Sécurité en cryptographie quantique utilisant la détection homodyne d'états cohérents à faible énergie

Manuel Sabban

École Doctorale
d'Informatique,
Télécommunications
et Électronique de Paris

Thèse

présentée pour obtenir le grade de docteur

de Télécom ParisTech

Spécialité : Électronique et Communications

Manuel Sabban

Sécurité en cryptographie quantique utilisant la détection homodyne d'états cohérents à faible énergie

Soutenance prévue le 29 avril 2009

M. Jean-Marc Merolla	Rapporteurs
Pr Paul Voss	
Pr Patrick Bellot	Examinateurs
M^{me} Eleni Diamanti	
Pr Francisco Mendieta	
M. Nicolas Pelloquin	
Pr Philippe Gallion	Directeur de thèse

Mignonne, allons voir si la rose
Qui ce matin avait déclose
Sa robe de pourpre au soleil,
A point perdu cette vêprée,
Les plis de sa robe pourprée,
Et son teint au vôtre pareil.

Las ! Voyez comme en peu d'espace,
Mignonne, elle a dessus la place,
Las, las ! Ses beautés laissé choir !
Ô vraiment marâtre Nature,
Puis qu'une telle fleur ne dure
Que du matin jusques au soir !

Donc, si vous me croyez, mignonne,
Tandis que votre âge fleuronne
En sa verte nouveauté,
Cueillez, cueillez votre jeunesse
Comme à cette fleur, la vieillesse
Fera ternir votre beauté.

Pierre de Ronsard, À Cassandre

Table des matières

Remerciements

Je voudrais aussi remercier particulièrement Bernard Robinet, directeur de l'école doctorale Edite de Paris pour son accueil chaleureux quand j'ai eu besoin de lui et aussi lors de mes nombreuses démarches administratives qui passaient par sa signature.

J'aimerais également remercier Bruno Thèdrez pour l'accueil dans le département Comélec et les nombreuses discussions que j'ai eu avec lui au sujet du clonage quantique.

J'aimerais également remercier Didier Érasme pour l'accueil au sein de l'équipe d'optique et au sein de l'équipe d'enseignement. L'enseignement que j'ai efféctué à Télécom ParisTech m'a beaucoup apporté.

Je remercie particulièrement Jean-Marc Merolla et Paul Voss pour avoir bien voulu se charger de rapporter mon travail de thèse.

Je remercie Patrick Bellot, Eleni Diamanti, Nicolas Pelloquin d'avoir accepté de me faire l'honneur de faire partie du jury de ma thèse. Je remercie chaudement Francisco Mendieta d'en avoir assuré la présidence.

Je veux également remercier chaleureusement mon directeur de thèse Philippe Gallion pour ces quatre années passées à travailler sous sa direction avisée depuis le stage de deuxième année de master. J'ai une pensée particulière pour tous ces moments ou il a su trouver les mots justes pour me permettre de garder intacte ma motivation et développer mon goût de la science. J'aimerais aussi souligner l'apport scientifique indéniable que nos discussions m'ont apporté.

J'aimerais aussi remercier Francisco Mendieta et Qing Xu pour la qualité de l'apport scientifique et des encouragements qu'ils m'ont apportés.

J'aimerais tout particulièrement remercier Chantal Cadiat et Danièle Childz pour le support logistique qu'elles ont apporté à cette thèse.

Je tiens également à remercier chaleureusement tous les collègues doctorants avec qui j'ai vécu d'agréables années. Je remercie les permanents avec

qui j'ai pu interagir pendant ces quelques années passées à leurs côtés.

Je veux encore remercier mes proches, pour m'avoir supporté pendant ces années de thèse. Je pense notamment à mes parents, ma soeur et mes amis Freddie, Jul, Manathan, Mit, Ryo, Schultzy et Vince||. J'ai une pensée toute particulière pour ma compagne Marion.

Je remercie chaleureusement les relecteurs de ma thèse qui m'ont fait part de leurs pertinentes remarques avant les relectures finales par Philippe Gallion. Je remercie donc mon père Jean-Claude, Mit, Manathan, Marion et Ryo.

J'ai une pensée émue pour Sylvain Soufflet qui par son enseignement rigoureux a su m'insuffler le goût des sciences physique, et donc m'a permis de me lancer sur la voie de ce doctorat.

Introduction

La cryptologie est à la fois une discipline ancienne, mais également une science moderne. En effet, des ouvrages datant de l'antiquité traitant de l'utilisation de moyens cryptologiques sont encore connus de nos jours. Jules César a également fait usage de cryptographie pour ses communications. Ces faits historiques ont été utilisés plus tard au Moyen-Âge pour créer de nouvelles méthodes de chiffrements. Mais ce n'est qu'au XX^{e} siècle que Shannon jeta des bases mathématiques à ces théories. On sait depuis Vernam que les conditions d'un chiffre parfait comportent l'usage unique d'une clef aussi longue que le message à transmettre. Cette condition forte est souvent irréalisable en pratique. Toute la difficulté est alors d'inventer des algorithmes de chiffrement fournissant un compromis entre la sécurité et le coût de mise en œuvre. Une deuxième difficulté est la pérennité à cause de l'augmentation de la puissance de calcul des ordinateurs suivant pour l'instant la loi de Moore. En effet, est-ce que ce qui est chiffré hier sera toujours en sécurité demain lorsque la nécessité du secret est pérenne ? Comment faire évoluer les algorithmes d'hier pour qu'ils soient toujours inviolables demain ?

Une approche mathématique moderne a permis un grand travail sur les protocoles de cryptographie moderne. Ils sont nombreux, et même les plus utilisés comme RSA et 3DES ne sont pas formellement prouvés comme étant inviolable par une attaque de type force brute. D'ailleurs nous savons déjà que l'approche par un ordinateur quantique abaisserait considérablement le temps de calcul pour casser ces chiffrements. Ce qui est chiffré par des moyens classiques aujourd'hui pourra être facilement cassé demain, c'est inquiétant pour certaines applications qui nécessitent une protection pendant de grandes durées. Le seul chiffrement inconditionnellement sûr est le chiffre de Vernam. Son problème est que ses conditions d'utilisation habituelle nécessitent une rencontre physique des protagonistes Alice et Bob pour s'échanger une clef aussi longue que le message à communiquer utérieurement.

En utilisant le principe d'incertitude d'Heisenberg, Bennett et Brassard ont créé les bases d'un nouveau système de distribution de clefs quantiques noté BB84. La cryptographie quantique offre une solution pour utiliser ce chiffre de Vernam assurant une sécurité absolue sans nécessité de rencontre physique entre Alice et Bob. En effet, en utilisant un protocole de distribution de clef quantique comme BB84, Alice et Bob sont en mesure d'échanger une clef sans restriction sur la longueur. Ce système garantit la sécurité ab-

solue d'une transmission, dans le présent et dans le futur grâce aux lois de la physique. Aucune amélioration de la puissance de calcul ne peut changer cet état de fait. La première démonstration de ce nouveau système de cryptographie quantique a été effectuée en 1992 sur une distance d'une trentaine de centimètres par voie aérienne. Il s'agit cependant de limites fondamentales que nous ne pouvons qu'approcher, vu qu'il existe un certain nombre de difficultés à surmonter car en effet nous sommes confrontés à des dispositifs et un canal pourvus de défauts. Il n'existe pas encore de sources à photons uniques exhibant des performances satisfaisantes et à un coût raisonnable. Les compteurs de photons ont un rendement très faible de l'ordre de 10%, notoirement aux longueurs d'ondes des télécommunications optiques compte tenu de la faible énergie des photons et de l'importance des effets thermiques.

Le travail proposé est une réflexion sur la sécurité de certains protocoles de distribution de clefs quantiques. Nous avons choisi d'utiliser la phase d'états cohérents à faible énergie pour porter notre information. Deux principaux axes sont mis en valeurs. Le premier est une étude sur l'apport d'un mode différentiel sur un protocole à modulation de phase utilisant des compteurs de photons, et le deuxième correspond à une réflexion sur l'apport d'un double seuil dans les mesures à détection homodyne. Les études proposées au fil de ce manuscrit s'inscrivent en complémentarité des travaux expérimentaux menés par mon collègue et ami M. Xu.

Tout d'abord le premier chapitre présente un historique des procédés cryptographiques en s'attardant quelque temps sur certains chiffrements comme par exemple ceux de César, de Vigénère et d'Enigma. Il amène les bases mathématiques nécessaires à l'étude des chiffrements classiques. Il introduit aussi dans les grandes lignes les différents types de chiffrements utilisés actuellement.

Ensuite, dans le second chapitre, nous mettons en place les outils et les concepts de mécanique quantique que nous serons amenés à utiliser plus tard. Nous introduisons aussi l'intérêt d'un algorithme quantique qui sert à la décomposition en facteurs premiers, ainsi qu'un état de l'art des ordinateurs quantiques qui y sont associés. Nous définissons les protocoles de cryptographie quantique que nous proposons d'utiliser.

Dans un troisième chapitre, nous faisons une description du matériel disponible. L'accent est mis sur ses limitations de manière à pouvoir en tirer une modélisation réaliste.

Le quatrième chapitre est consacré à l'attaque par détournement de photon surnuméraire appelé en anglais « Photon Number Splitting Attack ». L'idée est d'utiliser à la fois le taux d'erreur quantique et la statistique de détection pour atteindre une sécurité élevée.

Enfin le cinquième chapitre traite des attaques sur un protocole utilisant de la détection homodyne à double seuil. Les attaques envisagées sont l'attaque par interception et renvoi, l'attaque par utilisation de la base de Breidbart, et l'attaque par vol de photons surnuméraires.

Chapitre 1

Sécurité et cryptographie

La cryptographie est une discipline qui a évolué depuis l'antiquité. Différentes approches de la sécurité ont été envisagées au cours des siècles. La cryptographie est alors devenue une science grâce aux intérêts militaire, politique, religieux et financier qu'elle a suscitée et à la qualité des personnalités qui s'y sont successivement intéressées. De nos jours, la cryptographie moderne est devenue un domaine de recherche d'intérêt stratégique pour la sécurisation des données et des transmissions.

Dans ce chapitre nous définissons d'abord quelques termes et notations importantes. Ensuite nous décrivons l'évolution de la cryptographie au cours du temps jusqu'à la cryptographie moderne.

1.1 Définitions et terminologie

1.1.1 Définitions

Étymologiquement, le mot cryptographie est composé du grec κρυπτος *caché* et de γραφν *lire*, ce qui nous amène à concevoir la cryptographie comme l'art de communiquer en langage secret. Plus précisément, on appelle cryptographie l'étude de la création de messages chiffrés appelés aussi cryptogrammes.

Le plus souvent, le chiffrement d'un message se fait à partir d'un algorithme ou chiffre, et d'une clef. Déchiffrer est alors l'opération qui consiste à retrouver le message initial à l'aide de la clef et décrypter, une opération qui consiste à retrouver le message initial sans la clef. La science qui traite du décryptage est appelée cryptanalyse. Les domaines de la cryptographie et de la cryptanalyse forment la cryptologie.

Notons également que la stéganographie est l'art de cacher un message dans un autre objet. Évidemment, on peut faire usage de cryptographie et de stéganographie pour un même message, ce qui revient à cacher simultanément l'existence du message et à en rendre le contenu inintelligible pour un tiers.

1.1.2 Terminologie

Les intervenants des opérations de cryptologie sont toujours désignés par les même prénoms. Bruce Shneier a recensé les plus utilisés [37]. Alice et Bob sont les opérateurs de bonne foi du système cryptologique, et Ève en est l'attaquante. Ainsi, le plus souvent Alice souhaite envoyer un message à Bob sans qu'un tiers, Ève, ne puisse apprendre une quelconque information sur ce message. Dans ce manuscrit, nous n'utiliserons que ces trois acteurs.

1.2 Historique

1.2.1 Première utilisation de communication sécurisée

La sécurisation des transmissions d'information a été très tôt reconnue comme très importante. Le plus ancien usage de cet art nous est rapporté par Hérodote [20] qui relate entre autres les différends entre la Perse et la Grèce au V^{e} siècle av J-C. Démarate, roi de Sparte exilé en Perse a réussi à prévenir la Grèce, au moyen d'un ingénieux procédé, de l'imminence d'une invasion perse et a permis ainsi d'éviter une catastrophe pour les grecs.

1.2.2 Chiffre de César

Quelques siècles plus tard, Jules César a également utilisé un procédé de sécurisation de données. Il utilise un chiffre qui consiste simplement à décaler les lettres dans l'alphabet.

```
CECI EST UN MANUSCRIT DE THESE
```

Ainsi, en utilisant un chiffre qui consiste à décaler de trois lettres de manière analogue au procédé de Jules César, nous obtenons le cryptogramme suivant.

```
FHFL HVW XP QDPXVFULW GH WKHVH
```

Le chiffre de César n'est pas sûr car il est vulnérable à une attaque utilisant la fréquence d'usage des lettres, propre à une langue. En français la lettre la plus utilisée est le « e ». En considérant que la lettre la plus utilisée dans le cryptogramme correspond à la lettre la plus utilisée en français, on a une grande chance d'obtenir la mesure du décalage de la lettre « e » et la clef de chiffrement. Dans le cryptogramme précédent, nous observons cinq occurences de la lettre « H », et c'est effectivement le chiffré de la lettre « E ».

1.2.3 Chiffre de Vigenère

Pour pallier au problème généré par le chiffre de César, les cryptographes ont imaginé utiliser un décalage différent pour chaque lettre du message à transmettre.

Un chiffrement intéressant a été développé par Battista aux alentours de 1467 après Jésus-Christ, bien qu'il fut plus tard attribué à Vigenère. Il utilise un procédé analogue à celui de César, mais change de décalage pour chaque caractère du message, suivant une clef choisie préalablement par les protagonistes de la communication. Il constitue donc un chiffre par substitution polyalphabétique.

Supposons qu'Alice et Bob disposent d'une clef composée de p caractères. Pour chiffrer m_n, le n$^{\text{ième}}$ caractère du message m, il suffit d'effectuer l'opération $c_n \equiv m_n + k_{n \bmod p} \bmod 26$. De manière pratique le chiffrement et le déchiffrement s'effectuent grâce au tableau 1.1 qui est appelé carré de Vigenère. La première ligne sert à choisir le caractère en clair à chiffrer, et la première colonne le caractère clef à utiliser. Le caractère chiffré se trouve alors à l'intersection de ces deux lignes. Ce procédé permet ainsi de déterminer le caractère chiffré à partir du caractère clair et de la clef ou grâce à une opération inverse, de déterminer le caractère clair à partir du caractère chiffré et de la clef

Ainsi dans notre exemple, nous recevons dans un message un caractère « J », sachant que la clef correspondante est « H ». Le caractère déchiffré est « Q ».

Le défaut principal de cette nouvelle méthode de chiffrement, est la longueur limitée de la clef. Comme la clef est plus courte que le message, elle se trouve répétée. Ainsi l'attaquant peut essayer de déterminer la longueur de la clef grâce à des répétitions de certains motifs dans le message chiffré. En effet, lorsque dans le texte chiffré, on peut retrouver plusieurs fois le même motif, il est fort probable que ce soit le même texte clair qui en soit à l'origine. Cela permet de déduire un multiple du nombre de caractères de la clef. Une fois la longueur de la clef connue, une attaque en fréquence analogue au chiffre de César est possible.

Nous présentons un exemple de chiffrement de Vigenère ci-après. Nous avons chiffré la phrase « DISTRIBUTION QUANTIQUE DE CLEF POUR CRYPTOGRAPHIE QUANTIQUE » par la clef « BLEU ». Le cryptogram-

Caractères de la clef \ Caractères du message	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

FIG. 1.1 – Carré de Vigenère

me est présenté sur la troisième ligne, et l'alignement des caractères est présenté sur la quatrième ligne.

```
DISTRIBUTION QUANTIQUE DE CLEF POUR CRYPTOGRAPHIE QUANTIQUE
BLEUBLEUBLEU BLEUBLEUB LE UBLE UBLE UBLEUBLEUBLEU BLEUBLEUB
ETWNSTFOUTSH RFEHUTUOF OI WMPJ JPFV WSJTNPRVUQSMY RFEHUTUOF
123456789012 345678901 23 4567 8901 2345678901234 567890123
```

Ici on peut remarquer que le motif « `RFEHUTUOF` »est répété deux fois, il est donc probable que nous soyons en présence du même texte clair. En remarquant qu'il y a vingt-quatre caractères entre les deux occurences de « `RFEHUTUOF` », nous pouvons conclure que la longueur de la clef divise vingt-quatre. D'après le placement du premier motif douze caractères après le début de la séquence, nous pouvons en déduire que la longueur de la clef divise douze. Nous pourrions regrouper les caractères composant le chiffré en douze groupes de lettres, chaque groupe étant chiffré à l'aide du même caractère de la clef pour en effectuer une attaque en fréquence analogue à celle du chiffre de César.

1.2.4 Enigma et le début de la cryptographie moderne

1.2.4.1 Description d'Enigma

Après la première guerre mondiale, Arthur Scherbius, aidé de son ami Richard Ritter, invente un système révolutionnaire de chiffrement. Le but est de s'affranchir du passé, et de faire oublier l'humiliation cryptographique allemande de la première guerre mondiale. Il invente un procédé automatisé qui ne nécessite plus aucun calcul des protagonistes. L'appareil est complètement électromécanique. Il est doté d'un clavier ainsi que d'un jeu de vingt-six ampoules en guise d'interface avec l'utilisateur. Pour l'opération de chiffrement, il suffisait d'entrer un caractère au clavier et une lumière correspondant au caractère chiffré s'allumait. La figure 1.2 est une photographie d'une machine Enigma[1].

La machine Enigma est composée pour ses versions courantes de trois rotors et d'un réflecteur. La figure 1.3 est une photographie des rotors en place dans une machine Enigma[1]. Chaque rotor possède vingt-six contacts sur chacune des deux faces dont les raccordements internes sont propres à la conception de la machine. À chaque fois que l'opérateur appuie sur une touche du clavier, les rotors tournent d'un cran, et changent les contacts entre chaque rotor. Le réflecteur permet de renvoyer le signal de manière à ce qu'il fasse un aller-retour et traverse deux fois chaque rotor. Sur notre schéma de principe présenté en figure 1.4, ne sont représentés, pour des raisons de simplicité, que quatre caractères et deux rotors. À titre d'exemple, le trajet effectué par le signal lorque l'opérateur appuie sur la touche B

[1] Emprunté à **http ://www.ilord.com**

FIG. 1.2 – Photo d'une machine Enigma

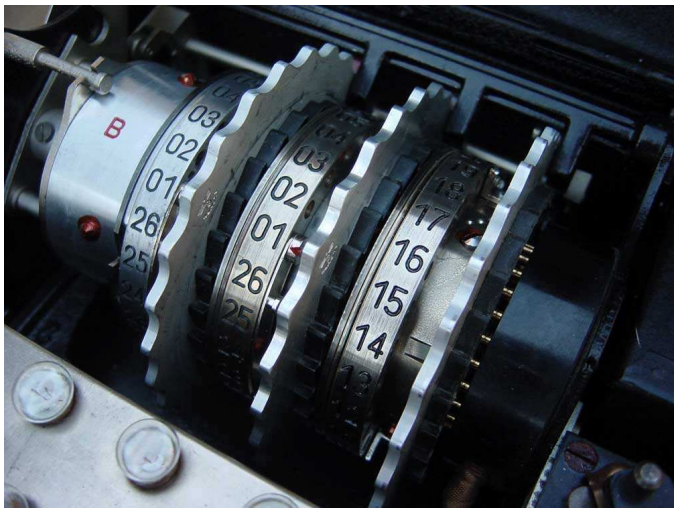

FIG. 1.3 – Photo des rotors dans une machine Enigma

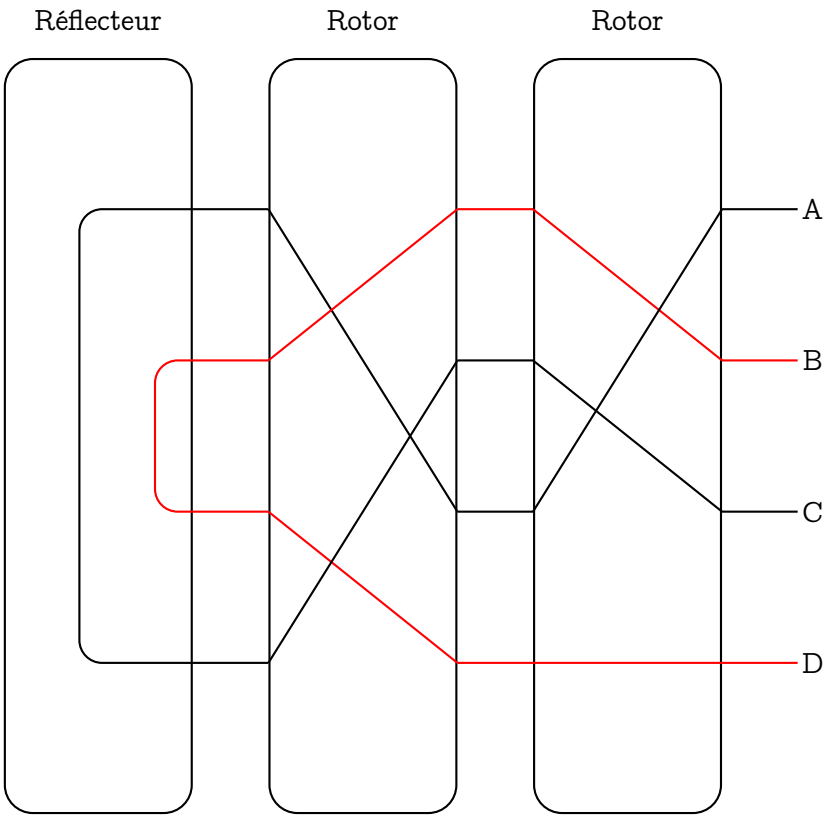

Fig. 1.4 – Principe d'Enigma

a été représenté en rouge. L'opérateur obtient D comme caractère chiffré. Pour effectuer l'opération de déchiffrement l'opérateur n'a qu'à appuyer sur la touche correspondant au caractère chiffré pour obtenir ainsi le caractère déchiffré.

Pour augmenter la sécurité d'Enigma, l'armée allemande changeait quotidiennement la position initiale des rotors ainsi que le raccordement du clavier au premier rotor. Un carnet contenant toutes ces informations pour chaque jour du mois était édité tous les mois et envoyé à tous les opérateurs de machine Enigma.

1.2.4.2 Décryptage d'Enigma

Après la première guerre mondiale, un « bureau du chiffre » fut créé à Varsovie. Les cryptologues de ce nouveau bureau ont largement contribué aux victoires polonaises de la guerre russo-polonaise de 1919-1920. Lors de

l'entrée en vigueur d'Enigma dans les années 30, ils décidèrent donc de s'attaquer au décryptage d'Enigma.

La difficulté est d'obtenir le cablage interne de la machine allemande, et les codes d'initialisation du jour. Marian Rejewsky a eu l'idée d'une approche mathématique du problème. Il commence par remarquer que dans chaque message les trois premiers caractères sont répétés deux fois. Se doutant qu'il s'agit là d'un paramètrage permettant d'initialiser la machine pour déchiffrer le message qui suit, il se base sur cette faiblesse pour son décryptage. Après avoir obtenu un schéma de cablage interne par les services d'espionnage français, il construit une machine életromécanique qu'il appelle « bombe » dont il se sert pour faire une recherche exhaustive des paramètres d'initialisation. Cela lui permet chaque jour, d'obtenir les paramètres du jour en moins de deux heures. À la veille de l'invasion de la Pologne par l'Allemagne, le bureau du chiffre polonais transmet à la France et à l'Angleterre tous les plans et toutes les reflexions qui avaient été menées sur le décryptage du chiffrement d'Enigma.

1.2.5 Shannon et la sécurité inconditionnelle

1.2.5.1 Information mutuelle et entropie de Shannon

i. Information mutuelle

Pour étudier et comparer les systèmes cryptograhiques, nous avons besoin d'un modèle mathématique de l'information. Considérons pour ce faire deux variables $x_i \in \{x_1, x_2, \cdots, x_n\}$ et $y_j \in \{y_1, y_2, \cdots, y_m\}$. Nous souhaitons déterminer quantitativement l'information que donne l'événement $Y = y_j$ sur l'événement $X = x_i$. Si X et Y sont statistiquement indépendants nous pouvons raisonnablement postuler que ces variables ne partagent pas d'information. Si maintenant X et Y sont si statistiquement liés que l'événement $Y = y_j$ détermine l'événement $X = x_i$, l'information est simplement celle contenue dans l'événement $X = x_i$. Sachant que $P(x_i|y_j)$ est la probabilité conditionnée par l'événement $Y = y_i$ de l'événement $X = x_i$, une mesure de cette information vérifiant ces conditions est donnée par [24, 54] :

$$I(x_i, y_j) = \log_2 \frac{P(x_i|y_j)}{P(x_i)} \tag{1.1}$$

En effet, dans le cas ou X et Y sont statistiquement indépendants $P(x_i|y_j) = P(x_i)$ et il vient $I(x_i, y_j) = 0$. Si X et Y sont statistiquement liés $P(x_i|y_j) = 1$ et il vient $I(x_i, y_j) = -\log_2(P(x_i))$. L'information n'est contenue que dans l'événement x_i : c'est une auto-information.

La quantité $I(x_i, y_j)$ est appelée information mutuelle entre x_i et y_j. L'unité utilisée pour mesurer l'information dépend uniquement de la base du logarithme utilisé. Dans ce manuscrit, nous avons fait le choix de mesurer les informations mutuelles en bit, le logarithme est donc utilisé en base deux.

Si on calcule l'espérance de notre expression d'information mutuelle, nous obtenons une information mutuelle moyenne qui nous donne une mesure de l'information sur X que nous donne la connaissance de Y.

$$\begin{aligned} I(X,Y) &= E\left(\log_2 \frac{P(X|Y)}{P(X)}\right) \\ &= \sum_{x,y} \log_2 \frac{P(x|y)}{P(x)} \end{aligned} \tag{1.2}$$

Dorénavant, nous utiliserons l'expression 1.2 comme définition de l'information mutuelle.

ii. Entropie de Shannon

Considérons l'espérance de l'information mutuelle :

$$\begin{aligned} I(X,Y) &= \sum_{x,y} P(x,y) \log_2 \frac{P(x|y)}{P(x)} \\ &= -\sum_{x,y} P(x,y) \log_2 P(x) + \sum_{x,y} P(x,y) \log_2 P(x|y) \\ &= -\sum_{x} P(x) \log_2 P(x) + \sum_{x,y} P(x,y) \log_2 P(x|y) \\ &= H(X) - H(X|Y) \end{aligned} \tag{1.3}$$

Cette expression définit l'entropie de Shannon qui est une mesure de l'incertitude d'un événement donné. Nous pouvons noter que $H(X)$ est la même expression que l'auto-information précédemment définie.

Ce qui nous donne comme définition :

$$H(X) = -\sum_{x} P(x) \log_2 P(x) \tag{1.4}$$

De la même manière :

$$H(Y|X) = -\sum_{x,y} P(x,y) \log_2 P(y|x) \tag{1.5}$$

Sachant que que $\ln(x) \leqslant x - 1$ on peut démontrer que $H(X) \geqslant 0$ et que $H(Y|X) \geqslant 0$.

1.2.5.2 Chiffrement de Vernam

Shannon [38] décrit à l'aide d'une approche scientifique la sécurité des systèmes. Il décrit un système cryptographique comme trois ensembles $\mathcal{M}$, $\mathcal{K}$ et $\mathcal{E}$ qui représentent respectivement l'ensemble des messages en clair,

l'ensemble des clefs et l'ensemble des cryptogrammes dans lesquel un message clair M et une clef K engendre un cryptogramme E. La nouveauté de Shannon est de traiter M,K et E comme des variables aléatoires. Notons m la taille de l'alphabet utilisé (par exemple $m = 26$ pour l'alphabet usuel ou encore $m = 2$ pour un alphabet composé de 1 et 0). Nous notons n la longueur du message à chiffrer.

Il commence par analyser le chiffrement de Vernam (1 926). Dans ce système les ensembles $\mathcal{M}$, $\mathcal{K}$ et $\mathcal{E}$ sont identiques. Un message $M = (x_1, x_2, \cdots, x_n)$ est transformé en un chiffré $E = (y_1, y_2, \cdots, y_n)$ par la méthode suivante en utilisant une clef k_i qui est une réalisation de k :

$$\forall i \in \mathbb{N}, \text{ tel que } i \leq n, y_i = x_i + k_i \bmod m \tag{1.6}$$

Notons dès à présent que la méthode employée est analogue au chiffrement de Vigenère à l'unique différence près, qu'ici la longueur de la clef est nécéssairement égale à la longueur du message transmis.

1.2.5.3 Sécurité inconditionnelle

Ève peut essayer de calculer la probabilité de réalisation d'un message connaissant le cryptogramme transmis $p(M|E)$. L'interception du message ne doit donc donner aucune information à Ève. En terme d'entropie de Shannon, cela revient à écrire que la connaissance d'un cryptogramme n'apporte aucune information sur le message clair dont il est issu.

$$H(M|E) = H(M) \Longleftrightarrow I(M, E) = 0 \tag{1.7}$$

i. Cas du chiffre de Vernam

Montrons tout d'abord que le chiffre de Vernam est inconditionnellement sûr. Nous avons ici $\mathcal{M} = \mathcal{K} = \mathcal{E} = \{0, 1\}^n$ avec n la longueur du message. La variable aléatoire K est équidistribuée, $p(K = k) = \frac{1}{n}$. Le chiffrement est effectué par la relation :

$$E = M \oplus K \tag{1.8}$$

Lorque Ève intercepte un cryptogramme $y \in \mathcal{E}$, elle en est réduite à vérifier que chaque valeur x du message est possible puisque $y - x$ est une clef possible.

$$p(M = x|E = y) = \frac{p(M = x, E = y)}{p(E = y)} \tag{1.9}$$

Ici, $p(M = x|E = y)$ est la probabilité conditionnelle que l'événement $M = x$ survienne, alors que l'événement $E = y$ est réalisé. De la même manière

$p(M = x, E = y)$ est la probabilité conjointe des événements $M = x$ et $E = y$. Pour calculer 1.9 nous allons calculer $p(M = x, E = y)$ et $p(E = y)$.

$$\begin{aligned} p(M = x, E = y) &= p(M = x, K = y - x) \\ &= p(M = x)p(K = y - x) \\ &= \frac{1}{n}p(M = x) \end{aligned} \tag{1.10}$$

$$\begin{aligned} p(E = y) &= \sum_x p(E = y|M = x)p(M = x) \\ &= \sum_x p(K = y - x)p(M = x) \\ &= \frac{1}{n}\sum_x p(M = x) \\ &= \frac{1}{n} \end{aligned} \tag{1.11}$$

Les équations 1.9, 1.11 et 1.10 nous permettent de déduire :

$$p(M = x|E = y) = p(M = x) \tag{1.12}$$

Il vient ensuite que $H(M|E) = H(M)$. On retrouve la condition 1.7, et le chiffre de Vernam est inditionnellement sûr.

ii. Propriété des systèmes inconditionnellement sûrs

Nous savons, d'après la définition de l'information mutuelle et de l'entropie, que :

$$I((M, K)|E) = H(M|E) - H(K|(M, E)) \tag{1.13}$$

où nous avons noté (M, K) la variable aléatoire constituée du couple des variables aléatoires M et K. Comme les entropies sont positives nous pouvons écrire que :

$$\begin{aligned} H(M|E) &\leqslant I((M, K)|E) \\ &\leqslant H(K|E) - H(M|(K, E)) \end{aligned} \tag{1.14}$$

Or il nous apparaît que $H(M|(K, E)) = 0$ car l'information de la clef et du cryptogramme doit renseigner sur le message. L'expression précédente peut donc se simplifier.

$$\begin{aligned} H(M|E) &\leqslant H(K|E) \\ &\leqslant H(K) \end{aligned} \tag{1.15}$$

Ce résultat est vrai quel que soit le système cryptographique que nous étudions. Par contre, si ce système est parfait, et vérifie la condition de Shannon afférente alors ce résultat peut encore se simplifier.

$$H(M) \leqslant H(K) \tag{1.16}$$

L'information que donne la connaissance de la clef doit être au moins aussi grande que l'information liée à la connaissance de message. Donc si les messages sont équiprobables, le nombre de caractères de la clef doit être au moins supérieur au nombre de caractères du message. Il n'est donc pas possible d'obtenir une meilleure efficacité que le chiffrement de Vernam.

1.2.6 Chiffrement à clef symétrique

Le principe de base est très simple. Dans un procédé cryptographique classique il est très rare que les deux protagonistes Alice et Bob possèdent une clef partagée au moins aussi longue que les messages qu'ils doivent s'envoyer.

Alice et Bob disposent d'une clef partagée qu'ils utilisent pour chiffrer et déchiffrer leur correspondance. Ainsi quand Alice envoie un cryptogramme à Bob à l'aide d'une clef K, celui-ci utilise la même clef K pour déchiffrer le message d'Alice.

