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 Electrique

Mémoire de fin d'étude pour l'obtention du :

Diplôme Master en Télécommunications

Filière : Télécommunications
Spécialité : Système des Télécommunications

Thème

Distribution quantique de clé à variables continues par la modulation discrète

Présenté par :

M^elle MAKHLOUF Hassina

M^r MOUHOUB A/Rahim

Encadré par :

M^me BOUCHOUCHA Lydia

M^r BERRAH Smail

Membre du jury :

Président : M^r AZNI Mohamed

Examinateur : M^r BENAMIROUCHE Nadir

Année Universitaire : 2019/2020

Remerciements

Nous remercions Dieu tout puissant de nous avoir accordé de la force et de la volonté ainsi que les moyens afin de pouvoir accomplir ce travail.

La réalisation de ce mémoire est indissociable de son contexte familial et scientifique. Nombreux sont ceux qui nous ont soutenus, aidés et supportés.

On remercie notre encadreur "madame Bouchoucha Lydia" pour les efforts qu'elle a fait pour nous encourager le long de la préparation de ce travail.

Aux membres de jury qui nous ont honoré en acceptant le jugement de ce travail.

Abréviations

Alice : Pour designer l'émetteur du message.

Bob : Pour designer le récepteur.

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

DES : Data Encryption Standard.

AES : Advanced Encryption Standard.

RSA : Rivest, Shamir and Adleman.

QKD : Quantum Key Distribution.

CV-QKD : Continuous Variable - Quantum Key Distribution.

QBER : Quantum Bit Error Rate.

SNR : Signal to Noise Ratio.

Liste des figures

Chapitre I

Chapitre II

Chapitre III

Liste des tableaux

Table de matières

Chapitre I : Généralités sur la cryptographie

Chapitre II : Les protocoles de distribution quantique de clés

Chapitre III : Simulations des protocoles CV-QKD

Introduction générale

L'information est un élément constitutif dans tous les domaines. Depuis l'invention de l'écriture, l'humanité exprime le besoin de transmettre leurs informations de manière sécurisée en les rendant inintelligibles pour toute personne étrangère à l'échange, c'est-à-dire que les messages ne peuvent pas être compris par l'ennemi, même s'ils sont interceptés. Ils se servaient donc d'outils permettant de garder leurs confidences hors d'atteinte des yeux indiscrètes. La progression de ces outils primitifs à travers le temps, a permet de concevoir des règles de sécurité plus efficaces et plus logiques qui ont donné naissance à la cryptographie.

La cryptographie propose un ensemble de techniques permettant d'assurer la confidentialité, l'authentification, l'intégrité des données et la non-répudiation de la source de donnée. En effet, la cryptographie a pris un grand développent et est devenue une discipline qui utilise des concepts mathématiques et informatiques pour prouver sa sécurité.

En cryptographie, il est important de représenter les buts de l'ennemi et ses moyens, c'est à dire ce qu'il cherche à faire et la manière dont il agit avec le système. Cependant, face aux différentes exigences de sécurité de la communication, une autre méthode appelée "cryptographie quantique" s'est développé, cette technique est fondée sur une combinaison des concepts de la physique quantique et la théorie de l'information.

Dans notre travail, le but est de faire une étude sur le développement des techniques de la cryptographie quantique, en particulier les techniques à variables continues. En faite, nous nous proposons d'étudier en détail les protocoles directe et inverse dans le cas de la détection homodyne et la détection hétérodyne (modulation gaussienne), et nous avons aussi proposé d'étudier les deux protocoles : trois-états et quatre-états (modulation discrète).

Pour cela nous avons structuré notre travaille comme suit :

Le premier chapitre, nous allons donner un aperçu général sur la cryptographie, ainsi que les principes sur lesquels se basent la cryptographie quantique.

Dans le deuxième chapitre, nous étudierons certains protocoles de bases de la cryptographie quantique, à savoir ceux qui utilisent les variables discrètes ou à variables continues dans la génération d'une clé secrète. En mettant l'accent sur les protocoles CV-QKD à modulation gaussienne et à modulation discrète.

Le troisième chapitre, est divisé en deux parties. La première partie comporte une étude sur les protocoles de distribution quantique de clé à variables continues à modulation

gaussienne, et une deuxième partie consacrée pour les protocoles de distribution quantique de clé à variables continues à modulation discrète.

En termine par une conclusion et des perspectives.

I.1 Introduction

La cryptographie est une partie intégrante de la cryptologie [1], une science au croisement des mathématiques, de l'informatique et de la physique, qui étudie l'ensemble de techniques permettant de chiffrer un message et de le rendre inintelligible sauf pour son destinataire.

Dans ce chapitre, nous décrirons quelques généralités et principes sur la cryptographie, en se basant sur les notions de la mécanique quantique, et la théorie de l'information comme un moyen pour mesurer la sécurité apportée par un système de cryptographie.

Figure I.1 : Terminologies de la cryptographie.

I.2 L'objectif de la cryptographie

Le but fondamental de la cryptographie est de respecter adéquatement les objectifs majeurs de la sécurité suivants :

I.2.1 La confidentialité: elle englobe l'ensemble des dispositions qui assure que l'information reste secrète de toutes les personnes qui ne sont pas autorisées à y accéder [2].

I.2.2 L'intégrité: elle assure que l'information n'a pas été modifiée entre son envoi et sa réception [3].

I.2.3 L'authenticité: elle permet de certifier l'identité de la personne qui envoie le message de façon limiter l'accès aux données [4].

I.2.4 La non-répudiation: elle désigne l'assurance d'une transmission entre deux personnes, que l'expéditeur peut vérifier qu'un certain destinataire a reçu un message particulier [5].

I.3 Cryptographie classique

La cryptographie classique décrit la période avant les ordinateurs. Elle traite des systèmes reposant sur les lettres et les caractères d'une langue naturelle. Le principe c'est de remplacer des caractères par d'autres caractères, et les transposer dans des ordres différents.

I.3.1 Principes de Kerckhoffs

En1883, Auguste Kirchhoff énonça six principes à respecter [6] :

- Le système doit être matériellement, sinon mathématiquement, indéchiffrable.
- Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi.
- La clé doit pouvoir en être communiquée et retenue sans le secours de notes écrites et être chargée ou modifiée au gré des correspondants.
- Il faut qu'il soit applicable à la correspondance télégraphique.
- Il faut qu'il soit portatif et que son maniement n'exige pas le concours de plusieurs personnes.
- Enfin, il est nécessaire vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

I.3.2 Chiffre de César

Le chiffre de César consiste à décaler, dans un message à transmettre, toutes les lettres d'un certain nombre de place [7]. Le destinataire du message doit connaître ce décalage afin de pouvoir déchiffrer le message chiffré.

Exemple :

Si on code le mot "SECRET" à l'aide de la valeur 3 de la clé de César. L'alphabet est décalé de manière à commencer à la lettre D.

Ainsi l'alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Si on décale le début de 3 lettres, on obtient:

DEFGHIJKLMNOPQRSTUVWXYZABC

Où D=A, E=B, F=C, etc.

Avec ce procédé, le texte en claire "SECRET" est crypté en "VHFUHW".

I.4 Faiblesses de la cryptographie classique

La cryptographie classique rencontre des faiblesses malgré toutes les méthodes employées. Tel qu'un faible chiffrement, dans la mesure où il suffit de connaître l'astuce pour pouvoir déchiffrer n'importe quel message, ce qui permet à un espion de conserver le message chiffré en espérant pouvoir un jour le décoder. En plus de ça la durée de vie d'un secret est égale à la durée de vie de la méthode qui sert à la chiffrer.

I.5 Cryptographie moderne

Si la cryptographie classique est d'élaborer des méthodes permettant de transmettre des données de manière confidentielle, la cryptographie moderne s'intéresse en fait plus généralement aux problèmes de sécurité des communications [8]. Pour cela on utilise un certain nombre de mécanismes basés sur des algorithmes cryptographiques [9].

Les techniques de la cryptographie moderne se composent de grandes parties comme le montre la figure I.2 :

- La cryptographie symétrique (cryptographie à clé secrète).
- La cryptographie asymétrique (cryptographie à clé publique).

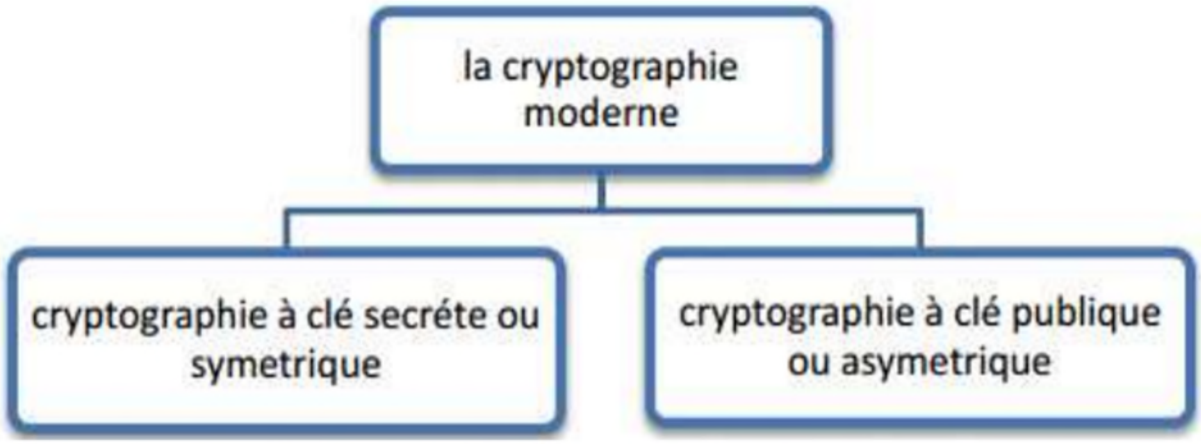

Figure I.2 : Les méthodes de la cryptographie moderne [10].

I.5.1 Cryptographie symétrique

En cryptographie symétrique aussi appelée cryptage à clé secrète, une seule clé suffit pour le cryptage. La clé de chiffrement peut être calculée à partir de la clé de déchiffrement et vice versa. En générale, les clés de chiffrement et de déchiffrement sont identique, l'émetteur et le destinataire doivent se mettre d'accord préalablement sur une clé qui doit être gardée secrète, car la sécurité d'un tel algorithme repose sur cette clé.

Les algorithmes les plus connus des systèmes cryptographiques symétriques sont:

- **DES (Data Encryption Standard):** La norme DES est adoptée par NSA en 1967. C'est un algorithme de chiffrement par bloc, il consiste à chiffrer un bloc de texte de 64 bits pour produire un cryptogramme de 64 bits a partir d'une clé de 56 bits [1].
- **AES (Advanced Encryption Standard):** L'AES est un algorithme de chiffrement par bloc utilisant des clés de 128, 192 ou 256 bits.

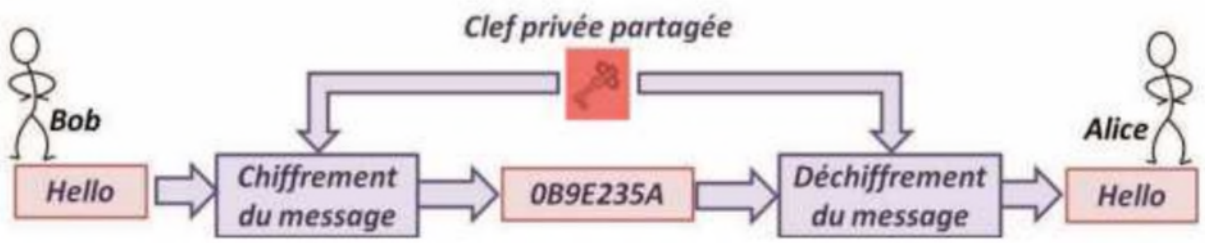

Figure I.3 : Cryptographie symétrique.

I.5.2 Cryptographie asymétrique

La cryptographie à clé publique (asymétrique) consiste en l'existence d'une paire de clés de chaque côté (émetteur et récepteur) liées mathématiquement. Chaque paire est composée d'une clé privée (et différente pour chaque utilisateur qui doit être gardée secrète), et d'une clé publique connu par tous les utilisateurs [11][09][12].

L'algorithme le plus connu des systèmes cryptographiques asymétriques est :

- **RSA** (d'après le nom des ses inventeurs, Ron Rivest, Adi Shamir et Leonard Adleman).

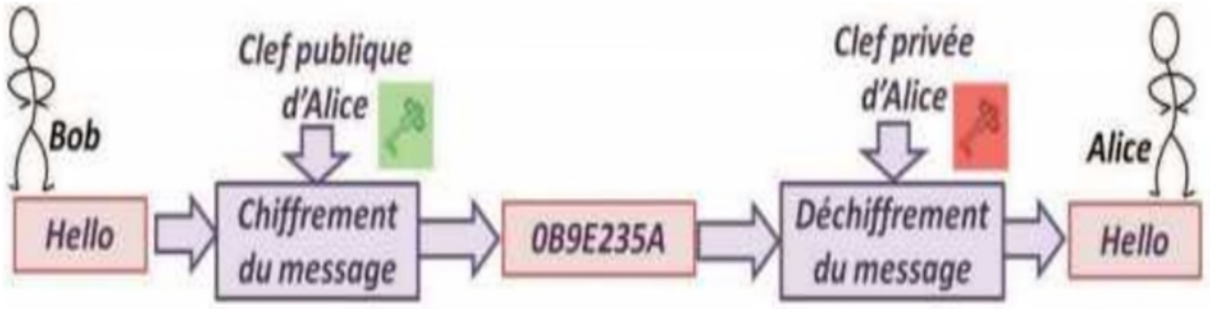

Figure I.4 : Cryptographie asymétrique.

I.6 Avantages et inconvénients de la cryptographie privée et publique

Cryptographie	Avantages	Inconvénients
Privée	-Clés relativement courtes (128 ou 256 bits). -Primitive de mécanismes cryptographiques et bonne performances et sécurité bien étudié. -Assure la confidentialité des données.	-Gestion des clés difficiles (nombreux clés). -Point faible de N entités susceptibles de communiquer secrètement il faut distribuer N*(N-1)/2 clés.
Publique	-Pas de secret à transmettre. -Nombre de clés à distribuer est réduit par rapport aux clés symétriques (privées). -Très utile pour échanger des messages facilement. -La distribution est simplifiée: la clé privée n'est jamais révélée ou transmise et la clé publique est disponible à tous les utilisateurs.	-Les algorithmes à clé publique nécessitent une capacité de traitement importante, ce qui n'est pas raisonnable pour les systèmes à ressources limitées. -La relation clés publique/clés privée impose: 1. La taille de clés et relativement longue. 2. Lenteur de canal.

