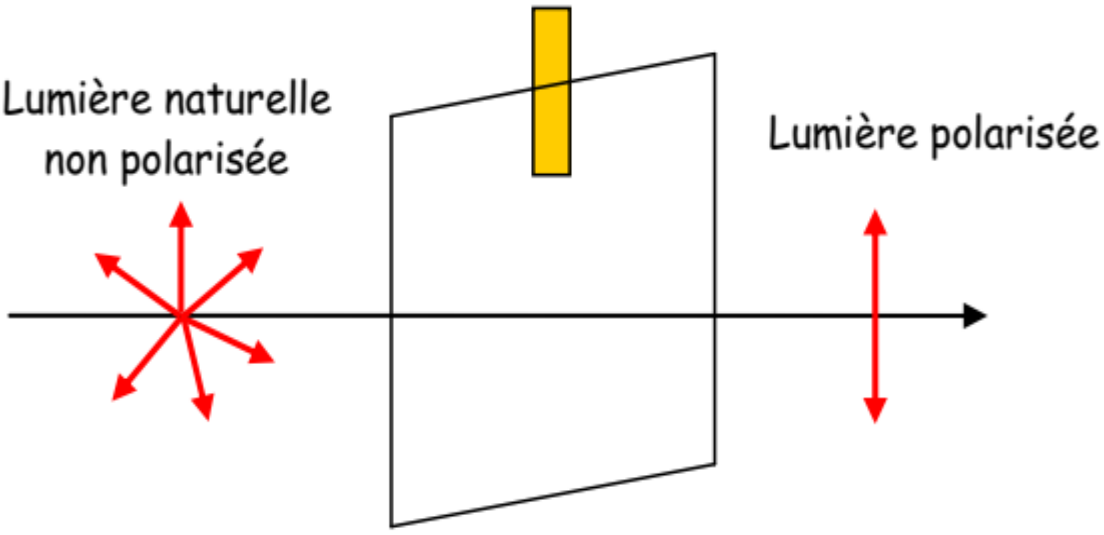

Figure I.4 : Principe de polarisation de la lumière par un polaroïd [7].

I.4.4. Polarisation des photons

Les photons sont des particules élémentaires (quanta) de la lumière, portant une quantité d'énergie invariante donnée par l'expression suivante :

$$E = hv \qquad (I.8)$$

- h est la constante de Planck ($h = 6.63 \times 10^{-34}$) J.s ;
- v est la vitesse de la lumière.

Un photon a des propriétés qui permettent de le décrire telle que la polarisation. La polarisation d'un photon, se fait de la même manière que la polarisation de la lumière. Il existe plusieurs polarisations représentées dans le tableau (I.1).

Base linéaire ⊕	$\|H\rangle = \|\rightarrow\rangle$	$\|V\rangle = \|\uparrow\rangle$
Base diagonale ⊗	$\|D\rangle = \|\nearrow\rangle$	$\|AD\rangle = \|\nwarrow\rangle$
Base circulaire ↻	$\|C\rangle = \|\circlearrowright\rangle$	$\|AC\rangle = \|\circlearrowleft\rangle$

Tableau I.1 : Les états de polarisation d'un photon.

Pour détecter la polarisation des photons, on utilise un filtre polarisant suivi d'un détecteur de photons. Si un photon polarisé par $|\rightarrow\rangle$ rencontre un filtre polarisant orienté $|\rightarrow\rangle$, il traverse ce filtre polarisant et il est enregistré par le détecteur. Par contre, si un photon polarisé $|\uparrow\rangle$ rencontre le même filtre, il est immédiatement arrêté, et le détecteur n'enregistre rien. D'autre part, si le photon est polarisé diagonalement ($|\nearrow\rangle, |\nwarrow\rangle$), une fois sur deux, il traverse le filtre, et une fois sur deux, il est arrêté. Si on peut distinguer entre une polarisation horizontale et verticale, il est impossible de distinguer en même temps entre une polarisation diagonale et anti-diagonale.

De la même façon, on peut utiliser un filtre polarisant $|\nearrow\rangle$; il laisse passer les photons polarisés dans la même direction, et arrête ceux polarisés $|\nwarrow\rangle$ et se comporte aléatoirement avec ceux polarisés $|\rightarrow\rangle$ et $|\uparrow\rangle$.

I.4.5. Principe d'incertitude de Heisenberg

En mécanique classique, la position *r* d'une particule ainsi que son impulsion *p* sont connues à tout instant. Par contre, en mécanique quantique, le principe d'incertitude de Heisenberg stipule qu'il est impossible de donner simultanément et avec une précision absolue la position et l'impulsion d'une particule.

L'incertitude de Heisenberg est donnée par la relation (I.9).

$$\Delta x \, \Delta px \geq \frac{\hbar}{2} \qquad (I.9)$$

On désigne par Δx et Δpx les fluctuations statistiques de la mesure sur la position et l'impulsion respectivement [8].

I.4.6. Théorème de non-clonage

L'information classique, peut être copiée librement d'un système à un autre. Tandis qu'en monde quantique, ce n'est plus le cas. Le théorème de non-clonage, énoncé en 1982 par Wootters, Zurek et Dieks, montre qu'il est impossible de cloner un état quantique arbitraire et inconnu ; C'est-à-dire qu'il n'existe pas de transformation unitaire *U* qui permette de cloner parfaitement l'état $|\psi\rangle$ tel que [9] :

$$U(|\psi\rangle|\mu\rangle) = |\psi\rangle|\psi\rangle \qquad (I.10)$$

Dans le cas d'un photon, il est impossible de le copier lorsqu'il se trouve dans un état non orthogonal. Un Qubit peut être dans un état de superposition quantique de $|0\rangle$ et de $|1\rangle$. C'est à cause de cette superposition qu'il n'existe pas de méthode de duplication de Qubits, puisqu'une particule en état de superposition donne une valeur connue seulement lors de sa mesure [10].

I.4.7. Intrication quantique

L'intrication est l'un des aspects les plus utilisé dans la sécurité de l'information par cryptographie quantique, mis en évidence par Einstein et Schrödinger dans les années 30.

Il s'agit d'un phénomène dans lequel deux particules (photons) ou groupe de particules se propagent dans deux directions opposées, et pour lesquelles la mesure des propriétés de l'une permet de prédire les propriétés de l'autre, quelle que soit la distance qui les sépare.
Ils forment ainsi un seul système.

En fait, tout état qui ne peut être écrit sous forme de produit tensoriel est dit état intriqué. Considérons deux états à deux Qubits :

$$|\Psi_1\rangle = \frac{1}{\sqrt{2}}|11\rangle + \frac{1}{\sqrt{2}}|10\rangle \qquad (I.11)$$

Et

$$|\Psi_2\rangle = \frac{1}{\sqrt{2}}|11\rangle + \frac{1}{\sqrt{2}}|00\rangle \qquad (I.12)$$

On voit que $|\Psi_1\rangle$ peut etre écrit sous forme de produit tensoriel :

$$|\Psi_1\rangle = |1\rangle\left(\frac{1}{\sqrt{2}}|1\rangle + \frac{1}{\sqrt{2}}|0\rangle\right) \qquad (I.13)$$

Par contre, $|\Psi_2\rangle$ n'étant pas un produit tensoriel, c'est un état intriqué.

Les états intriqués les plus célèbres sont les états de Bell, qui sont des états intriqués maximalement. Soient $|\phi\rangle$ et $|\psi\rangle$ des états définis dans les espaces de Hilbert $\mathcal{H}_A$ et $\mathcal{H}_B$ respectivement, tels que :

$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \qquad (I.14)$$

$$|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |01\rangle) \qquad (I.15)$$

Ces états sont appelés aussi les paires EPR qui forment une base orthonormée de l'espace d'état. L'unité de l'intrication est le « Ebit » (*entanglement bit*), définie comme étant la quantité d'intrication contenue dans un état de Bell [3].

I.5. La théorie d'information

La théorie d'information est une modélisation mathématique, essentiellement probabiliste qui est initiée par Claude Shannon en 1948. Elle a été utilisée pour les preuves de sécurité de la cryptographie quantique. Dans ce qui suit, nous donnerons les notions de bases de la théorie d'information.

I.5.1. La théorie d'information classique

I.5.1.1. Entropie de Shannon

Dans les systèmes de communications réels, nous transmettons en général de longues séquences de symboles à partir d'une source d'information. Ainsi, nous somme plus intéressé par l'entropie qu'une source produit plutôt que par le contenu de l'information de chaque symbole [11]. L'entropie de Shannon est donnée par l'équation (I.16).

$$H(X) = \sum_{i=1}^{m} p(x_i) \log_2 \left[\frac{1}{p(x_i)}\right] \qquad (I.16)$$

Où $p(x_i)$ désigne la probabilité que la variable X soit égale à x_i.

I.5.1.2. Entropie conjointe et conditionnelle

L'information émise par la source est représentée par X et l'information reçue par le destinataire est représentée par Y. Plus généralement, lorsque X et Y sont deux séquences aléatoires, l'entropie conjointe H s'écrit [12]:

$$H(X,Y) = \sum_{i,j} p(x_i, y_j) \log_2 \left[\frac{1}{p(x_i, y_j)}\right] \qquad (I.17)$$

Si la variable *X* est connue, alors l'entropie conditionnelle de *Y* est défini par l'équation (I.18) [12]:

$$H(Y|X) = H(X,Y) - H(X) \qquad (\text{I.}18)$$

I.5.1.3. Information mutuelle

L'information mutuelle contenue dans *X* et *Y* reflète les informations communes de *X* et *Y*.

$$I(X,Y) = H(X) + H(Y) - H(X,Y) \qquad (\text{I.}19)$$

D'après les équations (I.18) et (I.19), l'information mutuelle contenue dans *X* et *Y* s'écrit également

$$I(X,Y) = H(X) - H(X|Y) \qquad (\text{I.}20)$$

De la définition de l'entropie exprimée par les équations (I.16) et (I.17), $I(X,Y)$ s'écrit :

$$I(X,Y) = \sum_{i,j} p(x_i, y_j) \log_2 \left[\frac{p(x_i, y_j)}{p(x_i)p(y_j)}\right] \qquad (\text{I.}21)$$

La probabilité $p(x_i, y_j)$ s'écrit [12] :

$$p(x_i, y_j) = p(x_i)p(y_j|x_i) \qquad (\text{I.}22)$$

I.5.2. Théorie de l'information avec des variables continues

Notre étude est basée sur les protocoles de distribution quantique de clé à variables continues. Nous allons donc définir les notions d'entropies et d'informations mutuelles pour ce type de variables.

I.5.2.1. Entropie de Von Neumann

L'entropie de Von Neumann d'un état quantique ρ est une généralisation de l'entropie classique *H*, définie par analogie avec l'information classique. En effet, on peut toujours décomposer ρ dans sa base d'états propres $\{|i\rangle\langle i|\}$ [13]:

$$\rho = \sum_i \lambda_i |i\rangle\langle i| \qquad (\text{I.}23)$$

Nous pouvons interpréter ρ comme une source qui produit l'état $|i\rangle\langle i|$ avec des probabilité λ_i.

L'entropie classique $H(\lambda)$ s'écrit alors :

$$H(\lambda) = -\sum_i \lambda_i \, log_2 \, \lambda_i = -Tr(\rho \, log_2 \, \rho) \qquad (I.24)$$

L'entropie de Von Neumann est définie par (I.25):

$$S(\rho) = -Tr(\rho \, log_2 \, \rho) \qquad (I.25)$$

L'entropie d'un état gaussien s'écrit :

$$S(\rho) = \sum_i G\left(\frac{\lambda_i - 1}{2}\right) \qquad (I.26)$$

Où les λ_i sont les *n* valeurs propres symplectiques de γ, et la transmission G s'écrit :

$$G(x) = (x+1)\log_2(x+1) - x\log_2 x \qquad (I.27)$$

I.5.2.2.Entropie d'une variable continue

La distribution de probabilité des variables continues suit la loi (I.28):

$$p(X = x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-x_0)^2}{2\sigma^2}} \qquad (I.28)$$

Où x_0 est la valeur moyenne ; considérée nulle ($x_0=0$) dans tous ce qui suit. σ l'écart type et $V_X = \sigma^2$ la variance de la distribution.

On définit l'entropie *S* d'une variable aléatoire continue *X* :

$$S(X) = -\int p(X = x_i)\log_2 p(X = x_i)dx \qquad (I.29)$$

La distribution gaussienne maximise $S(X)$, donc pour une variable aléatoire gaussienne, on calcule analytiquement l'entropie différentielle [13] :

$$S(X) = -\int p(x)\log_2\left(\frac{1}{\sqrt{2\pi\sigma^2}}\right)dx + \int \log_2(e)\frac{x^2}{2\sigma^2}p(x)dx \qquad (I.30)$$

$$= \frac{1}{2}\log_2(2\pi\sigma^2) + \frac{1}{2}\log_2(e) \qquad (I.31)$$

$$= \frac{1}{2}\log_2(2\pi e\sigma^2) \qquad (I.32)$$

I.5.2.3.Entropie conjointe et conditionnelle

La matrice de covariance *K*, pour deux variables aléatoires *A* et *B*, s'écrit :

$$K = \begin{bmatrix} V_A & \langle AB \rangle \\ \langle AB \rangle & V_B \end{bmatrix}$$

Où $\langle AB \rangle$ est la corrélation entre les variables A et B.

On définit l'entropie conjointe pour deux variables aléatoires gaussiennes corrélées, par l'expression (I.33) [14] :

$$S(A,B) = \frac{1}{2}\log_2\big(det(K)\big) \qquad (\text{I.33})$$

L'entropie conditionnelle s'écrit :

$$S(B|A) = S(A,B) - S(A) = \frac{1}{2}\log_2\left(2\pi e \frac{det(K)}{V_A}\right) \qquad (\text{I.34})$$

Dans cette expression, on définit la variance conditionnelle $V_{B|A}$ par [11] :

$$V_{B|A} = \frac{det(K)}{V_A} = V_B - \frac{\langle AB \rangle^2}{V_A} \qquad (\text{I.35})$$

I.5.2.4. Information mutuelle

L'information mutuelle d'une distribution bipartite, a trois définitions équivalentes :

$$I_{AB} = S(B) - S(B|A) = \frac{1}{2}\log_2\left(\frac{V_B}{V_{B|A}}\right) \qquad (\text{I.36})$$

$$= S(A) - S(A|B) = \frac{1}{2}\log_2\left(\frac{V_A}{V_{A|B}}\right) \qquad (\text{I.37})$$

$$= S(A) + S(B) - S(A,B) = \frac{1}{2}\log_2\left(\frac{V_A V_B}{det(K)}\right) \qquad (\text{I.38})$$

Les concepts d'information mutuelle et de variance conditionnelle sont à la base des résultats théoriques prouvant la sécurité des protocoles de distribution quantique de clé utilisant des variables continues. Une partie du chapitre suivant sera consacré à l'étude de ces protocoles [13].