Pour ce type de chiffrement, on distingue deux grandes méthodes de chiffrement : les chiffrements par flot qui fonctionnent bit après bit sur le modèle de Vigenère ou de Vernam et les chiffrements par blocs, qui lorsqu'on leur donne n bits fournissent un cryptogramme de n bits.

1.2.6.1 Chiffrement par flot

L'idée est ici de générer par un algorithme une clef aussi longue que le message et de l'ajouter au message par exemple par une opération ou exclusif exactement à la manière du chiffre de Vernam. Cette clef est générée à partir d'une clef maître K dont la longueur conditionne la sécurité du chiffrement.

1.2.6.2 Chiffrement par blocs

Pour ce type de chiffrement, on utilise un bloc de taille n en entrée pour produire un bloc de taille identique n en sortie. Pour cela on utilise des fonctions de substitutions et de permutations (ou transpositions) sur un mode itératif. Prenons l'exemple de DES (Data Encryption Standard), qui est resté une norme jusqu'en 1998 [54].

Soient $\mathcal{M} = \mathcal{E} = \{0,1\}^{2n}$. Les ensembles $\mathcal{M}$ et $\mathcal{E}$ sont respectivement l'ensemble des messages et l'ensemble des cryptogrammes. Chaque message est décomposé en deux blocs L et R, tel que $M = (L, R)$ avec L et R éléments de $\{0,1\}^n$. On choisit la clef K de manière à ce qu'elle puisse être décrite

de la manière suivante $K = \{K_1, K_2, \cdots, K_d\}$ avec $K_i \in \{0,1\}^k$. On utilise une application F :

$$F : \{0,1\}^{k+n} \rightarrow \{0,1\}^n$$

Le cryptogramme E est défini de manière récursive par :

$$\begin{aligned} (L_0, R_0) &= (L, R) \\ L_i &= R_{i-1} \\ R_i &= L_{i-1} \oplus F(K_i, R_{i-1}) \end{aligned}$$

Le nombre de récursions est limité à d.

Pour déchiffrer le résultat (L_d, R_d), il suffit d'inverser les équations précédentes.

$$\begin{aligned} R_{i-1} &= L_i \\ L_{i-1} &= R_i \oplus F(K_i, L_i) \end{aligned}$$

On note qu'il n'est pas nécessaire d'inverser F pour déchiffrer. Dans la norme DES, $n = 32$, $k = 48$ et $d = 16$. Le vecteur K est généré à partir d'une clef maître de 56 bits. La fonction F est un produit d'une application linéaire avec une fonction de substitution. L'algorithme de chiffrement AES (Advanced Encryption Standard) est appelé à remplacer le vieillissant DES, qui, à cause de la faible taille de la clef, semble vulnérable à des attaques par force brute. Une attaque par force brute est une attaque où l'on effectue l'algorithme de chiffrement avec toutes les clefs les unes après les autres, jusqu'à obtenir le cryptogramme à décrypter.

1.2.7 Chiffrement à clef asymétrique

Ici Alice et Bob disposent tous deux d'une clef privée et d'une clef publique. La clef publique est mise à disposition de tout le monde à l'aide par exemple d'un serveur de clefs, alors que la clef privée doit absolument rester secrète pour son utilisateur.

Pour chiffrer un message qu'elle doit envoyer à Bob, Alice utilise la clef publique de Bob. Une fois que Bob réceptionne le cryptogramme d'Alice, Bob utilise sa clef privée pour déchiffrer le message.

Pour authentifier un message qu'elle doit envoyer à Bob, Alice utilise sa clef privée pour créer une empreinte du message qu'elle envoie à Bob. Bob utilise la clef publique d'Alice pour vérifier que l'empreinte d'Alice correspond bien à sa clef privée.

Dans ce système le plus gros souci est la confiance dans la clef publique. En effet, pour éviter une attaque où un tiers Ève injecte sa propre clef publique à la place d'Alice ou de Bob, Alice et Bob doivent se rencontrer pour échanger leurs clefs publiques en vérifiant leur identité.

Prenons l'exemple de l'algorithme RSA du nom de ses inventeurs, Rivest, Shamir et Adleman. Cet algorithme se base sur le théorème d'Euler-Fermat qui démontre que pour deux nombres premiers p et q et pour x premier avec $N = pq$ alors

$$x^{(p-1)(q-1)} \equiv 1 \bmod N. \tag{1.17}$$

La clef publique est composée d'un couple (N, e). La clef privée est composé du couple (N, d) tel que[2] $ed = (p-1)(q-1)+1$. Si m est le message à transmettre, Alice calcule et envoie :

$$y \equiv m^e \bmod N \tag{1.18}$$

Pour déchiffrer y, Bob n'a qu'à calculer :

$$\begin{aligned} m &\equiv y^d \bmod N \\ &\equiv m^{ed} \bmod N \end{aligned} \tag{1.19}$$

Dans le cas ou Bob cherche à envoyer un message authentifié à Alice il attache au message qu'il envoie à Alice le résultat du calcul suivant :

$$y \equiv m^d \bmod N \tag{1.20}$$

Pour vérifier que la signature émane de Bob, Alice effectue l'opération suivante :

$$\begin{aligned} m &\equiv y^e \bmod N \\ &\equiv m^{ed} \bmod N \end{aligned}$$

Si elle obtient une copie du message, elle est sûre que celui-ci émane de Bob. La sécurité de ce système est basé sur le fait que si p et q sont choisis suffisament grands, alors il est rhédibitoire en temps de calcul de chercher la décomposition en facteurs premiers de l'entier N. En effet, les algorithmes de décompositions en facteurs premiers d'un nombre N ont un temps de calcul exponentiel avec le nombre de digits de N.

[2]Pour des raisons de simplicité je n'ai pas pris en compte le fait qu'il s'agit ici d'une congruence modulo N. L'esprit de l'algorithme est néanmoins respecté

Chapitre 2

Bases mathématiques et introduction à la cryptographie quantique

La mécanique quantique est une théorie élaborée pour expliquer des phénomènes à des échelles très réduites. La continuité des dimensions physiques ne peut plus être un postulat, et l'hypothèse de quantification des grandeurs s'impose alors.

Dans ce chapitre, nous commençons par définir quelques grandeurs de mécanique quantique dont nous aurons besoin plus tard. Ensuite, nous appréhendons des systèmes quantiques plus complexes comme un ordinateur

quantique. Enfin, nous nous intéressons à la cryptographie quantique au travers une implémentation du protocole BB84 et de quelques réflexions sur sa sécurité.

2.1 Notions de mécanique quantique

2.1.1 Historique

À la fin du XIX^{e} siècle, deux types de mécanisme physique étaient étudiés. Il y avait la mécanique newtonienne dont on se servait pour décrire les mouvements et la théorie de l'électromagnétisme, qui proposait une explication globale des phénomènes tels que l'électricité, le magnétisme et l'optique. L'interaction entre rayonnement et matière s'expliquait aisément à l'aide de la force de Lorentz.

Au début du XX^{e} siècle, la physique subit de profonds changements, avec l'avènement de la théorie relativiste, où les lois classiques cessent d'être valables pour des corps matériels animés de vitesses proches de la vitesse de la lumière et de la théorie quantique quand les corps considérés sont à l'échelle atomique voire sub-atomique. Notons néanmoins que la théorie classique préexistante reste une approximation valable de ces nouvelles théories aux échelles courantes.

2.1.2 Quantification

Pendant la première moitié du XIX^{e} siècle la lumière était considérée comme ondulatoire, ce qui permettait d'expliquer nombre de phénomènes tels qu'interférences et diffractions. L'optique entrait donc dans la théorie électromagnétique.

Le rayonnement du corps noir, inexpliqué par la théorie électromagnétique, amena Planck à considérer une quantification des échanges d'énergie. Ainsi, seules les multiples de $h\nu$ sont acceptables comme énergie pour une onde électromagnétique de fréquence ν, la constante h était alors une nouvelle constante fondamentale. C'est Einstein qui proposa une nouvelle théorie corpusculaire finalisée, dans laquelle la lumière est composée de quantums d'énergie $h\nu$. Cela permit également d'apporter une interprétation simple du phénomène photoélectrique jusqu'alors inexpliqué.

On définit h comme la constante de Planck :

$$h \equiv 6\ .62\ 606\ 896 \cdot 10^{-34} Js \tag{2.1}$$

Et on définit également la constante de Planck réduite $\hbar$ par $\hbar = \frac{h}{2\pi}$. C'est Lewis, qui le premier introduit le terme photon dans un article publié dans *Nature* en décembre 1926.

2.1.3 Fonction d'onde

En mécanique quantique, si on cherche à étudier une particule quelconque, il faut substituer au concept classique de trajectoire celui d'un état dépendant du temps. Ainsi l'état quantique est caractérisé par une fonction d'onde $\psi(\vec{r},t)$, qui contient toutes les informations disponibles sur la particule. $\vec{r}$ et t matérialisent la dépendance de la fonction d'onde vis à vis de la position et du temps. $\psi(\vec{r},t)$ est appelée amplitude de probabilité alors que $|\psi(\vec{r},t)|^2$ forme une densité de probabilité.

L'évolution dans le temps de la fonction d'onde d'une particule placée à un potentiel $V(\vec{r})$ est régi par l'équation de Schrödinger.

$$i\hbar\frac{\partial}{\partial t}\psi(\vec{r},t) = \hat{H}\psi(\vec{r},t) \tag{2.2}$$

L'opérateur $\hat{H}$ est appelé hamiltonien du système.

$$\hat{H} = -\frac{\hbar^2}{2m}\Delta + V(\vec{r}) \tag{2.3}$$

2.1.4 Formalisme de Dirac

Une des propriétés des fonctions d'onde est d'appartenir à un espace de Hilbert $\mathcal{E}_H$. Par exemple, pour une particule en mouvement dans l'espace, $\mathcal{E}_H$ est l'espace des fonctions de carré sommable définies sur $\mathbb{R}^3$. La description de l'état fournie par cette fonction d'onde n'est pas unique. Une représentation équivalente de cette fonction d'onde peut par exemple être donnée par sa transformée de Fourier.

Dirac a proposé une écriture équivalente aux fonctions d'onde. Il propose de décrire les états par des vecteurs d'état. À la fonction d'onde $\psi(\vec{r},t)$ on associe un vecteur qu'on appelle le ket $|\psi(t)\rangle$ qui appartient à un espace des états $\mathcal{E}$ isomorphe à l'espace de Hibert $\mathcal{E}_H$. Cette notation va s'avérer très commode pour les manipulations formelles que nous aurons à faire. L'espace de Hilbert $\mathcal{E}_H$ est muni d'un produit scalaire hermitien $(\psi_1(\vec{r},t),\psi_2(\vec{r},t)) = (\psi_2(\vec{r},t),\psi_1(\vec{r},t))^\star$ dont la représentation dans l'espace des états $\mathcal{E}$ est donnée par :

$$\langle\psi_1(t)|\psi_2(t)\rangle = \langle\psi_2(t)|\psi_1(t)\rangle^\star \tag{2.4}$$

La construction du premier membre $\langle\psi_1(t)|$ est analogue à celle d'un ket, on appelle $\langle\psi_1(t)|$ un bra. En raison de l'interprétation probabiliste, les vecteurs d'état sont considérés normés.

$$\langle\psi(t)|\psi(t)\rangle = 1 \tag{2.5}$$

2.1.5 Principe d'une mesure

Soit une grandeur physique $\mathcal{A}$ que l'on souhaite mesurer. Cette grandeur physique est décrite par un opérateur A agissant sur $\mathcal{E}$. Nous considérons que

$|\Psi\rangle$ est le vecteur d'état dont dont on souhaite mesurer la grandeur physique $\mathcal{A}$. L'étude des états stationnaires solutions de l'équation de Schrödinger conduit à postuler [14] :

- Chaque mesure ne peut conduire qu'à une valeur propre de l'opérateur A.
- On obtient à l'aide d'un opérateur A la valeur propre a_n avec la probabilité $\mathcal{P}(a_n)$ suivante :

$$\mathcal{P}(a_n) = |\langle u_n|\psi\rangle|^2 \tag{2.6}$$

  où u_n est le vecteur propre correspondant à la valeur propre a_n de l'opérateur A associé à $\mathcal{A}$. On peut donc décomposer $|\psi\rangle$ dans le cas où a_n est non-dégénérée sur la base de $\{u_n\}$ tel que $|\psi\rangle = \sum_n a_n|u_n\rangle$. Si $\{u_n\}$ est une base de $\mathcal{E}$ alors cet opérateur est appelé une observable.
- Si la mesure de la grandeur physique $\mathcal{A}$ donne le résultat a_n alors l'état du système est la projection normée de ψ sur le sous-espace propre associé à a_n :

$$\frac{|u_n\rangle\langle u_n|\psi\rangle}{\sqrt{\langle\psi|u_n\rangle\langle u_n|\psi\rangle}} = \frac{|u_n\rangle\langle u_n|\psi\rangle}{|\langle u_n|\psi\rangle|} \tag{2.7}$$

Définissons $\langle A\rangle$ comme la moyenne des mesures d'une observable donnée. Lorsque l'on effectue la mesure d'une observable A sur un grand nombre N de systèmes identiques, la probabilité d'apparition de la valeur propre a_n s'approche de $\mathcal{P}(a_n)$. Notons $\mathcal{N}(a_n)$ le nombre de fois qu'on obtient la valeur propre a_n sur N mesures.

$$\lim_{N\to+\infty} \frac{\mathcal{N}(a_n)}{N} = \mathcal{P}(a_n) \tag{2.8}$$

Considérons la valeur moyenne $\langle A\rangle$ de ces N expériences.

$$\langle A\rangle = \frac{1}{N}\sum_{n=1}^{N} a_n\mathcal{N}(a_n) \tag{2.9}$$

Grâce à l'equation 2.8, et en faisant tendre N vers l'infini nous pouvons déduire[1] que

$$\begin{aligned}\langle A\rangle &= \sum_n a_n \mathcal{P}(a_n) \\ &= \sum_n a_n |\langle\psi|u_n\rangle|^2 \\ &= \sum_n a_n \langle\psi|u_n\rangle\langle u_n|\psi\rangle \\ &= \langle\psi|A\left(\sum_n |u_n\rangle\langle u_n|\right)|\psi\rangle \\ &= \langle\psi|A|\psi\rangle \end{aligned} \tag{2.10}$$

Au cours du calcul nous voyons apparaître l'opérateur $\sum_n |u_n\rangle\langle u_n|$. Nous remarquons que $|u_j\rangle\langle u_j|$ est l'opérateur projection sur l'état $|u_j\rangle$, $\sum_n |u_n\rangle\langle u_n|$ représente donc la somme des projecteurs sur tous les vecteurs de la base de notre espace de Hilbert, c'est-à-dire l'identité. Nous avons montré que la valeur moyenne des mesures d'une observable A d'un état $|\psi\rangle$ est donnée par $\langle\psi|A|\psi\rangle$.

2.1.6 Qubit

2.1.6.1 Bit classique

Le plus petit élément d'information dans un système d'information classique est le bit. Il peut communément prendre exclusivement les valeurs 0 ou 1 avec respectivement les probabilités $p(0)$ ou $p(1)$. Notons que les propriétés des probabilités exigent que $p(0) + p(1) = 1$. Mais l'état initial était 0 ou 1, et la mesure ne nous permet que d'acquérir cette valeur. En dehors des défauts inhérents à l'appareil de mesure, cette mesure ne modifie pas l'état du bit. Un ensemble de n bits correspond donc à un espace de dimension n.

2.1.6.2 Definition du qubit

Dans un système quantique, l'information est contenue dans une superposition d'état. Un système binaire analogue aux systèmes binaires classiques usuels peut être décrit sous la forme suivante :

$$|QuBit\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2.11}$$

On appelle α et β les amplitudes de probabilité correspondant aux états $|0\rangle$ et $|1\rangle$. Lors de la mesure de notre $|QuBit\rangle$ nous pouvons obtenir $|0\rangle$ avec une probabilité $|\alpha|^2$ ou $|1\rangle$ avec une probabilité $|\beta|^2$. Après la mesure l'état du

[1] Notons que nous avons, pour des raisons de simplicité, réduit ce calcul au cas simple non dégénéré.

$|QuBit\rangle$ est modifié et devient l'état mesuré. Et de même que précédemment pour le système classique, la somme des probabilités doit aussi ici égaler l'unité.

$$|\alpha|^2 + |\beta|^2 = 1 \tag{2.12}$$

La structure du qubit permet à un ensemble de n qubits de correspondre à un espace de dimension 2^n.

2.1.6.3 Sphère de Bloch

Nous avons représenté une sphère de Bloch sur la figure 2.1. La sphère de Bloch est un moyen commode de représenter géométriquement un qubit. En effet, nous pouvons décrire un qubit de la manière suivante :

$$|QuBit\rangle = \cos\theta|0\rangle + e^{i\phi}\sin\theta|1\rangle \tag{2.13}$$

Pour avoir une représentation unique (sauf pour $|0\rangle$ ou $|1\rangle$) nous pouvons nous restreindre à $\phi \in [0; 2\pi[$ et $\theta \in [0; \frac{\pi}{2}[$. La correspondance avec les points de la sphère unité est donnée par :

$$\begin{aligned} x &= \sin(2\theta)\cos\phi \\ y &= \sin(2\theta)\sin\phi \\ z &= \cos(2\theta) \end{aligned}$$

$|0\rangle$ est représenté par le point de plus grande cote, et $|1\rangle$ est représenté par le point de plus petite cote tandis que les points tels que $x^2+y^2 = 1$ et $z = 0$ où bien plus simplement tels que $\theta = \frac{\pi}{4}$ sont situés sur l'équateur.

2.1.7 Principe d'incertitude d'Heisenberg

2.1.7.1 Écart quadratique

Cherchons à caractériser la dispersion des mesures autour de la valeur $\langle A\rangle$. De manière intuitive nous pourrions considérer la différence entre $\langle A\rangle$ et la mesure A et effectuer la moyenne de cette différence sur les N différents résultats de cette mesure. Toutefois, nous pouvons immédiatement remarquer que cette moyenne serait nulle car les écarts négatifs compenseraient en moyenne les écarts positifs. Pour éviter la compensation de ces écarts, nous pouvons considérer la definition suivante :

$$\Delta A = \sqrt{\langle(\langle A\rangle - A)^2\rangle} \tag{2.14}$$

En utilisant le résultat 2.10 dans l'équation 2.14 pour l'opérateur $(\langle A\rangle - A)^2$ nous obtenons :

$$\Delta A = \sqrt{\langle\psi|(\langle A\rangle - A)^2|\psi\rangle}$$

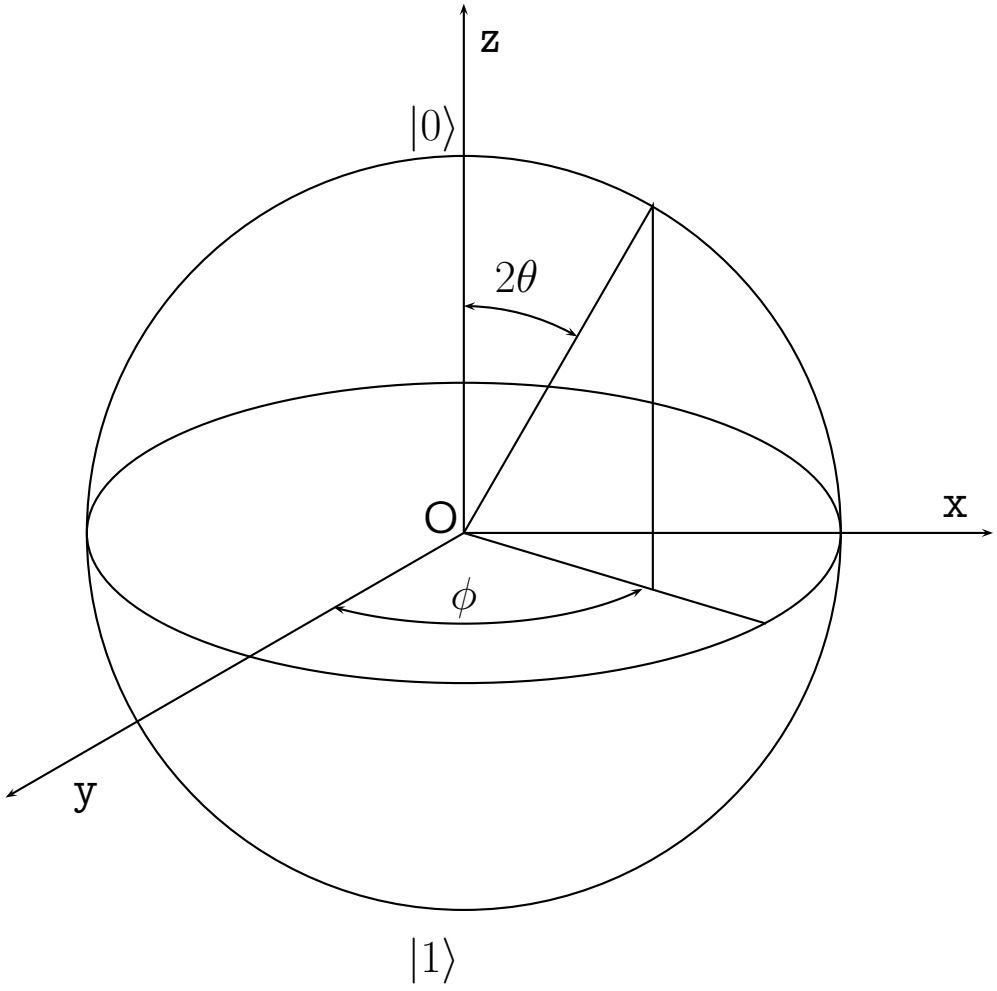

FIG. 2.1 – Sphère de Bloch

2.1.7.2 Principe d'incertitude

La notation $[P, Q]$ est utilisé pour noter le commutateur des observables P et Q. Ce commutateur est défini par :

$$[P, Q] = PQ - QP \tag{2.15}$$

Deux observables sont dites conjuguées si leur commutateur est imaginaire et vaut $i\hbar$. C'est souvent le cas, en particulier lorsque ces opérateurs correspondent à deux grandeurs classiques conjuguées comme par exemple la position et la quantité de mouvement.

Considérons maintenant deux observables P et Q conjuguées, un réel Λ quelconque et le ket $|\phi\rangle$ défini par :

$$|\phi\rangle = (P + i\Lambda Q)|\psi\rangle \tag{2.16}$$

Nous pouvons maintenant calculer le carré de la norme de ce vecteur $|\phi\rangle$ que nous venons de définir.

$$\begin{aligned} \langle\phi|\phi\rangle &= \langle\psi|(P - i\Lambda Q)(P + i\Lambda Q)|\psi\rangle \\ &= \langle\psi|P^2|\psi\rangle + \langle\psi|(\Lambda Q)^2|\psi\rangle + \langle\psi|i\Lambda PQ - i\Lambda QP|\psi\rangle \\ &= \langle\psi|P^2|\psi\rangle + \Lambda^2\langle\psi|Q^2|\psi\rangle + i\Lambda\langle[P, Q]\rangle \\ &= \langle P^2\rangle + \Lambda^2\langle Q^2\rangle - \Lambda\hbar \end{aligned} \tag{2.17}$$

L'expression 2.17 est une norme au carré. Elle peut aussi être vue comme un trinôme en Λ qui doit donc toujours être positif, ce qui se traduit par un discriminant négatif.

$$\langle P^2\rangle\langle Q^2\rangle \geq \frac{\hbar^2}{4} \tag{2.18}$$

Les observables P et Q peuvent être vues comme la somme d'une partie moyenne classique et d'une partie quantique fluctuante :

$$\begin{aligned} P &= \langle P\rangle + P' \\ Q &= \langle Q\rangle + Q' \end{aligned}$$

Les parties classiques ont la particularité de commuter ($[\langle P\rangle, \langle Q\rangle] = 0$), ce qui entraîne que $[P, Q] = [P', Q']$. Il en découle que le raisonnnement précédent s'applique aussi à P' et Q'.

$$\langle P'^2\rangle\langle Q'^2\rangle \geq \frac{\hbar^2}{4} \tag{2.19}$$

En utilisant la définition 2.14 de l'écart quadratique, nous pouvons exprimer ΔP^2 en fonction de $\langle P'^2\rangle$.

$$\begin{aligned} \Delta P^2 &= \langle(\langle P\rangle - P)^2\rangle \\ &= \langle P'^2\rangle \end{aligned} \tag{2.20}$$

Ce raisonnement s'applique également à l'observable conjugués Q, sous la forme $\Delta Q^2 = \langle Q'^2 \rangle$. Il vient alors :

$$\Delta P^2 \Delta Q^2 \geq \frac{\hbar^2}{4} \tag{2.21}$$

Comme la fonction racine carrée est croissante, nous pouvons directement déduire le principe d'incertitude d'Heisenberg :

$$\Delta P \Delta Q \geq \frac{\hbar}{2} \tag{2.22}$$

Ainsi la précision d'une mesure d'une observable fixe la valeur maximale de la précision de la mesure de l'observable conjuguée.

2.1.8 Opérateur de densité

2.1.8.1 État pur

i. Vecteur d'état

Nous avons l'habitude de décrire un état par son vecteur d'état : $|\psi\rangle = \sum_n c_n |u_n\rangle$. Les $\{|u_n\rangle\}$ forment alors une base orthonormée de l'espace des états. $\sum_n |c_n|^2 = 1$ car on considère $|\psi\rangle$ normé. En définissant un observable de matrice A par les éléments $\langle u_p|A|u_n\rangle = A_{np}$, sa valeur moyenne $\langle A \rangle$ est donnée par :

$$\begin{aligned} \langle A \rangle &= \langle \psi|A|\psi \rangle & (2.23) \\ &= \sum_{n,p} c_n^\star c_p A_{np} & (2.24) \end{aligned}$$

ii. Opérateur densité

On remarque cependant que $\langle u_p|\psi\rangle\langle\psi|u_n\rangle = c_n^\star c_p$. Il est donc naturel d'introduire la quantité $\rho = |\psi\rangle\langle\psi|$ comme opérateur densité. Ainsi l'opérateur densité est représenté dans la base orthonormée $\{|u_n\rangle\}$ par une matrice dite de « densité » dont les éléments sont $\rho_{pn} = \langle u_p|\rho|u_n\rangle$. Il est possible de déduire les propriétés suivantes sur la trace de cet opérateur densité :

$$\sum_n |c_n|^2 = \sum_n \rho_{nn} = \mathrm{Tr}\,\rho = 1 \tag{2.25}$$

À partir des équations (2.24) et (2.25) d'une part, et de la définition des éléments A_{np} de la matrice A on peut obtenir :

$$\begin{aligned} \langle A \rangle &= \sum_{n,p} \langle u_p|\rho|u_n\rangle\langle u_n|A|u_p\rangle \\ &= \sum_p \langle u_p|\rho A|u_p\rangle \\ &= \mathrm{Tr}\,\rho A & (2.26) \end{aligned}$$

La probabilité $\mathcal{P}(a_n)$ des différents résultats a_n que peut donner la mesure de l'observable A en notant[2] $|u_n\rangle\langle u_n| = P_n$ et en utilisant (2.24) et (2.26), est donnée par :

$$\begin{aligned}\mathcal{P}(a_n) &= |\langle\Psi|u_n\rangle|^2 \\ &= \langle\psi|u_n\rangle\langle u_n|\Psi\rangle \\ &= \langle\psi|P_n|\Psi\rangle \\ &= \mathrm{Tr}\, P_n\rho\end{aligned}$$

Cette expression de $P(a_n)$ nous renseigne sur la manière d'utiliser l'opérateur densité pour des mesures d'observable.

2.1.8.2 Mélange statistique d'états

Nous considérons maintenant un mélange statistique d'état. Les probabilités $p_1, p_2, \ldots, p_k, \ldots$ de trouver notre système dans les états $1, 2, \ldots, k, \ldots$ satisfont :

$$\begin{cases}\forall k \in \{0;1\} \\ \sum_k p_k = 1\end{cases}$$

La probabilité pour qu'une mesure de l'observable A donne le résultat a_n est donnée par

$$\begin{aligned}\mathcal{P}(a_n) &= \sum_k p_k |\langle\psi_k|u_n\rangle|^2 \\ &= \sum_k p_k \,\mathrm{Tr}\{\rho_k P_n\} \\ &= \mathrm{Tr}\{\rho P_n\}\end{aligned}$$

Ce qui nous permet de déduire ρ dans le cas d'un mélange statistique d'états.

$$\rho = \sum_k p_k \rho_k$$

2.1.9 Théorème de non-clonage et téléportation quantique

2.1.9.1 Théorème de non-clonage

La sécurité en cryptographie quantique est basée sur l'effondrement des états lors des mesures que nous avons déjà illustrées aux paragraphes 2.1.5 et 2.1.7.1. Il est impossible de copier parfaitement un photon de manière à obtenir deux photons identiques [47, 34]. Considérons une machine à cloner

[2] Nous avons volontairement omis ici le cas où a_n est une valeur propre dégénérée pour une meilleure lisibilité.

idéale. Soit l'état $|\psi\rangle$ l'état à copier, et $|b\rangle$ un état quelconque[3] sur lequel l'état ψ doit être copié. La machine peut être décrite par :

$$|\psi\rangle|b\rangle \Rightarrow |\psi\rangle|\psi\rangle \tag{2.27}$$

Avec $|A\rangle$ et $|B\rangle$ deux états quelconques, nous avons donc nécessairement

$$\begin{aligned} |A\rangle|b\rangle &\Rightarrow |A\rangle|A\rangle \\ |B\rangle|b\rangle &\Rightarrow |B\rangle|B\rangle \end{aligned} \tag{2.28}$$

Considérons le mélange statistique d'état $\alpha|A\rangle + \beta|B\rangle$ et donnons le à copier à notre machine à cloner idéale :

$$(\alpha|A\rangle + \beta|B\rangle)|b\rangle \Rightarrow (\alpha|A\rangle + \beta|B\rangle)(\alpha|A\rangle + \beta|B\rangle) \tag{2.29}$$

Nous remarquons que $(\alpha|A\rangle + \beta|B\rangle)|b\rangle$ peut également s'écrire sous la forme développée $\alpha|A\rangle|b\rangle + \beta|B\rangle|b\rangle$. Notre machine à cloner idéale doit également être capable de copier cet état sous cette forme.

$$\alpha|A\rangle|b\rangle + \beta|B\rangle|b\rangle \Rightarrow \alpha|A\rangle|A\rangle + \beta|B\rangle|B\rangle \tag{2.30}$$

Il est bien évident que les états de départs de la machine à cloner étant égaux, les états obtenus devraient également l'être. Pourtant 2.29 et 2.30 sont différents pour peu que $|A\rangle$ et $|B\rangle$ ne soient pas colinéaires. En utilisant les propriétés qui sont attendues d'une machine à cloner idéale, nous sommes arrivés à une incohérence vis à vis de notre hypothèse. Nous avons donc démontré par l'absurde qu'une machine à cloner idéale ne peut exister.

Par contre, rien n'empêche l'existence d'une machine à cloner qui serait approximative. En effet, au prix de la qualité du clonage, et d'une perte d'information sur l'état initial, nous pouvons tout à fait imaginer qu'un tel clonage approximatif soit possible.

2.1.9.2 Téléportation quantique

Charles Bennett et ses collègues ont proposé en 1992 un protocole permettant la téléportation quantique d'un qubit [7].Téléportation est pris dans le sens où un objet présent à un endroit donné est détruit pour le recréer à un autre endroit.

Appelons $|\Phi_1\rangle = a|0\rangle + b|1\rangle$ avec $|a|^2 + |b|^2 = 1$ ce Qubit à téléporter. Cette téléportation quantique nécessite qu'Alice et Bob partagent un état dit intriqué. Un état intriqué est un état composé de deux particules ayant chacune une état aléatoire et dont la mesure de l'état de l'une influence et effondre l'état de l'autre. Supposons qu'Alice et Bob partagent l'état suivant :

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0_A\rangle|0_B\rangle + |1_A\rangle|1_B\rangle) \tag{2.31}$$

[3] Si la machine était une photocopieuse, $|b\rangle$ serait une page blanche.