Table I.1: Les avantages et inconvénients de la cryptographie privée et publique [13] [14] [15].

I.7 La cryptographie quantique

La cryptographie quantique est structurée sur une belle combinaison des concepts de la physique quantique et la théorie de l'information dans le sens qu'elle applique les principes de la mécanique sans autre moyen technologique [16]. Elle ne permet pas directement la communication des messages intelligible, mais autorise la distribution de clé cryptographique, elle apparaît donc comme un complément de la cryptographie classique.

I.8 La mécanique quantique

La mécanique quantique donne la structure mathématique appropriée pour décrire un système physique. À un système quantique est associé un espace vectoriel complexe muni d'un produit scalaire : espace de Hilbert.

I.8.1 Equation de Schrödinger

Tout système quantique évolue dans le temps sous l'influence d'interactions entre lui et l'environnement. Cette évolution peut être représentée par une équation différentielle linéaire qui s'appelle l'équation de Schrödinger.

Tout d'abord, on considère le cas particulier d'une onde harmonique (localement) plane, ce qui s'écrit en notations complexes :

$$\Psi (r, t) = \Psi_0 \, e^{i(k.r-wt)} \tag{1.1}$$

Puis, utilisant les relations proposées par Broglie :

$$\Psi (r, t) = \Psi_0 \, e^{i/\hbar(p.r-Et)} \tag{1.2}$$

On remarque alors, qu'en dérivant l'onde par rapport au temps, on obtient :

$$\frac{\partial}{\partial t} \Psi (r, t) = - \frac{i}{\hbar} E\Psi_0 e^{i/\hbar(p.r-Et)} = - \frac{i}{\hbar} E\Psi (r, t) \tag{1.3}$$

De même, le gradient de cette fonction d'onde donne :

$$\nabla\Psi (r, t) = \frac{i}{\hbar} p\Psi (r, t) \tag{1.4}$$

Nous avons donc, pour toute onde Ψ de cette forme, en tout point et à tout instant :

$$i \hbar \frac{\partial}{\partial t}\Psi = E\Psi \tag{1.5}$$

$$- i \hbar \nabla \Psi = p\Psi \tag{1.6}$$

Pour une particule donnée, d'après la mécanique classique, l'énergie mécanique est donnée par :

$$E = E_c + E_p = 1/2 \, mv^2 + V(r) = p^2/2m + V(r) \tag{1.7}$$

Cette quantité apparaît en fait plus naturellement dans la formulation hamiltonienne de la mécanique classique : la somme de l'énergie potentielle et de l'énergie cinétique est appelée hamiltonien, qui s'identifie ici à l'énergie mécanique totale. En multipliant par la fonction d'onde :

$$p^2/2m\Psi + V\Psi = E\Psi \tag{1.8}$$

Et enfin en utilisant les résultats précédents, nous avons :

$$\frac{(-i\hbar\nabla)2}{2m}\Psi + V\Psi = i\hbar \frac{\partial}{\partial t}\Psi \tag{1.9}$$

Ce que l'on peut écrire sous l'une ou l'autre des deux formulations suivantes :

Toute fonction d'onde Ψ vérifie, à tout instant et en tout point :

$$- \hbar^2/2m \, \Delta\Psi(r, t) + V(r) \, \Psi (r, t) = i\hbar \frac{\partial\Psi(r,t)}{\partial t} \tag{1.10}$$

C'est à dire :

$$H\Psi = E\Psi \tag{1.11}$$

Où la quantité H est appelée opérateur hamiltonien.

I.8.2 Principe d'incertitude de Heisenberg

Le principe d'incertitude de Heisenberg a été énoncé en 1926. Son principe montre qu'il est impossible de mesurer simultanément, avec une précision absolue, la position et la vitesse d'une particule dans le domaine de l'atome. En effet de l'analyse de fourier, quelle que soit la fonction d'onde, on a les inégalités [17] :

$\Delta_x \Delta p_x \geq \frac{h}{2}$ $\Delta_y \Delta p_y \geq \frac{h}{2}$ $\Delta_z \Delta p_z \geq \frac{h}{2}$ avec $h = 6.626*10^{-34}$ Js (1.12)

Où les Δ_x Δ_y Δ_z et Δp_x Δp_y Δp_z représentent les incertitudes sur la position de l'impulsion.

I.8.3 Théorème non-clonage

Le non-clonage est basé sur le principe d'incertitude, il n'existe aucune façon de connaître 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 quantum. En effet, W. K. Wooters et W. H. Zurek ont démontré ce procédé, en supposons qu'on peut cloner un qubit de l'état |a> dans un seconde qubit de l'état |0>. Soit U une transformation unitaire de clonage :

$$U|a>|0> = |a>|a> \qquad \forall |a> \tag{1.13}$$

Soient |a> et |b> deux états quantiques orthogonaux, tels que :

$$U|a>|0> = |a>|a> \quad , \quad U|b>|0> = |b>|b> \tag{1.14}$$

On considère un autre état |c> tel que :

$$|c> = \frac{1}{\sqrt{2}}(|a> + |b>) \tag{1.15}$$

L'utilisation de la linéarité de l'opérateur unitaire et le clonage des états donne une part :

$$U|c>|0> = \frac{1}{\sqrt{2}}(|a> \otimes |a> + |b> \otimes |b>) \tag{1.16}$$

Et d'autre part :

$$U|c>|0> = |c>|c> \tag{1.17}$$

Or :

$$\frac{1}{\sqrt{2}}(|a> \otimes |a> + |b> \otimes |b>) \neq \frac{1}{\sqrt{2}}(|aa> \otimes |ab> + |ba> \otimes |bb>) \tag{1.18}$$

L'inégalité est une conséquence de la linéarité des opérateurs, il est donc impossible de cloner un état quantique arbitraire. Par exemple, le théorème affirme que pour un qubit dans un état $|\phi> = \alpha|0> + \beta|1>$, on ne peut pas produire l'état $|\phi>|\phi>$ sans connaître les valeurs de α et β.

I.9 La théorie de l'information

La théorie de l'information définit le concept d'information et sa description mathématique. De ce fait il est désormais possible de connaître de manière quantitative une information ainsi que les dégradations qu'elle peut subir. Elle explique comment compresser au maximum l'information et la transmettre de façon à réduire au maximum le taux d'erreur

sur un canal bruité. Les données sont modélisées comme des processus aléatoires et les canaux de transmission comme des termes probabilistes [18]. La signification des données n'est pas étudiée par cette théorie [18], seule la probabilité d'apparition d'une donnée l'est.

I.9.1 Entropie de Shannon H (X)

L'entropie de Shannon a plusieurs significations, tel qu'elle représente 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, etc...

Certains messages peuvent voir une probabilité d'apparition différente. Ainsi, les messages avec une forte probabilité devront être codés sur un nombre petit de bits, alors que ceux qui ont une faible probabilité pourront être codés sur un nombre de bits plus conséquent. Grâce 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 pouvant valoir un ensemble de messages différents se trouvant dans l'ensemble χ vaut [18] :

$$H(\chi) = -\sum_{x\in\chi} p(x) * \log\big(p(x)\big)\ bits \qquad (1.19)$$

- Où p(x) représente la probabilité d'avoir la valeur x.
- L'entropie sera toujours ≥ 0.

I.9.2 Entropie conditionnelle de Shannon H (X|Y)

Supposons que Y représente la version de X avec une certaine modification due à un bruit. L'entropie conditionnelle H (X|Y) est la valeur moyenne de l'incertitude sur X sachant que Y est connu.

$$H(X|Y) = H(X,Y) - H(Y) \qquad (1.20)$$

Si X et Y sont indépendants, alors H (X|Y) = H (X). Inversement, si X est totalement déterminé par Y, alors H (X|Y) = 0.

I.9.3 Entropie conjointe de Shannon H (X,Y)

Représentons (X,Y) comme une paire de variables aléatoire dont la distribution de probabilité vaut p (x,y).

$$H(X,Y) = H(X) + H(Y|X) = H(Y) + H(X|Y) \qquad (1.21)$$

I.9.4 Information mutuelle

L'information émise par la source est représentée par X et L'information reçue 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 entropie mutuelle) est définie par :

$$I(X;Y) = H(X) + H(Y) - H(X,Y) = I(Y;X) \quad (1.22)$$

Ce qui se peut se ramener à :

$$I(X;Y) = H(X) - H(X|Y) \quad (1.23)$$

I.10 Limites de la cryptographie quantique

L'application de la physique quantique à la cryptographie est actuellement limitée à l'échange de clés cryptographiques. Comme il est encore techniquement difficile de générer et d'isoler un photon. Il existe toujours une probabilité d'avoir deux photons ou plus envoyé à la destination, ce qui pose un problème puisque la fiabilité d'une transmission quantique est basée sur la propriété du non clonage d'un photon [19]. De plus, du point de vue des performances, le débit d'échange demeure inférieur au mégabit par seconde [19].

I.11 Conclusion

Dans ce chapitre, nous avons définit la cryptographie ainsi son objectif. En suite, nous avons présenté le cas de la cryptographie classique, cryptographie moderne où nous avons cité ces deux types (clé secrète et clé publique). En suite, nous avons parlé sur la cryptographie quantique et ces notions de bases (mécanique quantique et théorie d'information).

II.1 Introduction

La distribution quantique de clé (en anglais "QKD" qui signifier Quantum Key Distribution), représente la première application pratique de l'information quantique. Elle permet à deux parties distantes de communiquer avec intimité absolue, même en présence d'une écoute indiscrète.

Aujourd'hui deux familles de protocoles de distribution quantique de clé coexistent, et que nous allons d'écrire ci-dessous à savoir les protocoles à variables continues et les protocoles à variables discrètes.

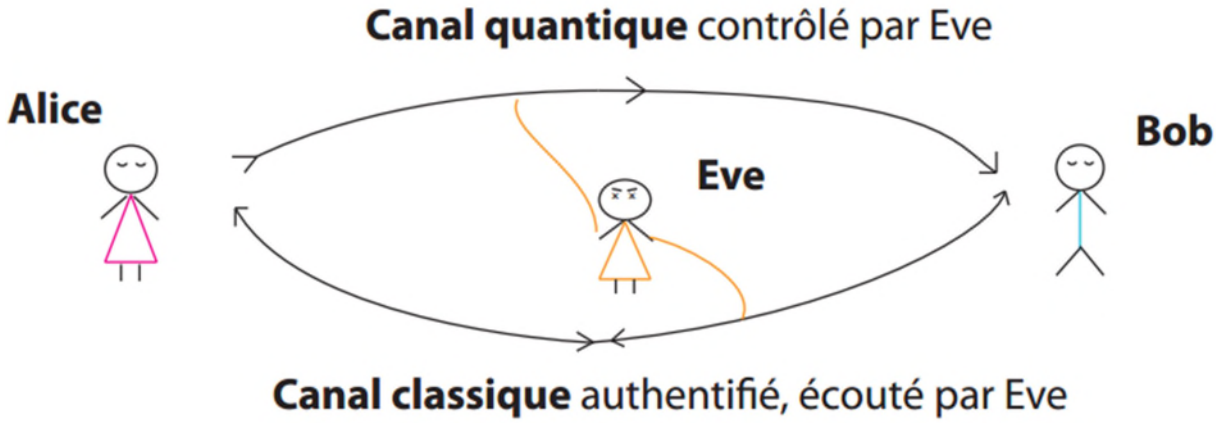

Figure II.1 : Schéma générale d'un système de distribution quantique de clé.

II.2 Etapes d'un protocole de distribution quantique de clé

Un protocole QKD, est un ensemble de programmes susceptibles de communiquer sur le réseau afin de réaliser une certaine fonctionnalité, toute en suivant les étapes suivantes [20]:

II.2.1 Communication quantique : Alice et Bob échangent des états quantiques à travers le canal quantique et effectuer des mesures sur ces états.

II.2.2 Estimation des paramètres : Alice et Bob annoncent au hasard un sous-ensemble sélectionnés dans leurs données. Ils peuvent non seulement estimer la quantité d'information échangée restante, mais aussi évaluer indirectement la quantité maximum d'information interceptée par l'espion. Cette évaluation est possible grâce à la nature quantique des états transmis, qui limite la quantité d'information accessible simultanément à Alice, Eve et Bob.

II.2.3 Correction d'erreurs : Alice et Bob modifier les informations publiques sur une chaine classique authentifiée et se mettre d'accord sur une chaine de bits commune. Cette étape augmente la quantité d'information de l'écoute clandestine. Alice et Bob peuvent abandonner le protocole à ce stade, si la quantité totale d'informations de l'écoute clandestine après toutes les étapes précédentes est supérieure à la taille de la chaine de bits commune.

II.2.4 Amplification de la confidentialité : Alice et Bob extraient de leur chaine de bit commune une chaine de bits plus courte au sujet de laquelle l'écouteur connaît un van-quantique d'informations. cela se fait en appliquant un hachage fonction à leur chaine de bits commune.

II.3 Les protocoles à variables discrètes

Les protocoles avec des variables discrètes offrent en générale de meilleures performances, car ils sont moins sensibles au bruit. Ils encodent l'information dans des variables discrètes comme la phase ou la polarisation de photons uniques.

II.3.1 Les protocoles à photons uniques

Le protocole BB84, est un schéma de distribution de clé quantique développé par Charles Bennett et Gilles Brassard en 1984 [21][22]. Il s'agit d'une méthode standard pour nommer un protocole, dans la pratique l'information est codée via la polarisation des photons, en utilisant deux bases conjuguées, qui sont la base de rectilinéaire $B_+ = \{|0_+>, |1_+>\}$, et la base circulaire (ou diagonale) $B_x = \{|0_x>, |1_x>\}$. En fonction des états |0> et |1>, les états de B_+ et B_x s'écrivent comme suit [23]:

$$|0_+> = |0> \quad (2.1)$$

$$|1_+> = |1> \quad (2.2)$$

$$|0_x> = \frac{1}{\sqrt{2}}(|0> + |1>) \quad (2.3)$$

$$|1_x> = \frac{1}{\sqrt{2}}(|0> - |1>) \quad (2.4)$$

Le but du protocole est de fournir à deux utilisateurs autorisés, Alice et Bob une clé secrète. En outre, la mise en œuvre du protocole nécessite deux canaux, un canal de transmission quantique et un canal public. Les détails du protocole sont donnés comme suit [23]:

- Alice génère des états de polarisation ou qubits de façon aléatoire, puis elle envoie une suite de photons polarisées à Bob par un canal quantique.
- Bob reçoit les photons d'Alice et chacun décide, indépendamment de l'autre, d'effectuer une mesurer sur les polarisations avec une probabilité 1/2, suivant la base B_+ ou Bx.
- Alice et Bob comparent leurs bases en utilisant un canal de communication classique, puis ils rejettent tous les cas où Bob n'a pas fait le bon choix comme Alice. Cette opération est connue sous le nom de la réconciliation des bases.

