Algorithme de réconciliation et méthodes de distribution quantique de clés adaptées au domaine fréquentiel

Matthieu Bloch

N° d'ordre : 1199 Année 2006

THÈSE

présentée à

L'U.F.R DES SCIENCES ET TECHNIQUES
DE L'UNIVERSITÉ DE FRANCHE-COMTÉ

pour obtenir le

GRADE DE DOCTEUR DE L'UNIVERSITÉ DE FRANCHE-COMTÉ
Spécialité Sciences pour l'Ingénieur

Algorithme de réconciliation et méthodes de distribution quantique de clés adaptées au domaine fréquentiel

par

Matthieu Bloch

Soutenue le 11 Décembre 2006 devant la commission d'examen :

Président	Hervé Maillotte	Professeur à l'Université de Franche-Comté
Rapporteurs	Philippe Gallion	Professeur à l'Ecole Nationale Supérieure des Télécommunications
	Philippe Grangier	Directeur de Recherche au CNRS
Examinateurs	Nicolas Cerf	Professeur à l'Université Libre de Bruxelles
	Steven McLaughlin	Professeur au Georgia Institute of Technology
	Laurent Larger	Professeur à l'Université de Franche-Comté
	Jean-Marc Merolla	Chargé de Recherche au CNRS

Sommaire

Remerciements

Le travail de recherche présenté dans ce manuscrit a été réalisé au laboratoire GTL-CNRS Télécom, dans le cadre d'une collaboration entre l'Université de Franche-Comté et le Georgia Institute of Technology. Je remercie sincèrement Steven McLaughlin et Jean-Marc Merolla qui m'ont encadré au cours de ces trois années et m'ont permis de profiter pleinement des opportunités offertes par cette collaboration internationale.

Mes remerciements vont également à Philippe Gallion et Philippe Grangier qui ont eu la lourde tâche de rapporter ce manuscrit, ainsi qu'à Nicolas Cerf, Laurent Larger, et Hervé Maillotte qui ont accepté de faire partie du jury.

Au cours de ces trois années de thèse, j'ai eu l'occasion de collaborer avec Jérôme Lodewyck et Andrew Thangaraj. Leurs qualités humaines et scientifiques ont grandement contribué aux résultats présentés ici.

Ces remerciements ne seraient pas complets sans mentionner mes camarades de galère : Xavier Bavard, David Boivin, Johann Cussey, Stéphane Donnet, Nicolas Gastaud, Marc Hanna, Olivier Konne, Pierre-Ambroise Lacourt, Lydie Lasnier, Alexandre Locquet, Samuel Moëc, Damien Nirousset, Aurélien Pallavisini, Frédéric Patois, Stéphane Poinsot, et Jérôme et Muriel Vasseur.

Introduction

Le développement des réseaux de communication a radicalement changé notre façon d'échanger de l'information. L'augmentation des débits des lignes de transmission a tout d'abord autorisé des communications de plus en plus élaborées. Alors qu'il y 20 ans les communications en temps réel étaient encore limitées aux conversations téléphoniques, il est aujourd'hui possible de diffuser une vidéo conférence d'un bout à l'autre de la planète de manière quasi-instantanée. Mais l'augmentation de la capacité des réseaux s'est aussi accompagnée d'une évolution de la nature des messages échangés. A travers le réseau Internet, on peut désormais non seulement communiquer à distance avec une personne physique mais aussi accéder à virtuellement n'importe quel service. En conséquence les réseaux véhiculent un nombre de plus en plus important de données bancaires, médicales, commerciales, administratives, etc.

La croissance de la connectivité des réseaux s'est malheureusement aussi accompagnée d'une augmentation de leur vulnérabilité. Une fois un message envoyé, il est devenu difficile de garantir que ce dernier ne sera ni intercepté, stocké, dupliqué ou voir même dans le pire des cas modifié avant d'atteindre son destinataire légitime. Autant l'interception d'un courriel ne prête généralement pas à conséquence, autant l'accès à certaines des données mentionnées précédemment peut porter préjudice. Cette nécessité de protéger un volume de données sensibles de plus en plus important a bouleversé le champ d'application de la cryptographie. Alors qu'elle n'était utilisée qu'à des qu'à des fins militaires il y a encore quelques dizaines d'années, la cryptographie est aujourd'hui au cœur même de toutes nos communications.

La sécurité des méthodes de cryptage les plus répandues repose sur des conjectures mathématiques laissant penser qu'il est impossible de déchiffrer un message crypté ou de retrouver une clé de cryptage en un temps raisonnable avec la puissance de calcul actuelle. Cette notion de sécurité *calculatoire* présente cependant un inconvénient majeur : la sécurité a une portée limitée dans le temps car elle peut être remise en cause par des progrès mathématiques ou technologiques. Par exemple, le cryptage RSA inventé en 1977 repose sur l'hypothèse qu'il est difficile de décomposer un grand nombre entier en facteurs premiers, mais l'algorithme proposé en 1995 par Peter Shor permettrait cependant d'effectuer cette opération en un temps très court si sa mise en œuvre sur un ordinateur quantique s'avérait possible. Sans même parier sur l'avènement hypothétique d'une technologique « quantique », une clé RSA de 512 bits était considérée tout à fait sûre au début des années 90, mais il n'a fallu que quelques mois pour casser ce code avec 300 ordinateurs en 1999. La taille des clés recommandée pour le RSA est d'ailleurs aujourd'hui de 1024 ou 2048 bits.

La cryptographie quantique permet de remédier à cet inconvénient en envisageant la sécurité d'une toute autre manière. Tout d'abord la sécurité est évaluée de manière

quantitative selon les critères de la théorie de l'information. Les messages ne sont plus envisagés comme des quantités déterministes mais comme des grandeur fondamentalement aléatoires, et un message crypté est sécurisé s'il semble totalement aléatoire à toute personne ne possédant pas la clé de décryptage. Cette notion de sécurité *inconditionnelle* est aujourd'hui acceptée comme la définition la plus stricte et la plus générale de la sécurité. La deuxième particularité de la cryptographie quantique est de coder l'information des états quantiques. Alors que la cryptographie classique autorise un éventuel espion à manipuler une copie parfaitement identique du message original, les lois de la mécanique quantique interdisent la duplication parfaite d'un état quantique sans altérer l'original. En 1984, Gilles Bennett et Charles Brassard ont ainsi proposé le premier protocole permettant effectivement d'exploiter les propriétés quantiques de photons uniques pour permettre des échanges de clés parfaitement secrètes entre deux destinataires légitimes. Bien que la sécurité de ce protocole et de ses dérivés repose sur des propriétés purement quantiques, il est apparu que l'on pouvait atteindre ce niveau de sécurité sans même utiliser des états spécifiquement quantiques, mais en travaillant seulement avec des états cohérents de la lumière, aisément générables et contrôlables. Cette constatation a permis à la cryptographie quantique expérimentale de bénéficier de toute la technologie développée pour les communications optiques.

La cryptographie quantique est aujourd'hui devenue un domaine de recherche à part entière, à l'interface entre l'information quantique, l'optoélectronique et la théorie de l'information. L'information quantique permet d'étudier les limites fondamentales des protocoles, la théorie de l'information permet de mettre au point les algorithmes utilisés en pratique et l'optoélectronique permet de réaliser la manipulation d'états quantiques de la lumière. La mise au point de systèmes performants repose sur la maîtrise et la compréhension de ces trois aspects, c'est donc avec une approche pluridisciplinaire que nous avons abordé tous les travaux de cette thèse.

Ce manuscrit est organisé en quatre chapitres. Le premier introduit les notions fondamentales de la cryptographie quantique, de la description des protocoles jusqu'au systèmes de transmission déjà réalisés. Le deuxième chapitre propose une nouvelle méthode de codage permettant de réaliser un système robuste et stable pour la cryptographie quantique à photons uniques, qui se démarque des travaux réalisés jusque là en exploitant un codage fréquentiel de l'information. La mise au point d'un tel système est rendue possible par une modélisation quantique des composants optoélectroniques utilisés pour les télécommunications optiques standard. Le principe de fonctionnement du système est validé expérimentalement en effectuant une transmission sur une fibre optique. Le troisième chapitre présente les travaux préliminaires permettant d'envisager la réalisation d'un système de distribution quantique de clés haut débit. Ce système permet de mettre en œuvre les récents protocoles de cryptographie quantique par « variables continues », basés sur l'utilisation d'états quasi-classiques de la lumière. Ce système repose sur la réalisation d'un dispositif de détection homodyne impulsionnelle dont nous présentons les caractéristiques expérimentales. Le quatrième et dernier chapitre présente un algorithme de réconciliation, qui est un élément clé des protocoles de cryptographie quantique par variables continues. L'analyse et l'optimisation de codes correcteurs d'erreurs permettent d'obtenir des performances supérieures à celles des algorithmes existants. Nous concluons finalement en faisant le bilan des travaux réalisés et présentant les perspectives et améliorations à apporter.

Chapitre 1

Distribution quantique de clé

Sommaire

Suite aux premières propositions de protocoles utilisant les propriétés quantiques de la lumière pour garantir des échanges de clés sécurisés [1, 2], la distribution quantique de clé (appelée aussi *cryptographie quantique*) a connu un franc succès auprès de la communauté scientifique. Entre 1992 et 2002, les systèmes de cryptographie quantique sont passés du stade d'expériences de principe [3] à celui de systèmes stables et automatisés [4] pouvant être employés sur des réseaux optiques. Bien que l'on soit aujourd'hui encore très loin d'un déploiement à grande échelle, l'existence de quelques systèmes commerciaux (IdQuantique [5], MagiQ [6], SmartQuantum [7]) souligne la maturité et l'intérêt réel de cette technologie. L'objectif de ce chapitre d'introduction est de présenter la distribution quantique de clé en mettant l'accent sur la description des outils algorithmiques et expérimentaux mis en œuvre dans les systèmes pratiques. En particulier les principaux résultats concernant la sécurité des différents protocoles de cryptographie quantique seront rappelés sans être redémontrés.

1.1 De la cryptographie classique à la cryptographie quantique

Bien que la sécurisation des données n'ait pris toute son importance qu'avec le développement des réseaux informatiques et du partage à grande échelle de l'information, cette problématique n'est pas récente. Les premières méthodes de cryptage sont apparues dès l'antiquité, et même si ces dernières ont été largement améliorées par la suite, certaines techniques utilisées aujourd'hui sont encore basées sur les mêmes principes. On peut considérer que la cryptographie a évolué en quatre grandes étapes :

1. **L'ère des cryptogrammes.** Un exemple de cryptogramme est le « code de César » consistant à utiliser une permutation des lettres de l'alphabet pour crypter un message. Même si la permutation n'est connue que de l'expéditeur et du destinataire légitime ce type de code n'offre qu'une protection très relative, car il est possible d'inverser la permutation en se basant sur les statistiques d'apparition des symboles du message.
2. **L'ère des machines cryptographiques.** L'utilisation de machines électromécaniques a permis d'améliorer notablement la complexité des algorithmes de cryptage. La machine « Enigma » utilisée pendant la Seconde Guerre Mondiale en est l'exemple le plus célèbre.
3. **La cryptographie moderne.** L'apparition des ordinateurs a rendu obsolètes de nombreuses méthodes de cryptage purement combinatoires. Pour faire face à la croissance de la puissance de calcul, les méthodes de cryptographie modernes s'appuient désormais sur des analyses mathématiques précises.
4. **La cryptographie physique.** Cette branche récente de la cryptographie vise à utiliser des propriétés physiques (telles que la présence de bruit) et non plus mathématiques pour garantir la confidentialité des transmissions. La cryptographie quantique en est l'exemple le plus abouti, mais on peut aussi citer la cryptographie par chaos [8] ou l'utilisation du bruit de Johnson [9] et du bruit de photon [10][1], et dans une certaine mesure les techniques de codage tirant parti du bruit statistique présent sur les canaux de transmission [11, 12].

Par souci de concision, seules les principales techniques utilisées en cryptographie moderne seront brièvement présentées dans ce chapitre. Une description bien plus complète et détaillée peut être trouvée dans les références [13, 14].

1.1.1 Objectifs de la cryptographie

Le paradigme de la cryptographie moderne est représenté de façon imagée figure 1.1. Dans ce scénario, Alice cherche à envoyer un message à Bob tout en garantissant la confidentialité et l'intégrité du message. En d'autres termes un destinataire illégitime, représenté par l'espion Eve, ne doit ni comprendre ni pouvoir modifier le message lors de sa transmission. Il est important de remarquer dès maintenant qu'il n'existe pas de

[1] La sécurité des systèmes présentés dans ces références est sujette à controverse, néanmoins il est clair que l'utilisation de phénomènes physiques complique grandement la tâche d'un éventuel espion et peut compléter avantageusement les méthodes de cryptographie standard.

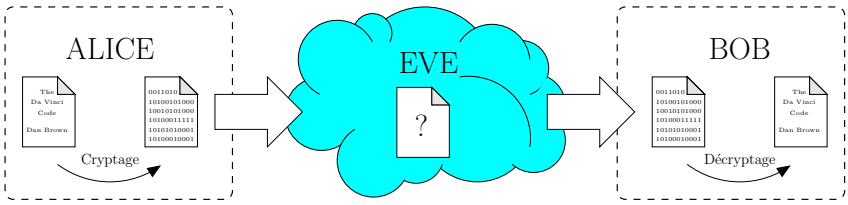


FIG. 1.1 – Paradigme de la cryptographie moderne.

méthode de cryptage rendant un message totalement indéchiffrable. En effet, lors de la transmission d'un message crypté contenant k bits d'information, une stratégie d'espionnage peu efficace mais tout à fait valide consiste simplement à tenter de deviner le contenu du message. Dans le pire des cas les bits du message sont parfaitement aléatoires et la probabilité de succès est alors de 2^{-k}. Ce résultat ne signifie pas que toute tentative de cryptage est vouée à l'échec, mais souligne au contraire le caractère probabiliste attaché à la notion de sécurité. On retient généralement deux définitions de sécurité :

1. **La sécurité calculatoire.** Ce type de sécurité repose sur certaines hypothèses restrictives concernant la technologie et les capacités de calcul d'Eve, et garantit uniquement que le temps de calcul ou la mémoire nécessaires pour décrypter un message sont « déraisonnables ». Une méthode de cryptage est considérée sécurisée si la complexité algorithmique du décryptage est équivalente à celle d'un problème mathématique réputé difficile à résoudre (problème « NP »). C'est cette notion de sécurité qui est utilisée pour évaluer les protocoles de cryptographie actuels, et bien qu'elle soit tout à fait satisfaisante dans beaucoup de situations, son inconvénient majeur est d'avoir une portée limitée dans le temps. Les méthodes réputées inviolables il y a 20 ans sont aujourd'hui facilement décryptables avec des ordinateurs standard, et leur puissance de calcul croissante force les cryptographes à réviser régulièrement leurs algorithmes.
2. **La sécurité inconditionnelle.** Cette notion de sécurité ne fait aucune hypothèse sur les capacités technologiques d'Eve, et évalue la sécurité selon les critères très généraux de la théorie de l'information. Il n'existe malheureusement que peu de méthodes garantissant une telle sécurité, et la cryptographie quantique est la seule technique pratique existant à ce jour.

1.1.2 Principes et limites des techniques de cryptographie standard

La cryptographie moderne ne se limite pas à l'étude de méthodes de cryptage/décryptage, mais couvre aussi les problématiques de signature des données, d'authentification des communications, d'intégrité des messages, etc. Présenter de façon rigoureuse toutes les facettes de la cryptographie sort largement du cadre de ce manuscrit, et nous nous restreindrons à une présentation très succincte des principales méthodes de cryptage. Ces dernières se répartissent en deux grandes catégories, les méthodes de cryptage dites symétriques et celles dites asymétriques. Ces méthodes ont chacune leurs avantages et inconvénients, aucune n'offre de solution parfaite et dans de nombreuses applications les deux méthodes sont généralement combinées.

Cryptage symétrique.

Le principe du cryptage symétrique est illustré par le diagramme de la figure 1.2. Alice et Bob disposent d'une même clé secrète k et d'algorithmes leur permettant de crypter ($\mathcal{E}$) ou décrypter ($\mathcal{D}$) un message m à l'aide de cette clé. L'espion Eve n'a accès qu'au message crypté c mais a généralement connaissance des algorithmes $\mathcal{E}$ et $\mathcal{D}$ utilisés par Alice et Bob.

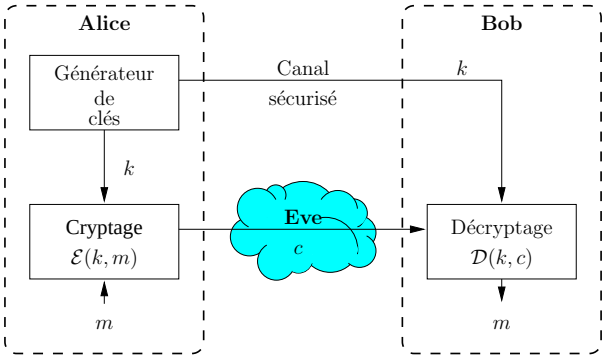


FIG. 1.2 – Principe du cryptage symétrique.

Le principal avantage de cette technique est son très haut débit de cryptage. Le cryptage AES (*Advanced Encryption Standard*) peut par exemple être réalisé directement sur des puces et atteindre des débits de l'ordre du gigaoctet par seconde [15]. En revanche la sécurité du système repose non seulement sur l'existence d'algorithmes difficiles à cryptanalyser, mais aussi sur la possibilité de pouvoir distribuer des clés de façon efficace et parfaitement sûre entre Alice et Bob. Par ailleurs la gestion de clés secrètes sur un réseau de N utilisateurs peut devenir un véritable casse-tête dans la mesure où le nombre de clés nécessaires est alors $N(N-1)/2$.

Cryptage asymétrique.

Le cryptage asymétrique a été envisagé pour la première fois dans les années 70 afin de remédier au problème de la distribution de clé. Comme indiqué dans le diagramme de la figure 1.3, son principe est radicalement différent du cryptage symétrique et Bob dispose cette fois-ci de deux clés distinctes. La clé publique k_{pub} permettant de crypter les messages est accessible à toute personne désirant communiquer avec lui, en revanche la clé privée k_{priv} utilisée pour le décryptage est gardée secrète. De façon très imagée, la clé publique joue le rôle d'un coffre fort ouvert que toute personne peut verrouiller, mais dont seul Bob possède la clé.

Bien évidemment cette méthode de cryptage n'est valide que si la connaissance de k_{pub} ne permet pas de remonter à la clé secrète k_{priv}. En pratique les deux clés ne peuvent pas être complètement indépendantes, et sont généralement construites en exploitant des conjectures mathématiques laissant supposer qu'il est impossible de reconstruire k_{priv} à partir de k_{pub} en un temps raisonnable. A titre d'exemple, la sécurité du protocole RSA repose sur le problème de la factorisation d'un nombre entier en facteurs premiers[2]. Les

[2]En réalité il ne s'agit que d'une conjecture puisque l'équivalence entre la sécurité du RSA et la décomposition en facteurs premiers n'a pas été prouvée

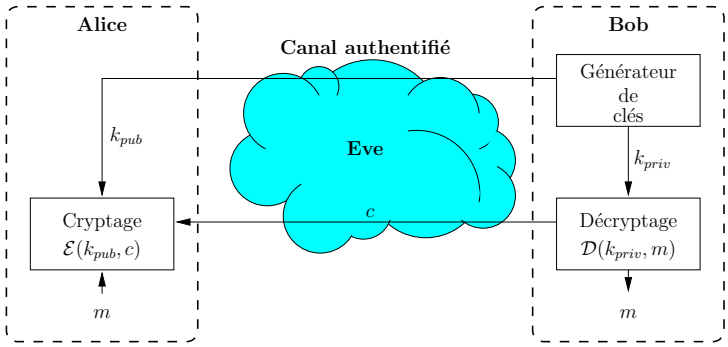
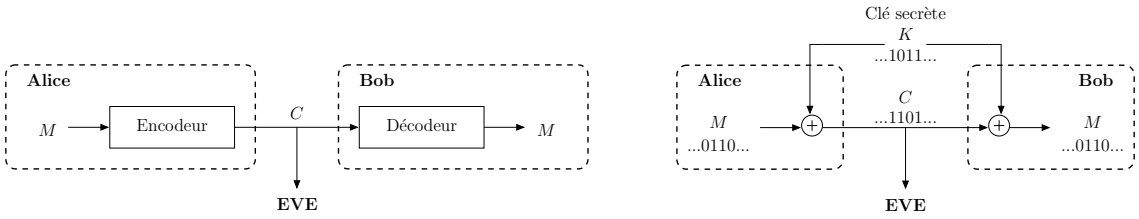


FIG. 1.3 – Principe du cryptage asymétrique.

débits de cryptage atteignables avec ces méthodes sont un à deux ordres de grandeur inférieurs à ceux des cryptages symétriques, cependant la gestion des clés sur un réseau de N utilisateurs est grandement simplifiée car seules N paires de clés privées et publiques sont nécessaires.

Limite fondamentale des méthodes de cryptographie classique.

La théorie de l'information apporte une réponse assez inattendue au problème des communications sécurisées. Le modèle d'une transmission telle qu'elle est envisagée en cryptographie standard est représenté figure 1.4(a). Alice dispose d'un système lui permettant de coder un message m composé de k bits en un message crypté c de n bits, lequel est alors transmis à Bob sur un canal sans pertes et sans bruit supposé totalement accessible à Eve. Au récepteur, un décodeur permet à Bob d'inverser l'opération d'Alice et de retrouver m à partir de c. Du point de vue de la théorie de l'information, la transmission est sécurisée si Eve ne peut obtenir aucune information sur m en connaissant c, soit $I(C; M) = 0$ où I est l'information mutuelle de Shannon [16], C et M sont les variables aléatoires correspondant aux messages c et m. Shannon a démontré que la seule méthode



(a) Modèle général. (b) Cryptage par masque jetable

FIG. 1.4 – Modèle cryptographique d'une transmission sécurisée.

de cryptage permettant d'aboutir à ce résultat est la technique du « masque jetable » (*one-time pad*) [17], consistant à utiliser une clé secrète aléatoire aussi longue que le message et à transmettre la somme modulo 2 de la clé et du message, voir figure 1.4(b). Il est donc impossible de garantir la sécurité inconditionnelle d'une transmission avec les méthodes de cryptographie standard, basées sur l'utilisation répétée d'une clé de quelques centaines de bits. Le résultat de Shannon est même beaucoup plus décourageant, car bien qu'il soit tout à fait envisageable d'utiliser un cryptage par masque jetable, il est nécessaire de

trouver un moyen efficace de distribuer des clés secrètes à Alice et Bob, et cette solution ne fait donc que transposer la difficulté.

Il pourrait donc sembler que la sécurisation inconditionnelle des transmissions soit un défi perdu d'avance, mais en réalité le modèle de la figure 1.4 est bien trop pessimiste dans la mesure où il ne tient pas compte des contraintes physiques des canaux de transmission. En pratique un canal de transmission présente des pertes et introduit du bruit, ce qui vient corrompre les messages transmis. Cette idée a conduit Wyner à introduire le modèle de transmission plus réaliste de la figure 1.5 (*wiretap channel* [11, 12, 18]), où Bob et Eve n'ont accès aux messages envoyés par Alice qu'au travers des canaux bruités. Les communications doivent alors satisfaire les critères d'intégrité (un message doit être décodé sans erreur par Bob) et de sécurité (Eve ne doit avoir aucune information sur le message transmis) apparemment contradictoires. Plus formellement en reprenant les notations de

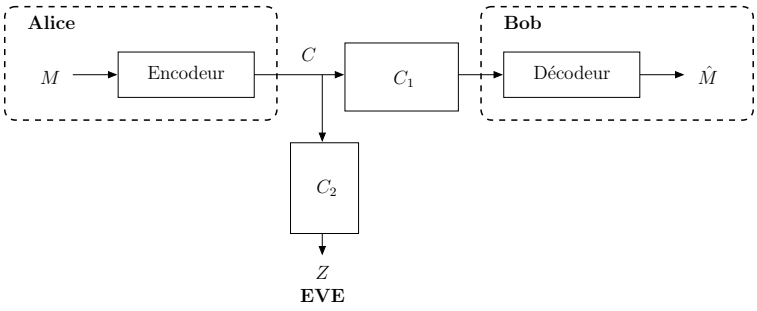


FIG. 1.5 – Modèle réaliste de transmission sécurisée.

la figure 1.5, ces exigences s'écrivent pour un message M de n bits :

$$\begin{aligned} \Pr\left[M \neq \hat{M}\right] &\rightarrow 0 \quad \text{quand} \quad n \rightarrow \infty, \\ \frac{H(M|Z)}{k} &\rightarrow 0 \quad \text{quand} \quad n \rightarrow \infty. \end{aligned}$$

Le résultat surprenant démontré par Wyner est qu'il est parfois possible de construire des codeurs et décodeurs satisfaisant simultanément ces deux critères. Il faut cependant noter qu'il n'existe pas de méthode permettant de construire des systèmes pratiques dans le cas le plus général, et des solutions ne sont connues que dans des cas relativement simples [19]. Par ailleurs le critère de sécurité précédent signifie uniquement que le taux auquel Eve accède à l'information est asymptotiquement nul, ce qui n'exclut pas qu'elle puisse de temps à autre décoder totalement un message.

1.1.3 Principe général des protocoles de cryptographie quantique

L'inconvénient majeur du modèle de Wyner et qu'il suppose non seulement une connaissance *a priori* des canaux de transmission entre Alice/Bob et Alice/Eve mais aussi que l'espion soit purement passif. L'idée à la base de la cryptographie quantique est de s'affranchir de ces hypothèses en supposant uniquement que les opérations d'Eve respectent les contraintes imposées par la mécanique quantique. Il est important de souligner que ces lois fondamentales limitent les actions d'Eve mais ne permettent pas pour autant de garantir

la transmission sécurisée de messages confidentiels entre Alice et Bob. La distribution quantique de clés n'assure que la distribution de clés secrètes (aléatoires), pouvant être utilisées par la suite en association avec des méthodes de cryptage symétrique standard telles qu'un masque jetable.

De nombreux protocoles de cryptographie quantique ont été proposés au cours des dernières années, et bien que chacun présente des caractéristiques particulières qu'il est nécessaire de prendre en compte pour analyser la sécurité de façon rigoureuse, tous suivent plus ou moins le même schéma. L'objectif de cette section est de décrire ces protocoles d'un point de vue très général, en faisant abstraction des propriétés quantiques mais en mettant l'accent sur les aspects algorithmiques classiques parfois négligés dans les articles. Les aspects physiques et expérimentaux seront abordés dans les sections 1.2 et 1.3 ainsi qu'aux chapitres 2 et 3.

Le schéma général d'un système de distribution de clé quantique est représenté figure 1.6. Alice et Bob disposent de deux canaux pour communiquer, un canal *quantique* sur lequel aucune restriction n'est imposée (en particulier Eve a toute liberté pour l'altérer) et un canal *classique* sans bruit et *authentifié* qu'Eve peut écouter mais non modifier. L'authentification et l'intégrité des messages est généralement assurée par des protocoles utilisant une clé secrète, ce qui suppose qu'Alice et Bob disposent au préalable d'une telle clé pour initialiser le protocole, et sacrifient une fraction des clés générées par la suite pour assurer l'authentification des messages futurs. La distinction faite entre les deux canaux

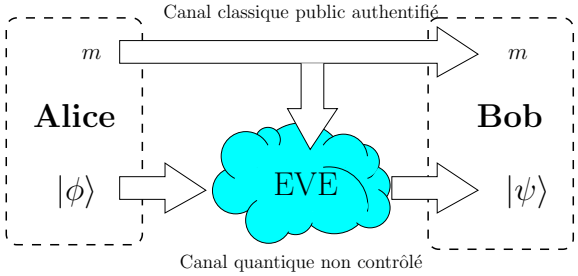


FIG. 1.6 – Schéma général d'un système de distribution de clé quantique.

tient uniquement au type d'information véhiculé, états quantiques dans le premier cas et bits d'information classiques dans le second, mais non à leur nature physique. La plupart des protocoles de distribution quantique de clé procèdent alors en 4 étapes :

Transmission quantique. Alice génère aléatoirement N réalisations $\{x_i\}_{i=1..N}$ d'une variable aléatoire $X \in \mathcal{X}$ qu'elle code sur une série d'états quantiques $\{|\phi\rangle_i\}_{i=1..N}$ choisis de manière adéquate, puis qu'elle envoie à Bob à travers le canal quantique. L'ensemble $\mathcal{X}$ (typiquement $\{0,1\}$ ou $\mathbb{R}$) ne sera précisé que lorsque les méthodes de codage seront abordées en détail dans les sections 1.2 et 1.3. De son côté Bob effectue des mesures sur les états $\{|\psi\rangle_i\}_{i=1..N}$ qu'il reçoit et obtient N réalisations $\{y_i\}_{i=1..N}$ d'une variable aléatoire $Y \in \mathcal{X}$ corrélée à X. Dans la mesure où aucune restriction n'est imposée au canal quantique, Eve peut elle aussi avoir accès à des données corrélées. Considérer qu'Eve obtient N réalisations d'une variable aléatoire $Z \in \mathcal{X}$ corrélée à X et Y reviendrait à limiter ses actions à des attaques *individuelles* sur chacun des états quantiques transmis, mais en toute généralité la mécanique quantique l'autorise à effectuer des attaques *cohérentes* sur

plusieurs états simultanément. Pour cette raison l'information d'Eve est représentée par la réalisation e_q d'une variable aléatoire globale $E_Q \in \mathcal{E}_\mathcal{Q}$.

Analyse de la transmission. En rendant public un sous-ensemble de $(N-n)$ symboles sélectionnés au hasard dans leurs données, Alice et Bob peuvent non seulement estimer la quantité d'information échangée restante, mais aussi évaluer indirectement la quantité maximum d'information interceptée par l'espion. Cette évaluation est possible grâce au caractère totalement aléatoire des messages échangés, qui permet d'estimer les statistiques des données non dévoilées à partir d'un échantillon représentatif, mais surtout grâce à la nature quantique des états transmis, qui limite la quantité d'information accessible simultanément à Alice, Eve et Bob. Cette situation est fondamentalement différente du scénario classique envisagé par Wyner où les canaux de Bob et d'Eve sont indépendants mais connus. Dans le cas présent aucune hypothèse n'est faite sur la manière dont Eve agit sur le canal quantique, mais le codage sur les états quantiques est réalisé de manière à ce que les manipulations d'Eve se répercutent dans les données reçues par Bob sous la forme d'une déviation statistique. Une analyse précise (et non triviale) des codages et mesures utilisés permet alors de relier la quantité d'information obtenue par Eve à des grandeurs statistiques simples telles qu'un taux d'erreur binaire (*Binary Error Rate*, BER) [1] ou une variance [20]. Si Alice et Bob estiment qu'Eve a intercepté au moins autant d'information qu'ils n'en ont échangée, le protocole est réinitialisé. Dans le cas contraire une clé secrète peut être générée à partir des symboles non dévoilés $\{x_i\}_{i=1..n}$ et $\{y_i\}_{i=1..n}$.

Réconciliation. Même en l'absence d'un espion, les contraintes environnementales s'exerçant sur le canal de transmission et les imperfections des systèmes expérimentaux sont sources d'erreurs, et les séquences de bits non dévoilés $\{x_i\}_{i=1..n}$ et $\{y_i\}_{i=1..n}$ ne sont donc jamais parfaitement identiques. Dans cette section nous considérerons que la séquence correcte de référence est celle d'Alice. La correction des erreurs (appelée réconciliation dans ce contexte) ne peut se faire qu'en échangeant des bits d'information supplémentaires sur le canal public. Dans la mesure où Eve a accès à cette information, il est nécessaire de limiter ces échanges au maximum, et idéalement d'atteindre la limite fixée par la théorie de l'information : $H(X^n|Y^n)$ bits où H est l'entropie de Shannon [21]. Les taux d'erreur typiques sont de l'ordre de 10^{-1}, et sont trop élevés pour appliquer les codes correcteurs standards plutôt conçus pour travailler avec des taux de l'ordre de 10^{-3} [22]. Plusieurs algorithmes spécifiques ont donc été proposés pour corriger efficacement ces forts taux d'erreur [23, 24]. Ces méthodes appelées protocoles de correction binaires (*Binary Correction Protocol*, BCP) sont généralement basées sur de simples calculs de parités et des échanges interactifs entre Alice et Bob. A titre d'exemple, les deux BCP les plus couramment utilisés sont présentés ci-après. En dépit de leur simplicité, la quantité d'information I_{rec} dévoilée par ces protocoles approche la limite théorique $H(X^n|Y^n)$.

Exemple 1.1.1 (CASCADE)**:** Le protocole de correction binaire CASCADE [23] permet de corriger efficacement les erreurs dans une longue séquence binaire ($\mathcal{X} = \mathcal{Y} = \{0, 1\}$) en procédant par itérations successives. A chaque itération i, Alice et Bob divisent leurs séquences $\{x_m\}_{m=1..n}$ et $\{y_m\}_{m=1..n}$ de n bits en blocs de taille k_i. Chaque bloc j ($1 \leq j \leq \left\lceil \frac{n}{k_i} \right\rceil$ où $\lceil \bullet \rceil$ est la partie entière

supérieure) est formé des bits dont l'index appartient à l'ensemble

$$K_j^{(i)} = \left\{ m : 1 \leq m \leq n \text{ et } (j-1)k_i + 1 \leq \pi^{(i)}(m) \leq jk_i \right\},$$

où $\pi^{(i)}$ est une permutation de $\{0,1\}^n$ choisie au préalable. Alice et Bob calculent alors les parités de chacun de leurs blocs

$$a_j^{(i)} = \bigoplus_{m \in K_j^{(i)}} x_m \qquad b_j^{(i)} = \bigoplus_{m \in K_j^{(i)}} y_m$$

et les comparent publiquement. Quand un bloc contient un nombre pair d'erreurs les parités s'accordent ($a_j^{(i)} = b_j^{(i)}$) et aucune correction n'est effectuée. En revanche, lorsqu'un bloc contient un nombre impair d'erreurs les parités divergent ($a_j^{(i)} \neq b_j^{(i)}$) et Alice et Bob corrigent alors un bit erroné y_l du bloc en procédant par bissection : en divisant le bloc de taille k_i par deux, et en échangeant les parités de chaque sous-bloc, Alice et Bob peuvent isoler y_l dans un des deux sous-blocs de taille $k_i/2$, et réitérer la même opération sur ce sous-bloc. La bissection s'arrête lorsque la position de y_l est déterminée, auquel cas il suffit à Bob d'inverser sa valeur. Les parités de l'ensemble des blocs

$$\mathcal{K}(l) = \left\{ K_j^{(m)} : l \in K_j^{(m)}, 1 \leq m < i, 1 \leq j \leq \left\lceil \frac{n}{k_m} \right\rceil \right\}$$

contenant y_l aux itérations précédentes deviennent alors incorrectes. L'ensemble total $\mathcal{K}$ des blocs contenant un nombre impair d'erreur est initialisé à $\mathcal{K} = \mathcal{K}(l)$. En procédant de nouveau par bissection, Alice et Bob corrigent une erreur $y_{l'}$ dans le plus petit bloc de $\mathcal{K}$, puis déterminent l'ensemble des blocs incorrects $\mathcal{K}(l')$ contenant $y_{l'}$ aux itérations précédentes, et mettent à jour l'ensemble total des blocs incorrects

$$\mathcal{K} \leftarrow (\mathcal{K} \cup \mathcal{K}(l')) \setminus (\mathcal{K} \cap \mathcal{K}(l')).$$

Cette opération est alors répétée tant que $\mathcal{K} \neq \varnothing$. L'itération i se termine lorsque tous les blocs contiennent un nombre pair d'erreurs. Les performances de CASCADE dépendent beaucoup du choix des tailles de blocs k_i à chaque itération, mais en optimisant ces tailles en fonction du taux d'erreur binaire initial p, quatre itérations suffisent généralement pour corriger toutes les erreurs en excédant d'environ 10% la limite optimale $nh(p)$, où $h(p) = -p\log_2 p - (1-p)\log_2(1-p)$.

Exemple 1.1.2 (WINNOW)**:** Le protocole WINNOW [25] fonctionne sur le même principe que CASCADE, et corrige les erreurs en plusieurs passes successives. A chaque itération i Alice et Bob divisent leurs séquences $\{x_m\}_{m=1..n}$ et $\{y_m\}_{m=1..n}$ en blocs de taille $N_i = 2^{m_i} - 1$ ($m_i \in \mathbb{N}$) et échangent les parités correspondantes. Comme précédemment une permutation est appliquée entre chaque itération. Quand les parités s'accordent un bit est éliminé du bloc, lorsqu'elles divergent Alice et Bob corrigent une erreur en échangeant m_i bits

calculé à partir d'un code de Hamming [22] puis éliminent $m_i + 1$ bits du bloc. L'élimination à chaque itération d'autant de bits qu'il n'a été dévoilé est appelée « maintien de confidentialité ». Cette opération évite à Alice et Bob de calculer par la suite des parités sur des bits connus d'Eve et réduit le nombre de bits à traiter aux itérations suivantes. Par ailleurs la correction d'erreur ne requiert que 2 communications unidirectionnelles (parité du bloc d'Alice et syndrome si nécessaire), contrairement à la bisection interactive utilisée par CASCADE. Le choix de la taille des blocs est cependant un paramètre encore plus crucial pour le protocole WINNOW, car les codes de Hamming peuvent introduire des erreurs supplémentaires lorsque les blocs contiennent plus de deux bits erronés. Les performances de WINNOW sont similaires à celles de CASCADE en terme de correction d'erreurs, mais en pratique toutes les communications entre Alice et Bob doivent être authentifiées et la réduction du nombre de bits à communiquer apportée par WINNOW présente un réel avantage.

Nous considérerons par la suite qu'Alice et Bob n'utilisent pas de maintien de confidentialité et qu'ils disposent à l'issue de la réconciliation d'une même séquence aléatoire binaire $\{s_i\}_{i=1..n_{rec}}$ composée de n_{rec} bits. Le nombre de bits dévoilés lors de la réconciliation est $nH(X|Y)(1+\epsilon_{rec})$, où ϵ_{rec} est le pourcentage de bits dévoilés en surplus de la limite théorique.

Amplification de confidentialité. La dernière étape des protocoles de distribution quantique de clé est la génération proprement dite de la clé secrète à partir de la séquence commune à Alice et Bob. Cette étape est généralement omise dans la plupart des articles expérimentaux car l'extraction de la clé se fait à l'aide d'un algorithme déterministe dépendant uniquement de l'information estimée d'Eve. Néanmoins, puisque c'est l'existence d'une méthode pratique qui a donné tout son intérêt à la distribution quantique de clé, nous rappellerons ici les principaux résultats théoriques associés. Le principe de l'amplification de confidentialité est d'extraire une fraction $\{k_i\}_{i=1..k}$ de la séquence initiale $\{s_i\}_{i=1..n_{rec}}$ à l'aide d'une fonction déterministe, et de faire en sorte que l'incertitude d'Eve sur $\{k_i\}_{i=1..k}$ soit maximale. En d'autres termes, si K est la variable aléatoire représentant la séquence finale de k bits et e est l'information totale d'Eve, l'amplification de confidentialité doit « uniformiser » K et garantir $H(K|E=e) \approx k$. En pratique, les familles universelle$_2$ de fonctions de hachage définies ci-dessous peuvent remplir ce rôle.

Une famille $\mathcal{G}$ de fonctions $G : \mathcal{A} \to \mathcal{B}$ est universelle$_2$ (universelle pour alléger les notations) si

$$\forall\, x_1, x_2 \in \mathcal{A} \qquad x_1 \neq x_2 \Rightarrow \Pr\left[G(x_1) = G(x_2)\right] \leq \frac{1}{|\mathcal{B}|},$$

où $|\mathcal{B}|$ est le cardinal de l'ensemble $\mathcal{B}$ et G est la variable aléatoire représentant le choix d'une fonction $g \in \mathcal{G}$ selon une distribution uniforme.

Exemple 1.1.3 ([26])**:** En identifiant $\{0,1\}^n$ à $\mathrm{GF}(2)^n$, où $\mathrm{GF}(2)$ est le corps de Galois contenant deux éléments, il est possible d'associer à toute matrice binaire $M \in \{0,1\}^{k\times n}$ une fonction

$$h_M : \{0,1\}^n \to \{0,1\}^k : x \mapsto xM^T.$$

La famille de fonctions de hachage $\mathcal{H} = \left\{h_M : M \in \{0,1\}^{n\times k}\right\}$ est universelle.

Exemple 1.1.4 ([27])**:** En identifiant $\{0,1\}^n$ à $\mathrm{GF}(2^n)$ il est possible d'associer à toute élément $c \in \mathrm{GF}(2^n)$ une fonction

$$h_c : \mathrm{GF}(2^n) \to \{0,1\}^k : x \mapsto k \text{ bits du produit } cx.$$

La famille de fonctions de hachage $\mathcal{H} = \{h_c : c \in \mathrm{GF}(2^n)\}$ est universelle.

L'amplification de confidentialité avec de telles fonctions repose alors sur le résultat suivant adapté de [28]. Soient $S \in \mathcal{S}$ une variable aléatoire représentant les données communes à Alice et Bob, e une réalisation particulière de la variable aléatoire $E \in \mathcal{E}$ décrivant toute l'information accessible à Eve. Soit G une variable aléatoire représentant une fonction de hachage choisie aléatoirement (et selon une distribution uniforme) parmi une famille universelle$_2$ de fonctions de hachage $\mathcal{S} \to \{0,1\}^k$. Si une borne inférieure r_{min} de l'entropie de Rényi d'ordre deux $R(S|E=e)$ est connue, et si $K = G(S)$ est retenu comme clé, alors

$$H(K|G, E=e) \geq k - \frac{2^{k-r_{min}}}{\ln 2}.$$

Plusieurs points méritent d'être soulignés. Tout d'abord l'incertitude sur S connaissant e doit être bornée à l'aide de l'entropie de Rényi R et non pas l'entropie de Shannon H. En effet l'entropie de Shannon ne permet pas de distinguer les situations où Eve récupère systématiquement une fraction de l'information à chaque transmission, et celle où elle récupère toute l'information sur une fraction des transmissions [29]. L'entropie de Rényi permet en revanche de pénaliser cette deuxième situation, et est donc plus adaptée. Le résultat porte ensuite sur la quantité $H(K|G, E=e)$ qui est une moyenne sur l'ensemble des fonctions de la famille universelle $\mathcal{G}$. Il est possible que pour un choix particulier de $g \in \mathcal{G}$, la quantité $H(K|G=g, E=e)$ soit significativement différente de k même si $k \ll r_{min}$, mais une telle situation n'apparaît qu'avec une probabilité négligeable.

Afin d'appliquer ce résultat à la distribution quantique de clé, il faut prendre en compte l'information totale détenue par Eve, composée non seulement de l'information $E_Q \in \mathcal{E}_Q$ interceptée lors la transmission quantique, mais aussi des messages $M \in \mathcal{M}$ obtenus lors de la réconciliation sur le canal public. L'étape d'analyse de la transmission ne fournit qu'une limite inférieure de $R(S|E_Q = e_q)$ et non pas de $R(S|E=e) = R(S|E_q = e_q, M=m)$, mais comme démontré dans [29, Corollaire 5.3],

$$R(S|E_Q = e_q, M=m) \geq R(S|E_Q = e_q) - \log_2|\mathcal{M}| - 2s - 2$$

avec une probabilité $1 - 2^{-s}$. La quantité $\log_2|\mathcal{M}|$ est simplement le nombre de bits communiqués durant la réconciliation. Ainsi le nombre minimum de bits r à retrancher de n_{rec} est

$$\boxed{r = n_{rec} - r_{min} + nH(X|Y)(1+\epsilon_{rec}) + 2s + 2,}$$

où s est un paramètre de sécurité additionnel, et $\epsilon_{rec} > 0$ est le pourcentage de bits dévoilés lors de la réconciliation en surplus de la limite idéale. Alice choisit en général une taille de clé $k = n_{rec} - r - r_0$ légèrement inférieure et sélectionne aléatoirement et uniformément une fonction de hachage $g : \{0,1\}^{n_{rec}} \to \{0,1\}^k$ au sein d'une famille

universelle de fonctions de hachage $\mathcal{G}$ publiquement connue. Les paramètres g et k sont alors transmis à Bob via le canal public, et Alice et Bob génèrent finalement leur clé commune $\{k_i\}_{i=1..k} = g(\{s_i\}_{i=1..n_{rec}})$. En reprenant les notations précédentes, l'incertitude d'Eve est alors

$$\boxed{H(K|G, E = e) \geq k - \frac{2^{-r_0}}{\ln 2}.}$$

En pratique il suffit donc de choisir s et r_0 de l'ordre de la dizaine de bits pour obtenir une clé secrète.

Conclusion. La figure 1.7 résume de façon imagée l'évolution de l'information d'Alice, Bob et Eve au cours des différentes étapes d'un protocole de cryptographie quantique. La

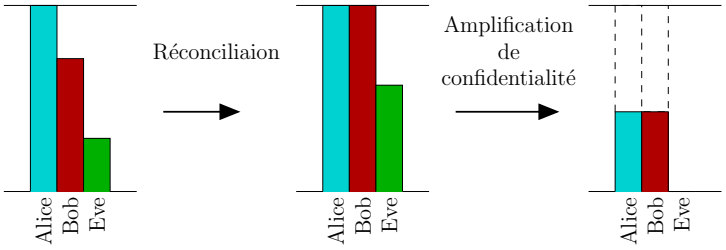


FIG. 1.7 – Evolution de l'information d'Alice, Bob et Eve au cours d'une distribution quantique de clé [30].

transmission quantique et l'analyse associée permettent tout d'abord à Alice d'envoyer de l'information à Bob, et ensuite de garantir qu'Eve n'en a pas reçu autant. Après réconciliation de leurs données Alice et Bob possèdent la même quantité d'information, et l'amplification de confidentialité leur permet finalement de ne conserver que la fraction inconnue d'Eve. Encore une fois, ni Alice ni Bob ne peuvent prévoir à l'avance quelle sera la séquence de bits retenue comme clé à l'issue du protocole. La clé extraite dépend de certains choix aléatoires d'Alice (choix d'une fonction universelle), et de l'estimation de l'information obtenue par Eve une fois la transmission quantique effectuée.

1.2 Cryptographie quantique par photons uniques

Cette section présente un état de l'art des différents codages basés sur des qubits pouvant être utilisés lors de la phase de transmission quantique, ainsi que des systèmes expérimentaux réalisés. Les sources sont ici supposées être des sources idéales à photons uniques, ou leur approximation par des sources lasers émettant des états cohérents fortement atténués.

1.2.1 Protocoles de cryptographie quantique

Protocole BB84

Le protocole BB84 [1] proposé par Gilles Bennett et Charles Brassard a marqué le début de la cryptographie quantique. Le principe relativement simple de ce protocole est

d'utiliser 4 qubits formant deux bases incompatibles d'un espace de Hilbert complexe de dimension de 2 pour coder l'information, par exemple :

Bit codé	0	1
Base 1	$\|0\rangle$	$\|1\rangle$
Base 2	$\|+\rangle = \frac{\|0\rangle + \|1\rangle}{\sqrt{2}}$	$\|-\rangle = \frac{\|0\rangle - \|1\rangle}{\sqrt{2}}$

où les états $|0\rangle$ et $|1\rangle$ sont orthogonaux par hypothèse. On vérifie aisément l'orthogonalité de la base 2 ($|\langle +|-\rangle| = 0$) et l'incompatibilité des deux bases ($|\langle +|0\rangle|^2 = |\langle +|1\rangle|^2 = |\langle -|0\rangle|^2 = |\langle -|1\rangle|^2 = 0.5$).

Alice génère tout d'abord deux séquences binaires aléatoires indépendantes $\{x_i\}_{i=1..N} \in \{0,1\}^N$ et $\{a_i\}_{i=1..N} \in \{0,1\}^N$. En fonction de la valeur de a_i, chaque bit x_i est ensuite codé dans une des deux bases de la manière suivante :

- $a_i = 0$: codage dans la base $\{|0\rangle, |1\rangle\}$: $x_i \rightarrow |x_i\rangle$
- $a_i = 1$: codage dans la base $\{|+\rangle, |-\rangle\}$: $x_i \rightarrow \frac{|0\rangle + (-1)^{x_i}|1\rangle}{\sqrt{2}}$.

La matrice de densité des états transmis par Alice est alors

$$\rho = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \frac{1}{2}(|+\rangle\langle +| + |-\rangle\langle -|),$$

ce qui signifie qu'il est impossible de déterminer la base utilisée par Alice pour coder ses bits.

De son côté Bob génère lui aussi une séquence binaire aléatoire $\{b_i\}_{i=1..N} \in \{0,1\}^N$. A la réception de chacun des qubits et en fonction de la valeur de b_i, il choisit alors de projeter l'état reçu dans une des deux bases :

- $b_i = 0$: projection dans la base $\{|0\rangle, |1\rangle\}$
- $b_i = 1$: projection dans la base $\{|+\rangle, |-\rangle\}$

Lorsque le codage d'Alice est incompatible avec la mesure de Bob ($a_i \neq b_i$) le résultat de la projection est totalement aléatoire et ne fournit aucune information sur la valeur du bit transmis x_i ; dans le cas contraire ($a_i = b_i$) x_i est parfaitement déterminé.

Une fois les N bits reçus, Alice rend publiques les N bases de codages utilisées en révélant la séquence $\{a_i\}_{i=1..N}$. Cette opération ne fournit aucune information sur la valeur des bits transmis, mais permet à Bob d'éliminer ses mesures incompatibles ($a_i \neq b_i$). En moyenne 50% des bits transmis par Alice sont ainsi mis de côté, mais idéalement, si la transmission n'est pas perturbée, les mesures de Bob déterminent sans ambiguïté les 50% des bits restants.