Il est impossible de factoriser l'état $|\Psi^+\rangle$ sous la forme $|\phi_1\rangle \otimes |\phi_2\rangle$ et donc d'effectuer une mesure distincte pour le qubit A et le qubit B. Les qubits A et B sont donc intriqués. Par contre, bien qu'intriqué, rien n'empêche de donner à Alice le qubit A et à Bob le Qubit B. Alice possède alors le qubit à téléporter et le qubit A. Elle va mesurer les deux qubits qu'elle a en sa possession, mais pour cela elle a besoin d'une base pour décrire les différents états possibles.

$$\begin{aligned}
|\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|0_A\rangle|0_B\rangle + |1_A\rangle|1_B\rangle \\
|\Psi^-\rangle &= \frac{1}{\sqrt{2}}(|0_A\rangle|0_B\rangle - |1_A\rangle|1_B\rangle \\
|\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|0_A\rangle|1_B\rangle + |1_A\rangle|0_B\rangle \\
|\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|0_A\rangle|1_B\rangle - |1_A\rangle|0_B\rangle
\end{aligned}$$

Nous pouvons donc maintenant écrire les différents couples possibles en fonction de cette base :

$$\begin{aligned}
|0\rangle|0\rangle &= \frac{1}{\sqrt{2}}(|\Psi^+\rangle + |\Psi^-\rangle) \\
|1\rangle|1\rangle &= \frac{1}{\sqrt{2}}(|\Psi^+\rangle - |\Psi^-\rangle) \\
|0\rangle|1\rangle &= \frac{1}{\sqrt{2}}(|\Phi^+\rangle + |\Phi^-\rangle) \\
|1\rangle|0\rangle &= \frac{1}{\sqrt{2}}(|\Phi^+\rangle - |\Phi^-\rangle)
\end{aligned}$$

Récapitulons l'état global de notre système avant qu'Alice n'effectue sa mesure.

$$\begin{aligned}
|\Phi_1\rangle|\Psi^+\rangle &= (a|0\rangle + b|1\rangle)(\frac{1}{\sqrt{2}}(|0_A\rangle|0_B\rangle + |1_A\rangle|1_B\rangle) \\
&= \frac{1}{2}(a|0\rangle|0_A\rangle|0_B\rangle + a|0\rangle|1_A\rangle|1_B\rangle + b|1\rangle|0_A\rangle|0_B\rangle + b|1\rangle|1_A\rangle|1_B\rangle) \\
&= \frac{1}{\sqrt{2}}[a(|\Psi^+\rangle + |\Psi^-\rangle)|0_B\rangle + a(|\Phi^+\rangle + |\Phi^-\rangle)|1_B\rangle \\
&\quad + b(|\Phi^+\rangle - |\Phi^-\rangle)|0_B\rangle + b(|\Psi^+\rangle - |\Psi^-\rangle)|1_B\rangle] \\
&= \frac{1}{2}[|\Psi^+\rangle(a|0_B\rangle + b|1_B\rangle) + |\Psi^-\rangle(a|0_B\rangle - b|1_B\rangle) \\
&\quad + |\Phi^+\rangle(a|1_B\rangle + b|0_B\rangle) + |\Phi^-\rangle(a|1_B\rangle - b|0_B\rangle)] \qquad (2.32)
\end{aligned}$$

Ceci nous permet de remarquer que lorsqu'Alice effectue sa mesure, elle obtient un des quatre vecteurs de base ($|\Psi^+\rangle$, $|\Psi^-\rangle$, $|\Phi^+\rangle$ et $|\Phi^-\rangle$), et suivant le résultat qu'elle trouve, elle connaît le qubit que Bob possède en fonction du

qubit $|\Phi_1\rangle$ qu'elle souhaitait téléporter. Notons également qu'elle ne dispose plus du qubit $|\Phi_1\rangle$. Elle n'a plus qu'à envoyer à Bob le résultat de cette mesure à travers un canal classique et Bob, suivant ce qu'Alice lui envoie, doit éventuellement effectuer une opération supplémentaire pour obtenir le qubit initial $|\Phi_1\rangle$.

- Si Alice mesure $|\Psi^+\rangle$ alors Bob ne fait rien, il a déjà le qubit $|\Phi_1\rangle$.
- Si Alice mesure $|\Psi^-\rangle$ alors Bob doit multiplier son qubit par la matrice suivante :
$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{2.33}$$
- Si Alice mesure $|\Phi^+\rangle$ alors Bob doit multiplier son qubit par la matrice suivante :
$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{2.34}$$
- Si Alice mesure $|\Phi^-\rangle$ alors Bob doit multiplier son qubit par la matrice suivante :
$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \tag{2.35}$$

Nous avons montré un exemple historique de téléportation quantique. Cela montre que pour effectuer une telle téléportation quantique il est nécessaire d'avoir un état intriqué par qubit, et de disposer d'un canal classique. Cette téléportation n'a fait que transporter un qubit, étant donné que ni Alice ni Bob ne connaît ce qubit. En conclusion, rien ne s'oppose à la téléportation quantique, à partir du moment où l'état initial est détruit, et l'état final reste inconnu.

2.2 Ordinateur quantique

2.2.1 Définition

L'ordinateur quantique est une machine qui manipule des qubits. Pour cela, il faut lui donner un certain nombre de possibilités. D'abord il faut qu'elle puisse initialiser ces qubits, c'est-à-dire leur donner une valeur de départ. Il est également nécessaire que la machine puisse agir sur un qubit sans modifier d'autres parties du système ou d'autres qubits. Enfin, pour manipuler les qubits, l'ordinateur quantique doit posséder un nombre de portes quantiques suffisant pour réaliser toutes les opérations quantiques autorisées sur les qubits [16]. Notons que ces portes doivent conserver les propriétés des qubits c'est à dire que $|\alpha|^2 + |\beta|^2 = 1$ et donc qu'elles doivent être unitaires. On représente habituellement ces portes par des matrices unitaires. Prenons comme premier exemple la porte d'Haramad [8].

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{2.36}$$

Entrée	$\|00\rangle$	$\|01\rangle$	$\|10\rangle$	$\|11\rangle$
Sortie	$\|00\rangle$	$\|01\rangle$	$\|11\rangle$	$\|10\rangle$

TAB. 2.1 – Tableau décrivant les entrées et les sorties possibles de la porte cNOT

Elle transforme le qubit $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ en

$$H|\phi\rangle = \frac{1}{\sqrt{2}}\left((\alpha+\beta)|0\rangle + (\alpha-\beta)|1\rangle\right) \tag{2.37}$$

Une autre porte quantique est la porte rotation. Celle-ci est définie par la matrice suivante :

$$R(\theta) = \begin{bmatrix} 1 & 0 \\ 0 & e^{2i\pi\theta} \end{bmatrix} \tag{2.38}$$

De la même manière que dans le cas classique, on cherche un ensemble de portes logiques universelles à partir desquelles on peut exécuter toutes les fonctions réalisables sur les qubits. Un tel ensemble de portes peut être constitué de la porte d'Haramad, des portes rotations et d'une dernière porte appelée porte « cNOT »pour control-NOT [3] qui opère sur un couple de qubits. Les entrées et les sorties de cette porte cNOT sont décrites dans le tableau 2.1. En fait, si le premier qubit est $|0\rangle$, la sortie est inchangée, alors que si le premier qubit est $|1\rangle$ les amplitudes de probabilités du deuxième qubit sont inversées. Pour analyser en détail l'effet de la porte cNOT il nous faut décrire les états possibles par une base. Étant donné que cette porte agit sur deux qubits, il y a donc quatre états purs possibles, dont nous pouvons nous servir pour définir une base :

$$|00\rangle = \begin{bmatrix}1\\0\\0\\0\end{bmatrix} \quad |01\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix} \quad |10\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix} \quad |11\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix} \tag{2.39}$$

L'effet de la porte cNOT est rappelé dans le tableau 2.1. Nous pouvons également décrire l'effet de la porte cNOT par une matrice unitaire opérant sur les vecteurs de bases définis à l'équation 2.39 :

$$cNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{2.40}$$

Voyons l'effet de cette porte sur les qubits $|0,\Psi\rangle$ et $|1,\Psi\rangle$ avec $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Définissons pour l'occasion le qubit $|\Phi\rangle = \beta|0\rangle + \alpha|1\rangle$.

$$\begin{aligned} cNOT(|0,\Psi\rangle) &= cNOT(|0\rangle(\alpha|0\rangle + \beta|1\rangle)) \\ &= \alpha cNOT(|00\rangle) + \beta cNOT(|01\rangle) \\ &= |0,\Psi\rangle \end{aligned} \tag{2.41}$$

$$\begin{aligned} cNOT(|1,\Psi\rangle) &= cNOT(|1\rangle(\alpha|0\rangle + \beta|1\rangle)) \\ &= \alpha cNOT(|10\rangle) + \beta cNOT(|11\rangle) \\ &= \alpha|11\rangle + \beta|10\rangle \\ &= |1,\Phi\rangle \end{aligned} \tag{2.42}$$

Pour pouvoir opérer, un ordinateur quantique a également besoin d'un système de mesure. Celui-ci doit bien évidemment respecter les lois de la mécanique quantique, ainsi les mesures effectuées sont régies par les probabilités édictées par les lois de la mécanique quantique.

2.2.2 Factorisation d'un nombre premier

L'intérêt majeur de posséder un tel ordinateur quantique est de pouvoir l'utiliser pour des algorithmes spécialement pensés pour y être exécutés. En effet, le fait de pouvoir opérer sur des qubits, peut être intéressant. Ainsi, Peter W. Shor a mis au point un algorithme de factorisation de nombres en facteurs premiers [40]. Le nombre d'opérations élémentaires utilisées par l'algorithme classique qui sert à décomposer un nombre N de l digits en facteurs premiers croit exponentiellement avec l [27]. L'utilité essentielle d'un nouvel algorithme quantique pour effectuer cette factorisation, est que le nombre d'opérations est de loin inférieur à l'algorithme classique. En effet, l'algorithme quantique utilise un nombre d'opérations élémentaires polynomial avec le nombre de qubits en entrée [40].

Utilisé pour factoriser le nombre $N = pq$ défini dans notre exemple du chiffrement RSA de chiffrement asymétrique, cet algorithme pourrait bien servir à casser nombre de systèmes de chiffrement classique basés sur le théorème d'Euler-Fermat, et ainsi sonner le glas de ces systèmes de chiffrements asymétriques.

2.2.3 L'ordinateur quantique : Réalité, rêve ou cauchemar ?

Avant de commencer à fabriquer un ordinateur quantique, il semble nécessaire de savoir construire et mettre bout à bout les différentes portes logiques nécessaires à son opération. Ces portes ont été réalisées, et leur faisabilité a été démontrée par exemple pour effectuer une décomposition du nombre $N = 15$ à l'aide d'un registre composé de quatre qubits [45].

Le problème principal, pour avoir un ordinateur quantique qui soit intéressant, il faut augmenter le parallèlisme en entrée, c'est-à-dire le nombre de qubits qu'il est capable de traiter à la fois [26]. Le problème est donc de pouvoir concaténer un grand nombre de portes pour créer un ordinateur quantique, en gardant à l'esprit que l'on doit pouvoir manier un qubit sans perturber les autres qubits alentour [25].

2.3 Cryptographie quantique

2.3.1 Le protocole BB84

Le protocole BB84 est un protocole de distribution de clefs. En effet, le but est de générer une clef partagée entre Alice et Bob n'autorisant aucun tiers à acquérir une information pertinente sur cette clef. Cette clef doit pouvoir servir à un chiffre de Vernam, et conduire ainsi à une transmission d'information inconditionnellement sûre.

De nombreuses implémentations de distributions quantiques de clefs sont basées sur BB84 [35, 10, 6, 1, 21, 32, 52, 29, 31]. Alice et Bob sont dotés d'un canal de transmission (espace libre ou fibre optique) par lequel sont envoyés les qubits et d'un canal dit public sur lequel ils doivent pouvoir s'authentifier. L'attaquante Ève est dotée de toutes technologies connues et inconnues autorisées par les lois de la mécanique quantique.

2.3.1.1 Description du protocole BB84

i. Remarques préliminaires

Le premier protocole de cryptographie quantique a été présenté par Charles H. Bennett et Gilles Brassard en 1984. Le protocole a été présenté en utilisant des états de polarisation, mais il est utilisable avec d'autres grandeurs comme la phase ou la fréquence. Il nécessite quatre états qui constituent deux bases orthonormées. Nous noterons ces états $|A_1\rangle$, $|A_2\rangle$, $|B_1\rangle$ et $|B_2\rangle$. $|A_1\rangle$ et $|A_2\rangle$ forment tous deux une base A tandis que $|B_1\rangle$ et $|B_2\rangle$ forment une deuxième base B. Par construction on a donc :

$$\begin{aligned} \langle A_1|A_2\rangle &= 0 \\ \langle B_1|B_2\rangle &= 0 \end{aligned} \tag{2.43}$$

On désire également que la mesure d'un état $|A_1\rangle$ ou $|A_2\rangle$ sur la base B ou d'un état $|B_1\rangle$ ou $|B_2\rangle$ sur la base A ne donne pas d'informations. Nous verrons que cela peut être réalisé si :

$$\begin{aligned} |A_1\rangle &= \frac{|B_1\rangle + |B_2\rangle}{\sqrt{2}} \\ |A_2\rangle &= \frac{|B_1\rangle - |B_2\rangle}{\sqrt{2}} \\ |B_1\rangle &= \frac{|A_1\rangle + |A_2\rangle}{\sqrt{2}} \\ |B_2\rangle &= \frac{|A_1\rangle - |A_2\rangle}{\sqrt{2}} \end{aligned} \tag{2.44}$$

État	bit
A_1	0
A_2	1
B_1	0
B_2	1

TAB. 2.2 – Correspondance entre les états de BB84 et leur valeur

Notons que les équations 2.43 et 2.44 conduisent directement à :

$$\langle A_{1,2}|B_{1,2}\rangle = \frac{1}{\sqrt{2}} \tag{2.45}$$

Ce protocole doit définir des valeurs pour les états qu'il représente, on peut choisir par exemple les valeurs du tableau 2.2. Imaginons maintenant qu'Alice souhaite envoyer le bit 0 à Bob. Elle choisit par exemple la base A, elle envoie donc l'état A_1. Bob, lorsqu'il reçoit le qubit envoyé par Alice, doit choisir entre une mesure sur la base A et une mesure sur la base B :

– Si Bob effectue sa mesure sur la base A alors :

$$\begin{aligned} \mathcal{P}(A_1) &= |\langle A_1|A_1\rangle|^2 & \mathcal{P}(A_2) &= |\langle A_1|A_2\rangle|^2 \\ &= 1 & &= 0 \end{aligned} \tag{2.46}$$

– Si Bob effectue sa mesure sur la base B alors :

$$\begin{aligned} \mathcal{P}(B_1) &= |\langle A_1|B_1\rangle|^2 & \mathcal{P}(B_2) &= |\langle A_1|B_2\rangle|^2 \\ &= \frac{1}{2} & &= \frac{1}{2} \end{aligned} \tag{2.47}$$

Nous remarquons donc que Bob obtient un résultat correct dans deux situations :

1. Lorsque Bob fait le bon choix de base, c'est-à-dire le même qu'Alice.
2. Une fois sur deux lorsqu'il fait le mauvais choix de base, c'est à dire son choix diffère de celui d'Alice.

ii. Le protocole BB84

1. Alice choisit une base. Elle envoie 0 ou 1 sur cette base. Elle effectue de même pour tous les bits. Alice garde en mémoire tous les choix qu'elle a fait, aussi bien les bases que les valeurs des bits qu'elle a envoyés.
2. Bob reçoit chaque qubit. Pour en effectuer une mesure, il choisit également une base pour chaque qubit. Bob garde également en mémoire les choix de base qu'il fait, ainsi que les valeurs des mesures obtenues.

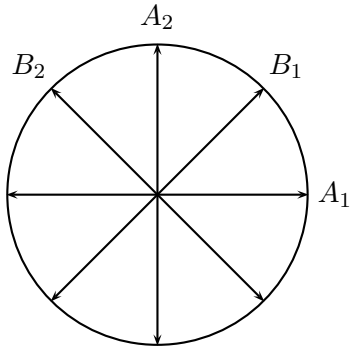

FIG. 2.2 – Bases de BB84 pour des états de polarisation

3. Alice et Bob annoncent sur un canal public authentifié les choix de bases qui ont été faits. Ils ne gardent alors que les valeurs des bits pour lesquels leurs choix ont coincidé, et rejettent les autres. Cette étape s'appelle la réconciliation.
4. Alice et Bob appliquent des algorithmes sur la clef obtenue de manière à détecter d'éventuelles erreurs, et à amoindrir l'information volée par un éventuel tiers Ève. Cette étape s'appelle l'amplification de sécurité.

2.3.1.2 Le protocole BB84 utilisé à l'aide d'états de polarisation

Le protocole originel proposé par Bennett et Brassard était censé utiliser un codage en polarisation [5]. . Une implémentation a été conduite par Bennett en 1992 utilisant quelques centimètres d'espace libre comme medium de transmission [6]. Cette mise en pratique de BB84 souffre de plusieurs problèmes : d'abord, il est difficile d'obtenir une source de photon unique ; une source cohérente fortement atténuée de manière à ce qu'il y ait en moyenne moins d'un photon par qubit a été utilisée. Ensuite, le protocole BB84 est défini pour un canal de communication sans bruit et sans pertes, et il a ici été adapté pour une communication bruitée.

De plus, d'autres problèmes surviennent lorsqu'on essaie d'augmenter la portée utile de la transmission. On utilise pour cela des fibres optiques plutôt que l'espace libre ce qui est moins source d'erreur et de perte, mais la polarisation souffre de défauts de propagations ce qui force à la contrôler et à la compenser de manière active [10, 35].

Un exemple de représentation géométrique d'états polarisés qui pourraient servir lors d'une telle transmission est présenté dans la figure 2.2.

2.3.1.3 Le protocole BB84 utilisé à l'aide d'états de phases

Pour diminuer les contraintes sur la polarisation, des implémentations de BB84 utilisent un encodage de phase en faisant une lecture liée à la phase du protocole BB84 originel [29, 32, 52]. Ces systèmes de transmission

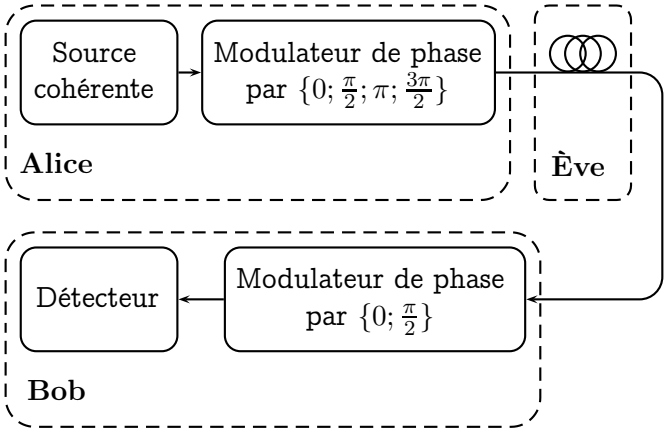

FIG. 2.3 – Schéma de principe du lien entre Alice et Bob, pour un encodage basé sur la phase

peuvent utiliser une référence de phase transitant ou non sur bras séparé. Un exemple d'implémentation d'un tel système est présenté sur la figure 2.3. Nous supposons qu'Alice et Bob disposent d'un bras de référence de phase non représenté sur la figure. La détection est assurée par intérférométrie, ce qui signifie que la différence de trajet entre la lumière assurant la référence de phase et la lumière signal doit être inférieure à la longueur de cohérence de la lumière de manière à assurer la stabilité du système.

Une approche différentielle peut aussi être utilisée [15]. Dans un tel système, la référence est le signal lui même. En fait, l'information utile est rangée dans la différence entre deux symboles et non pas dans les symboles qui arrivent. Et l'on ne mesure que la différence de phase entre deux qubits.

2.3.1.4 Le protocole BB84 utilisé grâce à un encodage en fréquence

Une implémentation à photon unique utilisant BB84 sur un encodage en fréquence à été mise au point en 1999 [31]. Il s'agit d'utiliser les bandes latérales pour coder les qubits. Les modulations sont réalisées par des oscillateurs contrôlés en tension, ce qui permet également une gestion fine de la phase.

2.3.2 Erreurs et protocoles de réconciliation

Pour être utilisable, la clef brute, obtenue après l'annonce sur un canal public des choix de bases, doit subir des modifications pour en améliorer la sécurité. En effet, il faut réduire les erreurs entre Alice et Bob, et aussi réduire la connaissance l'information que possède Ève de cette clef. On appellera N la longueur de la clef.

2.3.2.1 Comparaison publique et estimation d'erreurs

Tout d'abord, pour une obtenir une liaison sécurisée il faut s'assurer qu'Alice et Bob possèdent un clef similaire. Il faut alors estimer le taux d'erreur entre Alice et Bob. Nous appelons ce taux QBER (Quantum Bit Error Rate). Cette étape consiste à utiliser le canal public authentifié pour comparer certains bits de la clef, et ainsi obtenir une estimation de ce QBER. Ces bits étant dévoilés publiquement, ils sont donc sacrifiés, et ne peuvent plus être utilisés par la suite dans la clef finale. Deux contraintes sont à prendre en compte pour estimer le nombre de bits à sacrifier ; tout d'abord, il faut utiliser assez de bits de la clef pour que l'estimation soit correcte, et ne pas en utiliser trop, puisque cela écourte la longueur de la clef d'autant. Appelons c_p la longueur de la clef sacrifiée dans la comparaison publique, et e l'estimation du taux d'erreur obtenue.

2.3.2.2 Correction d'erreur

i. Correction d'erreur

La clef brute présente un taux d'erreur estimé par la comparaison publique. Pour diminuer ce QBER, Alice et Bob utilisent à nouveau le canal public authentifié pour diminuer les différences de version de la clef d'Alice et de Bob. Cette opération s'effectue au détriment de la longueur de la clef. Un protocole très simple pour obtenir un tel résultat est présenté ci-après :

1. Alice choisit deux bits au hasard, et calcule leur somme modulo 2.
2. Alice annonce quels sont les deux bits, et le résultat qu'elle a obtenu.
3. Bob annonce s'il obtient le même résultat.
4. Si le résultat est le même, Alice et Bob gardent un des deux bits et jettent l'autre, si le résultat est différent ils jettent les deux bits.

Donc, au prix sur la taille de la clef, Alice et Bob arrivent à détecter d'éventuelles erreurs. Appelons c_e la longueur de la clef utilisée pour corriger les erreurs de la clef brute.

ii. Le protocole cascade

C'est un protocole itératif qui agit sur des blocs [9]. Alice et Bob se mettent d'accord de la taille d'un bloc initial dont ils transmettent la parité sur le canal publique. Deux cas de figure peuvent alors se produire :

– La parité obtenue chez Alice et Bob est identique. Les blocs comparés ont donc un nombre pair de différence, c'est à dire que la clef dans les mains d'Ève possède un nombre pair d'erreurs. Alice et Bob conviennent d'un nouveau bloc à étudier de manière analogue au premier bloc. Les blocs peuvent se chevaucher.

– La parité obtenue chez Alice et Bob est différente, les blocs comparés ont alors un nombre impair de différence. Alice et Bob découpent alors le bloc analysé en deux blocs, et procèdent de manière analogue pour trouver duquel vient la différence de parité. Il procèdent ainsi par dichotomie pour trouver et corriger l'erreur. Ils passent ensuite à un nouveau bloc.

Alice et Bob peuvent convenir d'un mélange aléatoire commun de bits entre chaque traitement de blocs. Alice et Bob arrêtent le protocole après un nombre de passes convenu à l'avance. Il ne faut pas perdre de vue que ce protocole donne des informations qu'Ève peut récupérer sur le canal public. Les bits dont la valeur a été divulguée à des fins de corrections d'erreurs, ne peuvent plus être utilisés dans une clef sécurisée. Nous pouvons donc rapprocher ces bits divulgués au nombre c_e précédemment défini.

iii. Décompte de la sécurité restante

La comparaison publique et les corrections appauvrissent la sécurité de notre clef. Les bits divulgués ne peuvent plus être utilisés dans la clef finale. Grâce à l'étude de Shannon [38], nous allons faire le décompte c_r des bits non encore divulgués :

$$c_r = nH(e) - c_e - c_p - c_s \tag{2.48}$$

$H(e)$ est l'entropie de la communication, c'est-à-dire le taux d'information qu'Alice et Bob sont en mesure de partager. Le paramètre c_s est une marge de sécurité. Cette équation peut encore se réécrire sous la forme suivante :

$$c_r = -n\left(e\log_2 e + (1-e)\right)\log_2(1-e) - c_e - c_p - c_s \tag{2.49}$$

2.3.2.3 Amplification de confidentialité

Il s'agit ici de réduire l'information détenue par Ève de la clef commune entre Alice et Bob. Pour cela, nous utilisons à nouveau le canal public authentifié. Alice et Bob sacrifient à nouveau une partie de la clef pour réduire l'information d'Ève. Une manière très simple d'en comprendre le principe est le protocole très simple suivant :

1. Alice choisit deux bits au hasard, et calcule leur somme modulo 2.
2. Alice annonce quels sont les deux bits.
3. Alice et Bob ne gardent qu'un des deux bits, et jettent l'autre.

En fait, si Ève ne connaissait qu'un des deux bits, elle perd cette information, car elle ne connaît pas le résultat. Appelons c_a la longueur de clef à sacrifier. c_a est calculé pour faire baisser l'information d'Ève a un niveau prédéfini.

Une autre méthode un peu moins gourmande et plus malléable est d'utiliser une fonction de hachage ou à sens unique de $\{0,1\}^n$ vers $\{0,1\}^{n-c_a}$ [6].

2.3.3 Attaque de BB84

2.3.3.1 Attaque intuitive

i. Description de l'attaque

Envisageons tout d'abord, pour appréhender la sécurité du protocole BB84, une attaque simple sur ce protocole. Imaginons une clef de longueur n. Nous supposons qu'Ève subtilise le photon à chaque fois qu'il en en passe un sur le lien entre Alice et Bob. Ève accomplit alors les opérations suivantes :

1. Ève choisit une base, y mesure chaque photon intercepté et stocke dans une mémoire le couple base et mesure réalisée.
2. Ève renvoie le résultat de sa mesure à Bob.

Nous sommes donc maintenant en présence de trois cas de figure :

1. Alice et Bob effectuent un choix de base différent.
   Si Alice et Bob effectuent un choix de base différent pour la lecture d'un même qubit, alors leurs mesures sont tout simplement abandonnées. C'est le cas le plus simple. Ève ne peut espérer gagner aucune information sur la clef brute. Étant donné la figure 2.4, nous pouvons conclure que la moitié des mesures sont abandonnées, c'est-à-dire que ce cas de figure se produit avec une probabilité d'un demi sur la totalité des qubits émis par Alice.
2. Ève a effectué le même choix de base qu'Alice et Bob
   Tout d'abord, nous nous plaçons dans le cas où Alice et Bob font un choix de base concordant. Ève fait alors le même choix de base qu'Alice et Bob, et son intervention ne perturbe pas la mesure de Bob, puisqu'elle lui envoie exactement le même état qu'elle reçoit. Ève est alors indécelable. La probabilité que tous les intervenants du système fasse le même choix est d'un quart, ce que nous pouvons vérifier grâce à la lecture de la figure 2.4.
3. Ève a effectué un choix de base différent de celui d'Alice
   Ce cas de figure intervient quand Alice et Bob font le même choix de base et qu'Ève fait un choix différent. Ce cas de figure se produit avec une probabilité d'un quart. Notons, qu'étant donné qu'Ève fait une mesure sur une base différente de celle d'Alice, elle perturbe l'état. La mesure de Bob est alors aléatoire, et a une probabilité d'un demi de produire le résultat attendu.

ii. Sécurité attendue après cette attaque intuitive

Les choix de bases différents sont abandonnés. Le cas 2 représente 50% des états conservés tandis que le cas 3 représente les 50% restant. Ceci conduit

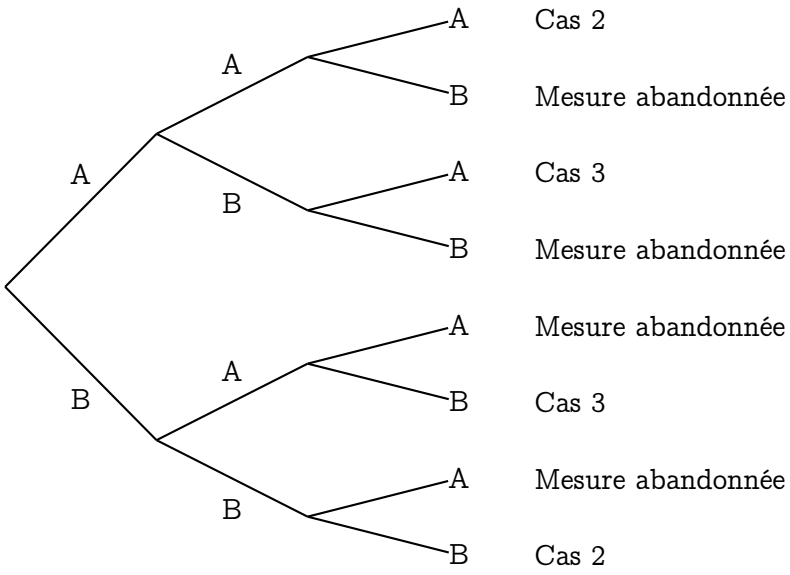

Fig. 2.4 – Arbre illustrant l'attaque intuitive

donc à un taux d'erreurs appelé Quantum Bit Error Rate (QBER) dans notre cas de 25%.

2.3.3.2 Sécurité et attaque cohérente et incohérente

i. Attaque cohérente

Dans cette attaque Ève possède une sonde sur le lien d'Alice et Bob grâce à laquelle elle peut prélever de l'information. Elle n'est limitée que par le théorème de non-clonage, et les lois usuelles de la mécanique quantique. On peut envisager un tel système tel que représenté sur la figure 2.5. En contrepartie, Ève dispose de moyens illimités de traitements d'information quantique en terme de capacités de mémoire quantique et de calculs. Elle peut effectuer toutes les opérations désirées à un moment choisi à sa discrétion par exemple à l'occasion de la phase de réconciliation. Étant donné que la réconciliation peut introduire une dépendance entre certains qubits, qui peuvent être partiellement connus par Ève, nous pouvons imaginer qu'il peut s'avérer intéressant de pouvoir agir collectivement sur les qubits ou bits d'information dont elle dispose.

ii. Attaque incohérente

L'attaque incohérente est différente de l'attaque cohérente, en ce sens qu'elle impose des restrictions sur les capacités d'Ève. En effet, dans cette

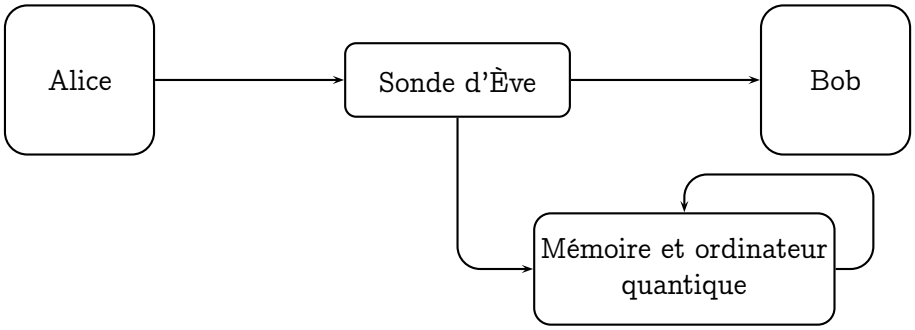

Fig. 2.5 – Attaque cohérente sur le lien entre Alice et Bob

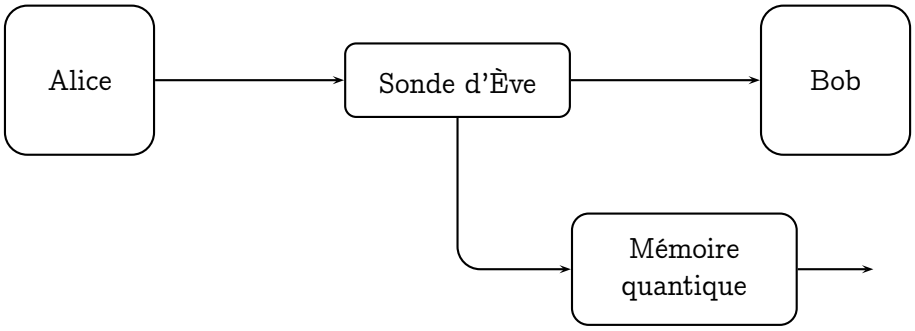

Fig. 2.6 – Attaque incohérente sur le lien entre Alice et Bob

attaque, elle ne peut travailler collectivement sur les bits ou qubits qu'elle a obtenus grâce à sa sonde. Elle est obligé de s'occuper qubit après qubit de l'information qui transite par le lien entre Alice et Bob. Ève possède néanmoins une mémoire quantique pour chaque qubit qu'elle souhaite stocker. Le dispositif est représenté sur la figure 2.6.

iii. Dispositifs réels

Les attaques cohérentes utilisent des dispositifs encore très difficile voire impossible à réaliser, et qui mettront encore beaucoup de temps à apparaître sur le marché. Par contre les dispositifs d'attaque incohérente semble plus réalisables, en effet, le travail sur les mémoires quantiques semble commencer à produire ses effets [13]. Par contre, comme on l'a déjà vu, les ordinateurs quantiques ne sont pas encore en mesure de traiter les données tel qu'envisagé pour mener à bien une attaque cohérente.

Ainsi dans ce manuscrit, nous nous occuperons uniquement d'attaques incohérentes dans la mesure ou traiter des attaques cohérentes serait plus

compliqué et moins utile que des attaques incohérentes plus faciles à mener.

2.3.4 Sécurité de BB84

2.3.4.1 Code correcteur d'erreur quantique

Peter Shor et John Preskill ont trouvé un lien entre la sécurité de BB84 et la capacité de correction de code correcteur d'erreur quantique. Nous nous proposons d'étudier ce lien.

i. Idée générale

Pour pallier aux erreurs induites par un canal de transmission peu fiable, nous pouvons penser à deux solutions évidentes :

- Augmenter la puissance de transmission
- Répéter plusieurs fois le message

Un code correcteur d'erreurs exploite la deuxième idée. Les paramètres importants d'un code correcteur d'erreur est son efficacité (utilisation de peu de redondance d'information et sa capacité à corriger des erreurs nombreuses. Dans le monde de l'information quantique, les canaux de transmissions ne font pas défaut à l'injection d'erreur dans une communication, par le couplage d'un photon avec l'environnement extérieur.