- Si le test de comparaison montre qu'il y a eu la présence évidente de l'espion, ils rejettent les données échangées et reviennent à la première étape. Sinon, ils conservent les données de l'étape 4. Ces données construisent la clé secrète qui n'est pas connue que par Alice et Bob.
- En fin de communication, il y a toujours des erreurs qui sont introduites par le canal quantique et peut être par Eve. Ainsi, Alice et Bob utilisent des techniques classiques pour augmenter la sécurité et corriger ces erreurs. Ces techniques sont l'amplification de confidentialité (fonction de hachage) et code correcteur (redondance).

II.3.2 Les protocoles à photons intriqués

Il s'agit d'un protocole inventé par Ekert en 1991 [24]. L'idée est de partager des particules ou photons intriqués $|\phi^+>$ pour générer à distance des mesures corrélés entre Alice et Bob. En revanche, il est difficile à réaliser en pratique à grande distance. L'intrication d'un 2-qubit est très sensible aux interactions avec l'environnement. Il s'agit du phénomène de décohérence. Alice prépare un grand nombre N de 2-qubits tous dans le même état [23]:

$$|\phi^+> = \frac{1}{\sqrt{2}} (|00> + |11>) \qquad (2.5)$$

Ces états, dites intriqués, ont la propriété qu'on ne peut pas les séparer. pour avoir $|00>$ comme résultat de mesure la probabilité est 1/2. Il en est de même pour le qubit $|11>$. On peut dire que les résultats de mesure sont corrélés.

II.4 Les protocoles à variables continues

Récemment, plusieurs types de protocoles sont utilisés pour coder l'information. Des communications exploitent le degré de liberté de l'espace de phase, remplaçant la sphère de Bloch d'un système à deux niveaux, connus sous le nom de variable continue CV. Les variables continues quantiques ont émergé comme un nouvel outil pour développer de nouveaux protocoles quantiques. Pour cette raison, il y a deux types d'états continus [23]:

- Les états cohérents $|\alpha>$, qui sont des états à incertitude minimale autour de leur moyenne, avec $\alpha \in C$.
- Les états comprimés qui peuvent être choisis pour avoir une stratégie bien définie sur les quadratures.

II.4.1 La réconciliation

Cet algorithme permet de réduire la quantité d'information qu'Eve a obtenue. Il sert à supprimer les bruits dus au canal de communication, ainsi ceux causés par les appareils de mesure ou par Eve.

La réconciliation s'exprime en deux façons :

II.4.1.1 Réconciliation directe

Alice envoie des données de correction à Bob, qui corrige ses erreurs pour avoir les mêmes valeurs qu'Alice [25]. Cette technique ne fonctionne plus dès lors que la transmission du canal quantique est inférieure à 50% (pertes > 3 dB) [25]. Dans ce cas, l'espion pourrait théoriquement accéder à plus de la moitié du faisceau émis par Alice et donc extraire davantage d'information que Bob, ce qui interdit toute communication sécurisée.

II.4.1.2 Réconciliation inverse

Dans cette technique, le flux d'information de correction est inversé par rapport à la direction du flux d'information quantique. Dans ce cas, Bob envoie des données de correction à Alice, qui modifie ses valeurs pour obtenir les même que Bob. D'une certaine manière, Alice va copier les erreurs mesurées par Bob.

II.4.2 La détection

II.4.2.1 Détection Homodyne

Dans ce cas Alice envoie à Bob les états cohérents X et P. Bob reçoit ces états puis effectue ses mesures en utilisant la détection homodyne, où le signal est mélangé avec un oscillateur à une lame séparatrice équilibrée. Selon le protocole, Bob mesure une seule composante en quadrature en sélectionnant au hasard entre $\theta = 0$ et $\theta = \pi/2$ pour chaque mode entrant [26].

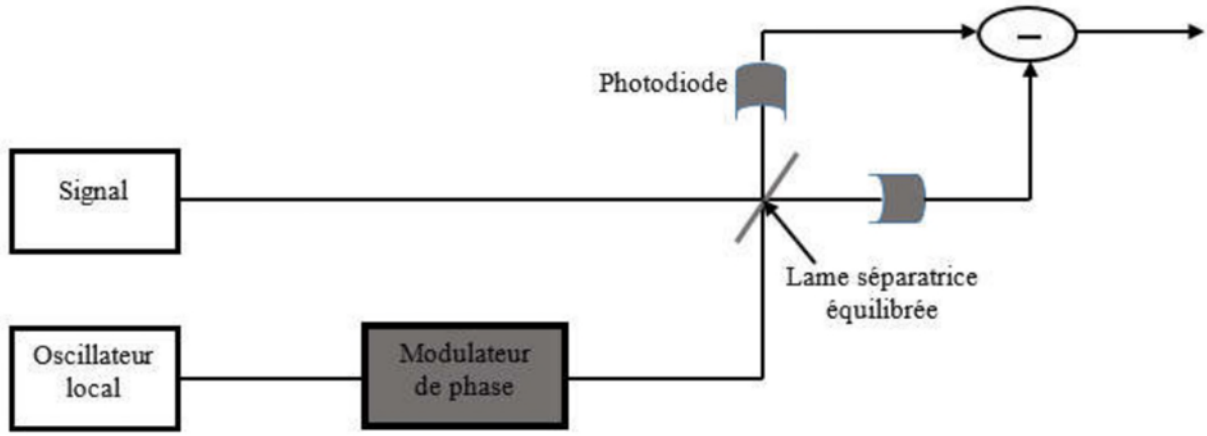

Figure II.2 : Schéma bloc d'une détection Homodyne [26].

II.4.2.2 Détection Hétérodyne

Alice envoie à Bob une suite d'états cohérents modulés dans le plan complexe avec une variance V_A. Ce signal est modifié par la transmission G et le bruit ajouté ramené à

l'entrée χ du canal quantique. Après réception, Bob divise le faisceau en deux parties et mesure respectivement les quadratures X et P sur chacune des voies [27].

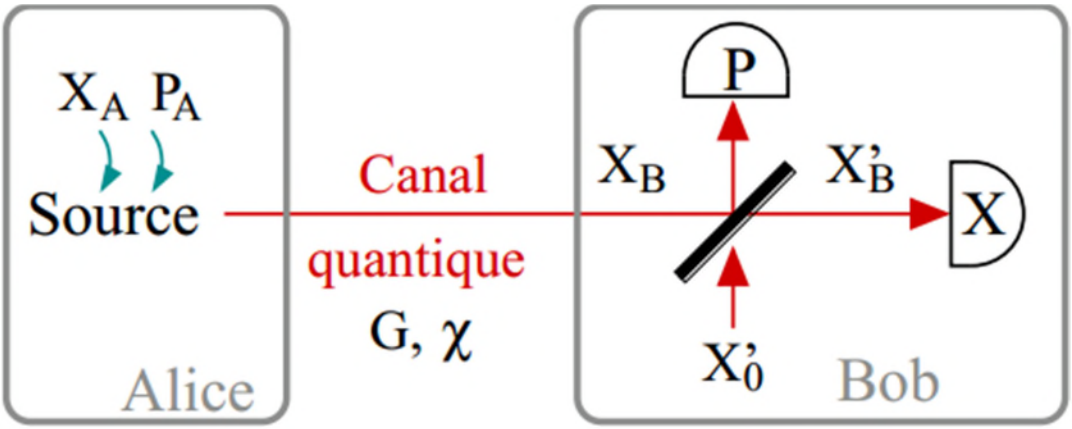

Figure II.3 : Représentation d'une détection Hétérodyne.

II.5 Les protocoles CV-QKD à modulation gaussienne

La modulation gaussienne modélise la transmission quantique des variables continues entre Alice et Bob. Elle exprime les perturbations subies par un état cohérent envoyé par Alice dans un canal ajoutant un bruit gaussien. Dans ce qui suit, nous notons (X_A, P_A) la valeur classique de la modulation choisie par Alice. Les opérateurs quantiques de l'état sortant du dispositif d'Alice s'expriment donc :

$$X = X_A + X_0 \quad (2.6)$$

$$P = P_A + P_0 \quad (2.7)$$

Où X_0 et P_0 représentent les quadratures du bruit de photon de variance N_0 associé à l'état cohérent.

L'état quantique mesuré par Bob est modifié par le canal quantique éventuellement contrôlé par l'espion, et par les imperfections de la détection de Bob. On écrit alors la quadrature X_B mesurée par Bob :

$$X_B = g\,(X + X_{CB}) = g\,(X_A + X_0 + X_{CB}) \equiv g\,(X_A + X_N) \quad (2.8)$$

Où X_{CB} est le bruit gaussien, $G = g^2 = T\eta \leq 1$ est la transmission totale en intensité entre Alice et Bob, produit de la transmission T du canal quantique et de l'efficacité η de la détection de Bob, et X_N le bruit ramené à l'entrée.

II.6 Les protocoles CV-QKD à modulation discrète

Récemment, de nouveaux protocoles utilisant une modulation discrète ont été développés et expérimentalement mis en œuvre. La modulation discrète est plus robuste

contre l'excès de bruit, et elle peut réaliser la tâche de distribuer des clés secrètes sur longue distance. Dans ce cadre on site:

II.6.1 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 clef, il est nécessaire d'échanger plus d'autre information pour le secret de la clef [28]. Le protocole à trois-états a proposé d'employer trois états, au lieu de quatre dans BB84, et trois détecteurs, au lieu de deux pour BB84, pour casser la symétrie de BB84. Ceci réduit la probabilité d'espionnage pour obtenir de bon états, et ainsi que minimise la quantité de l'information utile envoyée par Alice. D'ailleurs, nous pouvons également découvrir sa présence sur la ligne.

II.6.2 Protocole à six-états

Un protocole à six-états 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 la même base est (à) seulement 1/3 [28], 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'erreur QBER. Si l'espion mesure tous les photons, le QBER est 33%, en comparaison à 25% dans le cas du protocole BB84 [28].

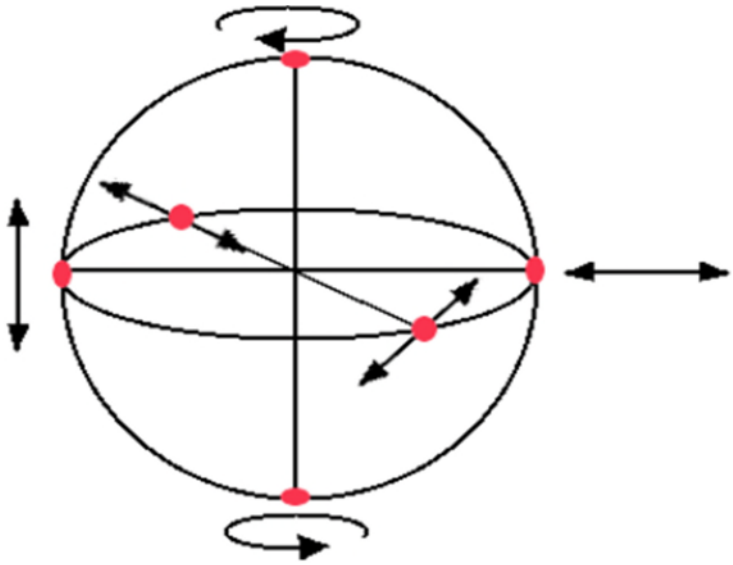

Figure II.4 : Trois paires de bases utilisées dans le protocole à six-états.

II.7 Conclusion

Dans ce chapitre, nous avons présenté quelques protocoles de distribution quantique de clé. Commençant par les protocoles à variables discrète où nous avons interprété le cas d'un photon unique et intriqué. En suite, nous avons fait une étude sur les protocoles à

variables continues. Comme nous avons énoncé une étude sur les CV-QKD dans le cas d'une modulation gaussienne et discrète que nous allons détailler dans le chapitre suivant.

III.1 Introduction

Dans ce chapitre, nous étudierons les protocoles de distribution quantique de clé à variables continues à modulation gaussiennes et à modulation discrète. Et pour pouvoir simuler les différentes équations nous allons utiliser le langage de développent informatique MATLAB.

D'abord, nous allons commencer par CV-QKD à modulation gaussiennes où on fait une comparaison dans le cas d'une détection homodyne et hétérodyne entre le protocole directe et inverse. Ensuite, on ferait une étude sur les CV-QKD à modulation discrète où on fait une étude sur les protocoles à quatre-états et à trois-états.

III.2 Simulation CV-QKD à modulation gaussiennes

III.2.1 Influence du gain du canal de transmission sur le bruit ajouté

On a les opérateurs quantiques de l'état sortant du dispositif d'Alice s'expriment :

$$X = X_A + X_0 \quad \textbf{(III.1)}$$

$$P = P_A + P_0 \quad \textbf{(III.2)}$$

Où X_0 et P_0 sont les quadratures de bruit du photon de variance N_0 associé à l'état cohérent, et on a la quadrature X_B mesurée par Bob :

$$X_B = g\,(X + X_{CB}) = g\,(X_A + X_0 + X_{CB}) \equiv g\,(X_A + X_N) \quad \textbf{(III.3)}$$

Avec $G = g^2 = T\eta \leq 1$ est la transmission totale en intensité entre Alice et Bob, produit de la transmission T du canal quantique et de l'efficacité η de la détection de Bob, X_{CB} est le bruit gaussien, et X_N le bruit ramené à l'entrée.

Donc :

$$X^2_N = X^2_{CB} + X^2_0 \equiv V_N = X + 1 \quad \textbf{(III.4)}$$

Où X^2_N est le bruit ramené à l'entrée, X^2_{CB} est le bruit ajouté ramené à l'entrée, et X^2_0 est l'unité de bruit du photon initiale.