I.5.2.5. Théorème de Holevo

La formule (ou borne) de Holevo permet de déterminer une borne supérieure à l'entropie mutuelle quantique d'un état bipartite p_{AB}. Si l'on considère une mesure de Bob, pouvant

donner un ensemble de résultats $\{x_i\}$ avec des probabilités p_i, l'information mutuelle est bornée par l'équation (I.39)

$$S(A{:}B) \leq S(p_A) - \sum_i p_i S\left(p_A^{x_i}\right) \qquad (\text{I.39})$$

Où $p_A^{x_i}$ correspond à l'état d'Alice conditionné au résultat x_i sur la mesure de Bob. Il a été démontré que cette borne de Holevo peut être utilisée pour borner l'information acquise par l'espion dans un protocole de cryptographie quantique [15].

I.5.3. Le Quantum bit (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. L'expression du Qubit est donnée par [16] :

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad (\text{I.40})$$

Où α et β sont des coefficients complexes, ils représentent les amplitudes de probabilité d'obtenir l'état $|0\rangle$ et l'état $|1\rangle$ respectivement lors d'une mesure de l'état$|\psi\rangle$.

En général, la représentation géométrique du Qubit est donnée par la sphère de Bloch illustré sur figure I.5. L'état $|\psi\rangle$ est un point de la surface de la sphère ; la superposition des états $|0\rangle$ et $|1\rangle$ permet de représenter une infinité de quantité d'information [12].

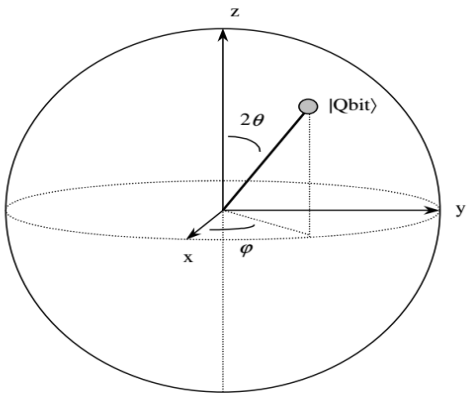

Figure I.5 : La sphère de Bloch [12].

I.6. Conclusion

Au cours de ce chapitre, nous avons définit la cryptographie classique puis, nous avons met l'accent sur ses limites et l'évolution vers la cryptographie quantique, qui est basée sur les principes de la mécanique quantique et de la théorie de l'information pour des preuves de

sécurité contre un espion. Ceci nous permettrons de mieux comprendre les protocoles de distribution quantique de clé qui est l'objet du chapitre suivant.

Chapitre II
Protocoles de distribution quantique de clé

II.1. Introduction

La distribution quantique de clé, est un ensemble de protocoles cryptographique qui permettent à deux interlocuteurs d'échanger une clé secrète afin de garantir la sécurité inconditionnelle, en s'appuyant sur les lois fondamentales de la mécanique quantique (théorème de non-clonage et le principe d'incertitude de Heisenberg).

Dans ce chapitre, nous décrirons le principe de la distribution quantique de clé en premier lieu, par la suite nous définirons quelques protocoles à variables discrètes et d'autres à variables continues qui feront l'objet de notre étude.

II.2. Principe de la distribution quantique de clé

Le système de QKD nécessite habituellement deux canaux de transmission ; un canal quantique (fibre optique, espace libre), et un canal public authentifié (radio, internet), ce système est illustré sur la figure II.1.

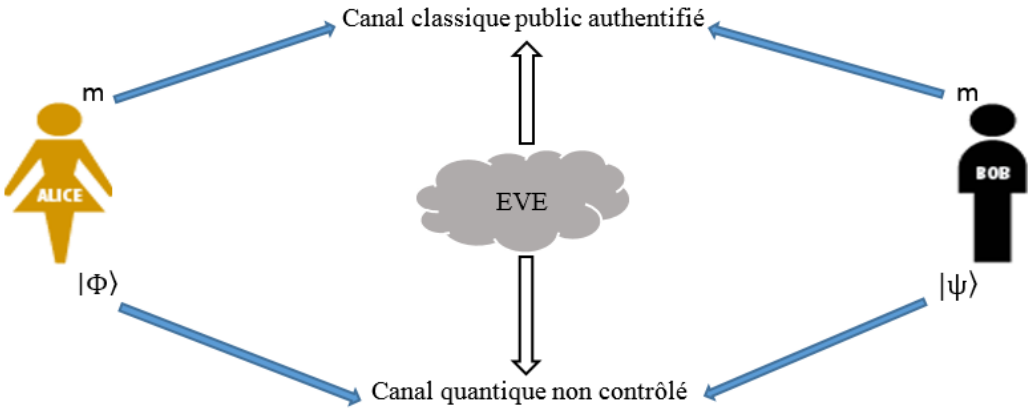

Figure II.1 : Schéma globale d'un système de distribution quantique de clé.

Au cours de ces dernières années, plusieurs protocoles de distribution quantique de clé ont été proposés. Pour analyser la sécurité de façon rigoureuse, il est nécessaire de prendre en compte les caractéristiques particulières de chaque protocole qui suivent la même procédure suivante :

- *Extraction de la clé brute :* Alice envoie sur le canal de transmission quantique, une séquence de symboles choisit d'une manière aléatoire. Bob effectue ses mesures sur la suite reçu, il obtient alors une séquence de bits appelée « clé brute ». D'autre part, Eve peut elle aussi avoir accès à ces données envoyées.

- *Estimation d'erreur :* Cette étape, permet à Alice et Bob d'estimer la quantité d'informations échangées via le canal public, et d'évaluer l'information interceptée par Eve selon des grandeurs statistiques telles que le taux d'erreur binaire quantique.
- *Réconciliation :* Alice et Bob effectuent un traitement de leurs données corrélées, par le canal public authentifié, selon un algorithme de correction d'erreurs.

  Pour corriger leurs données, Alice ou Bob génère un ensemble de bits à l'aide d'un code correcteur, puis il l'envoie à l'autre côté qui effectue la correction.

  A l'issue de cette étape, Alice et Bob obtiennent une clé tamisée, qui est utilisée dans la transmission des messages, à des fins de confidentialité, d'authentification ou autres.
- *Amplification de confidentialité :* L'amplification de confidentialité est la dernière étape de la procédure de distribution quantique de clé. C'est une technique qui permet de générer une clé secrète plus petite à partir de la clé tamisée. l'extraction de la clé secrète se fait à l'aide d'un algorithme qui élimine tous les bits connus par Eve.

  Cette procédure est expliquée dans le schéma de la figure II.2 :

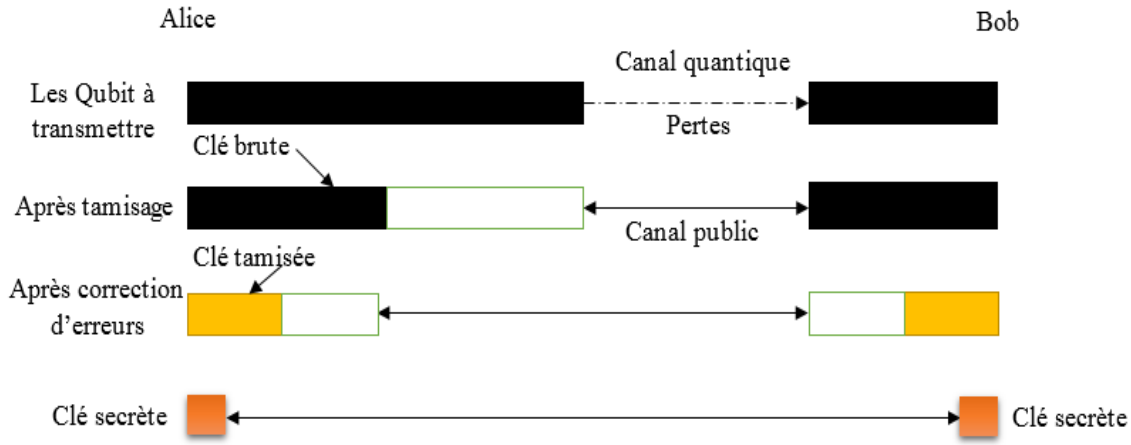

Figure II.2 : Schéma de la procédure suivie par les QKD.

II.3. Protocoles à variables discrètes

Les protocoles à variables discrètes sont des protocoles de génération de clé secrète où l'information est codée sur la polarisation, la phase, l'amplitude ou la fréquence d'un photon unique, ou d'un photon intriqué. Ces protocoles sont moins sensible au bruit ce qui permet une meilleure performance.

Dans Cette partie, nous présenterons quelques protocoles à variables discrètes, en commençant par le plus connu BB84 qui est basé sur la polarisation d'un photon unique. Ensuite le protocole utilisant le codage de phase B92, puis nous définirons brièvement les

protocoles inspirés de BB84 (à trois états, à six états). Et enfin, les protocoles à photon intriqué E91 avec ses deux approches.

II.3.1. Protocole BB84

En 1984, Gilles Brassard et Claude Bennett ont publiés le premier protocole de distribution quantique de clé BB84 [17]. Il permet à deux interlocuteurs distants de générer une clé de chiffrement aléatoire. Pour coder l'information, ce protocole utilise quatre états formant deux bases conjuguées d'un espace de Hilbert à deux dimensions (figure II.3), la base rectilinéaire $B_+ = \{|0_+\rangle, |1_+\rangle\}$, et la base diagonale $B_\times = \{|0_\times\rangle, |1_\times\rangle\}$.

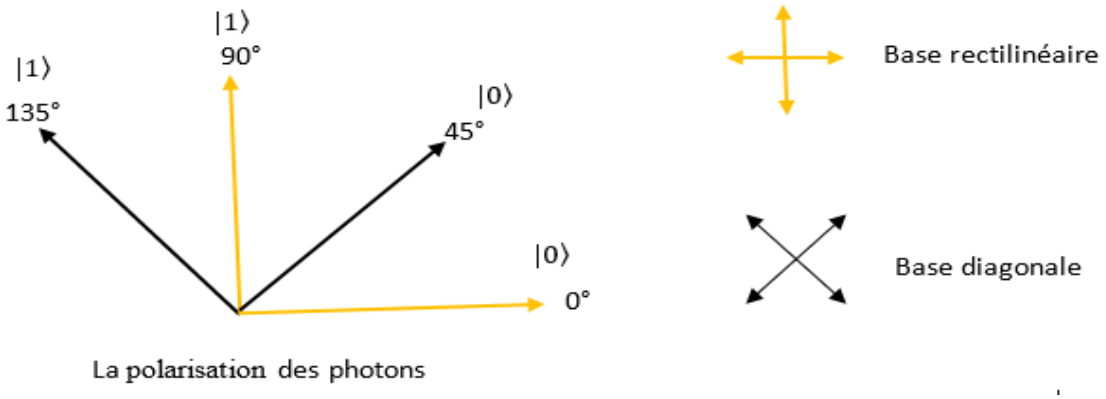

Figure II.3 : Les états de polarisation du protocole BB84.

En fonction des états $|0\rangle$ et $|1\rangle$, les bases (B_+ et $B_\times$) s'écrivent comme suit [18] :

$$|0_+\rangle = |0\rangle \qquad \text{(II. 1)}$$

$$|1_+\rangle = |1\rangle \qquad \text{(II. 2)}$$

$$|0_\times\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad \text{(II. 4)}$$

$$|1_\times\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \qquad \text{(II. 4)}$$

Le protocole BB84 suit les étapes suivantes :

1. Alice génère aléatoirement une suite de photons polarisés, et choisit l'une des deux bases. Ces photons seront transmis à Bob par un canal quantique.
2. Bob reçoit les photons envoyés et mesure leur polarisation en choisissant aléatoirement l'une des deux bases.

3. Bob annonce à Alice ces choix de bases via un canal classique, mais pas la valeur binaire associée à chaque photon.
4. Alice et Bob comparent leur choix de bases. Si le résultat est identique ils le conserve sinon il le rejet.
5. En comparant publiquement leurs résultats, Alice et Bob peuvent détecter la présence d'Eve. Alors, ils effectuent une correction d'erreur. Si le taux d'erreurs QBER (Quantum Bit Error Rate) est plus faible (<15%), donc il n'y a pas d'espion, cependant la communication est sécurisée. Sinon, Alice et Bob rejettent les données échangées et recommencent de la première étape.

Exemple explicatif de cet échange :

Alice	*Symbole*	0	0	1	1	1	0	0	1
	Base	×	+	+	×	+	+	×	+
	Polarisation du photon	↗	→	↑	↖	↑	→	↗	↑
Bob	*Base*	×	+	×	×	+	+	+	+
	Polarisation du photon	↗	↑	↖	↖	→	→	↑	↑
	Symbole	0	1	1	1	0	0	1	1
Alice Et Bob	*Décision*	✓	⋈	⋈	✓	⋈	✓	⋈	✓
	Clé secrète	0			1		0		1

Tableau II.1 : Exemple de distribution quantique de clé via le protocole BB84.

Un autre exemple en présence d'Eve:

Alice	*Symbole*	0	1	0	1
	Base	+	+	×	+
	Polarisation du photon	→	↑	↗	↑
Eve	*Base*	+	×	+	×
	Polarisation du photon	→	↖	↑	↗
	Symbole	0	1	1	0
Bob	*Base*	+	+	×	+
	Polarisation du photon	→	→	↖	↑
	Symbole	0	0	1	1
Alice Et Bob	*Décision*	✓	⋈	⋈	✓
	Clé secrète	0			1

Tableau II.2 : Exemple de distribution quantique de clé via le protocole BB84 en présence d'Eve.

II.3.2. Protocole B92

Le protocole B92 est une version simplifiée du protocole BB84, inventé en 1992 lorsque Charles Bennett s'est rendu compte qu'il n'était pas nécessaire d'utiliser deux bases orthogonales. Il trouve qu'une seule base non-orthogonale simple est suffisante pour garantir la détection d'un espion. L'idée de ce protocole est de coder la valeur d'un Qubit sur la phase d'un photon.

La seule différence entre B92 et BB84, est que le B92 utilise seulement deux états de polarisation $\{|\rightarrow\rangle, |\nearrow\rangle\}$, alors que le BB84 utilise 4 états de polarisation $\{|\rightarrow\rangle, |\uparrow\rangle, |\nearrow\rangle, |\nwarrow\rangle\}$. La figure II.4 montre les états de polarisation du protocole B92.