Nous avons décrit un code correcteur d'erreur par un système qui ajoute de la redondance au système de transmission. On pourrait objecter à cause du théorème de non-clonage une impossibilité de créer de la redondance pour un état quantique, mais il s'agit en fait d'étaler l'information d'un état sur plusieurs états.

Les erreurs dues à l'interaction d'un qubit avec l'extérieur sont composées par deux types :

- L'erreur de retournement : Cette erreur transforme le qubit $|0\rangle$ en $|1\rangle$ et vice-versa. En fait, formellement, pour obtenir cette erreur[42], il suffit d'appliquer la matrice de Pauli σ_x définie par

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{2.50}$$

  Ainsi le qubit $\alpha|0\rangle + \beta|1\rangle$ est transformée en $\alpha|1\rangle + \beta|0\rangle$.
- L'erreur de phase : Cette erreur transforme le qubit $\alpha|0\rangle + \beta|1\rangle$ en $\alpha|0\rangle - \beta|1\rangle$. Pour obtenir cette erreur il suffit d'appliquer la matrice de Pauli σ_z définie par :

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.51}$$

- L'erreur de phase et de retournement : Cette erreur est en fait la somme des deux erreurs précédentes et transforme le qubit $\alpha|0\rangle + \beta|1\rangle$ en

$\alpha|1\rangle - \beta|0\rangle$. Par application de la matrice de Pauli $i\sigma_y$ définie par :

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{2.52}$$

Pour obtenir ce qui se passe dans la réalité pour un qubit qui interagit avec l'extérieur, nous avons la combinaison linéaire de ces trois interactions et de l'identité. Si on appelle U l'interaction d'un photon avec l'extérieur alors nous avons :

$$U = c_0 I + c_1\sigma_x + c_2\sigma_y + c_3\sigma_z \tag{2.53}$$

Dans cette équation c_0, c_1, c_2 et c_3 sont des constantes complexes.

Prenons maintenant un exemple de code correcteur quantique simple[41]. Shor a inventé un code qui transforme un qubit en neuf qubits :

$$\begin{aligned} |0\rangle &\rightarrow \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle) \\ |1\rangle &\rightarrow \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle) \end{aligned} \tag{2.54}$$

Si une erreur d'inversion survient sur l'un des qubit, on peut voir que l'étude des deux autres triplets permettra de déduire et de corriger l'erreur. Si en revanche une erreur de phase survient sur l'un des qubit, l'étude des deux autres qubits du triplet permettra également de déduire et de corriger l'erreur.

Il faut également noter le peu d'efficacité de ce code, car il faut utiliser neuf qubits pour coder l'information d'un seul qubit.

ii. Généralisation : CSS

Calderbank et Shor ont inventé un code correcteur d'erreurs quantique plus efficace, équivalent à un code proposé par Steane. Ce code a donc été nommé d'après ses inventeurs, soit le Calderbank-Shor-Steane code[12].

$\mathbb{F}_2^n$ est l'espace des vecteurs de $\mathbb{F}_2$ de dimensions n. Nous pouvons illustrer la construction d'un code correcteur quantique à l'aide d'un code $[7, 4, 3]$ de Hamming, dont les mots de codes sont :

0000000	0001011	0010110	0011101
0100111	0101100	0110001	0111010
1000101	1001110	1010011	1011000
1100010	1101001	1110100	1111111

Nous définissons le code correcteur d'erreur quantique $\mathcal{Q}$ avec un taux de $\frac{k}{n}$ comme une application de $\mathcal{H}_2^k$ dans $\mathcal{H}_2^n$. Pour être plus précis, $\mathcal{H}_2^n$ est ici un sous espace de dimension 2^k de $\mathcal{H}_2^n$. En appelant U l'effet de l'extérieur sur notre système et en supposant que U n'affecte que t qubits, l'idée est de pouvoir retrouver $x \in \mathcal{H}_2^k$ depuis l'état $U\mathcal{Q}|x\rangle$.

M est une matrice génératrice pour C_1.

$$|c_w\rangle = 2^{-\frac{\dim C_1}{2}} \sum_{v \in F_2^{\dim C_1}} (-1)^{vMw} |vM\rangle \tag{2.55}$$

Nous définissons $C^\perp$ par $C^\perp = \{v \in \mathcal{F}_2^n, v.c = 0, \forall c \in C\}$. Ceci implique que si $w_1 + w_2 \in C_1^\perp$ alors $|c_{w_1}\rangle = |c_{w_2}\rangle$ car $vMw_1 = vMw_2$. Dans le cas contraire, si $w_1 + w_2 \notin C_1^\perp$, notons que comme $\sum_v (-1)^{vMw} |vM\rangle = 0$, alors $\langle c_{w_1} | c_{w_2} \rangle = 0$, et $|c_w\rangle$ est une base de l'ensemble $\mathcal{H}_{C_1}$. $\mathcal{H}_{C_1}$ est le sous-espace de $\mathcal{H}_2^n$ généré par les vecteurs $|c\rangle$ avec $c \in \mathcal{C}_1$. Un code correcteur Q est un sous-espace de $\mathbb{C}^{2n}$. Un tel code Q est construit à partir de deux codes linéaires C_1 et C_2, C_2 étant inclus dans C_1 :

$$\{0\} \in C_2 \in C_1 \in \mathcal{F}_2^n \tag{2.56}$$

$$\begin{aligned} |c_0\rangle &= \frac{1}{4}(|0000000\rangle + |001101\rangle + |0100111\rangle + |0111010\rangle \\ &\quad + |1001110\rangle + |1010011\rangle + |1101001\rangle + |1110100\rangle \\ &\quad + |0001011\rangle + |0010110\rangle + |0101100\rangle + |0110001\rangle \\ &\quad + |1000101\rangle + |1011000\rangle + |1100010\rangle + |1111111\rangle) \end{aligned} \tag{2.57}$$

$$\begin{aligned} |c_1\rangle &= \frac{1}{4}(|0000000\rangle + |001101\rangle + |0100111\rangle + |0111010\rangle \\ &\quad + |1001110\rangle + |1010011\rangle + |1101001\rangle + |1110100\rangle \\ &\quad - |0001011\rangle - |0010110\rangle - |0101100\rangle - |0110001\rangle \\ &\quad - |1000101\rangle - |1011000\rangle - |1100010\rangle - |1111111\rangle) \end{aligned} \tag{2.58}$$

En appliquant le changement de base suivant :

$$\begin{aligned} |0\rangle &\rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle &\rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned} \tag{2.59}$$

Nous obtenons :

$$\begin{aligned} |s_0\rangle &= \frac{1}{2\sqrt{2}}(|0000000\rangle + |0011101\rangle + |0100111\rangle + |0111010\rangle \\ &\quad + |1001110\rangle + |1010011\rangle + |1101001\rangle + |1110100\rangle) \\ |s_1\rangle &= \frac{1}{2\sqrt{2}}(|0001011\rangle + |0010110\rangle + |0101100\rangle + |0110001\rangle \\ &\quad + |1000101\rangle + |1011000\rangle + |1100010\rangle + |1111111\rangle) \end{aligned}$$

Dans la base $|c_W\rangle$, nous pouvons corriger t erreurs de retournements de bits, car les mots de code sont la superposition des vecteurs de base $|v\rangle$ avec $v \in C_1$. De même manière que quand la base c_w, la base $|s_w\rangle$ permet de corriger t erreurs de retournements de bit, car les mots de code sont la superposition des vecteurs de base $|v\rangle$ avec $v \in C_2^{\perp}$. L'intérêt de de l'utilisation de ces deux représentations est que des erreurs de phases dans la représentation $|c_w\rangle$ sont des erreurs de retournement dans la représentation $|s_w\rangle$.

iii. Preuve de BB84

L'idée est ici d'utiliser un code CSS pour corriger les erreurs induites par l'extérieur ou par Ève lors de l'exécuation du protocole BB84. Cela présuppose déjà que les erreurs induites par le canal quantique doivent être en nombre moins élevé que la capacité de correction du code utilisé. Si le nombre d'erreurs est trop élevé, le protocole doit être annulé et la cle rejetée.

Une chose importante, est que Ève ne doit pas pouvoir utiliser sa connaissance du code correcteur d'erreur pour retirer de l'information supplémentaire.

Ainsi Shor et Preskill [42] présentent une version du protocole BB84 satisfaisant ces contraintes :

1. Alice choisit $(4+\delta)n$ bits au hasard qu'elle encore sur une base B_A au hasard.
2. Alice envoie les qubits correspondants à Bob
3. Bob reçoit les qubits, et les mesure sur une base B_B au hasard.
4. Alice annonce publiquement B_A
5. Bob rejette toutes les mesure ou son choix de base est différent de celui d'Alice. Il doit rester à Bob au moins $2n$ bits pour continuer le protocole
6. Alice et Bob sacrifient n bits au hasard pour évaluer le taux d'erreurs
7. Alice annonce publiquement $u+v$, u étant un mot de code de C_1 pris au hasard, et v les bits restants qu'elle à envoyé à Bob
8. Bob retranche $u+v$ des bits qu'il a reçu $v+\epsilon$ (ϵ est l'erreur induite par le canal et par Ève). La connaissance de C_1 et donc de u, permet de s'affranchir de ϵ.

Gottesman, Lo, Lütkenhaus et Preskill [19] ont amélioré cette preuve de sécurité pour des systèmes dont les éléments (source, détecteurs...) ont des faiblesses. Par exemple, la source ne fournit pas des états à photon unique, ou alors l'attaquant parvient à avoir une connaissance partielle des bases choisies par Alice. Dans cette étude, un deuxième attaquant Fred est présent. Celui-ci exploite les défauts de la source pour otenir une information sur la base

choisie par Alice qu'il transmet à Ève qui peut ainsi effectuer une mesure sans détruire l'état mesuré.

$$S = (1 - \Delta) - H_2(E) - (1 - \Delta)\left(1 - H_2(\frac{E}{1 - \Delta})\right) \tag{2.60}$$

E est le taux d'erreurs quantique, tandis que H_2 est l'entropie binaire. Δ est le rapport entre le nombre d'impulsions multiphotons et le nombre de détections. C'est la fraction dont on considère que Fred a pu inférer une information sur les bases choisies par Alice. Il faut quand même noter que l'arsenal des systèmes réels dont Ève peut être doté est très limité à l'heure actuelle. Par exemple, les mémoires quantiques quoiqu'existantes sont inutilisable. Donc, garder un bit en mémoire quantique jusqu'à la réconciliation reste à l'heure actuelle peu vraisemblable.

2.3.5 États leurres

Dans cette thèse le chapitre 4 est consacré à une étude statistique des attaques dites par vol de photon surnuméraires ou « Photon Number Splitting Attack ». Une autre approche appelée « Decoy State » ou états leurres est de permettre à Alice de produire des états d'énergie différente[28, 53, 22]. L'attaquant Ève ne peut distinguer ces états leurres des états normaux, et doit donc les traiter de manière identique. Si Alice divulgue lors de la réconciliation quels étaient les états leurres, alors ils donnent à Bob une information supplémentaire pour la réconciliation et la présence d'Ève.

Lo, Ma et Chen montrent que le taux de génération de la clé peut être amélioré grâce à l'utilisation de ces états leurres par rapport à la l'étude de Gottesman présenté au paragraphe précédent[19].

$$S \geq \frac{1}{2}\left(-Q_\mu f(E_\mu) H_2(E_\mu) + Q_1(1 - H_2(e_1))\right) \tag{2.61}$$

La fonction f représente l'efficacité du protocole de correction d'erreurs par rapport à la borne de Shannon. Q_μ est le gain pour les états cohérents émis par Alice, tandis que Q_1 est le gain pour les impulsions à photon unique émises par Alice. De même manière E_μ est le taux d'erreur quantique moyen, tandis que e_1 est le taux d'erreur quantique uniquement sur les impulsions à photon unique. Q_1 et Q_μ jouent le rôle ici du rapport Δ du paragraphe précédent. H_2 reste la fonction d'entropie binaire.

En conclusion, l'utilité de ce résultat est de pouvoir augmenter la distance de liaison entre Alice et Bob.

Chapitre 3

Modélisation des systèmes réels

Les systèmes de distribution quantique de clefs utilisent des systèmes réels que nous allons nous attacher à décrire, et ensuite à modéliser. Nous allons d'abord nous préoccuper des sources. Pour réaliser des systèmes pratiques de distribution quantique de clefs, nous pouvons envisager plusieurs types de sources de photons. Nous étudierons tout d'abord les sources à photon unique puis, des sources à impulsions atténuées. Nous considérerons en dernier lieu des récepteurs qu'ils soient ou non à avalanche c'est-à-dire des photodiodes PIN ou des compteurs de photons.

3.1 Sources pour la cryptographie quantique

3.1.1 Sources de photons uniques

3.1.1.1 Définition

Une source à photon unique idéale est une source de lumière capable de produire à la demande et seulement à la demande et à chaque sollicitation un photon et un seul à une longueur d'onde de télécommunications par exemple de 1 550nm.

En pratique, il reste toujours un faible nombre d'impulsions multiphotons. Nous pouvons essayer de caractériser la propension d'une source réelle à photon unique à émettre des impulsions multiphotons [11]. Soit $p(n)$ la

probabilité d'émission de n photons.

$$\begin{aligned} f_{il} &= \frac{p(n \geq 2)}{p(n \geq 1)} \\ &= \frac{\sum_{n=2}^{+\infty} p(n)}{\sum_{n=1}^{+\infty} p(n)} \end{aligned} \tag{3.1}$$

Plus la grandeur f_{il} est petite, plus la qualité de la source à photon unique est bonne. Il faut aussi que le nombre d'impulsions vides ne soit pas trop élevé.

3.1.1.2 Description des systèmes réels

Différentes approches ont été utilisés pour tenter de construire des sources à photons uniques. Il existe par exemple des sources à photons uniques constituées d'un unique dipôle ou d'une molécule [11, 2, 43] voire d'une boîte quantique [46]. Les boîtes quantiques sont des nanocristaux de matériau semi-conducteur de dimension inférieure à 10nm, et sont utilisées de manière analogue aux sources à dipole.

En fait, le phénomène utilisé est simplement une désexcitation radiative qui fournit un unique photon. On utilise un matériau construit de manière à ne compter qu'un seul site susceptible de fournir une telle désexcitation. On utilise alors une pompe pour faire entrer le système dans un état excité, et lui permettre de se désexciter pour lui faire émettre un photon. Pour que le photon suivant soit émis, le système doit nécessairement être au préalable excité à nouveau. Si le temps d'excitation de notre système est plus court que temps de vie de l'état excité, alors la probabilité d'obtenir une impulsion multiphoton reste particulièrement faible.

Des systèmes de cryptographie quantique basés sur des sources à photon unique ont été proposés [39]. Cela a conduit à un système en air libre, avec création d'une clef à 9500bits par seconde. Ces résultats sont encourageants. L'idée est d'utiliser ce genre de système pour sécuriser les communications avec des satellites.

3.1.2 Photons uniques et cryptographie quantique

3.1.3 Opérateurs création et annihilation

Nous allons chercher à introduire ici le concept d'opérateur de création et d'annihilation [14, 4]. Pour cela nous allons nous intéresser à un oscillateur harmonique.

3.1.3.1 Système classique

Soit une particule de masse m se déplaçant dans un potentiel $V(x)$ sans frottement dans une seule direction ne dépendant que de la position x.

$$V(x) = \frac{1}{2}kx^2 \tag{3.2}$$

De ce potentiel $V(x)$ dérive une force $F = -kx$. Le mouvement de la particule est régi par l'équation fondamentale de la dynamique.

$$m\frac{\mathrm{d}^2x}{\mathrm{d}t^2} = -kx \tag{3.3}$$

Et l'équation du mouvement se trouve aisément par résolution de l'équation différentielle 3.3.

$$x = x_M \cos(\omega t - \theta) \tag{3.4}$$

x_M et θ dépendent évidemment des conditions initiales. L'énergie cinétique de notre particule peut s'écrire :

$$\begin{aligned} \mathcal{E}_c &= \frac{1}{2}m\left(\frac{\mathrm{d}x}{\mathrm{d}t}\right)^2 \\ &= \frac{p^2}{2m} \end{aligned} \tag{3.5}$$

Nous avons ici introduit $p = m\dfrac{\mathrm{d}x}{\mathrm{d}t}$ qui est la quantité de mouvement. L'énergie de la particule est la somme de l'énergie potentielle et de l'énergie cinétique. La conservation de l'énergie implique que la somme de l'énergie potentielle et cinétique reste constante.

$$\mathcal{E} = \frac{p^2}{2m} + \frac{1}{2}m\omega^2x^2 \tag{3.6}$$

3.1.3.2 Système quantique

En mécanique quantique, x et p sont remplacés par les observables X et P qui ne commutent pas :

$$[X, P] = i\hbar \tag{3.7}$$

L'équation aux valeurs propres régissant notre système devient :

$$\left(-\frac{\hbar^2}{2m}\frac{\mathrm{d}^2}{\mathrm{d}x^2} + \frac{1}{2}m\omega^2x^2\right)\phi(x,t) = E\phi(x,t) \tag{3.8}$$

$\phi(x,t)$ est la fonction d'onde, tandis que E est valeur propre d'énergie. E est la valeur de l'énergie dont $\phi(x)$ est l'état. Notons qu'en écrivant une

dépendance sinusoïdale de $\phi(x,t)$ vis-à-vis du temps, on reconnaît l'équation de Schrödinger. En effet avec $\phi(x,t) = \phi(x)\exp(i\omega t)$:

$$\begin{aligned} i\hbar\frac{\partial}{\partial t}\phi(x,t) &= -\hbar\omega\phi(x)\exp(i\omega t) \\ &= E\phi(x,t) \end{aligned} \tag{3.9}$$

Cette équation peut également s'écrire sous la forme indépendante du temps :

$$\hat{H}|\phi\rangle = E|\phi\rangle \tag{3.10}$$

Nous reconnaissons l'hamiltonien H du système. Commençons tout d'abord par définir $\hat{X}$, $\hat{P}$ et $\hat{H}$:

$$\hat{X} = \sqrt{\frac{m\omega}{\hbar}}X \qquad \hat{P} = \frac{1}{\sqrt{m\omega\hbar}}P \qquad \hat{H} = \frac{1}{\hbar\omega}H \tag{3.11}$$

$\hat{X}$, $\hat{P}$ et $\hat{H}$ gardent respectivement les propriétés de X, P et H, c'est-à-dire qu'ils restent des observables. Le choix de définir ces nouvelles observables est guidé tout d'abord par un soucis de normalisation. En effet les observables obtenues correspondent à des grandeurs sans dimension. Il vient de l'équation 3.11 et de la définition de $\hat{H}$ que :

$$\hat{H} = \frac{1}{2}(\hat{X}^2 + \hat{P}^2) \tag{3.12}$$

3.1.3.3 Définition des opérateurs création et annihilation

Comme $\hat{X}$ et $\hat{P}$ sont des opérateurs qui ne commutent pas, nous ne pouvons pas factoriser $\hat{H}$ en $(\hat{X} - i\hat{P})(\hat{X} + i\hat{P})$. Nous pouvons cependant introduire :

$$\hat{a} = \frac{1}{\sqrt{2}}(\hat{X} + i\hat{P}) \qquad \hat{a}^\dagger = \frac{1}{\sqrt{2}}(\hat{X} - i\hat{P}) \tag{3.13}$$

a est appelé opérateur annihilation, et $a^\dagger$, son conjugué hermitique, est appelé opérateur création. Attardons-nous quelque peu sur $\hat{a}^\dagger\hat{a}$.

$$\begin{aligned} \hat{a}^\dagger\hat{a} &= \frac{1}{2}(\hat{X} - i\hat{P})(\hat{X} + i\hat{P}) \\ &= \frac{1}{2}(\hat{H} - 1) \end{aligned} \tag{3.14}$$

De la même manière, $\hat{a}\hat{a}^\dagger = \frac{1}{2}(\hat{H}+1)$, ce qui amène au commutateur $[\hat{a}, \hat{a}^\dagger] = 1$.

3.1.3.4 Définition de l'opérateur nombre

Définissons l'opérateur $N = \hat{a}^\dagger \hat{a}$. Notons également que :

$$\begin{aligned} [N, \hat{a}] &= \hat{a}^\dagger \hat{a}\hat{a} - \hat{a}\hat{a}^\dagger \hat{a} \\ &= (\hat{a}^\dagger \hat{a} - \hat{a}\hat{a}^\dagger)\hat{a} \\ &= -\hat{a} \end{aligned} \tag{3.15}$$

De la même manière $[N, \hat{a}^\dagger] = \hat{a}^\dagger$. Écrivons l'équation aux valeurs propres de N. Soit λ une valeur propre de N.

$$N|\phi_\lambda\rangle = \lambda|\phi_\lambda\rangle \tag{3.16}$$

ce qui revient à écrire :

$$H|\phi_\lambda\rangle = (\lambda + \frac{1}{2})\hbar\omega)|\phi_\lambda\rangle \tag{3.17}$$

3.1.3.5 Propriété des valeurs propres de l'opérateur nombre

i. Les valeurs propres sont positives

Considérons la norme du vecteur $\hat{a}|\phi_\lambda\rangle$, qui par essence est positive.

$$\begin{aligned} ||\hat{a}|\phi_\lambda\rangle||^2 &= \langle\phi_\lambda|\hat{a}^\dagger \hat{a}|\phi_\lambda\rangle \\ &= \langle\phi_\lambda|N|\phi_\lambda\rangle \\ &= \lambda\langle\phi_\lambda|\phi_\lambda\rangle \\ &= \lambda||\phi_\lambda|| \end{aligned} \tag{3.18}$$

Les normes sont positives, λ est donc une grandeur positive. Les valeurs propres de l'opérateur nombre sont positives.

ii. Construction

Or il apparaît évident que $||\hat{a}|\phi_\lambda\rangle||^2 \geq 0$, il vient alors que $\lambda \geq 0$. Considérons $N\hat{a}|\phi_\lambda\rangle$. En utilisant la relation de commutation de N et de $\hat{a}$ nous avons :

$$\begin{aligned} N\hat{a}|\phi_\lambda\rangle &= (\hat{a}N - \hat{a})|\phi_\lambda\rangle \\ &= (\lambda\hat{a} - \hat{a})|\phi_\lambda\rangle \\ &= (\lambda - 1)\hat{a}|\phi_\lambda\rangle \end{aligned} \tag{3.19}$$

Nous avons montré à travers le calcul 3.19, qu'à partir du moment où $|\phi_\lambda\rangle$ est non nul et que $|\phi_\lambda\rangle$ est vecteur propre de N, alors $\hat{a}|\phi_\lambda\rangle$ l'est également. Le vecteur $\hat{a}|\phi_\lambda\rangle$ est alors associé à la valeur propre $\lambda - 1$. On pourrait montrer de manière analogue en utilisant le commutateur $[N, \hat{a}^\dagger]$ que si $|\phi_\lambda\rangle$ est vecteur propre de N alors $\hat{a}^\dagger N$ est également vecteur propre de N avec la valeur propre $\lambda + 1$.

iii. Ensemble des valeurs propres

Considérons une valeur propre λ de N associée au vecteur $|\phi_\lambda\rangle$. Appliquons $\hat{a}$ de manière répétée. Comme les valeurs propres de N sont positives, le spectre admet un plus petit élément λ_{min} associé à $|\phi_{\lambda_{min}}\rangle$. Il vient donc, en rappelant la condition de non nullité énoncée au paragraphe ii, que $\hat{a}|\phi_{\lambda_{min}}\rangle = 0$. Étant donné l'équation 3.18, λ_{min} est alors nulle. Il en résulte, compte tenu des conditions de construction que le spectre de N est formé des entiers naturels positifs.

iv. Non-dégénérescence des états propres de l'opérateur nombre

1. Nous avons à l'état fondamental :

$$\begin{aligned} \hat{a}|\phi_0\rangle &= 0 \\ (\hat{X} + i\hat{P})|\phi_0\rangle &= 0 \end{aligned} \tag{3.20}$$

   Au vu de $\hat{X} + i\hat{P}$, l'espace solution est de dimension unitaire, l'état fondamental est non-dégénéré.

2. État n

   Supposons que l'état n soit non dégénéré, et montrons que l'état $n+1$ l'est également. Soit $N|\phi_{n+1}^k\rangle = (n+1)|\phi_{n+1}^k\rangle$. k est l'indice de dégénérescence de l'état $|\phi_{n+1}\rangle$. Par hypothèse on sait que $\hat{a}|\phi_{n+1}^k\rangle$ est vecteur propre de N, non dégénéré. Il existe donc c^k tel que :

$$\begin{aligned} \hat{a}|\phi_{n+1}^k\rangle &= c^k|\phi_n\rangle \\ \hat{a}^\dagger\hat{a}|\phi_{n+1}^k\rangle &= \hat{a}^\dagger c^k|\phi_n\rangle \\ (n+1)|\phi_{n+1}^k\rangle &= \frac{c^k\hat{a}^\dagger}{n+1}|\phi_n\rangle \end{aligned} \tag{3.21}$$

   On sait que $\hat{a}^\dagger|\phi_n\rangle$ est vecteur propre de N avec la valeur propre $n+1$. Nous remarquons donc que tous les $|\phi_{n+1}^k\rangle$ sont proportionnels à $\hat{a}^\dagger|\phi_n\rangle$. Supposons que les états propres $|n\rangle$ sont normalisés. Il en découle $\hat{a}|n\rangle = \sqrt{n}|n-1\rangle$ et $\hat{a}^\dagger|n\rangle = \sqrt{n}|n+1\rangle$ ce qui explique les noms d'opérateur annihilation et création. Ces opérateurs font passer de l'état d'énergie $(n+\frac{1}{2})h\lambda$ à l'état d'énergie $(n+\frac{1}{2}) \pm 1\hbar\lambda$: ils rajoutent ou enlèvent un quantum d'énergie $h\lambda$. De la même manière l'opérateur nombre N est associé au nombre de quanta.

3.1.4 États cohérents et statistique d'émission

Les particules qui nous intéressent sont des photons. Les sources dont nous disposons sont considérées cohérentes. Il nous importe donc de caractériser la source par les états qu'elle est capable de délivrer. Un état cohérent est

défini par $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$ [4, 18] où α est la valeur moyenne de la norme de $|\alpha\rangle$. On voit immédiatement que l'opérateur $\hat{a}$ admet α pour valeur propre avec $|\alpha\rangle$ comme vecteur propre associé. Nous remarquons la propriété suivante de l'état cohérent : si on applique l'opérateur création à un état cohérent, cela reste un état cohérent. Nous allons essayer de décrire un état cohérent, suivant les propriétés que nous connaissons. Écrivons tout d'abord $|\alpha\rangle$ sous la forme $|\alpha\rangle = \sum_n C_n|n\rangle$ car $\{|n\rangle\}$ est une base des états propres de $\hat{a}$.

$$\begin{aligned} |\alpha\rangle &= \sum_c C_n|n\rangle \\ \hat{a}|\alpha\rangle &= \sum_{n\geq 0} C_n\hat{a}|n\rangle \\ \alpha|\alpha\rangle &= \sum_{n\geq 1} C_n\sqrt{n}|n-1\rangle \\ \alpha|\alpha\rangle &= \sum_{n\geq 1} C_{n+1}\sqrt{n+1}|n\rangle \end{aligned} \tag{3.22}$$

Il faut maintenant déterminer C_0.

$$\begin{aligned} \alpha C_{n-1} &= C_n\sqrt{n} \\ \alpha C_{n-2} &= C_{n-1}\sqrt{n-1} \\ \alpha C_{n-3} &= C_{n-2}\sqrt{n-2} \\ &\vdots \\ \alpha C_1 &= C_2\sqrt{2} \\ \alpha C_0 &= C_1 \end{aligned} \tag{3.23}$$

Il vient alors immédiatement $\alpha^n C_0 = C_n\sqrt{n!}$. Nous cherchons à ce que notre état cohérent soit normalisé, cette condition nous permet de déterminer C_0. Écrire que $|\alpha\rangle$ doit être normalisé revient à écrire $\langle\alpha|\alpha\rangle = 1$ et pour nous cette condition se traduit par $\sum_n C_n^2 = 1$. Utiliser l'expression de C_n en fonction de C_0 :

$$\sum_n \left(\frac{\alpha^n C_0}{\sqrt{n!}}\right)^2 = 1 \tag{3.24}$$

Nous pouvons déduire C_0 de cette écriture, en effet nous reconnaissons le développement en série entière d'une fonction exponentielle :

$$C_0 = e^{-\frac{1}{2}|\alpha|^2} \tag{3.25}$$

Il vient maintenant pour l'expression de notre état cohérent développé en états de nombre :

$$|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2}\sum_n \frac{\alpha^n}{\sqrt{n!}}|n\rangle \tag{3.26}$$

Il ne reste plus qu'à calculer la probabilité d'observer n quanta dans un état cohérent :

$$\begin{aligned} \mathcal{P}(n) &= |\langle n|\alpha\rangle|^2 \\ &= |\frac{e^{-\frac{1}{2}|\alpha|^2}\alpha^n}{\sqrt{n!}}|^2 \end{aligned} \tag{3.27}$$

Nous reconnaissons une loi de probabilité poissonnienne, de paramètre $|\alpha|^2$. Intéressons-nous à la valeur moyenne de l'opérateur nombre :

$$\begin{aligned} \langle N\rangle &= \langle\alpha|N|\alpha\rangle \\ &= \mathrm{Tr}\,|\alpha\rangle\langle\alpha|N \\ &= \sum_n \langle n|\alpha\rangle\langle\alpha|N|n\rangle \\ &= \sum_n n|\langle n|\alpha\rangle|^2 \\ &= \sum_n n\mathcal{P}(n) \end{aligned} \tag{3.28}$$

Cette valeur moyenne est égale à l'espérance de la probabilité d'observer n photons dans un état cohérent, c'est donc aussi le paramètre de notre probabilité poissonnienne soit $|\alpha|^2$. C'est aussi le nombre moyen de photons par impulsion. Par soucis de simplicité, nous noterons dorénavant $\mu = |\alpha|^2$. Nous avons montré que la distribution des photons suit strictement une loi poissonnienne. Ce n'est pas une approximation.

3.1.5 Sources de photons atténués

En guise de source de photons, nous utilisons un laser fortement atténué, de manière à ce qu'il ne délivre que peu d'impulsions multiphotons. Ce laser émet des états cohérents. Nous avons vu que ceux-ci ont la particularité de suivre une densité de probabilité de présence poissonnienne. En choisissant un nombre moyen de photons donnés, nous sommes en mesure de choisir un nombre arbitrairement bas d'impulsions multiphotons. En contrepartie, il faudra compter sur un nombre élevé d'impulsions vides. Typiquement les communications se font en utilisant $0,1$ à $0,3$ photons par qubit.

3.2 Récepteur

3.2.1 Détection homodyne

3.2.1.1 Photodiode PIN

Une photodiode est un composant à semi-conducteur capable d'aborder la lumière [30]. Dans une jonction PN utilisée couramment se trouvent une

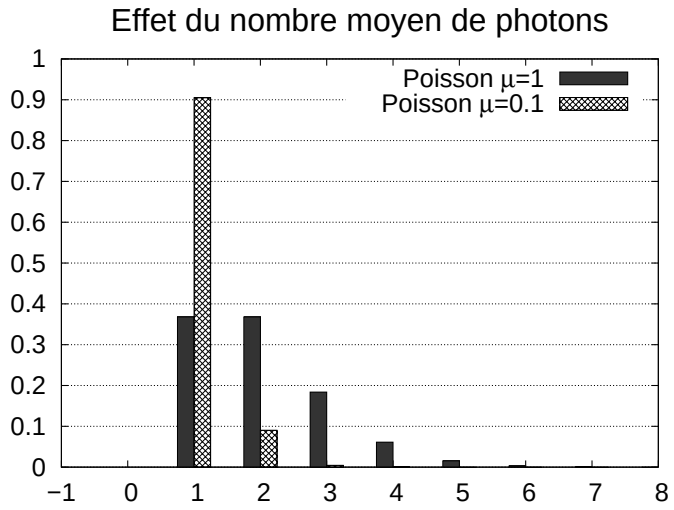

FIG. 3.1 – Nombre de photons par impulsion en fonction du nombre moyen de photons

zone P, déficitaire en électron et une zone N, excédentaire en électrons. Ce déséquilibre force les électrons à migrer jusqu'à trouver un équilibre stable, qui voit se former une zone de charge d'espace et une différence de potentiel. Suivant que l'on compense ou non cette différence de potentiel, la jonction est dite passante ou bloquée. En effet, si l'on compense entièrement la différence de potentiel, la zone de charge d'espace se trouve annulée, et la diode se comporte comme un conducteur, on dit que la polarisation est directe. Si la différence de potentiel n'est pas compensée, alors la diode se comporte comme un matériau isolant et on dit que la diode est polarisée en inverse. Si l'on applique aucune tension sur la jonction, la diode n'est alors pas polarisée.