Si le signal mesuré par Bob est limité au bruit du photon, on a $GN_N = 1$, donc $X = (1/G) - 1 \equiv X_0$. Finalement, on exprime le bruit ajouté par le canal quantique :

$$X = X_0 + \varepsilon \quad \textbf{(III.5)}$$

Avec $X_0 = (1/G) - 1$

Tel que X est le bruit ajouté ramené à l'entrée, X_0 est le bruit ajouté dû aux pertes, et ε est l'excès de bruit.

Dans la figure III.1 nous faisons varier la transmission du canal G de 0.1 à 1 dans l'équation **(**III.5**)**, pour un canal sans excès de bruit.

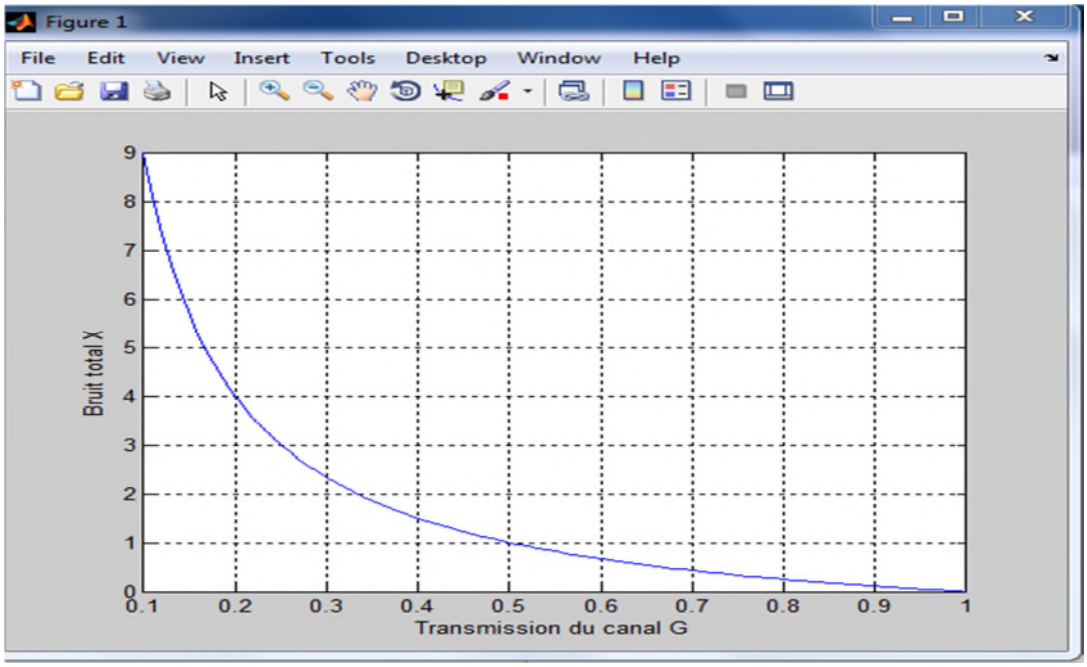

Figure III.1 : Evolution du bruit total en fonction de G.

Après avoir faire la simulation sur MATLAB nous avons obtenu la courbe illustrée sur la figure III.1. Nous constatons qu'au début de la transmission la valeur du bruit total est élevée. Puis, elle diminue avec l'augmentation de la transmission du canal G, cela indique que lorsque la valeur de transmission G augmente, la qualité de la liaison est meilleure.

III.2.2 Les informations mutuelles des protocoles à variables continues à modulation gaussienne

Dans cette partie, nous exposerons les différents résultats de simulation concernant les informations mutuelles des protocoles à variables continues, dans le cas général et dans le cas des attaques individuelles.

III.2.2.1 Cas général

On a :

La transmission de canal G varié de 0 à 1, l'excès de bruit $\varepsilon = 0$, et la variance de modulation $V = 40$.

III.2.2.1.1 Protocole à détection homodyne à réconciliation directe

On a :

$$I_{AB} = 1/2 \log_2 (1 + SNR) \qquad \text{avec} \quad SNR = V_A/V_N$$

$$I_{AB}=1/2\log_2(1+V_A/V_N)=1/2\log_2(1+V_A/(1+X))$$

(III.6) Et :

$$I_{AE} = 1/2 \log_2 (1+V_A/ 1+X_E) = 1/2 \log_2 (1+V_A/ 1+(1/X)) \qquad \textbf{(III.7)}$$

$$\Delta I = I_{AB} - I_{AE} \qquad \textbf{(III.8)}$$

Les courbes illustrées sur la figure III.2 représentent les informations mutuelles, entre Alice et Bob "I_{AB}" (équation III.6), Alice et Eve "I_{AE}" (équation III.7), et l'information secrète "ΔI" (équation III.8) dans le cas d'un protocole direct.

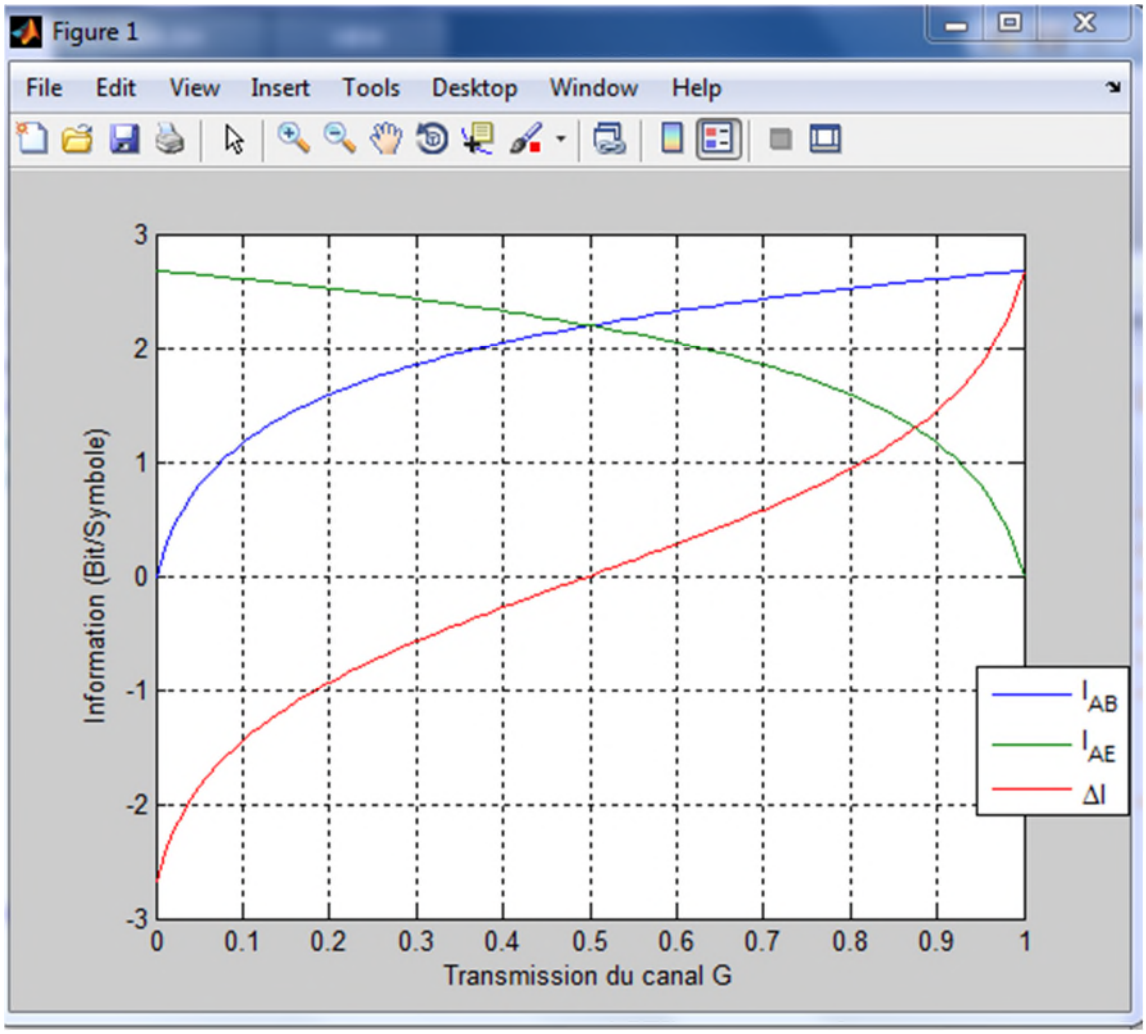

Figure III.2 : L'information mutuelle dans le cas d'un protocole direct avec détection homodyne.

D'après les résultats de simulation, nous remarquons que l'information secrète "ΔI" est positive pour les valeurs de transmission du canal quantique supérieure à 1/2, cela indique que Bob acquiert plus d'information sur les données d'Alice "$I_{AB}>I_{AE}$". Par contre, lorsque l'information secrète "ΔI" est inférieur à 1/2, cela veut dire qu'Eve acquiert plus d'information que Bob sur les données d'Alice "$I_{AE}>I_{AB}$", d'où la transmission est annulée.

III.2.2.1.2 Protocole à détection homodyne à réconciliation inverse

On a :

$$I_{BE} = 1/2 \log_2 (G^2 (X + V) (X + 1/V)) \text{ où } V = V_A + 1 \quad \textbf{(III.9)}$$

$$\Delta I = I_{AB} - I_{BE} \quad \textbf{(III.10)}$$

Dans ce cas, l'information mutuelle entre Alice et Bob "I_{AB}" ne change pas (équation III.6), mais au lieu de calculer "I_{AE}" on calcul "I_{BE}" (équation III.9) qui est l'information mutuelle entre Bob et Eve, cela nous amène à obtenir l'information secrète "IΔ" (équation III.10).

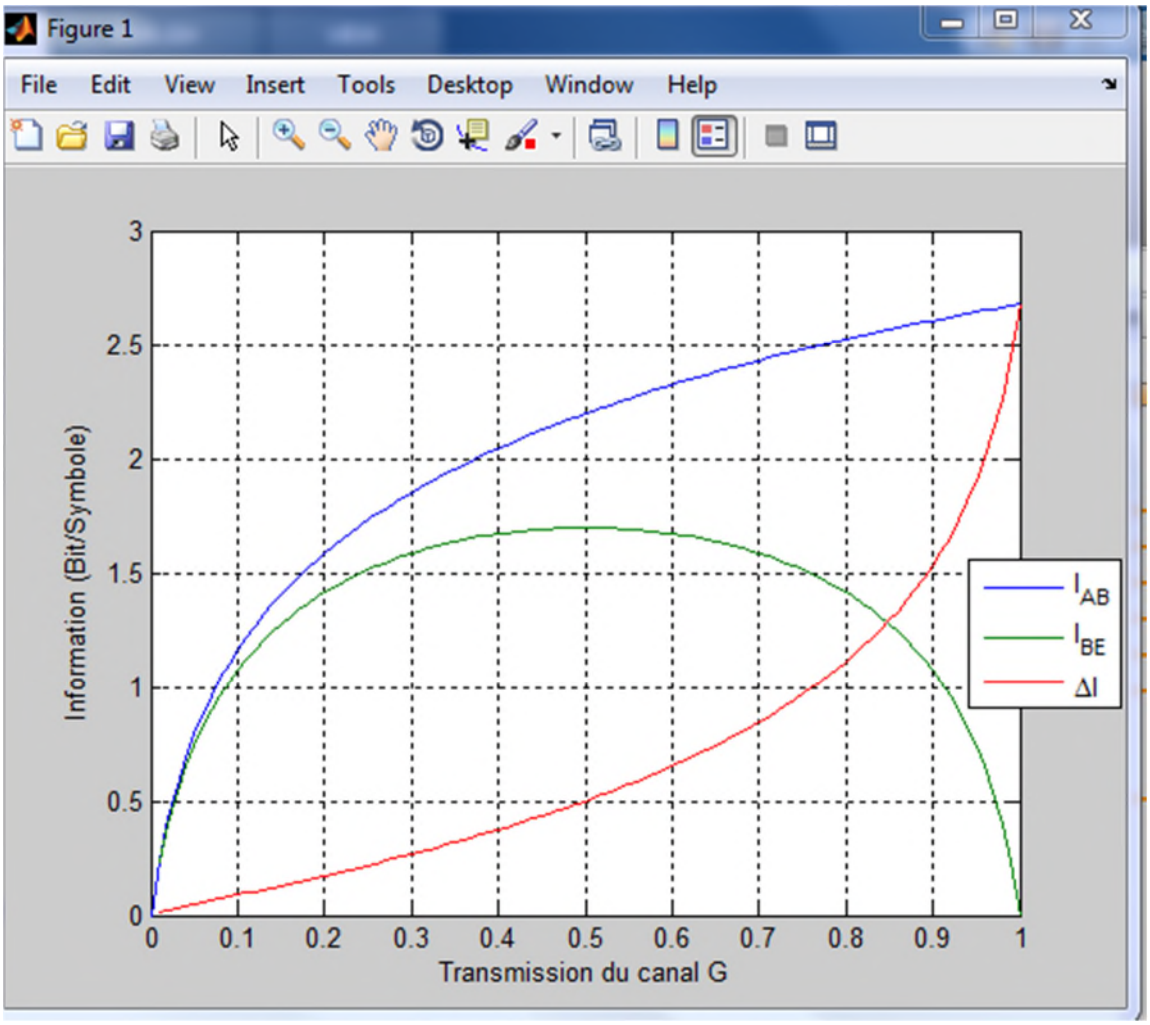

Figure III.3 : L'information mutuelle dans le cas d'un protocole inverse avec détection homodyne.

Nous remarquons selon la figure III.3, que l'information mutuelle entre Alice et Bob "I_{AB}" est supérieur à c'elle entre Bob et Eve "I_{BE}", le long de la transmission du canal, cela fait apparaître l'information secrète "IΔ" toujours positive, la chose qui nous amène à avoir la possibilité de distribuer une clé secrète.

- **Comparaison:**

En comparant les résultats de simulation des deux protocoles, nous concluons que les protocoles inverses fonctionnent d'une manière satisfaisante sur toutes valeurs de la transmission G, contrairement aux protocoles directs qui sont limités qu'à des valeurs de transmission fortes.