L'analyse de la transmission repose principalement sur le théorème de non clonage [31], qui interdit à Eve de dupliquer avec une fidélité maximale les états qu'elle intercepte. Afin d'illustrer simplement la manière dont le BB84 exploite cette propriété, nous considérerons ici qu'Eve n'effectue qu'une attaque interception/émission (*intercept/resend*). Cette attaque consiste à :

1. intercepter une fraction η des qubits transmis par Alice,
2. projeter les états individuellement dans la base $\{|0\rangle, |1\rangle\}$ (il n'est pas nécessaire d'alterner entre les deux bases car le codage d'Alice les exploite de façon symétrique),
3. renvoyer à Bob les qubits correspondants aux résultats des mesures.

Dans 50% des interceptions, la base d'Eve est compatible avec le codage d'Alice, et lui permet de déterminer le qubit envoyé sans ambiguïté. Le qubit envoyé à Bob est donc correct et Eve ne révèle pas sa présence. En revanche lors des interceptions restantes, la base d'Eve est incompatible ; le résultat de sa mesure est alors totalement aléatoire et elle n'obtient donc aucune information sur le bit d'Alice. De plus comme le qubit réémis n'est plus dans la base utilisée par Alice, Bob obtient un résultat erroné une fois sur deux lorsqu'il utilise une base compatible avec le codage d'Alice. Cette attaque permet donc à Eve d'obtenir une fraction $\eta/2$ de l'information transmise par Alice, mais augmente le taux d'erreur de Bob de $\eta/4$ qui n'obtient donc plus que $1 - h(\eta/4)$ bits d'information par symbole transmis. Afin de distinguer clairement ce taux d'erreur d'un taux d'erreur classique, ce pourcentage d'erreur est appelé taux d'erreur binaire quantique (*Quantum Bit Error Rate*, QBER). Il suffit donc à Alice et Bob de sacrifier une partie de leurs données pour évaluer leur QBER et ainsi déduire l'information d'Eve.

Eve peut bien sûr mettre en œuvre des attaques bien plus efficaces que celle décrite précédemment, mais même son attaque optimale introduit une perturbation statistique augmentant le QBER d'Alice et Bob [32].

Protocole EPR

Le protocole EPR proposé par Ekert [2] est une variation du BB84 basée sur l'utilisation du paradoxe EPR. Contrairement au BB84 où Bob mesure des états préparés par Alice, le protocole EPR suppose qu'Alice et Bob partagent N paires de qubits idéalement dans un état de Bell

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

Ces derniers effectuent alors aléatoirement et simultanément l'une des 3 mesures suivantes sur leurs qubits respectifs

Alice	**Bob**
$A_1 = Z_1$	$B_1 = Z_2$
$A_2 = X_1$	$B_2 = \dfrac{Z_2 + X_2}{\sqrt{2}}$
$A_3 = \dfrac{Z_1 + X_1}{\sqrt{2}}$	$B_3 = \dfrac{Z_2 - X_2}{\sqrt{2}}$

où $Z_i = |0\rangle\langle 0| - |1\rangle\langle 1|$ et $X_i = |0\rangle\langle 1| + |1\rangle\langle 0|$ ($i \in \{1, 2\}$). Alice et Bob révèlent ensuite les mesures effectuées et séparent leurs données en deux groupes distincts. Le premier groupe contient les résultats obtenus lorsque des opérations identiques ont été appliquées et sont en théorie parfaitement corrélés :

$$\langle\beta_{00}|A_1 B_1|\beta_{00}\rangle = \langle\beta_{00}|A_3 B_2|\beta_{00}\rangle = 1.$$

Le second groupe contient les résultats obtenus lorsque des mesures différentes ont été effectuées, et permettent de vérifier une violation des inégalités de Bell si les paires de qubits étaient effectivement dans l'état $|\beta_{00}\rangle$:

$$\langle\beta_{00}|A_1 B_2 + A_1 B_3 + A_2 B_1 - A_2 B_3|\beta_{00}\rangle = 2\sqrt{2}.$$

La source des états de Bell n'est pas nécessairement sous le contrôle d'Alice et Bob, mais puisqu'Eve ne connaît pas à l'avance les mesures effectuées par Alice et Bob, toute

intervention perturbe les états et se traduit par une moindre violation des inégalités de Bell. En fonction du résultat de leur test, Alice et Bob peuvent là encore mettre en œuvre les étapes de réconciliation et d'amplification de confidentialité pour générer une clé secrète.

Bien que ce protocole exploite de manière astucieuse le paradoxe EPR, la violation des inégalités de Bell n'est en réalité pas nécessaire pour garantir la sécurité du système [33]. En effet, si Alice et Bob effectuent aléatoirement et simultanément une des deux mesures suivantes

Alice	**Bob**
Z_1	Z_2
X_1	X_2

il n'est pas difficile de vérifier que le protocole est strictement équivalent au BB84. Il est intéressant d'un point de vue expérimental que le protocole BB84 ne requiert pas explicitement l'utilisation d'états intriqués difficiles à générer efficacement ; néanmoins plusieurs preuves de sécurité inconditionnelle exploitent la formulation équivalente du BB84 basée sur des paires EPR [32].

Protocole B92

Puisque c'est l'incompatibilité de deux bases qui garantit la sécurité du BB84, il est naturel de se demander si l'utilisation de 4 états est absolument nécessaire. Le protocole B92 [34] proposé par Charles Bennett est un protocole particulièrement simple n'utilisant que deux états $|u_0\rangle$ et $|u_1\rangle$ non orthogonaux.

Alice génère tout d'abord une séquence aléatoire binaire $\{x_i\}_{i=1..N} \in \{0,1\}^N$, puis émet une séquence d'états $\{|\psi_i\rangle\}_{i=1..N}$ choisis de la façon suivante :

$$|\psi_i\rangle = \begin{cases} |u_0\rangle = \beta|0\rangle + \alpha|1\rangle & \text{si } x_i = 0 \\ |u_1\rangle = \beta|0\rangle - \alpha|1\rangle & \text{si } x_i = 1 \end{cases} \quad \text{avec} \quad 0 < \alpha < 1/\sqrt{2} \text{ et } \beta = \sqrt{1-\alpha^2}$$

A la réception de chaque état, Bob effectue aléatoirement une projection sur la base $\{|u_0\rangle, |\overline{u}_0\rangle\}$ ou $\{|u_1\rangle, |\overline{u}_1\rangle\}$ ($\langle\overline{u}_i|u_i\rangle = 0$ pour $i \in \{0,1\}$). Cette mesure lui permet en moyenne de déterminer sans ambiguïté une fraction β^2 des états transmis par Alice, et est caractérisée par la POVM (*Positive Operator Valued Measure*) $\{F_0, F_1, F_?\}$ où

$$F_0 = |\overline{u}_1\rangle\langle\overline{u}_1|/2, \quad F_1 = |\overline{u}_0\rangle\langle\overline{u}_0|/2, \quad F_? = 1 - F_0 - F_1.$$

Une fois les N mesures terminées, Bob révèle publiquement les instances auxquelles il a obtenu un résultat concluant[3] (sans pour autant révéler la projection qu'il a effectuée) et élimine les autres instances. Si la transmission n'a pas été perturbée, les données restantes d'Alice et Bob sont parfaitement corrélées. Comme dans le cas du BB84, il est alors possible d'estimer l'information interceptée par Eve à partir du QBER, puis de générer une clé secrète après réconciliation et amplification de confidentialité. Si Bob utilise des détecteurs de photons réalistes ne lui permettant que de distinguer l'état vide des états multiphotons, la sécurité inconditionnelle de ce protocole ne peut être démontrée que

[3]Le fait que la POVM précédente ne soit pas optimale réduit inutilement le débit des clés de Bob mais ne modifie pas la sécurité du protocole.

dans le cas où le canal est sans pertes et sans bruit [35, 36]. En effet, en présence de pertes, Eve peut très bien effectuer la même POVM que Bob et ne retransmettre un qubit que lorsqu'elle obtient un résultat concluant. En revanche si Bob dispose d'un détecteur lui permettant de différencier les états à photon unique de l'état vide et des états multiphotons, il est alors possible de garantir la sécurité inconditionnelle, même en présence de bruit et pertes sur le canal [37].

Pour des raisons pratiques, le B92 est généralement mis en œuvre avec des états cohérents fortement atténués plutôt qu'avec des photons uniques. Dans ce cas la POVM mentionnée précédemment peut être réalisée de manière très simple comme représenté figure 1.8. Alice code ici sa séquence aléatoire sur les états non orthogonaux $|u_0\rangle =$

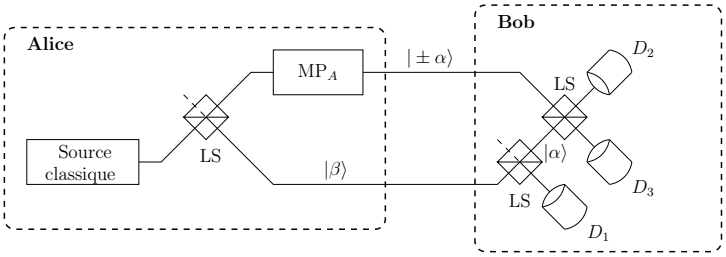


FIG. 1.8 – Dispositif expérimental du protocole B92

$|\alpha\rangle$ et $|u_1\rangle = |-\alpha\rangle$. Ceux-ci sont obtenus en envoyant une impulsion laser d'intensité classique $|\beta\rangle$ ($\beta \gg \alpha$) sur une lame séparatrice déséquilibrée et en déphasant l'impulsion atténuée de façon appropriée avec le modulateur de phase $\mathrm{MP_A}$. Cette impulsion qualifiée de « référence forte » tient lieu de référence de phase et est elle aussi transmise à Bob. Au récepteur, Bob sépare la référence en deux impulsions à l'aide d'une lame séparatrice de réflectivité α/β, et fait interférer l'impulsion atténuée $|\alpha\rangle$ avec l'état transmis par Alice. Lorsqu'un seul des détecteurs $\mathrm{D_2}$ ou $\mathrm{D_3}$ se déclenche, le signal d'Alice est alors déterminé sans ambiguïté.

Bien que Bennett n'ait introduit ce schéma expérimental que pour des raisons pratiques, l'utilisation d'une référence permet cependant de pallier aux inconvénients liés à l'utilisation de seulement deux états. En effet, lorsque Bob vérifie systématiquement la présence de la référence de phase à l'aide du détecteur $\mathrm{D_1}$, Eve ne peut plus bloquer les impulsions pour lesquelles elle n'obtient pas de résultat concluant sans introduire d'erreur dans les mesures de Bob. La sécurité inconditionnelle du B92 avec référence forte a été démontrée dans le cas de détecteurs de photons réalistes pour un dispositif expérimental légèrement différent [38] (Bob dispose d'un oscillateur local propre qu'il verrouille à la phase de la référence forte), et dans le cas de détecteurs permettant de discriminer les états à photon unique de l'état vide et des états multiphotons [39].

Autres protocoles

De nombreuses variations aux protocoles précédents ont été proposées, et une liste de références très complète est disponible dans l'article de revue [30]. Il est cependant intéressant de mentionner certaines extensions des protocoles précédents :

- **Protocole à 6 états**. Le protocole BB84 peut être modifié pour utiliser trois bases incompatibles au lieu de deux [40]

Bit codé	0	1
Base 1	$\|+;1\rangle = \|0\rangle$	$\|-;1\rangle = \|1\rangle$
Base 2	$\|+;2\rangle = \frac{\|0\rangle + \|1\rangle}{\sqrt{2}}$	$\|-;2\rangle = \frac{\|0\rangle - \|1\rangle}{\sqrt{2}}$
Base 3	$\|+;3\rangle = \frac{\|0\rangle + i\|1\rangle}{\sqrt{2}}$	$\|-;3\rangle = \frac{\|0\rangle - i\|1\rangle}{\sqrt{2}}$

La probabilité qu'Alice et Bob utilisent la même base est alors seulement de 1/3, mais ce protocole est plus robuste aux attaques d'Eve que le BB84 à 4 états. En particulier une attaque interception/réémission introduit un QBER de 33% au lieu de 25%.

– **Protocole 4+2**. Ce protocole proposé par Huttner et ses collaborateurs [41] est une extension du protocole B92 avec référence forte. Comme dans le cas du BB84, Alice encode cette fois-ci aléatoirement ses données de deux manières, sur les états non orthogonaux $|\pm\alpha\rangle$ ou $|\pm i\alpha\rangle$. En introduisant un déphasage approprié au récepteur, Bob peut lui aussi alterner entre deux POVM et n'obtient de résultats concluants que si sa POVM est compatible avec le codage d'Alice. Comme décrit dans le chapitre 2, ce protocole peut être mis en œuvre de façon astucieuse en utilisant des bandes latérales de modulation [42].

– **Protocole par codage temporel**. L'idée originale de ce protocole [43, 44] est de transmettre des impulsions à 1 photon présentant une incertitude temps-fréquence minimale, et de coder l'information sur des délais de durée inférieure à la durée des impulsions (figure 1.9). Le décodage s'effectue en mesurant les temps d'arrivée

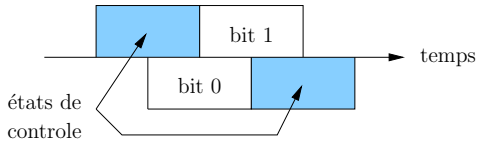


FIG. 1.9 – Méthode de codage temporel.

des photons et en évaluant ces délais. A cause du recouvrement des impulsions, cette mesure ne peut pas être réalisée sans ambiguïté. Comme dans le cas du BB84 il est alors possible d'exploiter cette incertitude pour assurer la sécurité du protocole. Plus précisément les interventions d'un espion modifient nécessairement la durée de cohérence des impulsions, et peuvent donc être détectées si Bob effectue des contrôles de cohérence (statistiques) sur un ensemble d'impulsions sélectionnées au hasard. Cette méthode de codage est particulièrement attractive d'un point de vue expérimental car les mesures de Bob peuvent être réalisées sans aucun composant optique actif, et les transmissions peuvent potentiellement atteindre de très hauts débits. Plusieurs protocoles basés sur les mêmes idées ont été proposés par la suite [45].

1.2.2 Mises en œuvre expérimentales du protocole BB84

Codage en polarisation

Le protocole BB84 se met œuvre naturellement avec un codage en polarisation car la description quantique de la polarisation d'un photon unique se fait dans un espace

de Hilbert de dimension 2. Les états de polarisation horizontale ($|\rightarrow\rangle$), verticale ($|\uparrow\rangle$), +45 ($|\nearrow\rangle$) et -45 ($|\searrow\rangle$) forment ainsi deux bases incompatibles pouvant être utilisées pour coder l'information d'Alice :

Bit codé	0	1
Base 1	$\|\rightarrow\rangle$	$\|\uparrow\rangle$,
Base 2	$\|\nearrow\rangle = \frac{\|\rightarrow\rangle + \|\uparrow\rangle}{\sqrt{2}}$	$\|\searrow\rangle = \frac{\|\rightarrow\rangle - \|\uparrow\rangle}{\sqrt{2}}$.

En pratique ces 4 états s'obtiennent soit en envoyant les états émis par une source unique à travers un modulateur électro-optique de polarisation [3, 46], soit en multiplexant les sorties de 4 sources différentes émettant chacune un état de polarisation bien défini [47]. La seconde solution est souvent retenue lorsque les états émis sont des états cohérents fortement atténués, auquel cas il est relativement aisé et peu coûteux d'utiliser plusieurs sources.

Un exemple de système expérimental utilisant le codage en polarisation est représenté figure 1.10. Alice utilise ici un modulateur électro-optique de polarisation (MEO-P). A

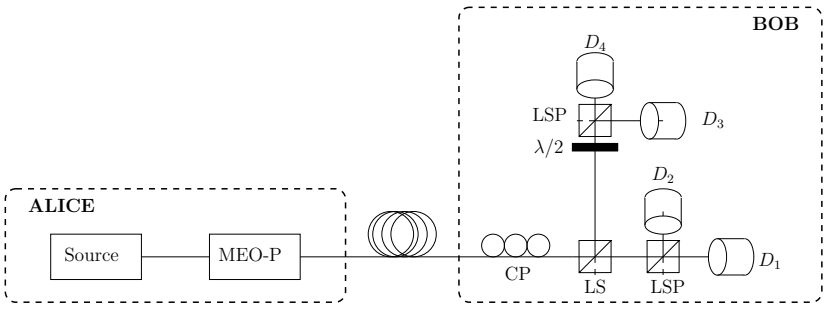


FIG. 1.10 – BB84 avec codage en polarisation.

cause des contraintes environnementales s'exerçant sur un canal quantique (variations de température et de pression, etc.), la polarisation des états envoyés par Alice n'est généralement pas maintenue lors de la propagation, et avant de pouvoir décoder Bob doit donc compenser de façon active ces rotations de polarisation avec un contrôleur de polarisation (CP). Une fois la polarisation corrigée, Bob effectue le décodage avec des composants purement passifs. Le choix de la base de mesure se fait à l'aide d'une lame séparatrice (LS) équilibrée qui dirige aléatoirement l'état reçu vers une des deux mesures possibles. Dans le premier cas, une lame séparatrice de polarisation (LSP) effectue la projection sur l'un des états de base $\{|\rightarrow\rangle, |\uparrow\rangle\}$, puis les compteurs de photons D_1 et D_2 permettent de déterminer le résultat de cette mesure. La projection sur les états de base $\{|\nearrow\rangle, |\searrow\rangle\}$ s'effectue en faisant tourner la polarisation de 45 avec une lame demi-onde ($\lambda/2$), puis en utilisant un dispositif similaire.

Le codage en polarisation n'est pas bien adapté à la propagation sur fibre optique, car la dispersion de polarisation (*Polarization Mode Dispersion*, PMD) et les pertes dépendantes de la polarisation (*Polarization Dependent Loss*, PDL) induites par la biréfringence de la fibre compliquent le décodage. Les systèmes les plus aboutis fonctionnant sur fibre optique utilisent d'ailleurs plutôt le codage en phase présenté dans la section suivante. En revanche le codage en polarisation est tout à fait adapté à la propagation en espace libre, et peut très bien être envisagé pour des communications Terre-satellite.

Le tableau 1.1 présente les distances de transmission et les débits obtenus avec les principaux systèmes développés. Des distributions quantiques de clés utilisant différents types de sources ont été réalisées aussi bien sur fibre optique (†) qu'en espace libre (∗). Les systèmes basés sur des sources laser atténuées bénéficient de toute la technologie

Source	Référence	λ (nm)	d	Débit de clé
Impulsions atténuées	Gordon (2005) [48]	850	6.55 km (†)	20000 bits/s
	Kurtsiefer (2002) [49]	?	23.4 km (∗)	100 bits/s
Photon unique	Beveratos (2002) [46]	≈ 690	50 m (∗)	7700 bits/s
	Alléaume (2004) [50]	≈ 690	30 m (∗)	16000 bits/s
Photons intriqués	Poppe (2004) [51]	810	1.45 km (†)	76 bits/s
	Peng (2005) [52]	702	10.5 km (∗)	10 bits/s
	Marcikic (2006) [53]	810	1.5 km (∗)	850 bits/s

TAB. 1.1 – Performances des principaux systèmes utilisant un codage en polarisation

élaborée pour les télécommunications optiques, et offrent aujourd'hui des performances bien supérieures aux systèmes basés sur des sources de photons uniques ou de photons intriqués.

Codage en phase

La mise en œuvre du protocole BB84 sur fibre optique utilise très souvent un codage en phase bien plus robuste que le codage en polarisation décrit précédemment. Le principe de ce codage est basé sur l'utilisation d'interférences à un photon et est illustré sur la figure 1.11. Le dispositif de transmission de clé s'apparente alors globalement à un interféromètre de Mach-Zehnder équilibré dont Alice et Bob ne contrôlent chacun qu'une moitié. Plus précisément, l'état envoyé par Alice sur la lame séparatrice peut s'écrire

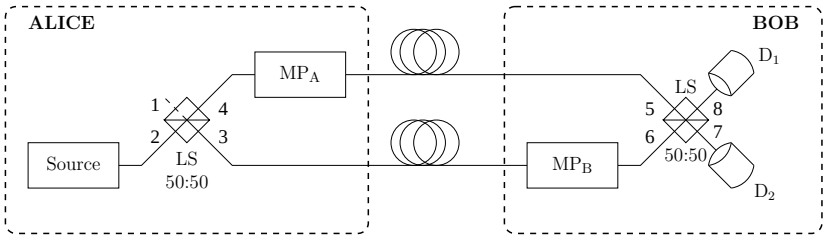


FIG. 1.11 – Codage en phase avec un interféromètre équilibré.

dans la base de Fock $|1\rangle_2$, où l'indice précise l'entrée ou la sortie de la lame séparatrice considérée. En introduisant un déphasage ϕ_A sur l'une des sorties, l'état transmis à Bob est alors

$$|\phi_A\rangle = \frac{|1\rangle_3 + e^{i\phi_A}|1\rangle_4}{\sqrt{2}}.$$

A la réception, Bob introduit à son tour un déphasage ϕ_B sur l'une des entrées de sa lame séparatrice. En supposant le canal sans perte, les états $|1\rangle_3$ et $|1\rangle_4$ se transforment selon

$$|1\rangle_3 = |1\rangle_6 \rightarrow e^{i\phi_B}(|1\rangle_7 + |1\rangle_8)/\sqrt{2} \quad et \quad |1\rangle_4 = |1\rangle_5 \rightarrow (-|1\rangle_7 + |1\rangle_8)/\sqrt{2},$$

et l'état en sortie de la séparatrice de Bob est donc

$$|\phi_B, \phi_A\rangle = \frac{\left(e^{i\phi_B} - e^{i\phi_A}\right)}{2}|1\rangle_7 + \frac{\left(e^{i\phi_B} + e^{i\phi_A}\right)}{2}|1\rangle_8.$$

Les compteurs de photons D_1 et D_2 supposés parfaits se déclenchent alors avec les probabilités respectives

$$P_1 = \sin^2(\frac{\phi_B - \phi_A}{2}) \qquad \text{et} \qquad P_2 = \cos^2(\frac{\phi_B - \phi_A}{2}).$$

En choisissant des valeurs de ϕ_A appropriées, Alice peut ainsi créer 4 qubits formant deux bases incompatibles du même espace de Hilbert. Par exemple :

Bit codé	0	1
Base 1	$\|0\rangle$	$\|\pi\rangle$,
Base 2	$\|-\pi/2\rangle = \frac{\|0\rangle + i\|\pi\rangle}{\sqrt{2}}$	$\|\pi/2\rangle = \frac{\|0\rangle - i\|\pi\rangle}{\sqrt{2}}$,

A l'aide des probabilités de détection précédentes, on vérifie aisément que Bob détermine sans ambiguïté le bit codé par Alice lorsque $\phi_B = 0$ et $\phi_A \in \{0, \pi\}$ ou $\phi_B = \pi$ et $\phi_A \in \{-\pi/2, \pi/2\}$, et n'obtient aucune information dans les autres cas de figure. Le choix de la phase ϕ_B peut donc s'identifier formellement à la sélection de la base de décodage.

En pratique le système représenté figure 1.11 est délicat à mettre en œuvre car il suppose de pouvoir contrôler la différence de chemin optique entre les deux bras de l'interféromètre avec une précision inférieure à la longueur d'onde des photons. Lors d'une transmission sur fibre optique de quelques kilomètres, les variations typiques de chemin optique sont cependant de l'ordre du millimètre alors que les longueurs d'ondes utilisées sont de l'ordre du micromètre. Pour cette raison, la majorité des systèmes est basée sur le schéma de la figure 1.12. Au lieu de « séparer » spatialement un photon sur les deux bras d'un interféromètre équilibré et de coder son information sur la différence de phase entre ces deux bras, Alice « sépare » un photon sur deux impulsions successives à l'aide d'un interféromètre déséquilibré, et code son information sur la différence de phase entre les deux impulsions. Alice doit ainsi seulement assurer la stabilité de son interféromètre déséquilibré, et le codage reste insensible aux variations de chemin optique du canal de transmission, tant que le temps caractéristique de ces dernières reste supérieur au déséquilibre de l'interféromètre (typiquement de l'ordre de quelques nanosecondes). Plus

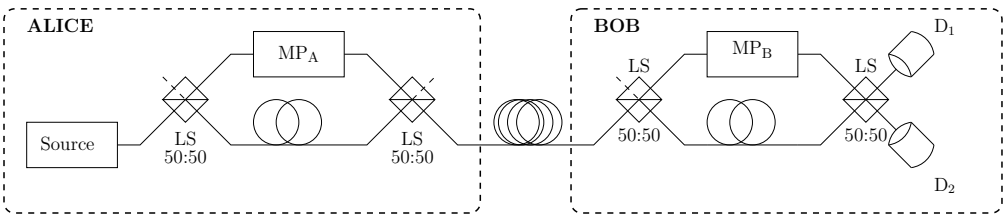


FIG. 1.12 – Codage en phase utilisant 2 interféromètres déséquilibrés.

précisément, Alice code son information en envoyant les photons dans un interféromètre

de Mach-Zehnder déséquilibré contenant un modulateur de phase (MP_A) dans le bras court. L'état transmis à Bob s'écrit alors

$$|\phi_A\rangle = \frac{|1\rangle_l - e^{i\phi_A}|1\rangle_c}{2},$$

où les indices c et l font respectivement référence aux bras court et long de l'interféromètre par lequel le photon a transité. Au récepteur Bob utilise un dispositif similaire à celui d'Alice. Puisqu'il est impossible de distinguer un photon empruntant le bras long de l'interféromètre d'Alice et le bras court de l'interféromètre de Bob (état $|1\rangle_{lc}$) d'un photon empruntant le bras court de l'interféromètre d'Alice et le bras long de l'interféromètre de Bob (état $|1\rangle_{cl}$), Bob obtient en sortie de son dispositif des interférences à un photon similaires à celles décrites précédemment. Après quelques calculs, on peut montrer que les états incidents sur les détecteurs D_1 et D_2 s'écrivent respectivement :

$$\begin{aligned} |D_1\rangle &= \frac{|1\rangle_{l,l} + (e^{i\phi_B} - e^{i\phi_A})|1\rangle_{l,c} - e^{i\phi_B}e^{i\phi_A}|1\rangle_{c,c}}{4}, \\ |D_2\rangle &= \frac{|1\rangle_{l,l} - (e^{i\phi_B} + e^{i\phi_A})|1\rangle_{l,c} + e^{i\phi_B}e^{i\phi_A}|1\rangle_{c,c}}{4}. \end{aligned}$$

Il est important de remarquer que puisque seule une des sorties de l'interféromètre est utilisée, la probabilité de coder un photon émis par la source avec succès n'est que de 50%. Par ailleurs, les photons ayant transité par des bras de même longueur dans les interféromètres d'Alice et Bob (états $|1\rangle_{cc}$ et $|1\rangle_{ll}$) ne créent pas d'interférences, en conséquence la probabilité qu'un photon émis par la source soit codé par Alice puis décodé par Bob n'est que de 25%. Il faut aussi souligner que les modulateurs de phase MP_A et MP_B sont en général sensibles à la polarisation, et Bob doit donc maintenir l'alignement des polarisations afin de décoder correctement les états qu'il reçoit.

Le système « Plug&Play » [4] développé dans le Groupe de Physique Appliquée de l'Université de Genève, permet d'effectuer astucieusement un alignement automatique de la polarisation. Le schéma expérimental de ce système est représenté figure 1.13. La trans-

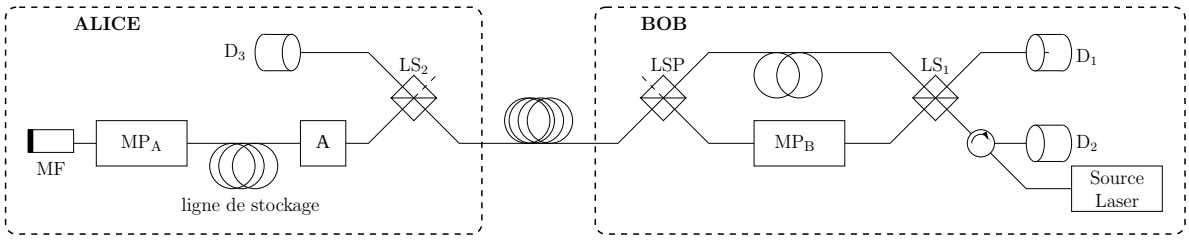


FIG. 1.13 – Système « Plug&Play ».

mission est initialisée par Bob qui injecte une impulsion laser intense dans son dispositif à travers un circulateur. L'impulsion se sépare ensuite en deux sur la lame séparatrice LS_1. La première moitié de l'impulsion P_1 se propage sur le bras long de l'interféromètre, et la polarisation est ajustée de telle sorte que l'impulsion soit totalement transmise sur la lame séparatrice de polarisation LSP. De même, la seconde moitié de l'impulsion P_2 se propage sur le bras court, et la polarisation est ajustée de façon à ce que l'impulsion soir

totalement réfléchie par LSP. Les impulsions envoyées sur le canal ont donc des polarisations orthogonales, mais ne contiennent à ce stade aucune information. En arrivant dans le dispositif d'Alice, les impulsions sont de nouveau séparées sur une lame séparatrice (LS_2). La première partie est envoyée sur un détecteur standard (D_3), et fournit un signal de synchronisation. La seconde partie est atténuée (A), envoyée dans une ligne de stockage, puis réfléchie par un miroir de Faraday. Alice active alors le modulateur de phase MP_A pour effectuer le codage en phase décrit précédemment. L'atténuation d'Alice est ajustée de sorte que les impulsions quittant son dispositif contiennent en moyenne moins d'un photon. Grâce au miroir de Faraday, la polarisation des impulsions arrivant sur la lame séparatrice de polarisation LSP est exactement orthogonale à leur polarisation de départ. P_1 se propage alors sur le bras court de l'interféromètre, P_2 se propage sur le bras long, et Bob active son modulateur de phase MP_B pour sélectionner sa base de décodage. Les impulsions interfèrent au même instant sur la lame séparatrice LS_1, puis les compteurs de photons D_1 et D_2 détectent finalement la sortie empruntée par le photon.

Les variations de polarisation étant relativement lentes par rapport au temps d'aller-retour des impulsions, le système « Plug&Play » permet de compenser parfaitement ces fluctuations. Contrairement au système basé sur deux interféromètres, toutes les impulsions donnent ici lieu à des interférences. Cependant, à cause de sa configuration bidirectionnelle, le « Plug&Play » ne peut pas fonctionner avec des sources de photons uniques. Une version unidirectionnelle potentiellement compatible a été proposée [54], mais comme dans le système à deux interféromètres l'efficacité de codage et décodage des impulsions n'est alors que de 25%.

Le tableau 1.2 résume les performances de plusieurs dispositifs mettant en œuvre un codage en phase. Tous ces systèmes fonctionnent sur fibre optique et utilisent des impulsions atténuées contenant $\mu < 1$ photons par impulsion.

Référence	μ	λ	d	Débit
Stucki *et al* (2002) [55]	$\mu = 0.2$	1550 nm	67 km	50 bits/s (clé)
Guerreau *et al* (2003) [56]	$\mu = 0.2$	1550 nm	40 km	400 bits/s (brut)
Yuan (2005) *et al* [57]	$\mu = 0.2$	1550 nm	20.3 km	1700 bits/s (*sifted*)

TAB. 1.2 – Performances des systèmes BB84 basés sur un codage en phase

Contrairement au codage en polarisation, les résultats obtenus avec un codage en phase ne sont en général pas rapportés très précisément. Certains articles ne fournissent qu'un débit de photons détectés (brut) ou un débit après réconciliation (*sifted*), et il est donc difficile de comparer de façon objective tous ces systèmes. Nous avons choisi arbitrairement de présenter les résultats obtenus avec des systèmes testés sur des fibres déployées, mais des transmissions sur des distances bien plus impressionnantes ont déjà été réalisées [54].

1.2.3 Sécurité des systèmes réels

La réalisation des dispositifs expérimentaux présentés dans la section précédente a représenté une avancée significative de la cryptographie quantique. Cependant, même les systèmes les plus aboutis ne sont encore que de grossières approximations du système idéal pour lequel la sécurité inconditionnelle a été démontrée. L'utilisation de sources

lasers atténuées au lieu de sources de photons uniques est souvent considérée comme la faille majeure, mais toutes les imperfections des composants utilisés peuvent affecter la fidélité des états préparés ainsi que les mesures de Bob, et sont donc autant de failles qu'un espion pourrait exploiter et qu'il faudrait pouvoir prendre en compte. Bien qu'il n'existe pas actuellement de preuve de sécurité inconditionnelle s'appliquant sans aucune restriction aux dispositifs expérimentaux, les preuves les plus récentes [58] considèrent des situations de plus en plus réalistes, et il est peu probable que les améliorations futures modifient de façon significative les résultats actuels.

Les preuves de sécurité inconditionnelle sont relativement complexes, et l'objectif de cette section est uniquement de rappeler les principaux résultats démontrés en précisant clairement les hypothèses associées. Afin de pouvoir appliquer aisément ces résultats à des cas pratiques, les expressions des débits de clés seront présentées uniquement pour un système réaliste aux caractéristiques suivantes :

- **Emetteur.** Alice utilise une source de photons uniques ou d'états cohérents atténués contenant en moyenne $\mu \ll 1$ photon par impulsion. Dans ce dernier cas, la probabilité d'émettre une impulsion contenant plusieurs photons est alors $\mu_m = 1 - e^{-\mu} - \mu e^{-\mu}$. Le codage effectué par Alice est supposé parfait, mais d'efficacité limitée η_A.
- **Canal quantique.** Les pertes de canal se traduisent par une efficacité de transmission $\eta_T = 10^{-\alpha d}$, où α est l'atténuation linéique (typiquement 0.2 dB/km dans de la fibre en silice à 1550 nm.) et d la distance de transmission.
- **Récepteur**. Le dispositif de mesure de Bob est supposé parfaitement aligné, mais les pertes des composants et l'efficacité limitée des compteurs de photons se traduisent par une efficacité η_B. Les détecteurs de photons peuvent parfois se déclencher sans pour autant avoir reçu de photons, ces « coups d'obscurité » (*dark count*) sont susceptibles d'apparaître avec une probabilité p_{dc}.
- **Réconciliation.** L'efficacité de la réconciliation est caractérisée par la fraction $\epsilon_{rec} > 0$ de bits dévoilés en plus de la limite de Shannon. Généralement ϵ_{rec} dépend du QBER e.
- **Clés secrètes.** Les clés sont supposées suffisamment longues pour pouvoir négliger la perte de débit liée aux estimations du QBER e (l'estimation peut se faire à l'aide d'un échantillon de taille négligeable).

Les probabilités de détection d'un photon par Bob selon qu'Alice utilise une source à photons uniques ou des impulsions atténuées sont alors respectivement

$$\boxed{\begin{aligned} p_{exp}^{sp} &= \eta_A \eta_T \eta_B + p_{dc}, \\ p_{exp}^{mp} &= 1 - e^{-\mu \eta_T \eta_B} + p_{dc}. \end{aligned}}$$

Lorsque Alice utilise des impulsions laser atténuées, il est toujours possible d'ajuster l'atténuation pour obtenir la valeur de μ désirée en sortie du dispositif, et l'efficacité η_A ne rentre alors plus en compte.

Limites ultimes de distance et de débit

Les pertes introduites par les composants de Bob ainsi que les coups d'obscurité des compteurs de photons fixent une distance de transmission limite au delà de laquelle aucun échange de clé sécurisé n'est possible [59]. En effet lorsque le QBER e (mesuré sur

les bits reçus par Bob) dépasse 25%, Eve peut mettre en œuvre une attaque interception/réémission et obtenir autant d'information que Bob.

Lorsque Alice utilise une source à photons uniques, le QBER mesuré est au mieux crée uniquement par les coups d'obscurité et donc de l'ordre de $e \geq 0.5 p_{dc}/p_{exp}^{sp}$. La condition $e < 0.25$ impose alors

$$\boxed{d_{max}^{sp} \leq \frac{10 \log \eta_A \eta_B - 10 \log p_{dc}}{\alpha}.} \tag{1.1}$$

Lorsque Alice utilise une source d'états cohérents atténués, Eve peut mettre en œuvre une attaque dite PNS (*Photon Number Splitting*). Cette attaque consiste à effectuer une mesure quantique non destructive pour évaluer le nombre de photons contenus dans les impulsions émises par Alice, puis à extraire un photon des impulsions multiphotons. Le photon est conservé dans une mémoire quantique, et lorsque Bob révèle la base de projection utilisée pour chacun des photons qu'il a détectés, Eve peut alors effectuer la mesure appropriée et obtenir le même résultat sans dévoiler son intervention. En présence de pertes, Eve peut en plus bloquer les impulsions ne contenant qu'un seul photon et ne faire parvenir à Bob que les impulsions multiphotons, sans pour autant modifier le taux de comptage attendu. Un échange de clé secrète n'est alors possible que si Bob reçoit un nombre non nul d'impulsions à un photon, et si le taux d'erreur sur cette proportion est comme précédemment inférieur à 25%. Le QBER est ici $e \geq 0.5 p_{dc}/(p_{exp}^{mp} - \mu_m)$, et en supposant $\mu \ll 1$ la distance maximale est alors

$$\boxed{d_{max}^{mp} \leq \frac{-10}{\alpha} \log \left(\frac{p_{dc}}{\eta_B \mu} + \frac{\mu}{2\eta_B} \right).}$$

En optimisant la valeur de μ, la limite est au mieux

$$\boxed{d_{max}^{mp} \leq \frac{10 \log \eta_B - 5 \log 2 p_{dc}}{\alpha}.}$$

De la même façon, les débits de clés ne peuvent pas excéder le taux de comptage de photon du récepteur de Bob, qui est fixé par les pertes des dispositifs et l'atténuation du canal de transmission [60]. En fonction de la source utilisée Alice et Bob peuvent dans le meilleur des cas échanger des clés à des taux

$$\boxed{\begin{aligned} r_{max}^{sp} &\leq \eta_A \eta_T \eta_B + p_{dc}, \\ r_{max}^{mp} &\leq 1 - e^{-\eta_T \eta_B \mu} + p_{dc}. \end{aligned}}$$

Sécurité en présence d'attaques individuelles

L'analyse du protocole BB84 effectuée par Lütkenhaus ne considère que des attaques individuelles sur les qubits émis par Alice [60]. Les dispositifs d'Alice et Bob sont supposés hors du contrôle d'Eve, et hormis lorsque Alice utilise des états cohérents pouvant contenir plusieurs photons, Eve ne peut obtenir aucune information sur le choix de la base d'Alice. Par ailleurs le dispositif de Bob fonctionne de façon identique quelle que soit la base de décodage utilisée.

Lorsque Alice utilise une source à photons uniques, le débit de clés secrètes en bits par photon émis est alors

$$\boxed{G_L^{sp} = \frac{1}{2} p_{exp}^{sp}\big(1 - \log_2(1 + 4e - 4e^2) - (1 + \epsilon_{rec})h(e)\big),}$$

où $h(e) = -e\log_2(e) - (1-e)\log_2(1-e)$. Lorsque Alice utilise des états cohérents fortement atténués, le débit devient

$$\boxed{G_L^{mp} = \frac{1}{2} p_{exp}^{mp}\big\{\alpha^{-1}\left[1 - \log_2\left(1 + 4e\alpha - 4(e\alpha)^2\right)\right] - (1 + \epsilon_{rec})h(e)\big\}.}$$

avec

$$\boxed{\alpha = \frac{p_{exp}^{mp}}{p_{exp}^{mp} - \mu_m}.} \tag{1.2}$$

Le terme entre crochets s'obtient après une analyse précise de l'amplification de confidentialité, mais on peut néanmoins expliquer intuitivement les différents termes intervenant dans la formule. Puisque qu'Eve peut obtenir toute l'information transportée par des impulsions multiphotons avec une attaque PNS, seule la fraction Ω_1 d'impulsions à photon unique détectées par Bob peut effectivement transporter des bits secrets. Puisque Bob n'a aucun moyen de déterminer si les impulsions qu'il reçoit sont des impulsions à photon unique, l'estimation de Ω_1 doit se faire dans le pire des cas, c'est-à-dire lorsque Bob détecte toutes les impulsions multi-photons. On obtient donc :

$$\Omega_1 = \frac{p_{exp}^{mp} - \mu_m}{p_{exp}^{mp}}. \tag{1.3}$$

Les impulsions à photon unique peuvent elles aussi avoir été manipulées par Eve, et il est donc nécessaire d'évaluer le QBER e_1 sur cette fraction des impulsions pour déterminer le nombre de bits à retrancher par amplification de confidentialité. Encore une fois, il faut considérer le scénario le plus défavorable où toutes les erreurs surviennent sur des impulsions à photon unique :

$$e_1 = \frac{p_{exp}^{mp}}{p_{exp}^{mp} - \mu_m} e. \tag{1.4}$$

Sécurité en présence d'attaques cohérentes

Les preuves de sécurité de Mayers [61] et Inamori [62] généralisent l'étude de Lütkenhaus au cas où Eve met en œuvre des attaques cohérentes. Comme précédemment, Eve ne peut interagir qu'avec les états transmis sur le canal quantique, et n'a pas accès aux dispositifs d'Alice et Bob. Les imperfections du système d'Alice se limitent à l'émission d'impulsions multiphotons, et les résultats des mesures de Bob sont indépendants de la base de décodage utilisée.

Les débits de clés obtenus avec une source de photons uniques et une source d'états cohérents atténués sont alors respectivement[4]

$$\boxed{G_{ILM}^{sp} = \frac{1}{2} p_{exp}^{sp}(1 - h(e) - (1 + \epsilon_{rec})h(e)),}$$

[4]L'expression n'est pas tout à fait celle reportée dans la référence [62], mais une version légèrement améliorée suggérée dans [58]

$$G_{ILM}^{mp} = \frac{1}{2} p_{exp}^{mp} \left\{ \frac{p_{exp}^{mp} - \mu_m}{p_{exp}^{mp}} \left[1 - h\left(e \frac{p_{exp}^{mp}}{p_{exp}^{mp} - \mu_m} \right) \right] - (1 + \epsilon_{rec}) h(e) \right\}. \tag{1.5}$$

Les quantités intervenant dans ces expressions (p_{exp}, μ_m, e) peuvent toutes être mesurées expérimentalement, et l'analyse de sécurité ne requiert aucune caractérisation du détecteur de Bob.

Sécurité en présence d'attaques cohérentes (bis)

L'analyse de Gottesman et de ses collaborateurs [58] est particulièrement intéressante, car ces derniers considèrent la situation réaliste où les imperfections de la source d'Alice et des détecteurs de Bob sont limitées mais peuvent en revanche être exploitées par un deuxième adversaire (Fred). Fred est alors susceptible de coopérer avec Eve avec certaines restrictions. Cette analyse suppose qu'Alice et Bob soient capables de caractériser leurs dispositifs expérimentaux et d'en identifier les failles, mais permet de prendre en compte des défauts réalistes tels que

- le « marquage » des qubits émis par Alice : comme dans le cas d'impulsions multiphotons, Eve peut parfois connaître le bit transmis par Alice.
- le fonctionnement inégal du dispositif de Bob en fonction de la base de décodage (voir chapitre 2).
- le mauvais alignement des bases utilisées au codage et décodage.

Les débits de clés obtenus en supposant que les seules imperfections sont les impulsions multiphotons, sont identiques à ceux estimés précédemment.

Les figures 1.14 et 1.15 représentent les débits de clés atteignables avec un système réaliste. Les caractéristiques du dispositif de Bob sont $\eta_B = 18\%$ et $p_{dc} = 2 \times 10^{-4}$, et dans le cas d'une source émettant des états cohérents, le nombre moyen de photons par impulsion μ est choisi pour optimiser le débit. L'efficacité d'Alice est $\eta_A = 1$ pour simplifier la comparaison des deux types de source, et la réconciliation est supposée parfaite ($\epsilon_{rec} = 0$).

A cause de l'estimation très pessimiste du nombre d'impulsions à photon unique parvenant à Bob, l'utilisation d'états cohérents réduit de façon dramatique les distances de transmissions. Il faut en effet choisir $\mu \approx \eta_T$, et les débits sont alors de l'ordre de $\mathcal{O}(\eta_T^2)$ au lieu de $\mathcal{O}(\eta_T)$. Il est cependant intéressant de noter que les attaques cohérentes ne semblent pas améliorer significativement les possibilités d'Eve.

Plusieurs modifications du protocole BB84 ont été envisagées pour limiter la perte de débit liée aux attaques PNS [63–65]. En particulier, l'utilisation d'états cohérents « leurres » [65] permet à Alice et Bob d'atteindre des débits de l'ordre de $\mathcal{O}(\eta_T)$ sans modifier fondamentalement ni le protocole BB84, ni les architectures des systèmes basés sur des états cohérents. Le principe de cette technique est d'autoriser Alice à faire varier aléatoirement le nombre moyen de photons μ dans ses impulsions. Eve ne peut pas distinguer ces états « leurres » des autres états, et doit donc traiter identiquement toutes les impulsions qu'elle intercepte. Une fois la transmission effectuée, si Alice dévoile à Bob quels étaient les état leurres, ces derniers peuvent alors estimer de façon précise la proportion Ω_1 d'impulsions à photon unique émises par Alice et détectées par Bob, ainsi que le

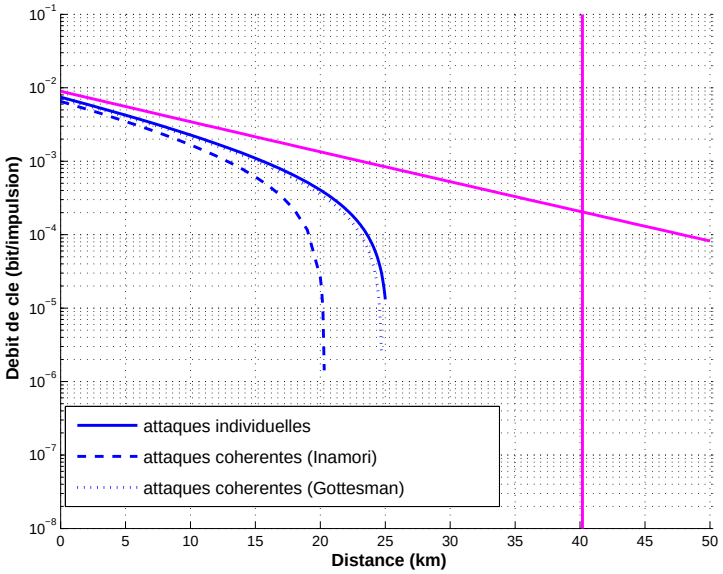


FIG. 1.14 – Débits de clés atteignables pour un système réaliste avec des états cohérents atténués.

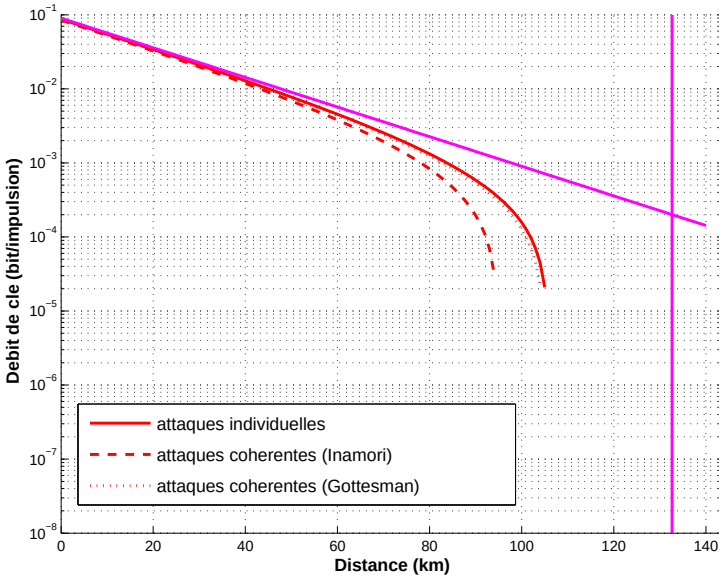


FIG. 1.15 – Débits de clés atteignables pour un système réaliste avec des photons uniques.

QBER e_1 associé. Cette meilleure estimation se traduit directement par une augmentation du débit de clé calculé avec l'équation (1.5).

1.3 Cryptographie quantique par variables continues

Les principaux facteurs technologiques limitant aujourd'hui les débits des systèmes de cryptographie quantique par photons uniques, sont liés au choix de la méthode de codage. En effet l'efficacité des sources utilisées est très limitée (au mieux de l'ordre de quelques pourcents pour les sources de photons uniques), et les compteurs de photons ne peuvent pas fonctionner au delà d'une certaine cadence, typiquement de l'ordre du mégahertz, et avec une efficacité de détection de l'ordre de 15% aux longueurs d'ondes télécom. L'utilisation d'états quantiques de plus grande intensité, et donc plus aisés à détecter, permet de remédier en partie à ces inconvénients. En particulier le codage de l'information sur des variables prenant un ensemble continu de valeurs, telles que les quadratures du champ électromagnétique, offre une alternative intéressante aux codages standard basés sur des qubits.

1.3.1 Protocoles

Suite à l'étude de Ralph en 1999 [66], de nombreux protocoles exploitant les quadratures du champ électromagnétique ont été analysés. Les premiers travaux [67–72] ont tous en commun d'exploiter des caractéristiques spécifiquement quantiques de la lumière telles que la compression *(squeezing)* ou l'intrication. L'intérêt de ces protocoles est essentiellement théorique car les états quantiques requis sont difficiles à créer expérimentalement, et très peu robustes aux pertes. Frédéric Grosshans et Philippe Grangier ont cependant démontré que des échanges de clés quantiques étaient possibles sans aucun des aspects quantiques mentionnés précédemment, en utilisant uniquement des états cohérents « quasi-classiques » de la lumière [73]. Nous ne décrirons dans cette section que les protocoles exploitant ce résultat et ayant donné lieu à des réalisations expérimentales.