Dans une photodiode, il se trouve une zone dite intrinsèque entre la zone P et la zone N. Quand la lumière d'un photon se présente sur le substrat de la photodiode avec assez d'énergie une paire électron-trou est libérée. L'énergie E_g de référence est propre au matériau utilisé pour construire la photodiode, elle est par exemple de $1.12eV$ pour le silicium. Cela crée un courant électrique proportionnel au nombre de photons incidents. La création de ce photo-courant est indépendante de la polarisation, mais la mesure du photo-courant peut se simplifier avec une polarisation adéquate. Comme l'énergie portée par un photon vaut $h\nu$, il faut que la fréquence ν soit supérieure à $\frac{E_g}{h}$.

De plus, on appelle efficacité η, le rapport du nombre de paires créées sur le nombre de photons incidents. Cette efficacité peut atteindre 80%. On appelle courant d'obscurité le courant qui parcourt la photodiode lorsque celle-ci n'est pas éclairée.

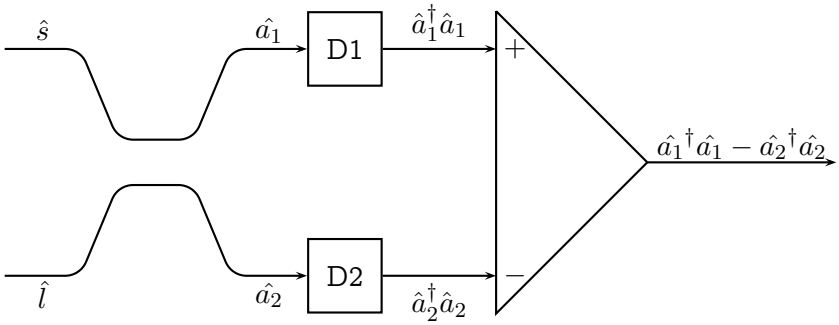

FIG. 3.2 – Récepteur homodyne avec deux photodiodes composant D1 et D2

3.2.1.2 Théorie de la détection homodyne

Nous présentons ici une théorie quantique simplifiée de la détection homodyne [17, 18]. Le dispositif est présenté sur la figure 3.2. La grandeur $\hat{s}$ est le signal, la grandeur $\hat{l}$ est un oscillateur local tandis que $\hat{a}_1$ et $\hat{a}_2$ sont les grandeurs composites après la traversée du coupleur par le signal.

Nous considérons un coupleur 50 : 50, et donc nous avons :

$$\begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix} \begin{pmatrix} \hat{s} \\ \hat{l} \end{pmatrix} \tag{3.29}$$

On obtient donc :

$$\begin{aligned} \hat{a}_1 &= \frac{1}{\sqrt{2}}(\hat{s} - i\hat{l}) \\ \hat{a}_2 &= \frac{1}{\sqrt{2}}(-i\hat{s} + \hat{l}) \end{aligned}$$

Par conjugaison hermitienne, nous obtenons :

$$\begin{aligned} \hat{a}_1^\dagger &= \frac{1}{\sqrt{2}}(\hat{s}^\dagger + i\hat{l}^\dagger) \\ \hat{a}_2^\dagger &= \frac{1}{\sqrt{2}}(+i\hat{s}^\dagger + \hat{l}^\dagger) \end{aligned}$$

Les photodiodes D1 et D2 sont sensibles au nombre de photons, c'est-à-dire à l'opérateur nombre :

$$\begin{aligned} \hat{a}_1^\dagger \hat{a}_1 &= \frac{1}{2}(\hat{s}^\dagger + i\hat{l}^\dagger)(\hat{s} - i\hat{l}) \\ &= \frac{1}{2}(\hat{s}^\dagger \hat{s} + \hat{l}^\dagger \hat{l} - i(\hat{s}^\dagger \hat{l} - \hat{l}^\dagger \hat{s})) \end{aligned} \tag{3.30}$$

On montre de la même manière que :

$$\hat{a}_2^\dagger \hat{a}_2 = \frac{1}{2}(\hat{s}^\dagger \hat{s} + \hat{l}^\dagger \hat{l} + i(\hat{s}^\dagger \hat{l} - \hat{l}^\dagger \hat{s})) \tag{3.31}$$

Après la soustraction des deux signaux, nous obtenons en sortie :

$$\begin{aligned} \hat{N} &= \hat{a}_1^\dagger \hat{a}_1 - \hat{a}_2^\dagger \hat{a}_2 \\ &= -i(\hat{s}^\dagger \hat{l} - \hat{l}^\dagger \hat{s}) \end{aligned} \tag{3.32}$$

En exprimant $\hat{s}$ et $\hat{l}$ en fonction de leur terme en phase et en quadrature nous obtenons :

$$\begin{aligned} \hat{s} &= \hat{s}_1 + i\hat{s}_2 \\ \hat{l} &= -\hat{l}_2 + i\hat{l}_1 \end{aligned} \tag{3.33}$$

$\hat{s}^\dagger$ et $\hat{l}^\dagger$ sont les conjugués hermitiens de $\hat{s}$ et $\hat{l}$. En exprimant en fonction de leurs termes en phase et en quadrature nous obtenons donc :

$$\begin{aligned} \hat{s}^\dagger &= \hat{s}_1 - i\hat{s}_2 \\ \hat{l}^\dagger &= -\hat{l}_2 - i\hat{l}_1 \end{aligned} \tag{3.34}$$

En utilisant ces écritures décomposées en termes en phase et en quadrature, nous obtenons pour $\hat{N}$.

$$\begin{aligned} \hat{N} &= -i(\hat{s}^\dagger \hat{l} + \hat{l}^\dagger \hat{s}) \\ &= j\left((\hat{s}_1 - i\hat{s}_2)(-\hat{l}_2 + i\hat{l}_1) - (-\hat{l}_2 - i\hat{l}_1)(\hat{s}_1 + i\hat{s}_2)\right) \\ &= 2(\hat{s}_1 \hat{l}_1 + \hat{s}_2 \hat{l}_2) \end{aligned} \tag{3.35}$$

Pour ce calcul, nous avons utilisé le fait que $\hat{s}_1$ et $\hat{l}_2$ d'une part et $\hat{s}_2$ et $\hat{l}_1$ commutent, car il sont issus de grandeurs pouvant faire sans pénalité l'objet de mesures indépendantes. Décomposons chaque terme en la somme d'une valeur moyenne classique et d'une partie fluctuante quantique.

$$\begin{aligned} \hat{s}_1 &= S_1 + \Delta\hat{s}_1 \qquad S_1 = \langle \hat{s}_1 \rangle \\ \hat{s}_2 &= S_2 + \Delta\hat{s}_2 \qquad S_2 = \langle \hat{s}_2 \rangle \\ \hat{l}_1 &= L_1 + \Delta\hat{l}_1 \qquad L_1 = \langle \hat{l}_1 \rangle \\ \hat{l}_2 &= L_2 + \Delta\hat{l}_2 \qquad L_2 = \langle \hat{l}_2 \rangle \end{aligned}$$

D'abord nous considérons que l'oscillateur local est composé d'une seule quadrature, nous choisissons L_1, donc $L_2 = 0$. Ensuite nous nous plaçons dans le cas où l'onde de référence est forte, c'est-à-dire que $L_1^2 \gg S_1^2 + S_2^2$. Dans ce cas nous obtenons :

$$\hat{N} \approx 2(S_1 + \Delta\hat{s}_1)L_1 \tag{3.36}$$

Il apparaît donc que les fluctuations de l'oscillateur référence sont rejetées. Seules les fluctuations du signal contribuent au bruit en sortie. Elles sont d'ailleurs les fluctuations du vide entrant dans le coupleur et amplifiées sans bruit par le gain de l'oscillateur référence.

Plaçons-nous maintenant dans un cas légèrement différent. Supposons que l'oscillateur local fasse un angle $\Phi + \frac{\pi}{2}$ par rapport à $\hat{s} = \hat{s}_1$ considéré comme l'origine des phases. Nous avons donc $\hat{l} = le^{i(\Phi+\frac{\pi}{2})}$. En reprenant un calcul analogue au calcul précédent, ces conventions nous mènent directement au résultat :

$$\hat{N}\hat{s}_1 l \cos\Phi \tag{3.37}$$

3.2.2 Compteur de photons

3.2.2.1 Photodiodes à avalanche

Lorsque l'on augmente la polarisation électrique en inverse, la zone de charge d'espace continue de s'agrandir jusqu'à ce que le champ électrique en son sein atteigne la valeur maximale acceptable par le matériau utilisé. La force liée au champ électrique devient supérieure à la cohésion des électrons du cristal, ceux-ci sont alors arrachés. La tension n'augmente plus, et le cristal devient conducteur. Par exemple, dans le silicium, la valeur maximale du champ électrique est de $10^6 Vcm^{-1}$. Cet effet s'appelle l'effet Zéner.

De plus l'accélération acquise par ces porteurs peut être suffisante pour ioniser et libérer du cristal des porteurs voisins, c'est le phénomène d'avalanche. Le gain obtenu peut être très élevé.

Un désavantage de ces photodiodes est leur faible efficacité. En effet, l'efficacité de telles photodiodes est typiquement de l'ordre de 0.1. Le système de détection doit également prendre en compte un temps mort utilisé pour éteindre l'avalanche puis repolariser la photodiode (c'est en fait un réarmement préalable à une nouvelle mesure).

Ces photodiodes à avalanche souffrent également d'un taux de coup d'obscurité. C'est l'équivalent du courant d'obscurité de la photodiode PIN. De temps en temps, alors qu'aucun photon ne devrait être détecté, une avalanche se produit. Cet effet [44] est principalement dû à des électrons libres qui se trouvent piégés pendant l'avalanche, et qui n'ont pas le temps de diffuser pendant le temps mort de repolarisation. Cela impose un choix minimal pour le temps mort, et ainsi influe sur la fréquence maximale de mesure qui peut être choisie.

3.2.2.2 Modélisation du récepteur à compteur de photons

Le matériel disponible au laboratoire contient deux compteurs de photons construits par Id Quantique. Sur ces détecteurs, des données techniques constructeurs indiquent que le choix du temps mort, du taux de coup d'obscurité et de l'efficacité participent d'un compromis [23]. Dans nos simulations nous choisirons un compromis acceptable au vu des valeurs proposées. Soient une probabilité de coup d'obscurité de 2.10^{-5} et une efficacité de 10%.

Chapitre 4

Attaque par vol de photons surnuméraires

L'attaque par vol de photon surnuméraire ou *Photon Number Splitting Attack* en anglais est une attaque incohérente basée sur la non-perfection des sources dites atténuées. En effet, à chaque fois que plus de deux photons se présentent au dispositif d'Ève, elle en prélève un pour effectuer les mesures qui lui semblent les plus adéquates.

Dans ce chapitre nous étudions les détecteurs à avalanche. Nous les plaçons ensuite dans un contexte de détection directe de phase, puis enfin dans le cas de direction différentielle de phase.

4.1 Distribution après l'attaque par « vol de photon surnuméraire »

L'idée de cette attaque est d'exploiter la faiblesse des sources dites atténuées utilisées dans les transmissions quantiques. En effet, alors qu'une source idéale transmettrait un et un seul photon par qubit, nous nous contentons d'utiliser une source poissonnienne fortement atténuée, de manière à

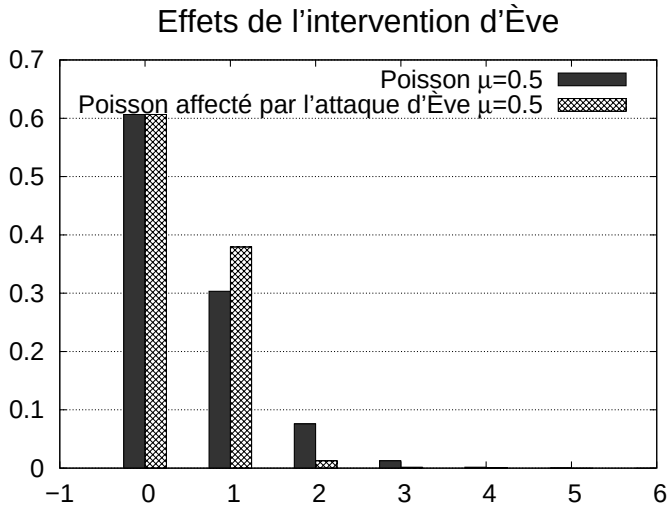

FIG. 4.1 – Probabilité d'impulsion multiphoton suivant le nombre moyen de photons après intervention d'Ève

n'obtenir que rarement des impulsions multiphotons comme présenté dans le chapitre précédent par la figure 3.1. L'attaque se passe comme suit :

- S'il ne passe aucun photon, l'attaquant Ève ne fait rien.
- S'il passe un et un seul photon, l'attaquant bloque un taux ϵ de photons. Notons que ϵ est compris entre 0 et 1.
- S'il passe au moins deux photons, Ève en prélève un et un seul.

La distribution de photons se trouve donc ainsi modifiée :

$$\begin{cases} p(0) = e^{-\mu} + \epsilon\mu e^{-\mu} \\ p(1) = \mu(1-\epsilon)e^{-\mu} + \frac{\mu^2 e^{-\mu}}{2} \\ \forall k \in \mathbb{N} - \{0,1\},\ p(k) = \frac{\mu^{k+1} e^{-\mu}}{(k+1)!} \end{cases} \tag{4.1}$$

Ève a perturbé la statistique poissonnienne originelle. La nouvelle statistique est présentée également dans la figure 4.1 à coté de la statistique poissonnienne dont elle résulte. Nous voyons nettement l'augmentation du nombre d'impulsions à photon unique au détriment de l'augmentation du nombre d'impulsions à deux photons. Dans cet exemple nous avons choisi de fixer le paramètre ϵ à zéro, cela simule le cas oùu Ève ne bloque aucun photon au cours de son attaque. Cela permet d'analyser aisément l'incidence d'Ève sur la statistique poissonnienne orginale.

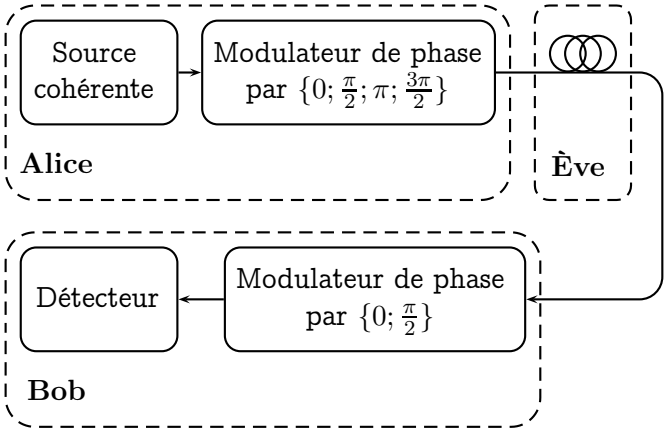

Fig. 4.2 – Schéma de principe du lien entre Alice et Bob, pour un encodage basé sur la phase

4.2 Statistique de détection avec des compteurs de photons

Nous considérons ici une photodiode à avalanche dotée d'un rendement quantique η, ce qui signifie que si un photon arrive sur le détecteur celui-ci a une probabilité η d'être détecté, ou par équivalence une probabilité $1-\eta$ de ne pas être détecté. Si maintenant deux photons indépendants atteignent quasi-simultanément la photodiode, celle-ci a une probabilité $(1-\eta)^2$ de ne détecter aucun des deux photons. Ceci revient à écrire que la photodiode à une probabilité $1-(1-\eta)^2$ de détecter un au moins des deux photons. Plus généralement, en faisant l'hypothèse d'indépendance des photons dans le détecteur, si k photons arrivent sur la photodiode, la probabilité d'obtenir une détection est donnée par :

$$1-(1-\eta)^k \tag{4.2}$$

Étant donnée une photodiode de rendement 10%, l'équation 4.2 peut être simplifiée en $1-0,9^k$. notons que nous obtenu l'équation 4.2 par un raisonnement indirect impliquant la probabilité de non détection des photons. Un raisonnement n'impliquant que les probabilités de détection n'est pas possible-car la diode ne peut détecter plusieurs photons arrivant quasi-simultanément.

4.3 Détection idéale de phase

Nous considérons ici un protocole de type BB84 utilisant un codage de phase. L'information est donc directement stockée par la valeur de la phase.

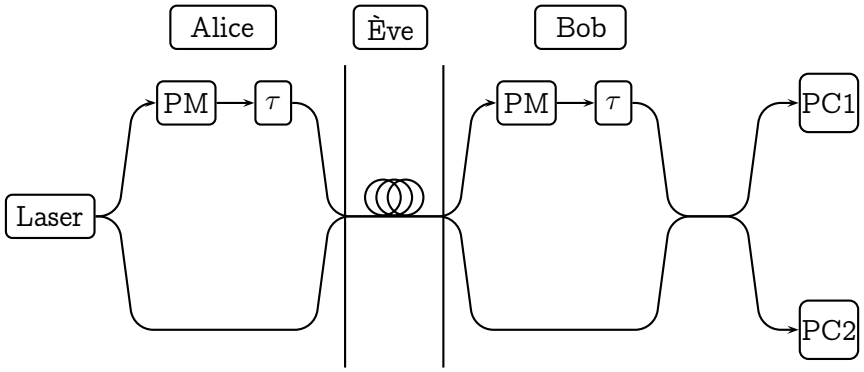

FIG. 4.3 – Montage expérimental, en mode compteurs de photons

La figure 4.2 montre l'arrangement possible d'un protocole avec utilisation d'une phase absolue. L'action d'Ève est limitée au lien reliant Alice et Bob, car nous considérons qu'Ève n'a ni accès au laboratoire d'Alice, ni à celui de Bob et ne peut modifier leurs systèmes d'émission et de détection.

Pour détecter la phase, nous utilisons une onde de référence. Le système est composé de deux interféromètres de Mach-Zehnder représentés sur la figure 4.3. Le premier est placé dans le laboratoire d'Alice tandis que le second est placé dans le laboratoire de Bob. Ève est cachée dans la ligne de fibre optique. Les retards τ matérialisent la présence dans chaque intérféromètre d'un bras court et d'un bras long. L'interférence du signal bras court-bras long avec le signal bras long-bras court nécessite une valeur de τ constante pour les deux bras longs. Les photons qui font les trajets bras court-bras court et bras long-bras long ne sont pas pris en compte. Le résultat des interférences est mesuré sur les compteurs de photons PC1 et PC2. La visibilité de l'interféromètre participe du taux d'erreur de mesures que l'on appellera QBER. Notons que de par la construction du système, et plus spécifiquement du choix des ses récepteurs, nous ne pouvons nous permettre aucun recul sur les décisions de détection. En effet la detection fournit un résultat binaire, sans aucun matériel permettant de remettre en question la mesure ou de prendre un quelconque recul vis à vis de ce résultat.

Le tableau 4.1 renseigne sur la conclusivité des mesures observées chez Bob par rapport aux choix de base faits chez Alice, en accord avec le protocole BB84. Le choix de l'état chez Alice détermine à la fois le choix de la valeur d'un bit (0 ou 1) et le choix de la base (A ou B), alors que Bob ne choisit que la base, et effectue une mesure de déphasage grâce à deux photodétecteurs et un interféromètre de Mach-Zehnder. Le choix des phases d'Alice et Bob correspond uniquement aux choix des bases du protocole BB84. La grandeur

Alice			Bob		Clef
Bases	Bit	Phase	Bases	Phase	Bit
A	0	$+0$	A	$+0$	C
			B	$+\frac{\pi}{2}$	NC
A	1	$+\pi$	A	$+0$	C
			B	$+\frac{\pi}{2}$	NC
B	0	$+\frac{\pi}{2}$	A	$+0$	NC
			B	$+\frac{\pi}{2}$	C
B	1	$+\frac{3\pi}{2}$	A	$+0$	NC
			B	$+\frac{\pi}{2}$	C

Tab. 4.1 – Modulation de phase d'Alice et Bob

mesurée qui permet de conclure est le déphasage observée par Bob. En cas de concordance de base entre Alice et Bob, si ce déphasage est nul, alors le bit envoyé est 0, si ce déphasage vaut π alors le bit envoyé est 1. Si les bases ne concordent pas, la valeur mesurée est alors $\frac{\pi}{2}$ à π près et ne permet pas de conclure.

4.3.1 Probabilité de détection

Nous voulons obtenir la probabilité p_{Bob} de détecter au moins un photon. Nous connaissons la probabilité de présence de k photons grâce à l'équation 3.27 et la probabilité d'en détecter au moins un parmi ces k photons grâce à l'équation 4.2. La probabilité que k photons parviennent au détecteur, et que celui-ci en détecte au moins un parmi k est donnée par :

$$p_{Bob}(k) = \frac{\mu^k e^{-\mu}}{k!}(1-(1-\eta)^k)$$

Le résultat que nous cherchons est l'ensemble des probabilités pour tous les k entiers. Donc pour obtenir la probabilité voulue, il suffit de faire la somme des probabilités $p_{Bob}(k)$ pour k variant de 0 à l'infini.

$$\begin{aligned} p_{Bob} &= \sum_{k=0}^{\infty} \frac{\mu^k e^{-\mu}}{k!}(1-(1-\eta)^k) \\ &= e^{-\mu}((e^{\mu}-1)-(e^{(1-\eta)\mu}-1)) \\ &= 1-e^{-\mu}-e^{-\eta\mu}+e^{-\mu} \\ p_{Bob} &= 1-e^{-\eta\mu} \end{aligned} \tag{4.3}$$

La probabilité d'obtenir une détection dans le cas d'un système de détection directe de phase sans intervention d'Ève, ne dépend pas que du produit du rendement quantique du détecteur et du paramètre d'intervention de de trafic

de la source. Ce produit forme le paramètre d'une exponentielle décroissante constituant notre probabilité de détection. En effet, lorsque le rendement η augmente, ou bien quand le nombre moyen de photons μ augmente, on observe une augmentation de la probabilité de détection sur le photodétecteur de Bob. Il faut également remarquer que l'efficacité η (comprise entre 0 et 1) agit chez Bob comme un facteur diminuant le nombre moyen de photons μ. En effet, du point de vue de Bob tout se passe comme s'il avait un détecteur parfait, et une statistique de photons poissonnienne de nombre moyen de photons $\eta\mu$.

4.3.2 Probabilité de détection après l'attaque

Pour chercher la probabilité de détection d'un photon chez Bob, il nous faut combiner les équations 4.2 et 4.1 de manière similaire à ce qui a été fait au paragraphe 4.3.1 pour obtenir l'équation 4.3. Nous obtenons ce calcul :

$$\begin{aligned}
p_{Bob} &= e^{-\mu} \times 0 + ((1-\epsilon)\mu e^{-\mu} + \frac{\mu^2}{2}e^{-\mu}) \times \eta \\
&\quad + \sum_{k=2}^{\infty} \frac{\mu^{k+1}e^{-\mu}}{(k+1)!}\left(1-(1-\eta)^k\right) \\
&= \eta(1-\epsilon)\mu e^{-\mu} + \frac{\eta\mu^2 e^{-\mu}}{2} \\
&\quad + e^{-\mu}\left(\sum_{3}^{\infty}\frac{\mu^k}{k!} - \frac{1}{1-\eta}\sum_{3}^{\infty}\frac{(\mu(1-\eta))^k}{k!}\right) \\
&= \eta(1-\epsilon)\mu e^{-\mu} + \frac{\eta\mu^2 e^{-\mu}}{2} + 1 - \frac{\mu^2 e^{-\mu}}{2} - \mu e^{-\mu} \\
&\quad - e^{-\mu} - \frac{e^{-\eta\mu}}{1-\eta} + \frac{e^{-\mu}\mu^2(1-\eta)}{2} + \mu e^{-\mu} + \frac{e^{-\mu}}{1-\eta} \\
p_{Bob} &= 1 + (1-\epsilon)\eta\mu e^{-\mu} - \frac{e^{-\mu\eta}}{1-\eta} + e^{-\mu}\frac{\eta}{1-\eta} \qquad (4.4)
\end{aligned}$$

Cette intervention de l'attaquant sur notre système devrait représenter une diminution de la probabilité de détection. Nous nous proposons d'analyser cette perte en terme de probabilité de détection. Pour cela, commençons par exprimer la différence $D(\mu)$ entre l'expression 4.3 et 4.4.

$$\begin{aligned}
D(\mu) &= 1 - e^{-\eta\mu} - (1 + \epsilon\eta\mu e^{-\mu} - \frac{e^{\mu\eta}}{1-\eta} + e^{-\mu}\frac{\eta}{1-\eta}) \\
&= (1-\epsilon)\eta\mu e^{-\mu} + \frac{\eta}{1-\eta}(e^{-\mu\eta} - e^{-\mu}) \\
D(\mu) &= \frac{\eta}{1-\eta}e^{-\eta\mu} + \frac{\eta}{1-\eta}e^{-\mu}((1-\eta)(\epsilon-1)\mu - 1)
\end{aligned}$$

Nous cherchons tout d'abord le signe de $D(\mu)$. Soit $E(\mu) = \frac{1-\eta}{\eta}e^{\mu}D(\mu)$. Comme η est un rendement compris entre 0 et 1, $E(\mu)$ est donc du même

signe que $D(\mu)$. L'étude du signe de $D(\mu)$ revient donc à l'étude du signe de $E(\mu)$.

$$\begin{aligned} E(\mu) &= \frac{1-\eta}{\eta} e^{\mu} D(\mu) \\ E(\mu) &= e^{-\mu(\eta-1)} + (1-\eta)(\epsilon-1)\mu - 1 \end{aligned}$$

Pour obtenir le signe de $E(\mu)$ nous allons étudier les variations de $E(\mu)$ à l'aide de sa dérivée.

$$\frac{\mathrm{d}E}{\mathrm{d}\mu} = -(\eta-1)e^{-\mu(\eta-1)} + (1-\eta)(\epsilon-1) \tag{4.5}$$

Étudions le signe de l'expression de $\frac{dE}{d\mu}$.

$$\begin{aligned} \frac{\mathrm{d}E}{\mathrm{d}\mu} > 0 &\iff (1-\eta)e^{-\mu(\eta-1)} + (1-\eta)(\epsilon-1) > 0 \\ &\iff e^{-\mu(\eta-1)} > 1-\epsilon \\ &\iff \mu > \frac{\ln(1-\epsilon)}{1-\eta} \end{aligned}$$

Notons que $\mu_0 = \frac{\ln(1-\epsilon)}{1-\eta}$ est négatif, ce qui montre que $\frac{dE}{d\mu}$ est positif sur notre intervalle d'intérêt $\mathbb{R}^+$.

$$\begin{aligned} E(0) &= 0 \\ \lim_{\mu\to\infty} E(\mu) &= +\infty \end{aligned} \tag{4.6}$$

Tous ces éléments sont représentés dans le tableau 4.2. La lecture de ce tableau nous apprend que $E(\mu)$ est positif et donc que $D(\mu)$ l'est également.

Nous pouvons aller encore plus loin et obtenir les variations de $D(\mu)$. Pour cela reprenons :

$$\begin{aligned} E(\mu) &= \frac{1-\eta}{\eta} e^{\mu} D(\mu) \\ \frac{\mathrm{d}E}{\mathrm{d}\mu} &= \frac{1-\eta}{\eta} e^{\mu} D\mu + \frac{1-\eta}{\eta} e^{\mu} \frac{\mathrm{d}D}{\mathrm{d}\mu} \\ \frac{\mathrm{d}D}{\mathrm{d}\mu} &= \frac{\eta}{1-\eta} \frac{\mathrm{d}E}{\mathrm{d}\mu} + e^{\mu} D(\mu) \end{aligned} \tag{4.7}$$

Pour illustrer cette étude, nous avons représenté la différence $D(\mu)$ sur la figure 4.4. Nous avons donc vérifié le caractère néfaste de l'intervention d'Ève sur la capacité de détection de Bob.

μ	0	$+\infty$
$\frac{\mathrm{d}E}{\mathrm{d}\mu}(\mu)$	$+$	
$E(\mu)$	0 ↗	$+\infty$

TAB. 4.2 – Tableau de variation de $E(\mu)$

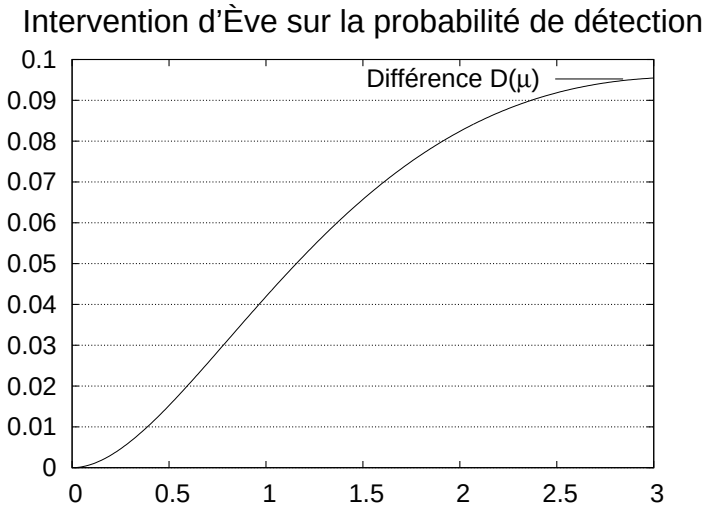

FIG. 4.4 – Différence des probabilités de détections sans et avec la présence d'Ève en fonction du nombre moyen de photons

4.3.3 Information mutuelle

Pour mesurer la sécurité réalisée sur le lien entre Alice et Bob, nous devons utiliser une expression de l'information mutuelle. Nous pouvons définir la quantité de sécurité (X, Y_{Bob}, Y_{Eve}) par la différence entre l'information mutuelle entre Alice et Bob d'une part $(I(X, Y_{Bob}))$ et l'information mutuelle entre Alice et Ève $(I(X, Y_{Eve}))$ d'autre part. X est la variable aléatoire correspondant au signal généré par Alice tandis que Y_{Bob} et Y_{Eve} sont les variables aléatoires des signaux qui arrivent chez Bob et Ève.

$$S(X, Y_{Bob}, Y_{Eve}) = I(X, Y_{Bob}) - I(X, Y_{Eve}) \tag{4.8}$$

La condition nécessaire pour que le lien soit sécurisé est que S soit positif. En effet, la clef ne peut être considérée comme fiable que si la quantité d'information mutuelle entre Alice et Bob est supérieure à celle entre Alice et Ève. Le but est donc de maximiser $S(X, Y_{Bob}, Y_{Eve})$ de manière à pouvoir générer une clef la plus sécurisée et la plus large possible.

4.3.3.1 Modélisation du canal

Nous faisons l'hypothèse d'un canal à effacement. En effet nos détecteurs ont une efficacité très basse de l'ordre de 10%, donc il arrive souvent qu'ils ne détectent pas les photons incidents, c'est ce que nous appelons effacement. Nous notons e_r l'événement effacement.

$$X = \{0; 1\} \qquad Y = \{0; 1; e_r\}$$

X est l'ensemble des entrées possibles de notre canal, et Y est l'ensemble des sorties possibles. Nous tenons compte des coups d'obscurité à travers le paramètre α. Si les deux détecteurs cliquent en même temps à cause d'un coup d'obscurité, alors nous faisons comme s'il y avait un effacement, car aucune décision ne peut être prise. Ainsi nous avons pris en compte dans notre modèle deux types de problèmes dans la détection, les erreurs et les effacements.

$$\begin{cases} p(0|1) = p(1|0) = \alpha(1-\alpha)(1-\mathcal{P}) \\ p(1|1) = p(0|0) = \alpha(1-\alpha) + (1-\alpha)^2\mathcal{P} \\ p(e_r|1) = p(e_r|0) = \alpha^2 + \alpha(1-\alpha)\mathcal{P} + (1-\alpha)^2(1-\mathcal{P}) \end{cases} \tag{4.9}$$

Dans nos simulations nous choisissons une valeur de $2 \cdot 10^{-5}$ pour la probabilité de coup d'obscurité α comme précisé au paragraphe 3.2.2.2. $\mathcal{P}$ est la probabilité d'obtenir un clic par le détecteur, il s'agit de p_{Bob} dans le cas où le détecteur est chez Bob.

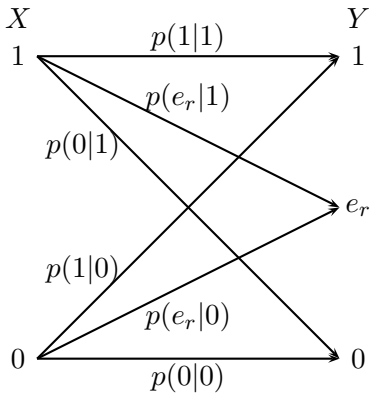

FIG. 4.5 – Défintion du canal à effacement

4.3.3.2 Calcul de l'information mutuelle

De plus $I(X,Y)$ est donné par :

$$I(X,Y) = \sum_{x,y} p(y|x)p(x)\log\frac{p(y|x)}{\sum_{x'} p(y|x')p(x')} \tag{4.10}$$

En faisant appel aux équations 4.9 et 4.10 nous pouvons déduire :

$$\begin{aligned} I(X,Y) = (1-\alpha)(\alpha+\mathcal{P}-\mathcal{P}\alpha)\log_2\frac{2\left(\alpha(1-\alpha)+(1-\alpha)^2\mathcal{P}\right)}{\alpha(1-\alpha)(2-\mathcal{P})+(1-\alpha)^2\mathcal{P}} \\ +(1-\alpha)\alpha(1-\mathcal{P})\log_2\frac{2\alpha(1-\alpha)(1-\mathcal{P})}{\alpha(1-\alpha)(2-\mathcal{P})+(1-\alpha)^2\mathcal{P}} \end{aligned}$$

$I(X,Y_{Bob})$ et $I(X,Y_{Eve})$ se calculent de manière analogue grâce à l'équation 4.11

La figure 4.6 représente l'influence de l'intervention d'Ève sur l'évolution de l'information mutuelle entre Alice et Bob.