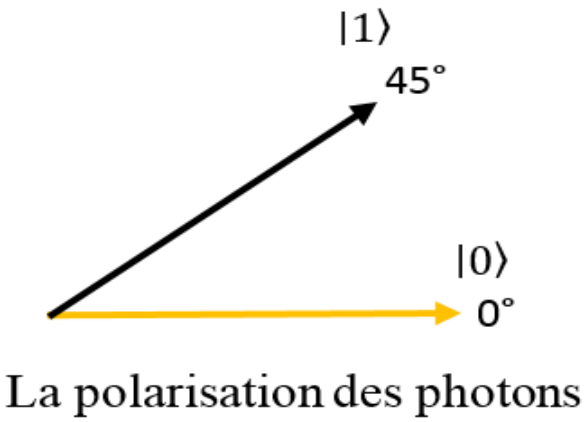

Figure II.4 : Les états de polarisation du protocole B92.

Le fonctionnement de ce protocole est identique à celui du protocole BB84.

1. Alice génère aléatoirement une séquence binaire, et choisit l'une des deux bases, puis elle encode chaque bit sur la phase d'un photon.
2. Bob mesure l'état quantique du photon sur l'une des deux bases qu'il choisit aléatoirement.
3. Puis, Alice et Bob échangent leur choix de base sur un canal classique. Lorsqu'il n'y a pas de coïncidence, les symboles correspondants sont rejetés. Dans le cas contraire ils les conservent, et constituant alors une clé de chiffrement commune.

II.3.3. Protocole à trois états

Le protocole à trois états est l'amélioration de BB84, ce dernier est symétrique dans son utilisation de polarisation, pour casser cette symétrie, le protocole à trois états emploie trois états et trois détecteurs au lieu de quatre états et deux détecteurs dans le protocole BB84. Ceci

réduit la probabilité d'espionnage pour obtenir de bons états, et ainsi de minimiser la quantité d'information utile envoyée par Alice [19].

II.3.4. Protocole à six états

Le protocole de distribution quantique de clé à six états ou à trois bases a été proposé par Pasquinucci et Gisin en 1999. C'est une généralisation du célèbre protocole BB84 de 4 états avec une base supplémentaire dite base circulaire notée $(B_{\circlearrowleft}, B_{\circlearrowright})$ qui correspond à l'état de polarisation circulaire gauche et droite avec :

$$|\circlearrowleft\rangle = \frac{|0\rangle + i|1\rangle}{\sqrt{2}} \qquad \text{(II. 5)}$$

$$|\circlearrowright\rangle = \frac{|0\rangle - i|1\rangle}{\sqrt{2}} \qquad \text{(II. 6)}$$

Donc les six états de polarisation de ce protocole sont : $\{|\rightarrow\rangle, |\uparrow\rangle, |\nearrow\rangle, |\nwarrow\rangle, |\circlearrowleft\rangle, |\circlearrowright\rangle\}$.

D'abord, Alice envoie un état choisi aléatoirement parmi les six états, ensuite, Bob effectue des mesures dans les bases (B_+ ou $B_\times$) ou $(B_{\circlearrowleft}, B_{\circlearrowright})$. Dans ce cas, la probabilité préalable qu'Alice et Bob utilisent la même base est réduite à 1/3 par rapport au protocole BB84 qui utilise quatre états de polarisation, ce qui donne une probabilité de 1/2.

Cependant, ce protocole tient un avantage de plus haute symétrie comparé au protocole BB84. La figure II.5 représente la sphère Poincaré avec les six états de polarisations.

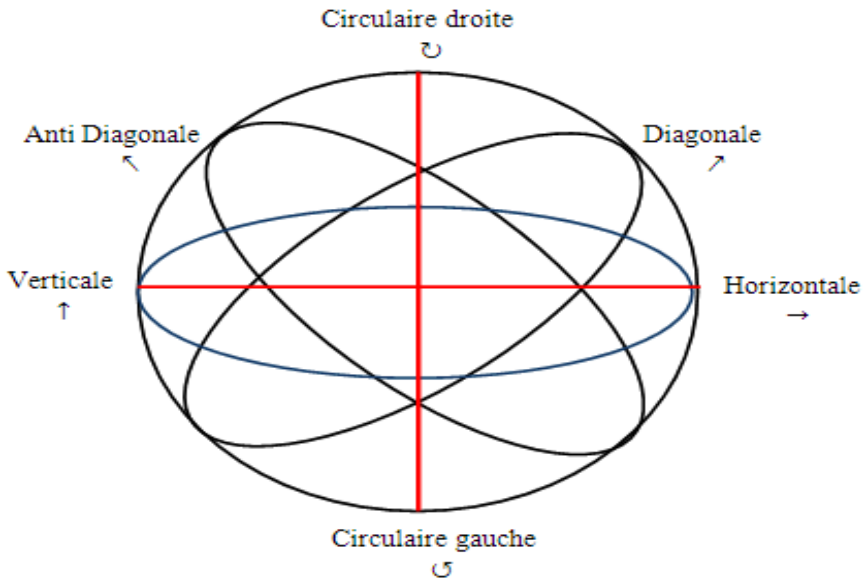

Figure II.5 : Sphère de Poincaré.

II.3.5. Protocole à états intriqués

En 1991, Artur Ekert proposa une nouvelle approche à la distribution quantique de clé

qui est différente du protocole BB84. Ce protocole nommé E91 (**E**kert 19**91**), utilise les états intriqués EPR (Einstein, Podolsk, Rosen) qui est une variante du protocole BB84 par codage de polarisation. L'idée de ce protocole, est d'utiliser des photons intriqués pour générer à distance des mesures corrélées chez Alice et Bob. Par conséquent, la sécurité de l'un implique la sécurité de l'autre. Il existe deux approches pour représenter ce protocole.

- *La première approche :* Est une approche standard, qui consiste à mettre une source de paires de photon intriqué au milieu du canal de transmission entre Alice et Bob, appelée source EPR. Les deux photons intriqués sont codées sur l'un des quatre états choisis aléatoirement par la source EPR et les envois dans deux directions opposées ; l'un vers Alice, l'autre vers Bob comme il est représenté sur la figure II.6.

  Ensuite, Alice et Bob choisiraient chacun une base aléatoire sur laquelle mesurant l'état du photon reçu. En comparant leurs résultats, Alice et Bob ne conservent leurs mesures que si leurs choix de base de mesure coïncident avec le choix de base de la source.

Figure II.6 : La première approche du E91.

- *La deuxième approche :* Est l'approche la plus simple, dont la source de photons intriqués est incluse dans le côté d'Alice. Dans ce cas, Alice génère une paire de photons intriqués, dont elle garde l'un d'eux et envoie l'autre à Bob (figure II.7). Après la réception, Alice et Bob mesurent leur photons respectif dans B_+ ou $B_\times$, en choisissant une base aléatoirement et indépendamment. En comparant publiquement les bases de mesure, Si les bases d'Alice et Bob sont les mêmes ils conservent le résultat sinon ils le rejettent [18].

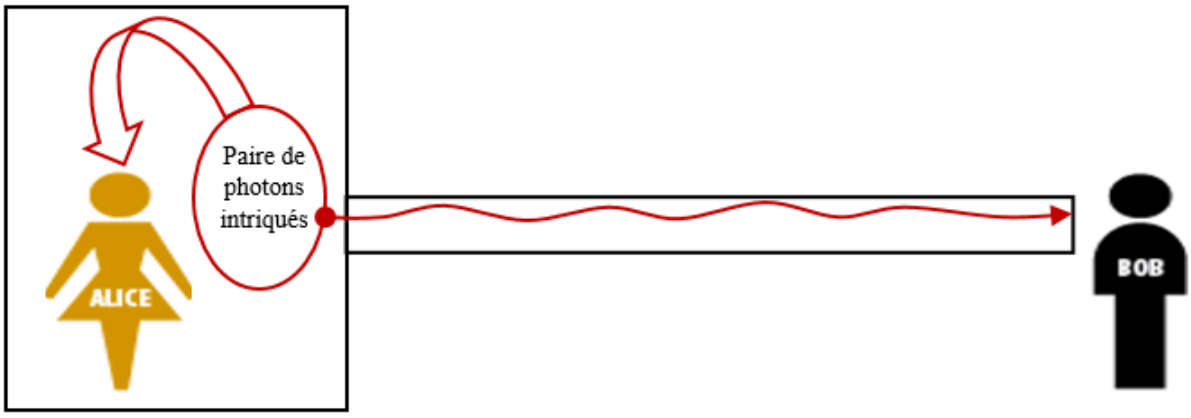

Figure II.7 : La deuxième approche du E91.

II.4. Étude des protocoles à variables continues

Récemment, les variables continues, ont émergées comme un nouvel outil dans le domaine de l'information quantique, elles servent à développer de nouveaux protocoles qui permet de simplifier grandement le dispositif expérimental, en particulier la détection, où les compteurs de photons sont remplacés par la détection homodyne ou hétérodyne, ainsi que l'utilisation des impulsions à grand nombre de photons qui permet de coder beaucoup plus d'informations.

De façon simplifiée, le système de distribution quantique de clé à variables continues (CV-QKD), utilise une source de lumière cohérente de bonne qualité, telle qu'une diode laser. Le faisceau lumineux est découpé à haute cadence, en des impulsions de lumière intenses, qui contiennent chacune un grand nombre de photons [20].

Ces variables comportent un ensemble d'états indépendants pour encoder l'information. Cependant il existe trois types d'états continus :

- *L'état vide* $|0\rangle$: c'est l'état gaussien le plus simple, défini comme état fondamental de l'oscillateur harmonique, tel que $\hat{a}|0\rangle = 0$. Le nombre moyen de photons dans cet état est nul [13].
- *Les états comprimés :* sont des états de moyenne nulle et d'incertitude minimale qui peuvent être choisis pour avoir une stratégie bien définie sur deux quadratures ; dont l'une est comprimée et l'autre est amplifiée [21].
- *Les états cohérents* $|\alpha\rangle$ *:* qui sont des états à incertitude minimale autour de leur moyenne, avec $|\alpha\rangle \in \mathbb{C}$, et $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$ [3].

Les états cohérents sont beaucoup plus faciles à générer que les états comprimés. Ainsi, pour les schémas de base de QKD, les états comprimés ne sont pas assez pratiques [3]. Pour cette raison, nous nous focaliserons sur le codage de l'information sur les états cohérents.

Les variables continues sont représentées par les quadratures $\hat{X}$ et $\hat{P}$ en référence à la position et à l'impulsion d'un oscillateur harmonique, qui sont caractérisées par la relation de commutation [13]:

$$\left[\hat{X}, \hat{P}\right] = 2iN_0 \qquad \text{(II. 7)}$$

Où N_0 est une constante de normalisation du niveau de bruit quantique.

Ce commutateur est associé à la relation d'incertitude de Heisenberg qui traduit l'impossibilité de réaliser une mesure simultanée des deux quadratures $\hat{X}$ et $\hat{P}$ avec une précision arbitraire :

$$\Delta X \, \Delta P \geq N_0 \qquad \text{(II. 8)}$$

Où ΔX *et* ΔP correspondent à l'écart type du bruit sur la mesure associé respectivement aux quadratures *X* et *P*.

Bruit de photon

Le bruit de photons limite tout système de détection de flux lumineux. Les photons arrivent sur le détecteur de façon totalement désordonnée. Ce désordre est lié simplement à la source lumineuse. Si la surface du détecteur reçoit en moyenne N_0 photons pendant un temps d'intégration τ, l'écart type sur le nombre de photons reçus est égal à $\sqrt{N_0}$. Où la variance de bruit de photon N_0=1.

Le bruit de photons se traduit au niveau des détecteurs quantiques par le bruit de Schottky (*shot noise*) [22].

II.4.1. État cohérent et état gaussiens

Les états cohérents ont été introduits en mécanique quantique, pour représenter des paquets d'onde possédant de bonnes propriétés de « cohérence ». La découverte des premiers états cohérents a été attribuée à Schrödinger en 1926, où ils sont apparus comme les solutions de l'équation de l'oscillateur harmonique quantique les plus proches de l'oscillateur classique qui lui est associé. Ils constituent des éléments de l'espace de Hilbert [23].

Les états cohérents sont des états gaussiens ; donc ils sont modélisés par un canal gaussien qui exprime les perturbations subies par un état cohérent envoyé par Alice dans un canal quantique ajoutant un bruit gaussien. Dans ce modèle, Alice prépare aléatoirement un état cohérent centré à (X_A, P_A), d'une distribution gaussienne de moyenne zéro et de variance $V_A N_0$, sachant que $V_A \gg 1$. Les opérateurs quantiques de l'état sortant du dispositif d'Alice

s'expriment donc par (II.9) et (II.10).

$$X = X_A + X_0 \qquad \text{(II. 9)}$$

$$P = P_A + P_0 \qquad \text{(II. 10)}$$

Alors elle l'envoie à Bob à travers le canal quantique caractérisé par une transmission $G = g^2 = T\eta \leq 1$ (où T est la transmission du canal quantique et η est l'efficacité du détecteur) et un bruit en excès ε. Le bruit total ajouté par le canal est exprimé par (II.11).

$$\chi = \frac{1}{G} - 1 + \varepsilon \qquad \text{(II. 11)}$$

Où $\chi_0 = \frac{1}{G} - 1$, est le bruit dû aux pertes.

Après avoir reçu l'état, Bob mesure aléatoirement l'une des quadratures *X* ou *P* donc on parle d'une détection homodyne, mais s'il mesure simultanément les deux quadratures, alors on parle d'une détection hétérodyne. Afin d'extraire l'information secrète on exécute une réconciliation directe ou inverse.

On écrit alors la quadrature X_B mesurée par Bob :

$$X_B = g(X_A + X_0 + X_{CB}) = g(X_A + X_N) \qquad \text{(II. 12)}$$

Où X_0 le bruit de photon, X_{CB} le bruit gaussien et X_N bruit ramené à l'entrée [13] [24].

II.4.2. La Réconciliation d'information

La sécurité du protocole de CV-QKD à la détection homodyne ou hétérodyne contre un intrus, a été établie en utilisant la réconciliation d'information, qui est une forme de correction d'erreur. Elle peut être réalisée de deux façons différentes:

- *La réconciliation directe :* la clé est construite à partir des données envoyées par Alice. Pour un total de transmission inférieure à 50% (pertes > 3 dB), l'information que possède Bob sur les données d'Alice, est généralement plus faible que l'information que possède Eve sur ces mêmes données, dans ce cas aucune clé secrète ne peut être distillé.
- *La réconciliation inverse :* dans une telle réconciliation, les symboles de Bob servent de référence. Cependant, Alice corrige ses bits selon les données de Bob.

  En utilisant ce type de réconciliation, la limite de perte de 3 décibels peut être surmontée. Dans un tel scénario, les informations d'Alice sur les résultats de mesure de Bob sont toujours plus grandes que celles d'Eve, qui cumule ses propres erreurs aux erreurs de Bob.

II.4.3. La détection Homodyne

Pendant la phase de transmission de clés, Alice envoie des états cohérents modulés aléatoirement X et P. Bob reçoit ces états cohérents bruyants avec un débit de symbole donné, puis il effectue ses mesures en utilisant la technique de détection homodyne, où le signal est mélangé avec un laser de référence (l'oscillateur local, OL) à un séparateur de faisceau équilibré.