Protocoles directs et inverses

Le principe général des protocoles, initialement proposé par Nicolas Cerf pour des états comprimés [72], consiste à transmettre des états cohérents $|\alpha\rangle$ dont l'amplitude α suit une distribution continue gaussienne. Alice génère tout d'abord deux séquences de nombres aléatoires $\{x_k\}_{k=1..N} \in \mathbb{R}^N$ et $\{p_k\}_{k=1..N} \in \mathbb{R}^N$ selon une distribution gaussienne de moyenne nulle et de variance $V_A N_0$ ($V_A \gg 1$), où N_0 est la variance du bruit quantique. Elle transmet ensuite successivement à Bob les états cohérents $\{|x_k + ip_k\rangle\}_{k=1..N}$. De son côté Bob dispose d'une séquence binaire aléatoire $\{b_k\}_{k=1..N} \in \{0,1\}^N$, et à la réception de chacun des états, il choisit d'effectuer une détection homodyne de la quadrature X ($b_k = 0$) ou la quadrature P ($b_k = 1$). Une fois les N états reçus, Bob dévoile alors les quadratures mesurées en révélant $\{b_k\}_{k=1..N}$, Alice ne conserve alors que l'information correspondante et néglige le reste. A la fin de cette étape, Alice et Bob partagent donc un ensemble de données continues corrélées suivant des distributions gaussiennes. En comparant publiquement un sous-ensemble de leurs données, ils peuvent alors estimer les caractéristiques du canal de transmission (pertes et bruit) puis évaluer l'information

échangée et interceptée par Eve. Il est alors possible de mettre en œuvre réconciliation et amplification de confidentialité pour générer une clé secrète. Cependant, à la différence des variables binaires, il est important de distinguer la manière dont s'effectue la réconciliation. Si les symboles d'Alice servent de référence, le protocole est qualifié de *direct*, en revanche si les symboles de Bob servent de référence, le protocole est qualifié d'*inverse*. Afin d'illustrer cette distinction, nous rappellerons les résultats obtenus dans le cas où Eve effectue des attaques individuelles sur les symboles émis par Alice.

En se limitant au cas des attaques individuelles, la sécurité des protocoles direct et inverse découle directement d'inégalités de type Heinsenberg entre les différentes mesures d'Alice, Bob, et Eve. Les canaux de transmission peuvent être modélisés par les équations suivantes

$$X_B = \sqrt{G_X}(X_A + \delta X_A + N_{X,B}), \qquad P_B = \sqrt{G_P}(P_A + \delta P_A + N_{P,B}),$$
$$X_E = \sqrt{H_X}(X_A + \delta X_A + N_{X,E}), \qquad P_E = \sqrt{H_P}(P_A + \delta P_A + N_{P,E}).$$

X_A et P_A représentent les variables aléatoires classiques générées par Alice selon une distribution gaussienne $\mathcal{N}(0, V_A N_0)$, et les fluctuations quantiques des états cohérents transmis sont représentées par δX_A et δP_A de distribution gaussienne $\mathcal{N}(0, N_0)$. Les variables $N_{X,B} \sim \mathcal{N}(0, \chi_{X,B} N_0)$, $N_{P,B} \sim \mathcal{N}(0, \chi_{P,B} N_0)$, $N_{X,E} \sim \mathcal{N}(0, \chi_{X,E} N_0)$ et $N_{P,E} \sim \mathcal{N}(0, \chi_{P,E} N_0)$ représentent les bruits ajoutés par le canal quantique et les appareils de détection sur les mesures de quadrature de Bob et Eve. Ces bruits sont supposés non corrélés à la modulation d'Alice et aux fluctuations quantiques. Puisque la modulation d'Alice est symétrique et que Bob alterne aléatoirement ses mesures de quadrature, on peut de plus considérer que $G_X = G_P = G$, $H_X = H_P = H$, $\chi_{X,B} = \chi_{P,B} = \chi_B$ et $\chi_{X,E} = \chi_{P,E} = \chi_E$.

Ainsi, les signaux mesurés par Bob sont obtenus en envoyant les signaux gaussiens d'Alice de variance $V_A N_0$ à travers un canal introduisant un bruit additif gaussien de variance $(1 + \chi_B)N_0$. L'information échangée est donc

$$I_{AB} = I_{BA} = \frac{1}{2}\log_2(1 + \frac{V_A}{1 + \chi_B}).$$

De la même façon, si l'on considère le protocole direct, l'information obtenue par Eve est

$$I_{AE} = \frac{1}{2}\log_2(1 + \frac{V_A}{1 + \chi_E}).$$

Les mesures d'Eve ne sont cependant pas indépendantes des mesures de Bob, le principe d'incertitude d'Heisenberg fixe en effet une limite à l'information qu'Eve et Bob peuvent acquérir simultanément. Comme démontré dans [73] les variances des bruits d'Eve et Bob doivent vérifier

$$\chi_B \chi_E \geq 1.$$

Avec une réconciliation directe, Alice et Bob peuvent donc échanger au maximum

$$\overrightarrow{\Delta I} = \max\{I_{AB} - I_{AE}, 0\} = \max\left\{\frac{1}{2}\log_2 \frac{V_A + 1 + \chi_B}{\chi_B(V_A + 1) + 1}, 0\right\}$$

bits de clé secrète. $\overrightarrow{\Delta I}$ n'est alors non nul que si $\chi_B < 1$. Pour un canal de transmission G, le bruit ajouté peut s'écrire $\chi_B = (1 - G)/G + \epsilon$, où ϵ est la contribution au bruit

du dispositif de détection seul. Dans le meilleur des cas $\epsilon = 0$, et un échange de clé n'est possible que si $G > 0.5$, soit pour un canal présentant moins de 3 dB de pertes.

En réalité, une distribution de clé est aussi possible lorsque $I_{AB} - I_{BE} > 0$, correspondant au cas du protocole inverse où les données de Bob et non plus celles d'Alice servent de référence. Intuitivement cette situation est plus favorable que la précédente car il est plus difficile pour Eve d'obtenir de l'information sur les mesures de Bob que sur la modulation d'Alice. Comme dans le cas des protocoles directs, les estimations d'Eve et Alice ne sont pas indépendantes. Par exemple, si Alice essaye d'obtenir une estimation optimale de X_B minimisant la variance de son erreur, et si Eve tente d'obtenir une estimation optimale de P_B, leurs estimateurs s'écrivent

$$\hat{X}_{B|A} = \frac{\langle X_B X_A \rangle}{\langle X_A^2 \rangle} X_B \quad \text{et} \quad \hat{P}_{B|E} = \frac{\langle P_B P_E \rangle}{\langle P_E^2 \rangle} P_B,$$

et les variances des erreurs respectives sont notées $V_{X_B|X_A}$ et $V_{P_B|P_E}$. Les relations de commutation entre les différents opérateurs mesurés imposent alors les inégalités

$$V_{X_B|X_A} V_{P_B|P_E} \geq N_0 \quad \text{et} \quad V_{P_B|P_A} V_{X_B|X_E} \geq N_0.$$

Dans le cas où les quadratures X et P sont utilisées de façon symétrique, les relations précédentes se réduisent à $V_{B|A} V_{B|E} \geq N_0$. La contribution majeure de Frédéric Grosshans et de ses collaborateurs a été de remarquer qu'Eve et Bob n'ont accès qu'à la matrice de densité ρ_A des états envoyés par Alice, et que par conséquent la relation précédente doit être vérifiée pour tous les états compatibles avec ρ_A qu'Alice aurait pu générer [73–75]. En particulier si Alice utilise l'intrication maximale compatible avec ρ_A, la variance des mesures d'Eve doit satisfaire

$$V_{B|E} \geq \frac{N_0}{G(\frac{1}{V_A+1} + \chi_B)}.$$

L'information obtenue par Eve est donc au maximum

$$I_{BE} = \frac{1}{2} \log_2 G^2 (V_A + 1 + \chi_B) \left(\frac{1}{V_A + 1} + \chi_B \right).$$

Alice et Bob peuvent donc générer

$$\overleftarrow{\Delta I} = \max \{ I_{AB} - I_{BE}, 0 \} = \max \left\{ -\frac{1}{2} \log_2 G^2 (1 + \chi_B) \left(\frac{1}{V_A + 1} + \chi_B \right), 0 \right\}.$$

bits de clé secrète. Contrairement au cas du protocole direct, $\overleftarrow{\Delta I}$ peut cette fois rester positif pour toutes les valeurs de l'atténuation du canal. En réintroduisant la notation $\chi_B = (1 - G)/G + \epsilon$, la condition $\overleftarrow{\Delta I} > 0$ implique $\epsilon < (V - 1)/2V$ ce qui signifie qu'une clé peut être échangée tant que le bruit additionnel introduit par le dispositif de détection n'est pas trop important.

La sécurité de ces protocoles a été généralisée au cas d'attaques cohérentes de taille finie [76] puis au cas d'attaques collectives [77, 78], et plus récemment l'optimalité des attaques gaussiennes a été démontrée [79, 80]. Le même protocole peut par ailleurs être mis en œuvre au cas où Bob mesure simultanément les quadratures X et P des états qu'il reçoit [81].

Protocoles avec postsélection

Les protocoles avec postsélection présentent certaines similitudes avec ceux décrits précédemment [82]. Alice émet une série d'états cohérents $\{|x_k + ip_k\rangle\}_{k=1..N}$, où les données aléatoires $\{x_k\}_{k=1..N} \in \mathbb{R}^N$ et $\{p_k\}_{k=1..N} \in \mathbb{R}^N$ suivent une distribution gaussienne de moyenne nulle. De son côté Bob génère une séquence de bits aléatoires $\{b_k\}_{k=1..N} \in \{0,1\}^N$ et à la réception de chaque état alterne entre des détections homodynes de quadrature X (si $b_k = 0$) et P (si $b_k = 1$). Une fois les N états reçus, Bob annonce alors publiquement les quadratures choisies. Plutôt que d'effectuer une réconciliation sur leurs données continues, Alice et Bob interprètent les déplacements positifs de quadrature comme un bit « 0 » et les déplacements négatifs de quadrature comme un bit « 1 ». Afin de simplifier encore plus la décision de Bob, Alice dévoile publiquement les valeurs $\{\alpha_k\}_{k=1..N}$ et $\{\theta_k\}_{k=1..N}$, où $\alpha_k = |x_k + ip_k|$ et $\theta_k = \arg(x_k + ip_k) \mod \pi$. Cette information ne caractérise pas complètement les états envoyés, puisque qu'il reste toujours une incertitude sur le signe de la quadrature, mais permet d'interpréter chacun des états transmis comme appartenant soit à l'ensemble $\left\{\left|\alpha_k e^{i\theta_k}\right\rangle, \left|-\alpha_k e^{-i\theta_k}\right\rangle\right\}$ si Bob a mesuré la quadrature X, soit à l'ensemble $\left\{\left|i\alpha_k e^{i\theta_k}\right\rangle, \left|-i\alpha_k e^{-i\theta_k}\right\rangle\right\}$ si Bob a mesuré la quadrature P. Lorsque l'attaque de l'espion consiste uniquement à se substituer passivement aux pertes, en introduisant une lame séparatrice de transmission η équivalente à celle attendue par Bob, les états obtenus par Bob et Eve sont respectivement

$$|\sqrt{\eta}(x_k + ip_k)\rangle_B \quad \text{et} \quad \left|\sqrt{1-\eta}(x_k + ip_k)\right\rangle_E.$$

Si Bob mesure par exemple la quadrature X, la mesure optimale d'Eve lui permettant de discriminer les deux états non orthogonaux $\left\{\left|\alpha_k e^{i\theta_k}\right\rangle, \left|-\alpha_k e^{-i\theta_k}\right\rangle\right\}$ est alors connue, et lui fournit I_{AE} bits d'information dépendant uniquement du recouvrement des états

$$\beta_k = \left|\left\langle \sqrt{1-\eta}\alpha_k e^{i\theta_k}| - \sqrt{1-\eta}\alpha_k e^{-i\theta_k}\right\rangle\right|^2 = \exp(-4(1-\eta)\alpha_k^2 \cos^2\theta_k).$$

De la même façon, il est possible d'évaluer le taux d'erreur de Bob et l'information échangée I_{AB} en fonction de β_k et de la mesure de quadrature y_k de Bob. Cette paramétrisation des informations mutuelles permet d'identifier deux régimes :

$$\begin{aligned} I_{AB}(y_k, \beta_k) - I_{AE}(\beta_k) &> 0, \\ I_{AB}(y_k, \beta_k) - I_{AE}(\beta_k) &\leq 0, \end{aligned}$$

et donc de ne conserver *a posteriori* que les données où Alice et Bob possèdent un avantage sur Eve.

Plusieurs systèmes expérimentaux utilisant une postsélection ont été mis en œuvre [83, 84], cependant les analyses de sécurité sont encore limitées à des attaques passives.

1.3.2 Systèmes expérimentaux

La cryptographie quantique par variables continues ne s'est réellement développée que sous l'impulsion des travaux de Frédéric Grosshans et Philippe Grangier, et on ne retrouve donc pas la diversité de systèmes existant avec la cryptographie quantique par photons uniques. Nous ne présenterons ici que les deux réalisations les plus abouties mettant en œuvre les protocoles inverses décrits dans la section précédente.

Le schéma expérimental du dispositif réalisé au laboratoire Charles Fabry d'Orsay [20, 75, 85] est représenté figure 1.16. Alice envoie des impulsions laser sur une lame séparatrice

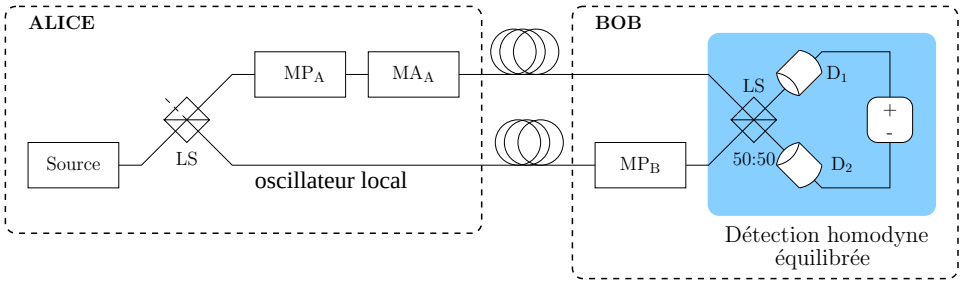


FIG. 1.16 – Dispositif de cryptographie quantique par variables continues.

déséquilibrée, et crée ainsi un oscillateur local intense et un état cohérent $|\alpha\rangle$ contenant en moyenne une centaine de photons. La phase et l'amplitude de l'état cohérent sont modulées par les modulateurs MP$_A$ et MA$_A$, de sorte que les quadratures suivent une distribution gaussienne. Au récepteur, Bob effectue une détection homodyne de l'état envoyé par Alice, et choisit la quadrature mesurée en déphasant l'oscillateur local à l'aide du modulateur de phase MP$_B$. Par ailleurs comme dans le cas du codage en phase du protocole BB84, ce système peut être utilisé sur une fibre optique déployée en remplaçant le multiplexage spatial de l'oscillateur local par un multiplexage temporel.

En s'inspirant du dispositif « Plug&Play » utilisé pour la cryptographie quantique à photons uniques, le Groupe de Physique Appliquée de l'Université de Genève a mis au point un dispositif « Go&Return » [86] extrêmement stable et alignant automatiquement la polarisation (figure 1.17). Les impulsions laser injectées dans le dispositif de Bob avec une lame séparatrice déséquilibrée (2 :98) se séparent tout d'abord en deux sur une lame séparatrice équilibrée (LS). L'impulsion passant par le bras long de l'interféromètre traverse un isolateur (I) dans le sens bloquant, et se trouve donc atténuée d'environ 60 dB. La seconde impulsion passant par le bras court de l'interféromètre, fournit l'oscillateur local nécessaire à la détection homodyne. Les contrôleurs de polarisation sont ajustés de façon à ce que les deux impulsions aient des polarisations orthogonales. De son côté,

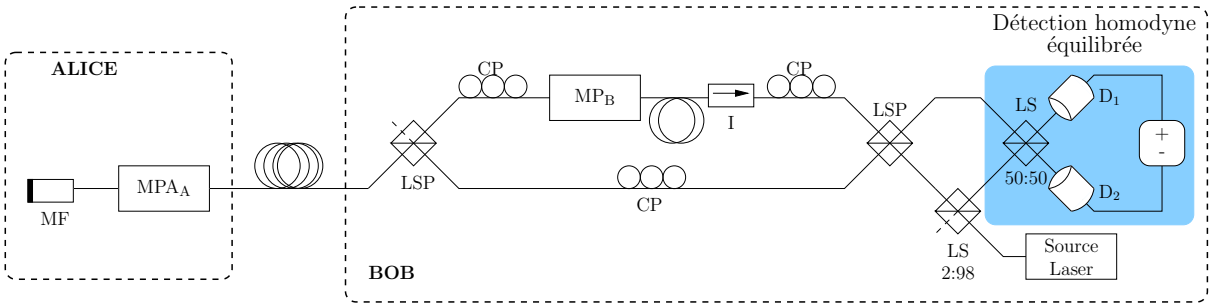


FIG. 1.17 – Dispositif « Go&return » de cryptographie quantique par variables continues.

Alice réfléchit les impulsions lui parvenant à l'aide d'un miroir de Faraday (MF), et modifie simultanément la phase et l'amplitude de l'impulsion atténuée avec un modulateur à deux électrodes (MPA). Grâce au miroir de Faraday, les impulsions retournent sur la lame séparatrice de Bob avec une polarisation orthogonale à celle de départ. L'oscillateur

local parcourt donc le bras long de l'interféromètre de Bob, mais traverse l'isolateur dans le sens passant et ne subit qu'une faible atténuation ; l'état cohérent de faible intensité codé par Alice emprunte le bras court. Les deux impulsions interfèrent au même instant sur la lame séparatrice équilibrée, et les sorties sont alors recombinées pour effectuer une détection homodyne.

1.3.3 Sécurité des systèmes réels basés sur des protocoles inverses

Les systèmes expérimentaux souffrent de plusieurs imperfections qu'il faut prendre en compte pour évaluer le niveau réel de sécurité :

- les composants électroniques et le bruit de phase de la diode se traduisent par un excès de bruit ϵ,
- la détection homodyne de Bob a une efficacité limitée $\eta_h < 1$,
- la réconciliation des variables continues ne s'effectue qu'avec une efficacité $\beta < 1$ (l'efficacité est liée au surplus de bits dévoilés ϵ_{rec}, voir chapitre 4),
- si Eve a accès aux dispositifs de mesure de Bob, les pertes des composants pourraient être exploitées.

Dans une situation réaliste, on peut cependant considérer qu'Eve n'a pas accès à la détection homodyne de Bob, et dans ce cas les informations mutuelles (en bits/symboles transmis) sont [20] :

$$\boxed{\begin{aligned} I_{AB} &= \frac{1}{2}\log_2 \frac{\eta_h G V_A + 1 + \eta_h G\epsilon}{1 + \eta_h G\epsilon}, \\ I_{BE} &\leq \frac{1}{2}\log_2 \frac{\eta_h G V_A + 1 + \eta_h G\epsilon}{\eta_h/[1 - G + G\epsilon + G/(V_A+1)] + 1 - \eta_h}, \end{aligned}}$$

et le débit d'information secrète échangée par symbole est

$$\boxed{\Delta I = \beta I_{AB} - I_{BE}.}$$

La figure 1.18 représente la quantité ΔI lors d'une transmission sur une fibre d'atténuation 0.2 dB/km. Les valeurs des paramètres considérées ici sont celles obtenues sur le système de Jérôme Lodewyck [85] : $\epsilon = 0.06$, $V_A = 40$, $\eta_h = 0.6$ et $\beta = 0.75$. Alice émet par ailleurs ses symboles à un taux d'un mégahertz. Les débits atteignables avec une réconciliation parfaite des variables continues ($\beta = 1$) sont plusieurs ordres de grandeurs au dessus de ceux atteint par les systèmes à photons uniques, mais en pratique l'efficacité des algorithmes est plutôt de l'ordre de 75% et réduit de façon dramatique les débits et distances de transmission réalistes. Le chapitre 4 est entièrement consacré à l'étude de nouveaux algorithmes de réconciliation plus efficaces.

1.4 Conclusion : développements futurs

Longtemps considérée comme une simple curiosité de laboratoire, la distribution quantique de clés est aujourd'hui une discipline mature. Les débits de clés restent cependant encore très faibles comparés aux débits des communications optiques, et pour pallier à ce problème les recherches actuelles s'orientent dans deux directions différentes :

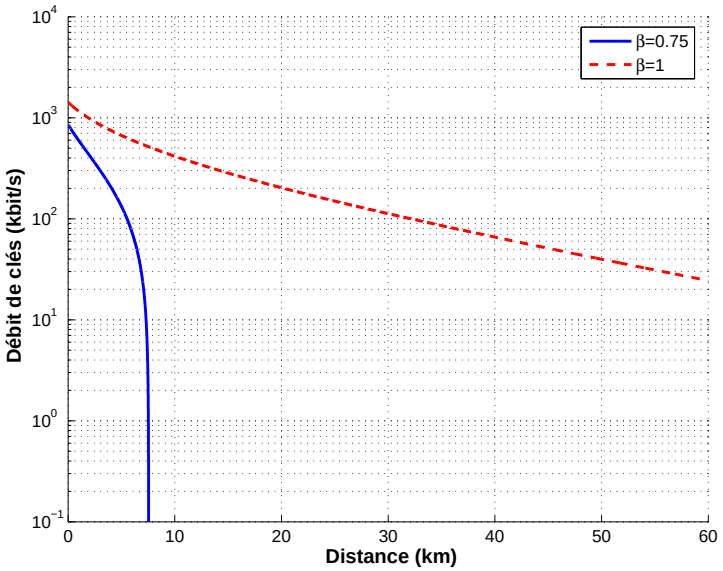


FIG. 1.18 – Débits de clés atteignables avec les protocoles inverses.

– l'amélioration de la technologie : les aspects théoriques et pratiques des systèmes basés sur le protocole BB84 sont parfaitement maîtrisés, les seuls facteurs limitant réellement les débits et les distances de transmission sont les efficacités des sources et détecteurs, ainsi que la stabilité des systèmes ;
– l'étude de nouveaux protocoles : les variables continues sont un exemple de protocole prometteur permettant d'envisager des transmissions très haut débit (plusieurs mégaoctets/s) sur des distances de quelques dizaines de kilomètres.

Chapitre 2

Système de cryptographie quantique par codage en fréquence

Sommaire

Comme nous l'avons présenté dans la section 1.2, les systèmes expérimentaux de cryptographie quantique par photon unique utilisés sur fibre optique, sont généralement basés sur un codage en phase de l'information. Cette solution est plus robuste qu'un codage en polarisation mais ne résout pas pour autant toutes les difficultés techniques. La stabilisation des interféromètres à fibre mis en œuvre dans la plupart des systèmes, peut s'avérer particulièrement délicate sur de longues périodes de temps. De plus, les modulateurs de phase intégrés sont sensibles aux fluctuations de polarisation induites par les contraintes environnementales s'exerçant sur le canal de transmission. Plusieurs solutions basées sur des systèmes de compensation actifs [57] ou sur une astucieuse configuration « plug&play » [55] ont déjà été apportées à ces problèmes. Dans ce chapitre nous présenterons une approche alternative basée sur un codage en fréquence de l'information. Ce travail s'inscrit dans la continuité des thèses effectuées sur ce thème au laboratoire GTL-CNRS Télécom. Bien que l'approche utilisée ici soit fondamentalement différente des travaux précédents, les résultats expérimentaux présentés ont largement bénéficié de l'expérience accumulée depuis 1999.

Ce chapitre s'organise en trois sections. Nous présenterons successivement les outils expérimentaux permettant d'envisager une manipulation en fréquence d'états quantiques

ainsi que les modèles associés, les principes théoriques des systèmes de cryptographie quantique basés sur un codage en fréquence, et les résultats expérimentaux obtenus.

2.1 Manipulation en fréquence d'états quantiques

La « manipulation en fréquence » désigne ici toutes les opérations permettant de modifier les différentes composantes spectrales d'un état quantique, et donc de coder de l'information en utilisant explicitement des modes du champ à différentes fréquences. Nous ne décrirons ici que les opérations aisément réalisables expérimentalement, plus particulièrement avec des composants optiques intégrés utilisés dans les télécommunications optiques.

2.1.1 Outils de la manipulation en fréquence

Sources

Les états quantiques crées expérimentalement ne sont pas stationnaires, et par exemple, au lieu de générer des états de Fock $|\psi\rangle = |1\rangle_{\omega_0}$ et $|\phi\rangle = |1\rangle_{\omega_1}$ parfaitement orthogonaux, une source réelle génère les états :

$$|\psi'\rangle = \int_\omega \xi(\omega-\omega_0) a_\omega^\dagger |0\rangle \quad \text{et} \quad |\phi'\rangle = \int_\omega \xi(\omega-\omega_1) a_\omega^\dagger |0\rangle,$$

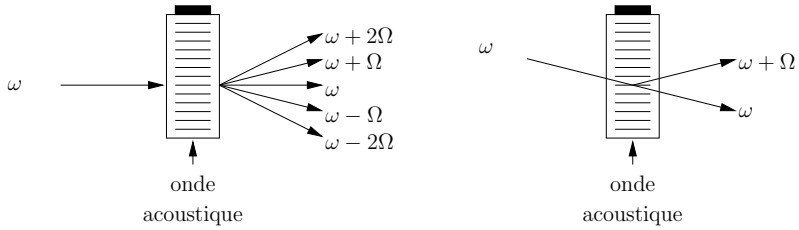
où $a_\omega^\dagger$ est l'opérateur création dans le mode de pulsation ω et $\xi(\omega)$ représente le profil spectral. En général, ces deux états ne sont pas orthogonaux ($\langle\psi'|\phi'\rangle \neq 0$). Néanmoins si l'on considère un profil spectral gaussien :

$$\xi(\omega) = \left(\frac{1}{2\pi\sigma^2}\right)^{1/4} e^{-\frac{\omega^2}{4\sigma^2}},$$

le recouvrement des deux états s'écrit $\langle\psi'|\phi'\rangle = e^{-\frac{(\omega_1-\omega_0)^2}{8\sigma^2}}$. Si la condition $\sigma^2 \ll (\omega_1-\omega_0)^2$ est remplie, il est alors possible de considérer que $\langle\psi'|\phi'\rangle \approx 0$. Les dispositifs expérimentaux présentés dans ce chapitre sont basés sur des états cohérents atténués, générés à partir d'une diode laser de largeur de raie 5 MHz à 1550 nm, pour laquelle la condition précédente est remplie. Nous présenterons donc tous les résultats en considérant que les états sont émis par une source idéale monochromatique. Il n'est par ailleurs pas complètement irréaliste d'envisager des sources de photons quasi-monochromatiques, comme rapporté dans les références [87, 88].

Modulateurs acousto-optique

Le principe de fonctionnement des modulateurs acousto-optiques est illustré figure 2.1. L'effet acousto-optique est obtenu en envoyant une onde ultrasonore (20 kHz à quelques GHz) dans un milieu transparent aux longueurs d'ondes optiques (liquide, solide cristallin ou gaz). En se propageant dans le milieu, l'onde acoustique induit des variation périodiques de l'indice de réfraction, et le matériau se comporte alors comme un réseau de diffraction de pas égal à la longueur d'onde Λ de l'onde acoustique. On distingue deux régimes de fonctionnement limite :



(a) Régime de Raman-Nath (b) Régime de Bragg

FIG. 2.1 – Modulateur acousto-optique.

- Le régime de *Raman-Nath* (figure 2.1(a)) correspond à la situation où le milieu peut être considérée infiniment mince et se comporte comme un masque de phase en déplacement. Il apparaît alors plusieurs ordres de diffraction se propageant dans des directions θ_k données par $\sin\theta_k \approx k\lambda/\Lambda$. Chaque ordre de diffraction est aussi décalé de $k\Omega$ en fréquence.
- Le régime de *Bragg* (figure 2.1(b)) correspond au cas limite d'un réseau épais. Contrairement au régime précédent, il devient nécessaire de prendre en compte les interférences au sein du milieu entre les réflexions partielles de l'onde lumineuse incidente sur les différentes couches d'indice. Lorsque l'angle d'incidence θ de l'onde lumineuse est tel que $\sin\theta = \lambda/(2\Lambda)$ (angle de Bragg), il n'apparaît alors qu'un seul ordre de diffraction.

Un modulateur acousto-optique dans le régime de Raman-Nath présente peu d'intérêt pour notre application en raison du grand nombre de modes fréquentiels et spatiaux apparaissant en sortie ; mais en revanche, il est tout à fait réaliste de recombiner les deux modes apparaissant en régime de Bragg à l'aide d'un coupleur 2 :1.

Dans ce dernier cas, la description quantique de l'effet acousto-optique peut être obtenue de manière simple en considérant une interaction photon-phonon. Un phonon est une particule fictive représentant l'oscillation du réseau créée par l'onde acoustique et qui possède une énergie E_a et un moment cinétique $\mathbf{p}_a$ définis par :

$$E_a = \hbar\Omega \quad \text{et} \quad \mathbf{p}_a = \hbar\mathbf{k}_a,$$

où $\mathbf{k}_a$ est le vecteur d'onde et Ω la fréquence de l'onde acoustique. L'effet acousto-optique est alors le résultat de deux phénomènes :

- la collision (supposée élastique) d'un photon à la fréquence ω_0 et d'un phonon, qui s'annihilent pour créer un photon dans le mode diffracté à la fréquence $\omega_0 + \Omega$.
- l'annihiliation d'un photon à la fréquence $\omega_0 + \Omega$, qui crée un phonon et un photon dans le mode non diffracté à la fréquence ω_0.

Comme pour des photons, il est possible d'introduire des opérateurs annihilation et création de phonon, respectivement notés a_Ω et $a_\Omega^\dagger$. En supposant le système sans pertes, l'Hamiltonien s'écrit alors :

$$\mathcal{H} = \underbrace{\hbar\omega_0 a_{\omega_0}^\dagger a_{\omega_0} + \hbar\left(\omega_0+\Omega\right) a_{\omega_0+\Omega}^\dagger a_{\omega_0+\Omega} + \hbar\Omega a_\Omega^\dagger a_\Omega}_{\mathcal{H}_0} + \underbrace{g a_\Omega a_{\omega_0} a_{\omega_0+\Omega}^\dagger + g^* a_\Omega^\dagger a_{\omega_0}^\dagger a_{\omega_0+\Omega}}_{\mathcal{H}_{\text{eff}}},$$

où g est une constante paramétrant l'interaction. Le terme $\mathcal{H}_{\text{eff}}$ représente uniquement la contribution de l'interaction, le terme $\mathcal{H}_0$ représente lui l'énergie libre des photons et

phonons. L'évolution des différents opérateurs dans le temps s'obtient en résolvant les équations d'Heisenberg :

$$\frac{d}{dt}a_\omega = \frac{1}{j\hbar}[a_\omega, \mathcal{H}] \quad \text{pour} \quad \omega \in \{\Omega, \omega_0, \omega_o + \Omega\}\,.$$

En introduisant les opérateurs $\hat{\mathcal{A}}_\omega = a_\omega e^{i\omega t}$, les équations se simplifient :

$$\frac{d}{dt}\hat{\mathcal{A}}_\omega = \frac{1}{j\hbar}\left[\hat{\mathcal{A}}_\omega, \mathcal{H}_{\text{eff}}\right] \quad \text{pour} \quad \omega \in \{\Omega, \omega_0, \omega_o + \Omega\}\,.$$

Puisqu'en pratique l'énergie transportée par l'onde acoustique est bien supérieure à celle d'un phonon unique, on peut considérer qu'elle se comporte comme une onde classique. Les opérateurs $\hat{\mathcal{A}}_\Omega$ et $\hat{\mathcal{A}}_\Omega^\dagger$ peuvent alors être remplacés par des constantes complexes β et β^*. En notant $m = |g\beta|$ et $\phi = \arg(g\beta)$, le système de deux équations restant se résout aisément :

$$\begin{aligned}\hat{\mathcal{A}}_{\omega_0}(t) &= \cos\left(\tfrac{mt}{\hbar}\right)\hat{\mathcal{A}}_{\omega_0}(0) - e^{-j(\phi-\pi/2)}\sin\left(\tfrac{mt}{\hbar}\right)\hat{\mathcal{A}}_{\omega_0+\Omega}(0),\\ \hat{\mathcal{A}}_{\omega_0+\Omega}(t) &= \cos\left(\tfrac{mt}{\hbar}\right)\hat{\mathcal{A}}_{\omega_0+\Omega}(0) + e^{j(\phi-\pi/2)}\sin\left(\tfrac{mt}{\hbar}\right)\hat{\mathcal{A}}_{\omega_0}(0).\end{aligned}$$

L'interaction lors du passage dans un modulateur acousto-optique n'a lieu que pendant une durée finie t_0, et les opérateurs $\mathcal{A}_\omega(t_0) = \mathcal{A}_\omega^{out}$ obtenus en sortie sont donc reliés aux opérateurs $\mathcal{A}_\omega(0) = \mathcal{A}_\omega^{in}$ en entrée par :

$$\boxed{\begin{aligned}\hat{\mathcal{A}}_{\omega_0}^{out} &= \cos(\theta)\,\hat{\mathcal{A}}_{\omega_0}^{in} - e^{-j(\phi-\pi/2)}\sin(\theta)\,\hat{\mathcal{A}}_{\omega_0+\Omega}^{in},\\ \hat{\mathcal{A}}_{\omega_0+\Omega}^{out} &= \cos(\theta)\,\hat{\mathcal{A}}_{\omega_0+\Omega}^{in} + e^{j(\phi-\pi/2)}\sin(\theta)\,\hat{\mathcal{A}}_{\omega_0}^{in},\end{aligned}}$$

avec $\theta = mt_0/\hbar$. Le système se comporte donc de façon similaire à une lame séparatrice dont les coefficients de réflexion et transmission ainsi que le déphasage, sont contrôlés par l'amplitude de l'onde acoustique.

Filtres optiques : cavité Fabry-Perot et filtre de Bragg

Une cavité Fabry-Perot massive (encore appelée filtre ou interféromètre de Fabry-Perot) est constituée de deux miroirs plans partiellement réfléchissants, séparés d'une distance $L/2$. Une onde électromagnétique envoyée sur ce dispositif subit des réflexions multiples entre les miroirs et peut interférer constructivement ou destructivement. Le Fabry-Perot se comporte donc comme un filtre, transmettant certaines fréquences et réfléchissant les autres. Ce filtre est caractérisé par son intervalle spectral libre $\text{ISL} = c/L$, qui est la distance entre deux pics de transmission, et sa finesse $F = \Delta\nu/\text{ISL}$, qui est la largeur spectrale à mi-hauteur des pics de transmission $\Delta\nu$ ramenée à l'ISL. Plus la finesse est élevée, plus le filtre sera sélectif. La fonction de transfert exacte de la cavité dépend des coefficients de transmission et réflexion des miroirs. En faisant varier la distance entre les miroirs, par exemple en montant ces derniers sur des cales piézo-électriques, les pics des transmissions balaient le spectre optique. En détectant la puissance en sortie de la cavité et en visualisant le signal électrique sur un oscilloscope, on peut donc observer le spectre d'un signal optique.

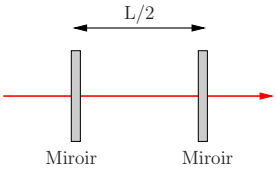


FIG. 2.2 – Cavité Fabry-Perot.

Les principaux inconvénients de ces cavités massives sont leur grande sensibilité aux vibrations mécaniques et leur encombrement. Dans les systèmes de communication optique, on leur préfère les réseaux de Bragg (aussi appelés filtres de Bragg), qui permettent d'effectuer un filtrage selon le même principe, mais qui sont parfaitement intégrés [89]. Un filtre de Bragg est une fibre optique dans laquelle l'indice de réfraction du coeur est perturbé de façon quasi-périodique. Un mode du champ électromagnétique qui se propage est alors réfléchi par les couches successives d'indice. Les longueurs d'onde pour lesquelles ces réflexions donnent lieu à des interférences constructives sont réfléchies tandis que toutes les autres sont transmises. Comme indiqué sur la figure 2.3, les signaux réfléchis et transmis peuvent être récupérés en associant le filtre à un circulateur. Deux réseaux de Bragg

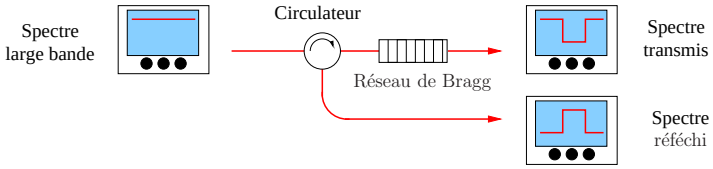


FIG. 2.3 – Filtre de Bragg associé a un circulateur.

peuvent être associés pour former une cavité Fabry-Perot sur fibre, et réaliser ainsi des filtres optiques possédant une bande passante très étroite (de l'ordre de la centaine de MHz).

Du point de vue quantique, les filtres optiques se modélisent comme un système à deux entrées et deux sorties, représenté figure 2.4. En supposant le filtre sans perte et en

FIG. 2.4 – Modèle quantique d'un filtre optique.

notant $r(\omega)$ et $t(\omega)$ ses fonctions de transfert en réflexion et transmission, les opérateurs annihilation à la pulsation ω en entrée et sortie sont reliés de la façon suivante [90] :

$$a_\omega^{out,1} = t(\omega)a_\omega^{in,1} + r(\omega)a_\omega^{in,2},$$

$$a_\omega^{out,2} = t(\omega)a_\omega^{in,2} + r(\omega)a_\omega^{in,1}.$$

2.1.2 Modélisation quantique d'un modulateur électro-optique

Lorsqu'un milieu diélectrique est soumis à un champ électrique $\mathbf{E}(\mathbf{r},t)$, les charges liées se déplacent hors des positions d'équilibre et font apparaître des moments dipolaires élémentaires $\mathbf{p}(\mathbf{r},t)$. Le moment dipolaire moyen induit par unité de volume est appelé le champ de polarisation macroscopique $\mathbf{P}(\mathbf{r},t)$. Nous supposerons dans la suite que la réponse du milieu peut être considérée comme instantanée. Dans un milieu linéaire, la polarisation est proportionnelle au champ incident :

$$\mathbf{P}(\mathbf{r},t) = \epsilon_0 \chi^{(1)} \mathbf{E}(\mathbf{r},t),$$

où $\chi^{(1)}$ est un scalaire appelé susceptibilité linéaire. Dans un milieu non linéaire, la polarisation résulte de termes d'ordre plus élevé du champ électrique :

$$\mathbf{P}(\mathbf{r},t) = \epsilon_0 \big(\chi^{(1)} \mathbf{E}(\mathbf{r},t) + \chi^{(2)} \mathbf{E}^2(\mathbf{r},t) + \chi^{(3)} \mathbf{E}^3(\mathbf{r},t) + \ldots\big),$$

où les susceptibilités non linéaires $\chi^{(i)}$ sont des tenseurs d'ordre i. Dans certains milieux présentant une susceptibilité d'ordre 2 non nulle (tels que le Niobate de Lithium ($LiNbO_3$)), l'application d'un champ électrique quasi-statique[1] $\mathbf{E}_e$ lors de la propagation d'une onde optique $\mathbf{E}_o$ fait apparaître un terme $\chi^{(2)}\mathbf{E}_e\mathbf{E}_o$ dans la polarisation. Ce phénomène appelé *effet électro-optique linéaire* peut s'interpréter comme une modulation de l'indice du milieu par le champ électrique $\mathbf{E}_e$, et permet de moduler la phase de l'onde optique. Une description complète et rigoureuse de cet effet peut être trouvée dans la référence [91].

Comme dans le cas des modulateurs acousto-optiques, nous adopterons un modèle simplifié de l'effet linéaire électro-optique basé sur la création et l'annihilation de photons. La situation considérée ici est celle d'une onde optique à la pulsation ω_0 se propageant dans un modulateur soumis à un champ électrique sinusoïdal de pulsation Ω. Les hypothèses sont alors les suivantes :

- seuls les modes aux pulsations Ω et $\omega_0 + n\Omega$ ($n \in \mathbb{Z}$) interviennent lors des interactions,
- l'onde optique et l'onde électrique se propagent dans la même direction,
- les conditions d'accord de phase nécessaires à la réalisation de phénomènes $\chi^{(2)}$ purement optiques ne sont pas remplies.
- les seules interactions possibles sont :
  1. la collision élastique d'un photon radio-fréquence à la pulsation Ω et d'un photon à la pulsation $\omega_0 + n\Omega$, qui s'annihilent pour créer un photon à la fréquence $\omega_0 + (n+1)\Omega$,
  2. l'annihilation d'un photon à la fréquence $\omega_0+(n+1)\Omega$ donnant lieu à la création d'un photon radio fréquence et d'un photon à la pulsation $\omega_0 + n\Omega$,
- les interactions précédentes ont lieu avec un accord de phase parfait.

En notant $\omega_n = \omega_0 \pm n\Omega$ et $a_n = a_{\omega_n}$ ($n \in \mathbb{Z}$), l'Hamiltonien du système s'écrit :

$$\mathcal{H} = \underbrace{\hbar\Omega a_\Omega^\dagger a_\Omega + \sum_n \hbar\omega_n a_n^\dagger a_n}_{\mathcal{H}_0} + \underbrace{\sum_n \Big(g a_\Omega a_n a_{n+1}^\dagger + g^* a_\Omega^\dagger a_n^\dagger a_{n+1}\Big)}_{\mathcal{H}_{\text{eff}}},$$

[1] Un champ est considéré quasi-statique si sa période d'oscillation est bien supérieure au temps de réponse du milieu.

où g est la constante paramétrant l'interaction non linéaire $\chi^{(2)}$. Comme précédemment, on peut supposer le champ électrique d'intensité classique, introduire les opérateurs $\hat{\mathcal{A}}_n = a_n e^{i\omega_n t}$, puis remplacer $\mathcal{A}_\Omega$ par une constante complexe β. L'évolution du système s'obtient donc en résolvant le système d'équations différentielles :

$$\boxed{\frac{d}{dt}\hat{\mathcal{A}}_n = \frac{1}{j\hbar}\left[\hat{\mathcal{A}}_n, \mathcal{H}_{\text{eff}}\right] \ \forall n \in \mathbb{Z} \quad \text{avec} \quad \mathcal{H}_{\text{eff}} = \sum_n \left(g\beta\hat{\mathcal{A}}_n\hat{\mathcal{A}}_{n+1}^\dagger + (g\beta)^*\hat{\mathcal{A}}_n^\dagger\hat{\mathcal{A}}_{n+1}\right)} \tag{2.1}$$

Bien que ce système contienne une infinité d'équations, il est possible de trouver une solution analytique relativement simple. Comme décrit dans les paragraphes suivants, cette solution s'obtient de façon plus évidente dans le cas de la modulation de photons uniques, et se généralise ensuite au cas de l'équation (2.1).

Modulation de phase de photons uniques

Puisque seuls les modes de pulsation ω_n sont considérés lors de l'interaction dans le modulateur, il est possible d'étudier l'évolution d'un photon unique à la pulsation ω_k ($k \in \mathbb{Z}$) dans la base orthonormale $\{\omega_p\}_{p\in\mathbb{Z}}$, où l'état $|\omega_p\rangle = |1\rangle_{\omega_p}|0\rangle_{\omega\neq\omega_p}$ décrit la présence d'un photon dans le mode de pulsation ω_p. L'état du photon $|\omega_k\rangle$ à un instant t est notée $|\omega_k;t\rangle$, et l'évolution temporelle satisfait l'équation de Schrödinger :

$$j\hbar\frac{d}{dt}|\omega_k;t\rangle \quad = \quad \mathcal{H}|\omega_k;t\rangle.$$

En décomposant $|\omega_k;t\rangle = \sum_p |\omega_p\rangle\langle\omega_p|\omega_k;t\rangle$ dans la base $\{\omega_p\}_{p\in\mathbb{Z}}$, on obtient l'équation vérifiée par chaque composante :

$$\begin{aligned}
\forall p \in \mathbb{Z}, \quad j\hbar\frac{d}{dt}\langle\omega_p|\omega_k;t\rangle &= \langle\omega_p|\mathcal{H}_0 + \mathcal{H}_{\text{eff}}|\omega_k;t\rangle \\
&= \langle\omega_p|\sum_i \mathcal{H}_0 + \mathcal{H}_{\text{eff}}|\omega_i\rangle\langle\omega_i|\omega_k;t\rangle \\
&= \langle\omega_p|\sum_i \langle\omega_i|\omega_k;t\rangle\left(\hbar\omega_i|\omega_i\rangle + g\beta|\omega_{i+1}\rangle + (g\beta)^*|\omega_{i-1}\rangle\right) \\
&= \hbar\omega_p\langle\omega_p|\omega_k;t\rangle + (g\beta)\langle\omega_{p-1}|\omega_k;t\rangle + (g\beta)^*\langle\omega_{p+1}|\omega_k;t\rangle.
\end{aligned}$$

Une solution stationnaire de la forme $\langle\omega_p|\omega_k;t\rangle = \alpha_p(t)e^{-j\omega_p t}$ permet de faire disparaître le premier terme du second membre, et il faut donc trouver les solutions $\alpha_p(t)$ du système d'équations différentielles :

$$\forall p \in \mathbb{Z}, \quad j\hbar\frac{d}{dt}\alpha_p(t) = (g\beta)\,\alpha_{p-1}(t) + (g\beta)^*\alpha_{p+1}(t).$$

En introduisant $|g\beta| = m/2$ et $\arg(g\beta) = \phi$ puis en effectuant le changement de variable $x = mt/\hbar$, les équations s'écrivent :

$$\boxed{\forall p \in \mathbb{Z}, \quad \frac{d}{dx}\alpha_p(x) = \frac{e^{j(\phi-\pi/2)}\alpha_{p-1}(x) - e^{-j(\phi-\pi/2)}\alpha_{p+1}(x)}{2},} \tag{2.2}$$

satisfaisant les conditions initiales $\alpha_k(0) = 1$ et $\alpha_p(0) = 0$ pour $p \neq k$.

On peut remarquer que les fonctions de Bessel de première espèce J_p vérifient des relations similaires à celles de l'équation (2.2). En effet pour $p \geq 0$, les fonctions de Bessel J_p sont reliées aux polynômes de Chebyshev de première espèce T_p par :

$$J_p(x) = j^p T_p\left(j\frac{d}{dx}\right) J_0(x). \tag{2.3}$$

Ces polynômes satisfont par ailleurs les relations de récurrence :

$$\begin{aligned} &T_0 = 1, T_1 = x \\ &\forall p \geq 1, \quad T_{p+1}(x) = 2xT_p(x) - T_{p-1}(x). \end{aligned} \tag{2.4}$$

Cette récurrence peut être étendue à $p \in \mathbb{Z}$ en définissant $T_{-p}(x) = T_p(x)$. Cette extension est cohérente avec la définition de J_p pour $p < 0$ puisque $J_{-p}(x) = j^{-p}T_{-p}\left(j\frac{d}{dx}\right) J_0(x) = (-1)^p J_p(x)$. En combinant les équations (2.4) et (2.3) on obtient finalement la relation de récurrence vérifiée par les fonctions de Bessel :

$$\forall p \in \mathbb{Z} \quad \frac{d}{dx}J_p(x) = \frac{J_{p-1}(x) - J_{p+1}(x)}{2}.$$

On en déduit donc la solution du système d'équations (2.2) :

$$\forall p \in \mathbb{Z} \quad \alpha_p(t) = J_{p-k}\left(\frac{mt}{\hbar}\right) e^{j(p-k)(\phi-\pi/2)},$$

et la forme générale de l'évolution temporelle de l'état initial $|\omega_k\rangle$:

$$\boxed{|\omega_k; t\rangle = \sum_p |\omega_p\rangle J_{p-k}\left(\frac{mt}{\hbar}\right) e^{j(p-k)(\phi-\pi/2)} e^{-j\omega_p t}.} \tag{2.5}$$

Afin d'alléger les notations, les facteurs $e^{-j\omega_p t}$ seront omis par la suite.

Cas général de la modulation de phase

L'opérateur d'évolution temporelle associé à l'Hamiltonien de l'équation (2.1) est noté $\hat{\mathcal{U}}(t)$. Puisque l'Hamiltonien ne dépend pas explicitement du temps et que le vide $|0\rangle$ est un vecteur propre avec pour valeur propre 0, on peut remarquer que :

$$a_k^\dagger(t)|0\rangle = \hat{\mathcal{U}}^\dagger(t)a_k^\dagger(0)\hat{\mathcal{U}}(t)|0\rangle = \hat{\mathcal{U}}^\dagger(t)a_k^\dagger(0)|0\rangle = \hat{\mathcal{U}}(-t)a_k^\dagger(0)|0\rangle = |\omega_k; -t\rangle,$$

et proposer la solution générale du système (2.1) :

$$\boxed{\hat{\mathcal{A}}_k^\dagger(t) = \sum_p J_{p-k}\left(\frac{-mt}{\hbar}\right) e^{j(p-k)(\phi-\pi/2)} \hat{\mathcal{A}}_p^\dagger(0).} \tag{2.6}$$

Cette solution vérifie effectivement les équations du mouvement d'Heisenberg :

$$\begin{aligned}
\frac{1}{j\hbar}\left[\hat{\mathcal{A}}_k^\dagger(t),\mathcal{H}_{\text{eff}}\right] &= \frac{1}{i\hbar}\sum_n\sum_p\left[J_{p-k}\left(\frac{-mt}{\hbar}\right)e^{j(p-k)(\phi-\pi/2)}\hat{\mathcal{A}}_p^\dagger, g\beta\hat{\mathcal{A}}_n\hat{\mathcal{A}}_{n+1}^\dagger + g^*\beta^*\hat{\mathcal{A}}_n^\dagger\hat{\mathcal{A}}_{n+1}\right] \\
&= \frac{1}{j\hbar}\sum_p J_{p-k}\left(\frac{-mt}{\hbar}\right)e^{j(p-k)(\phi-\pi/2)}\left[\hat{\mathcal{A}}_p^\dagger, g\beta\hat{\mathcal{A}}_p\hat{\mathcal{A}}_{p+1}^\dagger + g^*\beta^*\hat{\mathcal{A}}_{p-1}^\dagger\hat{\mathcal{A}}_p\right] \\
&= -\frac{m}{2\hbar}\sum_{p'}\left(J_{p'-1-k}\left(\frac{-mt}{\hbar}\right) - J_{p'+1-k}\left(\frac{-mt}{\hbar}\right)\right)e^{j(p'-k)(\phi-\pi/2)}\hat{\mathcal{A}}_{p'}^\dagger \\
&= \sum_{p'}\frac{d}{dt}\left(J_{p'-k}\left(\frac{-mt}{\hbar}\right)\right)e^{j(p'-k)(\phi-\pi/2)}\hat{\mathcal{A}}_{p'}^\dagger \\
&= \frac{d}{dt}\hat{\mathcal{A}}_k^\dagger(t),
\end{aligned}$$

et les conditions initiales $\hat{\mathcal{A}}_k(t)\Big|_{t=0} = \hat{\mathcal{A}}_k(0)$.