Pour déterminer $I(X,Y_{Eve})$ il nous faut déterminer l'équivalent de la probabilité de détection pour Ève. Ève gagne de l'information quand il passe au moins deux photons sur la fibre. Étant donné qu'elle est omnipotente, on lui donne un détecteur d'efficacité unitaire.

$$\begin{aligned} \mathcal{P}_{Eve} &= 1-p(0)-p(1) \\ \mathcal{P}_{Eve} &= 1-e^{-\mu}-\mu e^{-\mu} \end{aligned} \tag{4.11}$$

Nous avons représenté la sécurité possible après une attaque par vol de photon surnuméraire dans le cas d'une détection absolue de phase sur la figure 4.6. On peut noter qu'à partir d'une valeur limite du nombre moyen de photons, la sécurité n'est plus possible. Sur la figure 4.7 nous remarquons aisément la présence d'un maximum. Un calcul de maximisation donne la

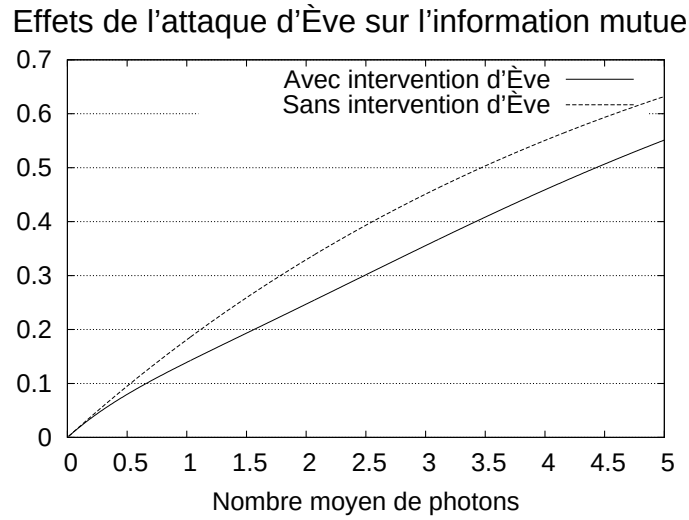

FIG. 4.6 – Effets de l'attaque d'Ève sur l'information mutuelle en bits entre Alice et Bob en fonction du nombre moyen de photons

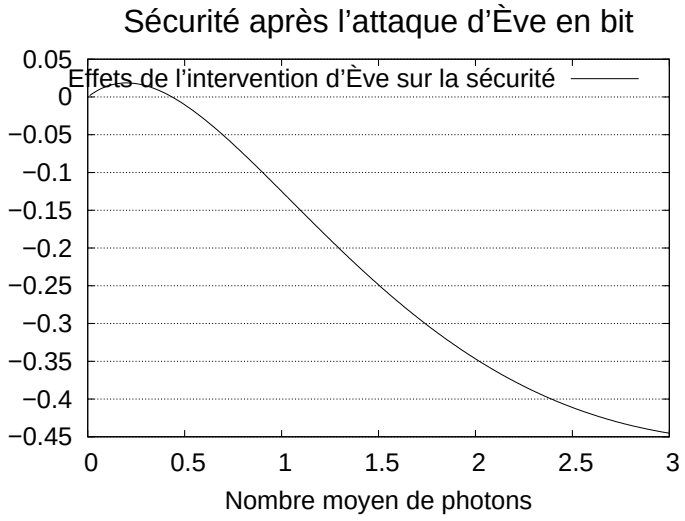

FIG. 4.7 – Effet de l'attaque d'Ève sur la sécurité entre Alice et Bob

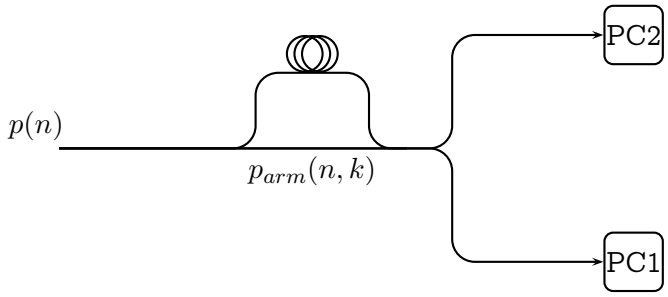

FIG. 4.8 – Détecteurs d'Alice et Bob pour des détections différentielles de phase

valeur optimale pour μ de 0.2003 . Notons que le niveau de sécurité est très peu élevé. Il faut souligner ici l'hypothèse d'omnipotence d'Ève qui a été formulée. En effet, elle possède un détecteur d'efficacité unité sans coups d'obscurité alors que Bob ne dispose que d'un détecteur d'efficacité 10%.

4.4 Détection différentielle de phase

4.4.1 BB84

Nous envisageons également d'utiliser un codage différentiel dans le protocole BB84. La différence fondamentale avec le système précédent est la nécessité pour un qubit d'interférer avec le précédent. Nous n'utilisons donc pas d'oscillateur local pour ce système.

Nous présentons dans la figure 4.8 le schéma du montage des photodiodes envisagé.

4.4.2 Bras de l'interféromètre

Appelons $p_{arm}(n,k)$ la probabilité d'obtenir k photons dans un des deux bras parmi n photons qui étaient à l'entrée de l'interféromètre. On peut définir $p_{arm}(n,k)$ comme suit :

$$\begin{cases} p_{arm}(n,k) = \frac{1}{2}(p_{arm}(n-1,k-1) + p_{arm}(n-1,k)) \\ p_{arm}(1,1) = p_{arm}(1,0) = \frac{1}{2} \end{cases} \tag{4.12}$$

En outre pour pouvoir élargir l'expression 4.12 au cas extrême où $k = 0$ il faut définir $\forall n \in \mathbb{N}$, $p_{arm}(n,-1) = 0$. Ceci se voit aisément après avoir remarqué que $\forall n \in \mathbb{N}$, $p_{arm}(n,0) = \frac{1}{2^n}$.

Soit la proposition :

$$p_{arm}(n,k) = \frac{1}{2^n} C_n^k. \tag{4.13}$$

i. Montrons 4.13 par récurrence

Rang initial $n = 1$ Notre hypothèse de départ est la suivante :

$$\forall k \in \{0,1\},\ p_{arm}(1,k) = \frac{1}{2} \tag{4.14}$$

Notre but est de montrer que la proposition au rang $n = 2$ est vraie. Pour cela, comparons $p_{arm}(2,k),\ k \in \{0,1,2\}$ au calcul résultant de l'équation 4.12.

$$\begin{aligned} p_{arm}(2,0) &= \frac{1}{4} \\ p_{arm}(2,1) &= \frac{1}{2} \\ p_{arm}(2,2) &= \frac{1}{4} \end{aligned}$$

$$\begin{aligned} \frac{1}{2^2} C_2^0 &= \frac{1}{4} \times \frac{2!}{0!2!} = \frac{1}{4} \\ \frac{1}{2^2} C_2^1 &= \frac{1}{4} \times \frac{2!}{1!1!} = \frac{1}{2} \\ \frac{1}{2^2} C_2^2 &= \frac{1}{4} \times \frac{2!}{2!0!} = \frac{1}{4} \end{aligned} \tag{4.15}$$

Ceci vérifie la propriété 4.13 au rang initial.

Rang n Notre hypothèse de départ devient ici la suivante :

$$\forall k \in \{0,..,n\},\ p_{arm}(n,k) = \frac{1}{2^n} C_n^k$$

Notre but est de montrer que si elle est vérifiée au rang n alors elle est vérifiée au rang $n+1$.

$$\begin{aligned} p_{arm}(n+1,k) &= \frac{1}{2}(p_{arm}(n,k) + p_{arm}(n,k-1)) \\ &= \frac{1}{2^{n+1}}(C_n^k + C_n^{k-1}) \\ p_{arm}(n+1,k) &= \frac{1}{2^{n+1}} C_{n+1}^k \end{aligned}$$

Ceci vérifie la propriété 4.13 au rang n pour tout n et conclut donc notre démonstration par récurrence.

$$\forall k \in \{0, .., n\},\ p_{arm}(n,k) = \frac{1}{2^n} C_n^k$$

Pour obtenir la distribution finale effectivement observée dans chaque bras de l'interféromètre, il n'y plus qu'à sommer le produit de $p_{arm}(n,k)$ et de la probabilité de présence de n photons à l'entrée du bras pour toutes les valeurs possibles de n qui sont supérieures à k. En effet il est nécessaire qu'il y ait plus de photons à l'entrée de l'interféromètre qu'en un des ses bras.

$$p_{arm}(k) = \sum_{n \geq k} \frac{1}{2^n} C_n^k p_{Bob}(n) \tag{4.16}$$

4.4.3 Interférences

Pour qu'un photon soit détecté correctement celui-ci doit interférer avec un autre photon venant de l'autre bras de l'interféromètre. La probabilité d'interférence est donc liée à la probabilité de peuplement dans chacun des bras. Notons que la probabilité de peuplement d'un bras est indépendante de l'autre bras (et vice-versa) puisqu'il s'agit d'une détection différentielle et que ces deux probabilités sont liées à deux événements ayant lieu à des temps bits différents.

$$p_{inter} = \left(p_{arm}(k \geq 1)\right)^2 \tag{4.17}$$

Étant donné que les deux bras de l'interféromètre se rejoignent, nous assistons à une nouvelle distribution de probabilité à l'entrée du détecteur.

$$p_{in}(k) = \sum_{r+s=k} p_{arm}(s) p_{arm}(r) \tag{4.18}$$

Les équations 4.17 et 4.18 nous conduisent à une nouvelle probabilité de détection. En effet, pour obtenir une détection il suffit qu'un photon soit détecté, mais pour obtenir une détection correcte il faut que le photon ait interféré auparavant.

Intéressons nous d'abord à la probabilité de détection. La probabilité qu'un des deux détecteurs clique, est donnée d'une manière analogue à l'équation 4.3.

$$\begin{aligned} p_{det} &= \sum_{k=1}^{+\infty} p_{in}(k)(1 - (1-\eta)^k) \\ p_{det} &= \sum_{k=1}^{+\infty} \sum_{r+s=k} p_{arm}(s) p_{arm}(r)(1 - (1 - \eta^k)) \end{aligned} \tag{4.19}$$

Maintenant, pour obtenir la probabilité d'avoir une détection correcte, il faut à la fois une détection et une interférence. En notant $p_{d\ corr}$ cette probabilité de détection correcte :

$$\begin{aligned} p_{d\ corr} &= p_{inter} * p_{det} \\ p_{d\ corr} &= (p_{arm}(k \geq 1))^2 \sum_{k=1}^{+\infty} \sum_{r+s=k} p_{arm}(s) p_{arm}(r)(1-(1-\eta)^k) \end{aligned}$$

4.4.3.1 Détecteurs

L'idée est ici la différence de détection au sein du détecteur de Bob suivant qu'il y ait ou non une attaque sur le lien.

i. Sans attaque

La distribution à l'entrée de l'interfèromètre est poissonnienne. En fait, l'interféromètre conserve le caractère poissonnien de la distribution. La probabilité de détection est donc simplement donnée par :

$$\begin{aligned} p_{det} &= \sum_{k=1}^{+\infty} \frac{u^k e^{-\mu}}{k!}(1-(1-\eta)^k) \\ p_{det} &= 1 - e^{-\eta\mu} \end{aligned} \tag{4.20}$$

Notons que le résultat obtenu est en tout point similaire au résultat 4.3. Il faut néanmoins ajouter qu'il s'agit uniquement de la probabilité de détection, et non pas de la probabilité d'obtenir un bit informatif.

ii. Avec attaque

Reprenons l'équation 4.19 et appliquons-la au cas où la liaison subit une attaque. Il nous faut donc comme probabilité p_{arm} à l'entrée de l'interféromètre la distribution modifiée par l'action d'Ève comme définie à l'équation 4.1.

$$\begin{aligned} p_{det} &= \sum_{k=1}^{+\infty} \sum_{r+s=k} p_{arm}(s) p_{arm}(k-s)(1-(1-\eta)^k) \\ &= \sum_{k=1}^{+\infty} \sum_{r+s=k} (1-(1-\eta)^k) \left(\sum_{i \geq s} \frac{1}{2^i} C_i^s p(i) \right) \left(\sum_{i \geq r} \frac{1}{2^i} C_i^r p(i) \right) \end{aligned}$$

La figure 4.9 présente la probabilité de détection suivant qu'Ève attaque ou non en fonction du paramètre « nombre moyen de photons »μ. On peut noter que les deux courbes sont au premier ordre identique à l'approche de 0 et s'écartent lorsque le nombre moyen de photons μ augmente.

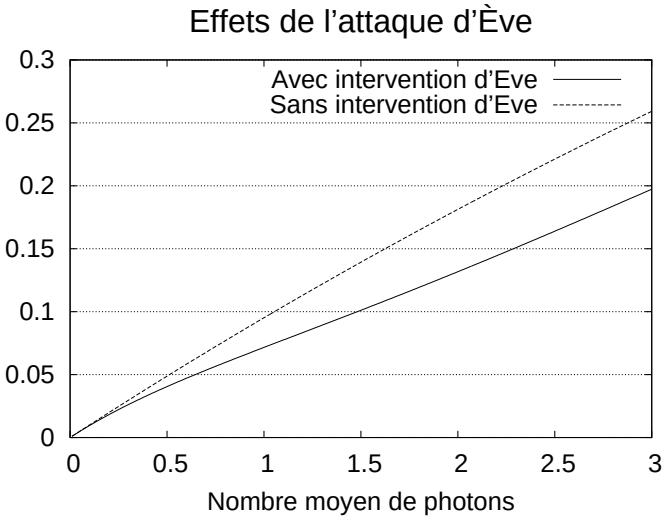

FIG. 4.9 – Différence de probabilité de détection si Ève est présente ou non

4.4.4 Information mutuelle

Nous allons maintenant étudier la sécurité obtenue sur la liaison grâce au calcul de l'information mutuelle. Pour cela nous devons reprendre l'équation 4.11 et l'appliquer à la détection de phase différentielle. Lorsqu'il n'y a pas interférence, c'est-à-dire quand un photon arrive seul sans homologue dans l'autre bras, il va activer un des deux détecteurs, dont la conséquence est une fois sur deux un résultat correct. L'information gagnée par Bob correspond donc à la moitié des détections aléatoires engendrées sans interférence et bien sûr aux détections engendrées par des interférences

$$\begin{aligned} \mathcal{P}_{Bob} &= p_{realdet} + \frac{1}{2}(p_{realdet} - p_{det}) \\ &= \frac{1}{2}(p_{realdet} + p_{det}) \\ \mathcal{P}_{Bob} &= \frac{1}{2}(1 + (p_{arm}(k>1))^2)p_{det} \end{aligned} \tag{4.21}$$

Ève obtient de l'information à chaque fois qu'elle vole deux bits à la suite. Il faut donc simplement qu'elle ait au moins un bit deux fois de suite car son détecteur est d'efficacité unitaire.

$$\begin{aligned} \mathcal{P}_{Eve} &= (1 - p(0) - p(1))^2 \\ \mathcal{P}_{Eve} &= (1 - e^{-\mu} - \mu e^{-\mu})^2 \end{aligned}$$

Nous avons représenté sur la figure 4.10 l'impact d'Ève effectuant une attaque par vol de photons surnuméraires en termes d'information mutuelle. On peut noter une baisse notable de cette information après l'attaque.

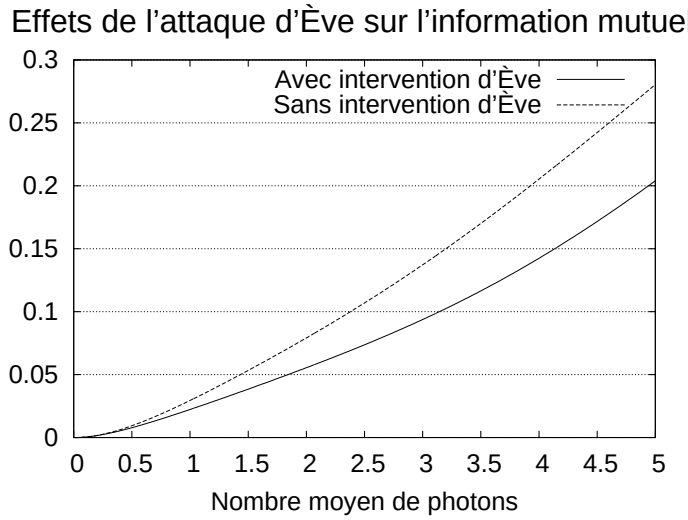

FIG. 4.10 – Effet de l'intervention d'Ève sur l'information mutuelle entre Alice et Bob dans le cas d'une détection différentielle de phase

Sur la figure 4.11 nous avons représenté la sécurité que nous sommes en droit d'attendre après l'intervention d'Ève. Comme précédemment dans le cas du lien à détecteur absolu de phase, nous avons relevé un seuil de nombre moyen de photons au delà duquel toute sécurité n'est plus envisageable. Il y a aussi à nouveau une valeur du paramètre de nombre de photons moyen μ pour laquelle la sécurité est maximale. Cette valeur est de 0.2710 .

Avec le système différentiel la sécurité d'un bit est divisé sur deux bits consécutifs, ce qui donne de meilleurs résultats que pour la détection directe de phase. Le côté différentiel ajoute une sécurité collective.

Si on étudie le taux de détection du côté de Bob, alors nous avons une évaluation de sécurité minimale propre à chaque photon. Cette étude conduit à ajouter une sécurité minimale propre à chaque photon.

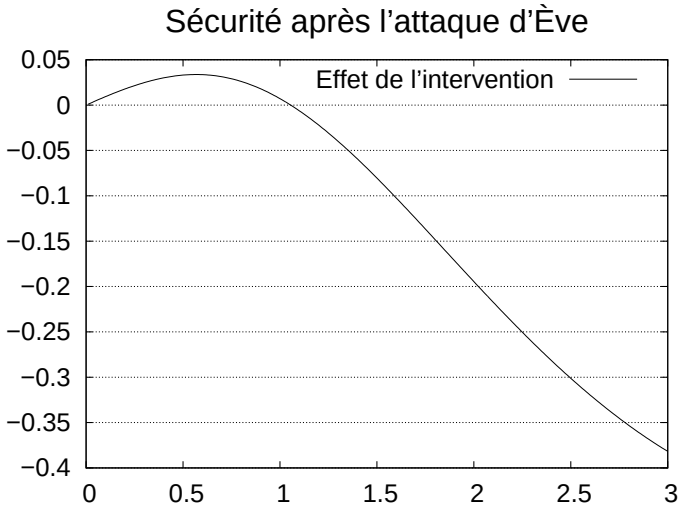

FIG. 4.11 – Effet de l'intervention d'Ève sur la sécurité

Chapitre 5

Système homodyne et robustesse à différents types d'attaques

Nous pouvons concevoir que si Bob décide d'abandonner des mesures « peu fiables » ou « peu informatives », nous obtiendrons une diminution

du taux d'erreur sur la liaison quantique. Mais comment définir une mesure « peu fiable » ? Et quel est l'impact sur la sécurité de la liaison ?

5.1 BB84 par homodynage à seuil

5.1.1 Protocole

Une approche d'homodynage à seuil peut être appliquée dans le but de pouvoir rejeter certains bits, dont la mesure est peu fiable [33].

Alice choisit aléatoirement un état cohérent dans l'ensemble $\{|\alpha\rangle, |i\alpha\rangle, |-\alpha\rangle, |-i\alpha\rangle\}$ avec $\alpha > 0$. Si Alice utilise une source cohérente atténuée l'état cohérent est un état propre de l'opérateur annihilation de photon $\hat{a} = x_1 + ix_2$ Bob choisit alors d'effectuer une mesure sur l'une de ces deux quadratures $\{\hat{x_1}, \hat{x_2}\}$. x_1 et x_2 ne commutent pas : $[x_1, x_2] = \frac{i}{2}$.

En termes d'opérateur densité d'états, nous avons :

$$\hat{\rho} = \frac{1}{4}\left(|\alpha\rangle\langle\alpha| + |-\alpha\rangle\langle-\alpha| + |i\alpha\rangle\langle i\alpha| + |-i\alpha\rangle\langle-i\alpha|\right)$$

Lorsque Bob choisit la base x_1 et que $|\alpha\rangle$ ou $|-\alpha\rangle$ a été envoyé ou lorsque que Bob choisit la base x_2 et que $|i\alpha\rangle$ ou $|-i\alpha\rangle$ a été envoyé, nous dirons que le choix de base a été correct. Dans tous les autres cas nous dirons que le choix de base a été mauvais. Étant donné que les mauvais choix de base sont rejetés lors de la réconciliation, tout le problème de Bob est de différencier $|\alpha\rangle$ et $|-\alpha\rangle$ d'une part et $|i\alpha\rangle$ et $|-i\alpha\rangle$ d'autre part. En d'autres termes si Alice annonce la quadrature, l'opérateur de densité est réduit à :

$$\rho_1 = \frac{1}{2}\left(|\alpha\rangle\langle\alpha| + |-\alpha\rangle\langle-\alpha|\right) \text{ ou } \rho_2 = \frac{1}{2}\left(|i\alpha\rangle\langle i\alpha| + |-i\alpha\rangle\langle-i\alpha|\right)$$

5.1.2 Mesures

Nous cherchons à effectuer une mesure avec un oscillateur formé $\hat{x_\Phi} = \cos\Phi\hat{x}_1 + \sin\Phi\hat{x}_2$ où x_1 et x_2 sont définis par la relation $\hat{a} = \hat{x}_1 + i\hat{x}_2$. Reprenons le résultat 3.37. Étant donné qu'une fonction gaussienne minimise l'écart quadratique, la distribution de notre grandeur de mesure x_Φ est gaussienne. La densité de probabilité de la mesure x_ϕ est donc gaussienne.

$$p(x_\Phi) = \frac{1}{\sigma\sqrt{2\pi}} \exp \frac{(x_\Phi - \alpha\cos\Phi)^2}{2\sigma^2} \tag{5.1}$$

La valeur de l'écart-type σ ne dépend que du commutateur $[\hat{x}_1, \hat{x}_2] = i$ et du principe d'Heisenberg. Nous obtenons donc ainsi $\sigma = \frac{1}{2}$. Il apparaît alors que $\hat{x}_\phi = \hat{x}_1\cos\phi + \hat{x}_2\sin\phi$ est donnée par :

$$|\langle x_\phi|\alpha\rangle|^2 = \sqrt{\frac{2}{\pi}} \exp\left(-2(x_\phi - \alpha\cos\phi)^2\right) \tag{5.2}$$

On note immédiatement que $\hat{x}_1 = \hat{x}_0$ et que $\hat{x}_2 = \hat{x}_{\frac{\pi}{2}}$. Et la mesure sur les bases x_1 et x_2 est calculée par $\langle x_i|\hat{\rho}_i|x_i\rangle$.

$$\langle x_i|\hat{\rho}_j|x_i\rangle = \begin{cases} \frac{1}{\sqrt{2\pi}}\left(\exp\left(-2(x_i-\alpha)^2\right) + \exp\left(-2(x_i+\alpha)^2\right)\right) \text{ si } i = j \\ \sqrt{\frac{2}{\pi}}\exp(-2x_i^2) \text{ si } i \neq j \end{cases}$$

5.1.3 taux d'erreur

Considérons une mesure à seuil x_0, et définissons la probabilité d'obtenir une mesure qui semble correcte lorsque la quadrature x_1 a été choisie.

$$\begin{aligned}
\mathcal{P}(x_0,n) &= \int_{-\infty}^{-x_0}\langle x_1|\hat{\rho}_1|x_1\rangle \mathrm{d}x_1 + \int_{x_0}^{\infty}\langle x_1|\hat{\rho}_1|x_1\rangle \mathrm{d}x_1 \\
&= \int_{-\infty}^{-x_0}|\langle x_1|\alpha\rangle|^2 \\
&\quad +|\langle x_1|-\alpha\rangle|^2\mathrm{d}x_1 + \int_{x_0}^{\infty}|\langle x_1|\alpha\rangle|^2 + |\langle x_1|-\alpha\rangle|^2\mathrm{d}x_1 \\
&= \int_{x_0}^{\infty}|\langle -x_1|\alpha\rangle|^2 + |\langle -x_1|-\alpha\rangle|^2 + |\langle x_1|\alpha\rangle|^2 + |\langle x_1|-\alpha\rangle|^2\mathrm{d}x_1 \\
&= \frac{1}{\sqrt{2\pi}}\int_{x_0}^{\infty} e^{-2(-x_1-\sqrt{n})^2} + e^{-2(-x_1+\sqrt{n})^2}\mathrm{d}x_1 \\
&\quad + e^{-2(x_1-\sqrt{n})^2} + e^{-2(x_1+\sqrt{n})^2}\mathrm{d}x_1 \\
&= \sqrt{\frac{2}{\pi}}\int_{x_0}^{\infty} e^{-2(x_1-\sqrt{n})^2} + e^{-2(x_1+\sqrt{n})^2}\mathrm{d}x_1 \\
&= \sqrt{\frac{2}{\pi}}\int_{x_0-\sqrt{n}}^{\infty} e^{-2x_1^2}\mathrm{d}x_1 + \int_{x_0+\sqrt{n}}^{\infty} e^{-2x_1^2}\mathrm{d}x_1 \\
&= \sqrt{\frac{1}{\pi}}\int_{\sqrt{2}(x_0-\sqrt{n})}^{\infty} e^{-x_1^2}\mathrm{d}x_1 + \int_{\sqrt{2}(x_0+\sqrt{n})}^{\infty} e^{-x_1^2}\mathrm{d}x_1 \\
&= \frac{1}{2}\left(\mathrm{erfc}(\sqrt{2}(x_0+\sqrt{n})) + \mathrm{erfc}(\sqrt{2}(x_0-\sqrt{n}))\right) \qquad (5.3)
\end{aligned}$$

La fonction $\mathrm{erfc}(x)$ est définie par :

$$\mathrm{erfc}(x) = \frac{2}{\pi}\int_x^{\infty} e^{-t^2}\mathrm{d}t \qquad (5.4)$$

$\mathcal{P}(x_0,n)$ est la probabilité d'obtenir une mesure qui remplit le critère du seuil. Si ce critère n'est pas rempli la mesure est rejetée, $\mathcal{P}(x_0,n)$ est donc également une efficacité. Nous l'appellerons efficacité de détection. Ceci nous permet d'obtenir maintenant le taux d'erreur dans le cas d'une mesure sans intervention d'Ève. En effet, comme on rejette toutes les mesures où $-x_0 < x < x_0$ il est nécessaire de normaliser l'habituel $|\langle x_1|\alpha\rangle|^2$.

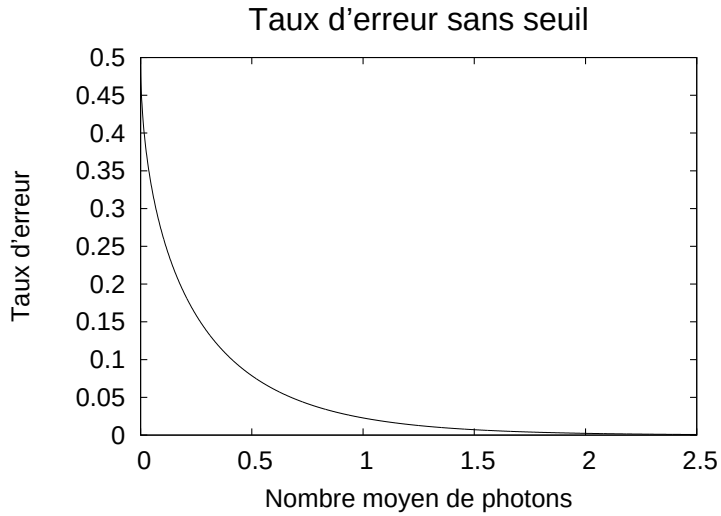

FIG. 5.1 – Évolution du taux d'erreur en fonction du nombre moyen de photon pour un seuil nul

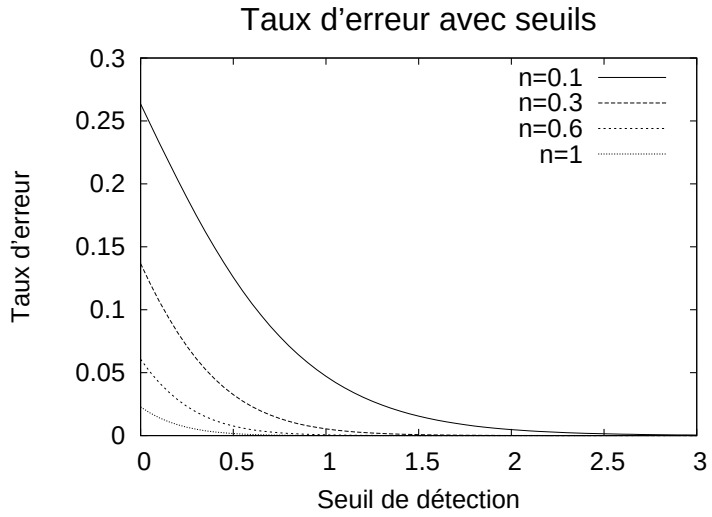

FIG. 5.2 – Évolution du taux d'erreur en fonction du seuil de la détection homodyne

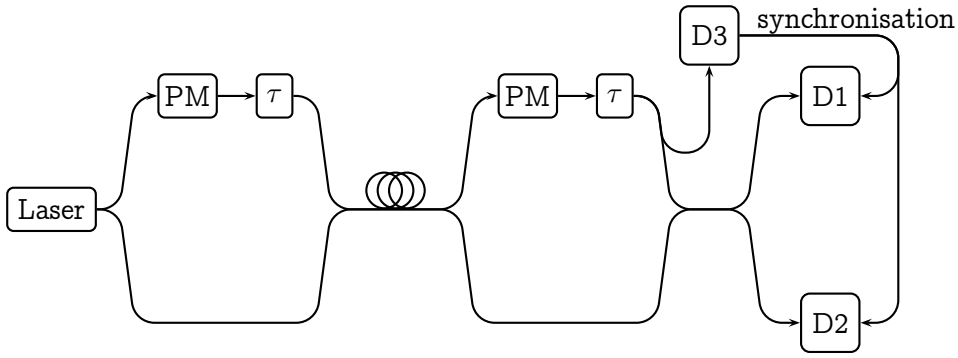

FIG. 5.3 – Montage expérimental, en mode détection homodyne

$$\begin{aligned} BER(x_0, n) &= \frac{1}{\mathcal{P}(x_0, n)} \int_{-\infty}^{-x_0} |\langle x_1|\alpha\rangle|^2 \mathrm{d}x_1 \\ &= \frac{1}{2\mathcal{P}(x_0, n)} \operatorname{erfc}(\sqrt{2}(x_0 + \sqrt{n})) \end{aligned} \tag{5.5}$$

L'arrangement de l'appareillage spécifique à la détection est détaillé dans la figure 5.3. Nous avons quasiment le même dispositif que dans le cas des compteurs de photons, de manière à pouvoir passer de l'un à l'autre facilement. Deux photodiodes PIN remplacent les compteurs de photons précédemment utilisés. Nous avons rajouté sur ce schéma une photodiode D3 sur laquelle est envoyée une petite partie de l'oscillateur local, de manière à pouvoir régler finement la synchronisation des détecteurs [50, 51, 48]. Le flux sortant de l'oscillateur local interfère ainsi avec le flux venant d'Alice pour être recueilli sur les compteurs de photons AP.

5.2 Attaque par interception et renvoi

5.2.1 Description de l'attaque

Plaçons-nous dans le cas où Ève intervient. Elle capture tous les photons avant qu'il n'arrivent chez Bob pour en faire une mesure. Si elle veut éviter d'être repérée, elle doit renvoyer vers Bob une version de ce qu'elle a reçu, et pour cela elle doit en faire une mesure avant le processus de réconciliation entre Alice et Bob [36, 49].