Selon le protocole, Bob mesure une seul composante en quadrature en sélectionnant au hasard entre $\theta = 0$ et $\theta = \pi/2$ pour chaque mode entrant [25]. Le principe d'une détection homodyne est illustré sur la figure II.8.

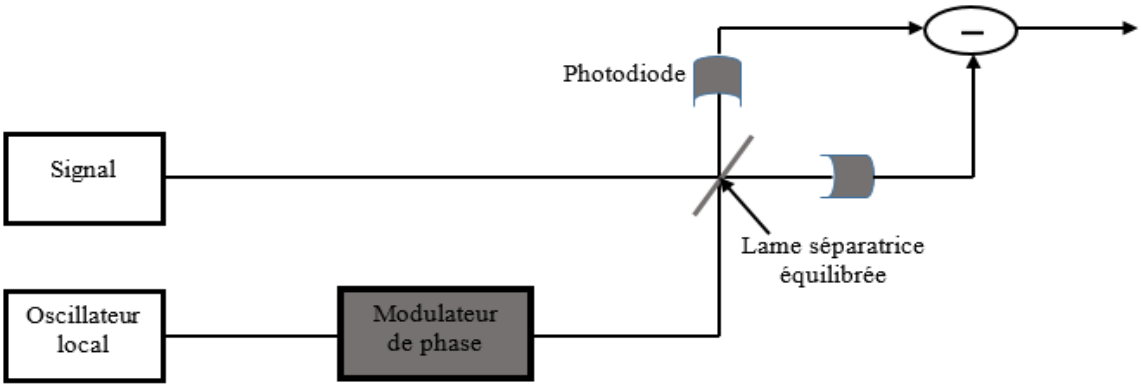

Figure II.8 : Schéma bloc d'une détection homodyne.

En 2002, Grosshans et Grangier ont proposés le premier protocole CV-QKD appelé protocole GG02, qui utilise des états cohérents produits facilement avec une source laser commune. Ce protocole met en jeu une modulation gaussienne des deux quadratures d'états cohérents sur le côté d'Alice et applique une détection homodyne sur le côté de Bob sur une des quadratures choisies au hasard [26].

II.4.4. La détection hétérodyne

Nous parlons de la détection hétérodyne lorsque Bob utilise un séparateur de faisceau équilibré pour séparer les états entrants, et deux détecteurs homodyne pour mesurer les deux composantes en quadrature simultanément (Figure II.9), une avec $\theta = 0$ pour mesurer X et l'autre avec $\theta = \pi/2$ pour mesurer P. L'utilisation de la détection hétérodyne au lieu de la détection homodyne doublera l'information mutuelle pour chaque symbole pour la valeur de la perte supplémentaire de 3 dB introduite par le séparateur de faisceau hétérodyne [25].

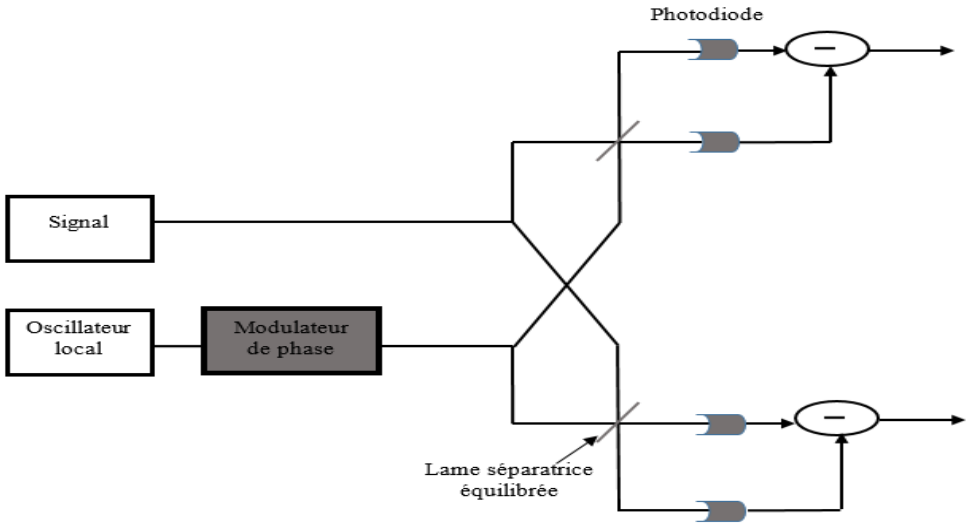

Figure II.9 : Schéma bloc d'une détection hétérodyne.

II.4.5. Principe de fonctionnement des protocoles CV-QKD

Les protocoles CV-QKD, sont décrits par les étapes suivantes :

1. Alice choisit aléatoirement deux nombres réels x_A et p_A, d'une distribution gaussienne de moyenne zéro et de variance $V_A N_0$.
2. Elle prépare l'état cohérent $|x_A + ip_A\rangle$ et elle l'envoie à Bob à travers un canal quantique.
3. Bob choisit au hasard de mesurer une quadrature soit X ou P cas du protocole GG02, ou mesure les deux quadratures à la fois dans le cas d'une détection hétérodyne.
4. Concernant le protocole GG02, Bob utilise un canal public pour informer Alice de son choix de quadrature, elle peut donc abandonner la quadrature non choisie.
5. Ensuite, Alice et Bob partagent un ensemble de données corrélés afin d'obtenir une clé secrète commune. Puis, ils effectuent l'estimation des paramètres de transmission T et l'excès de bruit ε du canal quantique. Enfin, ils réconcilient les données restantes (correction de l'erreur) par l'amplification confidentielle [25].

Arrivant à ce stade, Alice et Bob peuvent maintenant calculer les différentes informations mutuelles.

II.4.6. Types d'attaques

On distingue trois types d'attaques qu'Eve peut implémenter :

- *Attaques individuelles :* Ce sont les attaques les plus simples. Eve est autorisée à interagir de manière individuelle avec chaque état cohérent envoyé par Alice, et à

stocker son état dans une mémoire quantique. Puis elle attend que Bob révèle ses choix de quadrature pour réaliser la mesure la plus adaptée en fonction de cette dernière [13]. La figure II.10, montre la modélisation de ce type d'attaque.

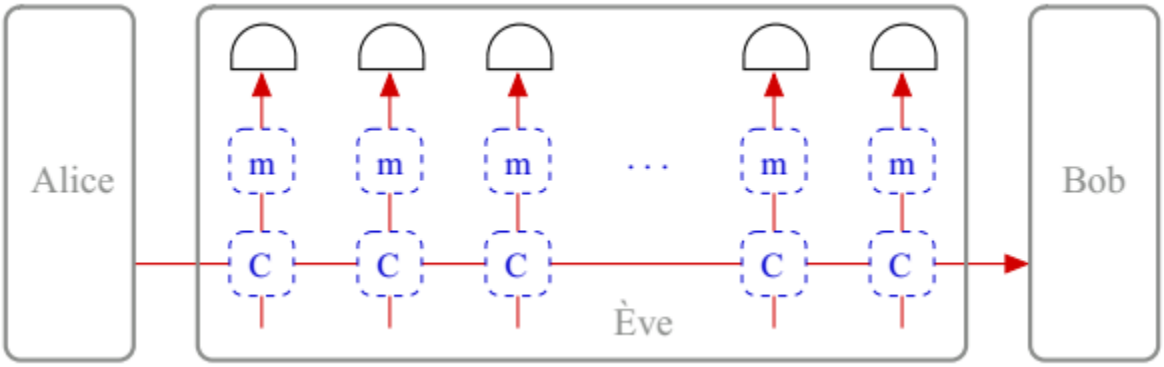

Figure II.10 : Modélisation de l'attaque individuelle [13].

- *Attaques collectives :* Sont une généralisation des attaques individuelles où Eve a la possibilité d'attendre la fin de la phase de réconciliation pour effectuer ses mesures [27]. Comme illustré sur la figure II.11.

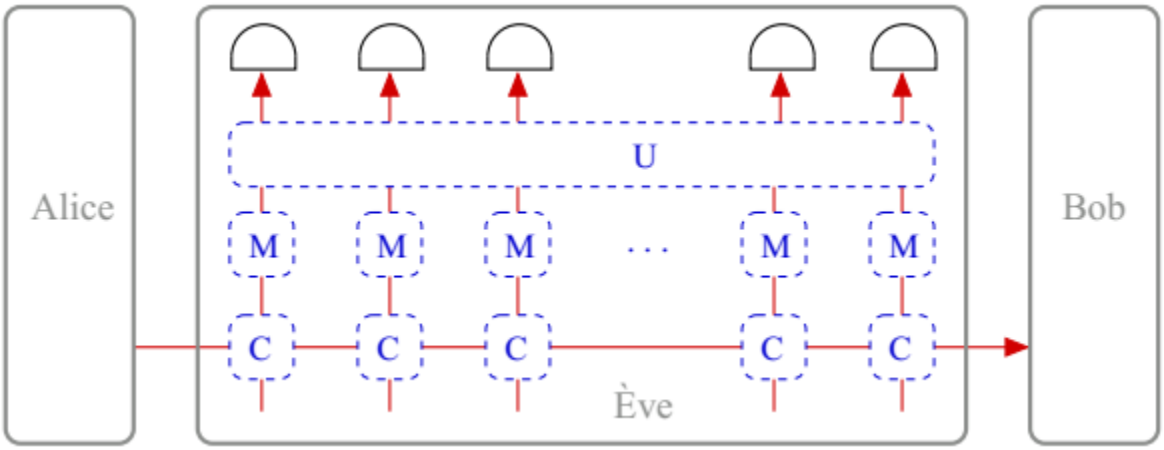

Figure II.11 : Modélisation de l'attaque collective [13].

- *Attaques cohérentes :* ce sont les attaques les plus puissantes, ou Eve n'est limitée que par les lois de la mécanique quantique. Elle peut préparer un ensemble de ressources intriquées stockées dans une mémoire quantique, qu'elle fait interagir avec chaque état envoyé par Alice, ensuite elle attend la fin de la phase de réconciliation pour faire des mesures collectives [21]. La modélisation de ce type d'attaque est représentée sur la figure II.12.

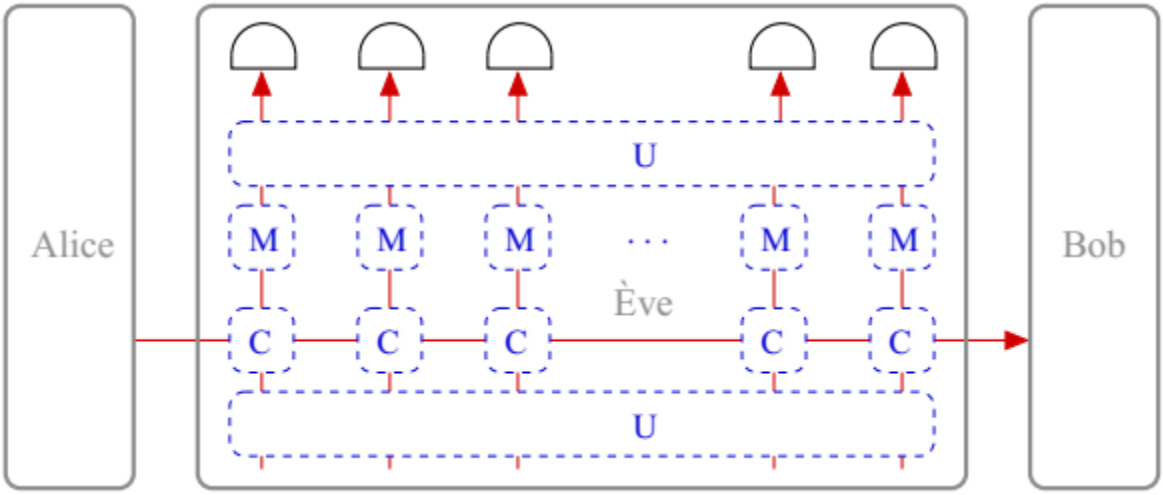

Figure II.12 : Modélisation de l'attaque cohérente [13].

II.4.7. Information et variables continues

Dans un premier temps, nous allons déterminer les informations mutuelles ainsi que l'information secrète pour le cas général, puis nous étendons au cas des attaques individuelles et collectives de l'espion.

II.4.7.1.Cas général

Nous nous plaçons dans le cas général d'une détection homodyne et hétérodyne, en s'appuyant sur les différentes notions et expressions abordés précédemment.

Dans le cas d'une détection homodyne, l'expression de l'information mutuelle I_{AB} entre Alice et Bob est obtenue par le théorème de Shannon (équation I.19).

$$I_{AB} = \frac{1}{2}\log_2 \frac{\langle X_B^2 \rangle}{G\langle X_N^2 \rangle} \qquad \text{(II. 13)}$$

D'après l'équation (II.12), on obtient :

$$I_{AB} = \frac{1}{2}\log_2 \frac{G\langle (X_A + X_N)^2 \rangle}{G\langle X_N^2 \rangle} \qquad \text{(II. 14)}$$

$$= \frac{1}{2}\log_2 \frac{\langle X_A^2 \rangle + \langle X_N^2 \rangle + \langle X_A X_N \rangle}{\langle X_N^2 \rangle} \qquad \text{(II. 15)}$$

$$= \frac{1}{2}\log_2 \left(1 + \frac{\langle X_A^2 \rangle}{\langle X_N^2 \rangle}\right) \qquad \text{(II. 16)}$$

$$= \frac{1}{2}\log_2 \left(1 + \frac{V_A}{V_N}\right) \qquad \text{(II. 17)}$$

En introduisant le rapport signal à bruit :

$$SNR = \frac{V_A}{V_N} \qquad \text{(II. 18)}$$

L'expression de I_{AB}, s'écrit alors :

$$I_{AB} = \frac{1}{2}\log_2(1 + SNR) \qquad \text{(II. 19)}$$

En utilisant la variance conditionnelle de *B* sachant *A* :

$$V_{B|A} = G\langle X_N^2 \rangle \qquad \text{(II. 20)}$$

$$V_{B|A} = GV_N \qquad \text{(II. 21)}$$

Et

$$V_B = G(V_A + V_N) \qquad \text{(II. 22)}$$

Ce qui donne :

$$I_{AB} = \frac{1}{2}\log_2 \frac{V_B}{V_{B|A}} \qquad \text{(II. 23)}$$

Avec nos paramètres du canal gaussien, on obtient :

$$I_{AB} = \frac{1}{2}\log_2 \frac{(V + \chi)}{(1 + \chi)} \qquad \text{(II. 24)}$$

Où $V = V_A+1$, est la variance totale de la modulation sortie d'Alice.