Modulation de phase d'un état cohérent

Afin de vérifier la validité des calculs, on peut appliquer le résultat général précédent à un état cohérent $|\alpha\rangle_k = e^{-\alpha^*\hat{\mathcal{A}}_k+\alpha\hat{\mathcal{A}}_k^\dagger}|0\rangle$ de pulsation ω_k. A l'aide de la formule de Baker-Hausdorff [92] on obtient l'état ayant évolué au cours d'une interaction de durée t :

$$\begin{aligned}
|\alpha;t\rangle_k &= \exp\left(-\alpha^*\hat{\mathcal{A}}_k(-t) + \alpha\hat{\mathcal{A}}_k^\dagger(-t)\right)|0\rangle \\
&= \exp\left\{\sum_p J_{p-k}\left(\frac{mt}{\hbar}\right)\left(-\alpha^* e^{-j(p-k)(\phi-\pi/2)}\hat{\mathcal{A}}_p + \alpha e^{j(p-k)(\phi-\pi/2)}\hat{\mathcal{A}}_p^\dagger\right)\right\}|0\rangle \\
&= \prod_p \exp\left\{J_{p-k}\left(\frac{mt}{\hbar}\right)\left(-\alpha^* e^{-j(p-k)(\phi-\pi/2)}\hat{\mathcal{A}}_p + \alpha e^{j(p-k)(\phi-\pi/2)}\hat{\mathcal{A}}_p^\dagger\right)\right\}|0\rangle \\
&= \bigotimes_p \left|J_{p-k}\left(\frac{mt}{\hbar}\right)\alpha e^{j(p-k)(\phi-\pi/2)}\right\rangle_p . \qquad (2.7)
\end{aligned}$$

Ce résultat est cohérent avec la décomposition en composantes de Fourier d'un champ classique modulé sinusoïdalement en phase :

$$E_0\exp\left[j\pi\frac{V_0}{V_\pi}\cos(\Omega t+\phi)\right] = \sum_n J_n(\pi\frac{V_0}{V_\pi})\exp\left[jn\left(\Omega t+\phi+\pi/2\right)\right].$$

Modulateur d'intensité de type Mach-Zehnder

Comme représenté sur la figure 2.5, un modulateur Mach-Zehnder est un interféromètre équilibré possédant un modulateur de phase dans l'un des bras et un déphasage relatif ψ réglable entre les bras. L'effet de ce composant sur un état quantique s'obtient donc directement à partir des résultats précédents, en particulier un photon unique $|\omega_k\rangle$ et un

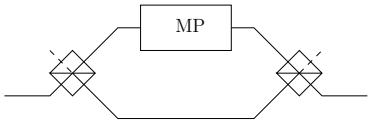


FIG. 2.5 – Modulateur d'intensité.

état cohérent $|\alpha_k\rangle$ à la pulsation ω_k se transforment selon :

$$|\omega_k\rangle \longrightarrow \frac{e^{j\psi} + J_0\left(\frac{mt}{\hbar}\right)}{2}|\omega_k\rangle + \sum_{p\neq k}\frac{J_{p-k}\left(\frac{mt}{\hbar}\right)e^{j(p-k)(\phi-\pi/2)}}{2}|\omega_p\rangle, \tag{2.8}$$

$$|\alpha\rangle_k \longrightarrow \left|\frac{J_0\left(\frac{mt}{\hbar}\right) + e^{j\psi}}{2}\alpha\right\rangle_k \bigotimes_{p\neq k}\left|\frac{J_{p-k}\left(\frac{mt}{\hbar}\right)\alpha e^{j(p-k)(\phi-\pi/2)}}{2}\right\rangle_p. \tag{2.9}$$

2.2 Systèmes de cryptographie par codage fréquentiel

2.2.1 Codage en phase dans le domaine fréquentiel

Les composants décrits dans la section précédente ont déjà été utilisés dans plusieurs expériences de cryptographie quantique [42, 56, 93–97]. Ces systèmes sont les répliques dans le domaine fréquentiel de ceux présentés dans la section 1.2.2, mais offrent certains avantages sur le plan expérimental. Afin de bien souligner la différence avec le système proposé dans la section 2.2.2, nous rappellerons ici brièvement leurs principales caractéristiques.

Codage en phase avec deux interféromètres

Au lieu de coder l'information sur la phase relative de deux impulsions séparées temporellement, on peut envisager d'utiliser la phase relative de deux bandes de fréquence au sein d'une même impulsion [93, 94]. L'équivalent dans le domaine fréquentiel de l'interféromètre déséquilibré réalisant l'opération dans le domaine temporel s'obtient très simplement à l'aide de modulateurs acousto-optiques. En effet, en ajustant l'intensité de l'onde acoustique de pulsation Ω, le modulateur peut se comporter comme une lame séparatrice équilibrée et transformer un photon unique $|\omega\rangle$ de pulsation ω selon :

$$|\omega\rangle \rightarrow \frac{|\omega\rangle + e^{j\phi}|\omega+\Omega\rangle}{\sqrt{2}}.$$

La figure 2.6 représente le système complet mettant en œuvre le protocole BB84. Des interférences à un photon apparaissent au récepteur entre les photons décalés en fréquence soit à l'émetteur, soit au récepteur. Les états $|D_1\rangle$ et $|D_2\rangle$ en sortie de l'interféromètre de Bob s'écrivent :

$$\begin{aligned}|D_1\rangle &= \frac{|\omega\rangle + \left(e^{j\phi_A} - e^{j\phi_B}\right)|\omega+\Omega\rangle - e^{j(\phi_A+\phi_B)}|\omega+2\Omega\rangle}{4},\\ |D_2\rangle &= \frac{|\omega\rangle - \left(e^{j\phi_A} + e^{j\phi_B}\right)|\omega+\Omega\rangle + e^{j(\phi_A+\phi_B)}|\omega+2\Omega\rangle}{4}.\end{aligned}$$

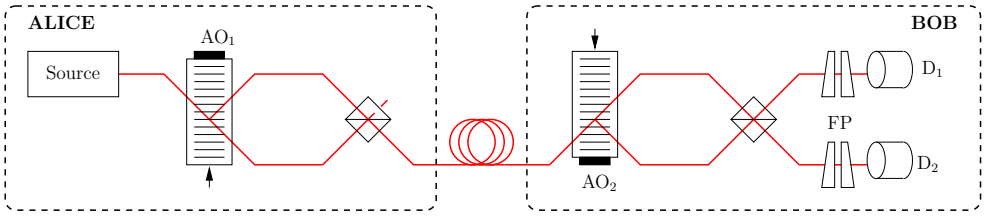


FIG. 2.6 – Mise en œuvre du BB84 avec des modulateurs acousto-optiques.

Contrairement au cas du codage temporel où la discrimination des interférences à un photon pouvait se faire en éliminant les détections en dehors de certaines fenêtre temporelles, il est ici nécessaire d'introduire un filtre optique avant les compteurs de photon pour ne sélectionner que la pulsation $\omega + \Omega$. Les fréquences typiques utilisées dans les modulateurs acousto-optiques sont de l'ordre de la dizaine ou centaine de MHz, ce qui nécessite des filtres optiques étroits, obtenus par exemple avec une cavité Fabry-Perot. Ces filtres sont cependant sensibles aux vibrations mécaniques et aux fluctuations thermiques, et bien que ce système soit réalisable en laboratoire, son utilisation sur une fibre déployée semble peu réaliste.

Système par modulation en bande latérale unique

L'utilisation de modulateurs électro-optiques pouvant être modulés à plus haute fréquence (quelques GHz) simplifie le filtrage et permet donc de pallier en partie aux inconvénients du système précédent. Comme décrit dans la section 2.1.2, les modulateurs électro-optiques génèrent cependant une infinité de fréquences dans le même mode spatial, et ne peuvent donc pas être utilisés dans la même configuration que les modulateurs acousto-optiques. Une approche possible consiste alors à coder l'information dans des bandes latérales de modulation [42]. La mise œuvre de ce codage repose sur les deux constatations suivantes :

1. En contrôlant un modulateur électro-optique avec un champ de faible intensité, seules les premières bandes latérales de modulation sont d'intensité non-négligeable, voir l'équation (2.1). La phase relative de ces bandes latérales par rapport au mode fondamental permet de coder l'information.
2. En effectuant une modulation appropriée au récepteur, il est possible d'obtenir des interférences complémentaires dans les deux bandes latérales.

Un des schémas possibles du système développé selon ce principe au laboratoire GTL-CNRS Telecom [42, 56, 95–97] est représenté figure 2.7. A l'émetteur, Alice envoie une

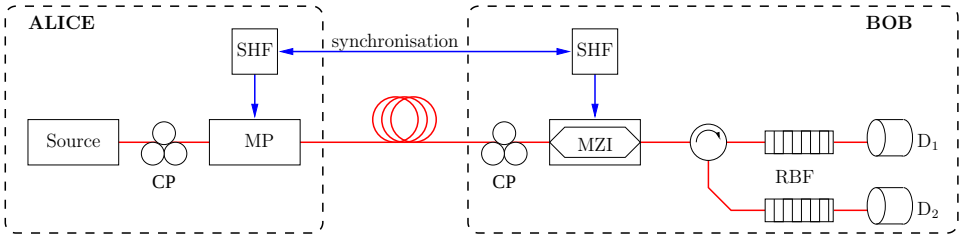


FIG. 2.7 – Système de cryptographie quantique par modulation en bande latérale unique.

impulsion laser (représentée par l'état cohérent $|\alpha\rangle_{\omega_0}$) de pulsation ω_0 dans un modulateur de phase, lequel est contrôlé par un signal modulant $V_0\cos(\Omega t+\phi_A+\pi/2)$ de faible amplitude. En reportant la condition $mt/\hbar=\pi V_0/V_\pi=a\ll 1$ dans l'équation (2.9), l'état émis s'écrit en première approximation :

$$|\phi_A\rangle=\left|-a\alpha e^{-j\phi_A}\right\rangle_{\omega_0-\Omega}\otimes|\alpha\rangle_{\omega_0}\otimes\left|a\alpha e^{j\phi_A}\right\rangle_{\omega_0+\Omega}.$$

L'atténuateur variable ajuste la puissance en sortie de manière à ce qu'il y ait en moyenne moins d'un photon par impulsion dans les bandes latérales.

Au récepteur l'état est modulé par un modulateur d'intensité Mach-Zehnder, contrôlé par un signal sinusoïdal $a\cos(\Omega t+\phi_B)$. En négligeant de nouveau les bandes latérales d'ordre supérieur à deux dans l'équation (2.9), on obtient l'état en sortie du Mach-Zehnder :

$$|\phi_A,\phi_B\rangle=\left|-a\alpha e^{-j\phi_A}\frac{1+e^{j\psi}}{2}-ja\alpha e^{-j\phi_B}\right\rangle_{\omega_0-\Omega}\otimes\left|\frac{1+e^{j\psi}}{2}\alpha\right\rangle_{\omega_0}\otimes\left|a\alpha e^{j\phi_A}\frac{1+e^{j\psi}}{2}-ja\alpha e^{j\phi_B}\right\rangle_{\omega_0+\Omega}.$$

Le biais du modulateur Mach-Zehnder permet de modifier la valeur du déphasage ψ. En particulier pour $\psi=\pi/2$ l'équation précédente devient :

$$|\phi_A,\phi_B\rangle=\left|-ja\alpha\left[e^{-j\phi_A}+e^{-j\phi_B}\right]\right\rangle_{\omega_0-\Omega}\otimes\left|\frac{1+e^{j\psi}}{2}\alpha\right\rangle_{\omega_0}\otimes\left|ja\alpha\left[e^{j\phi_A}-e^{j\phi_B}\right]\right\rangle_{\omega_0+\Omega}.$$

Les intensités des deux bandes latérales évoluent de façon complémentaire en fonction du déphasage, et permettent donc de mettre en œuvre un protocole similaire au BB84. La dénomination « bande latérale unique » du système vient du fait que les détections non-ambigües de Bob n'ont lieu que lorsque l'intensité d'une des deux bandes latérales s'annule. Plusieurs caractéristiques techniques du dispositif méritent d'être soulignées :

- L'utilisation d'une source idéale de photon unique n'est pas envisageable. En effet la majeure partie de l'intensité de l'état initial reste concentrée dans la bande centrale de fréquence ω_0 et ne donne pas lieu à des interférences. En d'autres termes un photon crée par Alice n'aurait qu'une probabilité très faible de coder de l'information.
- Il est crucial que l'oscillateur électrique de Bob soit synchronisé avec celui d'Alice.
- La dispersion du canal de transmission est à l'origine de fluctuations de la phase relative entre les différentes bandes de fréquence. Cependant si Alice transmet à Bob une seconde porteuse optique, modulée à la même fréquence que le signal et séparée de quelques nanomètres, le signal récupéré par Bob sert non seulement de synchronisation mais permet en plus de compenser les effets de la dispersion chromatique de la fibre [56].
- La bande centrale joue exactement le rôle de la référence introduite par Huttner et ses collaborateurs [41]. Le système de codage à bande latérale unique hérite donc de toutes les propriétés du protocole 4+2, en particulier de la sécurité vis-à-vis des attaques PNS.
- Le modulateur de Bob est sensible à la polarisation de l'état reçu, mais comme nous le verrons dans la section suivante cette dépendance peut être éliminée.

L'avantage majeur de ce dispositif est de ne pas nécessiter explicitement d'interféromètre[2] et d'être donc peu sensible aux fluctuations de température et aux vibrations.

[2]Le modulateur de Mach-Zehnder utilisé par Bob joue tout de même le rôle d'un interféromètre intégré.

2.2.2 Codage en fréquence

Le schéma de principe du dispositif expérimental permettant de réaliser une distribution de clé quantique à l'aide d'un véritable codage en fréquence est représenté figure 2.8. Bien qu'il soit peu probable que des sources de photon unique haut-débit et monochromatiques voient le jour avant plusieurs années, il est tout de même intéressant de décrire le comportement idéal qu'aurait ce système avec de telles sources.

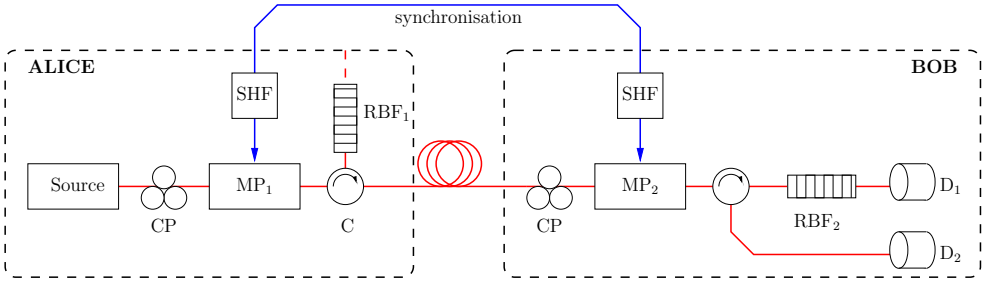


FIG. 2.8 – Principe du montage réalisant le codage en fréquence.

Nous supposerons dans un premier temps que tous les composants sont parfaits. A l'émetteur, les photons de pulsation ω_0 émis par la source de photon unique sont envoyés à travers un modulateur de phase (MP_1). Ce dernier est contrôlé par une tension sinusoïdale de pulsation $\Omega \ll \omega_0$. Le signal optique modulé est finalement filtré à l'aide d'un réseau de Bragg fibré (RBF_1) et d'un circulateur (C_1) ne sélectionnant que les pulsations ω_0 et $\omega_0 \pm \Omega$. En reprenant le résultat de l'équation (2.5) et en supposant le filtrage parfait, ce dispositif permet de créer tout état (normalisé) $|a,\theta\rangle$ de la forme :

$$|a,\theta\rangle = \frac{J_0(a)|1\rangle_{\omega_0} + J_1(a)e^{j\theta}|1\rangle_{\omega_0+\Omega} + J_{-1}(a)e^{-j\theta}|1\rangle_{\omega_0-\Omega}}{\sqrt{J_0(a)^2 + 2J_1(a)^2}},$$

où a est proportionnel à l'amplitude du signal électrique appliqué, et θ est la phase de ce même signal. Si ρ est la matrice densité des états en sortie du dispositif, la fidélité $\mathcal{F} = \langle a,\theta|\rho|a,\theta\rangle$ s'écrit :

$$\mathcal{F}(a) = J_0(a)^2 + 2J_1(a)^2.$$

$\mathcal{F}(a) < 1$ pour $a > 0$, puisqu'un photon peut alors être décalé en fréquence en dehors de la bande passante du filtre RBF_1 avec une probabilité non nulle. Alice peut en particulier générer les quatre états suivants :

$$\begin{aligned}
|+,1\rangle &= |a_0,0\rangle = \frac{1}{\sqrt{2}}|1\rangle_{\omega_0} + \frac{1}{2}|1\rangle_{\omega_0+\Omega} - \frac{1}{2}|1\rangle_{\omega_0-\Omega},\\
|-,1\rangle &= |a_0,\pi\rangle = \frac{1}{\sqrt{2}}|1\rangle_{\omega_0} - \frac{1}{2}|1\rangle_{\omega_0+\Omega} + \frac{1}{2}|1\rangle_{\omega_0-\Omega},\\
|+,2\rangle &= |0,0\rangle = |1\rangle_{\omega_0},\\
|-,2\rangle &= |a_1,0\rangle = \frac{1}{\sqrt{2}}|1\rangle_{\omega_0+\Omega} - \frac{1}{\sqrt{2}}|1\rangle_{\omega_0-\Omega},
\end{aligned} \tag{2.10}$$

où les paramètres $a_0 \approx 1.161$ et $a_1 \approx 2.405$ sont choisis de telle sorte que $J_0(a_0) = \sqrt{2}J_1(a_0)$ et $J_0(a_1) = 0$. Bien que ces états appartiennent à un espace de dimension trois,

$\{|+;1\rangle, |-;1\rangle\}$ et $\{|+;2\rangle, |-;2\rangle\}$ forment deux bases incompatibles d'un sous-espace de dimension deux, et peuvent donc être utilisés pour mettre en œuvre un codage de type BB84. Le BB84 impose cependant l'émission des 4 états avec des probabilités uniformes, alors que les fidélités obtenues ici ne sont pas identiques :

$$\boxed{\begin{array}{l}\mathcal{F}(a_0) = J_0(a_0)^2 + 2J_1(a_0)^2 \approx 0.953,\\ \mathcal{F}(0) = J_0(0)^2 + 2J_1(0)^2 = 1,\\ \mathcal{F}(a_1) = 2J_1(a_1)^2 \approx 0.539.\end{array}} \tag{2.11}$$

Alice doit donc biaiser sa statistique d'émission et tenter d'émettre les états précédents avec les probabilités suivantes :

$$\boxed{\begin{array}{l}\mathrm{P}\,[+;1] = \mathrm{P}\,[-;1] = 0.212,\\ \mathrm{P}\,[+;2] = 0.202,\\ \mathrm{P}\,[-;2] = 0.374.\end{array}} \tag{2.12}$$

Tous les états sont alors effectivement transmis à Bob avec une probabilité uniforme $p = 0.202$, et la probabilité totale qu'a donc Alice de coder son information est de 80%.

Au récepteur, Bob devrait pouvoir projeter l'état qu'il reçoit dans l'une des deux bases $\{|+;1\rangle, |-;1\rangle\}$ ou $\{|+;2\rangle, |-;2\rangle\}$, mais ces opérations ne sont malheureusement pas réalisables de manière simple expérimentalement. Le système de réception représenté figure 2.8 permet cependant de les effectuer approximativement et n'introduit que peu d'erreurs. Ce dispositif est constitué d'un second modulateur de phase (MP_2), contrôlé par un signal électrique d'amplitude $a'V_\pi/\pi$ et de de phase θ' synchronisé avec celui d'Alice, suivi par un circulateur C_2 et un réseau de Bragg (RBF_2) réfléchissant le contenu de la bande de fréquence ω_0 vers le détecteur D_2, et transmettant toutes les autres composantes spectrales vers le détecteur D_1. La remodulation d'un état $|a,\theta\rangle$ produit un nouvel état donné par :

$$\frac{\sum_p \left[J_0(a)J_p(a')e^{jp\theta'} + J_1(a)J_{p-1}(a')e^{j(\theta+(p-1)\theta')} + J_{-1}(a)J_{p+1}(a')e^{j(-\theta+(p+1)\theta')}\right]|1\rangle_{\omega_0+p\Omega}}{\sqrt{J_0(a)^2 + 2J_1(a)^2}},$$

et les détecteurs D_2 et D_1 se déclenchent avec les probabilités :

$$\begin{aligned}\mathrm{P}_2 &= \frac{1}{J_0(a)^2 + 2J_1(a)^2}\left|J_0(a)J_0(a') - J_1(a)J_1(a')\left[e^{j(\theta-\theta')} + e^{-j(\theta-\theta')}\right]\right|^2,\\ \mathrm{P}_1 &= 1 - \mathrm{P}_2.\end{aligned}$$

Puisque les états $|\pm;2\rangle$ ne contiennent pas les mêmes composantes spectrales, le filtrage seul suffit à les discriminer et il n'est pas nécessaire de moduler ($a' = 0$, $\theta' = 0$). La discrimination des états $|\pm;1\rangle$ ne peut elle se faire qu'approximativement en choisissant $a' = a_0$ et $\theta' = 0$. En effet, si l'état $|+;1\rangle$ ($a = a_0$, $\theta = 0$) est reçu, on a :

$$\begin{aligned}\mathrm{P}_2 &= \frac{1}{J_0(a_0)^2 + 2J_1(a_0)^2}\left|J_0(a_0)^2 - 2J_1(a_0)^2\right|^2 = 0,\\ \mathrm{P}_1 &= 1,\end{aligned}$$

et dans le cas de l'état $|-;1\rangle$ ($a = a_0$, $\theta = \pi$) :

$$\begin{aligned} \mathrm{P}_2 &= \frac{1}{J_0(a_0)^2 + 2J_1(a_0)^2}\left|J_0(a_0)^2 + 2J_1(a_0)^2\right|^2 \approx 0.953, \\ \mathrm{P}_1 &\approx 0.047, \end{aligned}$$

Les probabilités de déclenchement sur chaque détecteur dans toutes les configurations sont résumées dans le tableau 2.1.

Etat émis	a' ($\theta' = 0$)	P_1	P_2
$\|+;1\rangle$	0	0.5	0.5
	a_0	1	0
$\|-;1\rangle$	0	0.5	0.5
	a_0	0.047	0.953
$\|+;2\rangle$	0	1	0
	a_0	0.523	0.477
$\|-;2\rangle$	0	0	1
	a_0	0.523	0.477

TAB. 2.1 – Probabilités de détection des états émis par Alice.

On constate que la mesure de Bob introduit en moyenne 1.2% d'erreurs, même lorsque les composants sont supposés idéaux[3]. Cette augmentation indésirable du QBER ne devrait cependant pas affecter dramatiquement la sécurité du dispositif puisqu'elle n'est créée qu'à la réception et que l'on peut raisonnablement supposer que le dispositif de Bob n'est pas sous le contrôle d'Eve. De plus Alice et Bob peuvent vérifier les statistiques de détection dans toutes les configurations, y compris lorsque leur bases sont incompatibles, pour détecter une éventuelle attaque. L'analyse spécifique de la sécurité du systéme est rendue délicate par l'asymétrie de la mesure de Bob (seul l'état $|-;1\rangle$ donne lieu à des détections erronnées), et nous supposerons que les résultats standard obtenus pour le BB84 restent appliquables en prenant en compte l'augmentation du QBER.

Sensibilité à la polarisation

Les modulateurs de phase utilisés dans le dispositif sont sensibles à la polarisation du signal qu'il reçoivent. On pourrait envisager d'insérer un système de compensation actif, utilisant un signal à une autre longueur d'onde pour estimer les variations de polarisation des états transmis, mais une solution plus simple consiste à mettre en œuvre le dispositif représenté figure 2.9. Le signal reçu est projeté sur deux polarisations orthogonales à l'aide d'une lame séparatrice de polarisation (LSP_1). Chacun des signaux en sortie possède ainsi une polarisation parfaitement définie et indépendante de celle du signal en entrée. Deux modulateurs de phase contrôlés par la même tension effectuent la modulation sur chacune des voies, puis ces dernières sont recombinées sur une seconde lame séparatrice de polarisation (LSP_2) avant filtrage.

[3]On peut vérifier qu'il n'est pas possible d'obtenir un QBER moins élevé avec d'autres jeux de paramètres a' et θ'.

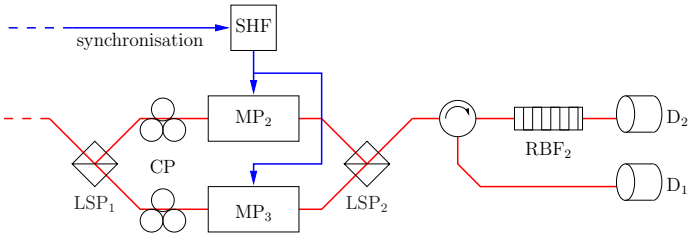


FIG. 2.9 – Récepteur insensible à la polarisation.

Sensibilité à la dispersion

Les calculs des probabilités de déclenchement précédents supposent implicitement que la phase accumulée au cours de la propagation est la même pour toutes les fréquences. Les déphasages sont en réalité différents à cause de la dispersion du milieu, et puisque l'espacement des composantes spectrales considérées sera de l'ordre de la dizaine de GHz, nous étudierons l'influence de la dispersion en nous contentant d'un développement à l'ordre deux de la constante de propagation autour de la pulsation ω_0 :

$$\beta(\omega) = \beta_0 + \beta_1(\omega - \omega_0) + \beta_2(\omega - \omega_0)^2. \tag{2.13}$$

Si un état $|a, \theta\rangle$ est transmis sur une fibre optique de distance L, l'état parvenant à Bob est (au déphasage $e^{j\beta_0 L}$ près) :

$$\frac{J_0(a)|1\rangle_{\omega_0} + J_1(a)e^{j(\theta-\beta_1\Omega L-\frac{\beta_2}{2}\Omega^2 L)}|1\rangle_{\omega_0+\Omega} + J_{-1}(a)e^{-j(\theta-\beta_1\Omega L+\frac{\beta_2}{2}\Omega^2 L)}|1\rangle_{\omega_0-\Omega}}{\sqrt{J_0(a)^2 + 2J_1(a)^2}},$$

et les probabilités de déclenchement après remodulation s'écrivent donc :

$$\begin{aligned} \mathrm{P}_2 &= \frac{1}{J_0(a)^2 + 2J_1(a)^2}\left|J_0(a)J_0(a') - 2J_1(a)J_1(a')e^{-j\frac{\beta_2}{2}\Omega^2 L}\cos\left(\theta - \beta_1\Omega L - \theta'\right)\right|^2, \\ \mathrm{P}_1 &= 1 - \mathrm{P}_2. \end{aligned}$$

Avec une valeur typique de $\beta_2 \approx 2\,10^{-26}$ s^2/m et $\Omega/2\pi < 10$ GHz, on peut considérer que $\frac{\beta_2}{2}\Omega^2 L \approx 0$ si L est inférieur à 100 km. Dans ces conditions, on obtient par exemple lors de la détection de l'état $|+;1\rangle$ avec $a' = a_0$:

$$\mathrm{P}_2 = J_1(a_0)^2(1 - \cos(\beta_1\Omega L - \theta'))^2.$$

Les contraintes environnementales s'exerçant sur la fibre se traduisent par une variation δL de la distance de transmission, qui induit une fluctuation $\delta\mathrm{P}_2$ de la probabilité de détection. La fluctuation maximum est donnée par :

$$\delta\mathrm{P}_2 = 4\beta_1\Omega J_1(a_0)^2\delta L,$$

et avec une valeur typique de $\beta_1 \approx 5\,10^{-9}$ s/m et $\Omega = 8$ GHz, cela signifie qu'il est nécessaire de contrôler δL au dixième de millimètre pour obtenir $\delta\mathrm{P}_2 \approx 1\%$. Un tel système est donc totalement inutilisable, même sur des courtes distances de transmission.

La méthode d'autocompensation développée pour le système par modulation en bande latérale unique [56] permet cependant de limiter l'influence de la dispersion. Le principe

de cette autocompensation est de transmettre un signal classique de référence, modulé en intensité à la pulsation Ω à une longueur d'onde ω_s proche de celle du signal utile. Le champ optique émis peut s'écrire :

$$E_s(t) = E_0 e^{j\omega_s t}(1 + m\cos(\Omega t)).$$

Après avoir parcouru le même trajet que le signal utile, et avoir été lui aussi affecté par la dispersion, le champ de référence au récepteur est :

$$E_s(t) = E_0 e^{j\omega_s t}(1 + m e^{j\frac{\beta_{2,s}}{2}\Omega^2 L}\cos(\Omega t - \beta_{1,s}\Omega L)),$$

où $\beta(\omega) = \beta_{0,s} + \beta_{1,s}(\omega - \omega_s) + \beta_{2,s}(\omega - \omega_s)^2$ est la constante de propagation associée. En détectant ce champ avec une photodiode, on obtient alors un signal électrique $V(t)$:

$$V(t) \propto 1 + 2m\cos(\frac{\beta_2}{2}\Omega^2 L)\cos(\Omega t - \beta_{1,s}\Omega L) + m^2\cos^2(\Omega t - \beta_1\Omega L).$$

La composante de fréquence Ω peut alors être filtrée, amplifiée et utilisée pour effectuer la remodulation du signal au récepteur. Dans ce cas, les probabilités de déclenchement sont :

$$\begin{aligned} \mathrm{P}_2 &= \frac{1}{J_0(a)^2 + 2J_1(a)^2}\left|J_0(a)J_0(a') - 2J_1(a)J_1(a')e^{-j\frac{\beta_2}{2}\Omega^2 L}\cos\left(\theta - (\beta_1 - \beta_{1,s})\Omega L - \theta'\right)\right|^2, \\ \mathrm{P}_1 &= 1 - \mathrm{P}_2. \end{aligned}$$

Comme le signal de référence est à une longueur d'onde proche du signal utile, on peut faire l'approximation :

$$(\beta_1 - \beta_{1,s}) \approx \beta_2(\omega_s - \Omega_0).$$

En détectant l'état $|+;1\rangle$ avec $a' = a_0$, on a cette fois :

$$\begin{aligned} \mathrm{P}_2 &= J_1(a_0)^2(1 - \cos(\beta_2(\omega_s - \omega_0)\Omega L - \theta'))^2, \\ \delta\mathrm{P}_2 &= 4\beta_2(\omega_s - \omega_0)\Omega J_1(a_0)^2\delta L, \end{aligned} \tag{2.14}$$

Si le signal de référence et le signal utile sont séparés de 5 nm, on peut maintenant tolérer une fluctuation δL de l'ordre de la centaine de mètres pour obtenir $\delta\mathrm{P}_2 \approx 1\%$.

2.3 Résultats expérimentaux

2.3.1 Comptage de photons

Nous rappellerons ici brièvement les caractéristiques du compteur de photons qui sera utilisé dans nos expériences. Le module a été réalisé et caractérisé par Alexandre Soujaeff lors de sa thèse. La photodiode est une photodiode à avalanche EPITAXX EPM 239 pouvant fonctionner à des températures comprises entre -60 C et -40 C. Cette gamme de température est atteignable avec un module de refroidissement à effet Peltier, comme indiqué sur le schéma de montage figure 2.10. Une thermistance et un contrôleur « Proportionnel-Intégral-Dérivé » permettent d'asservir la température de la photodiode. Une fois le système stabilisé (après une durée typique de l'ordre de 15 minutes) les fluctuations de température n'excèdent pas ± 0.07 C.

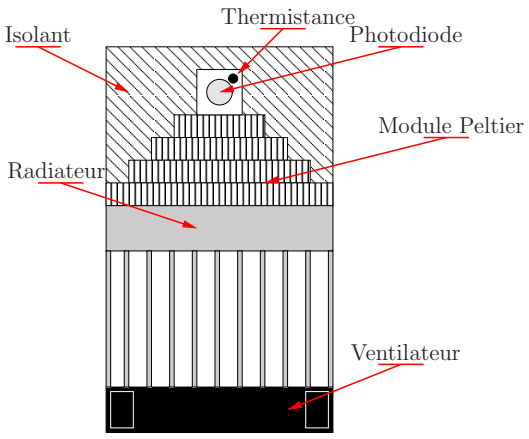


FIG. 2.10 – Système d'asservissement en température du compteur de photons.

Le dispositif fonctionne en mode « fenêtrage actif » (*active gating*) consistant à moduler la tension de polarisation de la diode autour d'une valeur V_p légèrement inférieure à la tension d'avalanche V_a. La modulation est effectuée avec un train d'impulsions de largeur τ , de fréquence de répétition F_{rep} et d'amplitude V_m telle que $V_m + V_p > V_a$. Puisque la photodiode ne réagit à l'arrivée de photons qu'aux instants où la tension de polarisation est supérieure à la tension d'avalanche, les impulsions jouent le rôle de « portes de détection ». Dans la suite du manuscrit, le nombre moyen de photons par impulsion sera évalué en photons par porte de détection. Les caractéristiques typiques du dispositif de comptage sont données dans le tableau 2.2.

Température	-55 C
Tension d'avalanche	$V_a \approx 50$ V
Tensions de polarisation	$V_p = 48$ V
Largeur des impulsions électriques	$\tau = 10$ ns
Fréquence de répétition	$F_{rep} = 200$ kHz
Amplitude des impulsions électriques	$V_m = 2.1$ V
Coups d'obscurité	$4.5\,10^{-6}$ coups par porte de détection
Efficacité de comptage	13%

TAB. 2.2 – Caractéristiques du dispositif de comptage.

Les résultats du comptage sont enregistrés avec une carte compteuse National Instruments et visualisés avec le logiciel Labview.

2.3.2 Validation expérimentale du modèle de modulateur de phase

Afin de valider le modèle de modulateur de phase proposé dans la section 2.1.2, il est nécessaire de vérifier que les amplitudes et déphasages des différentes bandes de fréquence ont bien la dépendance voulue. La réalisation expérimentale du dispositif de cryptographie quantique proposé section 2.2.2 permet d'effectuer une validation partielle, mais nous

avons aussi mesuré l'évolution du taux de comptage de photons en fonction de l'amplitude de la tension de contrôle dans plusieurs bandes de modulation.

Le dispositif expérimental utilisé est représenté figure 2.11, et les caractéristiques détaillées des composants décrites dans le tableau 2.3. La source est un laser fonction-

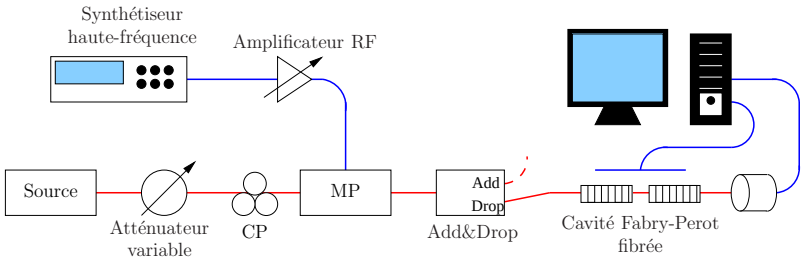


FIG. 2.11 – Mesure des probabilités de détection dans les bandes de modulation.

nant en régime continu à 1547.5 nm, fortement atténué pour n'émettre en moyenne que $\mu = 0.3$ photons par porte de détection. Le modulateur de phase est contrôlé par un signal de fréquence 5 GHz, obtenu en amplifiant la sortie d'un synthétiseur haute fréquence. Les bandes de modulation en sortie du modulateur sont sélectionnées à l'aide d'une cavité Fabry-Perot fibrée, possédant un intervalle spectral libre de 12.5 GHz et une finesse de 100 sur 0.8 nm. La cavité est asservie en température à l'aide d'un module à effet Peltier, ce qui permet d'ajuster la position de la caractéristique du filtre sur quelques nanomètres (le dispositif de contrôle a été réalisé par Frédéric Patois pour le système de modulation par bande latérale unique). De plus, afin d'éviter la détection de photons parasites, un filtre « Add & Drop » est inséré avant la détection. Le spectre en transmission des deux filtres, mesuré à l'analyseur optique APEX avec une résolution de 7 pm, est représenté figure 2.12. Le pic central de la cavité, qui présente environ 2 dB de pertes et une isolation de 35 dB à 6 GHZ, est positionné de manière à transmettre uniquement la bande latérale choisie. Les photons sont finalement détectés avec le dispositif de comptage décrit

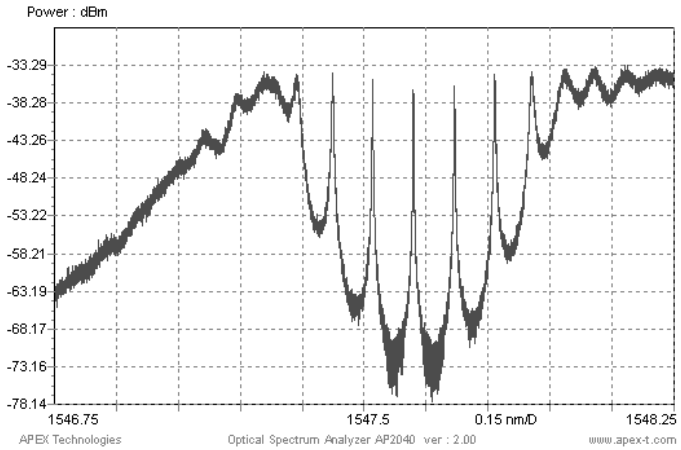


FIG. 2.12 – Spectre en transmission de la cavité Fabry-Perot et du filtre « Add & Drop ».

précédemment, à un taux de 200 kHz et avec des portes de détection de 10 ns.

Les taux de comptage obtenus sur les bandes de modulation d'ordre 0, +1, et +2 en fonction de l'amplitude V (en volts) du signal modulant sont donnés figure 2.13. En théorie

Modulateur de Phase	EOSPACE, bande passante 20 GHz, pertes 1.8 dB, puissance électrique maximum 27 dBm, V_π ≈5.5 V
Amplificateur HF	SHF 100 CP, bande passante 30 kHz-25 GHz, gain 18 dB, puissance maximum en entrée 10 dBm
Cavité Fabry-Perot	BRAGG PHOTONICS, cavité fibrée réalisée avec deux réseaux de Bragg photoinscrits, finesse 100 et intervalle spectral libre 12.5 GHz sur 0.8 nm
Filtre « Add & Drop »	JDS UNIPHASE, sortie « Drop » centrée à 1548.1 nm, bande passante 1 nm, pertes 0.8 dB, isolation 45 dB à 12 GHz
Source	ALCATEL 1905 LMI, accordable autour de 1547 nm, largeur de raie 2 MHz

TAB. 2.3 – Caractéristiques des composants utilisés.

l'intensité de la bande i est $J_i(\pi V/V_\pi)$, mais les mesures expérimentales sont ajustées par une fonction du type :

$$F_i(V) = J_i(\pi \frac{V}{V_\pi})\eta_i + \delta \quad i \in \{0, 1, 2\}$$

Le paramètre η_i représente l'atténuation totale du système (environ 6 dB de pertes, 13% d'efficacité de détection et 0.3 photons par porte) et prend en compte la variation de la transmission du filtre d'une série de mesure à l'autre. La bande passante du pic de transmission de la cavité Fabry-Perot est en effet de l'ordre de 100 MHz, et sa position est extrêmement sensible aux fluctuations de température. Le paramètre δ représente le bruit de détection causé par les coups d'obscurité du compteur de photon, ou la détection de photons à d'autres longueurs d'onde. Les valeurs des paramètres d'ajustement obtenues

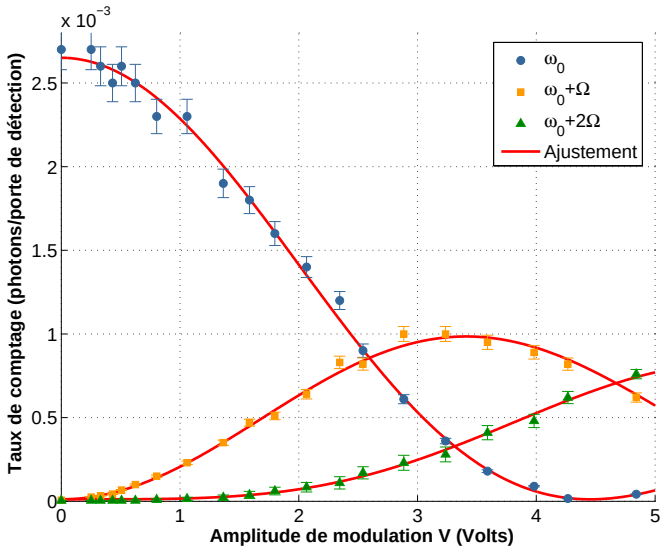


FIG. 2.13 – Nombre de coups de photons par porte de détection dans les bandes latérales de modulation.

en minimisant l'erreur quadratique entre les fonctions F_i et les mesures expérimentales sont :

$$\eta_1 = 2.6\ 10^{-3} \qquad \eta_2 = 2.9\ 10^{-3} \quad \eta_3 = 3.4\ 10^{-3}$$
$$V_\pi = 5.8\ \text{V} \qquad \delta = 1.2\ 10^{-5}$$

Ces résultats s'accordent relativement bien avec les prédictions du modèle et les valeurs des paramètres sont cohérentes avec les caractéristiques du système. On peut aussi constater qu'il est possible de faire disparaître le mode fondamental ω_0 tout en restant dans la plage acceptable de puissance électrique sur l'électrode du modulateur.

2.3.3 Cryptographie quantique par codage en fréquence

Validation de la méthode de codage

Le principe du codage en fréquence a été validé avec le dispositif expérimental de la figure 2.14, similaire au montage de principe de la figure 2.8. Puisque la transmission s'effectue sur quelques dizaines de centimètres, le système d'autocompensation n'est ici pas nécessaire. Comme précédemment, nous utilisons une source monochromatique

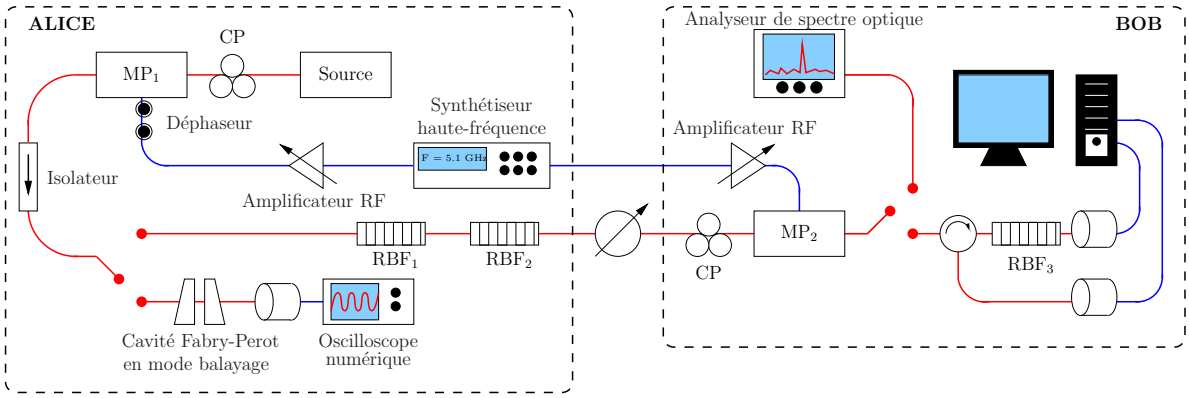
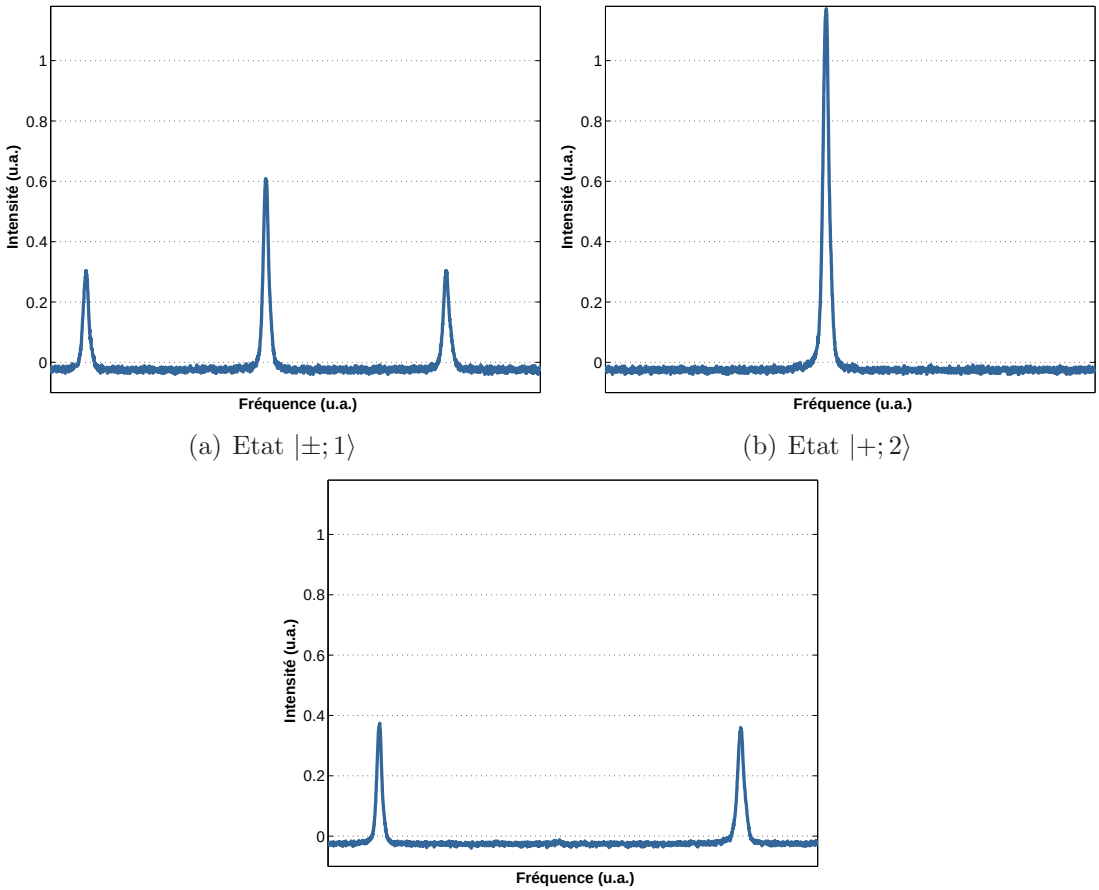


FIG. 2.14 – Montage expérimental de cryptographie quantique par codage en fréquence

à 1547.5 nm en régime continu. Les modulateurs de phase à l'émetteur et au récepteur ont des caractéristiques quasi-identiques, et sont contrôlés par des signaux de fréquence légèrement inférieure à 8 GHz issus d'un même synthétiseur haute-fréquence puis amplifiés. Le déphasage relatif entre ces tensions peut être ajusté manuellement avec des déphaseurs variables. Le filtrage en sortie du modulateur MP_1 est réalisé à l'aide de deux filtres de Bragg (RBF_1 et RBF_2) de 80 pm de bande passante ($\approx$ 10 GHz), positionnés de sorte à réfléchir les bandes de modulation d'ordre 2 et 3. Les bandes de modulation indésirables d'ordre supérieur à 4 sont transmises, mais leurs amplitudes sont négligeables dans la gamme de profondeur de modulation utilisée. La source et le modulateur sont protégés des signaux pouvant être réfléchis à l'aide un isolateur. Le filtrage au récepteur est effectué par un filtre de Bragg (RBF_3) de 80 pm de bande passante. L'isolation supérieure à 40 dB de tous les filtres permet d'obtenir un filtrage quasiment parfait. L'émetteur et le récepteur présentent des pertes similaires d'environ 3.2 dB, qui pourraient être réduite à un peu plus de 2 dB en soudant toutes les fibres.