III.2.2.1.3 Protocole à détection hétérodyne à réconciliation directe

On a :

$$I_{AB} = 2*1/2 \log_2 (1 + SNR) = \log_2 (1 + V_A/ V'_N) \text{ Avec : } V'_N = (1 + X + 1/G) N_0$$

$$I_{AB} = \log_2 (1 + V_A/1 + X + (1/G)) \quad \textbf{(III.11)}$$

Et :

$$I_{AE} = \log_2 \frac{V+XE+1/GE}{1+XE+1/GE} \quad \text{avec} \quad (XE > 1/X)$$

I_{AE} est maximale quand $XE + 1/G_E$ est minimal, donc :

$$I_{AE} = \log_2 \frac{V+1/X}{1+1/X} \quad \textbf{(III.12)}$$

Et :

$$\Delta I = I_{AB} - I_{AE} \quad \textbf{(III.13)}$$

Les courbes illustrées sur la figure III.4 représentent les informations mutuelles entre Alice et Bob "I_{AB}" (équation III.11), Alice et Eve "I_{AE}" (équation III.12), et c'elle de l'information secrète "ΔI" (équation III.13), dans le cas d'un protocole direct avec détection hétérodyne.

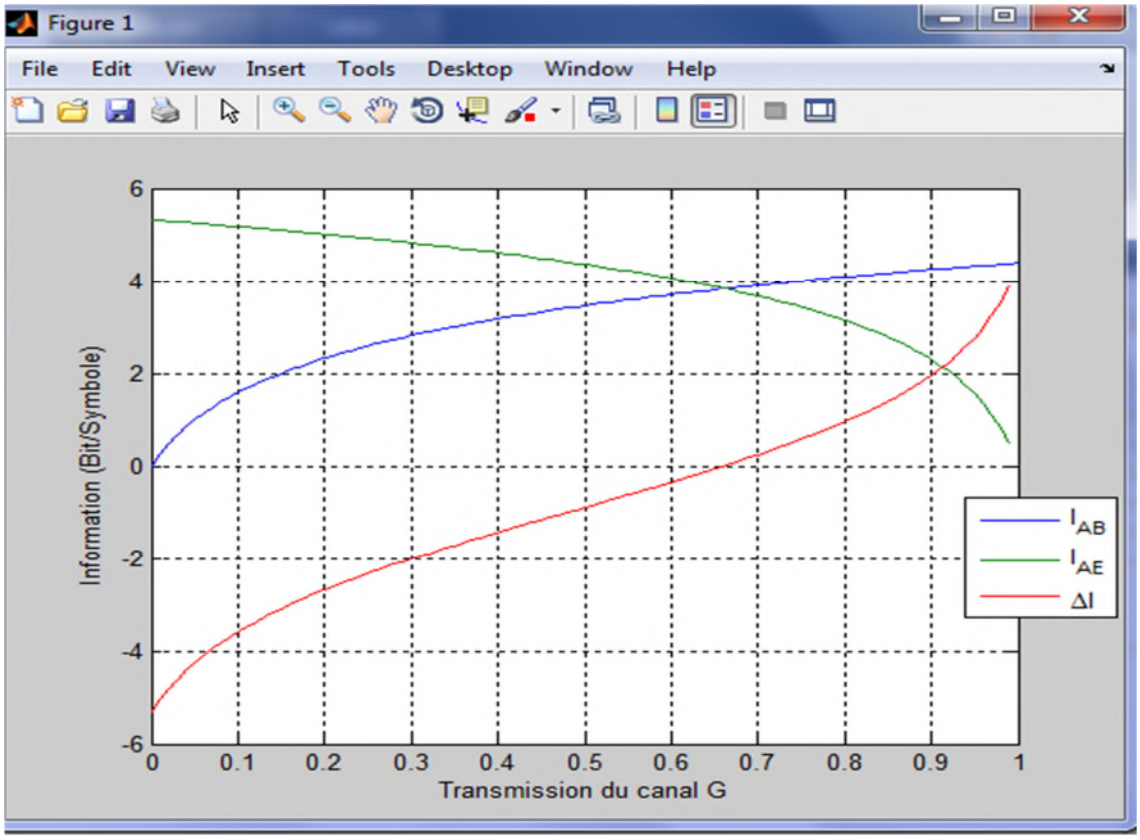

Figure III.4 : L'information mutuelle dans le cas d'un protocole direct avec détection hétérodyne.

III.2.2.1.4 Protocole à détection hétérodyne à réconciliation inverse

On a :

$I_{BE} = 2^* 1/2 \log_2 (V_{B'}/ V_{B'/E})$, où $V_{B'/E} = 1/2 (N_0 + V_{B/E}) \geq 1/2 (1 + 1/G(X + 1/V))$, N_0 est la variance conditionnelle pour le protocole hétérodyne.

Donc :

$$I_{BE} = \log_2 \left(\frac{G\left(V+X+\frac{1}{G}\right)}{\frac{1}{G\left(X+\frac{1}{V}\right)}+1} \right) \quad \textbf{(III.14)}$$

Et :

$$\Delta I = I_{AB} - I_{BE} \quad \textbf{(III.15)}$$

Les courbes représentées dans la figure III.5, sont c'elles de l'information mutuelle entre Alice et Bob "I_{AB}" (équation III.11), Bob et Eve "I_{BE}" (équation III.14), et l'information secrète "ΔI" (équation III.15), dans le cas d'un protocole à détection hétérodyne à réconciliation inverse.

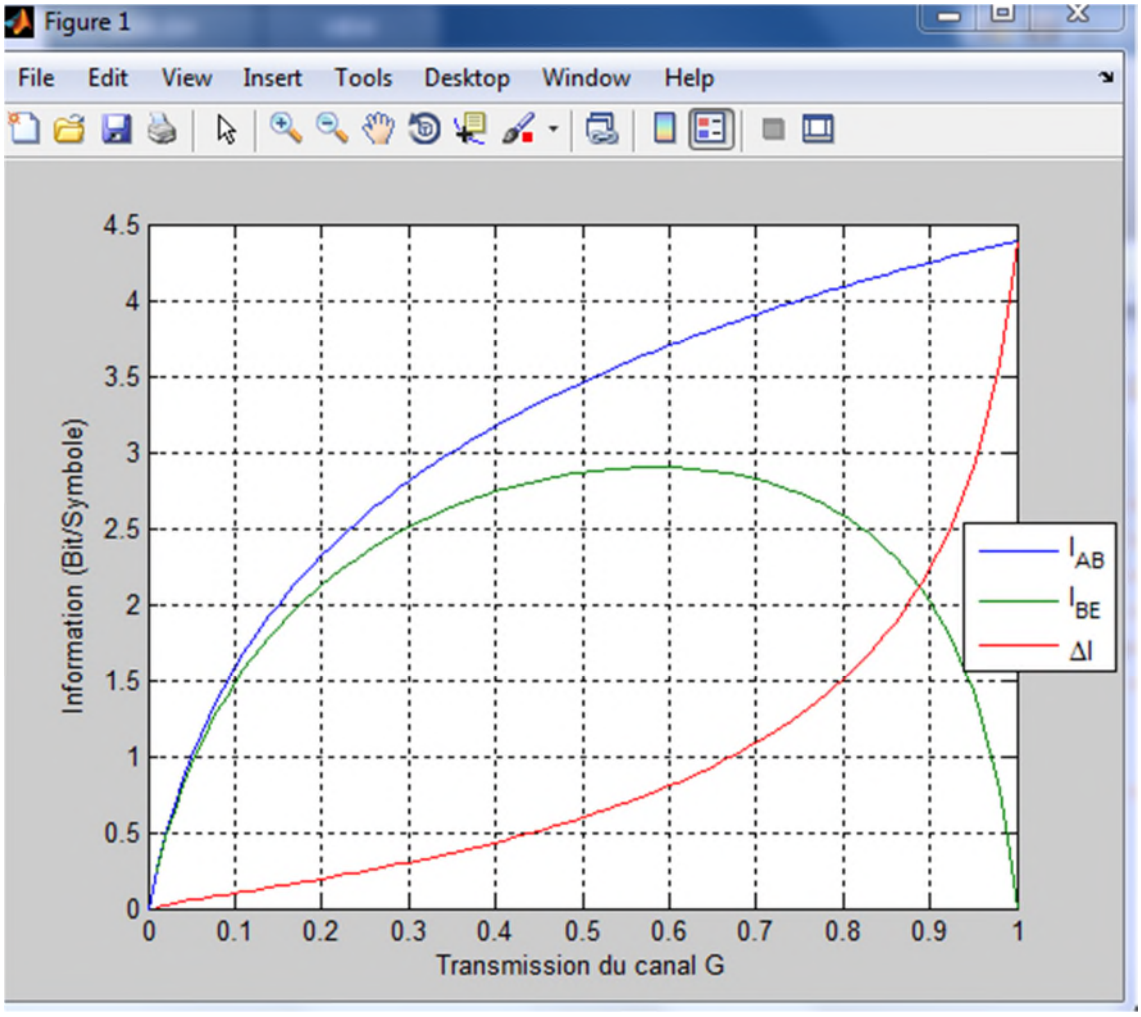

Figure III.5 : L'information mutuelle dans le cas d'un protocole inverse avec détection hétérodyne.

➢ **Comparaison:**

D'après les résultats de simulation, nous remarquons que dans les deux cas direct et inverse, l'information mutuelle entre Alice et Bob est la même. Par contre, lorsque nous calculons les informations mutuelles entre Alice et Eve, Bob et Eve, ainsi que l'information secrète, nous remarquons que, soit en détections homodyne ou hétérodyne les courbes sont presque identique, dans le cas d'un protocole directe et inverse, et la seule différence apparait dans l'information secrète où c'elle d'une détection hétérodyne est supérieur à c'elle d'une détection homodyne le long de toute la transmission.

III.2.2.1.5 Influence de la variance et l'excès de bruit sur les détections homodyne et hétérodyne

Influence de l'excès de bruit

La figure III.6 représente l'influence de l'excès de bruit sur la détection homodyne et la détection hétérodyne, où ε varie de 0 à 1, G = 0.5, V = 80.

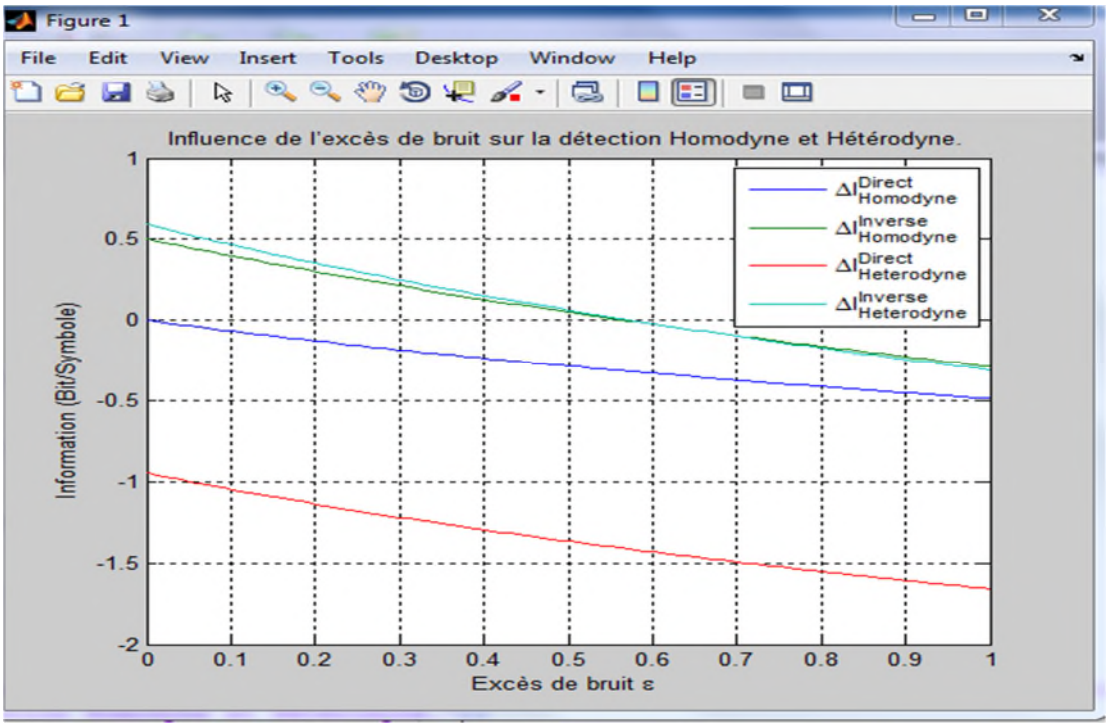

Figure III.6 : Influence de l'excès de bruit sur les détections homodyne et hétérodyne.

D'après les courbes de la figure III.6, nous remarquons que l'augmentation de l'excès de bruit fait diminuer l'information secrète dans les deux détections homodyne et hétérodyne, et que le maximum de la valeur de l'information secrète est atteint lorsque l'excès de bruit est nul, où nous obtenons une valeur de 0 pour un protocole direct et 0.55 dans le cas inverse. Par ailleurs, on remarque que le protocole inverse reste meilleur par rapport à celui direct concernent l'information mutuelle.

Influence de la variance

La figure III.7 représente l'influence de l'excès de bruit sur la détection homodyne et la détection hétérodyne, où V varie de 10 à 80, G = 0.5, ε = 0.