L'information dont dispose Eve sur les données d'Alice est notée I_{AE}, celle commune à Eve et Bob est notée I_{BE}.

$$I_{AE} = \frac{1}{2}\log_2 \frac{V_A}{V_{A|E}} \qquad \text{(II. 25)}$$

$$I_{AE} = \frac{1}{2}\log_2 \frac{V + \frac{1}{\chi}}{1 + \frac{1}{\chi}} \qquad \text{(II. 26)}$$

L'information qu'obtient Eve sur la clé de Bob est donnée par :

$$I_{BE} = \frac{1}{2}\log_2 \frac{V_B}{V_{B|E}} \qquad \text{(II. 27)}$$

$$I_{BE} = \frac{1}{2}\log_2 G^2(V + \chi)\left(\frac{1}{V} + \chi\right) \qquad \text{(II. 28)}$$

Pour la détection hétérodyne, où la mesure s'effectue sur les deux quadratures à la fois, l'information mutuelle entre Alice et Bob est donnée par :

$$I_{AB} = 2 \times \frac{1}{2}\log_2(1 + SNR) \qquad (II.29)$$

$$I_{AB} = \log_2 \frac{V_A}{V_N} \qquad (II.30)$$

La variance totale du bruit ramené à l'entrée s'exprime par :

$$V_N = 1 + \chi + \frac{1}{G} \qquad (II.31)$$

$$I_{AB} = \log_2 \left(\frac{V + \chi + \frac{1}{G}}{1 + \chi + \frac{1}{G}} \right) \qquad (II.32)$$

L'information mutuelle entre Alice et Eve et celle entre Bob et Eve, sont données par les équations (II.33) et (II.34) respectivement.

$$I_{AE} = \log_2 \left(\frac{V + \frac{1}{\chi}}{1 + \frac{1}{\chi}} \right) \qquad (II.33)$$

$$I_{BE} = \log_2 \left(\frac{G\left(V + \chi + \frac{1}{G}\right)}{\frac{1}{G\left(\chi + \frac{1}{V}\right)} + 1} \right) \qquad (II.34)$$

Donc, le taux de la clé secrète utile pour les deux détections est donnée se présente comme suit :

- Cas d'une réconciliation directe.

$$\Delta I = I_{AB} - I_{AE} \qquad (II.35)$$

- Cas d'une réconciliation inverse.

$$\Delta I = I_{AB} - I_{BE} \qquad (II.36)$$

Dans ce qui suit, on utilise le protocole inverse pour l'étude de l'influence des attaques individuelles et collectives sur les deux détections homodyne et hétérodyne.

II.4.7.2. Attaque individuelle

Pour la détection homodyne, l'information mutuelle entre Alice et Bob :

$$I_{AB}^{hom} = \frac{1}{2}\log_2(1+SNR) \qquad \text{(II. 37)}$$

$$= \frac{1}{2}\log_2\left(1+\frac{V_A}{1+\chi_{tot}}\right) \qquad \text{(II. 38)}$$

$$I_{AB}^{hom} = \frac{1}{2}\log_2\left(\frac{V+\chi_{tot}}{1+\chi_{tot}}\right) \qquad \text{(II. 39)}$$

Sachant que

$$\chi_{tot} = \chi_{line} + \frac{\chi_{hom}}{T} \qquad \text{(II. 40)}$$

$$\chi_{line} = \frac{1-T}{T} + \varepsilon \qquad \text{(II. 41)}$$

$$\chi_{hom} = \frac{1-\eta}{\eta} + \frac{v_{el}}{\eta} \qquad \text{(II. 42)}$$

Où v_{el} est le bruit électronique.

Remplaçons les équations (II.41) et (II.42) dans l'équation (II.40) on obtient :

$$\chi_{tot} = \frac{1-G}{G} + \varepsilon + \frac{v_{el}}{G} \qquad \text{(II. 43)}$$

L'information mutuelle entre Bob et Eve

$$I_{BE}^{hom} = \frac{1}{2}\log_2\frac{V_B}{V_{B|E}} \qquad \text{(II. 44)}$$

$$I_{BE}^{hom} = \frac{1}{2}\log_2\frac{T^2(V+\chi_{tot})\left(\frac{1}{V}+\chi_{line}\right)}{1+T\chi_{hom}\left(\frac{1}{V}+\chi_{line}\right)} \qquad \text{(II. 45)}$$

Dans le cas d'une détection hétérodyne, les différentes informations mutuelles sont données comme suit :

$$I_{AB}^{het} = 2\times\frac{1}{2}\log_2\frac{V_B}{V_{B|A}} \qquad \text{(II. 46)}$$

$$I_{AB}^{het} = \log_2\frac{V+\chi_{tot}}{1+\chi_{tot}} \qquad \text{(II. 47)}$$

Sachant que

$$\chi_{tot} = \chi_{line} + \frac{\chi_{het}}{T} \qquad \text{(II. 48)}$$

$$\chi_{het} = \frac{1 + (1-\eta) + 2v_{el}}{\eta} \qquad \text{(II. 49)}$$

L'information mutuelle entre Bob et Eve est :

$$I_{BE}^{het} = \log_2 \frac{V_B}{V_{B|E}} \qquad \text{(II. 50)}$$

$$I_{BE}^{het} = \log_2 \frac{T(V + \chi_{tot})(V + \chi_E)}{V\chi_E + 1 + \chi_{het}(V + \chi_E)} \qquad \text{(II. 51)}$$

Sachant que :

$$\chi_E = \frac{T(2-\varepsilon)^2}{\left(\sqrt{2 - 2T + T\varepsilon} + \sqrt{\varepsilon}\right)^2} + 1 \qquad \text{(II. 52)}$$

Pour les deux détections homodyne et hétérodyne, la quantité d'information secrète disponible après la transmission peut s'écrire :

$$\Delta I_{Shannon} = I_{AB} - I_{BE} \qquad \text{(II. 53)}$$

II.4.7.3. Attaque collective

Dans l'attaque précédente on a utilisé l'information mutuelle de Shannon. Devetak et Winter ont montré que l'information mutuelle à utiliser dans le cas de l'attaque collective est l'information mutuelle quantique de Holevo, χ_{BE}.

Pour la détection homodyne χ_{BE} s'écrit :

$$\chi_{BE} = G\left[\left(\frac{\lambda_1 - 1}{2}\right) + \left(\frac{\lambda_2 - 1}{2}\right) - \left(\frac{\lambda_3 - 1}{2}\right) - \left(\frac{\lambda_4 - 1}{2}\right)\right] \qquad \text{(II. 54)}$$

$$\chi_{BE} = G\left[\frac{\lambda_1 + \lambda_2}{2} - \frac{\lambda_3 + \lambda_4}{2}\right] \qquad \text{(II. 55)}$$

Avec

$$\lambda_{1,2}^2 = \frac{1}{2}\left(A \pm \sqrt{A^2 - 4B}\right) \qquad \text{(II. 56)}$$

$$\lambda_{3,4}^2 = \frac{1}{2}\left(C \pm \sqrt{C^2 - 4D}\right) \qquad \text{(II. 57)}$$

Avec

$$A = V^2(1-2T) + 2T + T^2(V+\chi_{line})^2 \qquad (II.58)$$

$$B = T^2(V\chi_{line}+1)^2 \qquad (II.59)$$

$$C_{hom} = \frac{V\sqrt{B} + T(V+\chi_{line}) + A\chi_{hom}}{T(V+\chi_{tot})} \qquad (II.60)$$

$$D_{hom} = \sqrt{B}\frac{V+\sqrt{B}\chi_{hom}}{T(V+\chi_{tot})} \qquad (II.61)$$

Dans le cas de la détection hétérodyne, les formules sont exactement les mêmes que pour le cas homodyne, juste les expressions de C_{het} et D_{het} qui sont données par :

$$C_{het} = \frac{A\chi_{het}^2 + B + 1 + 2\chi_{het}\left(V\sqrt{B} + T(V+\chi_{line})\right) + 2T(V^2-1)}{\left(T(V+\chi_{tot})\right)^2} \qquad (II.62)$$

$$D_{het} = \left(\frac{V+\sqrt{B}\chi_{het}}{T(V+\chi_{het})}\right)^2 \qquad (II.63)$$

L'information secrète s'écrit alors :

$$\Delta I_{Holevo} = I_{AB} - \chi_{BE} \qquad (II.64)$$

II.5. Conclusion

Dans le présent chapitre nous avons présenté les différents protocoles de distribution quantique de clé à savoir les protocoles à variables discrètes et à variables continues. En mettant l'accent sur derniers dans le cas d'utilisation des états cohérents gaussiens. Par la suite, nous avons présenté les deux types de détection de variables qui soit à détection homodyne ou hétérodyne, suivit des explications de leurs méthodes de réconciliation directe et inverse.

Afin de mieux comprendre, et d'assimiler leurs principes on a fait appel aux lois de la théorie d'information de Shannon et de Holevo. A la fin, nous avons discuté l'influence des attaques individuelles et collectives sur les protocoles à détection homodyne et hétérodyne.

Le chapitre suivant, sera consacré à la simulation des différentes informations mutuelles établies au cours de ce chapitre.

Chapitre III
Simulation des protocoles de distribution quantique de clé à variables continues

III.1. Introduction

Dans ce chapitre, notre but est focalisé sur les protocoles de distribution quantique de clé à variables continues. Pour cela, nous allons simuler les différentes équations abordées dans le chapitre précédent en utilisant l'environnement de développement MATLAB.

En premier lieu, nous nous intéresserons à faire une comparaison entre les protocoles direct et inverse dans le cas des détections homodyne et hétérodyne. En second lieu nous visualiserons l'influence des attaques individuelles et collectives sur la sécurité de ce type de protocoles.

Cela, nous permettra de déduire quelle détection et quel protocole nous offre plus de performance en termes de sécurité, de débit et de portée.

III.2. Influence du gain du canal de transmission sur le bruit ajouté

Afin de visualiser l'influence de la transmission sur le bruit ajouté, nous faisons une simulation sur l'évolution de bruit total en fonction de G pour un canal sans excès de bruit ; $\varepsilon = 0$. Pour cela, en faisant varier la transmission du canal G de 0.1 à 1 dans l'équation (II.11). La figure III.1 représente la courbe obtenue

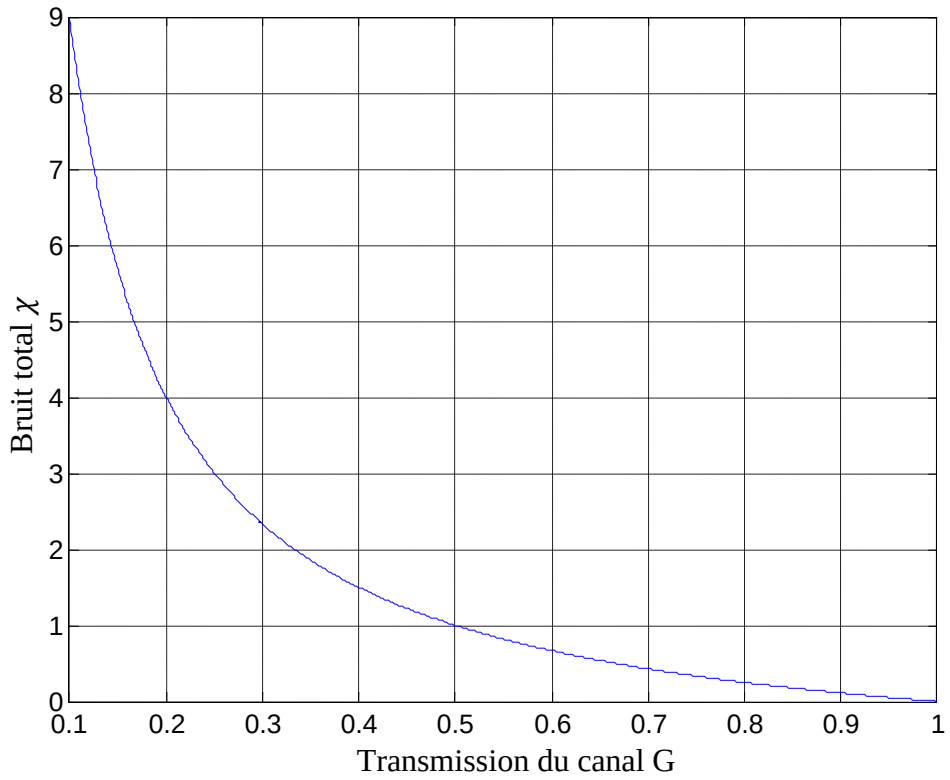

Figure III.1 : Influence de la transmission sur le bruit ajouté.

D'après la figure, au début de la transmission, le bruit total est très élevé, cela est dû aux imperfections du canal. Puis il diminue avec l'augmentation de la valeur de transmission du canal G. Nous concluons que la qualité de la liaison s'améliore avec l'augmentation de la transmission G. Donc, nos résultats expérimentaux suivent raisonnablement la prédiction théorique (équation II.11).

III.3. Les informations mutuelles des protocoles à variables continues

Dans cette partie, nous représentons les résultats de la simulation des différentes informations mutuelles et secrètes des protocoles à variables continues à détection homodyne et hétérodyne dans le cas général. Puis nous évaluerons l'influence des attaques individuelles et d'attaques collectives sur la sécurité des protocoles et le débit de la clé secrète.

III.3.1. Cas général

Dans ce cas, nous varions la transmission G de 0 à 1, en prenant la variance de modulation $V = 40$ et nous considérons un excès de bruit $\varepsilon = 0$.

- **La détection homodyne**

Les courbes des informations mutuelles ; entre Alice et Bob donnée par l'équation (II.24), et celle entre Alice et Eve donnée par l'équation (II.26), ainsi que l'information secrète (équation II.35) dans le cas du protocole direct, sont illustrées sur la figure (III.2).

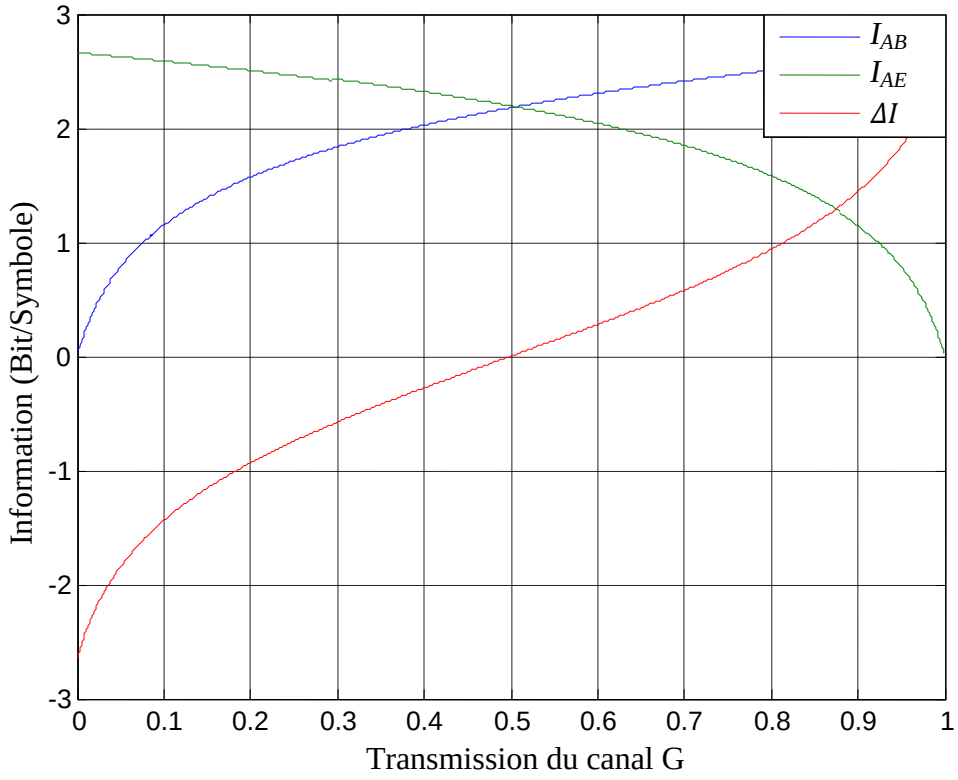

Figure III.2 : Informations mutuelles du protocole à détection homodyne dans le cas d'une réconciliation directe.