Pour générer chacun des états, l'amplitude de modulation à l'émetteur est tout d'abord ajustée manuellement en utilisant la source en régime classique (non atténué). La sortie de l'émetteur est dirigée vers une cavité Fabry-Perot en mode balayage, ce qui permet de visualiser rapidement le spectre des signaux émis. Les spectres classiques correspondant à la génération des états de l'équation (2.10) sont représentés figure 2.15. Le spectre des



(a) Etat $|\pm;1\rangle$ (b) Etat $|+;2\rangle$

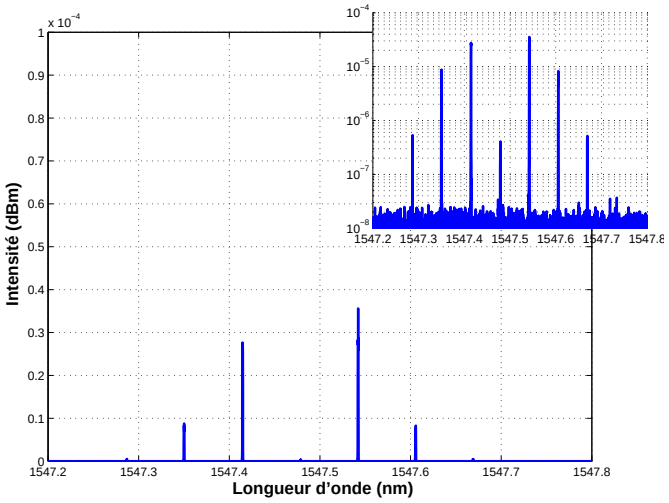
(c) Etat $|-;2\rangle$

FIG. 2.15 – Spectres optiques correspondant à la génération des états quantique.

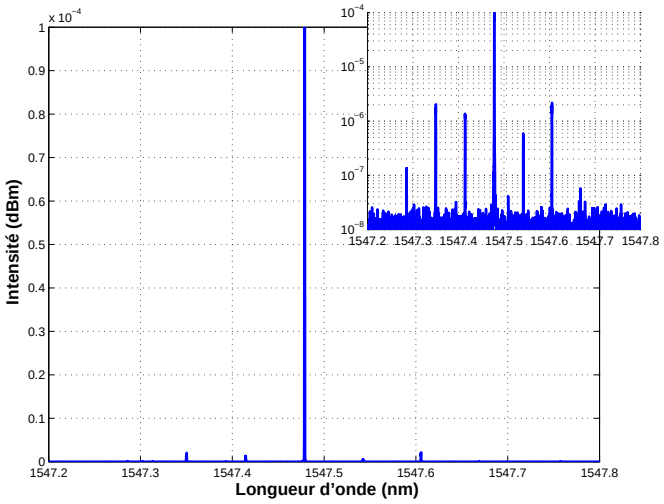
états $|\pm;1\rangle$ fait apparaître un léger déséquilibre des bandes latérales, vraisemblablement dû à la réponse non parfaitement linéaire des cales piézo-électriques modulant la largeur de la cavité.

La différence de phase entre les états $|\pm;1\rangle$ est réglée en reproduisant en régime classique les interférences décrites dans la section 2.2.2. Les spectres des signaux obtenus en sortie du second modulateur sont représentés figure 2.16. Comme précédemment, le déséquilibre entre les bandes latérales supérieures et inférieures est créé par le dispositif de mesure.

Les performances en régime quantique du système ont été évaluées en atténuant la source laser pour obtenir en moyenne $\mu = 0.1$ photon par porte de détection en sortie de l'émetteur. En faisant varier l'atténuation, on peut simuler différentes distances de transmission. Le QBER mesuré pour chacun des états transmis est représenté figure 2.17. Comme nous ne disposions que d'un seul compteur de photon, les mesures ont été prises successivement sur chacune des sorties du dispositif. Le QBER le plus faible est obtenu



(a) Réception de l'état $|+;1\rangle$



(b) Réception de l'état $|-;1\rangle$

FIG. 2.16 – Spectres optiques après modulation au récepteur (échelles linéaires et logarithmiques).

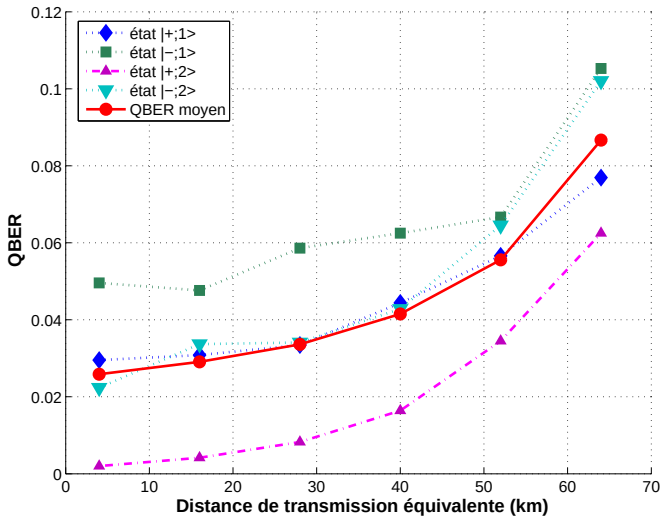


FIG. 2.17 – Evolution du QBER avec la distance de transmission équivalente (pertes de 0.25 dB.km^{-1}).

lors de la transmission de l'état $|+;2\rangle$, pour lequel la transmission et la détection sont purement passives. La transmission des autres états donne lieu à un taux d'erreur plus important, mais laisse tout de même envisager des distances de transmission de quelques dizaines de kilomètres.

Electronique de commande

Afin de réaliser une transmission plus réaliste sur fibre optique, nous avons mis en place un montage électronique piloté par Labview permettant à Alice et Bob de contrôler la phase ou l'amplitude de leurs signaux de modulation. Plutôt que de contrôler directement des signaux à 8 GHz, nous avons choisi de modifier la phase et l'amplitude de signaux à 2 GHz puis d'effectuer une translation de fréquence. Cette solution permet de réduire significativement le coût du système en travaillant dans une bande de fréquence standard (bande GSM) pour laquelle la technologie est parfaitement maîtrisée. Les chaînes de translation de l'émetteur et du récepteur ont été réalisées par Serge Grop lors de son stage de DESS. Les deux montages sont strictement identiques et constitués chacun :

- d'un amplificateur (Mini-Circuits ZX60-2531M) de bande passante $0.5-2.5$ GHz et de 28 dB de gain,
- d'un premier doubleur passif (Mini-Circuits KBA-20) permettant de translater le signal à 2 GHz à 4 GHz fonctionnant pour des puissances d'entrée de 11 à 15 dBm.
- d'un amplificateur (Mini-Circuits ZX60-5916M) de bande passante $1.5-5.9$ GHz et de 18 dB de gain,
- d'un second doubleur passif (MACOM FD93C) réalisant la translation finale à 8 GHz, fonctionnant pour des puissances d'entrée entre 12 et 20 dBm.
- d'un filtre centré autour de 8 GHz permettant de filtrer les harmoniques indésirables apparaissant lors des doublages.

Les spectres du signal électrique mesurés à l'émetteur aux différentes étapes du doublage sont indiqués figure 2.18.

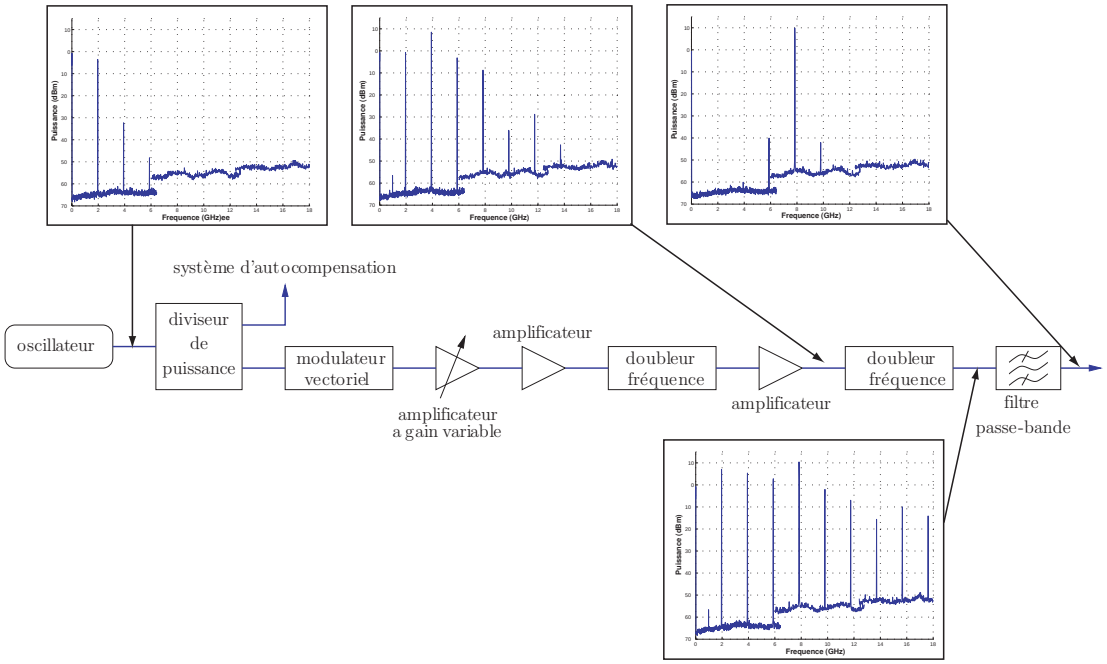


FIG. 2.18 – Montage électronique de commande de l'émetteur.

A l'émetteur, l'ajustement de la phase et de l'amplitude du signal à 2 GHz s'effectue grâce à un modulateur vectoriel (Analog Devices 8341) et d'un amplificateur à gain variable (Analog Devices 5330), pilotés par le logiciel Labview à travers une carte PCI-6711. L'utilisation de ces deux éléments est imposée par la chaîne de doublage qui limite la gamme de puissance utilisable. L'amplificateur à gain variable peu précis mais possédant une grande excursion permet un réglage grossier de l'amplitude du signal, laquelle est ensuite ajustée précisément avec le modulateur vectoriel. La carte PCI-6711 ne génère des signaux analogiques qu'avec une précision de 5 mV, mais permet tout de même de contrôler la phase et la puissance des signaux à 2 GHz avec des précisions respectives de 8 milliradians et 0.01 dBm.

Au récepteur le signal de modulation à 2 GHz obtenu avec le système d'autocompensation doit uniquement être allumé ou éteint ; le basculement entre les deux états est réalisé au moyen d'une bascule pilotable en tension (MACOM SW311). L'ajustement de la puissance se fait à l'aide d'un atténuateur variable manuel.

Transmission sur fibre

Le schéma complet du système de transmission réalisé est représenté figure 2.19. Les seules modifications par rapport à celui utilisé pour la démonstration de principe sont l'ajout de l'électronique de commande, et la mise en place du système d'autocompensation de la dispersion. Afin d'équilibrer plus précisément les sorties du détecteur, nous avons aussi rajouté un isolateur présentant 0.6 dB de pertes. Nous avons testé le système en régime classique, et sur 500 m de fibre optique, en émettant successivement les états $|+;2\rangle$, $|-;2\rangle$, $|+;1\rangle$, et $|-;1\rangle$ à la fréquence de 5 kHz, et en alternant modulation et non-modulation au récepteur à la fréquence de 2.5kHz. La figure 2.20 représente les puissance observées alors sur chacun des détecteur en sortie. Puisque l'on mesure ici des puissances,

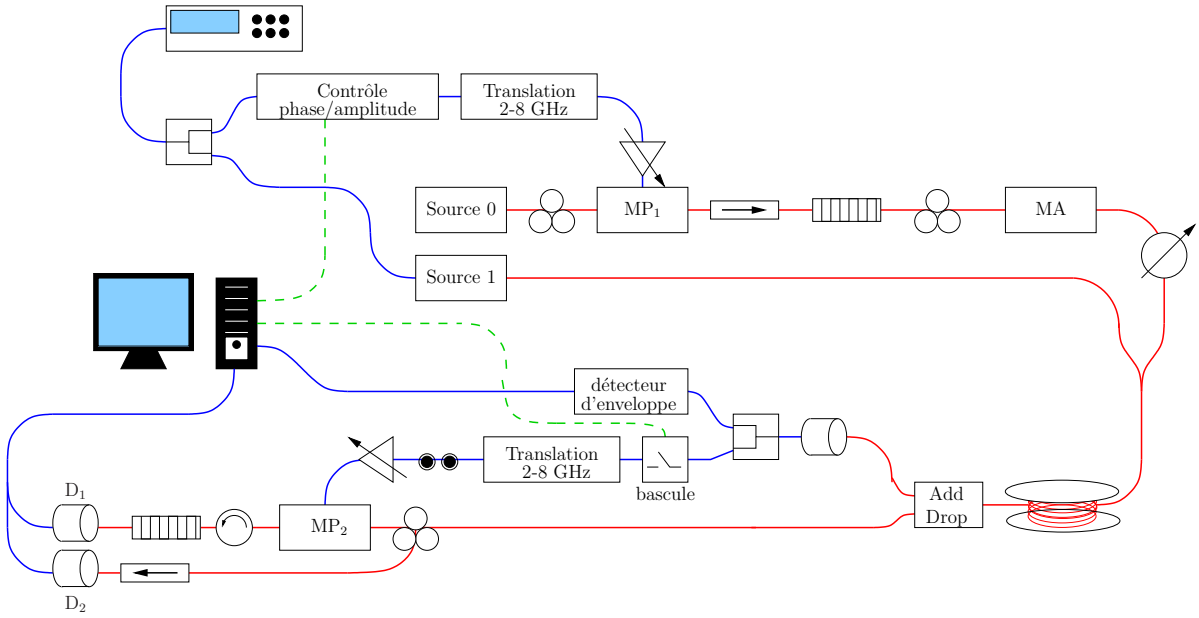


FIG. 2.19 – Dispositif complet de distribution quantique de clé

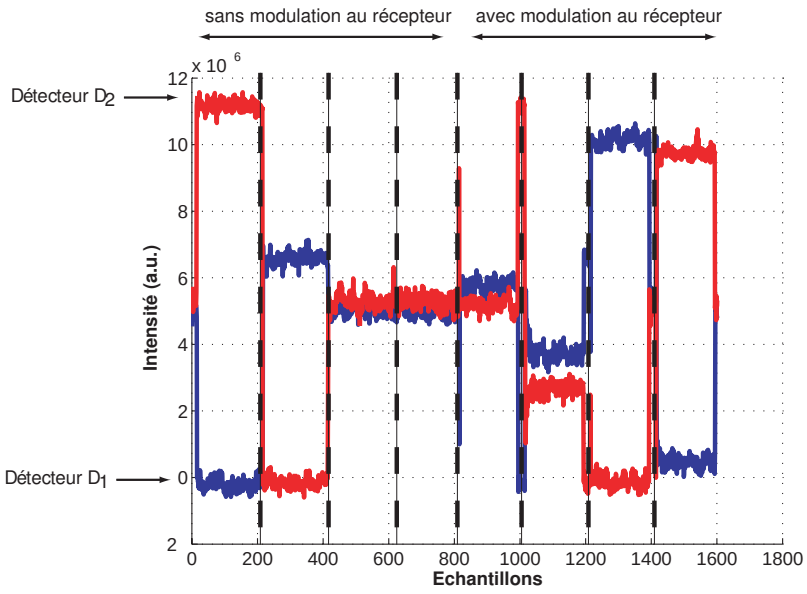


FIG. 2.20 – Puissances mesurées au récepteur sur chaque détecteur.

les différences de fidélité prédite pour des photons uniques se traduisent par des variations de la puissance totale détectée. En particulier, lors de la génération de l'état $|-;2\rangle$, près de la moitié de la puissance est perdue à l'émetteur avec le filtrage. Ces résultats nous permettent d'estimer le QBER à environ 2%.

2.3.4 Conclusion et perspectives

Le dispositif de distribution quantique de clé réalisé a permis de valider le principe de codage en fréquence proposé. La transmission réalisée sans isolation thermique ou mécanique spécifique confirme la robustesse du système. Pour autant, plusieurs aspects mériteraient d'être développés dans le futur. Sur le plan purement technique, toute l'électronique de commande devrait être réalisée sur des circuits intégrés de faible dimension, ce qui aurait le double avantage de réduire l'encombrement et le bruit électronique du dispositif. Sur le plan théorique, il serait nécessaire de caractériser plus spécifiquement la sécurité du système. Puisque l'opération réalisée par le récepteur est proche de la mesure idéale requise par le protocole BB84, la sécurité réelle du codage en fréquence ne devrait néanmoins pas être sensiblement différente de celle du BB84.

Chapitre 3

Système de cryptographie quantique par modulation gaussienne d'états cohérents

Sommaire

Les protocoles de cryptographie quantique basés sur des variables continues [72, 73] reposent sur la mesure de quadratures d'états quantiques. Cette mesure peut s'effectuer à l'aide d'une détection homodyne équilibrée, mais requiert alors la transmission d'une fréquence optique de référence cohérente en phase avec les signaux transmis. Si les distances de transmission sont faibles, on peut envisager de mettre en œuvre un multiplexage spatial de la référence et des signaux ; cette solution a par exemple permis de réaliser la première distribution de clé basée sur ces protocoles à variables continues [20]. Sur des distances plus importantes, le multiplexage spatial est cependant totalement inefficace, puisque les fluctuations des chemins optiques empruntés par les signaux et la référence ne sont pas identiques et détruisent la cohérence de phase. Pour y remédier, la solution envisagée par Jérôme Lodewyck au laboratoire Charles Fabry consiste à effectuer un multiplexage temporel [85] ; l'approche que nous avons choisie consiste à mettre en place un multiplexage fréquentiel.

Les deux sections de ce chapitre décrivent le dispositif de détection homodyne impulsionnelle réalisé, et l'architecture du système complet envisagé. Suite à la détérioration des filtres de Bragg indispensables pour le démultiplexage des signaux, nous n'avons pas pu mener à bien la mise en œuvre du système. Les résultats présentés ici ne permettent donc pas d'évaluer objectivement les performances du dispositif, mais identifient tout de même ses avantages et ses faiblesses.

3.1 Détection homodyne impulsionnelle

Principe des détections optiques cohérentes.

Les composantes de quadrature du champ optique sont des grandeurs qui dépendent directement de l'amplitude et de la phase du champ électromagnétique, ce qui rend leur détection délicate. En effet les fréquences des porteuses optiques sont de l'ordre de la centaine de térahertz et excluent donc toute détection directe de l'amplitude du champ. Les photodiodes ne permettent de mesurer que des grandeurs quadratiques du champ optique telle qu'une intensité, une puissance, ou un nombre de photons. L'accès aux valeurs des quadratures ne peut donc se faire qu'au moyen de systèmes interférométriques, où la mesure de battements relatifs avec un champ de référence synchrone permet de remonter aux quadratures du champ d'intérêt. La gamme de fréquence des battements est alors suffisamment faible pour que les signaux soient traités par un circuit électronique standard. Ces méthodes de détection, appelées *détections cohérentes* en raison de la cohérence de phase existant entre champ de référence et champ signal, sont réalisées depuis de nombreuses années dans le domaine des radiofréquences (jusqu'à quelques gigahertz). Leur application dans le domaine des télécommunications optiques est plus délicate en raison des difficultés pratiques liées à l'obtention d'une référence parfaitement en phase avec le signal. Les principaux formats de modulation utilisés sur les réseaux optiques sont d'ailleurs toujours principalement basés sur des modulations d'intensité. Néanmoins les détections cohérentes seront vraisemblablement amenées à se développer dans la prochaine décennie, car les formats de modulation cohérente ont de nombreux avantages en terme d'occupation spectrale et de résistance aux effets non linéaires [98].

Le principe des détections optiques cohérentes est illustré sur la figure 3.1. Le champ signal interfère sur une lame séparatrice équilibrée avec un champ de référence (encore appelé oscillateur local) dont l'intensité et la phase sont contrôlées. Les puissances des signaux résultants sont alors détectées indépendamment par deux photodiodes standard, puis une soustraction électronique permet d'éliminer la composante continue identique sur les deux bras, et de ne conserver que les termes d'interférences. Lorsque l'oscillateur local et le signal sont parfaitement synchrones, ce système de détection est appelé détection homodyne équilibrée ; dans le cas contraire on parle de détection hétérodyne équilibrée.

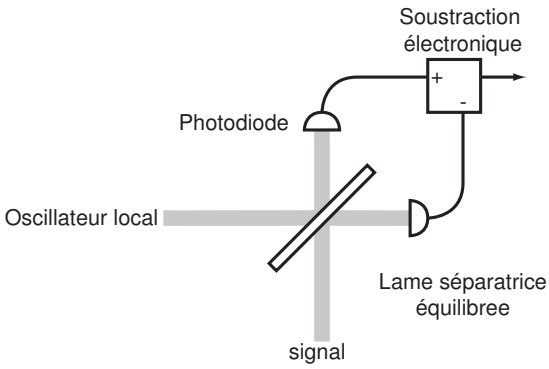


FIG. 3.1 – Principe des détections optiques cohérentes.

Cette section est consacrée à la description des aspects théoriques et expérimentaux d'une détection homodyne impulsionnelle équilibrée. Les travaux présentés ici s'inspirent très largement (dans la présentation comme dans la réalisation) de ceux réalisés au laboratoire Charles Fabry par Frédéric Grosshans [73] et Jérôme Wenger [75].

3.1.1 Théorie de la détection homodyne équilibrée

Description classique

Une description ondulatoire classique ne permet pas de rendre compte de toutes les propriétés d'une détection cohérente, en particulier elle n'explique pas certains phénomènes apparaissant avec des signaux de très faible énergie, mais elle en souligne néanmoins les principales caractéristiques. Par souci de simplicité nous ne considérerons ici qu'une détection homodyne parfaite, c'est à dire parfaitement équilibrée, sans pertes et sans bruit électronique ajouté. En notation complexe le champ signal et le champ de référence sont décrits respectivement par :

$$E_s(t) = E_s e^{j(\omega_0 t+\phi)} \qquad \text{et} \qquad E_0(t) = E_0 e^{j(\omega_0 t+\phi_0)}, \tag{3.1}$$

où ω_0 est la fréquence angulaire de la porteuse optique. Les champs obtenus après interférence sur la lame séparatrice s'écrivent alors :

$$E_+(t) = \frac{E_s e^{j\phi} + E_0 e^{j\phi_0}}{\sqrt{2}} e^{j\omega_0 t} \qquad \text{et} \qquad E_-(t) = \frac{E_s e^{j\phi} - E_0 e^{j\phi_0}}{\sqrt{2}} e^{j\omega_0 t}, \tag{3.2}$$

et à la sensibilité près de la photodiode, les intensités détectées sur chaque bras de la détection équilibrée sont finalement :

$$I_\pm \propto \underbrace{\frac{E_s^2}{2} + \frac{E_0^2}{2}}_{\text{intensité moyennes}} \pm \underbrace{E_s E_0 \cos(\phi - \phi_0)}_{\text{terme d'interférence}}. \tag{3.3}$$

La soustraction électronique des intensités élimine la composante commune qui ne porte pas d'information, pour ne conserver que le terme utile :

$$\delta I = I_+ - I_- \propto 2E_s E_0 \cos(\phi - \phi_0) = E_s \frac{X_{s,\phi_0}}{\sqrt{N_0}}. \tag{3.4}$$

La détection homodyne équilibrée permet donc de mesurer la quadrature du champ signal en phase avec l'oscillateur local. Cette quadrature est amplifiée d'un facteur proportionnel à l'intensité de l'oscillateur local, ce qui permet d'effectuer des mesures de champs extrêmement faibles avec une grande sensibilité. Par ailleurs, lorsque l'on utilise un oscillateur local intense, les niveaux de puissances après interférences sont suffisamment importants pour être détectés par des photodiodes PIN standard aux rendements quantiques très élevés (typiquement de l'ordre de 80%). En faisant varier la phase ϕ_0 de l'oscillateur local, on peut alors accéder à toutes les quadratures du champ signal.

Description quantique

Dans le formalisme de la mécanique quantique [92], les champs sont assimilés à des oscillateurs harmoniques et décrits à l'aide des opérateurs annihilation et création. En notant a_s et a_0 les opérateurs du champ signal et de l'oscillateur local, on obtient en sortie de la lame séparatrice :

$$a_+ = \frac{a_s + a_0}{\sqrt{2}} \qquad \text{et} \qquad a_- = \frac{a_s - a_0}{\sqrt{2}}, \tag{3.5}$$

et les observables correspondant aux intensités en sortie des photodiodes sont :

$$\hat{\mathbf{I}}_\pm \propto a_\pm^\dagger a_\pm = \frac{1}{2}\Big(a_s^\dagger a_s + a_0^\dagger a_0 \pm a_s^\dagger a_0 \pm a_0^\dagger a_s\Big). \tag{3.6}$$

Après soustraction des courants, l'observable mesuré par la détection homodyne équilibrée s'écrit donc :

$$\hat{\delta\mathbf{I}} = \hat{\mathbf{I}}_+ - \hat{\mathbf{I}}_- \propto a_s^\dagger a_0 + a_0^\dagger a_s. \tag{3.7}$$

En général, l'oscillateur local est un état cohérent $|\alpha_0\rangle$ très intense ($|\alpha_0|^2 \gg 1$) ce qui permet de simplifier notablement l'équation précédente. En effet quel que soit l'état $|\psi\rangle$ du signal, l'observable $\hat{\delta\mathbf{I}}$ est entièrement caractérisé par ses moments d'ordre n :

$$\mu_n = \langle\psi|\langle\alpha_0|\hat{\delta\mathbf{I}}^n|\alpha_0\rangle|\psi\rangle. \tag{3.8}$$

L'évaluation de ces moments se fait en réordonnant tous les termes suivant l'ordre normal, en particulier $a_0 a_0^\dagger = a_0^\dagger a_0 + 1$, et comme $|\alpha_0|^2 \gg 1$, il est possible de faire l'approximation :

$$\begin{aligned} \langle\alpha_0|{a_0}^p {a_0^\dagger}^q|\alpha_0\rangle &= \langle\alpha_0|\Big(a_0^\dagger a_0 + 1 + p - q\Big)^q a_0^{p-q}|\alpha_0\rangle \\ &= \big(|\alpha_0|^2 + 1 + p - q\big)^q \alpha_0^{p-q} \approx |\alpha_0|^{2q}\alpha_0^{p-q} \qquad \forall p > q \in \mathbb{N}. \end{aligned} \tag{3.9}$$

Cette simplification revient à considérer que les opérateurs a_0 et $a_0^\dagger$ commutent presque et peuvent alors être remplacés respectivement par α_0 et α_0^* dans l'équation (3.7). En introduisant $\phi_0 = \arg(\alpha_0)$, on peut donc considérer que l'observable mesuré est :

$$\boxed{\hat{\delta\mathbf{I}} \propto |\alpha_0|\ \left(a_s^\dagger e^{j\phi_0} + a_s e^{-j\phi_0}\right) = \frac{|\alpha_0|}{\sqrt{N_0}}\,\hat{\mathbf{X}}_{s,\phi_0}.} \tag{3.10}$$

La détection homodyne équilibrée donne directement accès à la quadrature du champ en phase avec l'oscillateur local. La valeur moyenne de l'observable $\hat{\delta\mathbf{I}}$ fournit bien sûr le résultat (3.4) obtenu avec une description classique, mais l'équation (3.10) permet aussi d'évaluer toutes les statistiques d'ordre supérieur. En particulier lorsque qu'aucun signal n'est présent, l'état correspondant est l'état vide $|0\rangle$, et bien que la valeur moyenne de la mesure soit nulle, la variance est $(\Delta X)^2 \propto |\alpha_0|^2$. Ce « bruit de photon » proportionnel à l'intensité de l'oscillateur local est un phénomène purement quantique, et sera utilisé par la suite pour vérifier le bon fonctionnement de la détection homodyne expérimentale. En effet, puisqu'un bruit classique de photodétection entraînerait une dépendance quadratique de la variance en fonction de l'intensité de l'oscillateur local, il suffit d'observer une dépendance linéaire pour s'assurer du bon équilibrage de la détection (voir section 3.1.5).

Approche semi-classique

Lorsque le signal reçu est un état gaussien (état cohérent ou état comprimé) $|\alpha_s\rangle$, la distribution statistique de ses quadratures est gaussienne, et il est alors possible d'adopter une description dite "semi-classique" [99]. En introduisant artificiellement un bruit gaussien sur les quadratures classiques X_s et P_s du champ électrique et en imposant une inégalité de type Heisenberg sur les variances ($\Delta X_s \Delta P_s \geq N_0$), on retrouve les résultats précédents sans s'encombrer du formalisme quantique. L'utilité de cette approche reste limitée aux phénomènes faisant intervenir au plus des statistique d'ordre deux, mais dans le cas des protocoles basés sur des états gaussiens, elle permet de souligner certaines ressemblances avec les communications classiques.

3.1.2 Détection homodyne impulsionnelle

La particularité de la détection homodyne utilisée ici est d'être résolue en temps. Le plus souvent, les détections homodynes sont au contraire résolues en fréquence, et les mesures de quadrature se font non pas en échantillonnant une impulsion optique à un instant donné, mais en mesurant le signal électrique obtenu dans une bande de fréquence limitée. La réalisation d'une détection résolue en fréquence est en général relativement aisée, car il est toujours possible de s'affranchir des bruits techniques (et plus particulièrement des bruits basse fréquence) en choisissant une bande de fréquence peu bruitée, et il n'est pas nécessaire que la bande passante de l'électronique de détection soit très élevée. Même si de tels systèmes sont particulièrement pratiques dans des expériences où la résolution temporelle du signal importe peu (tomographie quantique, etc.), il est moins évident de les incorporer dans un système de communication. En effet, lors d'une quelconque transmission il est inévitable de devoir prendre en compte l'aspect temporel du flot d'information, et il est beaucoup plus naturel d'essayer de mesurer des bits par impulsion qu'une quantité d'information présente dans une bande de fréquence. Par ailleurs, pour des applications cryptographiques il est important que les interceptions éventuelles d'un espion puissent être clairement définies, afin d'évaluer la sécurité du système dans le cadre le plus général possible. Jusqu'à présent les preuves de sécurité des protocoles basés sur des détections résolues en fréquence restent assez limitées [84].

La mise en œuvre d'une détection homodyne résolue en temps présente cependant plus de difficultés techniques. L'électronique de détection doit avoir une bande passante allant au minimum du quasi-continu à la fréquence de répétition des impulsions, et le bruit électronique doit être le plus faible possible sur toute cette bande. En pratique il est même nécessaire d'avoir une bande passante largement supérieure à la fréquence de répétition des impulsions, afin d'obtenir une réponse impulsionnelle d'amplitude élevée et donc un bon rapport signal à bruit lors de l'échantillonnage. Néanmoins, ces systèmes de détection sont aujourd'hui bien maîtrisés, et plusieurs groupes les ont déjà utilisés avec succès [75, 100, 101].

Description quantique de la détection impulsionnelle

Nous avons supposé dans les sections précédentes que les champs optiques étaient purement monochromatiques et continus. Cette description est insuffisante dans le cas d'impulsions, car il devient nécessaire de tenir compte de l'étendue spectrale du champ.

L'analyse de la détection homodyne précédente reste cependant valide en remplaçant les opérateurs a et $a^\dagger$ par de nouveaux opérateurs $\hat{\mathbf{A}}$ et $\hat{\mathbf{A}}^\dagger$ définis par :

$$\hat{\mathbf{A}}^\dagger = \frac{1}{\sqrt{2\pi}} \int \tilde{f}(\omega) a^\dagger(\omega) d\omega = \frac{1}{\sqrt{2\pi}} \int f(t) a^\dagger(t) dt \qquad \text{avec} \quad \int \left|\tilde{f}(\omega)\right|^2 d\omega = 1, \quad (3.11)$$

où $a^\dagger(\omega)$ est l'opérateur création standard à la fréquence ω, et $\tilde{f}(\omega) = \mathcal{F}[f(t)]$ est l'enveloppe spectrale de l'impulsion [102]. Les opérateurs $\hat{\mathbf{A}}$ et $\hat{\mathbf{A}}^\dagger$ vérifient les mêmes propriétés que leurs équivalents monomodes, et on peut donc définir de façon similaire des états de Fock, des états cohérents, et des états comprimés impulsionnels. Par la suite nous ne distinguerons plus explicitement le cas continu du cas impulsionnel dans les notations, et afin d'alléger les équations nous utiliserons les opérateurs a et $a^\dagger$.

3.1.3 Imperfections d'une détection expérimentale

Les caractéristiques des composants optiques et électroniques réels ne sont malheureusement jamais parfaites, et en pratique la qualité des mesures s'en trouve dégradée. Cette section détaille les différentes imperfections (déséquilibre, pertes, excès de bruit, etc.) pouvant apparaître lors de la réalisation expérimentale d'une détection homodyne impulsionnelle.

Déséquilibre entre les voies

La lame séparatrice n'étant jamais parfaite, il apparaît systématiquement un léger déséquilibre dans la détection. Une description classique suffit largement pour décrire l'influence de cette imperfection, et en introduisant une réflectivité et une transmission légèrement différentes :

$$R = \frac{1}{2} + \epsilon \quad \text{et} \quad T = \frac{1}{2} - \epsilon \qquad \text{avec} \quad |\epsilon| \ll \frac{1}{2}, \quad (3.12)$$

les intensités détectées par chaque photodiode sont :

$$\begin{aligned} I_+ &= \left|\sqrt{T}E_s e^{j\phi} + \sqrt{R}E_0 e^{j\phi_0}\right|^2 = \frac{E_s^2}{2} + \frac{E_0^2}{2} + \epsilon\big(E_0^2 - E_s^2\big) + E_s E_0 \cos(\phi - \phi_0) + \mathcal{O}(\epsilon^2), \\ I_- &= \left|\sqrt{R}E_s e^{j\phi} + \sqrt{T}E_0 e^{j\phi_0}\right|^2 = \frac{E_s^2}{2} + \frac{E_0^2}{2} + \epsilon\big(E_s^2 - E_0^2\big) - E_s E_0 \cos(\phi - \phi_0) + \mathcal{O}(\epsilon^2). \end{aligned} \quad (3.13)$$

La différence des photocourants devient alors :

$$\begin{aligned} \delta I = 2E_s E_0 \cos(\phi - \phi_0) + 2\epsilon\big(E_0^2 - E_s^2\big) &\approx 2E_s E_0 \cos(\phi - \phi_0) + 2\epsilon E_0^2 \\ &\approx E_0 \left(\frac{X_{s,\phi_0}}{\sqrt{N_0}} + 2\epsilon E_0\right). \end{aligned} \quad (3.14)$$

Le premier terme de cette expression correspond au signal utile et varie linéairement avec l'amplitude de l'oscillateur local intense. En revanche, le second terme est introduit par le déséquilibre et croît de façon quadratique avec cette même amplitude. La variance du signal total est donc la somme du bruit de photon proportionnel à la puissance de

l'oscillateur local, et d'un bruit classique augmentant comme le carré de la puissance. Les mesures effectuées avec une détection homodyne déséquilibrée restent alors résolues au bruit de photon tant que la variance de δI reste de l'ordre de E_0^2, c'est à dire tant que $\epsilon \ll 1/2E_0$. Par la suite nous utiliserons un oscillateur local comprenant environ 10^8 photons par impulsions, ce qui impose un équilibrage de l'ordre de 10^{-5}.

Pertes optiques sur les voies

Nous supposerons ici que la détection est parfaitement équilibrée et que les pertes optiques sur chaque bras sont identiques. Ces pertes peuvent être modélisées par des lames séparatrices de transmission η (figure 3.2(a)) qui couplent les modes $a_\pm$ de chaque bras à des modes vides $a_{v,\pm}$. Les modes détectés par les photodiodes s'écrivent alors :

$$a_\pm = \sqrt{\eta}\frac{a_s \pm a_0}{\sqrt{2}} + \sqrt{1-\eta}a_{v,\pm}, \tag{3.15}$$

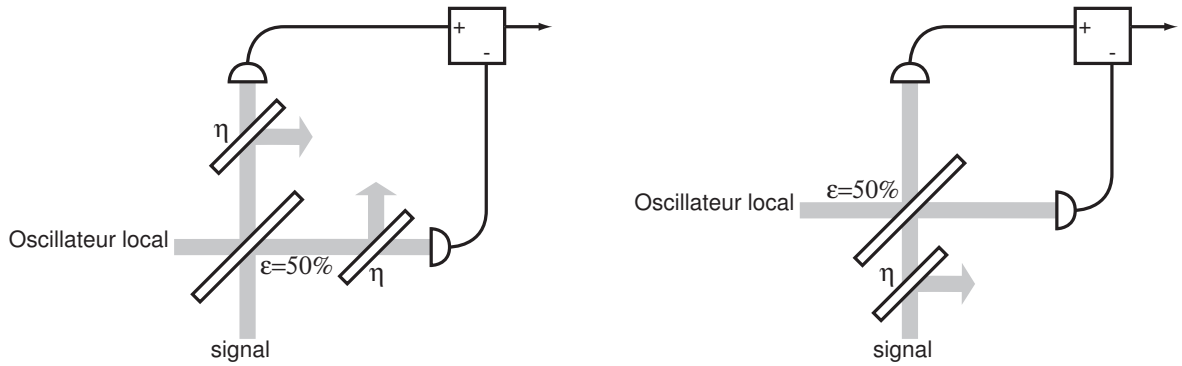
et la différence des photocourants devient donc :

$$\delta\hat{\mathbf{I}} = \eta\frac{|\alpha_0|}{\sqrt{N_0}}\hat{\mathbf{X}}_{s,\phi_0} + \sqrt{\frac{\eta(1-\eta)}{2N_0}}\,|\alpha_0|\left(\hat{\mathbf{X}}_{v,+} + \hat{\mathbf{X}}_{v,-}\right), \tag{3.16}$$

où $\hat{\mathbf{X}}_{v,+}$ et $\hat{\mathbf{X}}_{v,-}$ sont les quadratures des modes vides sur chacune des voies. L'indice ϕ_0 a été omis pour ces quadratures, car la distribution statistique des quadratures d'un mode vide est indépendante de la phase de l'oscillateur local. Par ailleurs, les couplages avec le vide n'étant pas corrélés entre les deux voies, la somme des quadratures peut être remplacée par la quadrature d'un mode vide unique $\sqrt{2}\hat{\mathbf{X}}_v$:

$$\delta\hat{\mathbf{I}} = \eta\frac{|\alpha_0|}{\sqrt{N_0}}\hat{\mathbf{X}}_{s,\phi_0} + \sqrt{\frac{\eta(1-\eta)}{2N_0}}\sqrt{2}\hat{\mathbf{X}}_v = \frac{\sqrt{\eta}|\alpha_0|}{\sqrt{N_0}}\left(\sqrt{\eta}\hat{\mathbf{X}}_{s,\phi_0} + \sqrt{1-\eta}\hat{\mathbf{X}}_v\right). \tag{3.17}$$

On peut donc considérer que l'on effectue la détection homodyne idéale (avec un oscillateur local de puissance $\eta|\alpha_0|^2$) d'un signal ayant subi des pertes avant interférence (figure 3.2(b)).



(a) Modélisation des pertes optiques sur les voies

(b) Modélisation équivalente

FIG. 3.2 – Modélisation des pertes optiques d'une détection homodyne équilibrée

Adaptation des modes de l'oscillateur local et du signal

Comme précédemment, la mauvaise adaptation des modes spatio-temporels peut être modélisée par une lame séparatrice d'efficacité η_m placée en amont de la détection sur la voie du signal. Une justification détaillée de cette modélisation peut être trouvée dans [103], nous nous contenterons ici d'en présenter l'idée générale. Lors de l'interférence sur la lame séparatrice, on peut considérer que l'oscillateur local agit comme un filtre venant amplifier les signaux possédant les mêmes modes de polarisation et les mêmes modes spatio-temporels. Lorsque le signal utile incident sur la lame séparatrice n'est pas exactement dans le même mode que l'oscillateur local, ce dernier vient en plus amplifier des modes vides indésirables. La différence des photocourants peut alors s'écrire de façon similaire à (3.17) :

$$\hat{\delta\mathbf{I}} = \frac{\sqrt{\eta_m}|\alpha_0|}{\sqrt{N_0}}\Big(\sqrt{\eta_m}\hat{\mathbf{X}}_{s,\phi_0} + \sqrt{1-\eta_m}\hat{\mathbf{X}}_v\Big). \tag{3.18}$$

Le coefficient η_m s'évalue très simplement en faisant interférer deux faisceaux de même intensité sur la lame séparatrice, puis en mesurant la visibilité des franges d'interférences obtenues. En effet les intensités sur chaque bras s'écrivent alors :

$$I_\pm = E_0^2\,(1 \pm \sqrt{\eta_m}\cos(\phi - \phi_0)), \tag{3.19}$$

et à partir de la visibilité $V = (I_{max} - I_{min})/(I_{max} + I_{min})$ on déduit la valeur de η_m :

$$\eta_m = \left(\frac{V}{1-V}\right)^2. \tag{3.20}$$

Excès de bruit de l'oscillateur local

Jusqu'à présent nous avons supposé que l'oscillateur local était assimilable à un champ classique α_0 sans bruit. En pratique ce dernier présente cependant des fluctuations classiques ou quantiques, dont on peut tenir compte en introduisant un opérateur δa_0 tel que $a_0 = \alpha_0 + \delta a_0$. Par hypothèse les moments de δa_0 sont négligeables devant $|\alpha_0|$ mais pas nécessairement devant l'amplitude du signal quantique a_s. En reprenant les calculs de la section 3.1.1 et en remplaçant cette fois l'opérateur création a_0 de l'oscillateur local intense par $\alpha_0 + \delta a_0$, les photocourants détectés sur chaque bras sont :

$$\hat{\mathbf{I}}_\pm \propto a_\pm^\dagger a_\pm = \frac{1}{2}\Big(a_s^\dagger a_s + (\alpha_0+\delta a_0)^\dagger(\alpha_0+\delta a_0) \pm a_s^\dagger\alpha_0 \pm \alpha_0^* a_s \pm a_s^\dagger\delta a_0 \pm \delta a_0^\dagger a_s\Big). \tag{3.21}$$

La différence des photocourants s'écrit donc :

$$\hat{\delta\mathbf{I}} = \frac{|\alpha_0|}{\sqrt{N_0}}\hat{\mathbf{X}}_{s,\phi_0} + a_s^\dagger\delta a_0 + \delta a_0^\dagger a_s \approx \frac{|\alpha_0|}{\sqrt{N_0}}\hat{\mathbf{X}}_{s,\phi_0}, \tag{3.22}$$

en supposant les fluctuations δa_0 négligeables devant $|\alpha_0|$. Une détection homodyne équilibrée s'affranchit donc complètement du bruit de l'oscillateur local intense, et les fluctuations des mesures peuvent donc être entièrement attribuées aux fluctuations quantiques du signal [104].

Fluctuations de phase

L'oscillateur local et le signal étant généralement issus d'une même source laser, le dispositif global de détection homodyne s'apparente à un interféromètre de Mach-Zehnder. Les fluctuations relatives de chemin optique d'un bras de l'interféromètre par rapport à l'autre induisent donc des fluctuations de phase entre l'oscillateur local et le signal. Afin que la détection homodyne permette effectivement de caractériser des états quantiques, il est impératif que ce bruit de phase classique ne vienne pas masquer le bruit de photon. Dans le cas d'états cohérents $|\alpha_s\rangle$, l'écart type du bruit de phase est :

$$\sqrt{\left\langle \hat{\mathbf{X}}_s \right\rangle^2 + \left\langle \hat{\mathbf{P}}_s \right\rangle^2}\,\delta\theta = 2\sqrt{N_0}|\alpha_s|\delta\theta, \tag{3.23}$$

où $\delta\theta$ représente l'écart type de la fluctuation de phase par rapport à l'oscillateur local. La condition $2\sqrt{N_0}|\alpha_s|\delta\theta \ll \sqrt{N_0}$ limite donc le nombre de photons utilisables dans le signal :

$$n_s = |\alpha_s|^2 \ll \frac{1}{4\delta\theta^2}. \tag{3.24}$$

Pour une valeur typique $\delta\theta \approx 10^{-3}$, il faut donc utiliser un nombre de photon $n_s \ll 2.5 \times 10^5$. En pratique les impulsions signal utilisées dans notre système contiendront au plus une centaine de photons.

Conclusion : efficacité globale de la détection homodyne

En tenant compte des différentes sources d'imperfections étudiées dans cette section, une détection homodyne réelle peut donc être modélisée par une détection homodyne idéale :

- en faisant subir au signal utile des pertes avant détection au travers d'une lame séparatrice de transmission η,
- et en atténuant la puissance de l'oscillateur de ce même facteur.

L'efficacité globale η de la détection est alors :

$$\boxed{\eta = \eta_p\ \eta_m\ \eta_{phot},} \tag{3.25}$$

où η_p est l'efficacité correspondant aux pertes optiques, η_m est l'efficacité d'adaptation des modes et η_{phot} est l'efficacité de détection des photodiodes. Par ailleurs la détection reste résolue au bruit de photon tant que le déséquilibre ϵ de la lame séparatrice équilibrée et le nombre de photons n_s du signal utile sont tels que :

$$\boxed{\epsilon \ll \frac{1}{2|\alpha_0|} \qquad \text{et} \qquad n_s \ll \frac{1}{4\delta\theta^2},} \tag{3.26}$$

où $\delta\theta$ est l'écart type de la fluctuation de phase entre le signal et l'oscillateur local.

3.1.4 Amplificateur de tension

Le système optoélectronique effectuant la soustraction électronique des signaux dans notre détection homodyne expérimentale est un circuit dit à amplification de tension. Le

principe de ce montage est d'effectuer une conversion courant/tension des photocourants issus des photodiodes avant d'amplifier le signal au moyen d'amplificateurs bas bruits. Traditionnellement, la conversion est effectuée à l'aide d'un montage transimpédance dont le schéma de principe est rappelé figure 3.3.

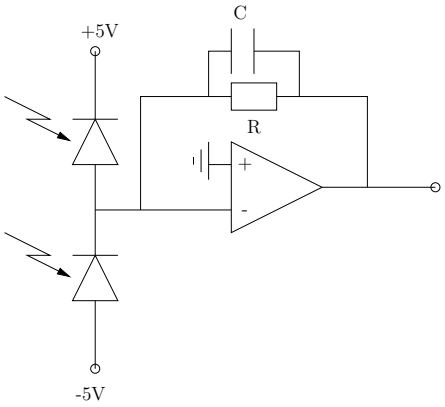


FIG. 3.3 – Montage transimpédance.

Il est possible en théorie de prévoir (et donc de contrôler) le comportement du bruit dans la chaîne d'amplification de ces circuits [105], mais la présence de la contre-réaction complique significativement les calculs et les circuits réalisés sur ce modèle se sont révélés bien plus bruités que prévus. Le montage retenu pour nos expériences est celui représenté figure 3.4, et s'inspire de celui proposé dans les références [75, 101].

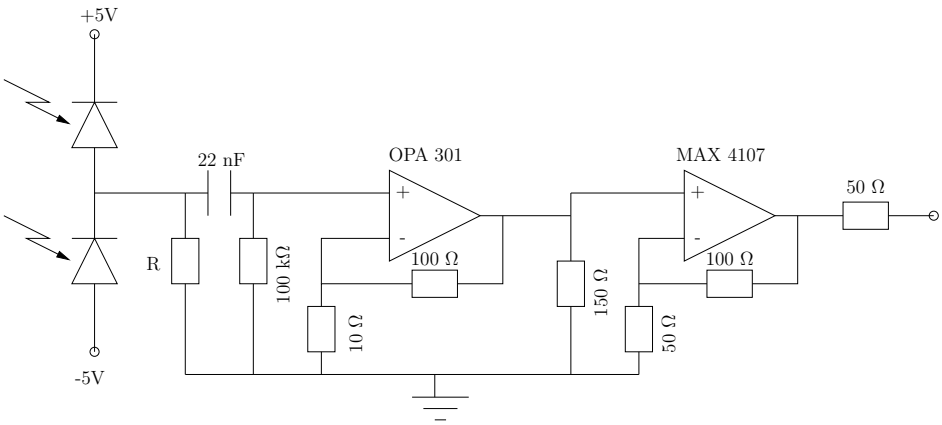


FIG. 3.4 – Circuit de détection à amplification de tension.

La conversion courant/tension s'effectue en envoyant les photocourants au travers de la résistance R. Afin d'obtenir un courant de fuite dans l'amplificateur le plus faible possible, le premier amplificateur opérationnel de la chaîne est un préamplificateur Texas Instruments OPA301 en configuration non-inverseuse, possédant une impédance d'entrée d'environ 10^{13} Ω et un bruit de courant d'environ 1.5 fA/$\sqrt{\text{Hz}}$. Le gain de ce premier amplificateur est $G_1 = 10$. Le second étage amplificateur est réalisé avec un amplificateur bas bruit MAX 4107 possédant un bruit en tension de 0.75 nV/$\sqrt{\text{Hz}}$, et le gain de l'étage est fixé à $G_2 = 20$. Le gain total du circuit est donc :

$$G_T = 200R \quad \text{V/A}. \tag{3.27}$$

Le bruit total de la chaîne amplificatrice est dominé par le bruit thermique de la résistance R, dont l'écart type (en tension) est :

$$\sigma = \sqrt{4k_bTBR} \quad \text{V}, \tag{3.28}$$

où B est la bande passante du circuit, k_B est la constante de Boltzmann, et T est la température de fonctionnement. Pour obtenir un bon rapport signal à bruit il faut alors choisir R la plus élevée possible, mais à cause du couplage de R avec la capacité d'entrée de l'OPA 301 ($C_i \approx 5$ pF) la bande passante du circuit diminue. En pratique, nous avons choisi $R \approx 10$ kΩ pour obtenir une bande passante d'environ 5 MHz.

La bande passante a été estimée expérimentalement de deux manières différentes, en mesurant tout d'abord la réponse impulsionnelle de chaque voie du circuit lorsque des impulsions optiques très courtes (≈ 8 ns) sont envoyées sur les photodiodes, puis en mesurant directement le spectre du bruit en sortie du circuit lorsque du bruit blanc est présent en entrée. Les amplitudes des fonctions de transfert ainsi obtenues sont représentées figure 3.5 lorsque $R = 8200$ Ω. La bande passante mesurée par ces deux méthodes est d'environ 5 MHz.