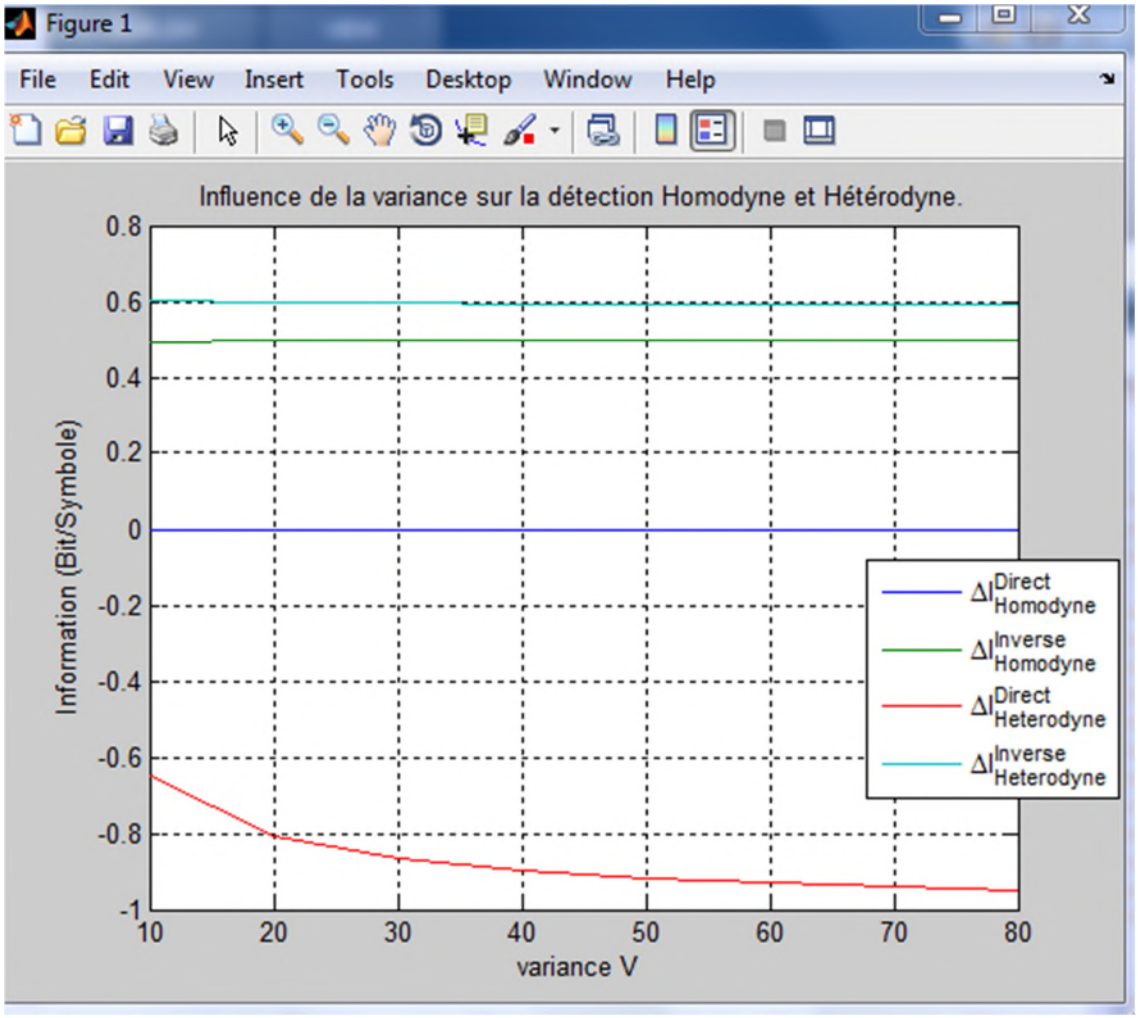

Figure III.7 : Influence de la variance sur les détections homodyne et hétérodyne.

La figure III.7 montre que, la variance influence d'une manière différente sur les protocoles, où nous remarquons que dans le cas directe nous obtenons des valeurs nulles et négatives (0 pour une détection homodyne, et à partir -0.7 pour la détection hétérodyne), contrairement dans le cas inverse où les valeurs sont positives.

III.2.2.2 Attaques individuelles

Nous faisons varier la transmission G de 0 à 1, l'excès de bruit ε = 0.01, on prenant la variance de modulation V = 20, Le bruit électronique υ_{el} = 0.01, et une efficacité de détection η = 1.

III.2.2.2.1 Cas d'une détection homodyne

Les courbes obtenues dans la figure III.8, permettent de visualiser l'influence de l'attaque individuelle sur la sécurité des protocoles dans le cas d'une détection homodyne.

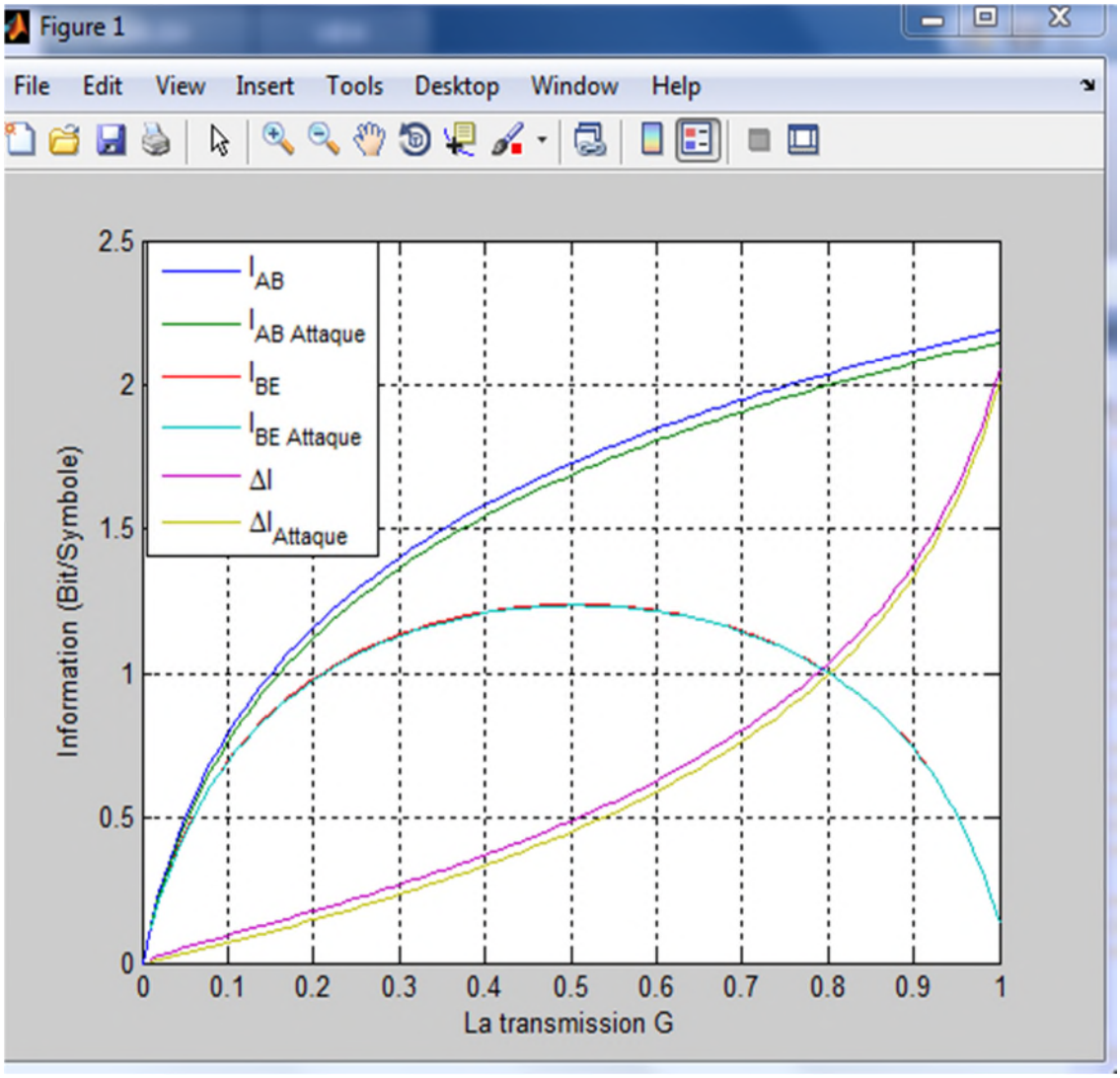

Figure III.8 : Comparaison entre les informations mutuelles dans le cas général et cas d'attaques individuelles pour la détection homodyne.

Selon les résultats obtenus, nous constatons que l'information dans le cas général est légèrement supérieur à c'elle dans le cas d'attaque individuelle, ce qui permet de dire que les attaques individuelles non pas une forte influence sur les protocoles à détection homodyne.

III.2.2.2.2 Cas d'une détection hétérodyne

Les courbes obtenues dans la figure III.9 permettent de visualiser l'influence de l'attaque individuelle sur la sécurité des protocoles dans le cas d'une détection hétérodyne.

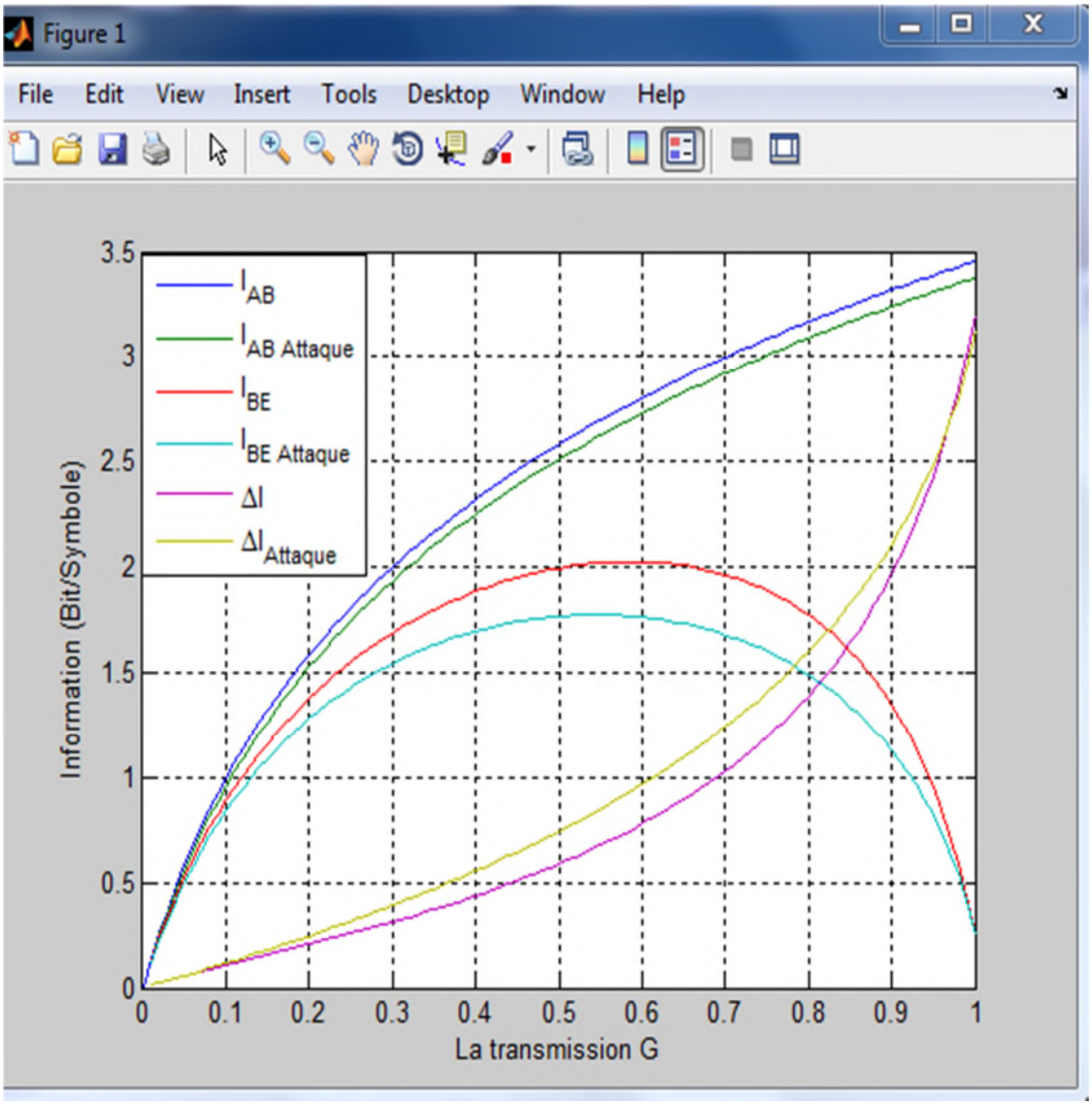

Figure III.9 : Comparaison entre les informations mutuelles dans le cas général et cas d'attaques individuelles pour la détection hétérodyne.

D'après les résultats obtenus, nous remarquons que contrairement au cas homodyne où l'information secrète dans le cas d'attaque est inférieur à c'elle du cas général. Mais dans ce cas, nous avons "$\Delta I_{Attaque} > \Delta I$" pour une transmission qui ne dépasse pas 0.95, ce qui amène à dire que dans ce cas Eve acquiert plus d'information que Bob, cela indique que à certaines valeurs les attaques individuelles influencent sur la détection hétérodyne.

III.3 Simulation CV-QKD à modulation discrète

III.3.1 Cas d'un protocole à quatre-états

Le CV-QKD utilise un protocole à quatre-états et un poste-sélection, et génère une clé sécurisée contre l'attaque de cloner enchevêtrement. Où Alice envoie à Bob un état cohérent $|\alpha e^{i\phi}>$ avec $\alpha = \sqrt{2}*\alpha'$ (α' est une constante > 0), et ϕ = 3pi/4 est la phase.

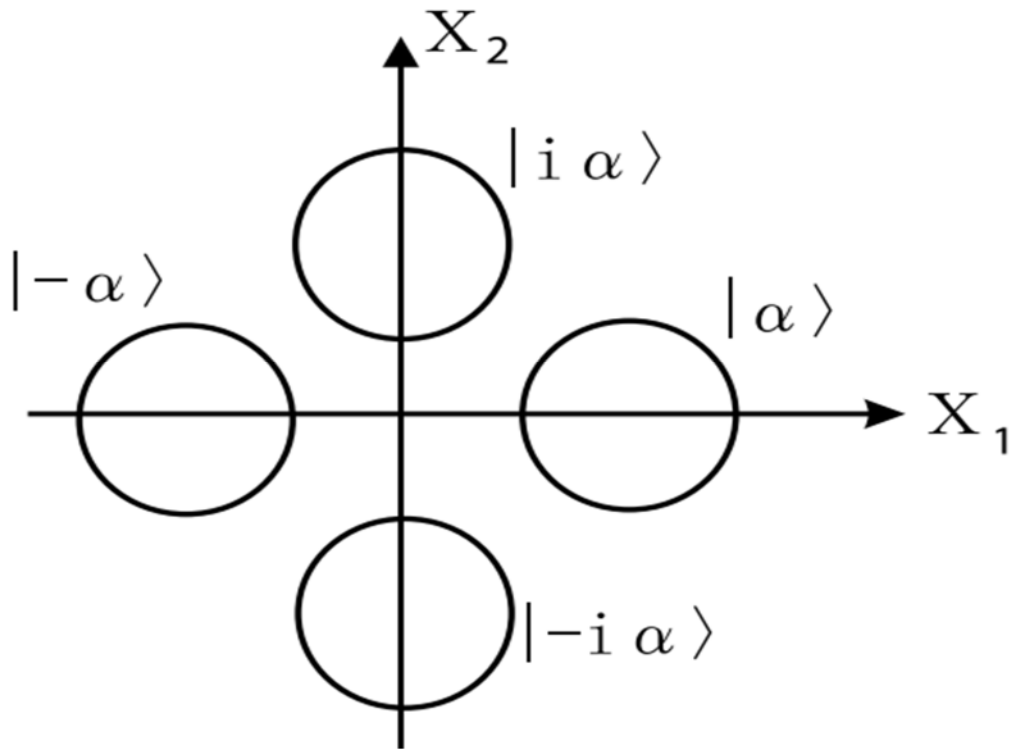

Figure III.10 : Représentation du protocole à quatre-états dans l'espace des phases [29].