Les résultats de notre simulation, montrent que l'information secrète ΔI est négative pour des valeurs de transmission du canal quantique inférieur à 1/2, ce qui veut dire qu'Eve acquiert plus d'information que Bob sur les données d'Alice ($I_{AE} > I_{AB}$) d'où la transmission sera annulée. Par contre, pour des transmissions supérieures à 1/2, l'information secrète est positive, dans ce cas, Bob obtient plus d'information sur les données émises par Alice ($I_{AB} > I_{AE}$).

Pour le protocole inverse, nous gardons la même information mutuelle entre Alice et Bob. Et nous calculons celle entre Bob et Eve donnée par l'équation (II.28), ainsi nous évaluons l'information secrète (équation II.36). La figure III.3 montre les résultats de la simulation.

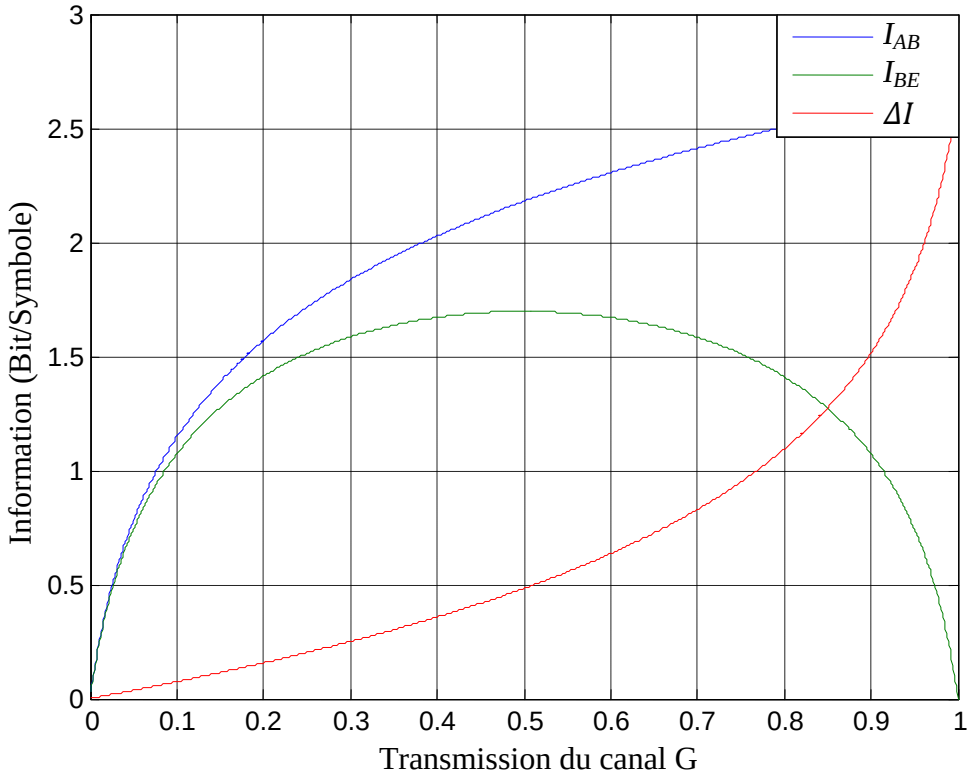

Figure III.3 : Informations mutuelles dans le cas du protocole inverse à détection homodyne.

Nous constatons que pour toute la transmission du canal quantique, l'information mutuelle entre Alice et Bob est toujours supérieur à celle entre Bob et Eve ($I_{AB} > I_{BE}$), d'où l'information secrète est toujours positive, ce qui donne la possibilité de distribuer une clé secrète sur tous le canal quantique.

En comparant les deux protocoles, nous concluons que ceux à réconciliation directe ne fonctionnent de manière satisfaisante que pour de fortes valeurs de transmission G. Cependant, le protocole à réconciliation inverse peut dépasser cette limite, en factionnant sur toute la transmission.

- **La détection hétérodyne**

La figure III.4, représente les courbes des différentes équations (II.32), (II.33), (II.35) attribuent respectivement aux informations mutuelles entre Alice et Bob, Alice et Eve, et l'information secrète, dans le cas de la détection hétérodyne avec protocole direct.

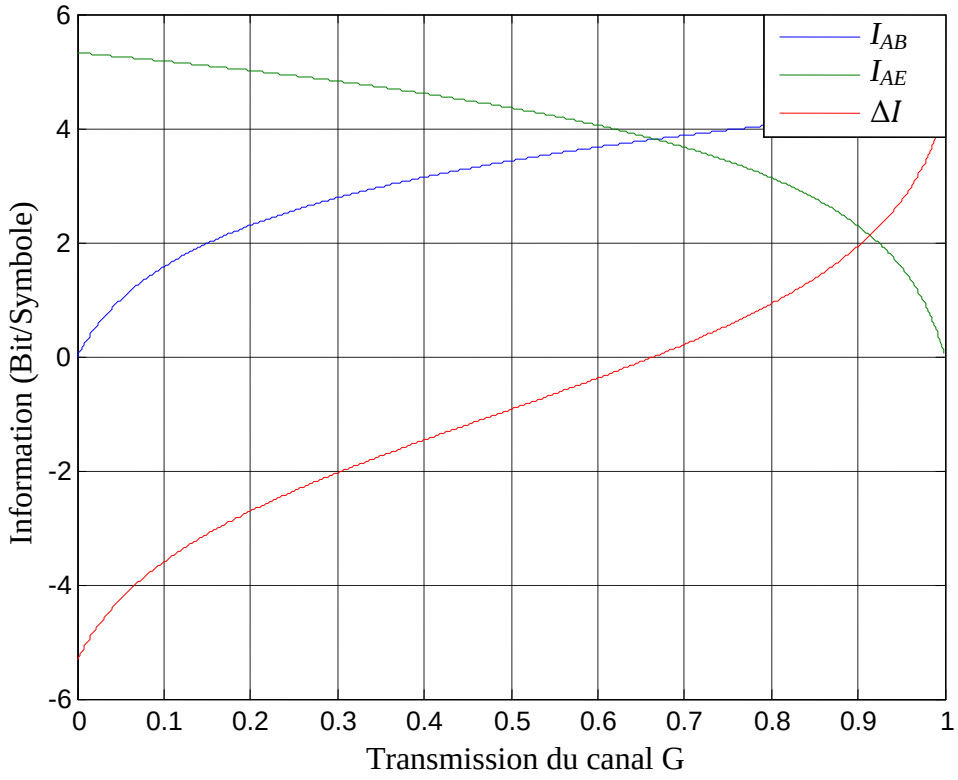

Figure III.4 : Informations mutuelles dans le cas du protocole direct à détection hétérodyne.

Les résultats de simulation du protocole à détection hétérodyne avec réconciliation inverse, sont illustrés sur la figure III.5. L'information mutuelle entre Alice et Bob est la même que celle en protocole direct, nous calculons l'information mutuelle entre Bob et Eve qui est donnée par l'équation (II.34), et l'information secrète introduite en équation (II.36).

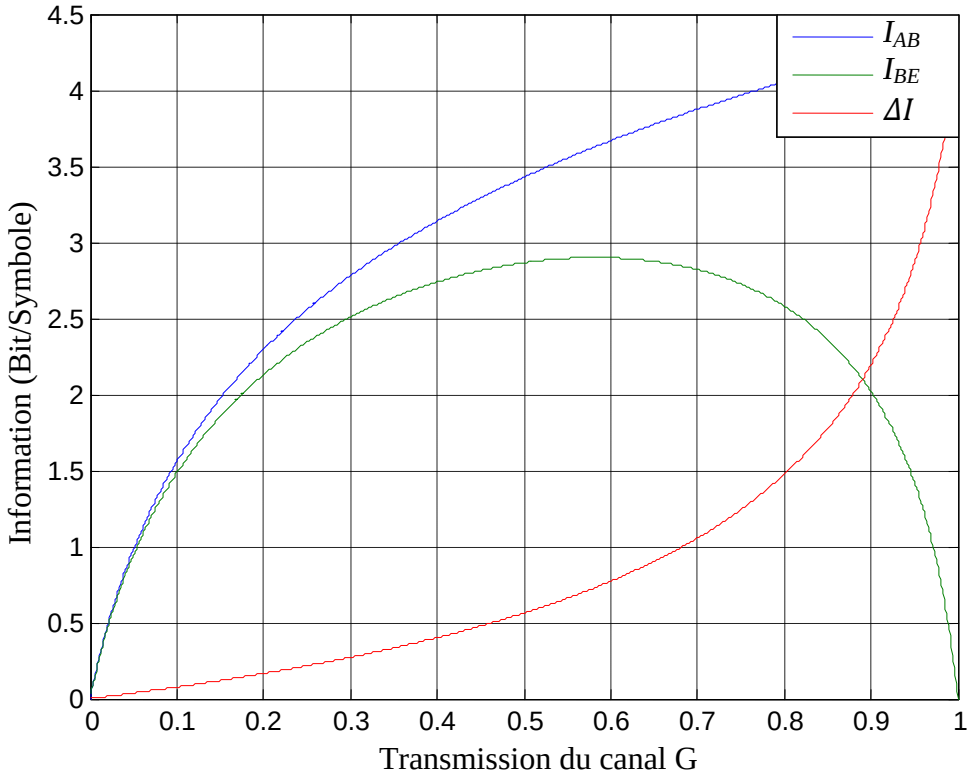

Figure III.5 : Informations mutuelles dans le cas du protocole inverse à détection hétérodyne.

Les courbes homodynes et hétérodynes sont presque identiques. Dans le cas d'une réconciliation directe, la clé secrète est obtenue pour des transmissions du canal supérieur à 1/2. Par contre, pour les protocoles à réconciliation inverse, la clé secrète est obtenue pour toute la transmission du canal G. Le taux de l'information secrète hétérodyne est supérieur au taux de l'information secrète homodyne (presque c'est le double).

III.3.1.1. Influence de la variance et le bruit d'excès sur les détections homodyne et hétérodyne

Le choix de la valeur de l'excès de bruit $\boldsymbol{\varepsilon}$ et de la variance V, n'est pas fait au hasard, mais plutôt après simulation des mêmes équations en faisant varier ces deux paramètres ; le premier de 0 à 1, et le deuxième de 10 à 80. Les résultats sont illustrés sur les figures III.6 et III.7.

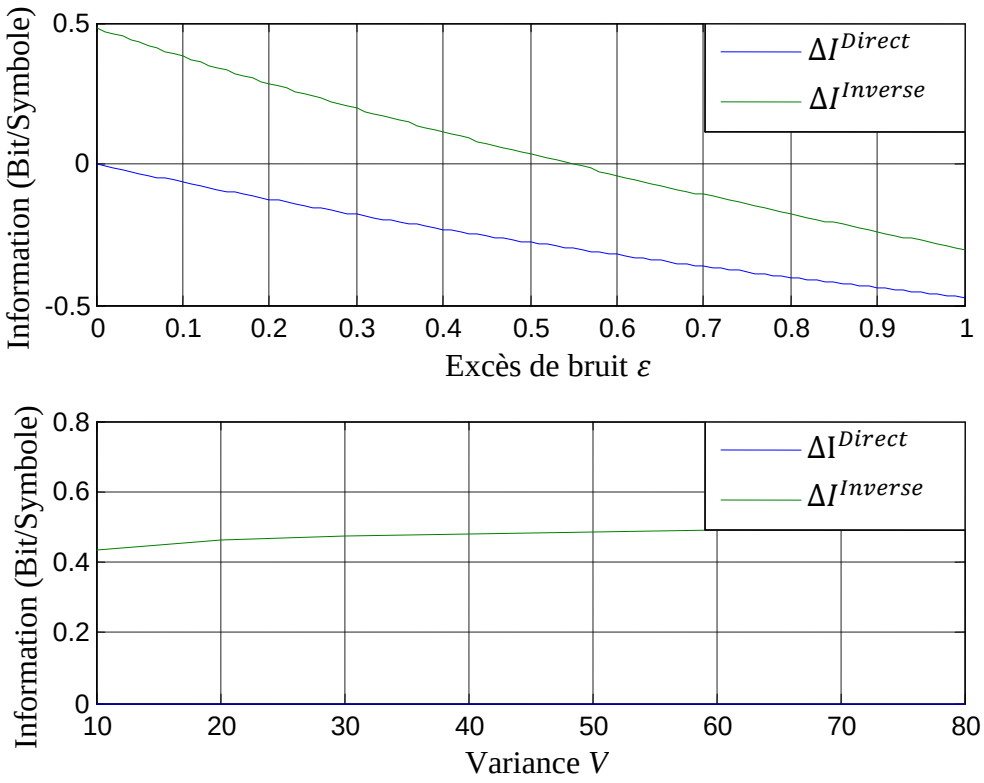

Figure III.6: Influence de la variance et le bruit d'excès sur la détection homodyne.