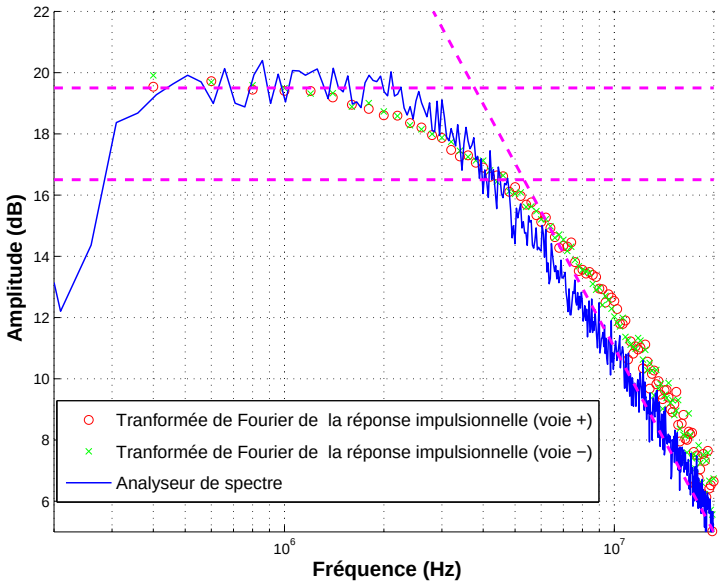


FIG. 3.5 – Fonction de transfert du circuit de détection homodyne.

3.1.5 Détection homodyne impulsionnelle du vide

Afin de tester le circuit de détection, nous avons réalisé une détection homodyne impulsionnelle du vide. Le schéma de principe du montage est représenté figure 3.6.

Un train d'impulsions de 170 ns à la fréquence de 200 kHz est généré en hachant le signal continu en sortie d'une diode laser avec un modulateur d'intensité. Un atténuateur variable permet d'ajuster le nombre de photons dans chacune de ces impulsions. Les impulsions sont alors envoyées sur une entrée d'un coupleur 2x2 équilibré dont les sorties sont connectées au circuit de détection homodyne. Les pertes sur chacun des bras de la détection homodyne sont ajustées à l'aide d'atténuateurs variables. La figure 3.7 représente le signal électrique en sortie du circuit électronique à la réception d'une impulsion.

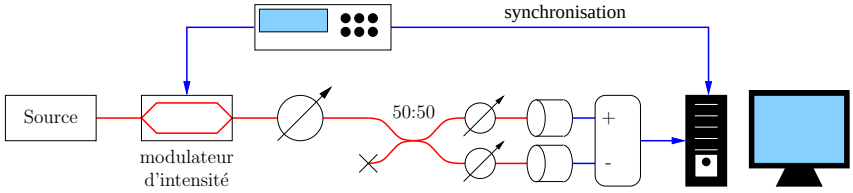


FIG. 3.6 – Détection homodyne impulsionnelle du vide.

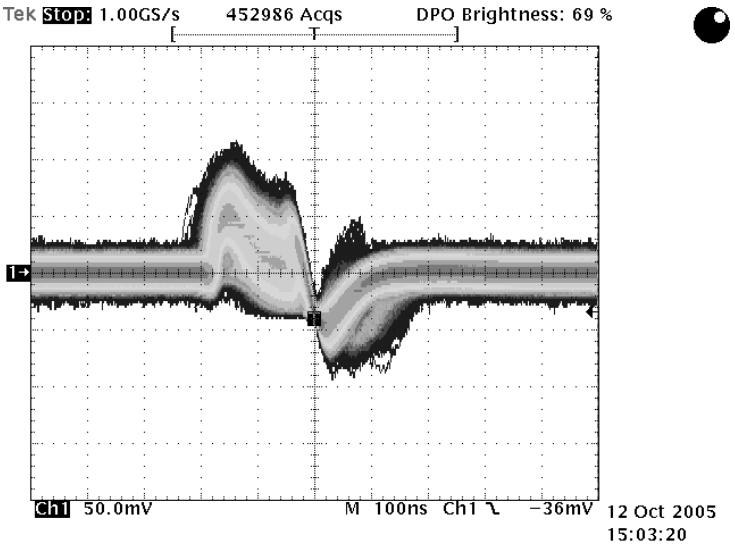


FIG. 3.7 – Impulsion électrique en sortie du circuit de détection.

Les phénomènes transitoires qui apparaissent en tête et queue de l'impulsion sont vraisemblablement causés par une différence de capacité des photodiodes. Cet effet pourrait être réduit en sélectionnant une paire de photodiodes aux caractéristiques plus proches que celles dont nous disposions. Une carte d'acquisition National Instruments PCI 6024E permet finalement d'enregistrer un échantillon par impulsion. L'instant exact d'acquisition est ajusté à l'aide d'une ligne à retard électrique, de manière à récupérer un échantillon au centre de l'impulsion et à s'affranchir ainsi des phénomènes transitoires. La variance du bruit introduit par la quantification sur 12 bits est d'environ 110 $(\mu\mathrm{V})^2$, ce qui est largement inférieur au bruit électronique du circuit, dont la variance est d'environ 3.1 $(\mathrm{mV})^2$.

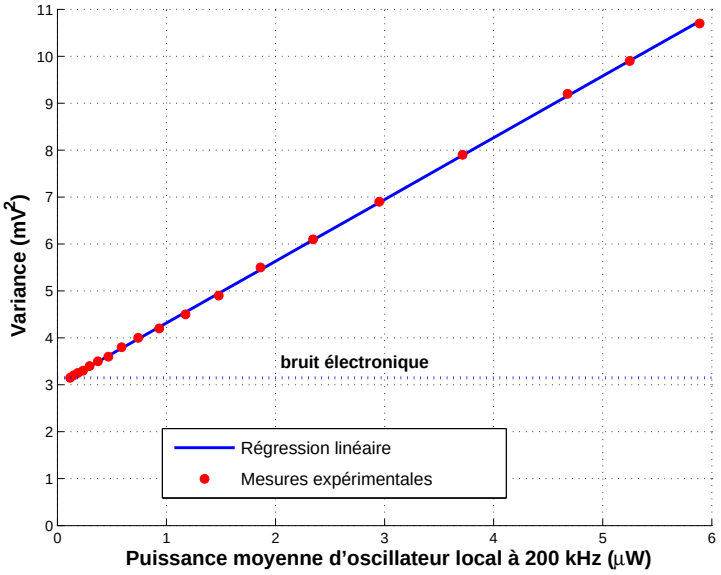


FIG. 3.8 – Calibration de la détection homodyne.

Afin de calibrer l'équilibre de la détection homodyne, il faut vérifier que la variance du bruit détecté croît linéairement avec la puissance de l'oscillateur local. Une fois la calibration effectuée, la pente de la droite obtenue permet de remonter au gain de la détection. Avec le montage précédent, on obtient d'après la figure 3.8 un gain d'environ 1.33 $(\mathrm{mV})^2/\mu\mathrm{W}$.

3.2 Dispositif expérimental de cryptographie quantique

3.2.1 Architecture du système

Multiplexage en fréquence

Le choix de la mise en œuvre d'un multiplexage fréquentiel a été motivé par trois facteurs. Tout d'abord, la technologie des filtres de Bragg est aujourd'hui parfaitement maîtrisée, ce qui rend possible le démultiplexage de signaux séparés d'une dizaine de GHz, avec une isolation d'au moins 40 dB. En associant deux filtres, il est donc tout à fait envisageable d'atteindre une isolation de 80 dB, et de démultiplexer ainsi un oscillateur local

intense contenant plusieurs centaines de millions de photons, et un signal n'en contenant qu'une centaine. De plus, les pertes des filtres de Bragg peuvent être de l'ordre de 0.1 dB. En second lieu, puisque l'oscillateur local et le signal se propagent en même temps, l'interféromètre nécessaire pour effectuer la détection homodyne au récepteur est équilibré. Dans le cas d'un multiplexage temporel, il faut au contraire utiliser un interféromètre déséquilibré, contenant plus de longueur de fibre, et donc potentiellement plus instable. Enfin, si l'oscillateur local et le signal sont séparés d'une dizaine de GHz, on peut envisager de manipuler simplement les états avec des modulateurs optiques.

Codage par modulation en bande latérale unique

Le contrôle en phase en en amplitude d'un état cohérent de faible intensité, et son multiplexage avec un oscillateur local intense, peuvent être réalisés avec une modulation en bande latérale unique. Cette modulation s'obtient en envoyant un état cohérent intense $|\alpha\rangle_{\omega_0}$ à la fréquence ω_0 dans un modulateur de Mach-Zehnder à deux électrodes (figure 3.9).

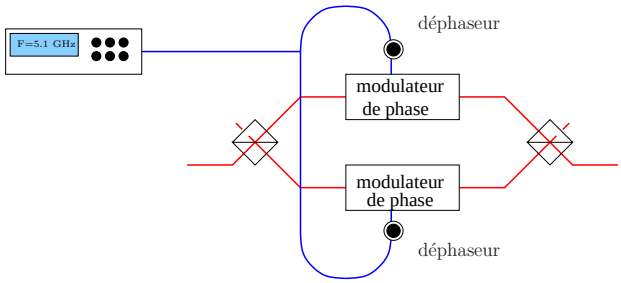


FIG. 3.9 – Modulation en bande latérale unique avec un modulateur à deux électrodes.

Les bras du modulateur sont modulés par deux signaux sinusoïdaux déphasés, issus du même synthétiseur haute fréquence. Ces signaux de modulation s'écrivent :

$$V_i(t) = V\cos\left(\Omega t + \phi_i\right) \quad i \in \{1,2\}\,. \tag{3.29}$$

Le déphasage ψ entre les deux voies peut en plus être modifié en contrôlant le biais du modulateur. En reprenant l'équation (2.9), l'état quantique en sortie du modulateur est alors :

$$\left|\frac{J_0\left(a\right)+e^{j\psi}}{2}\alpha_0\right\rangle_{\omega_0} \bigotimes_{p\neq 0} \left|\frac{J_p\left(a\right)\alpha_0}{2}(-j)^p\left[e^{jp\phi_1}+e^{j\psi}e^{jp\phi_2}\right]\right\rangle_{\omega_0+p\Omega}, \tag{3.30}$$

où a est proportionnel à l'amplitude V des signaux électriques. Si on choisit $\phi_1 = \phi_2 + \pi/2$ et $\psi = \pi/2$, on constate que :

$$\left|\frac{J_0\left(a\right)+e^{j\psi}}{2}\alpha_0\right\rangle_{\omega_0} = \left|\frac{J_0\left(a\right)+j}{2}\alpha_0\right\rangle_{\omega_0} \tag{3.31}$$

$$\left|\frac{J_{-1}\left(a\right)\alpha_0}{2}j\left[e^{-j\phi_1}+e^{j\psi}e^{-j\phi_2}\right]\right\rangle_{\omega_0-\Omega} = 0, \tag{3.32}$$

$$\left|\frac{J_1\left(a\right)\alpha_0}{2}(-j)\left[e^{j\phi_1}+e^{j\psi}e^{j\phi_2}\right]\right\rangle_{\omega_0+\Omega} = \left|J_1\left(a\right)\alpha_0 e^{j\phi_2}\right\rangle_{\omega_0+\Omega}. \tag{3.33}$$

Dans la situation qui nous intéresse, on cherche à contrôler des états cohérents contenant une centaine de photons, à partir d'une référence en contenant plusieurs millions. La profondeur de modulation est donc très faible ($a \ll 1$), ce qui nous permet de négliger toutes les bandes latérales de modulation d'ordre supérieur ou égal à deux, et la variation de puissance de la référence. Les conditions $\phi_1 = \phi_2 + \pi/2$ et $\psi = \pi/2$ correspondent alors à une situation de modulation en bande latérale unique, et le contrôle de la phase et de l'amplitude de l'état cohérent dans la bande latérale se fait directement en modifiant la phase et l'amplitude du signal électrique de modulation.

Le spectre classique, obtenu en sortie d'un modulateur Mach-Zenhder à deux électrodes (LUCENT, 40 Gbits/s) dans la configuration précédente, et modulé à 18 GHz, est représenté figure 3.10.

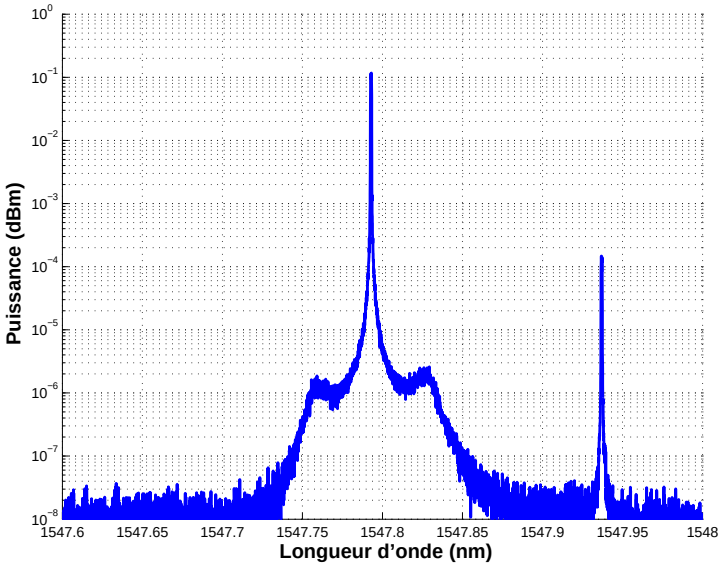


FIG. 3.10 – Modulation en bande latérale unique ($\Omega/2\pi$=18 GHz)

La puissance de la bande latérale gauche est au moins 40 dB en dessous de celle de la bande latérale droite. A 18 GHz de la fréquence d'émission de la diode (ALCATEL A1905 LMI), la puissance résiduelle est environ 70 dB en dessous de la puissance d'émission. En filtrant le signal émis par la diode, on peut cependant sans difficulté abaisser cette puissance de 40 dB supplémentaires, et envisager ainsi d'utiliser 10^{10} photons dans la bande centrale et une centaine dans la bande latérale.

Dispositif complet

Le dispositif du récepteur plus complexe, car il est non seulement nécessaire de démultiplexer l'oscillateur local et le signal, mais aussi d'effectuer une conversion de fréquence de l'oscillateur local avant la détection homodyne. Comme indiqué sur la figure 3.11, le démultiplexage ne nécessite qu'un circulateur suivi d'un réseau de Bragg. Un filtre d'isolation 40 dB suffirait ici à réfléchir entièrement le signal à la fréquence $\omega_0 + \Omega$.

La conversion de fréquence de l'oscillateur local peut de nouveau être réalisée avec une modulation en bande latérale unique. En reprenant les équations (3.31) et (3.30), l'état

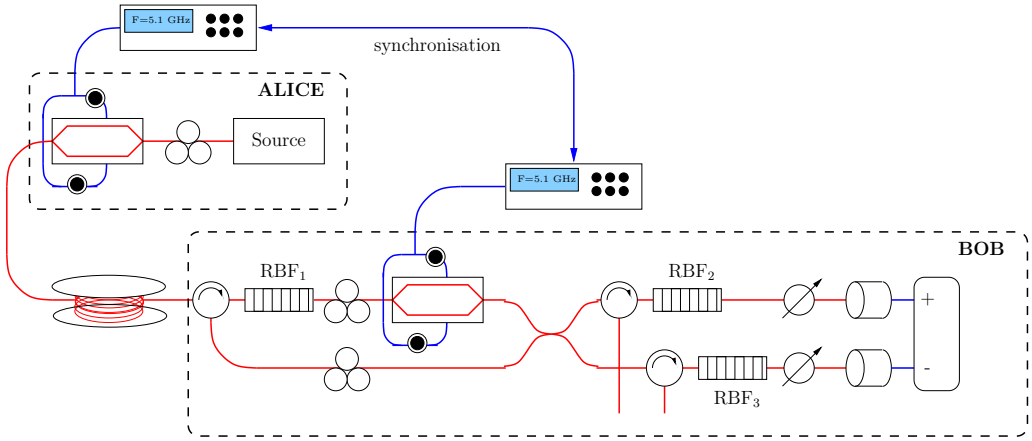


FIG. 3.11 – Système de cryptographie quantique par variables continues basé sur un multiplexage fréquentiel.

en sortie du modulateur à deux électrodes s'écrit :

$$\left|\frac{J_1(a')\,(1+j)}{4}\alpha_0 e^{j\phi'_2}\right\rangle_{\omega_0+\Omega} \otimes |\Psi\rangle, \tag{3.34}$$

où a' et ϕ'_2 sont l'amplitude et la phase du signal électrique de modulation, et $|\Psi\rangle$ représente tous les états à des fréquences différentes de $\omega_0+\Omega$. L'efficacité de la conversion de fréquence est maximale, si l'amplitude de modulation correspond au maximum de la fonction de Bessel J_1. Dans le meilleur des cas, l'oscillateur local effectivement utilisable pour la détection homodyne est alors :

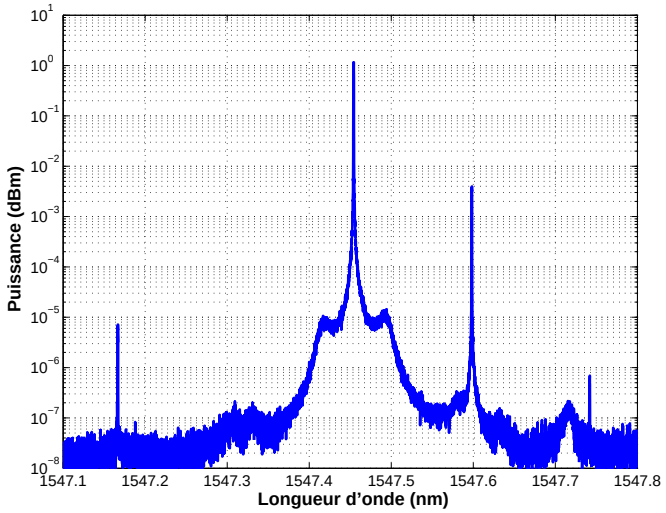
$$|\alpha_{OL}\rangle_{\omega_0+\Omega} = \left|\frac{0.338\,(1+j)}{4}\alpha_0 e^{j\phi'_2}\right\rangle_{\omega_0+\Omega}, \tag{3.35}$$

et on ne récupère ainsi qu'environ 1.5% du nombre de photon initial. Pour travailler avec un oscillateur local effectif contenant 10^8 photons, il faut donc au départ un signal en contenant 10^{10}.

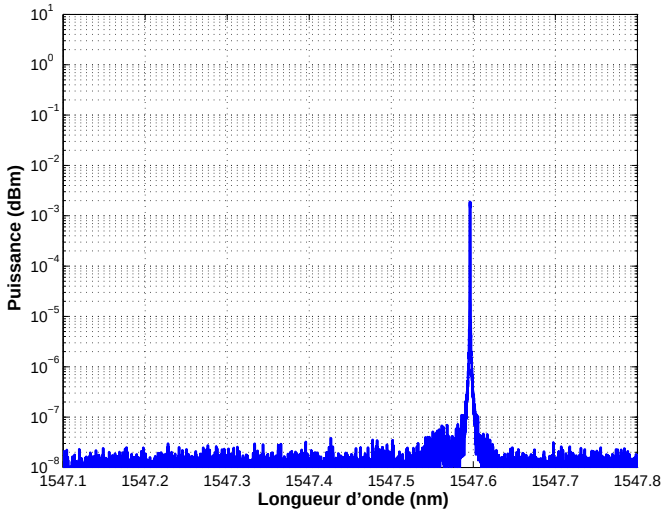
Une fois la conversion réalisée, le signal et l'oscillateur local $|\alpha_{OL}\rangle_{\omega_0+\Omega}$ interfèrent à travers un coupleur 2x2 équilibré. Les signaux obtenus en sortie doivent cependant être filtrés pour éliminer tout résidu de l'état $|\Psi\rangle$. Le filtrage de la fréquence $\omega_0+\Omega$ réalisé au travers de deux filtres de Bragg successifs, de 80 pm de bande passant, est représenté figure 3.12. L'isolation totale obtenue est supérieure à 80 dB, et la perte d'environ 2 dB.

3.2.2 Perspectives

Suite à la détérioration des filtres de Bragg, nous n'avons pas pu mettre en place le dispositif complet. Néanmoins, les résultats préliminaires ont permis de confirmer la faisabilité de la détection homodyne, du démultiplexage, et de la conversion de fréquence de l'oscillateur local. Plusieurs aspects importants doivent cependant encore être étudiés, et en particulier il serait nécessaire d'effectuer une caractérisation précise du bruit du système. Par exemple, le contrôle de l'amplitude et de la phase des bandes latérales doit être réalisé avec une précision inférieure à la variance du bruit quantique. Cette



(a) Signal avant filtrage.



(b) Signal après filtrage.

FIG. 3.12 – Filtrage d'un mode latéral.

précision dépend essentiellement de celle avec laquelle il est possible de contrôler le signal de modulation électrique à 20 GHz. Ensuite, comme dans le chapitre précédent, il est nécessaire de mettre en place un système d'autocompensation de la dispersion. Cette compensation n'est cependant pas parfaite et se traduit elle aussi par un bruit ajouté. Enfin, il est clair que le bruit électrique du circuit de détection homodyne ne permet pas pour l'instant d'envisager une transmission haut débit réelle.

Chapitre 4

Réconciliation de variables aléatoires

Sommaire

Comme nous l'avons brièvement évoqué au chapitre 1, l'efficacité des algorithmes de réconciliation fixe en pratique les débits et distances atteignables des systèmes de cryptographie quantique par variables continues. La conception d'algorithmes de réconciliation performants et spécifiques aux variables continues gaussiennes est donc absolument nécessaire pour permettre à ces nouveaux systèmes de concurrencer leurs analogues standard basés sur l'utilisation de photons uniques. La méthode de « réconciliation par tranches » *(sliced error correction)* proposée par Gilles Van Assche et ses collaborateurs à l'Université Libre de Bruxelles [24, 106] a permis de réaliser la première distribution de clé quantique utilisant des variables continues [20]. Son efficacité ne permet cependant pas d'envisager des transmissions sur plus de 10 kilomètres. Nous présenterons ici une nouvelle technique performante de réconciliation de variables continues s'inspirant des méthodes de modulation codée employées dans le domaine des communications numériques.

Ce dernier chapitre s'organise en trois sections. Nous rappellerons dans un premier temps le principe de la « réconciliation par tranches » et nous montrerons comment le problème de la réconciliation de variables continues peut s'énoncer comme un problème de transmission numérique. Nous présenterons ensuite brièvement les caractéristiques des codes LDPC *(Low Density Parity Check codes)* qui seront utilisés dans nos simulations.

Nous conclurons enfin ce chapitre en détaillant les résultats obtenus dans le cas de la réconciliation de variables aléatoires gaussiennes.

4.1 Réconciliation de variables aléatoires continues

Dans le scénario considéré ici, Alice et Bob ont respectivement accès aux n réalisations :

$$\mathbf{x} = (x_0, \ldots, x_{n-1}) \in \mathbb{R}^n \quad \text{et} \quad \mathbf{y} = (y_0, \ldots, y_{n-1}) \in \mathbb{R}^n$$

de deux variables aléatoires X et Y réelles corrélées. La densité de probabilité conjointe de ces deux variables est notée $p(x, y)$. L'objectif de la réconciliation des données est double, il s'agit pour Alice et Bob :

1. d'extraire $I(X;Y)$ bits d'information communs à partir des données continues $\mathbf{x}$ et $\mathbf{y}$,
2. de minimiser les échanges d'information permettant d'aboutir à ce résultat.

Afin de pouvoir intégrer facilement la réconciliation dans un protocole de cryptographie quantique, il est souhaitable que la séquence finale soit binaire puisqu'il est alors possible d'utiliser les techniques d'amplification de confidentialité mises au point pour les protocoles basés sur des photons uniques. Par ailleurs, on peut considérer que cette séquence n'est qu'une description binaire des données quantifiées d'Alice. La variable aléatoire représentant ces données quantifiées est notée $X_q = \mathcal{Q}(X)$, où $\mathcal{Q} : \mathbb{R}^d \mapsto \mathbb{R}^d$ $(d \in \mathbb{N}^*)$ est une fonction de quantification quelconque. En général la quantification inflige une pénalité car la quantité d'information réconciliable $I(X_q;Y)$ est alors toujours inférieure à $I(X;Y)$. Néanmoins, en choisissant une quantification infinitésimale des données d'Alice, $I(X_q;Y)$ peut approcher $I(X;Y)$ avec une précision arbitraire. Cette opération ne limite donc pas fondamentalement les performances de la réconciliation, et comme nous le verrons dans nos simulations, un nombre « raisonnable » d'intervalles suffit en pratique pour approcher $I(X;Y)$ avec une précision de 10^{-2}.

4.1.1 Compression de source avec information additionnelle

La réconciliation s'interprète naturellement comme une compression de source avec de l'information corrélée accessible au décodeur *(source coding with side information)*. Ce problème est un cas particulier de celui illustré figure 4.1, où deux sources représentées par les variables aléatoires X et Y doivent être compressées *séparément* et décodées *conjointement*. Le résultat étonnant démontré par Slepian et Wolf [21] pour des sources discrètes est que la compression indépendante des deux sources n'inflige pas de pénalité par rapport à une compression conjointe. Plus précisément, l'ensemble des taux de compression (R_X, R_Y) permettant une reconstruction parfaite des deux sources satisfont :

$$R_X \geq H(X|Y), \tag{4.1}$$
$$R_Y \geq H(Y|X), \tag{4.2}$$
$$R_X + R_Y \geq H(X,Y). \tag{4.3}$$

La réconciliation correspond à la situation où la source Y est directement accessible au décodeur. Le nombre minimum de bits qu'Alice doit transmettre à Bob pour que ce dernier

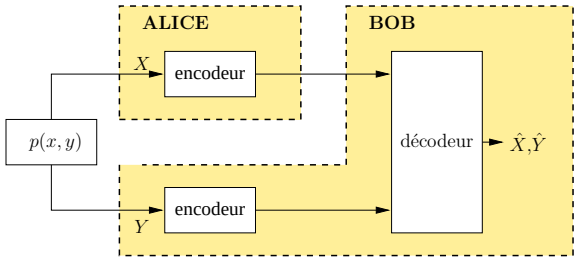


FIG. 4.1 – Compression indépendante de deux sources avec décodage conjoint.

reconstruise X sans erreur est donc :

$$\boxed{R_X \geq H(X|Y).} \tag{4.4}$$

Ce résultat reste valide lorsque X et Y sont des variables continues. En effet, en introduisant une quantification arbitrairement précise de X et Y représentée par les variables discrètes X_q et Y_q, on peut démontrer que le nombre de bits d'information à transmettre $H(X_q|Y_q)$ approche $H(X|Y)$ avec une précision arbitraire [16].

4.1.2 Réconciliation par tranches

La réconciliation par tranches proposée par Gilles Van Assche [24] est un protocole générique permettant de réconcilier des chaînes de symboles non binaires. Le principe de cette méthode est de convertir les symboles d'Alice et Bob en éléments binaires, puis d'utiliser des protocoles de correction binaires *(Binary Correction Protocol, BCP)* standard pour corriger les erreurs.

Principe général

La réconciliation par tranche est conçue pour des symboles multi-dimensionnels de $\mathbb{R}^d$, qu'Alice et Bob peuvent obtenir en regroupant leurs données $\mathbf{x} \in \mathbb{R}^n$ et $\mathbf{y} \in \mathbb{R}^n$ par blocs de taille d. Les l nouveaux symboles ainsi obtenus sont notés $\{x_i^{(d)}\}_{1..l}$ et $\{y_i^{(d)}\}_{1..l}$, et les variables aléatoires les représentant sont notées $X^{(d)} \in \mathbb{R}^d$ et $Y^{(d)} \in \mathbb{R}^d$. Une « tranche » $\mathcal{S}$ est définie comme une fonction $\mathcal{S} : \mathbb{R}^d \mapsto \mathrm{GF}(2)$. En choisissant m tranches $\{\mathcal{S}_i\}_{i=1..m}$ de façon appropriée, Alice peut partitionner $\mathbb{R}^d$ et associer à chaque symbole $x_i^{(d)}$ un label binaire $\mathcal{S}_{1..m}(x_i^{(d)}) = (\mathcal{S}_1(x_i^{(d)}), \ldots, \mathcal{S}_m(x_i^{(d)}))$. De son côté, Bob doit estimer la valeur des tranches d'Alice à partir de ses données corrélées. Le point clé de cette technique de réconciliation est que les tranches $\mathcal{S}_i$ sont corrigées *successivement*. Ainsi les « estimateurs de tranche » utilisés :

$$\tilde{\mathcal{S}}_1(y_i^{(d)}), \tilde{\mathcal{S}}_2(y_i^{(d)}, \mathcal{S}_1(x_i^{(d)})), \ldots, \tilde{\mathcal{S}}_m(y_i^{(d)}, \mathcal{S}_1(x_i^{(d)}), \ldots, \mathcal{S}_{m-1}(x_i^{(d)})), \tag{4.5}$$

prennent non seulement en compte la valeur du symbole $y_i^{(d)}$ dont Bob dispose, mais aussi la valeur des tranches déjà corrigées.

La définition exacte des tranches et de leurs estimateurs dépend de la distribution p_{XY}, néanmoins une fois que ces fonctions sont fixées, chaque tranche $i \in \{1..m\}$ est corrigée comme suit :

1. Alice calcule $\mathcal{S}_i(x_1^{(d)}), \ldots, \mathcal{S}_i(x_l^{(d)})$,
2. Bob calcule son estimation

$$\tilde{\mathcal{S}}_i(y_1^{(d)}, \mathcal{S}_{i-1}(x_1^{(d)}), \ldots, \mathcal{S}_1(x_1^{(d)})), \ldots, \tilde{\mathcal{S}}_i(y_l^{(d)}, \mathcal{S}_{i-1}(x_l^{(d)}), \ldots, \mathcal{S}_1(x_l^{(d)})),$$

3. les estimations erronnées de Bob sont corrigées à l'aide d'un BCP, tel que le protocole Cascade.

Performance de la réconciliation par tranches

Lorsque le codage s'effectue sur un nombre de symbole $l \to \infty$, il est possible d'après l'équation (4.4) de n'échanger que :

$$I_{min} = H(\mathcal{S}_{1..m}(X^{(d)})|Y^{(d)}) \tag{4.6}$$

bits d'information pour corriger toutes les erreurs. La correction successive des tranches à l'aide de BCP idéaux optimisés pour des canaux binaires symétriques impose cependant d'en échanger au moins :

$$I_{SEC} = \sum_{i=1}^{m} h(e_i), \tag{4.7}$$

où $e_i = \mathrm{P}\left[\mathcal{S}_i(X^{(d)}) \neq \tilde{\mathcal{S}}_i(Y^{(d)}, \mathcal{S}_{1..i-1}(X^{(d)}))\right]$ est le taux d'erreur binaire de la tranche i. En général, la réconciliation par tranche est donc sous-optimale puisque :

$$\begin{aligned} H(\mathcal{S}_{1..m}(X^{(d)})|Y^{(d)}) &\overset{(a)}{=} \sum_{i=1}^{m} H(\mathcal{S}_i(X^{(d)})|\mathcal{S}_{1..i-1}(X^{(d)}), Y^{(d)}), & (4.8)\\ &\overset{(b)}{\leq} \sum_{i=1}^{m} H(\mathcal{S}_i(X^{(d)})|\tilde{\mathcal{S}}_{1..i-1}(X^{(d)}), Y^{(d)}), & (4.9)\\ &\overset{(c)}{\leq} \sum_{i=1}^{m} h(e_i). & (4.10) \end{aligned}$$

L'égalité (a) s'obtient avec le développement en chaîne de l'entropie, l'inégalité (b) découle de la définition des estimateurs de tranche, et finalement (c) s'obtient en appliquant l'inégalité de Fano. Soulignons que l'écart entres les deux membres de cette dernière inégalité ne disparaît que si la dimension d des éléments est suffisamment large.

En pratique, les BCP utilisés ne sont pas parfaits, et dévoilent un surplus de bits $\xi h(e)$ par rapport à la limite idéale $h(e)$. Si ce surplus est aisément quantifiable pour des protocoles unidirectionnels, on ne peut obtenir qu'une borne supérieure dans le cas des protocoles interactifs tels que Cascade. En effet, en notant A l'information d'Alice, E l'information d'Eve et RA (RB) les parités dévoilées par Alice (Bob), $A|E \to RA|E \to RB|E$ ne forme généralement pas une chaîne de Markov lors d'une transmission quantique. Il est donc nécessaire de tenir compte de tous les bits échangés publiquement comme s'ils étaient indépendants, et non uniquement de ceux envoyés par Alice. En toute généralité, un BCP interactif dévoile donc environ $2(1+\xi)h(e)$ bits par symbole.

Choix des estimateurs de tranches

Puisque le nombre de bits dévoilés à chaque correction de tranche dépend de la correction des tranches précédentes, il est difficile d'optimiser les estimateurs $\tilde{\mathcal{S}}$ pour minimiser le nombre de bits total dévoilé lors de la réconciliation. En revanche, si l'on cherche uniquement à minimiser le nombre de bits dévoilés à chaque correction, l'estimateur optimal est simplement l'estimateur du maximum de vraisemblance [24] :

$$\tilde{\mathcal{S}}_i(y,\beta) = \arg\min_s \mathrm{P}\left[\mathcal{S}_i(X) = s | \mathcal{S}_{1..i-1} = \beta, Y = y\right]. \tag{4.11}$$

Limites de la réconciliation par tranches

En théorie il est préférable d'utiliser l'algorithme de réconciliation par tranches avec des symboles de grande dimension ($d \gg 1$) afin de réduire la différence entre les deux termes de l'inégalité (4.10). Il est cependant plus aisé en pratique de travailler avec $d = 1$ pour utiliser des BCP standard tels que Cascade et des codes correcteurs binaires. Cette simplification rend malheureusement l'algorithme largement sous-optimal. Le restant de ce chapitre est consacré à l'étude de nouveaux algorithmes de réconciliation améliorant les performances de la réconciliation par tranche dans le cas $d = 1$.

4.1.3 Codage canal avec information additionnelle

Reformulation du problème

La densité de probabilité conjointe $p(x, y)$ des variables aléatoires X et Y peut toujours s'écrire comme le produit $p(y|x)p(x)$. En d'autres termes, Bob aurait pu obtenir ses symboles $\mathbf{y}$ si Alice avait envoyé ses données $\mathbf{x}$ à travers un canal de transmission sans mémoire C_1, caractérisé par une probabilité de transition $p_1(y|x) = p(y|x)$.

De la même manière, on peut aussi introduire un canal de transmission artificiel entre les données d'Alice quantifiées et ses symboles continus. En effet, l'opération de quantification est définie par une partition $\{I_j\}_{0\ldots m-1}$ de $\mathbb{R}$ et m valeurs quantifiées $\hat{x}_j \in I_j$. En notant $\mathbf{1}_j(x) : \mathbb{R} \to \{0, 1\}$ la fonction indicatrice de chaque intervalle I_j, la fonction de quantification s'écrit explicitement :

$$\mathcal{Q} : \mathbb{R} \to \mathbb{R} : x \mapsto \sum_{j=1}^{m} \hat{x}_j \mathbf{1}_j(x). \tag{4.12}$$

La variable aléatoire $X_q = \mathcal{Q}(X)$ prend ainsi les valeurs discrètes $\{\hat{x}_j\}_{0\ldots m-1}$ avec les probabilités respectives $p_j = \Pr[X_q = \hat{x}_j] = \int p(x)\mathbf{1}_j(x)dx$. Le canal de transmission C_2 permettant d'obtenir les symboles continus $\mathbf{x}$ à partir des données quantifiées $\mathcal{Q}(\mathbf{x}) = (\mathcal{Q}(x_0), \ldots, \mathcal{Q}(x_{n-1}))$ est donc caractérisé par les probabilités de transition $p_2(x|\hat{x}_j) = p(x)\mathbf{1}_j(x)/p_j$. En conclusion, les symboles $\mathbf{y}$ auraient pu être générés en envoyant les symboles quantifiés $\mathcal{Q}(\mathbf{x})$ à travers un canal C_3 obtenu en concaténant les canaux C_1 et C_2, voir figure 4.2. Puisque les variables $X_q \to X \to Y$ forment une chaîne de Markov, la

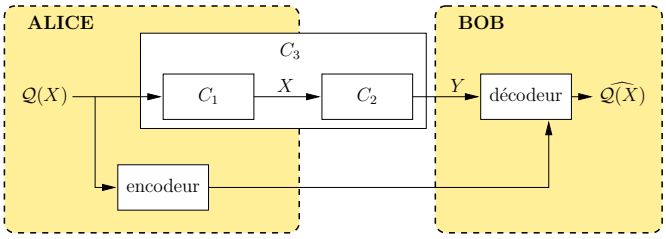


FIG. 4.2 – Réconciliation et codage canal.

probabilité de transition globale s'écrit :

$$p_3(y|\hat{x}_j) = \int p_1(y|x)p_2(x|\hat{x}_j)dx = \frac{\int p(x,y)\mathbf{1}_j(x)dx}{\int p(x)\mathbf{1}_j(x)dx}. \tag{4.13}$$

On retrouve ici un problème relativement classique de transmission numérique, la seule différence étant que les symboles $\mathcal{Q}(x)$ sont envoyés directement sur le canal C_3 sans passer par une phase de codage correcteur d'erreur. La redondance d'information permettant de corriger les erreurs de transmission est supposée directement accessible au récepteur (par exemple à travers un canal sans pertes).

Dans la mesure où la distribution de la variable X_q est fixée par la probabilité conjointe $p(x,y)$ et la quantification $\mathcal{Q}$, l'information mutuelle $I(X_q;Y)$ ne peut pas être optimisée, et calculer la capacité du canal C_3 n'a ici aucun sens. Néanmoins, il est tout de même possible d'appliquer le théorème de Shannon pour obtenir les taux R_c des codes correcteurs permettant à Bob de reconstruire X_q sans erreur :

$$R_c \leq I(X_q;Y) \leq I(X;Y). \tag{4.14}$$

Par abus de langage, la « capacité » du canal C_3 désignera par la suite l'information mutuelle $I(X_q;Y)$. Il est alors naturel de définir l'efficacité η d'un code de taux R_c :

$$\eta = \frac{R_c}{I(X;Y)} \leq \frac{I(X_q;Y)}{I(X;Y)}. \tag{4.15}$$

En remarquant que $R_c = H(X_q) - I_{red}$, où I_{red} est le nombre de bits d'information redondants (par symbole) introduits par le code correcteur, on vérifie aisément qu'un code d'efficacité maximum introduit une redondance minimale :

$$I_{red}^{min} = H(X_q) - I(X_q;Y) = H(X_q|Y). \tag{4.16}$$

La construction d'algorithmes de réconciliation revient donc à mettre en œuvre des codes correcteurs performants permettant de transmettre à la « capacité » du canal C_3.

4.1.4 Modulation codée

La reformulation du problème de la réconciliation en un problème de communication numérique est totalement artificielle, mais il devient alors naturel d'essayer d'adapter

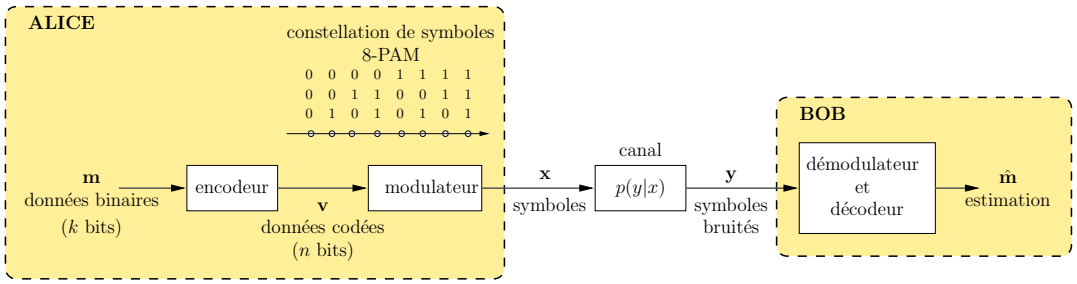


FIG. 4.3 – Principe général de la modulation codée.

certaines techniques de codage, et plus particulièrement les méthodes de modulation codée dont le principe est illustré figure 4.3.

Alice dispose d'une séquence binaire représentée par le vecteur $\mathbf{m}$ de k bits, qu'elle encode en une séquence $\mathbf{v}$ de n bits à l'aide d'un ou plusieurs codes correcteurs d'erreur. Ce codage introduit des corrélations entre les bits de $\mathbf{v}$, entièrement caractérisées par une matrice de parité $\mathbf{H}$ de dimension $(n-k) \times n$ telle que $\mathbf{v}\mathbf{H}^T = \mathbf{0}$. Les bits du vecteur $\mathbf{v}$ sont alors modulés, c.-à-d. regroupés en blocs de l bits identifiant un symbole $x \in \mathbb{R}^d$ parmi un ensemble discret (appelé constellation) d'au plus 2^l symboles. La fonction de modulation est notée :

$$\mu : \{0,1\}^l \to \mathbb{R}^d : (v_0 \dots v_{l-1}) \mapsto x. \tag{4.17}$$

Afin de simplifier l'analogie que nous ferons par la suite avec la réconciliation de variables continues réelles, nous supposerons ici que les symboles de la constellation sont réels ($d = 1$). Cette hypothèse simplificatrice ne nous permet d'envisager que des modulations d'amplitude *(Pulse Amplitude Modulation, PAM)*, comme c'est le cas figure 4.3 avec une modulation 8-PAM. La séquence de symboles $\mathbf{x}$ modulés est alors transmise à travers un canal bruité, supposé sans mémoire et caractérisé par une probabilité de transition $p(y|x)$. Au récepteur, Bob reconvertit les symboles reçus $\mathbf{y}$ en une séquence binaire et corrige les erreurs survenues en utilisant sa connaissance de $\mathbf{H}$. Le choix des labels, de la constellation de symboles, de la matrice $\mathbf{H}$ et des algorithmes de décodage conditionne fortement les performances d'un tel système. De nombreuses techniques telles que la modulation codée par treillis *(Trellis Coded Modulation, TCM)*, la modulation codée par entrelacement de bits *(Bit Interleaved Coded Modulation, BICM)* [107, 108] ou le codage multi-niveaux *(MultiLevel Coding, MLC)* [109, 110] ont été mises au point pour effectuer des transmissions à des débits proches de la capacité du canal.

Dans le cas de la réconciliation, si l'on identifie de façon unique chacune des m valeurs quantifiées $\hat{x}_j$ par un label de l bits ($l = \lceil \log_2 m \rceil$), la situation décrite figure 4.2 est similaire à un scénario de modulation codée. En notant $\mathcal{L}_j : \mathbb{R} \to \{0,1\}$ $(0 \leq j \leq l-1)$ les fonctions associant à chaque symbole réel x le j-ième bit du label de $\mathcal{Q}(x)$, le message équivalent au vecteur $\mathbf{v}$ de la modulation codée est un vecteur $\mathbf{v}'$ constitué de l'ensemble des bits $(\mathcal{L}_0(\mathbf{x}), \dots, \mathcal{L}_{l-1}(\mathbf{x}))$. La constellation de symboles est fixée par la quantification, et correspond à une modulation d'amplitude m-PAM. Le vecteur $\mathbf{v}'$ n'est cependant pas nécessairement un mot valide d'un code correcteur, et si $\mathbf{H}$ est la matrice de parité correspondante, en général $\mathbf{v}'\mathbf{H}^T = \mathbf{s} \neq \mathbf{0}$. Bob ne peut alors estimer correctement les symboles d'Alice que si cette dernière lui fait parvenir le syndrome $\mathbf{s}$ correspondant.

Parmi les nombreuses techniques de modulation codée existant, nous avons choisi

d'adapter les méthodes de BICM et MLC. Ces deux méthodes de modulation sont en effet connues pour permettre des transmissions à des taux proches de la capacité des canaux, et peuvent être utilisées avec des codes LDPC dont l'avantage est d'être à la fois performants et simples à mettre en œuvre. L'utilisation d'autre types de codes (tels que les Turbo-Codes) est tout aussi possible [106], mais leurs performances étant en général inférieures à celles des codes LDPC, il est peu probable que cela améliore l'efficacité de la réconciliation.

Réconciliation « BICM »

Le principe de la modulation codée par entrelacement de bits est illustré figure 4.4.

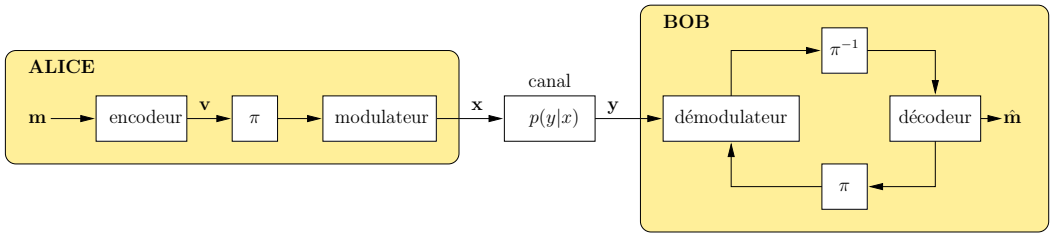


FIG. 4.4 – Principe de la modulation de type BICM.

Le message $\mathbf{m}$ d'Alice est codé à l'aide d'un encodeur unique en une séquence $\mathbf{v}$. Les bits de la séquence sont alors entrelacés pour former une séquence $\pi(\mathbf{v})$. Les bits de $\pi(\mathbf{v})$ sont modulés, et la séquence de symboles $\mathbf{x}$ correspondante est transmise sur le canal. Le rôle de l'entrelaceur (π) est de faire en sorte que les corrélations introduites par le codage soient indépendantes des corrélations introduites par la modulation. Ceci n'est effectivement le cas que si l'entrelaceur est de taille infinie, mais en pratique il suffit qu'il soit de l'ordre de quelques milliers de bits. Au récepteur les symboles reçus $\mathbf{y}$ sont démodulés, désentrelacés puis décodés. Comme nous le verrons dans la section 4.2, il est par ailleurs possible d'effectuer des itérations entre le démodulateur et le décodeur *(Bit Interleaved Coded Modulation with Iterative Decoding, BICM-ID)*.

L'algorithme de la réconciliation inspirée de cette technique est représenté figure 4.5.

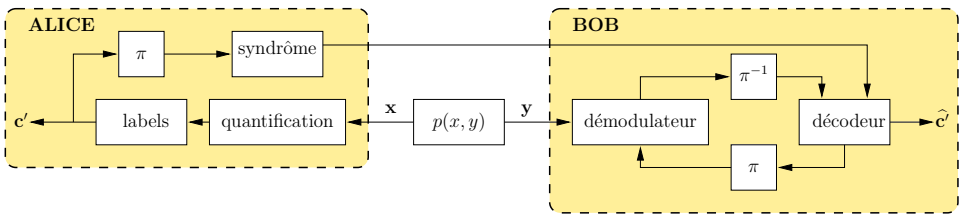


FIG. 4.5 – Réconciliation de type BICM.

Alice quantifie et étiquette ses symboles continus $\mathbf{x}$ pour obtenir une séquence binaire $\mathbf{v}' = (\mathcal{L}_0(\mathbf{x}), \ldots, \mathcal{L}_{l-1}(\mathbf{x}))$. Cette séquence est entrelacée, puis les syndromes $\mathbf{s} = \mathbf{v}'\mathbf{H}^T$ sont transmis à Bob. De son côté ce dernier effectue alors itérativement la démodulation et le décodage de ses symboles $\mathbf{y}$, en prenant en compte l'information additionnelle $\mathbf{s}$.

Réconciliation « MLC-MSD »

L'idée fondamentale de la modulation multi-niveaux part de la constatation que chaque symbole x transmis est décrit de façon unique par un label binaire $(x^0, \ldots, x^{l-1})$ de l bits, et donc l'information mutuelle $I(X;Y)$ entre le symbole émis et celui reçu est égale à l'information mutuelle $I(X^0, \ldots, X^{l-1}; Y)$ entre le label binaire et le symbole reçu. En appliquant la loi de développement en chaîne de l'information mutuelle, on obtient :

$$I(X;Y) = I(X^0, \ldots, X^{l-1}; Y) = \sum_{i=0}^{l-1} I(X^i; Y | X^0, \ldots, X^{i-1}). \tag{4.18}$$

Cette expression signifie que la transmission du symbole x sur le canal physique est équivalente à la transmission en parallèle des l bits x_i $(i \in \{1..l\})$ du label binaire, à condition que chaque canal i soit caractérisé par la probabilité de transition :

$$f(y|x^i, x^{i-1}, \ldots, x^0). \tag{4.19}$$

Le codage de chaque « niveau » du label binaire peut donc être effectué séparément. Le décodage doit toutefois se faire globalement puisque les canaux de transmission ne sont pas indépendants. L'équation (4.18) suggère cependant une méthode de décodage simple consistant à décoder successivement les niveaux i, en utilisant les résultats de décodage des niveaux précédents $1, \ldots, i-1$. Cette technique est appelée décodage multi-étape *(MultiStage Decoding, MSD)*. Une autre conséquence de l'équation (4.18) est que la capacité du canal C est égale à la somme des capacités C_i des l canaux parallèles, et que cette capacité est atteignable avec un décodage multi-étape.

La figure 4.6 illustre ce principe de modulation dans le cas où chaque symbole x de la constellation 4-PAM est identifié par un label (x^1, x^2) de 2 bits.

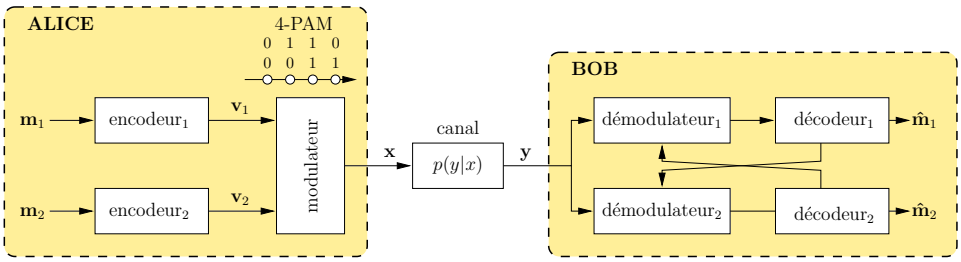


FIG. 4.6 – Principe de la modulation de type MLC.