Nous supposons qu'elle divise le signal qu'elle reçoit en deux, et qu'elle effectue une mesure sur chacune des quadratures x_1 et x_2. Considérons qu'Ève

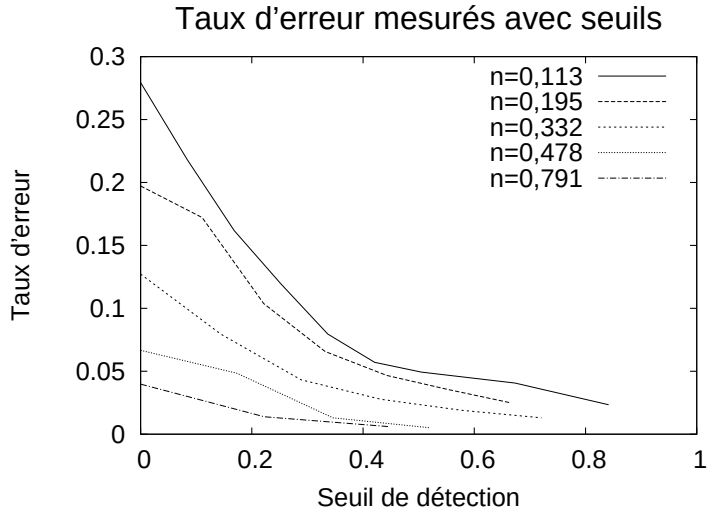

FIG. 5.4 – taux d'erreur mesurés

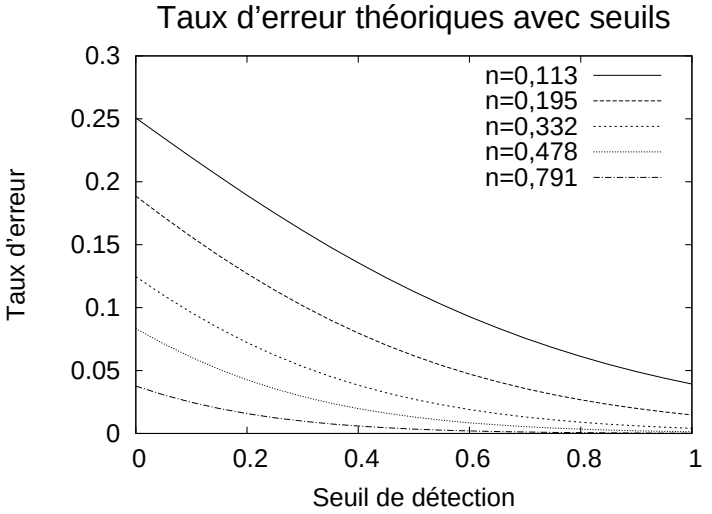

FIG. 5.5 – taux d'erreur théoriques corresondant aux mesures

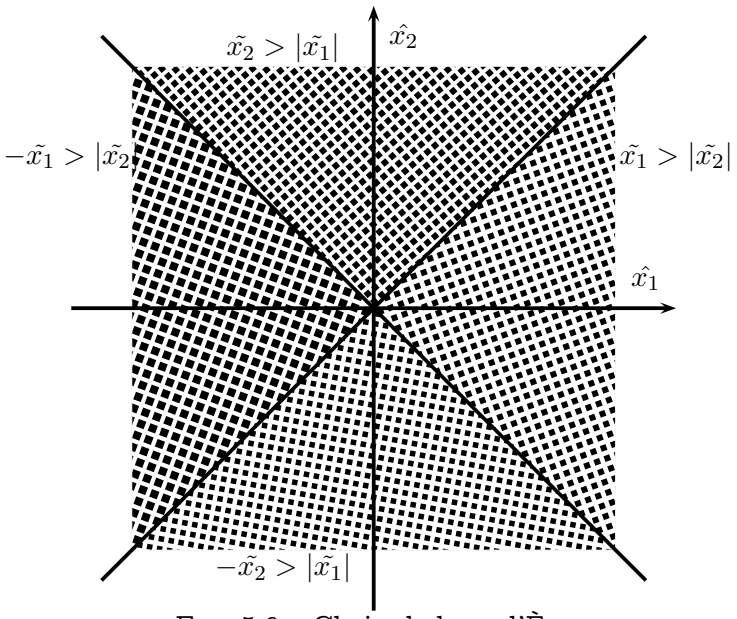

FIG. 5.6 – Choix de base d'Ève

obtient deux valeurs $\tilde{x_1}$ et $\tilde{x_2}$. On en conclut :

$$\begin{cases} |\alpha\rangle \text{ si } \tilde{x_1} > |\tilde{x_2}| \\ |i\alpha\rangle \text{ si } \tilde{x_2} > |\tilde{x_1}| \\ |-\alpha\rangle \text{ si } -\tilde{x_1} > |\tilde{x_2}| \\ |-i\alpha\rangle \text{ si } -\tilde{x_2} > |\tilde{x_1}| \end{cases}$$

Ces choix sont géomètriquement représentés sur la figure 5.6.

5.2.2 Transformation de l'opérateur densité

Nous cherchons à obtenir quelle est la transformation subie par l'opérateur densité après les manipulations d'Ève. Pour cela, nous allons considérer la densité de probabilité conjointe en x_1 et x_2 liée à la mesure d'Ève. Plaçons-nous dans le cas où Alice a envoyé $|\alpha\rangle$ et comme elle effectue une mesure sur la moitié du signal sur chaque quadrature, elle obtient :

$$\begin{aligned} \mathcal{Q}_n(x_1, x_2) &= |\langle x_1|\frac{\alpha}{\sqrt{2}}\rangle|^2 |\langle x_2|\frac{\alpha}{\sqrt{2}}\rangle|^2 \\ &= \frac{2}{\pi}\exp\left(-2(x_1 - \sqrt{\frac{n}{2}}) - 2x_2^2\right) \end{aligned}$$

La probabilité pour Ève de trouver le bon résultat est délimitée par la région afférente dans la figure 5.6. En effet, c'est la probabilité qu'elle fasse le choix $|\alpha\rangle$ si Alice a envoyé $|\alpha\rangle$, ce qui correspond à la région $\tilde{x_1} > \tilde{x_2}$.

La probabilité qu'Ève fasse le bon choix est donné par :

$$\begin{aligned}
\mathcal{P}_+(n) &= \iint_{x_1>|x_2|} \mathcal{Q}(x_1,x_2)\mathrm{d}x_1\mathrm{d}x_2 \\
&= \iint_{x_1>|x_2|} \frac{2}{\pi} e^{\left(-2(x_1-\sqrt{\frac{n}{2}})-2x_2^2\right)}\mathrm{d}x_1\mathrm{d}x_2 \\
&= \iint_{u>0,v>0} \frac{2}{\pi} e^{\left(-2\left(\frac{1}{2}(u+v)-\sqrt{\frac{n}{2}}\right)^2-2\left(\frac{1}{\sqrt{2}}(v-u)\right)^2\right)}\mathrm{d}u\mathrm{d}v \\
&= \frac{2}{\pi}\iint_{u>0,v>0} \exp\left(-2u^2-2v^2-n+2u\sqrt{n}+2v\sqrt{n}\right)\mathrm{d}u\mathrm{d}v \\
&= \frac{2}{\pi}e^{-n}\left(\int_0^\infty \exp(-2(u^2-u\sqrt{n}))\mathrm{d}u\right)^2 \\
&= \frac{2}{\pi}\left(\int_0^\infty \exp(-2(u-\frac{\sqrt{n}}{2})^2)\mathrm{d}u\right)^2 \\
&= \frac{2}{\pi}\left(\int_{-\frac{\sqrt{n}}{2}}^\infty \exp(-2u^2)\mathrm{d}u\right)^2 \\
&= \frac{1}{\pi}\left(\int_{-\sqrt{\frac{n}{2}}}^\infty \exp(-u^2)\mathrm{d}u\right)^2 \\
&= \frac{1}{4}\left(\mathrm{erfc}(-\sqrt{\frac{n}{2}})\right)^2
\end{aligned}$$

De la même manière nous montrons que la probabilité qu'Ève trouve le bon choix de base mais récupère le mauvais bit est donnée par :

$$\mathcal{P}_-(n) = \frac{1}{4}\left(\mathrm{erfc}(\sqrt{\frac{n}{2}})\right)^2$$

Et enfin, la probabilité qu'Ève trouve l'un des deux derniers choix est donnée par :

$$\mathcal{P}_\perp(n) = \frac{1}{4}\,\mathrm{erfc}(-\sqrt{\frac{n}{2}})\,\mathrm{erfc}(\sqrt{\frac{n}{2}})$$

L'état cohérent $|\alpha\rangle\langle\alpha|$ après la manipulation par Ève est donc transformé en une superposition d'état $\mathcal{P}_+(n)|\alpha\rangle\langle\alpha| + \mathcal{P}_-(n)|-\alpha\rangle\langle-\alpha| + \mathcal{P}_\perp(n)(|i\alpha\rangle\langle i\alpha| + |-i\alpha\rangle\langle-i\alpha|)$. En effectuant le même raisonnement sur les autres états cohérents envisageables nous obtenons :

$$\begin{aligned}
|\alpha\rangle\langle\alpha| &\rightarrow \mathcal{P}_+(n)|\alpha\rangle\langle\alpha| + \mathcal{P}_-(n)|-\alpha\rangle\langle-\alpha| \\
&\quad + \mathcal{P}_\perp(n)(|i\alpha\rangle\langle i\alpha| + |-i\alpha\rangle\langle-i\alpha|) \\
|-\alpha\rangle\langle-\alpha| &\rightarrow \mathcal{P}_+(n)|-\alpha\rangle\langle-\alpha| + \mathcal{P}_-(n)|\alpha\rangle\langle\alpha| \\
&\quad + \mathcal{P}_\perp(n)(|i\alpha\rangle\langle i\alpha| + |-i\alpha\rangle\langle-i\alpha|) \\
|i\alpha\rangle\langle i\alpha| &\rightarrow \mathcal{P}_+(n)|i\alpha\rangle\langle i\alpha| + \mathcal{P}_-(n)|-i\alpha\rangle\langle-i\alpha| \\
&\quad + \mathcal{P}_\perp(n)(|\alpha\rangle\langle\alpha| + |-\alpha\rangle\langle-\alpha|) \\
|-i\alpha\rangle\langle-i\alpha| &\rightarrow \mathcal{P}_+(n)|-i\alpha\rangle\langle-i\alpha| + \mathcal{P}_-(n)|i\alpha\rangle\langle i\alpha| \\
&\quad + \mathcal{P}_\perp(n)(|\alpha\rangle\langle\alpha| + |-\alpha\rangle\langle-\alpha|)
\end{aligned} \tag{5.6}$$

Et donc, par extension, les nouveaux opérateurs de densité d'état sont définis par :

$$\begin{aligned}
\hat{\rho_1} &= \frac{1}{2}(|\alpha\rangle\langle\alpha| + |-\alpha\rangle - \langle\alpha|) \\
\hat{\rho_1'} &= \frac{1}{2}(\mathcal{P}_+(n)|\alpha\rangle\langle\alpha| + \mathcal{P}_-(n)|-\alpha\rangle\langle-\alpha| \\
&\quad + \mathcal{P}_\perp(n)(|i\alpha\rangle\langle i\alpha| + |-i\alpha\rangle\langle-i\alpha|) \\
&\quad + \mathcal{P}_+(n)|-\alpha\rangle\langle-\alpha| + \mathcal{P}_-(n)|\alpha\rangle\langle\alpha| \\
&\quad + \mathcal{P}_\perp(n)(|i\alpha\rangle\langle i\alpha| + |-i\alpha\rangle\langle-i\alpha|)) \\
&= (\mathcal{P}_+(n) + \mathcal{P}_-(n))\hat{\rho_1} + 2\mathcal{P}_\perp(n)\hat{\rho_2}
\end{aligned}$$

De même ρ_2' est donné par :

$$\hat{\rho_2'} = (\mathcal{P}_+(n) + \mathcal{P}_-(n))\hat{\rho_2} + 2\mathcal{P}_\perp(n)\hat{\rho_1}$$

5.2.3 Nouvelle efficacité de mesure chez Bob

Comme précédemment nous nous intéressons d'abord à la probabilité d'avoir une détection au delà du seuil x_0 si $|\alpha\rangle$ est envoyé par Alice. Celle-ci se calcule bien entendu de manière analogue à la formule (5.3) :

$$\begin{aligned}
\mathcal{P}'(x_0, n) &= \int_{|x_1|>|x_0|} \langle x_1|\hat{\rho}_1'|x_1\rangle \mathrm{d}x_1 \\
&= \int_{|x_1|>|x_0|} \langle x_1|(\mathcal{P}_+(n) + \mathcal{P}_-(n))\hat{\rho_1} + 2\mathcal{P}_\perp(n)\hat{\rho_2})|x_1\rangle \mathrm{d}x_1 \\
&= (\mathcal{P}_+(n) + \mathcal{P}_-(n)) \int_{|x_1|>|x_0|} \langle x_1|\hat{\rho}_1|x_1\rangle \mathrm{d}x_1 \\
&\quad + 2\mathcal{P}_\perp(n) \int_{|x_1|>|x_0|} \langle x_1|\hat{\rho_2}|x_1\rangle \mathrm{d}x_1
\end{aligned} \tag{5.7}$$

De plus on a :

$$\begin{aligned}\int_{x_1>|x_0|}\langle x_1|\hat{\rho_2}|x_1\rangle \mathrm{d}x_1 &= \int_{x_1>|x_0|}\sqrt{\frac{2}{\pi}}\exp(-2x_1^2)\mathrm{d}x_1 \\ &= \sqrt{\frac{2}{\pi}}\int_{x_0}^{\infty}\exp(-2x_1^2)\mathrm{d}x_1 \\ &= \frac{1}{\sqrt{\pi}}\int_{x_0\sqrt{2}}^{\infty}\exp(-x_1^2)\mathrm{d}x_1 \\ &= \frac{1}{2}\operatorname{erfc}(x_0\sqrt{2}) \qquad (5.8)\end{aligned}$$

Il est aisé de remarquer que $\langle x_1|\hat{\rho_2}|x_1\rangle$ est paire ce qui nous permet de conclure à l'aide de l'équation 5.8 que

$$\int_{|x_1|>|x_0|}\langle x_1|\hat{\rho_2}|x_1\rangle \mathrm{d}x_1 = \operatorname{erfc}(x_0\sqrt{2}) \qquad (5.9)$$

D'où en utilisant les formules 5.7, 5.9 et la parité précédemment citée :

$$\mathcal{P}'(x_0,n) = (\mathcal{P}_+(n)+\mathcal{P}_-(n))\,\mathcal{P}(x_0,n) + 2\mathcal{P}\perp(n)\operatorname{erfc}(x_0\sqrt{2})$$

5.2.4 taux d'erreur chez Bob

Plusieurs facteurs sont à prendre en compte dans le taux d'erreur. En effet, il faut d'abord tenir compte de l'observation faite par Ève, et transformer l'expression $|\alpha\rangle\langle\alpha|$ de l'équation 5.5 comme le suggère l'équation 5.6.

$$\begin{aligned}BER'(x_0,n) &= \frac{1}{\mathcal{P}'(x_0,n)}\int_{-\infty}^{-x_0}\mathcal{P}_+(n)|\langle x_1|\alpha\rangle|^2 + \mathcal{P}_-(n)|\langle x_1|-\alpha\rangle|^2 \\ &\quad + 2\mathcal{P}_\perp(n)\langle x_1|\hat{\rho_2}|x_1\rangle\mathrm{d}x_1 \\ &= \frac{1}{\mathcal{P}'(x_0,n)}\int_{x_0}^{\infty}\mathcal{P}_+(n)|\langle x_1|-\alpha\rangle|^2 + \mathcal{P}_-(n)|\langle x_1|\alpha\rangle|^2 \\ &\quad + 2\mathcal{P}_\perp(n)\langle x_1|\hat{\rho_2}|x_1\rangle\mathrm{d}x_1 \\ &= \frac{1}{2\mathcal{P}'(x_0,n)}(\mathcal{P}_+(n)\operatorname{erfc}(\sqrt{2}(x_0+\sqrt{n})) \\ &\quad +\mathcal{P}_-(n)\operatorname{erfc}(\sqrt{2}(x_0-\sqrt{n})) + 2\mathcal{P}_\perp(n)\operatorname{erfc}(\sqrt{2}x_0))\end{aligned}$$

5.2.5 taux d'erreur chez Ève

Ève ne se contente pas de garder les valeurs qu'elle a mesurées. En effet, le processus réconciliation lui permet d'apprendre quelles bases ont été utilisées

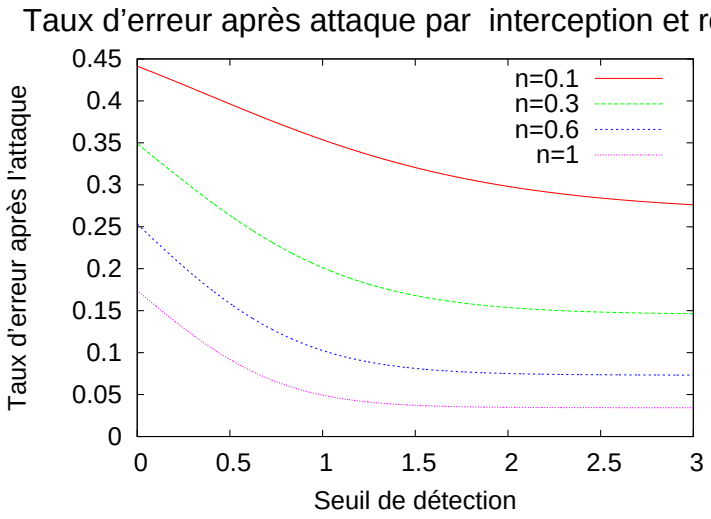

FIG. 5.7 – Évolution du taux d'erreur en fonction du seuil de la détection homodyne pour l'attaque par interception

par Alice et Bob. Elle peut, au cas où la réconciliation révèle que le choix de base d'Ève s'avère inexact, utiliser la mesure de valeur absolue la plus petite. En effet, cette mesure peut lui fournir une information précieuse au cas où la réconciliation révèle que l'état qu'elle a envoyé à Bob est faux. Donc même si elle se trompe en renvoyant un qubit chez Bob elle a toujours la possibilité de récupérer la valeur sur la base correcte lors de la réconciliation, ce qui permet une amélioration de son taux d'erreur. Et comme la mesure a été faite avec une amplitude divisée par deux, il est aisé de constater que $BER_{Eve}(n) = BER(0, \frac{n}{2})$.

5.2.6 Sécurité obtenue

Nous sommes intéressés par le différentiel d'information mutuelle entre Alice et Bob d'une part et Alice et Ève d'autre part. Soit $I(A, E)$ l'information mutuelle entre Alice et Ève et $I(A, B)$ l'information mutuelle entre Alice et Bob. Le différentiel qui nous intéresse est donc égal à $D = I(A, B) - I(A, E)$. Les informations mutuelles peuvent s'écrire en fonction de l'entropie de Shannon.

$$\begin{aligned} D &= I(A,B) - I(A,E) \\ &= H(A) - H(A|B) - H(A) + H(A|E) \\ &= H(A|E) - H(A|B) \\ &= -(BER_{Eve} \log_2 BER_{Eve} + (1 - BER_{Eve}) \log_2 (1 - BER_{Eve}) \\ &\quad + (BER \log_2 BER + (1 - BER) \log_2 (1 - BER) \end{aligned}$$

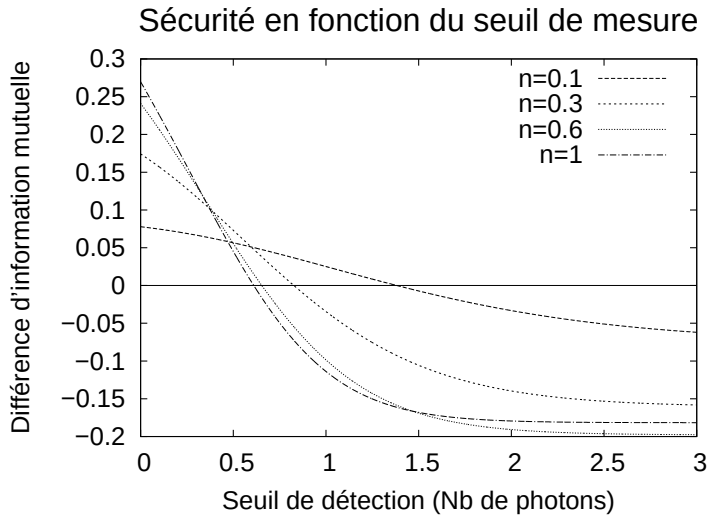

FIG. 5.8 – Évolution de l'information mutuelle en fonction du seuil de la détection homodyne pour l'attaque par interception

On remarque sur la figure 5.8 que le signe de l'information mutuelle peut s'inverser. Cela exprime évidemment qu'Ève obtient plus d'information que Bob. Cela doit être détecté, et la clef doit être abandonnée, car dans ce cas il n'y a plus d'amplification de confidentialité possible. Il est pour cela nécessaire, dans le cas pratique, de « sacrifier » une partie de la clef pour obtenir une estimation du taux d'erreur.

Sur la figure 5.9, la zone grisée représente la région où la sécurité est possible, la limite étant le lieu des points où le différentiel d'information mutuelle est nul.

5.2.7 Paramètres d'attaques d'Ève

5.2.7.1 Puissance

Une idée naïve serait pour Ève de renvoyer le signal plus fort qu'elle ne l'a reçu dans le but de faire baisser le taux d'erreur obtenu chez Bob après son intervention, et tenter ainsi de masquer sa présence. Nous allons donc calculer le nouveau $BER'_\beta(x_0, n)$ obtenu en multipliant le nombre moyen de photons qu'elle envoie par un paramètre β. Il convient de multiplier l'amplitude par

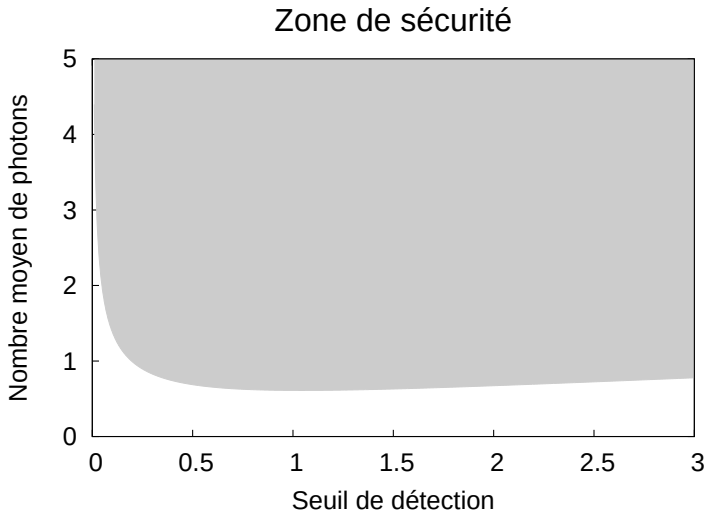

FIG. 5.9 – Zone de sécurité obtenue pour le couple nombre moyen de photons - seuil de détection

β dans ρ'_1 et ρ'_2.

$$\begin{aligned}\mathcal{P}'_\beta(x_0,n) &= \int_{x_1>|x_0|}\langle x_1|\hat{\rho}'_{1\beta}|x_1\rangle \mathrm{d}x_1 \\ &= (\mathcal{P}_+(n)+\mathcal{P}_-(n))\int_{x_1>|x_0|}\langle x_1|\hat{\rho}_{1,\beta}|x_1\rangle \mathrm{d}x_1 \\ &\quad + 2\mathcal{P}_\perp(n)\int_{x_1>|x_0|}\langle x_1|\hat{\rho_{2,\beta}}|x_1\rangle \mathrm{d}x_1 \qquad (5.10)\end{aligned}$$

L'expression $\langle x_1|\hat{\rho_{2,\beta}}|x_1\rangle$ ne dépend pas de β et on obtient donc après des calculs similaire au 5.2.3

$$\mathcal{P}'_\beta(x_0,n) = (\mathcal{P}_+(n)+\mathcal{P}_-(n))\mathcal{P}(x_0,\beta n) + 2\,\mathcal{P}_\perp(n)\,\mathrm{erfc}(\sqrt{2}\,x_0)$$

De la même manière, en faisant un calcul analogue au 5.2.4 on obtient pour le nouveau BER :

$$\begin{aligned}BER'_\beta(x_0,n) = \frac{1}{2\mathcal{P}'_\beta(x_0,n)}&(\mathcal{P}_+(n)\,\mathrm{erfc}(\sqrt{2}(x_0+\sqrt{\beta\,n})) \\ &+ \mathcal{P}_-(n)\,\mathrm{erfc}(\sqrt{2}(x_0-\sqrt{\beta\,n})) + 2\,\mathcal{P}_\perp(n)\,\mathrm{erfc}(\sqrt{2}\,x_0))\end{aligned}$$

On note effectivement une amélioration du taux d'erreur chez Bob, après augmentation du paramètre β. Il conviendrait pour Ève d'optimiser la différence $BER'_\beta(x_0,n) - BER(x_0,n)$ de manière à la rendre égale à 0 en jouant

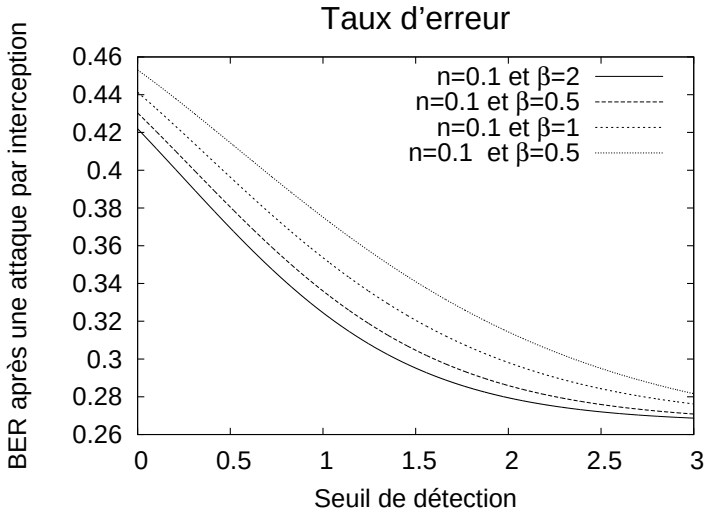

FIG. 5.10 – Évolution du taux d'erreur après attaque en fonction du paramètre de puissance β pour $n = 0.1$

sur β en fonction des paramètres x_0 et n. On note cependant que cette différence est nulle pour $n = 0$, en effet une intensité nulle implique que les taux d'erreur soient maximaux. En fait, plus l'intensité est faible, plus Ève est susceptible de corriger son intervention par cette méthode. Bob est en mesure d'effectuer des mesures de puissance.

Des variantes de BB84 utilisant des variations de puissance permettent de déjouer facilement ce type d'attaque qui changent la puissance du signal[53].

5.2.7.2 Probabilité d'attaque par bit variable

On peut aussi envisager un cas simple où Ève se contente de ne s'introduire dans la liaison qu'avec une certaine probabilité, dans l'idée de masquer ainsi son intervention. Elle gagne d'autant moins d'information qu'elle attaque moins de bits.

Soit Π la probabilité d'attaque de Ève.

$$\begin{aligned} BER_{Eve,\Pi}(x_0, n) &= \Pi BER(x_0, \frac{n}{2}) \\ BER'_{\Pi}(x_0, n) &= (1-\Pi)BER(x_0, n) + \Pi BER'(x_0, n) \end{aligned}$$

5.3 Attaque par utilisation de la base de Breidbart

5.3.1 Description de l'attaque

Dans cette attaque, Ève effectue une mesure de chaque photon dans la base dite de Breidbart : $\hat{x_{\frac{\pi}{4}}} = \frac{1}{\sqrt{2}}(\hat{x_1} + \hat{x_2})$. Elle renvoie $|\alpha e^{\frac{i\pi}{4}}\rangle$ si elle obtient

$x_{\frac{\pi}{4}} > 0$ et $|-\alpha e^{\frac{i\pi}{4}}\rangle$ sinon [36, 49].

Appelons $\mathcal{P}_E$ la probabilité qu'Ève renvoie $|\alpha e^{\frac{i\pi}{4}}\rangle$ si Alice a envoyé $|\alpha\rangle$.

$$\begin{aligned}
\mathcal{P}_E &= \int_0^\infty \langle x_{\frac{\pi}{4}}|\alpha\rangle^2 \\
&= \int_0^\infty \sqrt{\frac{2}{\pi}}\exp(-2(x_{\frac{\pi}{4}} - \alpha\cos\frac{\pi}{4}))^2 \\
&= \int_0^\infty \sqrt{\frac{2}{\pi}}\exp(-2(x_{\frac{\pi}{4}} - \frac{\alpha}{\sqrt{2}}))^2 \\
&= 1 - BER(0, \frac{n}{2})
\end{aligned}$$

5.3.2 Transformation de l'opérateur densité

Comme précédemment nous cherchons à obtenir la transformation subie par l'opérateur densité lors de la manipulation du signal par Ève.

$$\begin{aligned}
|\alpha\rangle\langle\alpha| &\rightarrow \mathcal{P}_E|\alpha e^{\frac{i\pi}{4}}\rangle\langle\alpha e^{\frac{i\pi}{4}}| \\
&\quad + (1-\mathcal{P}_E)|-\alpha e^{\frac{i\pi}{4}}\rangle\langle-\alpha e^{\frac{i\pi}{4}}| \\
|-\alpha\rangle\langle-\alpha| &\rightarrow \mathcal{P}_E|-\alpha e^{\frac{i\pi}{4}}\rangle\langle-\alpha e^{\frac{i\pi}{4}}| \\
&\quad + (1-\mathcal{P}_E)|\alpha e^{\frac{i\pi}{4}}\rangle\langle\alpha e^{\frac{i\pi}{4}}| \\
|i\alpha\rangle\langle i\alpha| &\rightarrow \mathcal{P}_E|\alpha e^{\frac{i\pi}{4}}\rangle\langle\alpha e^{\frac{i\pi}{4}}| \\
&\quad + (1-\mathcal{P}_E)|-\alpha e^{\frac{i\pi}{4}}\rangle\langle-\alpha e^{\frac{i\pi}{4}}| \\
|-i\alpha\rangle\langle-i\alpha| &\rightarrow \mathcal{P}_E|-\alpha e^{\frac{i\pi}{4}}\rangle\langle-\alpha e^{\frac{i\pi}{4}}| \\
&\quad + (1-\mathcal{P}_E)|+\alpha e^{\frac{i\pi}{4}}\rangle\langle+\alpha e^{\frac{i\pi}{4}}|
\end{aligned}$$

Nous pouvons donc maintenant calculer les opérateurs de densité ρ_1'' (respectivement ρ_2'') en remplaçant les expressions précédentes dans ρ_1 (respectivement ρ_2) comme cela a été fait dans la section précédente :

$$\begin{aligned}
\rho_1'' &= \frac{1}{2}\left(|\alpha e^{\frac{i\pi}{4}}\rangle\langle\alpha e^{\frac{i\pi}{4}}| + |-\alpha e^{\frac{i\pi}{4}}\rangle\langle-\alpha e^{\frac{i\pi}{4}}|\right) \\
\rho_2'' &= \frac{1}{2}\left(|\alpha e^{\frac{i\pi}{4}}\rangle\langle\alpha e^{\frac{i\pi}{4}}| + |-\alpha e^{\frac{i\pi}{4}}\rangle\langle-\alpha e^{\frac{i\pi}{4}}|\right)
\end{aligned}$$

5.3.3 Modification de l'efficacité de détection

Nous utilisons comme précédemment les opérateurs de densité d'état modifié :

$$\begin{aligned}\mathcal{P}''(x_0,n) &= \int_{-\infty}^{-x_0}\langle x_1|\rho_1''|x_1\rangle \mathrm{d}x_1 + \int_{x_0}^{\infty}\langle x_1|\rho_1''|x_1\rangle \mathrm{d}x_1 \\ &= \int_{x_0}^{\infty}|\langle x_1|\alpha e^{\frac{i\pi}{4}}\rangle|^2 + |\langle x_1| - \alpha e^{\frac{i\pi}{4}}\rangle|^2 \mathrm{d}x_1 \\ &= P(x_0,\frac{n}{2})\end{aligned}$$

5.3.4 taux d'erreur chez Bob

Nous procèdons de la même manière que précédemment :

$$\begin{aligned}BER''(x_0,n) &= \frac{1}{\mathcal{P}''(n)(x_0,n)}\int_{-\infty}^{x_0}(1-\mathcal{P}_E(n))|\langle x_1| - \alpha e^{\frac{i\pi}{4}}\rangle|^2 \\ &\quad + \mathcal{P}_E(n))|\langle x_1|\alpha e^{\frac{i\pi}{4}}\rangle|^2 \mathrm{d}x_1 \\ &= (1-\mathcal{P}_E(n))BER(x_0,\frac{n}{2}) + \\ &\quad \frac{\mathcal{P}_E(n)}{2\mathcal{P}''(x_0,n)}\operatorname{erfc}(\sqrt{2}(x_0-\sqrt{\frac{n}{2}}))\end{aligned} \tag{5.11}$$

5.3.5 taux d'erreur chez Ève

Le taux d'erreur chez Ève est le même que précédemment, vu qu'elle rejoue ses mesures de la même façon, et que la perte sur la mesure est la même.

$$BER''_{Eve}(n) = BER_{Eve}(n) = BER(0,\frac{n}{2}) = 1-\mathcal{P}_E$$

5.3.6 Sécurité obtenue

De la même manière que dans la section précédente nous mesurons la sécurité par le différentiel d'information mutuelle.

$$\begin{aligned}D = -(&BER_{Eve}\log_2 BER_{Eve} + (1-BER_{Eve})\log_2(1-BER_{Eve}) \\ &+ (BER\log_2 BER + (1-BER)\log_2(1-BER)\end{aligned}$$

Contrairement à l'attaque par interception et renvoi décrit dans la section précédente on remarque sur la figure 5.12 que le différentiel d'information mutuelle est toujours positif, ce qui signifie que la liaison génère toujours

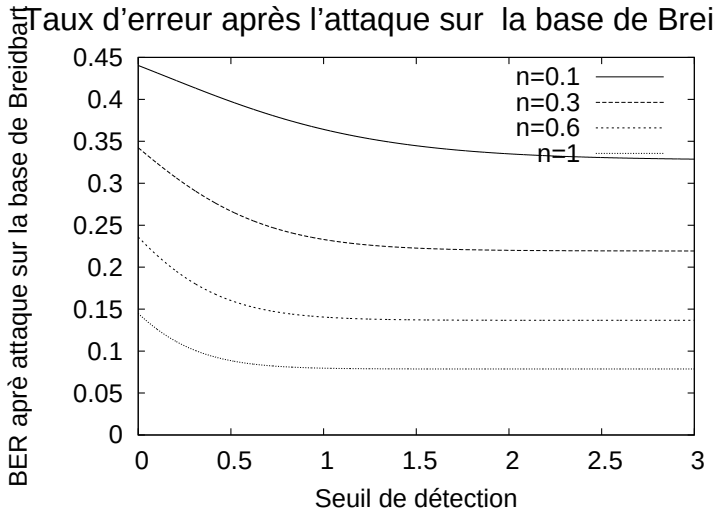

FIG. 5.11 – Évolution du taux d'erreur en fonction du seuil de la détection homodyne lors de l'attaque sur la base de Breidbart

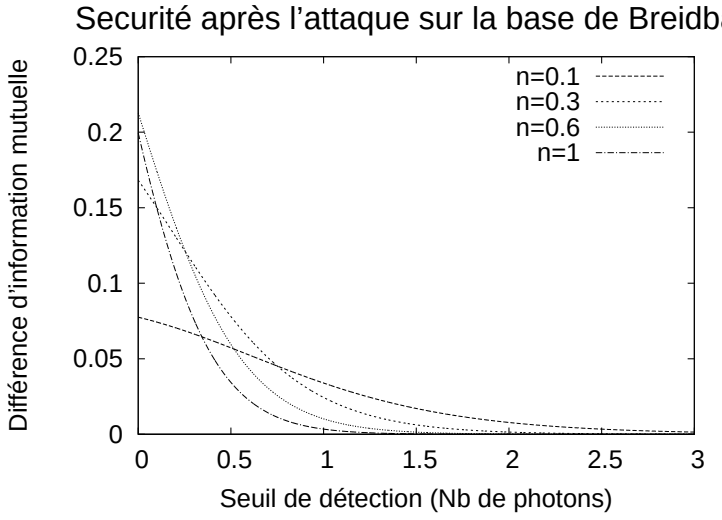

FIG. 5.12 – Différentiel d'information mutuelle après après l'attaque sur la base de Breidbart

assez de sécurité pour obtenir une clef après l'application d'un algorithme dit d'« amplification du secret ».