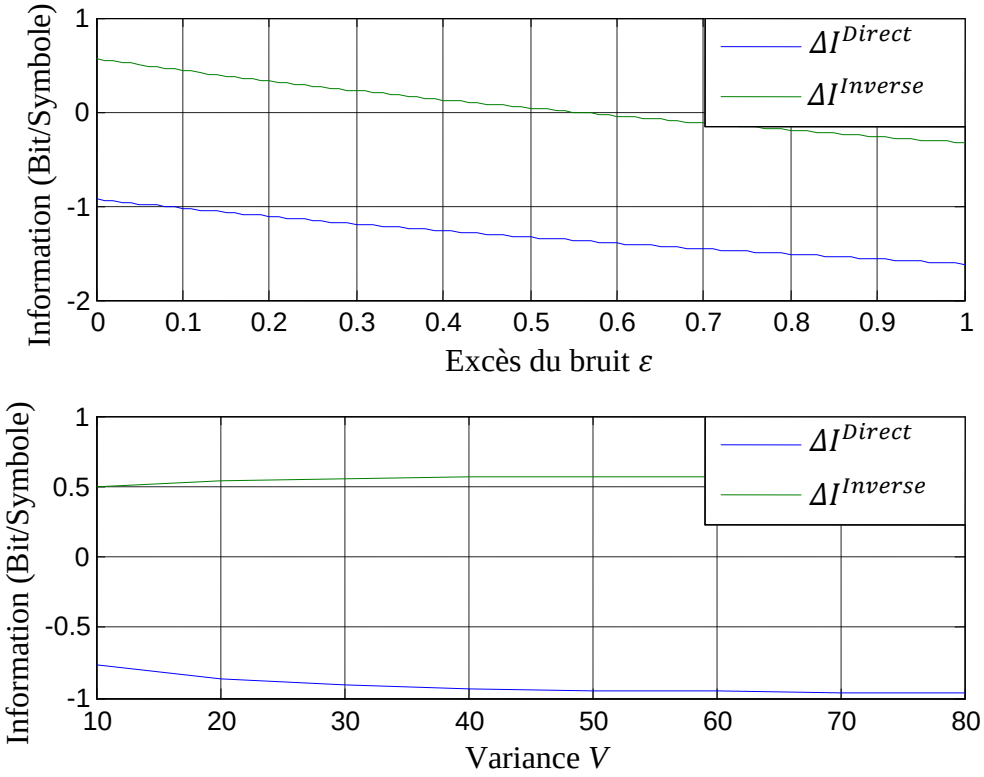

Figure III.7: Influence de la variance et le bruit d'excès sur la détection hétérodyne.

Pour les deux détections, nous voyons que l'excès de bruit ε fait très rapidement chuter l'information secrète ; pour atteindre zéro autour de 0,55 cas du protocole inverse et direct, le

débit maximal de l'information secrète est obtenu pour un excès de bruit nul ; d'où le choix de $\varepsilon = 0$.

La variance *V*, influence négativement sur le protocole direct ; où l'information secrète est nulle pour les différentes valeurs de la variance dans le cas homodyne, et négative (-0,75 bits/symboles) dans le cas hétérodyne. Dans le cas du protocole inverse, l'information secrète reste stable (0,5 bits/symboles) pour toute variation de la variance à partir de 20 pour les deux détections. Donc, on peut prendre n'importe quelle valeur juste qu'elle soit très supérieur à 1.

III.3.1.2. L'information secrète en fonction de la distance

Nous représentons sur la figure III.8, l'évolution du taux de l'information secrète en fonction de la distance.

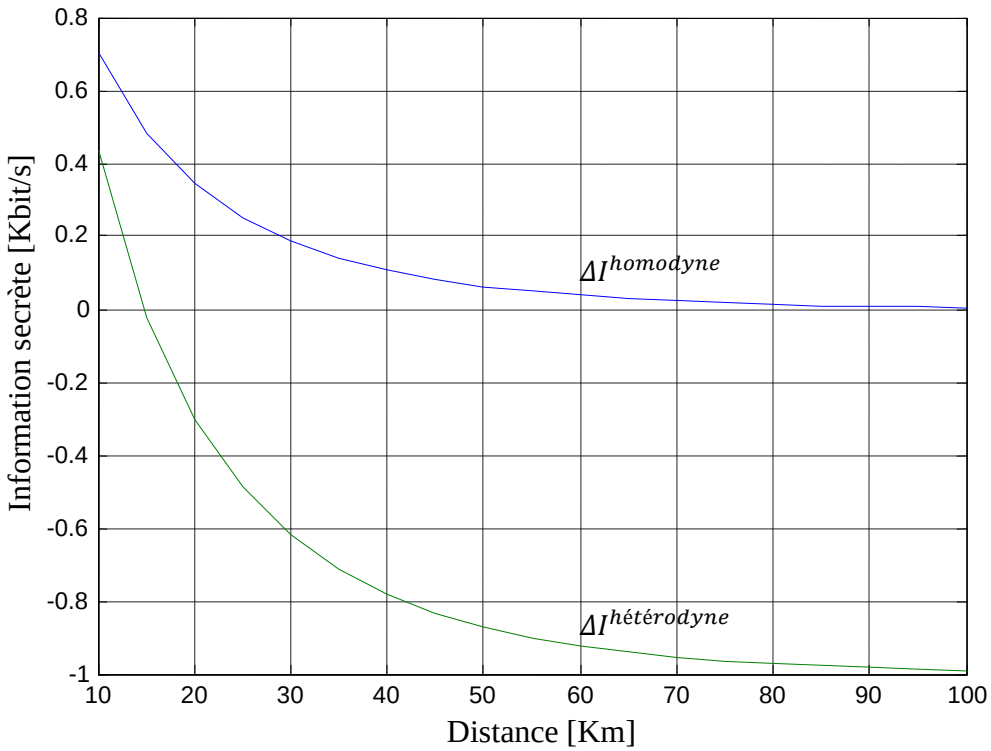

Figure III.8 : Informations secrète en fonction de la distance.

D'après la figure, nous constatons que plus la distance de transmission augmente, plus le taux de la clé secrète diminue. Dans le cas de la détection homodyne, nous obtenons un très haut débit (0.7 Kbit/s) sur une portée de quelques dizaines de km (jusqu'à 30 Km). Par contre, dans le cas de la détection hétérodyne le débit maximal est à 0,4 Kbit/s sur une faible distance (<15 Km), au delà de cette portée, la clé secrète sera perdue.

Nous déduisons alors, qu'en termes de distance, le protocole hétérodyne offre un débit sur une distance plus faible que celle du protocole homodyne.

Durant cette étude, nous avons constaté que le protocole à réconciliation inverse permet d'obtenir un taux de clé secrète supérieur à celui en réconciliation directe. Pour cela, dans ce qui suit, nous allons étudier la sécurité des protocoles CV-QKD contre les attaques individuelles et collectives dans le cas du protocole à réconciliation inverse.

III.3.2.Attaques individuelles

De la même façon que le cas général, nous varions la transmission G de 0 à 1, mais dans ce cas nous prenons la variance modulation $V = 20$, un excès de bruit $\varepsilon = 0.01$, un bruit électronique $v_{el} = 0.01$ et une efficacité de détection $\eta = 1$.

- **La détection homodyne**

Afin de visualiser l'influence de l'attaque individuelle sur la sécurité des protocoles CV-QKD à détection homodyne, nous gardons les mêmes graphes obtenus dans le cas général, et nous introduisons ceux des informations mutuelles entre Alice et Bob, entre Bob et Eve, ainsi que l'information secrète dans le cas de l'attaque individuelle, correspond successivement aux équations (II.39), (II.45), (II.53). Les résultats sont illustrés sur la figure III.9.

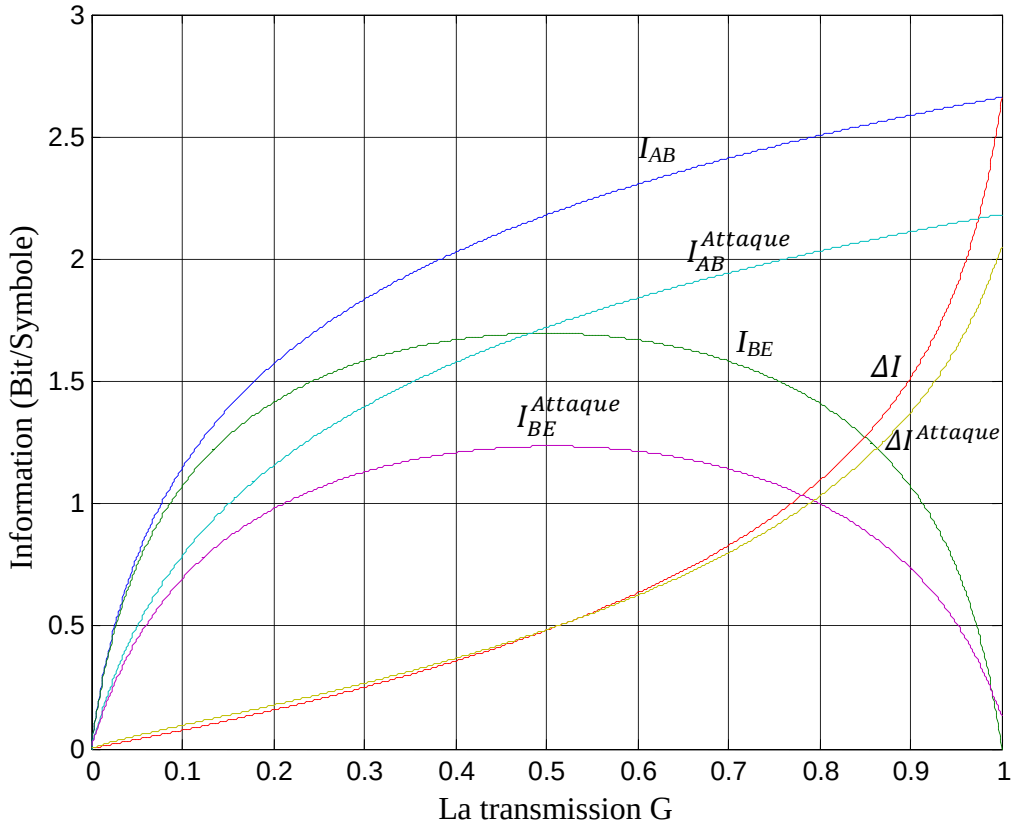

Figure III.9 : Comparaison entre les informations mutuelles dans le cas général et celles dans le cas d'attaques individuelles pour la détection homodyne.

D'après la figure, nous remarquons que le taux de la clé secrète dans le cas de l'attaque individuelle est légèrement inférieur à celui obtenu dans le cas général ; cela veut dire que les attaques individuelles n'ont pas trop d'influence sur les protocoles CV-QKD à détection homodyne.

- **Détection hétérodyne**

De la même manière nous visualisons sur la figure III.10, l'influence de l'attaque individuelle sur la détection hétérodyne. Nous gardons toujours les mêmes courbes hétérodyne du cas général et nous introduisons celles de l'attaque individuelle à détection hétérodyne correspond aux équations (II.47), (II.51), (II.53) attribuent respectivement aux informations mutuelles entre Alice et Bob, Bob et Eve, et l'information secrète, dans le cas de la détection hétérodyne.

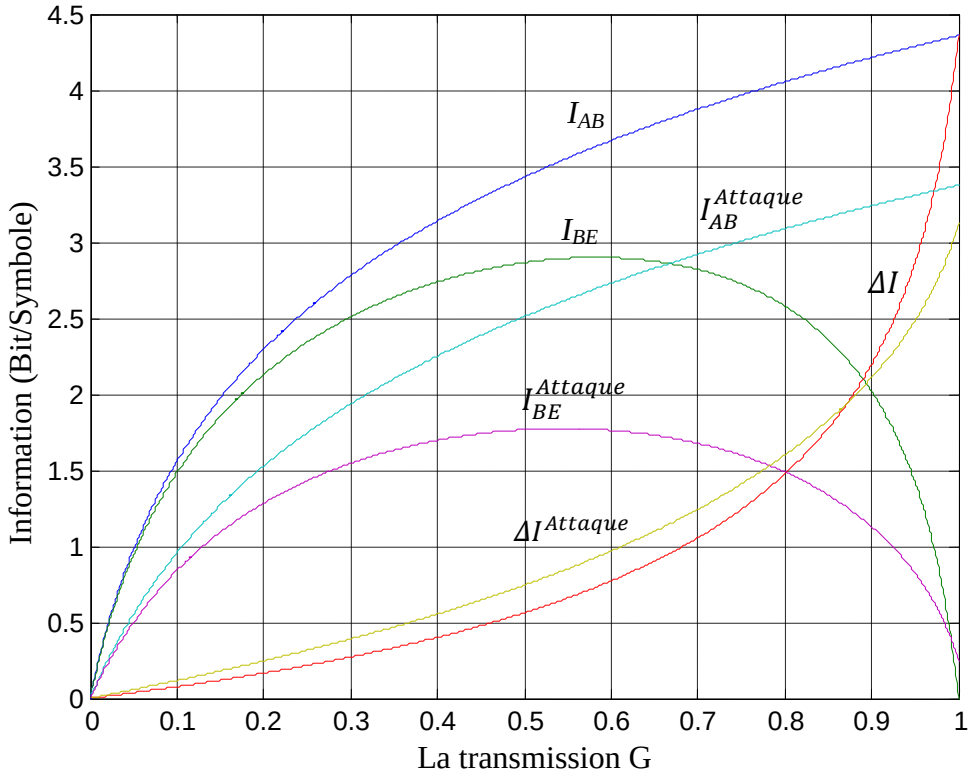

Figure III.10 : Comparaison entre les informations mutuelles dans le cas général et celles dans le cas d'attaques individuelles pour la détection hétérodyne.

Nous remarquons que l'information secrète dans le cas de l'attaque individuelle est supérieur à celle du cas général ($\Delta I^{Attaque} > \Delta I$) pour une transmission qui ne dépasse pas 0,88 ; c'est-à-dire que Eve a acquise plus d'informations que Bob. Au-delà de cette valeur, nous obtenons $\Delta I > \Delta I^{Attaque}$. On conclut, que l'attaque individuelle influence sur la détection hétérodyne pour des valeurs limitées.

III.3.3.Attaques collectives

Nous utilisons les mêmes valeurs de G, V, ε, v_{el} et η prisent dans l'attaque individuelle.

- **Détection homodyne**

En faisant une simulation des équations (II.39), (II.55), (II.64) ; nous obtenons les résultats illustrés sur la figure III.11 qui s'agissent de la comparaison entre les graphes du cas général et ceux obtenues en introduisant une attaque collective dans le cas de la détection homodyne.