Alice sépare tout d'abord ses données $\mathbf{m}$ en deux chaînes binaires $\mathbf{m}_1$ et $\mathbf{m}_2$ puis les encode séparément. Les chaînes codées $\mathbf{v}_1$ et $\mathbf{v}_2$ sont alors utilisées pour définir la séquence transmise de symboles $\mathbf{x}$. Au récepteur, Bob estime le message envoyé par Alice à partir de ses symboles $\mathbf{y}$. En théorie la procédure MSD est optimale, mais en pratique les codes correcteurs utilisés ne sont pas idéaux et les taux permettant effectivement de corriger toutes les erreurs à chaque niveau sont strictement inférieurs à la capacité du niveau. Il est cependant possible de réduire la perte de performance en effectuant des itérations successives entres les niveaux *(Iterative MultiStage Decoding, IMSD)*.

La méthode de réconciliation basée sur le principe de MLC-MSD est représentée figure 4.7.

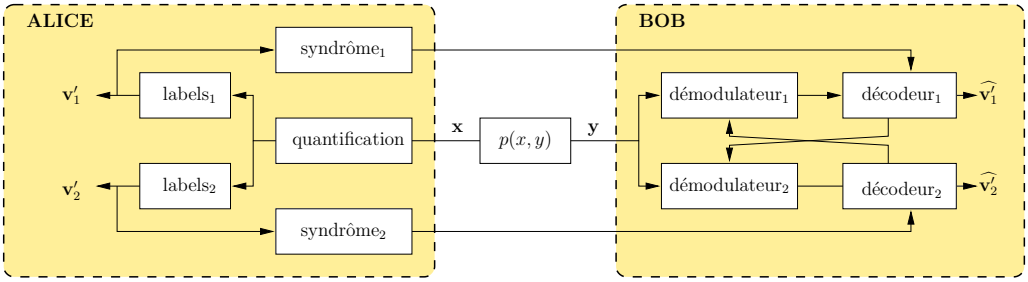


FIG. 4.7 – Réconciliation de type MLC.

Après quantification et étiquetage de ses données, Alice dispose de 2 séquences $\mathbf{v}'_1 = \mathcal{L}_1(\mathbf{x})$ et $\mathbf{v}'_2 = \mathcal{L}_2(\mathbf{x})$. A l'aide de 2 codes correcteurs d'erreurs différents, les syndromes $\mathbf{s}_1 = \mathbf{v}'_1\mathbf{H}_1^T$ et $\mathbf{s}_2 = \mathbf{v}'_2\mathbf{H}_2^T$ sont calculés puis envoyés à Bob. Ce dernier peut alors démoduler et décoder ses symboles pour estimer les données d'Alice.

Interprétation de la réconciliation par tranches

La réconciliation par tranches appliquée à des symboles réels ($d = 1$ en reprenant les notations de la section 4.1.2) peut s'interpréter comme un cas particulier de réconciliation MLC-MSD. En effet, si au lieu d'envoyer les syndromes $\mathbf{s}_i$ pour chaque niveau Alice met en œuvre un BCP, le décodage multi-étape est strictement équivalent à la réconciliation par tranches. Bien qu'en théorie cette procédure soit optimale, son efficacité est limitée lorsque les codes sont de taille finie, et comme nous l'avons mentionné dans la section 4.1.2, l'évaluation la plus générale du nombre de bits dévoilés par un BCP interactif est pénalisante. Nous pouvons donc espérer obtenir une meilleure efficacité en exploitant au maximum les possibilités du codage multi-niveaux, c.-à-d. :

1. en utilisant des codes unidirectionnels performants à la place des BCP,
2. en mettant en œuvre un décodage itératif, ce qui évite d'avoir à corriger toutes les erreurs d'un niveau avant de décoder le suivant.

Il faut cependant souligner que la réconciliation par tranches basée sur des BCP ne requiert que des échanges de parités. L'algorithme présente donc une faible complexité calculatoire, alors que l'utilisation de codes plus complexes et d'un décodage itératif requiert significativement plus d'opérations. En pratique le temps de calcul est un paramètre tout aussi important que l'efficacité pour obtenir des débits élevés.

4.2 Codes LDPC

Les codes LDPC ont été étudiés pour la première fois par Robert Gallager au début des années soixante [111], mais ont été complètement oubliés jusqu'à leur redécouverte dans les années 1990. Les performances impressionnantes de ces codes et leur simplicité en font aujourd'hui des concurrents très sérieux aux Turbo-Codes.

4.2.1 Caractéristiques et représentation des codes LDPC

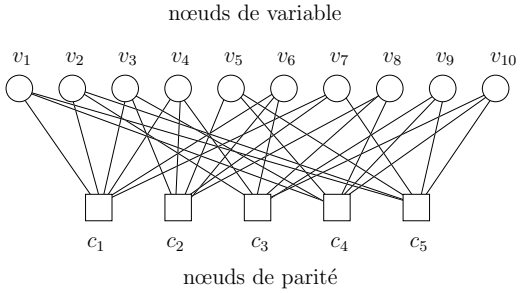
Comme son nom l'indique, un code LDPC est caractérisé par une matrice de parité $\mathbf{H} = \{h_{ij}\}_{i=1..n-k}^{j=1..n} \in GF(2)^{n-k,n}$ contenant un faible nombre de 1 par rapport au nombre de 0. Si cette matrice était générée aléatoirement, le nombre d'entrées non nulles de la matrice $\mathbf{H}$ serait de l'ordre de $\mathcal{O}(n^2)$, alors qu'il n'est ici que de $\mathcal{O}(n)$. Les codes LDPC sont généralement représentés par un graphe appelé graphe de Tanner, contenant deux types de nœuds :

- les nœuds de *variable*, qui représentent les bits du mot de code,
- les nœuds de *parité*, qui représentent les contraintes de parité imposée par la matrice $\mathbf{H}$.

Un nœud de variable j est connecté à un nœud de parité i si et seulement si l'élément h_{ij} de la matrice $\mathbf{H}$ est égal à 1. Le *degré* d'un nœud est alors défini comme le nombre de branches connectées à ce nœud. La figure 4.8 illustre cette représentation avec un exemple simple.

$$\mathbf{H} = \begin{array}{c} \begin{array}{cccccccccc} v_1 & v_2 & v_3 & v_4 & v_5 & v_6 & v_7 & v_8 & v_9 & v_{10} \end{array} \\ \left[\begin{array}{cccccccccc} 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{array}\right] \end{array} \begin{array}{c} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \end{array}$$

(a) Matrice de parité.



(b) Graphe de Tanner.

FIG. 4.8 – Matrice de parité et graphe de Tanner d'un code LDPC de taille $n = 10$ et de taux 1/2.

Un code LDPC est qualifié de *régulier* lorsque tous les nœuds de variable ont le même degré d_v et tous les nœuds de parité ont le même degré d_c. Dans le cas contraire on parle de code *irrégulier*. La distribution des degrés d'un graphe de Tanner est souvent résumée à l'aide de deux polynômes :

$$\lambda(x) = \sum_{i=1}^{d_v^{max}} \lambda_i x^{i-1}, \quad \rho(x) = \sum_{i=1}^{d_c^{max}} \rho_i x^{i-1}, \tag{4.20}$$

où :

- d_v^{max} (d_c^{max}) est le degré maximum des nœuds de variable (parité),
- λ_i (ρ_i) est la proportion de branches connectées aux noeuds de variable (parité) de degré i.

Les nombres de nœuds de variable $n_v^{(i)}$ et de nœuds de parité $n_c^{(i)}$ de degré i s'écrivent alors respectivement :

$$n_v^{(i)} = n\frac{\lambda_i/i}{\sum_{j\geq 1}\lambda_j/j} = n\frac{\lambda_i/i}{\int_0^1 \lambda(x)dx}, \quad \text{et} \quad n_c^{(i)} = (n-k)\frac{\rho_i/i}{\sum_{j\geq 1}\rho_j/j} = (n-k)\frac{\rho_i/i}{\int_0^1 \rho(x)dx}. \tag{4.21}$$

Puisque le nombre total de branches du graphe est $E = \sum_i in_v^{(i)} = \sum_i in_c^{(i)}$, on en déduit le taux du code :

$$r(\lambda, \rho) = \frac{n-k}{n} = 1 - \frac{\int_0^1 \rho(x)dx}{\int_0^1 \lambda(x)dx}. \tag{4.22}$$

Par exemple les distributions de degré du code représenté figure 4.8 sont $\lambda(x) = x^2$ et $\rho(x) = x^5$ (le code est régulier) et $r(\lambda, \rho) = 1/2$.

Soulignons que $r(\lambda, \rho)$ n'est le taux réel du code que si les contraintes de parité sont indépendantes, en pratique les taux peuvent être très légèrement inférieurs. Comme nous le verrons dans la section suivante, les distributions de degrés suffisent à caractériser un code LDPC.

4.2.2 Décodage des codes LDPC

Les meilleures performances affichées par les codes LDPC (et les Turbo-Codes) pour des tailles finies sont en grande partie dues au fait que leur décodage s'effectue de façon « molle » *(soft decoding)*. Plutôt que de calculer uniquement la valeur des bits *(hard decoding)*, ce type de décodage fournit en plus la confiance associée à la décision.

Pour une variable binaire $v \in \{0, 1\}$, la confiance est décrite par les probabilités $\Pr[v = 0]$ et $\Pr[v = 1]$. Puisque $\Pr[v = 0] + \Pr[v = 1] = 1$, un seul paramètre est nécessaire à la description, et l'on choisit souvent le logarithme du rapport des probabilités :

$$\lambda = \log\left(\frac{\Pr[v = 1]}{\Pr[v = 0]}\right). \tag{4.23}$$

Le signe de λ indique alors la valeur la plus probable de v : lorsque $\lambda > 0$ la valeur 1 est plus probable et vice-versa. La valeur absolue $|\lambda|$ fournit elle une indication sur la confiance de l'estimation : lorsque $|\lambda| = 0$ les valeurs 1 et 0 sont équiprobables, lorsque $|\lambda| = \infty$ la valeur de v est parfaitement connue.

L'objectif d'un code correcteur d'erreur est d'estimer la valeur d'un message $\mathbf{v}$ de n bits à partir d'une séquence de symboles reçus $\mathbf{y}$ (aussi appelés « observations ») et d'un syndrome $\mathbf{s}$. La probabilité de décodage erroné du i-ième bit v_i est minimisée en basant la décision sur le maximum *a posteriori* (MAP) :

$$\hat{v}_i = \arg\max_{v \in \{0,1\}} \Pr[v_i = v | \mathbf{y}, \mathbf{s}]. \tag{4.24}$$

De manière équivalente on peut utiliser le logarithme du rapport de vraisemblance *a posteriori* :

$$\lambda_i = \log\left(\frac{\Pr[v_i = 1 | \mathbf{y}, \mathbf{s}]}{\Pr[v_i = 0 | \mathbf{y}, \mathbf{s}]}\right), \tag{4.25}$$

et baser la décision sur le signe de λ_i. Dans le cas des codes LDPC, λ_i peut se calculer simplement à l'aide d'un algorithme itératif. Nous présenterons dans un premier temps cet algorithme de décodage dans le cas où la modulation s'effectue sur une constellation de deux symboles [111, 112], puis nous généraliserons le résultat au cas d'une constellation plus générale.

Constellation de deux symboles

Lorsque la constellation utilisée pour une modulation codée ne contient que deux symboles, la modulation est une fonction bijective $\mu : \{0,1\} \rightarrow \mathbb{R}$. Chaque symbole reçu est donc déterminé de façon unique par un seul bit. Par exemple la modulation antipodale consiste à associer aux bits 0 et 1 les symboles -1 et 1. En introduisant le vecteur $\mathbf{y}_{\neq i} = (y_0 \dots y_{i-1}, y_{i+1}, y_{n-1})$ qui contient toutes les observations à l'exception de y_i, λ_i peut se développer comme suit :

$$\begin{aligned}
\lambda_i = \log\left(\frac{\Pr[v_i = 1|\mathbf{y},\mathbf{s}]}{\Pr[v_i = 0|\mathbf{y},\mathbf{s}]}\right) &= \log\left(\frac{\Pr[v_i = 1|y_i,\mathbf{y}_{\neq i},\mathbf{s}]}{\Pr[v_i = 0|y_i,\mathbf{y}_{\neq i},\mathbf{s}]}\right) \\
&= \log\left(\frac{\Pr[y_i|v_i = 1,\mathbf{y}_{\neq i},\mathbf{s}]}{\Pr[y_i|v_i = 0,\mathbf{y}_{\neq i},\mathbf{s}]}\right) + \log\left(\frac{\Pr[v_i = 1|\mathbf{y}_{\neq i},\mathbf{s}]}{\Pr[v_i = 0|\mathbf{y}_{\neq i},\mathbf{s}]}\right) \\
&= \underbrace{\log\left(\frac{\Pr[y_i|v_i = 1]}{\Pr[y_i|v_i = 0]}\right)}_{\lambda_i^{int}} + \underbrace{\log\left(\frac{\Pr[v_i = 1|\mathbf{y}_{\neq i},\mathbf{s}]}{\Pr[v_i = 0|\mathbf{y}_{\neq i},\mathbf{s}]}\right)}_{\lambda_i^{ext}}. \quad (4.26)
\end{aligned}$$

Le terme λ_i^{int}, qui ne dépend que de la probabilité de transition du canal, est appelé *information intrinsèque* et est calculé par le démodulateur. Le terme λ_i^{ext}, qui dépend lui des corrélations entre bits introduites par le code correcteur d'erreur, est appelé *information extrinsèque* et est calculé par le décodeur.

Comme représenté sur le graphe de Tanner de la figure 4.9, le bit v_i est supposé intervenir dans p équations de parité. Pour chaque équation de parité $j \in \{0, \dots, p-1\}$, nous utiliserons les notations suivantes :

- $\mathbf{v}_j = (v_j^1, \dots, v_j^{d_j})$ est le groupe de bits autres que v_i intervenant dans l'équation de parité,
- $\mathbf{v}_j^{\oplus}$ est la parité du groupe $\mathbf{v}_j$,
- s_i^j est l'élément du syndrome $\mathbf{s}$ caractérisant l'équation de parité.

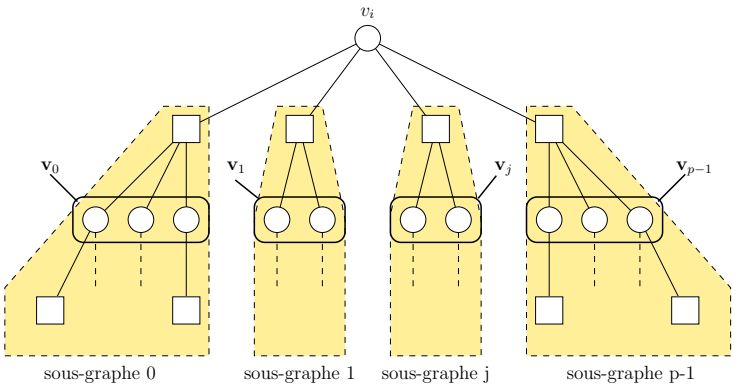


FIG. 4.9 – Graphe de Tanner vu depuis le nœud v_i

Les équations de parité et le syndrome imposent alors les relations :

$$\forall j \in \{0, \dots, p-1\} \quad v_i \oplus \mathbf{v}_j^{\oplus} = s_i^j \quad \Leftrightarrow \quad \forall j \in \{0, \dots, p-1\} \quad \mathbf{v}_j^{\oplus} = s_i^j \oplus v_i. \quad (4.27)$$

Si le graphe ne comporte pas de cycles, les p parités sont conditionnellement indépendantes lorsque $\mathbf{y}_{\neq i}$ est connu. L'information extrinsèque peut donc se réécrire :

$$\begin{aligned}
\lambda_i^{ext} &= \log\left(\frac{\Pr\left[\forall j\ \mathbf{v}_j^{\oplus} = s_i^j \oplus 1 | \mathbf{y}_{\neq i}, \mathbf{s}\right]}{\Pr\left[\forall j\ \mathbf{v}_j^{\oplus} = s_i^j \oplus 0 | \mathbf{y}_{\neq i}, \mathbf{s}\right]}\right), \\
&= \sum_{j=0}^{p-1} \log\left(\frac{\Pr\left[\mathbf{v}_j^{\oplus} = s_i^j \oplus 1 | \mathbf{y}_{\neq i}, \mathbf{s}\right]}{\Pr\left[\mathbf{v}_j^{\oplus} = s_i^j \oplus 0 | \mathbf{y}_{\neq i}, \mathbf{s}\right]}\right), \\
&= \sum_{j=0}^{p-1} \left(1 - 2s_i^j\right) \underbrace{\log\left(\frac{\Pr\left[\mathbf{v}_j^{\oplus} = 1 | \mathbf{y}_{\neq i}, \mathbf{s}\right]}{\Pr\left[\mathbf{v}_j^{\oplus} = 0 | \mathbf{y}_{\neq i}, \mathbf{s}\right]}\right)}_{\lambda_{j,\oplus}}.
\end{aligned} \tag{4.28}$$

Le rapport de vraisemblance $\lambda_{j,\oplus}$ peut s'exprimer en fonction des rapports de vraisemblance de chacun des bits intervenant dans le calcul de la parité. En effet, si b_1 et b_2 représentent deux variables binaires :

$$\begin{aligned}
\tanh\left(\frac{-\lambda_{b_1 \oplus b_2}}{2}\right) &= \frac{\Pr\left[b_1 \oplus b_2 = 0\right] - \Pr\left[b_1 \oplus b_2 = 1\right]}{\Pr\left[b_1 \oplus b_2 = 0\right] + \Pr\left[b_1 \oplus b_2 = 1\right]}, \\
&= \frac{\sum_{b \in \{0,1\}} \Pr\left[b_1 = b\right] \left(\Pr\left[b_2 = b\right] - \Pr\left[b_2 = \bar{b}\right]\right)}{\sum_{b \in \{0,1\}} \Pr\left[b_1 = b\right] \left(\Pr\left[b_2 = b\right] + \Pr\left[b_2 = \bar{b}\right]\right)}, \\
&= \frac{\left(\Pr\left[b_1 = 0\right] - \Pr\left[b_1 = 1\right]\right)\left(\Pr\left[b_2 = 0\right] - \Pr\left[b_2 = 1\right]\right)}{\left(\Pr\left[b_1 = 0\right] + \Pr\left[b_1 = 1\right]\right)\left(\Pr\left[b_2 = 0\right] + \Pr\left[b_2 = 1\right]\right)}, \\
&= \tanh\left(\frac{-\lambda_{b_1}}{2}\right) \tanh\left(\frac{-\lambda_{b_2}}{2}\right).
\end{aligned} \tag{4.29}$$

Ce développement se généralise par récurrence à des équations de parité faisant intervenir un nombre arbitraire de bits. En utilisant cette propriété, l'équation (4.28) se réécrit :

$$\lambda_{j,\oplus} = -2 \tanh^{-1}\left(\prod_{k=0}^{d_j - 1} \tanh \frac{-\lambda_{j,k}}{2}\right) \quad \text{avec} \quad \lambda_{j,k} = \log \frac{\Pr\left[v_j^k = 1 | \mathbf{y}_{\neq j}, \mathbf{s}\right]}{\Pr\left[v_j^k = 0 | \mathbf{y}_{\neq j}, \mathbf{s}\right]}. \tag{4.30}$$

Bien que les bits v_j^k et v_i ne soient pas indépendants (ils interviennent dans la même équation de parité) v_j^k est indépendant de v_i conditionnellement aux observations $\mathbf{y}_{\neq i}$. Le terme $\lambda_{j,k}$ est donc par définition indépendant de l'observation y_i, et si le graphe ne contient pas de cycles, ce terme est aussi indépendant de toutes les observations des bits auxquels v_j^k n'est connecté qu'au travers de v_i. La valeur de $\lambda_{j,k}$ ne dépend alors que des observations du sous-graphe j. Cette constatation permet donc de calculer *récursivement* λ_i en propageant les équations (4.26) et (4.30) dans les sous-graphes. Les rapports de vraisemblances calculés lors de la récursion peuvent alors s'interpréter comme des « messages » échangés entre les nœuds de variables et de parité.

Il est important de noter que l'expression de λ_i donnée dans l'équation (4.26) n'est valide que si la distribution *a priori* de v_i est uniforme. Ce n'est pas toujours le cas lors de la réconciliation puisque les mots de codes $\mathbf{v}$ sont obtenus par quantification d'une variable

continue quelconque, mais il suffit alors de modifier le terme d'information intrinsèque λ_i^{int} et d'utiliser les probabilités conjointes au lieu des probabilités conditionnelles :

$$\lambda_i^{int} = \log \frac{\Pr[y_i, v_i = 1]}{\Pr[y_i, v_i = 0]}. \tag{4.31}$$

L'algorithme « somme-produit » *(Sum-Product, SP)* permet de décoder les codes LDPC en exploitant cette propriété de récurrence [113]. Tous les rapports de vraisemblance λ_i ($i \in \{0, \ldots, n-1\}$) sont calculés simultanément, par échanges successifs de messages entre les nœuds de variable et parité. Les notations utilisées dans la description de l'algorithme table 4.1 sont les suivantes :

- les nœuds de variable et de parité sont notés $(v_0, \ldots, v_{n-1})$ et $(c_0, \ldots, c_{n-k-1})$,
- l'ensemble des indices des nœuds de parité connectés à un nœud de variable v_i est noté $\mathcal{M}(i)$ (il se déduit directement de la matrice de parité $\mathbf{H}$: $\mathcal{M}(i) = \{j : h_{j,i} = 1\}$) et de même l'ensemble des indices des nœuds de variable connectés à un nœud de parité c_j est noté $\mathcal{N}(j)$ ($\mathcal{N}(j) = \{i : h_{j,i} = 1\}$),
- le bit du syndrome associé au nœud de parité c_j et noté s_j,
- le message envoyé d'un nœud v_i à un nœud c_j durant l'itération ℓ est noté $v_{ij}^{(\ell)}$, et le message inverse est noté $u_{ji}^{(\ell)}$.

– **Initialisation.**

$$\forall i \in \{0..n-1\}\ \forall j \in \mathcal{M}(i) \qquad u_{ji}^{(0)} = 0,$$
$$\forall i \in \{0..n-1\}\ \forall j \in \mathcal{M}(i) \qquad v_{ij}^{(0)} = \lambda_i^{(0)} = \log \frac{\Pr[y_i, v_i = 1]}{\Pr[y_i, v_i = 0]},$$

– **Itérations.** Pour ℓ allant de 1 à ℓ_{max} :

$$\forall j \in \{0 \ldots n-k-1\}\ \forall i \in \mathcal{N}(j) \qquad u_{ji}^{(\ell)} = 2 \tanh^{-1} \prod_{k \in \mathcal{N}(j) \setminus i} \tanh \frac{v_{kj}^{(\ell-1)}}{2},$$
$$\forall i \in \{0 \ldots n\}\ \forall j \in \mathcal{M}(i) \qquad v_{ij}^{(\ell)} = \lambda_i^{(0)} + \sum_{k \in \mathcal{M}(i) \setminus j} (1 - 2s_k) u_{ki}^{(\ell)},$$

– **Terminaison.**

$$\forall i \in \{0..n\} \quad \lambda_i = \lambda_i^{(0)} + \sum_{k \in \mathcal{M}(i)} (1 - 2s_k) u_{ki}^{(\ell_{max})},$$
$$\forall i \in \{0..n\} \quad v_i = \text{signe}(\lambda_i).$$

TAB. 4.1 – Algorithme SP de décodage des codes LDPC.

Il est important de noter que les mises à jour des messages se font de manière à éviter des cycles dans les échanges d'information. Par exemple, le message $u_{ji}^{(\ell)}$ envoyé pendant l'itération ℓ par le nœud de parité j au nœud de variable i ne prend pas en compte le message $v_{ij}^{(\ell-1)}$ envoyé en sens inverse lors de l'itération précédente. Cette précaution permet de garantir que les valeurs λ_i calculées convergent en un nombre fini d'itérations

vers les vrais rapports de vraisemblance *a posteriori* lorsque le graphe est sans cycle. En pratique la plupart des graphes de codes LDPC présentent des cycles, néanmoins si la taille du code reste suffisamment grande (de l'ordre de quelques milliers de bits) l'algorithme SP permet toujours de corriger efficacement les erreurs [114]. Par ailleurs, l'ordre de mise à jour des différents messages n'est pas forcément tenu de respecter celui présenté ici. Si le graphe de Tanner ne contient pas de cycle, la convergence de l'algorithme est assurée quelque soit l'ordre choisi, mais la vitesse de convergence peut varier. Un ordre de mise à jour plus astucieux que celui décrit ici a récemment été proposé, et multiplie par près de deux la vitesse de convergence [115].

Lorsque la modulation antipodale est effectuée sur un canal gaussien (ajoutant un bruit de variance σ^2 au signal transmis) et que les symboles sont équiprobables, l'information intrinsèque se simplifie :

$$\lambda_i^{(0)} = \log \frac{\Pr\left[y_i, c_i = 1\right]}{\Pr\left[y_i, c_i = 0\right]} = \frac{2}{\sigma^2} y_i. \tag{4.32}$$

Lorsque seul le mot de code constitué de n bits « 1 » est transmis, $\lambda_i^{(0)}$ a une distribution de probabilité gaussienne de moyenne $m = 2/\sigma^2$ et de variance $4/\sigma^2 = 2m$. Les distributions gaussiennes de variance égale à deux fois la moyenne seront utilisées par la suite pour modéliser une information *a priori* gaussienne.

Constellation de plus de deux symboles

Nous supposerons ici que chaque symbole de la constellation est décrit par un label de l bits. Le message codé d'Alice de nl bits est noté

$$\mathbf{v} = (v_{0,1}, \ldots, v_{0,l}, v_{1,1}, \ldots, v_{1,l}, \ldots, v_{n-1,1}, \ldots, v_{n-1,l}),$$

et est modulé en une séquence $\mathbf{x} = (x_0, \ldots, x_{n-1})$ de n symboles. Bob n'en observe qu'une version dégradée $\mathbf{y}$. Comme précédemment, on peut isoler un terme d'information extrinsèque dans le rapport de vraisemblance *a posteriori* d'un bit $v_{i,i'}$:

$$\lambda_{i,i'} = \underbrace{\log\left(\frac{\Pr\left[y_i | v_{i,i'} = 1, \mathbf{y}_{\neq i}, \mathbf{s}\right]}{\Pr\left[y_i | v_{i,i'} = 0, \mathbf{y}_{\neq i}, \mathbf{s}\right]}\right)}_{\lambda_{i,i'}^{int}} + \underbrace{\log\left(\frac{\Pr\left[v_{i,i'} = 1 | \mathbf{y}_{\neq i}, \mathbf{s}\right]}{\Pr\left[v_{i,i'} = 0 | \mathbf{y}_{\neq i}, \mathbf{s}\right]}\right)}_{\lambda_{i,i'}^{ext}}. \tag{4.33}$$

Le terme extrinsèque est identique à celui obtenu dans l'équation (4.26), en revanche le terme intrinsèque ne peut plus se simplifier puisque le bit $v_{i,i'}$ ne détermine pas de façon unique l'observation y_i. En introduisant la variable conditionnelle x_i dans l'expression de

$\lambda_{i,i'}$ on obtient :

$$\begin{aligned}
\lambda_{i,i'} &= \log\left(\frac{f\left(y_i|v_{i,i'}=1,\mathbf{y}_{\neq i},\mathbf{s}\right)}{f\left(y_i|v_{i,i'}=0,\mathbf{y}_{\neq i},\mathbf{s}\right)}\right), \\
&= \log\frac{\sum_x f\left(y_i|x_i=x,v_{i,i'}=1,\mathbf{y}_{\neq i},\mathbf{s}\right)\Pr\left[x_i=x|v_{i,i'}=1,\mathbf{y}_{\neq i},\mathbf{s}\right]}{\sum_x f\left(y_i|x_i=x,v_{i,i'}=0,\mathbf{y}_{\neq i},\mathbf{s}\right)\Pr\left[x_i=x|v_{i,i'}=0,\mathbf{y}_{\neq i},\mathbf{s}\right]}, \\
&= \log\frac{\sum_{x\in\chi_{i',1}} f\left(y_i|x_i=x\right)\prod_{k\neq i'}\Pr\left[v_{i,k}=x^k|\mathbf{y}_{\neq i},\mathbf{s}\right]}{\sum_{x\in\chi_{i',0}} f\left(y_i|x_i=x\right)\prod_{k\neq i'}\Pr\left[v_{i,k}=x^k|\mathbf{y}_{\neq i},\mathbf{s}\right]},
\end{aligned} \tag{4.34}$$

où $\chi_{i',b}$ est l'ensemble des symboles de la constellation dont le i'-ième bit du label est b, et x^k représente le k-ième bit du label du symbole x. La dernière égalité est une conséquence de l'indépendance des variables $v_{i,k}$ conditionnellement à $\mathbf{y}_{\neq i}$. Les probabilités $\Pr\left[v_{i,k}=x^k|\mathbf{y}_{\neq i},\mathbf{s}\right]$ peuvent s'exprimer en fonction des rapports de vraisemblance $\lambda_{i,k}$ associés :

$$\Pr\left[v_{i,k}=x^k|\mathbf{y}_{\neq i},\mathbf{s}\right]=\frac{\exp\left(x^k\lambda_{i,k}\right)}{1+\exp\left(\lambda_{i,k}\right)}. \tag{4.35}$$

Par ailleurs, on peut de nouveau prendre en compte la non-uniformité de la distribution *a priori* des symboles en introduisant les probabilités conjointes, et le terme d'information intrinsèque utile s'écrit donc après quelques calculs :

$$\lambda_{i,i'}=\log\frac{\sum_{x\in\chi_{i',1}} f\left(y_i,x_i=x\right)\exp\left(\sum_{k\neq i'}x^k\lambda_{i,k}\right)}{\sum_{x\in\chi_{i',0}} f\left(y_i,x_i=x\right)\exp\left(\sum_{k\neq i'}x^k\lambda_{i,k}\right)}. \tag{4.36}$$

L'information intrinsèque dépend à la fois du canal de transmission à travers les termes $f(y_i,x_i)$, mais aussi des information extrinsèques $\lambda_{i,k}$ sur les autres bits intervenant dans le label binaire du symbole transmis. La possibilité d'effectuer des itérations entre le démodulateur et le décodeur apparaît clairement dans la structure de cette équation. En effet, bien qu'aucune information en provenance du décodeur ne soit accessible lors de la première démodulation ($\lambda_{i,k}=0$), les rapports de vraisemblance après une tentative de décodage peuvent être réutilisés pour améliorer le calcul de l'information intrinsèque. Cette équation ne dépend pas de la structure exacte du décodeur et s'applique donc à la fois au cas d'une modulation BIMC ou MLC/MSD.

L'algorithme de démodulation et décodage pour une modulation BICM basé sur l'algorithme SP est décrit table 4.2. Les notations utilisées sont les suivantes :

- les nœuds de variable au niveau i sont notés $(v_{i,0}\dots v_{i,n-1})$, les nœuds de parité sont notés $(c_0\dots c_{K-1})$,
- l'ensemble des indices des nœuds de parité connectés à un nœud de variable $v_{i,k}$ est noté $\mathcal{M}(i,k)$,

- l'ensemble des paires d'indices des nœuds de variable connectés à un nœud de parité c_j est noté $\mathcal{N}(j)$,
- le bit du syndrome associé au nœud de parité c_j et noté s_j,
- le message envoyé d'un nœud $v_{i,k}$ à un nœud c_j durant l'itération ℓ est noté $v^{(\ell)}_{(i,k)j}$, et le message inverse est noté $u^{(\ell)}_{j(i,k)}$.

- **Initialisation.**

$$\forall i \in \{0..n-1\}\ \forall k \in \{0..l-1\}\ \forall j \in \mathcal{M}(i,k) \qquad u^{(0)}_{j(i,k)} = 0,$$
$$\forall i \in \{0..n-1\}\ \forall k \in \{0..l-1\}\, \forall j \in \mathcal{M}(i,k)$$
$$v^{(0)}_{(i,k)j} = \lambda^{(0)}_{(i,k)} = \log \frac{\sum_{x \in \chi_{k,1}} f\left(y_i, x_i = x\right)}{\sum_{x \in \chi_{k,0}} f\left(y_i, x_i = x\right)},$$

- **Itérations.** Pour ℓ allant de 1 à ℓ_{max} :

$$\forall j \in \{0 \dots K-1\} \qquad \forall (i,k) \in \mathcal{N}(j)$$
$$u^{(\ell)}_{j(i,k)} = 2 \tanh^{-1} \prod_{(m,p) \in \mathcal{N}(j) \setminus (i,k)} \tanh \frac{v^{(\ell-1)}_{(m,p)j}}{2},$$
$$\forall i \in \{0 \dots n-1\} \qquad \forall k \in \{0..l-1\}\ \forall j \in \mathcal{M}(i,k)$$
$$v^{(\ell)}_{(i,k)j} = \lambda^{(\ell-1)}_{(i,k)} + \sum_{m \in \mathcal{M}(i,k) \setminus j} (1-2s_k) u^{(\ell)}_{m(i,k)},$$
$$\forall i \in \{0 \dots n-1\} \qquad \forall k \in \{0..l-1\}$$
$$\lambda^{(\ell)}_{(i,k)} = \log \frac{\sum_{x \in \chi_{k,1}} f\left(y_i, x_i = x\right) \exp\left[\sum_{m \neq k} x^m \left(\sum_{p \in \mathcal{M}(i,m)} (1-2s_p) u^{(\ell)}_{p(i,m)}\right)\right]}{\sum_{x \in \chi_{k,0}} f\left(y_i, x_i = x\right) \exp\left[\sum_{m \neq k} x^m \left(\sum_{p \in \mathcal{M}(i,m)} (1-2s_p) u^{(\ell)}_{p(i,m)}\right)\right]}.$$

- **Terminaison.**

$$\forall i \in \{0..n-1\}\ \forall k \in \{0..l-1\} \quad \lambda_{(i,k)} = \lambda^{(\ell_{max})}_{(i,k)} + \sum_{m \in \mathcal{M}(i,k)} (1-2s_m) u^{(\ell_{max})}_{m(i,k)},$$
$$\forall i \in \{0..n-1\}\ \forall k \in \{0..l-1\} \quad v_{i,k} = \text{signe}(\lambda_{(i,k)}).$$

TAB. 4.2 – Décodage des codes LDPC lors d'une modulation BICM.

Ici aussi il peut être intéressant de modifier l'ordre de mise à jour des différents messages par rapport à celui présenté ici afin d'accélérer la convergence de l'algorithme. En particulier, il peut être préférable de ne pas mettre à jour l'information intrinsèque $\lambda^{(\ell)}_{(i,k)}$ à chaque itération, car cette opération est coûteuse en temps de calcul.

L'algorithme de démodulation et de décodage pour une modulation MLC-MSD est

très similaire, et sera décrit dans le cadre de la réconciliation dans la section 4.2.4.

4.2.3 Construction de codes LDPC

La construction des matrices de parité des codes LDPC peut se faire de différentes façons. Les méthodes basées sur des constructions structurées (codes quasi-cycliques ou basés sur la géométrie Euclidienne [22]) permettent d'élaborer des codes aux plafonds d'erreur très bas (inférieurs à 10^{-12}), mais ne fonctionnant correctement que pour des rapports signal-à-bruit éloignés de la limite imposée par le théorème de Shannon. Les constructions aléatoires consistent à générer aléatoirement une matrice de parité à partir de distributions de degrés $\lambda(x)$ et $\rho(x)$, en évitant autant que possible de créer des cycles dans le graphe de Tanner associé. Les codes ainsi générés ont des plafonds d'erreurs plus élevés que leurs équivalents structurés, mais leurs performances peuvent être incroyablement proches de celles d'un code correcteur idéal [116].

L'analyse du décodage des codes LDPC générés aléatoirement peut s'effectuer avec la méthode « d'évolution de densité » [114]. Comme son nom l'indique, cette technique permet de prédire l'évolution de la densité de probabilité des messages $u^{(\ell)}$ et $v^{(\ell)}$ au cours des itérations de l'algorithme SP. L'évolution de densité est cependant un outil d'analyse asymptotique qui n'est en théorie valide que pour des codes de taille infinie, mais qui reste néanmoins utilisable lorsque la taille des codes considérés est suffisamment grande (typiquement de l'ordre de quelques milliers de bits). L'évolution de densité repose sur trois hypothèses :

1. le graphe de Tanner ne contient pas de cycles,
2. le code est utilisé sur un canal sans mémoire à entrée binaire et sortie symétrique, c.-à.d. que si $x \in \{0,1\}$ représente le bit en entrée et $y \in \mathbb{R}$ représente le symbole en sortie, la probabilité de transition du canal satisfait $p(y|x) = p(-y|\bar{x})$,
3. le canal de transmission est caractérisé par un paramètre ϵ qui mesure le degré de dégradation du canal (variance du bruit dans le cas d'un canal gaussien, probabilité d'erreur pour un canal binaire symétrique, etc.).

Les principaux résultats sont alors les suivants :

1. pour des distributions $\lambda(x)$ et $\rho(x)$ données, il existe un seuil ϵ^* du paramètre caractérisant le canal, en dessous duquel la probabilité de décodage erroné du code LDPC est strictement positive, et au dessus duquel elle est arbitrairement proche de zéro,
2. les performances de tous les codes LDPC construits aléatoirement selon ces distributions sont similaires.

Pour un canal et un taux de code donnés, il est donc possible d'optimiser les distributions de degré afin d'obtenir un seuil le plus faible possible. Ce seuil est toujours supérieur à la limite imposée par Shannon, mais il est conjecturé que le seuil tend vers cette limite lorsque le degré maximum de $\lambda(x)$ est arbitrairement grand.

L'optimisation des distributions de degré est une tâche ardue car le seuil est en général une fonction non-linéaire des polynômes $\lambda(x)$ et $\rho(x)$. Des distributions optimisées pour une transmission par modulation antipodale sur canal gaussien sont cependant disponibles dans la littérature et sur le site Internet du laboratoire LTHC de Lausanne [117].

4.2.4 Réconciliation avec des codes LDPC

L'algorithme de réconciliation de variables continues avec des codes LDPC s'obtient directement à partir de l'algorithme de la section précédente, en utilisant le canal de transmission équivalent de l'équation (4.13). Par exemple l'algorithme de réconciliation MLC-MSD est décrit dans la table 4.3. Les notations utilisées sont les suivantes :

- les nœuds de variable et de parité du code au niveau i sont respectivement notés $(v_{i,0} \dots v_{i,n-1})$ et $(c_{i,0} \dots c_{i,\beta(i)-1})$, où $\beta(i)$ est le nombre de nœuds à ce niveau,
- l'ordre de décodage des niveaux est déterminé par la séquence d'indice $(d_0, \dots, d_N)$ où $d_i \in \{0 \dots l-1\}$,
- l'ensemble des indices des nœuds de parité connectés à un nœud de variable $v_{i,k}$ au niveau i est noté $\mathcal{M}_i(k)$,
- l'ensemble des paires d'indices des nœuds de variable connectés à un nœud de parité $c_{i,j}$ au niveau i est noté $\mathcal{N}_i(j)$,
- le bit du syndrome associé au nœud de parité $c_{i,j}$ est noté $s_{i,j}$,
- le message envoyé d'un nœud $v_{i,k}$ à un nœud $c_{i,j}$ durant l'itération ℓ est noté $v^{(\ell)}_{i(k,j)}$, le message inverse est noté $u^{(\ell)}_{i(j,k)}$.

Il est important de souligner que cet algorithme est valable quelle que soit la distribution des variables continues, mais que rien ne garantit qu'il soit possible de construire des codes LDPC performants dans tous les cas. Les nombreuses études menées sur les codes LDPC laissent cependant penser qu'un code LDPC optimisé pour un canal (symétrique) particulier a de grande chance de fonctionner correctement sur un autre canal.

4.3 Réconciliation de variables gaussiennes

Dans cette section nous considérerons le cas particulier de la réconciliation de deux variables continues gaussiennes $X \sim \mathcal{N}(0,1)$ et $Y = X + \epsilon$, où $\epsilon \sim \mathcal{N}(0,\sigma)$ est un bruit gaussien de variance σ^2. Puisque la densité de probabilité est gaussienne et centrée, elle satisfait la propriété de symétrie $p(x,y) = p(-x,-y)$.

L'ensemble $\mathbb{R}$ est partitionné en k intervalles $\{I_j\}_{1..k}$ définissant une fonction de quantification selon l'équation (4.12). Nous supposerons les intervalles ordonnés sur la droite réelle, c'est à dire :

$$\forall m,n \in \{1..k\} \quad m < n \quad \Rightarrow \quad \forall x \in I_m \; \forall y \in I_n \; x < y. \tag{4.37}$$

De plus les intervalles sont choisis symétriques autour de 0 afin d'assurer la symétrie de la distribution conjointe des variables X_q et Y, et les bornes des intervalles sont optimisées afin de maximiser l'information mutuelle $I(X_q;Y)$. Chacune des valeurs quantifiées se décrit par une étiquette de $l = \lceil \log_2 k \rceil$ bits.

4.3.1 Choix des codes pour la réconciliation de type MLC

Calcul des taux théoriques des codes

La réconciliation MLC-MSD nécessite l'utilisation d'un code pour chaque niveau d'étiquetage. Le canal équivalent reliant les bits $\mathcal{L}_i(x)$ de chaque niveau i au symbole y de Bob

– **Initialisation.**

$$\forall k \in \{0..n-1\}\ \forall i \in \{0..l-1\}\ \forall j \in \mathcal{M}_i(k) \qquad u^{(0)}_{i(j,k)} = 0,$$
$$\forall k \in \{0..n-1\}\ \forall i \in \{0..l-1\} \forall j \in \mathcal{M}_i(k)$$
$$v^{(0)}_{i(k,j)} = \lambda^{(0)}_{(i,k)} = \log \frac{\sum_{x \in \chi_{k,1}} \int p(x,y)\mathbf{1}_i(x)dx}{\sum_{x \in \chi_{k,0}} \int p(x,y)\mathbf{1}_i(x)dx},$$

– **Itérations entre niveaux.** Pour i allant de 0 à N :
  – **Décodage du niveau d_i.** Pour ℓ allant de 1 à ℓ_{max} :

$$\forall j \in \{0 \dots \beta(d_i)\}\ \forall k \in \mathcal{N}_{d_i}(j) \qquad u^{(\ell)}_{d_i(j,k)} = 2\tanh^{-1} \prod_{m \in \mathcal{N}_{d_i}(j) \setminus k} \tanh \frac{v^{(\ell-1)}_{d_i(m,j)}}{2},$$
$$\forall k \in \{0 \dots n-1\}\ \forall j \in \mathcal{M}_{d_i}(k) \qquad v^{(\ell)}_{d_i(k,j)} = \lambda^{(\ell-1)}_{(d_i,k)} + \sum_{m \in \mathcal{M}_{d_i}(k) \setminus j} (1-2s_{d_i,m}) u^{(\ell)}_{d_i(m,k)}.$$

  – **Mise à jour de l'information intrinsèque du niveau d_{i+1}.** :

$$\forall k \in \{0 \dots n-1\}$$
$$\lambda^{(\ell)}_{(d_{i+1},k)} = \log \frac{\sum_{x \in \chi_{d_{i+1},1}} \int p(x,y)\mathbf{1}_k(x)dx \exp\left[\sum_{m \neq d_{i+1}} x^m \left(\sum_{p \in \mathcal{M}_m(k)} (1-2s_{m,p}) u^{(\ell)}_{m(p,k)}\right)\right]}{\sum_{x \in \chi_{d_{i+1},0}} \int p(x,y)\mathbf{1}_i(x)dx \exp\left[\sum_{m \neq d_{i+1}} x^m \left(\sum_{p \in \mathcal{M}_m(k)} (1-2s_{m,p}) u^{(\ell)}_{m(p,k)}\right)\right]}.$$

– **Terminaison.**

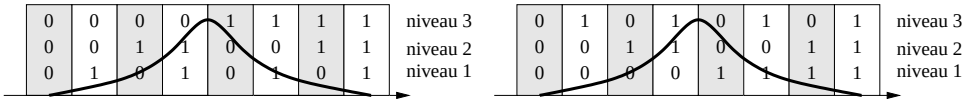
$$\forall k \in \{0..n-1\}\ \forall i \in \{0..l-1\} \quad \lambda_{(i,k)} = \lambda^{(\ell_{max})}_{(i,k)} + \sum_{m \in \mathcal{M}_k(i)} (1-2s_{k,m}) u^{(\ell_{max})}_{i(m,k)},$$
$$\forall k \in \{0..n-1\}\ \forall i \in \{0..l-1\} \quad v_{i,k} = \text{signe}(\lambda_{(i,k)}).$$

TAB. 4.3 – Décodage des codes LDPC lors d'une réconciliation MLC-MSD.

doit lui aussi être symétrique pour faciliter la construction des codes LDPC. L'étiquetage associé à la quantification doit donc vérifier la propriété suivante :

$$\forall i \in \{0..l-1\}, \forall b \in \{0,1\} \qquad p\left(y, \mathcal{L}_i(x) = b\right) = p\left(-y, \mathcal{L}_i(x) = \bar{b}\right). \tag{4.38}$$

Nous avons étudié deux étiquetages particuliers satisfaisant cette condition : l'étiquetage « naturel » et « anti-naturel ». Dans les deux cas le label binaire associé à chaque intervalle de quantification I_j est la description binaire du nombre $j+(2^l-k)/2$, mais comme illustré sur la figure 4.10, lors de l'étiquetage naturel les niveaux sont décodés par ordre de poids croissants alors que lors de l'étiquetage anti-naturel ils sont décodés par ordre de poids décroissants.



(a) étiquetage naturel. (b) étiquetage anti-naturel.

FIG. 4.10 – Stratégies d'étiquetage.

Les taux des codes requis à chaque niveau peuvent être déterminés à partir des informations mutuelles

$$I_i(\sigma) = I(\mathcal{L}_i(X_q); Y | \mathcal{L}_1(X_q) \dots \mathcal{L}_{i-1}(X_q), \sigma). \tag{4.39}$$

Même lorsque $\sigma = 0$, il est important de remarquer que $I_i(0)$ n'est pas toujours égal à 1 car la distribution sous-jacente des symboles quantifiés n'est pas uniforme. Pour une variance de bruit donnée σ^2, le taux optimal des codes permettant de décoder le niveau i lorsque les niveaux $0..i-1$ ont été corrigés, est donc :

$$\boxed{R^i_{opt} = 1 - (I_i(0) - I_i(\sigma)).} \tag{4.40}$$

Les courbes $I_i(\sigma)$ sont représentées sur les figures 4.11 et 4.12 en fonction du rapport signal-à-bruit $10\log(1/2\sigma^2)$ dans le cas où $k = 16$.

En régime de faibles rapports signal-à-bruit (≤ 2 dB), les premiers niveaux décodés avec un étiquetage naturel sont particulièrement bruités et l'information mutuelle est proche de 0. La construction de codes à des taux aussi faibles est très difficile, et il est beaucoup plus aisé de dévoiler entièrement la séquence plutôt que tenter de la coder. Dans le cas d'un étiquetage anti-binaire, cette simplification n'est en général pas possible car tous les niveaux ont des taux significativement différents de 0. Afin de réduire au maximum le nombre de codes à construire, nous avons donc utilisé un étiquetage naturel dans toutes nos simulations. En adaptant le nombre d'intervalles de quantification utilisés, nous sommes toujours parvenus à réduire à deux le nombre de codes effectivement utilisés quelque soit la variance du bruit σ^2.

A titre d'exemple, les taux des codes requis pour une variance $\sigma^2 = 1/3$, 16 intervalles de quantification et un étiquetage naturel sont 0.002/0.016/0.259/0.921. Soulignons que l'effet de la quantification est négligeable puisque $I(X_q; Y)$ diffère de $I(X; Y)$ par moins de 0.02 bits par symbole. Le fait de dévoiler entièrement les deux premiers niveaux a très peu

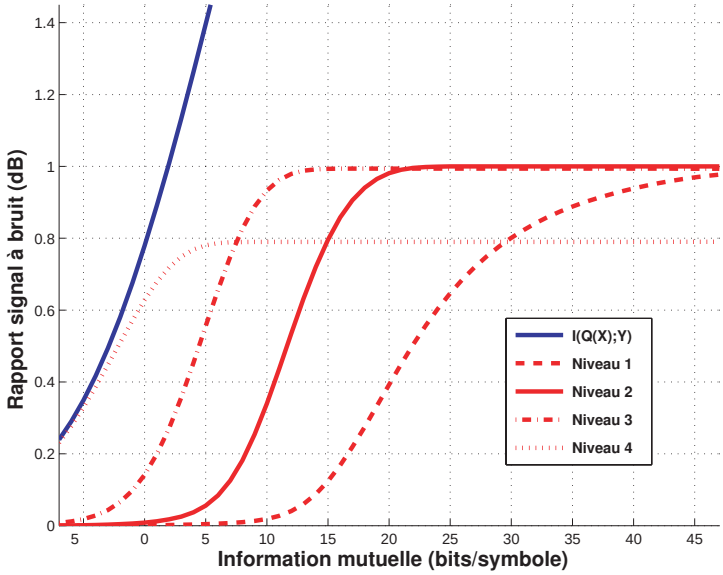


FIG. 4.11 – Courbes d'informations mutuelles par niveau avec un étiquetage naturel (quantification sur 16 niveaux).