III.3.1.1 Le taux clé secret en fonction de la distance

On a :

$$K = \beta I(A; B) - X(B; E) \quad \textbf{(III.16)}$$

Où K est le taux clé secret, β = 0.89 est une constante, I (A; B) = 1/2 $\log_2$ (1 + SNR) est l'information mutuelle entre Alice et Bob, et X (B; E) = $\alpha e^{i\phi}$.

Donc :

$$K = \beta (1/2 \log_2 (1 + SNR)) - \alpha e^{i\phi} \quad \text{avec} \quad SNR = TV_A/1 + T\varepsilon$$

$$K = \beta (1/2 \log_2 (1 + TV_A/1 + T\varepsilon)) - \alpha e^{i3pi/4} \quad \textbf{(III.17)}$$

La figure III.11 représente le taux clé secret (équation III.17) en fonction de la distance qui varie de 0 à 100km, pour un excès de bruit de 0.005, une variance de modulation exprimée par ($2*f^2$) où f est une constante f = 0.35, et une efficacité quantique de 0.89.

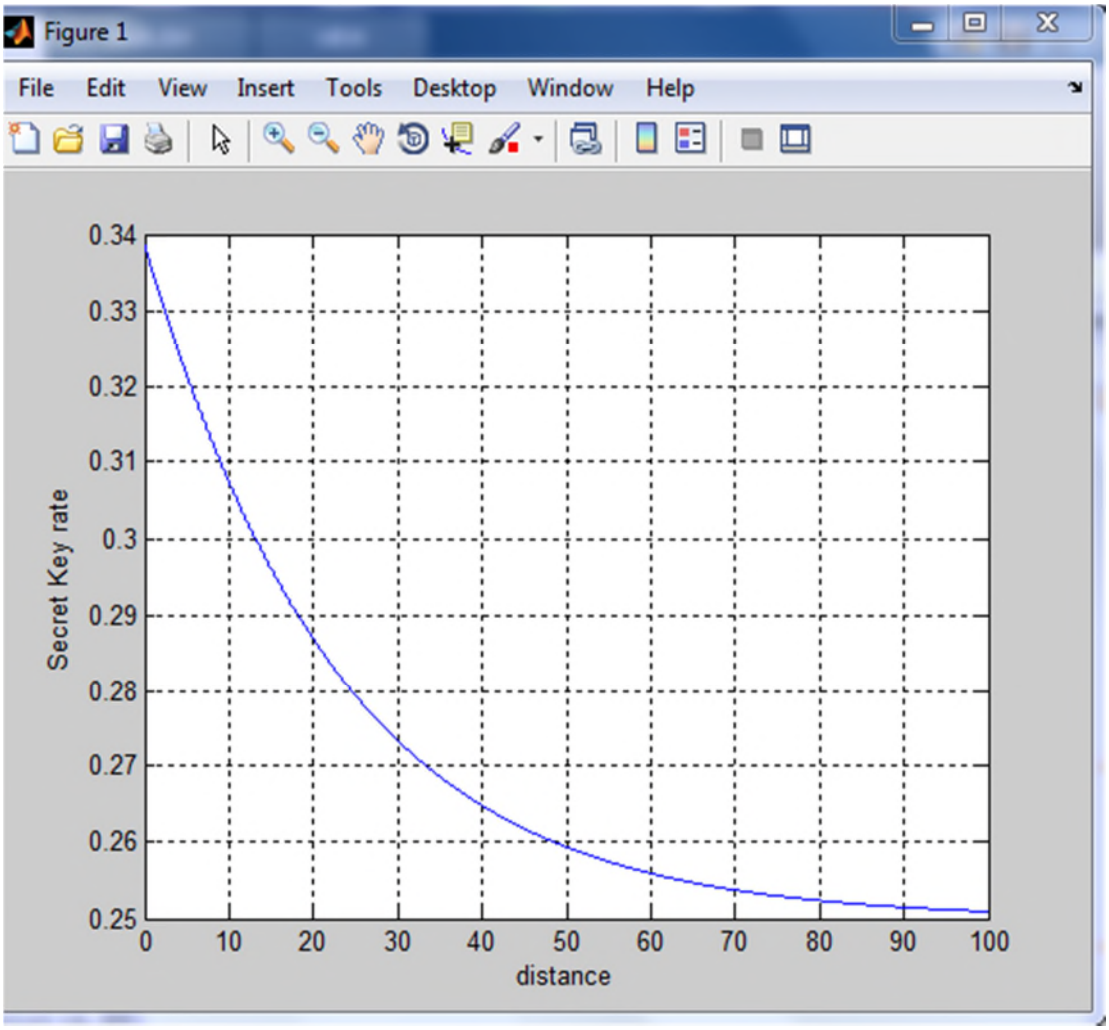

Figure III.11 : Taux clé secret d'un protocole à quatre-états en fonction de la distance.

D'après la figure III.11, nous remarquons que pour une distance de 0 km, le taux de clé secret est plus élevé, et que plus la distance augmente plus cette valeur s'approche de 0.

III.3.1.2 Le taux clé secret en fonction du SNR

Pour une distance qui varie de 0 à 100km, la figure III.12 représente le taux clé secret (équation III.17) en fonction du rapport signal bruit (SNR), avec une variance de modulation exprimée par la fonction ($2*f^2$) où f = 0.35 est une constante, un excès de bruit de 0.005, et une efficacité quantique d'une valeur de 0.89.

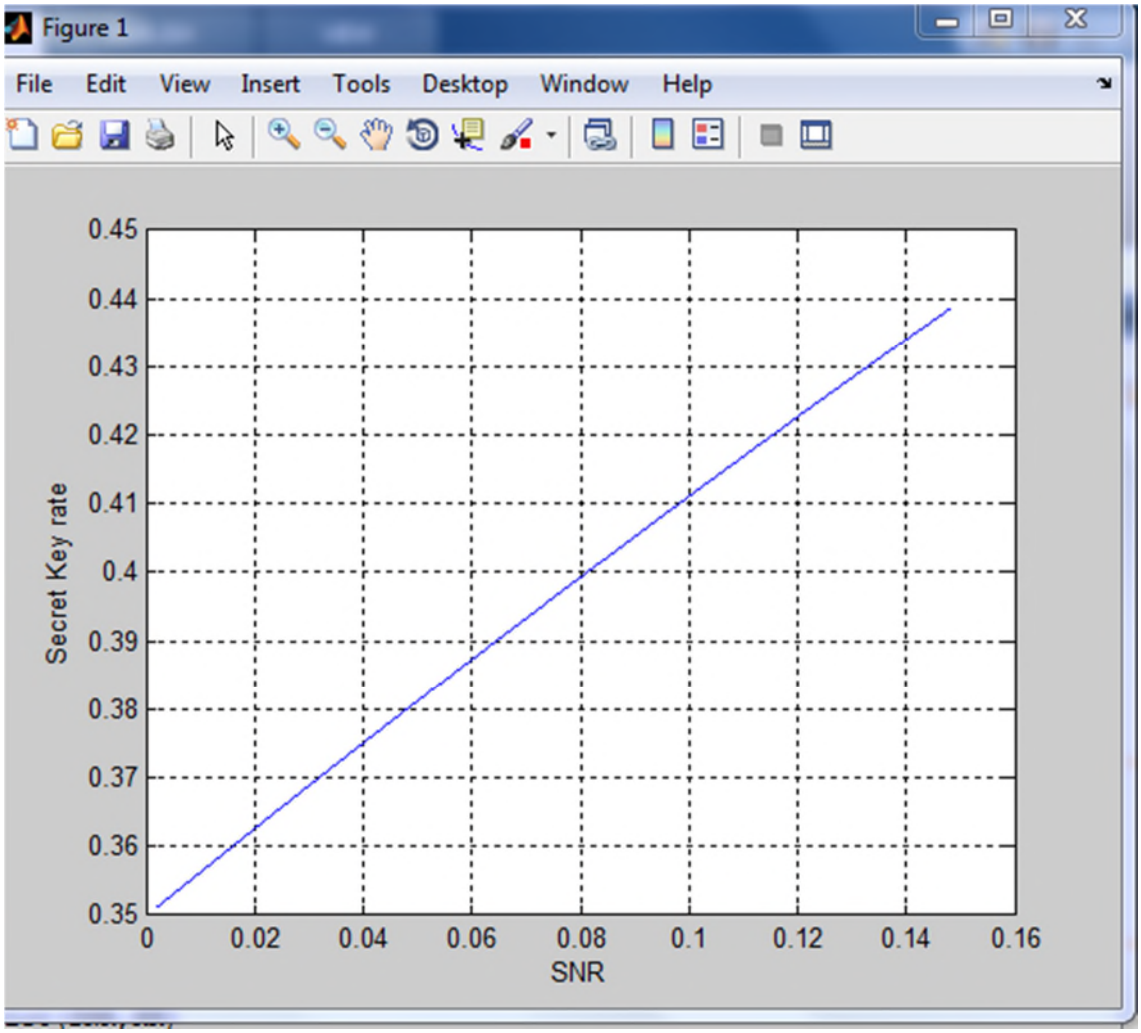

Figure III.12 : Taux clé secret d'un protocole à quatre-états en fonction du SNR.

D'après la figure III.12 nous remarquons que, même avec un faible rapport signal sur bruit une correction d'erreur peut être effectuée.

III.3.2. Cas d'un protocole à trois-états

Le codage du protocole à trois états est décrit schématiquement sur l'espace des phases. Alice envoie à Bob un état cohérent $|\alpha_1 e^{i\phi}>$ avec $\alpha_1 = (2/\sqrt{3})*\alpha'$ (α' est une constante > 0), et $\phi = 2pi/3$ est la phase.

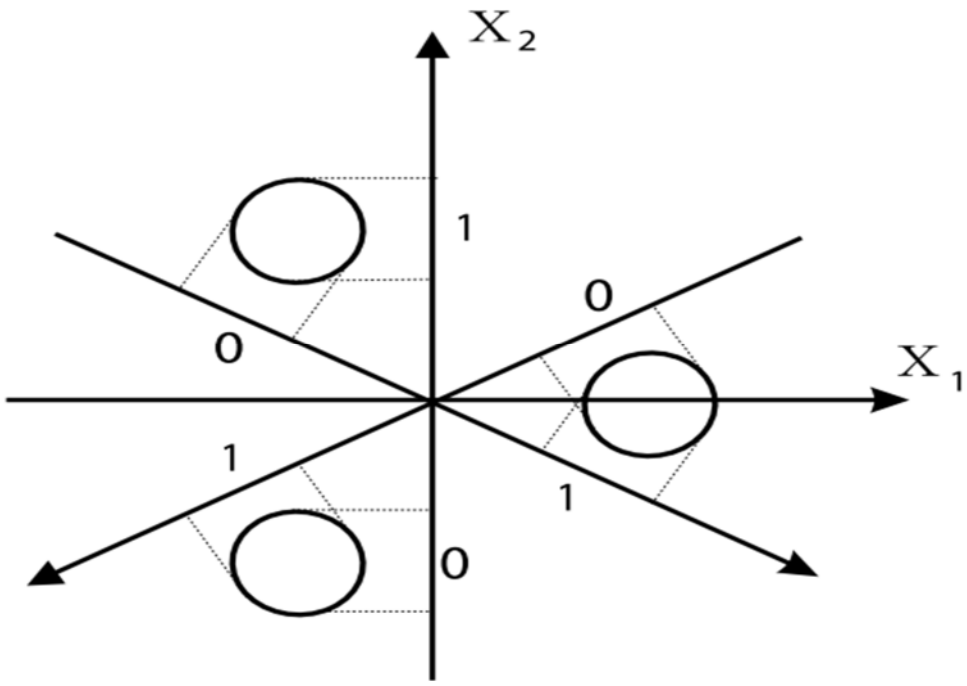

Figure III.13 : Représentation du protocole à trois-états dans l'espace des phases [29].

L'équation III.17 devient donc :

$$K = \beta\,(1/2\,\log_2(1 + TV_A/1 + T\varepsilon)) - \alpha_1\, e^{i2pi/3} \qquad \textbf{(III.18)}$$

III.3.2.1 Le taux clé secret en fonction de la distance

La figure III.14 représente le taux clé secret (équation III.18) en fonction de la distance qui varie de 0 à 100km, pour un excès de bruit de 0.005, une variance de modulation exprimée par ($2*f^2$) où f = 0.35 est une constante, et une efficacité quantique de 0.89.

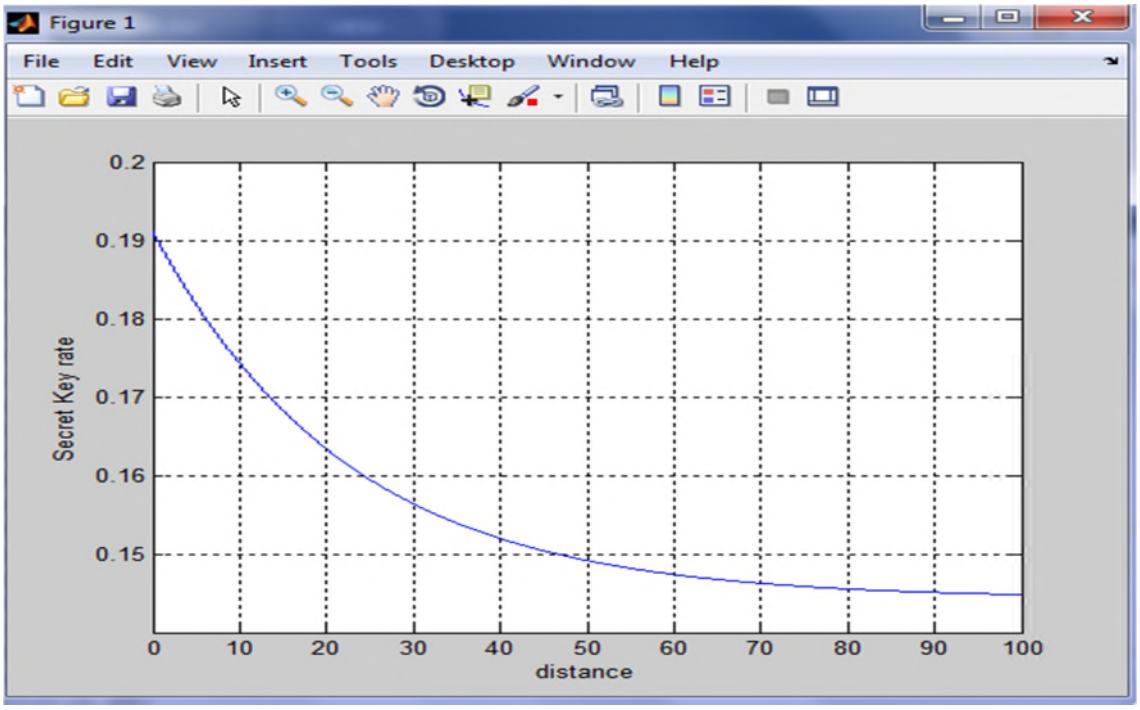

Figure III.14 : Taux clé secret d'un protocole à trois-états en fonction de la distance.