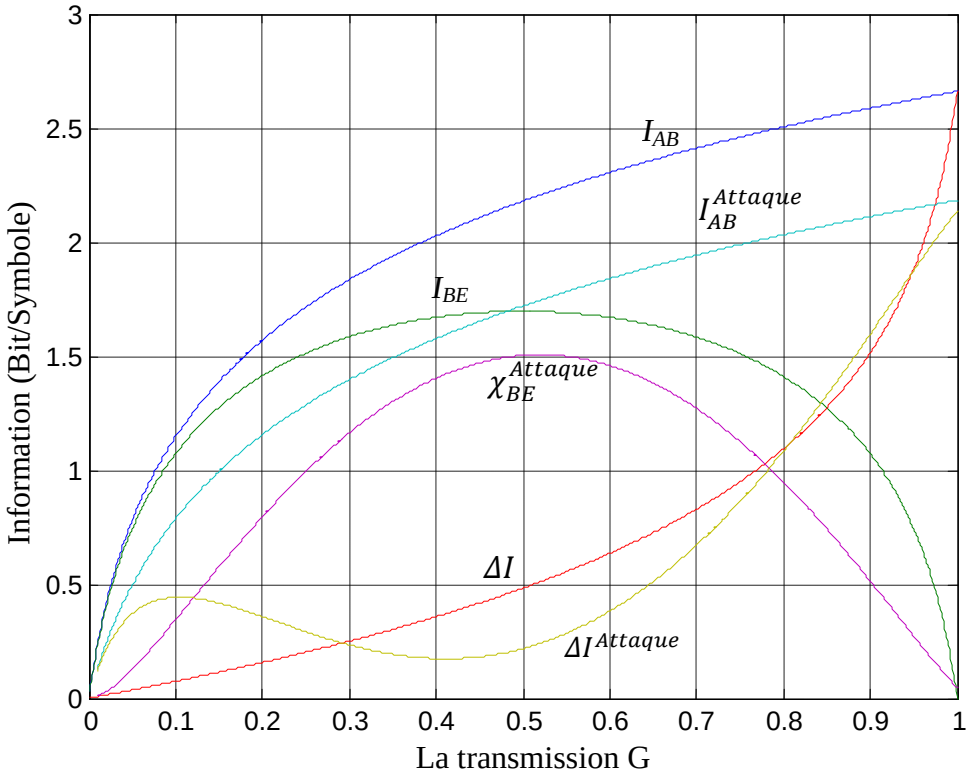

Figure III.11 : Comparaison entre les informations mutuelles dans le cas général et celles dans le cas d'attaques collectives pour la détection homodyne.

La figure montre que l'attaque collective influence sur les protocoles CV-QKD à détection homodyne d'une manière irrégulière pendant toute la transmission du canal G. Ce que veut dire que l'information qu'acquiert Eve est bornée sur des domaines de transmission bien définit.

- **Détection hétérodyne**

La simulation de l'attaque collective dans le cas de la détection hétérodyne avec comparaison au cas général donne les résultats de la figure III.12.

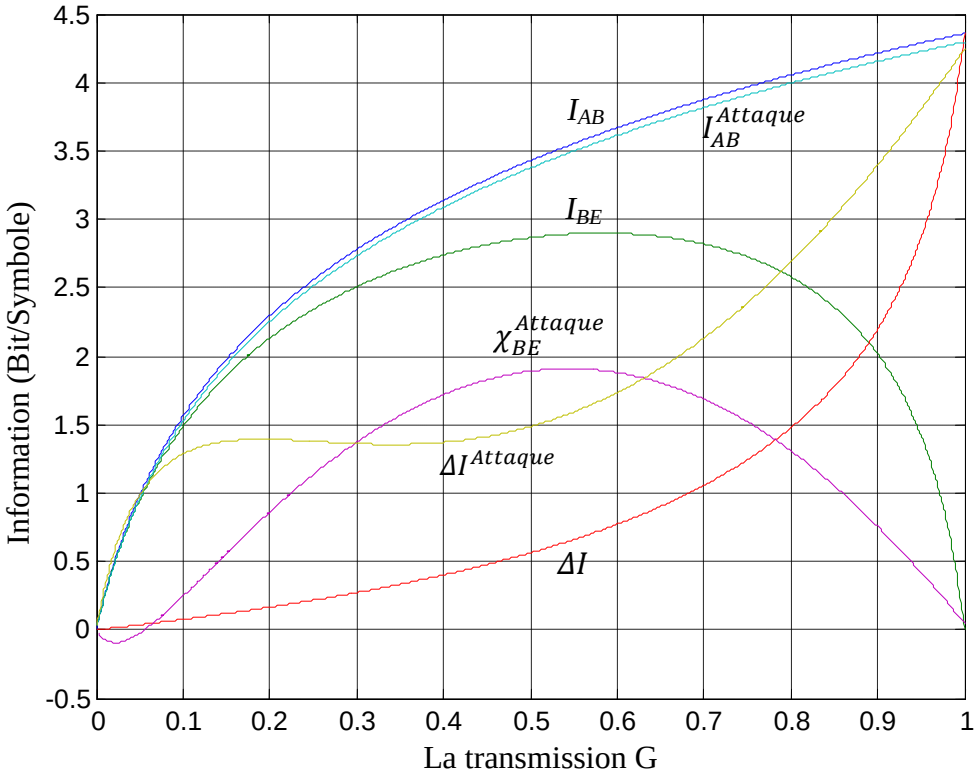

Figure III.12 : Comparaison entre les informations mutuelles dans le cas général et celles dans le cas d'attaques collectives pour la détection hétérodyne.

D'après la figure, nous voyons que $\Delta I^{Attaque} > \Delta I$ pour toute la transmission ; c'est-à-dire qu'Eve intercepte toutes les informations transmise sur le canal. Contrairement au cas homodyne, l'attaque collective influence sur les protocoles CV-QKD à détection hétérodyne pour toute la transmission.

III.4. Conclusion

Ce dernier chapitre présente les résultats de la simulation des protocoles de distribution quantique de clé CV-QKD, ainsi que les différentes attaques menaçant la sécurité de ces protocoles.

À l'issue de cette simulation, nous avons tiré plusieurs conclusions. D'abord, pour améliorer la qualité de la liaison, l'augmentation de la transmission G est fortement recommandée.

Nous avons déduit aussi que l'avantage de la réconciliation inverse par rapport à la réconciliation directe, est que la première offre une clé secrète sur toute la transmission, contrairement à la deuxième qui ne fonctionne qu'à des valeurs de transmission supérieure à

1/2 dans le cas des deux détections. D'autre part, chaque détection a un avantage par rapport à l'autre ; où la détection hétérodyne offre un meilleur débit et la détection homodyne offre une meilleure portée.

Cependant, il existe plusieurs paramètres qui influencent sur ces détections ; le premier paramètre est l'excès de bruit, qui influence négativement, donc dans les meilleurs cas nous l'avons considéré nul. Le deuxième paramètre est la variance. Cette dernière doit être très supérieure à 1, vu qu'elle donne des résultats stables à partir de la valeur 20.

Concernant les attaques, l'attaque collective a trop d'influence sur les protocoles CV-QKD, dont elle offre davantage de pouvoir à Ève.

Conclusion et perspectives

Conclusion et perspectives

Au cours de ce travail, nous avons tenté d'exposer quelques notions de bases de la cryptographie classique. Par la suite nous avons défini les théorèmes fondamentaux de la mécanique quantique ainsi que de la théorie de l'information. Pour mieux comprendre l'information quantique, nous avons introduit les notions nécessaires en présentant les outils mathématiques de base utilisés dans la description des états quantiques, tel que l'entropie de Von Neumann et le Qubit.

En exploitant les conséquences des différents phénomènes quantiques tel que le principe d'incertitude de Heisenberg, le théorème de non-clonage et la notion de l'intrication quantique, nous avons présenté deux dispositifs pour la distribution quantique de clés secrètes. Le premier utilise le codage discret de l'information sur les états de polarisation de photons uniques tel que le protocole BB84. Le second dispositif est basé sur l'encodage de l'information sur des variables continues, à savoir les quadratures d'une impulsion lumineuse.

L'objet de notre travail, c'est de trouver une solution permettant de construire des protocoles de communication sans aucune faille pour la sécurité.

Pour cela, nous nous sommes intéressés particulièrement aux protocoles de distribution quantique de clés à variables continues, où on a défini les protocoles à réconciliation directe et inverse. Ensuite, la détection homodyne et hétérodyne ainsi que leur principe. On a abordé également les différents types d'attaques qui menacent la sécurité de ces protocoles.

La simulation des protocoles à variables continues sous MATLAB, consiste à déterminer leur comportement quand un paramètre varie. Des courbes sont alors générées et analysées. Par conséquent nous avons déduit que le protocole à réconciliation inverse permet d'obtenir une clé secrète pour toute la transmission du canal quantique. Nous avons constaté aussi que la détection hétérodyne nous offre un débit d'information secrète plus haut que celui offert par la détection homodyne. Concernant les attaques, l'attaque individuelle n'influence pas trop sur ces protocoles, contrairement aux attaques collectives qui offrent davantage d'informations à Eve.

En termes de portée, la détection homodyne permet l'obtention d'une clé secrète sur des distances plus longues que celle de l'hétérodyne.

En général, nous avons constaté que les protocoles CV-QKD permettent d'atteindre des très hauts débits, sur une courte distance.

En effet, des recherches avancées sont en cours pour surmonter les difficultés techniques de transmission à longues distances, et cela en améliorant la vitesse et l'efficacité des algorithmes de réconciliation. Et résoudre les lacunes de sécurité introduites par les attaques collectives.

Bibliographie

Bibliographie

[1] Johannes Buchmann, Introduction à la cryptographie, France, Dunod, avril 2006.

[2] Renaud Dumont, Cryptographie et Sécurité informatique, Notes de cours provisoires. Université de Liège, 2009-2010.

[3] Abderrahim El Allati, Etude de cryptographie et de téléportation quantique et proposition de quelques protocoles quantiques, Thèses de doctorat, Université Mohammed V-AGDAL, Rabat, Janvier 2012.

[4] Y. Leroyer et G. Sénizergues, Introduction à l'information quantique, ENSEIRB MATMECA, 2016-2017.

[5] François Damanet, Dynamique quantique dissipative et application à la superradiance, Travail de fin d'études, Université de Liège, 2011-2012.

[6] Benbouya Fahem, Etude et simulation de la Cryptographie Quantique, Mémoire de fin d'études, Université Abderrahmane Mira Bejaia, 2012-2013.

[7] https://www.google.fr/eduscol.education.fr/rnchimie/phys/baillet/06/tp_pola.pdf.

[8] https://crppwww.epfl.ch/physgen4/repository/Notes_02.03.2009.pdf/La fonction d'onde et l'équation de Schrödinger.

[9] Dramix Florence, van den Broek Didier, Wens Vincent, La cryptographie quantique, Printemps des sciences, 2003.

[10] Liran Lerman, La cryptographie quantique, Support de cours, Département "Science Informatique", ULB.

[11] Hwei Hsu, Francis Gottet, Signaux et communication, 2ème édition, Dunod, Paris, 2004.

[12] Sébastien Agnolini, Contribution à l'étude et à la réalisation d'un système de distribution quantique de clef par codage en phase, Thèse de doctorat, Université Pierre et Marie Curie, 23 avril 2007.

[13] Jérôme Lodewyck, 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, décembre 2006.

[14] Raul Garcia-Patron Sanchez, Quantum Information with Optical Continuous Variables, from Bell Tests to Key Distribution, thèse de doctorat, Université libre de Bruxelles, 2007-2008.

[15] Simon Fossier, Mise en œuvre et évaluation de dispositifs de cryptographie quantique à longueur d'onde télécom, Thèse de doctorat, Université Paris-Sud 11, 23 octobre 2009.

[16] Marcin Niemiec, 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, 2011.

[17] Mart Haitjema, A Survey of the Prominent Quantum Key Distribution Protocols, http://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/

[18]Félix Bussiére, Cryptographie quantique à plusieurs participants par multiplexage en longueur d'onde, Thèses de doctorat, Université de Montréal, Octobre 2003.

[19] Nguyen Thanh Mai, Etudier et implémenter une simulation du protocole d'échange de clef quantique BB84, Rapport de stage de fin d'étude, Paris, Mai 2004-Janvier 2005.

[20] Rosa Tualle-Brouri, Dispositifs pour la cryptographie quantique, Mémoire de fin d'études, Université Paris XI, UFR Scientifique D'Orsay, septembre 2006.

[21] Rémi Blandino, Intrication de champ quantique mesoscopique pour les communications quanique, Thèse de doctorat, Université Paris XI, 25 mars 2013.

[22] Mr L. Jacubowiez PRAG, Mrs. J.F. Roch, J.P. Poizat et P. Grangier, Etude des sources de bruit dans un système de détection optique, Centre Universitaire d'Orsay Bat 503.

[23] Didier Robert, La cohérence dans tous ses états, SMF-Gazette-132, avril 2012.

[24] Tianyi Wang et al, Improving the maximum transmission distance of continuous-variable quantum key distribution with noisy coherent states using a noiseless amplifier, Physics Letters A 378 2808–2812, 2014.

[25] Fabian Laudenbach et al, Continuous-Variable Quantum Key Distribution with Gaussian Modulation-The Theory of Practical Implementations, quant-ph arXiv:1703.09278v3, 10 May 2018.

[26] Paul Jouguet, Sécurité et performance de dispositifs de distribution quantique de clés à variables continues, Thèse de doctorat. ParisTec, 18 septembre 2013.

[27] Eli Biham et Tal Mor, Security of Quantum Cryptography against Collective Attacks. Phys. Rev. Lett., vol. 78, Mar 1997.

Résumé

Ce mémoire se porte sur la distribution quantique de clés QKD, qui est une primitive cryptographique qui permet à deux interlocuteurs distants d'établir une clé secrète commune en présence d'un espion. On s'intéresse notamment aux protocoles de distribution quantique de clés à variables continues, où l'information est codée sur les quadratures d'une impulsion lumineuse. L'intérêt majeur de ces protocoles est qu'ils sont faciles à mettre en œuvre, car ils utilisent une simple source laser, comme ils permettent le transfert d'une grande quantité d'informations. La sécurité de ces protocoles repose sur les lois de la mécanique quantique, à savoir le principe d'incertitude de Heisenberg et le théorème de non-clonage. Une étape particulièrement délicate pour les protocoles à variables continues est la réconciliation, durant laquelle les deux extrémités de la communication, utilisent leurs résultats de mesure classiques pour se mettre d'accord sur une chaîne de bits identiques. Nous proposons d'abord un algorithme de réconciliation optimal pour les protocoles étudiés, ainsi que la meilleure détection qui assure plus de sécurité face aux différentes attaques.

Mots clés: cryptographie quantique, QKD, clé secrète, protocole, variables continues, quadratures, réconciliation, Qubits.

Abstract

This memory is about the quantum key distribution QKD that is a primitive cryptographic that allows two distant interlocutors to establish a common secret key in presence of an eavesdropper. We interested notably for the protocols of quantum key distribution with continuous variables, where information is coded on the quadratures of a luminous impulse. The major interest of these protocols is that they are easy to put in work, because they use a simple laser source, as they permit the transfer of a great deal of information. The security of these protocols rests on the laws of the quantum mechanics, to know the principle of uncertainty of Heisenberg and the theorem of no-cloning. A particularly delicate stage for the protocols to continuous variables is the reconciliation, during which the two extremities of the communication, use their results of measure classics to agree on a chain of identical bits. We first propose an optimal reconciliation algorithm for the studied protocols, as well as the best detection that assures more security facing the different attacks.

Keys words: quantum cryptography, QKD, secret key, protocol, continuous variables, quadratures, reconciliation, Qubits.