Il faut noter que dans l'attaque par interception et renvoi il y a une perte d'information au laboratoire d'Ève puisqu'elle « choisit »le bit à renvoyer parmi les quatre possibilités qu'elle a, alors que dans l'attaque par mesure sur la base de Breidbart, elle n'effectue pas le choix, elle renvoie ce qu'elle mesure.

5.4 Attaque par « vol de photon surnuméraire »

5.4.1 Description de l'attaque

Comme dans le chapitre 3.1.2, Ève est dotée d'un appareil permettant de connaître le nombre de photons qui se promènent sur la ligne. Quand il y en a au moins deux en un temps bit, elle opère son attaque qui consiste à en capturer un, et d'attendre la réconciliation entre Alice et Bob pour en lire le contenu grâce à une mémoire quantique. Ève n'a pas besoin de double-seuil, elle possède un appareil parfait au regard des lois de la mécanique quantique. En effet, nous donnons ici à Ève des détecteurs de photons idéaux. Nous lui donnons également toutes les données de références éventuelles dont elle pourrait avoir besoin pour construire un récepteur à base de compteurs de photons idéaux.

5.4.2 Modification de la distribution de photons par Ève

Dans ce système l'efficacité du récepteur est directement liée à la puissance qu'il reçoit. Dans le cas d'une distribution poissonnienne le nombre moyen de photons est égal à la puissance multipliée par le facteur $h\nu$. Après l'attaque d'Ève la distribution n'est plus poissonienne, ce qui implique que cette relation n'est plus respectée. Pour décrire la modification de l'opérateur densité, il faut être capable de décrire la nouvelle distribution.

5.4.2.1 Moyenne de la nouvelle distribution

Intéressons-nous à la nouvelle moyenne $\langle n' \rangle$ arrivant chez Bob après l'attaque.

$$\begin{aligned} \langle n' \rangle &= E(p_{Bob}) \\ &= 0 \times e^{-\mu} + 1 \times (\mu e^{-\mu} + \frac{\mu^2 e^{-\mu}}{2}) + \sum_{k=2}^{+\infty} k \frac{\mu^{k+1} e^{-\mu}}{(k+1)!} \end{aligned} \quad (5.12)$$

Soit $W(\mu) = \sum_{k=2}^{+\infty} k \frac{\mu^{k+1}}{(k+1)!}$. Notons dès à présent que $W(0) = 0$.

$$\begin{aligned} W(\mu) &= \sum_{k=2}^{+\infty} k\frac{\mu^{k+1}}{(k+1)!} \\ W(\mu) &= \sum_{k=0}^{+\infty} k\frac{\mu^{k+1}}{(k+1)!} - \frac{\mu^2}{2} \end{aligned} \tag{5.13}$$

Nous reconnaissons ici une série enitère. Nous pouvons exploiter les propriétés liées aux séries entières comme par exemple la dérivation. Donc par dérivation l'égalité 5.13 implique les égalites suivantes :

$$\begin{aligned} \frac{\mathrm{d}W}{\mathrm{d}\mu} &= \sum_{k=0}^{+\infty} \frac{k(k+1)\mu^k}{(k+1)!} - \frac{2\mu}{2} \\ \frac{\mathrm{d}W}{\mathrm{d}\mu} &= \mu\sum_{k=1}^{+\infty} \frac{\mu^{k-1}}{(k-1)!} - \mu \\ \frac{\mathrm{d}W}{\mathrm{d}\mu} &= \mu e^{\mu} - \mu \\ \frac{\mathrm{d}W}{\mathrm{d}\mu} &= \mu(e^{\mu} - 1) \end{aligned} \tag{5.14}$$

Pour revenir à l'expression $W(\mu)$ cherchée, nous procédons à l'intégration de l'équation 5.14 et obtenons le résultat à une constante K près.

$$W(\mu) = e^{\mu}(\mu - 1) - \frac{\mu^2}{2} + K \tag{5.15}$$

La connaissance de $W(0) = 0$ permet de déduire aisément que $K = 1$. En effectuant le remplacement de K par 1, il vient immédiatement :

$$W(\mu) = 1 - e^{\mu} + \mu e^{\mu} - \frac{\mu^2}{2}$$

En reprenant l'équation 5.12, et en utilisant le résultat du calcul de $W(\mu)$, nous pouvons écrire :

$$\begin{aligned} \langle n' \rangle &= \mu e^{-\mu} + \frac{\mu^2 e^{-\mu}}{2} + e^{-\mu} W(\mu) \\ \langle n' \rangle &= \mu e^{-\mu} + \frac{\mu^2 e^{-\mu}}{2} + e^{-\mu}(1 - e^{\mu} + \mu e^{\mu} - \frac{\mu^2}{2}) \\ \langle n' \rangle &= e^{-\mu}(1 + \mu) + \mu - 1 \end{aligned}$$

Nous avons donc le nombre moyen de photons $\langle n' \rangle$ qui arrivent chez Bob. Ce résultat nous permet également de calculer l'écart quadratique moyen à la moyenne $\langle (n' - \langle n' \rangle)^2 \rangle$ de cette distribution affectée par l'attaque d'Ève.

5.4.2.2 Variance de la nouvelle distribution

$$\begin{aligned}
\langle (n' - \langle n' \rangle)^2 \rangle &= \sum_{k=0}^{+\infty} (k - (e^{-\mu} + e^{-\mu} + \mu - 1))^2 \frac{e^{-\mu}\mu^{k+1}}{(k+1)!} \\
&= (\mu e^{-\mu} + e^{-\mu} + \mu - 1)^2 e^{-\mu} \\
&\quad + (1 - \mu e^{-\mu} - e^{-\mu} - \mu + 1)^2 (\mu e^{-\mu} + \frac{\mu}{2} e^{-\mu}) \\
&\quad + e^{-\mu} \sum_{k=2}^{+\infty} (k - (\mu e^{-\mu} + e^{-\mu} + \mu - 1))^2 \frac{\mu^{k+1}}{(k+1)!} \\
&= (e^{-\mu} + e^{-\mu} + \mu - 1)^2 e^{-\mu} \\
&\quad + (1 - (e^{-\mu} + e^{-\mu} + \mu - 1))^2 (\mu e^{-\mu} + \frac{\mu^2}{2} e^{-\mu}) \\
&\quad + e^{-\mu} \sum_{k=2}^{+\infty} \left((k+1) - (e^{-\mu} + e^{-\mu} + \mu) \right)^2 \frac{\mu^{k+1}}{(k+1)!}
\end{aligned}$$

Et connaissant la décomposition en séries entières de $e^{-\mu}$, nous pouvons remarquer les propriétés suivantes :

$$\begin{aligned}
\sum_{k=2}^{+\infty} \frac{\mu^{k+1}}{(k+1)!} &= e^{\mu} - 1 - \mu - \frac{\mu^2}{2} \\
\sum_{k=2}^{+\infty} (k+1) \frac{\mu^{k+1}}{(k+1)!} &= \mu \frac{\mathrm{d}\left(\sum_{k=2}^{+\infty} \frac{\mu^{k+1}}{(k+1)!} \right)}{\mathrm{d}\mu} \\
&= \mu e^{\mu} - \mu - \mu^2 \\
\sum_{k=2}^{+\infty} (k+1)^2 \frac{\mu^{k+1}}{(k+1)!} &= \mu \frac{\mathrm{d}\left(\sum_{k=2}^{+\infty} \frac{(k+1)\mu^{k+1}}{(k+1)!} \right)}{\mathrm{d}\mu} \\
&= \mu^2 e^{\mu} + \mu e^{\mu} - \mu - 2\mu^2
\end{aligned}$$

Reprenons le calcul précédent :

$$\begin{aligned}
\langle (n' - \langle n' \rangle)^2 \rangle &= (\mu e^{-\mu} + e^{-\mu} + \mu)^2 \\
&\quad + (\mu e^{-\mu} + e^{-\mu} + \mu)(-2e^{-\mu} - 2\mu e^{-\mu} - 2\mu) \\
&\quad + e^{-\mu} + 3\mu e^{-\mu} + \mu^2 + \mu \\
&= e^{-2\mu}(-2\mu^3 - 7\mu^2 - 6\mu - 1) \\
&\quad + e^{-\mu}(-3\mu^2 + 8\mu + 1) + 2\mu^3 + 4\mu^2) + \mu
\end{aligned}$$

5.4.3 Modification de l'opérateur densité chez Bob

Nous avons montré que :

$$\begin{aligned}\mathcal{P}(n) &= |\langle n|\alpha\rangle|^2 \\ &= \frac{e^{-|\alpha|^2}|\alpha|^{2n}}{n!}\end{aligned}$$

Nous avons bien évidemment, $|\alpha|^2 = \mu$. Nous allons chercher à calculer le nouvel opérateur densité ρ'. Si nous notons $|\alpha'\rangle$ le nouvel état résultant de l'intervention d'Ève sur un état cohérent, alors :

$$\rho' = |\alpha'\rangle\langle\alpha'| + |-\alpha'\rangle\langle-\alpha'| + |i\alpha'\rangle\langle i\alpha'| + |-i\alpha'\rangle\langle-i\alpha'| \tag{5.16}$$

L'attaque d'Ève se manifeste sur notre distribution par la disparition d'un photon quand au moins un photon arrive chez Ève.

$$\begin{aligned}\mathcal{P}'(n) &= |\langle n|\alpha'\rangle|^2 \\ &= \begin{cases}\mu e^{-\mu} + \frac{\mu^2}{2}e^{-\mu} \text{ si } n = 1 \\ \frac{\mu^{k+1}e^{-\mu}}{(n+1)!} \text{ si } n \geq 2\end{cases}\end{aligned} \tag{5.17}$$

Ceci implique pour l'état $|\alpha'\rangle$, qu'il existe $\{\theta_1, \cdots, \theta_k, \cdots\}$ tel que :

$$|\alpha'\rangle = \sqrt{\mu e^{-\mu} + \frac{\mu^2}{2}e^{-\mu}}e^{i\theta_1}|1\rangle + \sum_{k=2}^{+\infty}\sqrt{\frac{\mu^{k+1}e^{-\mu}}{(k+1)!}}e^{i\theta_k}|k\rangle \tag{5.18}$$

Nous avons $1 = \frac{1}{\pi}\int |\alpha\rangle\langle\alpha|(\mathrm{d}\alpha)^2$ qui conduit à :

$$|k\rangle = \frac{1}{\pi}\int |\alpha\rangle\langle\alpha|k\rangle(\mathrm{d}\alpha)^2 \tag{5.19}$$

En utilisant cette écriture de $|k\rangle$ dans l'expression de $|\alpha'\rangle$, on obtient :

$$\begin{aligned}|\alpha'\rangle &= \frac{1}{\pi}e^{-\frac{\mu}{2}}\sqrt{\mu + \frac{\mu^2}{2}}e^{i\theta_1}\int |\alpha\rangle\langle\alpha|k\rangle(\mathrm{d}\alpha)^2 \\ &\quad + \frac{1}{\pi}e^{-\frac{\mu}{2}}\sum_{k=2}^{+\infty}\sqrt{\frac{\mu^{k+1}}{(n+1)!}}e^{i\theta_k}\int |\alpha\rangle\langle\alpha|k\rangle(\mathrm{d}\alpha)^2|\alpha'\rangle\end{aligned} \tag{5.20}$$

En effectuant le produit scalaire de l'état cohérent α avec le bra $\langle k|$ correspondant au ket $|k\rangle$.

$$\begin{aligned}\langle k|\alpha\rangle &= e^{-\frac{1}{2}|\alpha|^2}\sum_{n=0}^{+\infty}\frac{\alpha^n}{\sqrt{n!}}\langle k|n\rangle \\ &= e^{-\frac{1}{2}|\alpha|^2}\frac{\alpha^n}{\sqrt{n!}}\end{aligned} \tag{5.21}$$

Il n'y a plus qu'à utiliser l'expression de $\langle k|\alpha\rangle$ dans notre expression de $|\alpha'\rangle$.

$$\begin{aligned}|\alpha'\rangle &= \frac{1}{\pi}e^{-\frac{\mu}{2}}\sqrt{\mu+\frac{\mu^2}{2}}e^{i\theta_1}\int e^{-\frac{1}{2}|\alpha|^2}\alpha^*|\alpha\rangle(\mathrm{d}\alpha)^2 \\ &\quad +\frac{1}{\pi}e^{-\frac{\mu}{2}}\sum_{k=2}^{+\infty}\sqrt{\frac{\mu^{k+1}}{(n+1)!}}e^{i\theta_k}\int e^{-\frac{1}{2}|\alpha|^2}(\alpha^*)^k|\alpha\rangle(\mathrm{d}\alpha)^2 \quad (5.22)\end{aligned}$$

Puis en appliquant la mesure x_{phi} il vient :

$$\begin{aligned}\langle x_\phi|\alpha'\rangle &= e^{-\frac{\mu}{2}}\sqrt{\mu+\frac{\mu^2}{2}}e^{i\theta_1}\int e^{-\frac{1}{2}|\alpha|^2}\alpha^*\langle x_\phi|\alpha\rangle(\mathrm{d}\alpha)^2 \\ &\quad +e^{-\frac{\mu}{2}}\sum_{k=2}^{+\infty}\sqrt{\frac{\mu^{k+1}}{(n+1)!}}e^{i\theta_k}\int e^{-\frac{1}{2}|\alpha|^2}(\alpha^*)^k\langle x_\phi|\alpha\rangle(\mathrm{d}\alpha)^2 (5.23)\end{aligned}$$

Il nous reste à calculer le module au carré de $\langle x_\phi|\alpha'\rangle$.

$$\begin{aligned}|\langle x_\phi|\alpha'\rangle|^2 &= e^{-\mu}|\sqrt{\mu+\frac{\mu^2}{2}}e^{i\theta_1}\int e^{-\frac{1}{2}|\alpha|^2}\alpha^*\langle x_\phi|\alpha\rangle(\mathrm{d}\alpha)^2 \\ &\quad +\sum_{k=2}^{+\infty}\sqrt{\frac{\mu^{k+1}}{(n+1)!}}e^{i\theta_k}\int e^{-\frac{1}{2}|\alpha|^2}\alpha^*\langle x_\phi|\alpha\rangle(\mathrm{d}\alpha)^2|^2 \quad (5.24)\end{aligned}$$

Nous savons que $|\langle x_\phi|\alpha\rangle|^2 = \sqrt{\frac{2}{\pi}}e^{-2(x_\phi-\alpha\cos\phi)^2}$. Par implication, il existe θ tel que

$$\langle x_\phi|\alpha\rangle = \left(\frac{2}{\pi}\right)^{\frac{1}{4}}e^{i\theta}e^{-(x_\phi-\alpha\cos\phi)^2} \quad (5.25)$$

Et donc, en injectant $\langle x_\phi|\alpha\rangle$ dans notre résultat :

$$\begin{aligned}|\langle x_\phi|\alpha'\rangle|^2 &= \sqrt{\left(\frac{2}{\pi}\right)}e^{-\mu}|\sqrt{\mu+\frac{\mu^2}{2}}e^{i\theta'_1}\int e^{-\frac{1}{2}|\alpha|^2}\alpha^*e^{-2(x_\phi-\alpha\cos\phi)^2}(\mathrm{d}\alpha)^2 \\ &\quad +\sum_{k=2}^{+\infty}\sqrt{\frac{\mu^{k+1}}{(n+1)!}}e^{i\theta'_k} \\ &\quad \times\int e^{-\frac{1}{2}|\alpha|^2}\alpha^*e^{-2(x_\phi-\alpha\cos\phi)^2}(\mathrm{d}\alpha)^2|^2 \quad (5.26)\end{aligned}$$

Il reste néanmoins à trouver les termes de phase θ', pour pouvoir construire le nouveau BER à obtenir chez Bob.

5.4.4 Information acquise par Ève

Alice utilise un nombre moyen de photons μ qu'elle envoie sur la ligne. À chaque fois qu'il y en a au moins deux Ève en récupère un et apprend

l'information qui en découle. La probabilité p_{Eve} qu'Ève ne récupère aucune information est donnée par :

$$e^{-\mu} - \mu e^{-\mu} \tag{5.27}$$

Par contre lorsque la détection chez Bob donne une erreur, ou est abandonnée, un bit obtenu par Ève lui est absolument inutile. Il ne faut donc tenir compte pour le gain d'information que de la probabilité $BCR_{PNS_{Eve}}$ que Bob obtienne un bit correct malgré l'attaque d'Ève.

$$BCR_{PNS_{Eve}} = \frac{1}{\mathcal{P}_{\mathcal{PNS}}(x_0, n)} \sum_{k=0}^{+\infty} \frac{\mu^{k+1} e^{-\mu}}{(k+1)!} \operatorname{erfc}(\sqrt{2}(x_0 - \sqrt{k}) \tag{5.28}$$

Grâce à l'équation 5.27 nous pouvons déduire le taux d'information par bit recueilli par Ève.

$$\begin{aligned} I(A,E) \quad = \quad & (1 - BCR_{PNS_{Eve}}) \log_2 (1 - BCR_{PNS_{Eve}}) - \\ & BCR_{PNS_{Eve}} \log_2 BCR_{PNS_{Eve}} \end{aligned} \tag{5.29}$$

Conclusions et perspectives

Parce que la polarisation est mal conservée lors de la propogation dans les fibres optiques, nous avons envisagé l'utilisation de la modulation de phase pour interpréter le protocole BB84. Nous avons fourni une étude de sécurité de la distribution de clef dans le cas d'un protocole utilisant des états cohérents à faible énergie à détection homodyne dans le cas d'une attaque par vol de photon surnuméraire. La détection homodyne est en effet une alternative crédible à l'utilisation de compteur de photon présentant une faible efficacité quantique et des effets thermiques importants à la longueur d'onde des télécommunications ainsi qu'une faible rapidité. La détection homodyne permet de bénéficier d'un gain de mélange sans pénalité de bruit autre que les fluctuations du vide. Elle permet une rapidité compatible avec les applications. Puis nous avons comparé ce résultat au cas d'un protocole différentiel. Après une étude détaillée de l'évolution de la densité de distribution des photons après une attaque d'Ève, nous avons révélé qu'on pouvait se servir du taux de détection en plus de l'information mutuelle pour affiner la détermination de la sécurité. Nous avons montré que la sécurité en était améliorée par un mécanisme où la sécurité est portée individuellement et collectivement par les photons. Nous avons rapporté que même si Ève est dotée de moyens les plus puissants permis par la mécanique quantique, il reste néanmoins une sécurité résiduelle. Le principal facteur limitant pour Alice et Bob est la faible efficacité des compteurs de photons actuellement disponibles. Cette étude prend en compte selon l'usage la pire situation pour Alice et Bob et la plus favorable pour Ève, cela laisse présager une implémentation largement réalisable. De plus, la faible efficacité des ces détecteurs laisse une marge de progression très élevée pour l'évolution du matériel. Ces protocoles et méthodes envisagées participent d'un avenir certain.

Nous avons également envisagé une stratégie de détection discriminant les bits de faible sécurité et ceux de sécurité plus forte. Au détriment du débit de distribution de la clef, nous pouvons grandement augmenter la sécurité de la clef, grâce à une détection homodyne à double seuil et sélection des opportunités de décision. Pour ce type de détection, nous avons mené l'étude de la sécurité au travers de deux attaques, interception et renvoi ainsi que l'utilisation de la base intermédiaire de Breidbart. Alors que le protocole a été étudié sour une approche ondulatoire, nous avons travaillé à une étude similaire pour une attaque par vol de photon surnuméraire. Dans ce cas-là, Ève est dotée d'un compteur de photons idéal tandis que Bob est limité à

un détecteur homodyne à double seuil.

Nous pourrions mener une étude en partant de celle de l'homodynage à double seuil en affectant un coefficient de sécurité sur chaque bit obtenu et élaborer par la suite une clef tenant compte de ce coefficient. Cela pourrait permettre de réduire l'effet binaire de la décision à seuil. Nous pourrions ainsi ajuster de manière plus fine le compromis entre sécurité et débit de clef.

Pour améliorer la complétude du travail, il faut envisager d'augmenter le panel d'attaques à prendre en compte. Pour la complétude de l'étude, une factorisation des attaques serait souhaitable. Il peut aussi s'avérer intéressant d'étudier les attaques dites cohérentes.

Bibliographie

[1] S. Agnolini and P. Gallion. Implementation of BB84 protocol by qpsk modulation using dual-electrode mach-zehnder modulator. *IEEE International Conference on Industrial Technology*, 2004.

[2] R. Alleaume, F. Treussart, J.-M. Courty, and J.-F. Roch. Photon statistics characterization of a single-photon source. *New Journal of Physics*, 6 :85, 2004.

[3] A. Barenco, D. Deutsch, A. Ekert, and R. Jozsa. Conditional quantum dynamics and logic gates. *Phys. Rev. Lett.*, 74(20) :4083–4086, May 1995.

[4] J.-L. Basdevant and J. Dalibart. *Mécanique quantique*. Les éditions de l'école polytechnique, 2006.

[5] C. Bennett, G. Brassard, et al. Quantum cryptography : Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, volume 175, 1984.

[6] C. H. Bennett, F. Bessette, G. Brassard, and L. Salvail. Experimental quantum cryptography. *Journal of Cryptology*, 5(1) :1–28, January 1992.

[7] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70(13) :1895–1899, Mar 1993.

[8] C. H. Bennett and P. W. Shor. Quantum inforamtion theory. *IEEE transactions on information theory*, 44(6), October 1998.

[9] G. Brassard and L. Salvail. Secret-key reconciliation by public discussion. In *EUROCRYPT '93 : Workshop on the theory and application of cryptographic techniques on Advances in cryptology*, pages 410–423, Secaucus, NJ, USA, 1994. Springer-Verlag New York, Inc.

[10] J. Breguet, A. Muller, and N. Gisin. Quantum Cryptography with Polarized Photons in Optical Fibres : Experiment and Practical Limits. *Journal of Modern Optics*, 41 :2405–2412, Dec. 1994.

[11] R. Brouri, A. Beveratos, J.-P. Poizat, and P. Grangier. Single-photon generation by pulsed excitation of a single dipole. *Phys. Rev. A*, 62(6) :063817, Nov 2000.

[12] A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54 :1098–1105, 1996.

[13] T. Chaneliere, D. N. Matsukevich, S. D. Jenkins, S. Y. Lan, T. A. B. Kennedy, and A. Kuzmich. Storage and retrieval of single photons transmitted between remote quantum memories. *Nature*, 438 :833, 2005.

[14] C. Cohen-Tannoudji, B. Diu, and F. Laloë. *Mécanique Quantique*, volume 1. Hermann, 1977.

[15] E. Diamanti. *Security and implementation of differential phase shift quantum key distribution systems.* PhD thesis, Stanford University, 2006.

[16] D. P. DiVincenzo. The physical implementation of quantum computation. *Fortschritte der Physik*, 48(09-11) :771–783, 2000.

[17] P. Gallion, F. J. Mendieta, and S. Jiang. *Progress in Optics*, volume 52, chapter Signal and quantum noise in optical communcation and in cryptography. Elsevier, January 2009.

[18] C. W. Gardiner. *Quantum Noise.* Springer-Verlag, 1991.

[19] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill. Security of quantum key distribution with imperfects devices. *Quantum Information and Computation*, 4, 2004.

[20] Hérodote. *Histoires.* Hachette, 1958.

[21] T. Honjo, K. Inoue, and H. Takahashi. Differential-phase-shift quantum key distribution experiment with aplanar light-wave circuit mach-zehnder interferometer. *Opt. Lett.*, 29(23) :2797–2799, 2004.

[22] W.-Y. Hwang. Quantum key distribution with high loss : Toward global secure communication. *Phys. Rev. Lett.*, 91(5) :057901, Aug 2003.

[23] Id Quantique. *id200, Single-Photon Detector Module, Operating Guide.*

[24] John G. Proakis. *Digital Communications.* McGraw Hill International Editions, 1995.

[25] R. Keyes. Challenges for quantum computing with solid-state devices. *Computer*, 38(1) :65–69, Jan. 2005.

[26] D. Kielpinski, A. Ben-Kish, J. Britton, V. Meyer, M. A. Rowe, C. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland. Recent results in trapped-ion quantum computing at nist. *Proceedings of the International Conference on Experimental Implementation of Quantum Computation*, pages 79–90, January 2001.

[27] D. Knuth. *The art of Computer Programming*, volume 2. Addison-Wesley, 2005.

[28] H.-K. Lo, X. Ma, and K. Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94(23) :230504, Jun 2005.

[29] C. Marand and P. D. Townsend. Quantum key distribution over distances as long as 30 km. *Opt. Lett.*, 20(16) :1695, 1995.

[30] H. Mathieu. *Physique des semiconducteurs et des composants électroniques*. Dunod, 2004.

[31] J.-M. Mérolla, Y. Mazurenko, J.-P. Goedgebuer, and W. T. Rhodes. Single-photon interference in sidebands of phase-modulated light for quantum cryptography. *Phys. Rev. Lett.*, 82(8) :1656–1659, Feb 1999.

[32] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin. "plug and play" systems for quantum cryptography. *Applied Physics Letters*, 70(7) :793–795, 1997.

[33] R. Namiki and T. Hirano. Security of quantum cryptography using balanced homodyne detection. *Phys. Rev. A*, 67(2) :022308, Feb 2003.

[34] W. T. Nicolas Gisin, Grégoire Ribordy and H. Zbinden. Quantum cryptography. *Reviews of modern physics*, January 2002.

[35] G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden. Automated 'plug and play' quantum key distribution. *Electronics Letters*, 34(22) :2116–2117, Oct 1998.

[36] M. Sabban, Q. Xu, P. Gallion, and F. Mendieta. Security evaluation of dual-threshold homodyne quantum cryptographic systems. In *International Conference on Quantum Information*, page JMB77. Optical Society of America, 2008.

[37] B. Schneier. *Applied Cryptography*. John Wiley and Sons, 1996.

[38] C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28 :656–715, 1949.

[39] A. Shields. Single photon quantum cryptography and devices. In *Conference on Lasers and Electro-Optics/International Quantum Electronics Conference and Photonic Applications Systems Technologies*, page IWE3. Optical Society of America, 2004.

[40] P. W. Shor. Algorithms for quantum computation : discrete logarithms and factoring. In *Foundations of Computer Science*, pages 124–134, Nov 1994.

[41] P. W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52(4) :R2493–R2496, Oct 1995.

[42] P. W. Shor and J. Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical Review Letters*, 85 :441, 2000.

[43] S. Takeuchi, R. Okamoto, and K. Sasaki. High-yield single-photon source using gated spontaneous parametric downconversion. *Appl. Opt.*, 43(30) :5708–5711, 2004.

[44] A. Tosi, S. Cova, F. Zappa, M. Itzler, and R. Ben-Michael. Ingaas/inp single photon avalanche diode design and characterization. In *Solid-State Device Research Conference*, pages 335–338, Sept. 2006.

[45] L. M. K. Vandersypen, M. Steffen, C. S. Y. Gregory Breyta, M. H. Sherwood, and I. L. Chuang. Experimental realization of shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature*, 414 :883–887, December 2001.

[46] M. B. Ward, O. Z. Karimov, P. Atkinson, D. C. Unitt, Z. Yuan, P. See, D. G. Gevaux, D. A. Ritchie, and A. J. Shields. Telecom wavelength quantum dot single photon source. In *Conference on Lasers and Electro-Optics/Quantum Electronics and Laser Science and Photonic Applications Systems Technologies*, page QMJ3. Optical Society of America, 2005.

[47] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299 :802–803, 1982.

[48] Q. Xu, M. C. e Silva, M. Sabban, P. Gallion, and F. Mendieta. Dual-threshold balanced homodyne detection at 1550nm optical fiber quantum key distribution system. *Journal of Lightwave Technology*, 2009. to be published.

[49] Q. Xu, M. Sabban, and P. Gallion. Homodyne detection of weak coherent optical pulse : Applications to quantum cryptography. *Microwave and Optical Technology Letters*, 2009. To be published.

[50] Q. Xu, M. Sabban, P. Gallion, and F. Mendieta. Dual-threshold receiver for 1550nm homodyne qpsk quantum key distribution system. In *Coherent Optical Technologies and Applications*, page CWC4. Optical Society of America, 2008.

[51] Q. Xu, M. Sabban, P. Gallion, and F. Mendieta. Quantum key distribution system using dual-threshold homodyne detection. In *Research, Innovation and Vision for the Future*, pages 1–8, July 2008.

[52] H. Zbinden, J. Gautier, N. Gisin, B. Huttner, A. Muller, and W. Tittel. Interferometry with faraday mirrors for quantum cryptography. *Electronics Letters*, 33(7) :586–588, Mar 1997.

[53] Y. Zhao, B. Qi, X. Ma, H.-K. LO, and L. Qian. Experimental quantum key distribution with decoy states. *Physical Review Letters*, 96 :070502, 2006.

[54] G. Zémor. *Cours de cryptographie*. Cassini, 2000.

Listes des publications

[MQPF08] Sabban M., Xu Q., Gallion P., and Mendieta F.J. Security evaluation of dual-threshold homodyne quantum cryptographic systems. In *International Conference on Quantum Information*, page JMB77. Optical Society of America, 2008.

[QeSMM+09] Xu Q., Costa e Silva M.B., Sabban M., Gallion P., and Mendieta F.J. Dual-threshold balanced homodyne detection at 1550nm optical fiber quantum key distribution system. *Journal of Lightwave Technology*, 2009. to be published.

[QMP09] Xu Q., Sabban M., and Gallion P. Homodyne detection of weak coherent optical pulse : Applications to quantum cryptography. *Microwave and Optical Technology Letters*, 2009. to be published.

[QMPF08] Xu Q., Sabban M., Gallion P., and Mendieta F.J. Dual-threshold receiver for 1550nm homodyne qpsk quantum key distribution system. In *Coherent Optical Technologies and Applications*, page CWC4. Optical Society of America, 2008.

[SGM08] Qing Xu 0006, Manuel Sabban, Philippe Gallion, and Francisco Mendieta. Quantum key distribution system using dual-threshold homodyne detection. In *RIVF*, pages 1–8. IEEE, 2008.