D'après la figure III.14, nous remarquons que le protocole à trois-états subit presque les mêmes changement qu'un protocole à quatre-états, où nous avons un taux de clé élevé au début de la transmission et plus la distance augmente cette valeur diminue.

III.3.2.2 Le taux clé secret en fonction du SNR

Pour une distance qui varie de 0 à 100km, la figure III.15 représente le taux clé secret (équation III.18) en fonction du rapport signal bruit (SNR), avec une variance de modulation exprimée par la fonction ($2*f^2$) où f = 0.35 est une constante, un excès de bruit de 0.005, et une efficacité quantique d'une valeur de 0.89.

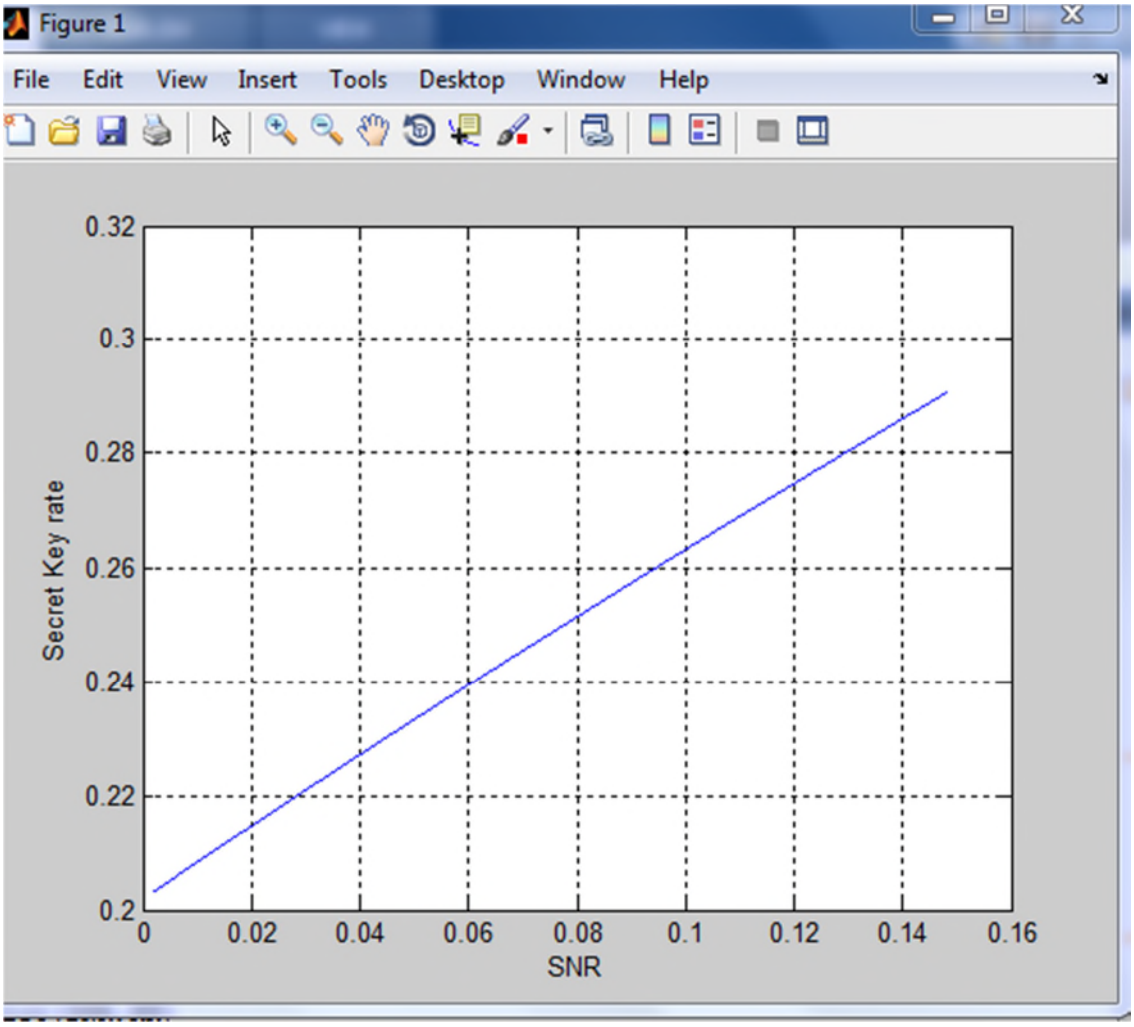

Figure III.15 : Taux clé secret d'un protocole à trois-états en fonction du SNR.

Nous remarquons que, à une valeur du SNR égale à 0 le taux de clé secret est à 0.2, c'est à dire que même avec un faible SNR une correction d'erreur peut être effectuée.

- **Comparaison :**

D'après les résultats de simulation, on remarque que soit dans un protocole à quatre-états ou à trois-états les courbes sont presque identiques, que ça soit dans le cas du taux clé secret en fonction de la distance ou en fonction du SNR.

III.4 Comparaison entre les protocoles CV-QKD à modulation gaussienne et à modulation discrète

Nous remarquons que dans le cas des CV-QKD à modulation gaussienne, le problème se pose quand on veut effectuer une QKD sur de longues distances. Dans ce cas, il existe deux possibilités pour lutter contre le bruit induit par les pertes dans le canal : soit augmenter la variance de modulation de sorte que le SNR reste raisonnablement élevé, ou travailler à faible SNR. Malheureusement, les deux approches ont tendance à échouer sur quelques dizaines de kilomètres. Par contre, dans le cas des CV-QKD à modulation discrète, l'efficacité reste remarquablement élevée car une correction d'erreur peut être introduite même avec un très faible SNR.

III.5 Conclusion

Dans ce chapitre, nous avons représenté les résultats de la simulation des protocoles de distribution quantique de clé à variables continues dans le cas des deux modulations gaussien et discrète.

Nous constatons que les CV-QKD, offrent une possibilité d'avoir une clé sécurisé le long de la transmission Par ailleurs nous déduisons que dans le cas d'une modulation gaussienne nous avons plus de chance d'avoir une sécurité de transmission dans le cas d'un protocole inverse, et que pour la modulation discrète la chance de sécurité est possible dans les deux cas (quatre-états et trois-états) car une correction d'erreur peut être introduite même à faible SNR.

Conclusion générale

La nécessité de sécuriser la transmission de données augmente chaque jour, et nécessite des dispositifs de chiffrement de données sécurisés pour préserver la confidentialité et l'authentification des échanges des applications critiques.

Ce travail se concentre sur les protocoles de distribution quantique de clé, dans le but d'atteindre une sécurité le long de la transmission. Pour cela, nous avons commencé par une étude générale sur la cryptographie classique et quantique. Ensuite, nous avons fait une étude détaillée sur la distribution quantique de clé en utilisant des relations et des formules mathématiques qui sont démontées par les lois de la théorie d'information et de la mécanique quantique, afin de rendre le protocole plus robuste aux pertes et accroître son efficacité.

Les simulations des protocoles de distribution quantique de clé sur MATLAB sont constituées de deux parties. Dans la première partie, nous avons simulé les deux protocoles directe (I_{AB}, I_{AE}, ΔI) et inverse (I_{AB}, I_{BE}, ΔI) pour les deux détections homodyne et hétérodyne (modulation gaussienne), où nous avons constaté d'après les courbes obtenues en fonction de la transmission du canal que le cas d'un protocole inverse offre une possibilité de produire une clé secrète pour toute la transmission. Ensuite, nous avons simulé puis comparer les protocoles à trois-états et à quatre-états (modulations discrète), en faisant varier le taux de clé secret en fonction de la distance et du SNR. Nous avons remarqué que pour les deux cas, y’a une chance d'avoir une sécurité même avec un faible SNR pour de longues distances.

D'après les résultats de ces simulations, nous concluons que le cas des protocoles à quatre-états et à trois-états offre une meilleure sécurité de transmission à longues distances.
Comme perspective, il serait intéressant de réaliser un multiplexage WDM afin d'augmenter le débit.

Références bibliographiques

[1] C. THUILLET, "Implantations cryptographiques sécurisées et outils d'aide à la validation des contremesures contre les attaques par canaux cachés", Thèse de Doctorat, Université BORDEAUX I, (France) ,30.Mars.2012.

[2] T. MEKHAZNIA, "Analyse cryptographique par les méthodes heuristique", Thèse de Doctorat, Université de BATNA 2(Algérie), 25. Février. 2017.

[3] B. DEBBAGH, N. BOUNEGEB, "Etude de comparaison de principaux systèmes crypto fournis par le package de Bouncy Castel plat forme Java SDK ", Mémoire de Master académique, Université KASDI MERBAH OUARGLA (Algérie), 05.Juin.2016.

[4] K. DICHOU, "contribution à l'étude des cartes à puce avancées", Thèse de Doctorat-LMD, Université M'HAMED BOGARA-BOUMERDES, 2016.

[5] M. BOUCHEMA, "Exploitation des transformées paramétriques dans le cryptage des images fixes", Mémoire de Magistère, Université FERHAT ABBAS -SETIF 1, (Algérie), 28. Décembre. 2012.

[6] A. Kerckhoffs. "La cryptographie militaire". Journal des sciences militaires IX, 5 (1883).

[7] Informatique pour Ingénieur. "Casser un code secret". Institut Galilée -Université Paris 13, 2014.

[8] F. OMARY, "Applications des algorithmes évolutionnistes à la cryptographie", Thèse de Doctorat d'état, Université MOHAMMED V - AGDAL RABAT (MAROC), 26. Juillet. 2006.

[9] A. K. BENHAOUA, "approche cryptographie base sur les algorithmes génétique pour la sécurité des réseaux Ad hoc", Mémoire de Magistère, Université D'ORAN ES-SENIA, (Algérie), 2005.

[10] M. VIDEAU, "Critère de sécurité des algorithmes de chiffrement à clé secrète", Thèse de Doctorat, Université de Paris 6, (France), 10. Novembre. 2005.

[11] Y. M.AIT AMEUR, "sécurisation de communication dans les réseaux d'ordinateurs (couche SSL) ", Mémoire de Master, Université Mohamed Khider Biskra, (Algérie), Juin.2014.

[12] M.A.FILALLI, "Etude et Implémentation Pipeline sur FPGA de l'algorithme de Chiffrement ASE", Mémoire de Magister, Université MOHAMED BOUDIAF d'ORAN, (Algérie), 29.Juin.

[13] B. KEBIR, S. RAHMOUNI, "Développement d'une application pour l'échange des messages sécurisé", Mémoire de fin d'études, Université de Abou Bakr Belkaid, Telemcén, (Algérie), Mai 2015.

[14] G. ZAIDI, "Sécurisation par dynamiques chaotiques des réseaux locaux sans fil au niveau de la couche MAC", Thèse de Doctorat, L'école Nationale d'Ingénieurs de Sfax, (Tunisie), 06. Décembre. 2012.

[15] A. KARRAY, "Conception, mise en œuvre et validation d'un environnement logiciel pour le calcul sécurisé sur une grille de cartes à puce de type Java", Thèse de Doctorat, Université BORDEAUX I, (France), 10. Décembre. 2008.

[16] S Aris, N Merabtine et M Benslama, "Solution aux limites pratiques dans les télécommunications quantiques", Université de Constantine - Algérie, Mars 2007.

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

[18] L. LERMAN, "La cryptographie quantique", Département "Science Informatique", ULB.

[19] S. Allou, K. Allouane, "Cryptographie et sécurité des réseaux implémentation de l'AES sous MATLAB", Mémoire fin d'études, Université MOULOUD MAMMERI, TIZI-OUZOU, (Algérie), 2008.

[20] P. JOUGUET, "Sécurité et performance de dispositifs de distribution quantique de clés à variables continues", Thèse de Doctorat, Institut Paris Tech (France), 18 Septembre 2013.

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

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

[23] A. EL ALLATI, "Etude de cryptographie et de téléportation quantiques et proposition de quelques protocoles quantiques", Thèse de Doctorat, Université MOHAMMED V-AGDAL (Maroc), 30 Janvier 2012.

[24] A. Ekert : Quantum Cryptography Based on Bell's Theorem. Phys. Rev. Lett., August 1991.

[25] J. WENGER, "Dispositifs impulsionnels pour la communication quantique à variables continues", Université Paris XI (France), 09 Septembre 2004.

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

[27] Jérôme Lodewyck. Dispositif de distribution quantique de clé avec desétats cohérents à longueur d'onde télécom. Physique Atomique [physics.atom-ph]. Université Paris Sud - Paris XI, 2006. Français.

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

[29] Takuya Hirano, "Efficient-phase-encoding protocols for continuous-variable quantum key distribution using coherent states and post selection", Gakushuin University, Japan, 1 September 2006.

Résumé

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

La distribution quantique de clé permet à deux parties distantes de communiquer avec intimité absolue, même en présence d'un espion. En se basant sur les lois de la mécanique quantique et de la théorie d'information.

Dans ce travail, nous avons présenté les concepts de bases de la cryptographie quantique pour prouver son efficacité dans des transmission sécurisées. Nous avons simulé puis comparer les CV-QKD à modulation gaussienne et CV-QKD à modulation discrète.

Abstract

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

Quantum key distribution allows two distant parties to communicate with absolute privacy, even in the presence of a spy. Based on the laws of quantum mechanics and information theory.

In this work, we presented the basic concepts of quantum cryptography to prove its efficiency in secure transmission. We have simulated and then compared the Gaussian modulated CV-QKD and the discrete modulated CV-QKD.

Mots clés

Cryptographie, canal quantique, protocole, variables continues, sécurité, théorème.