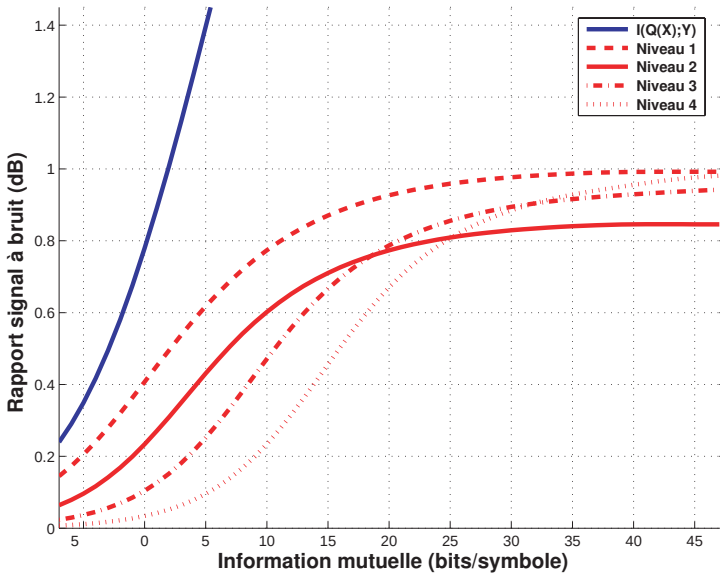


FIG. 4.12 – Courbes d'informations mutuelles par niveau avec un étiquetage anti-naturel (quantification sur 16 niveaux).

d'impact sur l'efficacité de la réconciliation, car ces derniers contribuent à l'information mutuelle totale $I(\hat{X};Y)$ à hauteur de 0.02 bits par symbole.

Afin de simplifier encore plus la construction des codes, nous avons utilisé pour chaque niveau des codes LDPC irréguliers optimisés pour une modulation antipodale sur un canal gaussien. Il est clair que le canal réel n'est pas gaussien, néanmoins la quantification et l'étiquetage choisis assurent que le canal équivalent vu par les bits quantifiés d'un même niveau est à sortie symétrique et que les probabilités *a priori* d'obtenir un 1 ou un 0 sont identiques. cette approximation ne semble pas compromettre l'efficacité de la réconciliation. L'algorithme d'évolution de densité permet d'obtenir des distributions irrégulières de degrés avec des seuils proches de la limite de Shannon, et les résultats de nombreuses optimisations sont disponibles dans la littérature [117]. La taille des blocs retenue est de de 200000 bits et les graphes de Tanner ont été générés aléatoirement en évitant les boucles de taille 2 et 4. Malgré la grande taille des blocs, les performances réelles de ces codes sont encore loin de celles des codes idéaux atteignant la limite de Shannon. La correction de toutes les erreurs n'est alors possible que si les taux des codes utilisés sont inférieurs aux taux théoriques déterminés par l'équation (4.40). La réduction du taux des codes à chaque niveau diminue l'efficacité de la réconciliation. En analysant le décodage itératif entre les niveaux il est cependant possible d'ajuster les taux pour limiter cette chute.

Détermination des taux pratiques des codes

Notre analyse plus réaliste du décodage repose sur l'utilisation de diagrammes EXIT *(EXtrinsinc Information Transfer charts)* [118] permettant de visualiser et de prédire les transferts d'information lors d'un décodage itératif. Si l'on souhaitait analyser précisément le processus itératif, il serait nécessaire de suivre l'évolution des densités de probabilités des rapports de vraisemblance calculés par chaque élément (décodeur, démodulateur, etc.). Les diagrammes EXIT simplifient cette analyse en ne suivant l'évolution que d'un seul paramètre : l'information mutuelle entre les rapports de vraisemblance et le bit réellement transmis. Chaque élément intervenant dans le décodage est alors vu comme une « boîte noire » recevant une information *a priori* I_A , et fournissant en sortie une information extrinsèque I_E . Le comportement de cette « boîte noire » est décrit par la courbe $I_A = T(I_E)$, appelée courbe EXIT. En général il n'existe pas d'expression analytique de la fonction T, mais il est possible de l'obtenir par des simulations de Monte-Carlo. Puisque l'information extrinsèque d'un élément est utilisée comme information *a priori* par l'élément suivant de la chaîne de décodage, on peut assembler les différentes courbes sur un même graphique et *visualiser* l'évolution de l'information. Ce principe est illustré figure 4.13 pour un décodage itératif comprenant deux éléments.

Dans la situation qui nous intéresse, seuls deux codes sont utilisés aux niveaux $l-1$ et $l-2$. Le décodage itératif comprend donc quatre éléments : les démodulateurs des niveaux $l-1$ et $l-2$ et les décodeurs associés.

La courbe EXIT du démodulateur du niveau $l-1$ s'obtient par simulation de Monte-Carlo. Tout d'abord N réalisations $(x_0 \dots x_{N-1})$ et $(y_0 \dots y_{N-1})$ des variables corrélées X et Y sont générées suivant la densité de probabilité $p(x,y)$. Chaque symbole x_i est ensuite quantifié puis étiqueté pour fournir l bits $(x_{i,0} \dots x_{i,l-1})$. Les rapports de vraisemblance $\lambda_{i,l-1}$ $(i \in \{0..n-1\})$ des bits démodulés au niveau $l-1$ sont calculés à l'aide de

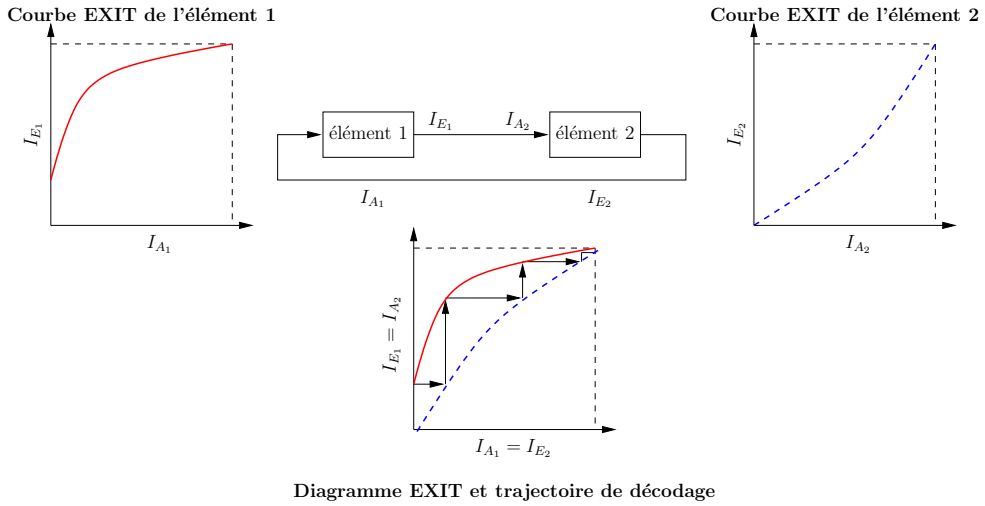


FIG. 4.13 – Principe de l'analyse basée sur les diagrammes EXIT.

l'équation (4.36), en utilisant comme rapports de vraisemblance extrinsèques :

- $\lambda_{i,k} = (2x_{i,k} - 1)\lambda_{max}$ si le niveau k est dévoilé, avec $\lambda_{max} \gg 1$,
- $\lambda_{i,k} = (2x_{i,k} - 1)z$ où z est la réalisation d'une variable gaussienne $\mathcal{N}(\eta, 2\eta)$ si le niveau $k = l - 2$ est l'autre niveau à décoder.

A partir d'un histogramme des réalisations $x_{i,l-1}$ et $\lambda_{i,l-1}$ ($i \in \{0..n-1\}$), on peut alors estimer la densité de probabilité conjointe des variables aléatoires X_{l-1} et Λ_{l-1} correspondantes et ainsi évaluer l'information mutuelle $I_E = I(X_{l-1}, \Lambda_{l-1})$. De façon similaire, on évalue l'information *a priori* $I_A = I(X_{l-2}, \Lambda_{l-2})$ à partir d'un histogramme des réalisations $x_{i,l-2}$ et $\lambda_{i,l-2}$ ($i \in \{0..n-1\}$). En réitérant cette simulation pour différentes valeurs de η, on obtient une description paramétrique $I_A = g(\eta)$ et $I_E = h(\eta)$ qui permet de remonter à la courbe EXIT $I_E = T(I_A)$. La courbe EXIT du démodulateur du niveau $l - 2$ s'obtient par la même technique en inversant les rôles des niveaux $l - 1$ et $l - 2$. Il est clair d'après l'équation (4.36) que les courbes EXIT des démodulateurs dépendent du choix de l'étiquetage et du rapport signal-à-bruit. Les courbes EXIT obtenues dans le cas d'un rapport signal-à-bruit de 3, d'une quantification sur 16 niveaux et d'un étiquetage naturel sont représentées figure 4.14.

La courbe EXIT des codes LDPC s'obtient par une procédure identique, en simulant le décodage d'un mot de code pour un syndrome donné (en pratique nous avons utilisé le décodage du vecteur nul avec un syndrome nul). Les courbes obtenues après 100 itérations de l'algorithme SP sont représentées figure 4.15. On constate que les codes de taux faible commencent à décoder (c.-à-d. à fournir de l'information extrinsèque) dès que l'information *a priori* dépasse légèrement leur taux, mais ne corrigent effectivement toutes les erreurs que lorsque une grande quantité d'information *a priori* est disponible. Les codes de taux élevé ont un comportement inverse, ils ne commencent à décoder qu'avec significativement plus d'information *a priori* que leur taux, mais décodent toutes les erreurs sans requérir beaucoup plus d'information. Lors du choix des codes utilisables en pratique pour la réconciliation, il est donc plus intéressant de réduire le code des taux élevés que celui des codes de taux faible.

Afin de présenter clairement la manière dont les taux des codes peuvent être choisis en pratique, nous détaillerons la procédure sur le même exemple que précédemment :

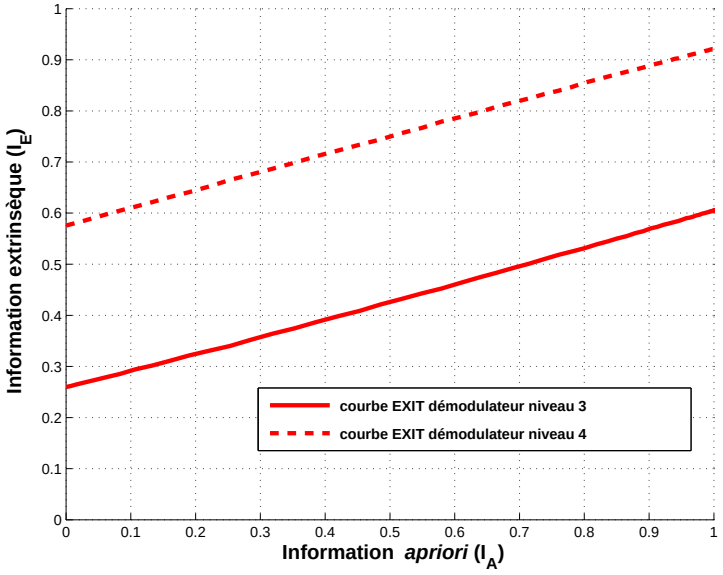


FIG. 4.14 – Courbes EXIT de deux démodulateurs (quantification sur 16 niveaux, rapport signal-à-bruit de 3, étiquetage naturel, deux niveaux des bits de poids faibles dévoilés).

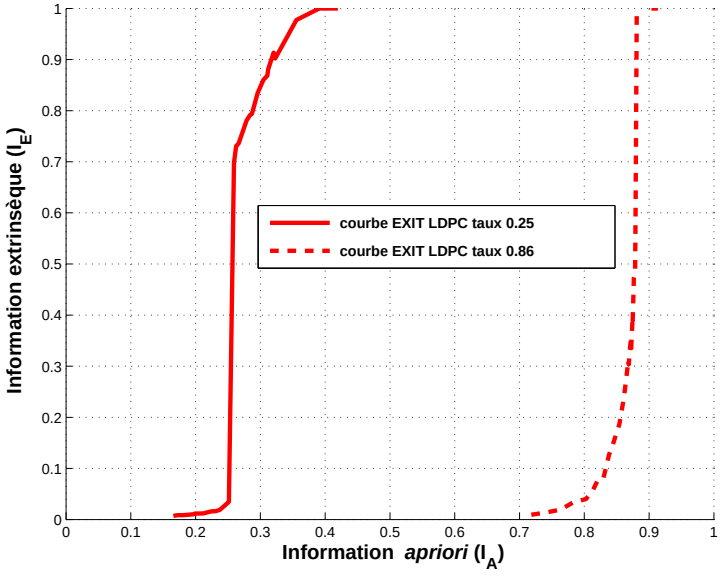


FIG. 4.15 – Courbes EXIT de deux codes LDPC.

rapport signal-à-bruit de 3, quantification sur 16 niveaux (labels de 4 bits) et étiquetage naturel. Les deux premiers niveaux qui nécessiteraient des codes de taux trop faibles (0.002 et 0.016) sont totalement dévoilés, et en théorie les niveaux suivants requièrent des codes de taux 0.259 et 0.921. Le code utilisé à la place du code de taux théorique 0.259, est déterminé en représentant les courbes EXIT de plusieurs codes de taux légèrement inférieur à 0.25. Le code retenu est celui de taux le plus élevé dont la courbe EXIT garantit qu'il commencera à décoder lorsque l'information *a priori* est de 0.259. Sur cet exemple il s'agit d'un code de taux 0.25. Le second code est déterminé en représentant le diagramme EXIT global du décodage comme sur la figure 4.16. Une fois l'information extrinsèque du premier code convertie en information *a priori* pour le second code grâce au démodulateur du niveau 4, la procédure de décodage ne continue que si le second code est capable de fournir de l'information extrinsèque. Dans l'exemple considéré ici, l'information extrinsèque fournie par un code de taux 0.86 suffit à améliorer l'information *a priori* disponible au premier code à travers le démodulateur du niveau 3, et permet donc d'obtenir une information extrinsèque maximale après quelques itérations.

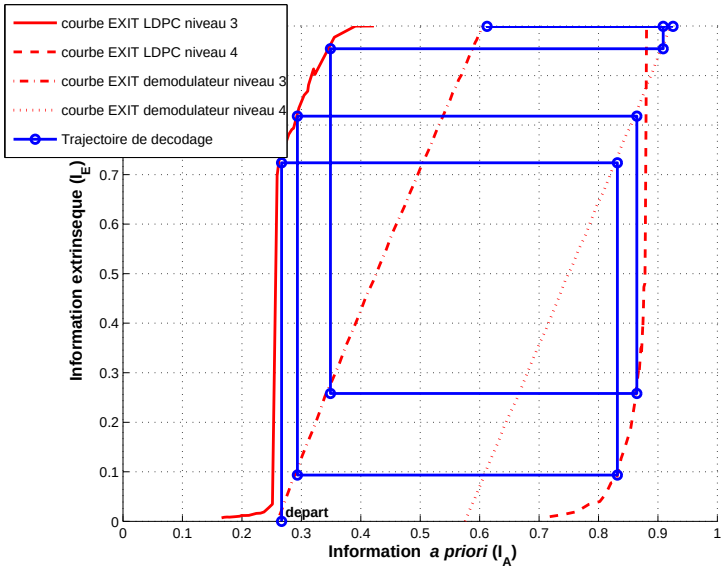


FIG. 4.16 – Trajectoire du décodage itératif lorsque $\sigma^2 = 1/3$ avec 16 niveaux de quantification et un étiquetage naturel. La trajectoire représentée est la moyenne de 10 trajectoires réelles de décodage.

On peut constater sur sur le diagramme EXIT que la trajectoire de décodage moyenne suit précisément les courbes EXIT des démodulateurs et décodeurs, ce qui valide *a posteriori* l'approche utilisée et la modélisation de l'information *a priori* des courbes EXIT par une information gaussienne. La figure 4.17 représente les histogrammes des rapports de vraisemblance réels obtenus lors de la première démodulation du niveau 3 (4.17(a)), de la première modulation du niveau 4 après correction partielle du niveau 3 (4.17(b)), et la seconde démodulation du niveau 3 après correction partielle du niveau 4 (4.17(c)). L'utilisation de densités gaussiennes est une approximation très grossière lors de la première démodulation, mais semble devenir plus correcte au cours des itérations. Cela explique donc en partie le bon accord observé entre les courbes EXIT estimées et les trajectoires réelles de décodage.

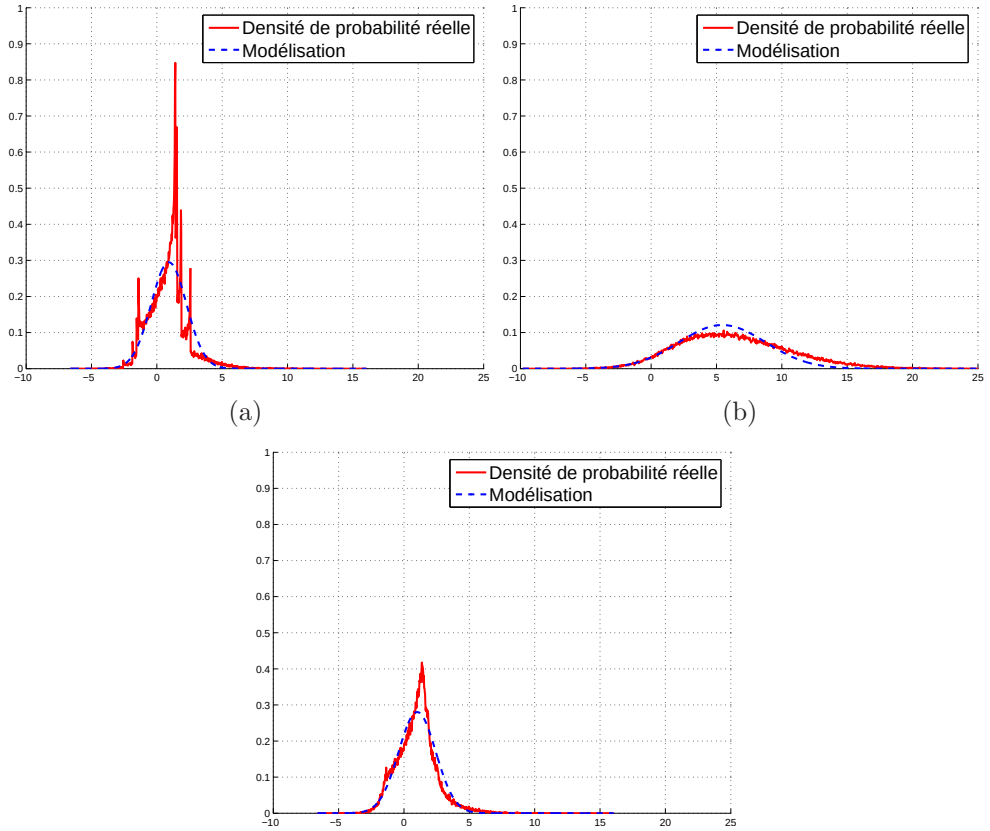


FIG. 4.17 – Densités de probabilité réelles des rapports de vraisemblance.

Les taux des codes déterminés de la même manière pour différents rapports signal-à-bruit sont donnés dans le tableau 4.4.

$1/\sigma^2$	Intervalles	$I(X_q;Y)$	$H(X_q)$	Taux théoriques	Taux pratiques
1	12 (4 bits)	0.49	3.38	0.001/0.008/0.187/0.915	0/0/0.16/0.86
3	16 (4 bits)	0.98	3.78	0.002/0.016/0.259/0.921	0/0/0.25/0.86
7	22 (5 bits)	1.47	4.23	0.002/0.020/0.295/0.924/1	0/0/0.28/0.86/1
15	32 (5 bits)	1.97	4.68	0.002/0.025/0.332/0.934/1	0/0/0.31/0.86/1

TAB. 4.4 – Taux des codes utilisés pour la réconciliation MLC-MSD.

Comme nous l'avons brièvement évoqué dans la section 4.2.3, les codes LDPC construits aléatoirement ont parfois des plafonds d'erreurs élevés. Il est donc possible qu'il reste quelques erreurs (en pratique une ou deux) après décodage. On peut cependant remédier à ce problème en utilisant un code algébrique (par un exemple BCH ou Reed-Solomon) de taux élevé (> 0.99) sur l'ensemble des bits.

Efficacité de la réconciliation

Le tableau 4.5 compare l'efficacité de l'algorithme de réconciliation MLC-MSD proposé avec celle de la réconciliation par tranche pour différents rapports signal-à-bruit. Nos simulations numériques ont été réalisées sur 50 blocs de 200000 bits et toutes les erreurs ont été

corrigées. Un code BCH binaire de taille 4095 et corrigeant 1 erreur par bloc a été appliqué aux bits des niveaux non dévoilés pour faire baisser le plafond d'erreur du décodage. Cette opération requiert l'envoi d'environ 0.008 bits d'information supplémentaire par symbole.

Les résultats de la réconciliation par tranche présentés sont ceux obtenus par Gilles Van Assche et Kim-Chi Nguyen dans [24, 106]. Les efficacités η_{SEC}^{max}, η_{SEC}^{1} et η_{SEC}^{2} font respectivement référence à l'efficacité de la réconciliation par tranche avec des codes binaires parfaits, avec le BCP Cascade en ne comptant que les bits échangés d'Alice vers Bob, et avec le BCP Cascade et des Turbo-Codes en comptant tous les bits échangés. η_{MLC} est l'efficacité de la réconciliation MLC-MSD obtenue en utilisant les codes et intervalles de quantification du tableau 4.4 et η_{MLC}^{max} est l'efficacité maximum atteignable en théorie avec des codes parfaits. L'efficacité atteignable en pratique par la réconciliation MLC-MSD est en générale supérieure à celle de la réconciliation par tranche. L'écart est d'autant plus important que le rapport signal-à-bruit est faible.

$1/\sigma^2$	η_{SEC}^{max}	η_{SEC}^{1}	η_{SEC}^{2}	η_{MLC}^{max}	η_{MLC}
1	75%	60%	<50%	98%	79.4%
3	87%	79%	67%	98%	88.7%
7	90%	84%	76%	98%	90.9%
15	92%	87%	82%	98.5%	92.2%

Tab. 4.5 – Efficacités des algorithmes de réconciliation.

4.3.2 Choix des codes pour la réconciliation de type BICM

Nous avons supposé dans la section précédente que l'étiquetage préservait une certaine symétrie, afin de pouvoir utiliser des codes optimisés pour une modulation antipodale sur un canal gaussien. Dans le cas de la réconciliation BICM, un code unique est appliqué à l'ensemble des bits obtenus après étiquetage, et les probabilités globales d'obtenir des bits 1 ou 0 sont généralement proches quelque soit l'étiquetage. Nous continuerons donc à utiliser les mêmes codes LDPC.

Le taux théorique permettant de corriger toutes les erreurs avec une réconciliation BICM est difficile à calculer, en revanche on peut en obtenir une borne supérieure. En reprenant la notation $\mathcal{L}_i(X)$ pour la variable aléatoire représentant le i-ième bit du label de X_q on a [107] :

$$R_{opt} \leq 1 - \frac{\max\left\{0, H(X_q) - \sum_{m=1}^{l} I(\mathcal{L}_m(X); Y)\right\}}{l}. \tag{4.41}$$

Dans le cas où l'on a $1/\sigma^2 = 3$, 16 intervalles de quantification et un étiquetage de Gray, le taux optimal du code est $R_{opt} \leq 0.274$. L'efficacité maximale de la réconciliation est donc au mieux $\eta_{\text{BICM}} = 88\%$. En pratique, il faut cependant s'assurer que l'agorithme de décodage puisse converger. Cette analyse peut de nouveau se faire avec des diagrammes EXIT, comme indiqué sur la figure 4.18. Les courbes EXIT des démodulateurs correspondant à différents étiquetages binaires ont été générées par simulations de Monte-Carlo en supposant l'information *a priori* gaussienne. On constate que tous les étiquetages ne

sont pas équivalents, et qu'il n'est pas possible d'obtenir une grande quantité d'information extrinsèque simultanément dans le régime des faibles et fortes informations *a priori*. Au vu des courbes EXIT des codes LDPC, l'efficacité de la réconciliation est optimisée en choisissant l'étiquetage de Gray, puisqu'il permet au démodulateur de générer le plus d'information extrinsèque possible pour des faibles informations *a priori*. Le décodage

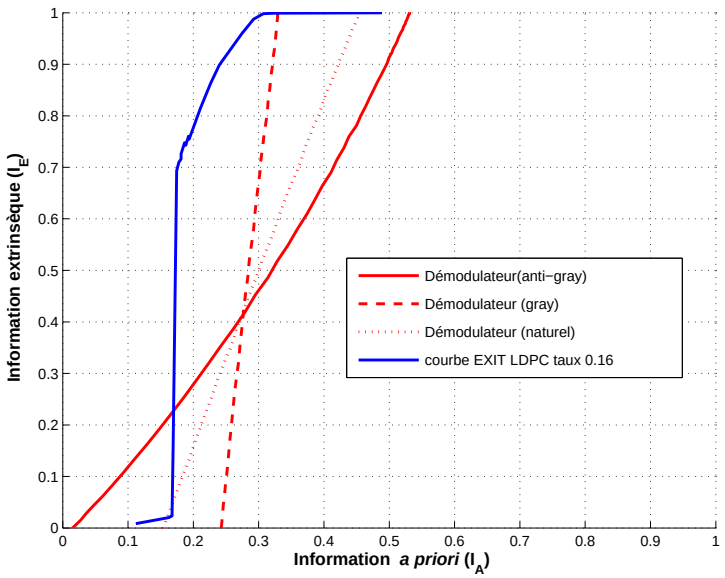


FIG. 4.18 – Diagramme EXIT d'une réconciliation BICM ($1/\sigma^2 = 3$, 16 intervalles de quantification).

converge alors avec succès si les courbes EXIT du démodulateur et du décodeur ne s'intersectent pas. Cette condition inflige une sévère pénalité sur le taux du code utilisable en pratique, et comme indiqué sur l'exemple de la figure 4.18 il est nécessaire d'utiliser un code LDPC de taux 0.16 pour garantir un décodage sans erreurs. L'efficacité atteignable n'est alors en réalité que $\eta_{\text{BICM}} = 42\%$.

Il n'est pas possible comme dans le cas de la réconciliation MLC-LSD de compenser les mauvaises performances du code LDPC. La simplification de l'algorithme de réconciliation apportée par l'utilisation d'un code unique s'accompagne d'une perte de flexibilité dans le choix des taux des codes, et fait chuter significativement l'efficacité réelle de la réconciliation BICM.

4.3.3 Conclusion : application à la distribution de clés

La figure 4.19 représente la distance maximale de transmission, pour laquelle un débit de clé 1 kbit/s est atteint avec les protocoles par variables continues, en fonction de l'efficacité de la réconciliation.

Les paramètres utilisés sont ceux du système réel présenté dans la section 1.3.3 et basé sur les protocoles inverses. Avec l'algorithme de réconciliation par tranches, l'efficacité est environ de 70% et la distance de transmission à 1 kbit/s n'est donc que d'environ 5 km. En utilisant l'algorithme de réconciliation MLC-MSD, l'efficacité dépasse 88% et permet donc d'envisager des transmissions sur plus de 20 km. En pratique, il faut cependant tenir

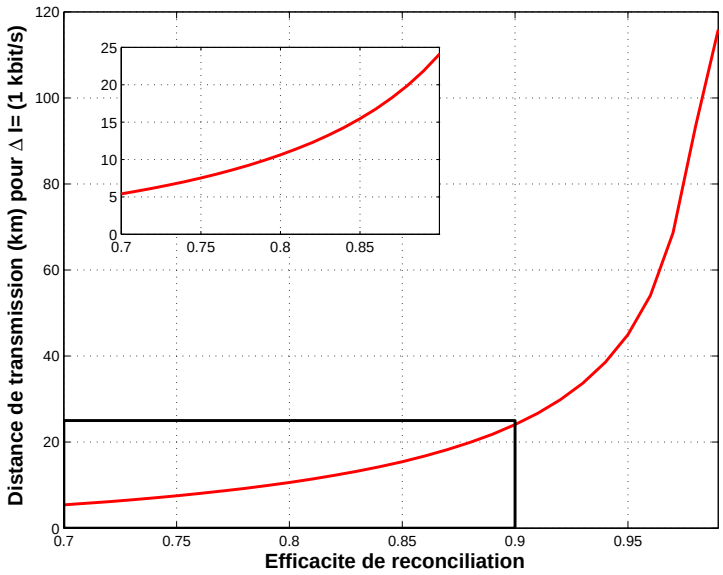


FIG. 4.19 – Distance maximale de transmission à un débit de 1 kbit/s

compte de la complexité non négligeable de l'algorithme de décodage, et l'amélioration de l'efficacité ne se traduit pas aussi directement en gain de distance.

Conclusion générale

Au cours de ces travaux de thèse, nous avons tenté de proposer des solutions alternatives et performantes aux systèmes de distribution de clé quantique déjà existants. Sur le plan expérimental, nous avons cherché à exploiter les possibilités qu'offrent le multiplexage et le codage en fréquence pour proposer des systèmes simples et robustes. Nous avons aussi étudié de façon plus théorique des algorithmes de réconciliation performants pour les protocoles à variables continues. Cette dernière étude s'est avérée être d'une grande importance pour permettre à ces nouveaux protocoles de fonctionner efficacement en pratique.

Le codage en fréquence proposé pour la cryptographie quantique par photons uniques se démarque des travaux déjà réalisés au laboratoire GTL-CNRS Télécom depuis 1999 en exploitant véritablement le contenu spectral d'états quantiques. La manipulation de ces états a été rendue possible par une modélisation quantique des modulateurs de phase. La faisabilité du codage a été démontrée en réalisant un système de transmission complet, et en effectuant une première transmission en régime classique sur 500 m de fibre optique. Cette expérience a permis de vérifier la robustesse et la stabilité du système, mais son niveau d'intégration et ses performances sont encore loin de concurrencer celles des systèmes les plus aboutis. Néanmoins, en réalisant une électronique de commande plus intégrée et moins bruitée, ainsi qu'en utilisant des compteurs de photons de bande passante plus élevée, il est tout à fait envisageable d'atteindre des débits de clés similaires. On peut légitimement s'interroger sur l'intérêt d'un tel dispositif alors que l'on dispose déjà de systèmes commerciaux opérationnels, mais au delà de la réalisation d'une transmission de clé, ce travail nous a permis d'explorer certaines possibilités offertes par le codage fréquentiel de qubits. Par la suite il est tout à fait envisageable de pousser loin cette étude.

La réalisation du système de cryptographie quantique par variables continues s'est en revanche avérée bien plus difficile que prévue. L'utilisation d'un multiplexage en fréquence de l'oscillateur local simplifie la partie optique du système en résolvant les problèmes d'isolation de l'oscillateur local, mais reporte la difficulté sur le contrôle en amplitude et en phase de signaux électriques haute fréquence. Suite à la détérioration des filtres optiques indispensables au démultiplexage des signaux, nous n'avons pas pu tester le système dans son intégralité, et il est difficile d'évaluer objectivement quelles pourraient être ses performances réelles. Le travail réalisé constitue donc uniquement la première étape vers la réalisation d'un système complet.

En remarquant l'analogie entre la réconciliation de variables continues et la modulation codée utilisée pour les communications numériques, nous avons mis au point un algorithme de réconciliation plus efficace que celui initialement proposé par Gilles Van Assche. Cet algorithme a été intégré au système développé au laboratoire Charles Fabry par Jérôme

Lodewyck, et son efficacité proche de 90% permet d'envisager des transmissions sur environ 30 km. La principale limitation aux débits du système reste encore la complexité de la réconciliation, et la mise en œuvre de l'algorithme actuel a d'ailleurs déjà nécessité de nombreuses optimisations. Nous envisageons d'apporter encore plusieurs améliorations à l'algorithme. Tout d'abord, il est possible de réduire la complexité du décodage des codes LDPC en modifiant l'algorithme SP [119]. Plutôt que d'utiliser des codes LDPC optimisés pour une modulation antipodale sur un canal Gaussien, il serait ensuite intéressant d'effectuer une optimisation globale et spécifique des codes LDPC pour la réconciliation. Une généralisation de l'évolution de densité prenant en compte le décodage itératif est en cours d'étude.

Bibliographie

[1] Charles H. Bennett et Gilles Brassard : Quantum Cryptography : Public Key Distribution and Coin Tossing. *In Proc. IEEE International Conference on Computer Systems and Signal Processing*, pages 175–179, Bangalore, India, 1984. IEEE, New York.

[2] Artur K. Ekert : Quantum Cryptography Based on Bell's Theorem. *Phys. Rev. Lett.*, 67(6):661–663, August 1991.

[3] Charles H. Bennett, François Bessette, Gilles Brassard, Louis Salvail et John Smolin : Experimental Quantum Cryptography. *Journal of Cryptology*, 5(1): 3–28, 1992.

[4] G. Ribordy, J.-D. Gautier, N. Gisin, 0. Guinnard et H. Zbinden : Automated "plug & play" quantum key distribution. *Elec. Lett.*, 34(22):2116–2117, October 1998.

[5] Id Quantique : http ://www.idquantique.com.

[6] MagiQ Technologies : http ://www.magitech.com.

[7] Smart Quantum : http ://www.smart-quantum.com.

[8] Apostolos Argyris, Dimitris Syvridis, Laurent Larger, Valerio Annovazzi-Lodi, Pere Colet, Ingo Fischer, Jordi García-Ojalvo, Claudio R. Mirasso, Luis Pesquera et K. Alan Shore : Chaos-based communications at high bit rates using commercial fiber-optic links. *Nature*, 438:343–346, November 2005.

[9] Laszlo B. Kish : Totally secure classical communication utilizing johnson (-like) noise and kirchoff's law. *Phys. Lett. A*, 352(3):178–182, March 2006.

[10] Eric Corndorf, Geraldo Barbosa, Chuang Liang, Horace P. Yuen et Prem Kumar : High-speed data encryption over 25km of fiber using two-mode coherent-state quantum cryptography. *Opt. Lett.*, 28(21):2040–2042, November 2003.

[11] A. D. Wyner : The Wire-Tap Channel. *The Bell System Technical Journal*, 54(8):1355–1367, October 1975.

[12] L. H. Ozarow et A. D. Wyner : Wire Tap Channel II. *AT&T Bell Laboratories Technical Journal*, 63(10):2135–2157, December 1984.

[13] Alfred J. Menezes, Paul C. van Oorschot et Scott A. Vanstone : *Handbook of applied cryptography*. CRC Press, Inc., 5th édition, October 1996.

[14] Mihir Bellare et Phillip Rogaway : Introduction to modern cryptography. Available online : http ://www-cse.ucsd.edu/users/mihir/cse207/classnotes.html, 2005.

[15] A. Hodjat et I. Verbauwhede : Area-throughput trade-offs for fully pipelined 30 to 70 gbits/s aes processors. *IEEE Transactions on Computers*, 55(4):366–372, April 2006.

[16] Thomas M. Cover et Joy A. Thomas : *Elements of Information Theory*. Wiley-Interscience, 2nd édition, 2006.

[17] Claude E. Shannon : A Mathematical Theory of Communication. *The Bell System Technical Journal*, 27:379–423,623–656, July,October 1948.

[18] Imre Csiszár et János Körner : Broadcast Channels with Confidential Messages. *IEEE Trans. Inf. Theory*, 24(3):339–348, May 1978.

[19] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin et J.-M. Merolla : Applications of ldpc codes to the wiretap channel. *IEEE Trans. Inf. Theory*, 53(8):2933–2945, Aug. 2007.

[20] Frédéric Grosshans, Gilles Van Assche, Jérôme Wenger, Rosa Brouri, Nicolas J. Cerf et Philippe Grangier : Quantum key distribution using gaussian-modulated coherent states. *Letters to Nature*, 421(6920):238–241, January 2003.

[21] David Slepian et Jack K. Wolf : Noiseless Coding of Correlated Information Sources. *IEEE Trans. Inf. Theory*, 19(4):471–480, July 1973.

[22] Shu Lin et Daniel J. Costello : *Error Control Coding*. Pearson Prentice Hall, 2nd édition, 2004.

[23] G. Brassard et L. Salvail : Secret-key Reconciliation by Public Discussion. *In* T. Helleseth, éditeur : *Advances in Cryptology-Eurocrypt'93*, pages 411–423. Springer-Verlag, 1993.

[24] Gilles Van Assche, Jean Cardinal et Nicolas J. Cerf : Reconciliation of a Quantum-Distributed Gaussian Key. *IEEE Trans. Inf. Theory*, 50(2):394–400, February 2004.

[25] W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. H. Nickel, C. H. Donahue et C. G. Peterson : Fast, efficient error reconciliation for quantum cryptography. *Phys. Rev. A*, 67(5):052303/1–8, May 2003.

[26] J. L. Carter et M. N. Wegman : Universal classes of hash functions. *Journal of Computer and System Sciences*, 18:143–154, 1979.

[27] M. N. Wegman et J.L. Carter : New hash functions and their use in authentication and set equality. *Journal of Computer Sciences and Systems*, 22:265–279, 1981.

[28] Charles H. Bennett, Gilles Brassard, Claude Crépeau et Ueli Maurer : Generalized Privacy Amplification. *IEEE Trans. Inf. Theory*, 41(6):1915–1923, 1995.

[29] Christian Cachin : *Entropy measures and unconditional security in cryptography.* Thèse de doctorat, Swiss Federal Institute of Technology Zürich, 1997.

[30] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel et Hugo Zbinden : Quantum Cryptography. *Rev. Mod. Phys.*, 74(1):145–195, January 2002.

[31] W. K. Wooters et W. H. Zurek : A single quantum cannot be cloned. *Nature*, 299(5886):802–803, October 1982.

[32] Peter W. Shor et John Preskill : Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Phys. Rev. Lett.*, 85(2):441–444, July 2000.

[33] Charles H. Bennett, Gilles Brassard et N. David Mermin : Quantum cryptography without bell's theorem. *Phys. Rev. Lett.*, 68(5):557–559, February 1992.

[34] Charles H. Bennett : Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68(21):3121–3124, May 1992.

[35] Zhang Quan et Tang Chaojing : Simple proof of the unconditional security of the bennett 1992 quantum key distribution protocol. *Phys. Rev. A*, 65:062301/1–6, 2002.

[36] Kiyoshi Tamaki, Masato Koashi et Nobuyuki Imoto : Unconditionally secure key distribution based on two nonorthogonal states. *Phys. Rev. Lett.*, 90(16):167904/1–4, April 2003.

[37] Kiyoshi Tamaki et Norbert Lütkenhaus : Unconditional security of the bennett 1992 quantum key-distribution protocol over a lossy and noisy channel. *Phys. Rev. A*, 69:032316/1–5, 2004.

[38] Masato Koashi : Unconditional security of coherent-state quantum key distribution with a strong phase-reference pulse. *Phys. Rev. Lett.*, 93(12):120501/1–4, September 2004.

[39] Kiyoshi Tamaki, Norbert L¨utkenhaus, Masato Koashi et Jamie Batuwantudawe : Unconditional security of the bennett 1992 quantum key-distribution scheme with strong reference pulse. arxiV :quant-ph/0607082.

[40] Dagmar Bruss : Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.*, 81(14):3018–3021, October 1998.

[41] B. Huttner, N. Imoto, N. Gisin et T. Mor : Quantum cryptography with coherent states. *Phys. Rev. A*, 51(3):1863–1869, March 1995.

[42] Laurent Duraffourg, Jean-Marc Merolla, Jean-Pierre Goedgebuer, Yuri Mazurenko et William T. Rhodes : Compact transmission system using single-sideband modulation of light for quantum cryptography. *Opt. Lett.*, 26(18):1427–1429, September 2001.

[43] Thierry Debuisschert et William Boucher : Time coding protocols for quantum key distribution. *Phys. Rev. A*, 70(4):042306/1–16, October 2004.

[44] William Boucher et Thierry Debuisschert : Experimental implementation of time-coding quantum key distribution. *Phys. Rev. A*, 72:062325/1–9, 2005.

[45] Damien Stucki, Nicolas Brunner, Nicolas Gisin, Valerio Scarani et Hugo Zbinden : Fast and simple one-way quantum key distribution. *App. Phys. Lett.*, 87:194108/1–3, 2005.

[46] Alexios Beveratos, Rosa Brouri, Thierry Gacoin, André Villing, Jean-Philippe Poizat et Philippe Grangier : Single photon quantum cryptography. *Phys. Rev. Lett.*, 89(18):187901/1–4, October 2002.

[47] Richard J Hughes, Jane E Nordholt, Derek Derkacs et Charles G Peterson : Practical free-space quantum key distribution over 10 km in daylight and at night. *New Jour. Phys.*, 4:43.1–43.14, 2002.

[48] Karen J. Gordon, Veronica Fernandez, Gerald S. Buller, Ivan Rech, Sergio D. Cova et Paul D. Townsend : Quantum key distribution system clocked at 2 GHz. *Opt. Expr.*, 13(8):3015–3020, April 2005.

[49] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P.M. Gormanand P.R. Tapster et J.G. Rarity : A step towards global key distribution. *Nature*, 419:450, October 2002.

[50] R Alléaume, F Treussart, G Messin, Y Dumeige, J-F Roch, A Beveratos, R Brouri-Tualle, J-P Poizat et P Grangier : Experimental open-air quantum key distribution with a single-photon source. *New Jour. Phys.*, 6:92, July 2004.

[51] A. Poppe, A. Fedrizzi, R. Ursin, H. R. Bohm, T. Lorunser, O. Maurhardt, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein et A. Zeilinger : Practical quantum key distribution with polarization entangled photons. *Opt. Expr.*, 12(16):3865 – 3871, August 2004.

[52] Cheng-Zhi Peng, Tao Yang, Xiao-Hui Bao, Jun Zhang, Xian-Min Jin, Fa-Yong Feng, Bin Yang, Jian Yang, Juan Yin, Qiang Zhang, Nan Li, Bao-Li Tian et Jian-Wei Pan : Experimental Free-Space Distribution of Entangled Photon Pairs Over 13 km : Towards Satellite-Based Global Quantum Communication. *Phys. Rev. Lett.*, 94:150501/1–4, April 2005.

[53] Ivan Marcikic, Antía Lamas-Linares et Christian Kurtsiefer : Free-space quantum key distribution with entangled photons. arXiv :quant-ph/0606072, June 2006.

[54] Xiao-Fan Mo, Bing Zhu, Zheng-Fu Han, You-Zhen Gui et Guang-Can Guo : Faraday-Michelson system for quantum cryptography. *Opt. Lett.*, 19(30):2632–2634, October 2005.

[55] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy et H. Zbinden : Quantum key distribution over 67 km with a plug&play system. *New Jour. Phys.*, 4:41.1–41.8, 2002.

[56] Olivier L. Guerreau, Jean-Marc Merolla, Alexandre Soujaeff, Frédéric Patois, Jean-Pierre Goedgebuer et François J. Malassenet : Long-Distance QKD Transmission using Single Sideband Detection Scheme with WDM Synchronization. *IEEE Jour. Selec. Top. Quant. Elec.*, 9(6):1533–1540, November/December 2003.

[57] Z. L. Yuan et A. J. Shields : Continuous operation of a one-way quantum key distribution system over installed telecom fibre. *Opt. Expr.*, 13(2):660–665, January 2005.

[58] D. Gottesman, H.-K. Lo, N. Lütkenhaus et J. Preskill : Security of quantum key distribution with imperfect devices. *Quant. Inf. Comp.*, 4(5):325–360, September 2004.

[59] Gilles Brassard, Norbert Lütkenhaus, Tal Mor et Barry C. Sanders : Limitations on practical quantum cryptography. *Phys. Rev. Lett.*, 85(6):1330–1333, August 2000.

[60] Norbert Lütkenhaus : Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A*, 61(5):052304/1–10, May 2000.

[61] Dominic Mayers : Unconditional security in quantum cryptography. *Journal of the ACM*, 48(3):351–406, May 2001.

[62] Hitoshi Inamori, Norbert Lütkenhaus et Dominic Mayers : Unconditional security of practical quantum key distribution. *European Physical Journal D*, 41(3):599–627, March 2007. (updated 2006).

[63] Antonio Acín, Nicolas Gisin et Valerio Scarani : Coherent pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks. *Phys. Rev. A*, 69(1):012309, January 2004.

[64] Valerio Scarani, Antonio Acín, Grégoire Ribordy et Nicolas Gisin : Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations. *Phys. Rev. Lett.*, 92(5):057901/1–4, February 2004.

[65] Hoi-Kwong Lo, Xiongfeng Ma et Kai Chen : Decoy State Quantum Key Distribution. *Phys. Rev. Lett.*, 94:230504–1/4, June 2005.

[66] T. C. Ralph : Continuous variable quantum cryptography. *Phys. Rev. A*, 61(1): 010303/1–4, December 1999.

[67] T. C. Ralph : Security of continuous variable quantum cryptography. *Phys. Rev. A*, 62(6):062306/1–7, December 2000.

[68] M. D. Reid : Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations. *Phys. Rev. A*, 62(6):062308/1–6, November 2000.

[69] K. Bencheikh, T. Symul, A. Jankovic et J. A. Levenson : Quantum key distribution with continuous variables. *Jour. Mod. Opt.*, 48(13):1903–1920, 2001.

[70] Mark Hillery : Quantum cryptography with squeezed states. *Phys. Rev. A*, 61(2):022309/1–8, January 2000.

[71] Daniel Gottesman et John Preskill : Secure quantum key distribution using squeezed states. *Phys. Rev. A*, 63(2):022309/1–18, January 2001.

[72] Nicolas J. Cerf, M. Lévy et Gilles Van Assche : Quantum distribution of Gaussian keys using squeezed states. *Phys. Rev. A*, 63(5):052311/1–5, May 2001.

[73] Frédéric Grosshans et Philippe Grangier : Continuous Variable Quantum Cryptography Using Coherent States. *Phys. Rev. Lett.*, 88(5):057902/1–4, February 2002.

[74] Frédéric Grosshans, Nicolas J. Cerf, Jérôme Wenger, Rosa Rualle-Brouri et Philippe Grangier : Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. *Quant. Inf. Comp.*, 3:535–552, 2003.

[75] Jérôme Wenger : *Dispositifs impulsionnels pour la communication quantique à variables continues*. Thèse de doctorat, Université Paris XI, September 2004.

[76] Frédéric Grosshans et Nicolas J. Cerf : Continuous-Variable Quantum Cryptography is Secure against Non-Gaussian Attacks. *Phys. Rev. Lett.*, 92(4):047905/1–4, January 2004.

[77] Frédéric Grosshans : Collective Attacks and Unconditional Security in Continuous Variable Quantum Key Distribution. *Phys. Rev. Lett.*, 94:020504/1–4, January 2005.

[78] Miguel Navascués et Antonio Ac´ ?n : Security Bounds for Continuous Variables Quantum Key Distribution. *Phys. Rev. Lett.*, 94:020505/1–4, January 2005.

[79] Raul Garcia-Patron et Nicolas J. Cerf : Unconditional optimality of gaussian attacks against continuous-variable qkd. *Phys. Rev. Lett.*, 97:19050/1–4, November 2006. arXiv :quant-ph/0608032.

[80] Miguel Navascues, Frédéric Grosshans et Antonio Acin : Optimality of gaussian attacks in continuous variable quantum cryptography. *Phys. Rev. Lett.*, 97:190502/1–4, November 2006. arXiv :0608034.

[81] Christian Weedbrook, Andrew M. Lance, Warwick P. Bowen, Thomas Symul, Timothy C. Ralph, et Ping Koy Lam : Quantum Cryptography Without Switching. *Phys. Rev. Lett.*, 93(17):170504/1–4, October 2004.

[82] Ch. Silberhorn, T. C. Ralph, N. Lutkenhaus et G. Leuchs : Continuous Variable Quantum Cryptography : Beating the 3 dB Loss Limit. *Phys. Rev. Lett.*, 89(16):167901/1–4, October 2002.

[83] S. Lorenz, N. Korolkova et G. Leuch : Continous variable quantum key distribution using polarization encoding and post selection. *App. Phys. B*, 79(3):273–277, 2004.

[84] Andrew M. Lance, Thomas Symul, Vikram Sharma, Christian Weedbrook, Timothy C. Ralph et Ping Koy Lam : No-Switching Quantum Key Distribution Using Broadband Modulated Coherent Light. *Phys. Rev. Lett.*, 95:180503/1–4, October 2005.

[85] Jérôme Lodewyck, Thierry Debuisschert, Rosa Tualle-Brouri et Philippe Grangier : Controlling excess noise in fiber-optics continuous-variable quantum key distribution. *Phys. Rev. A*, 72:050303/1–4, November 2005.

[86] M. Legré, H. Zbinden et N. Gisin : Implementation of continuous variable quantum cryptographyin optical fibres using a go-&-return configuration. *Quant. Inf. Comp.*, 6(4&5):326, 2006.

[87] Matthias Keller, Birgit Lange, Kazuhiro Hayasaka, Wolfgang Lange et Herbert Walther : Continuous generation of single photons with controlled waveform in an ion-trap cavity system. *Letters to Nature*, 431:1075–1078, October 2005.

[88] S. Tanzilli, W. Tittel, H. De Riedmatten, H. Zbinden, P. Baldi, M. De Micheli, D.B. Ostrowsky et N. Gisin : PPLN waveguide for quantum communication. *Euro. Phys. D*, 18:155–160, 2002.

[89] Andreas Othonos : Fiber bragg gratings. *Review of Scientific Instruments*, 68(12): 4309–4341, December 1997.

[90] M. Ley et R. Loudon : Quantum theory of high-resolution length measurement with a Fabry-Perot interferometer. *Jour. Mod. Opt.*, 34(2):227–255, February 1987.

[91] Amnon Yariv et Pochi Yeh : *Optical Waves in Crystals*. Wiley Interscience, 2003.

[92] J. J. Sakurai : *Modern Quantum Mechanics*. Addison Wesley Longman, revised edition édition, 1994.

[93] P. C. Sun, Y. Mazurenko et Y. Fainman : Long-distance frequency-division interferometer for communication and quantum cryptography. *Opt. Lett.*, 20(9): 1062–1064, May 1995.

[94] André Stefanov, Hugo Zbinden, Nicolas Gisin et Antoine Suarez : Quantum entanglement with acousto-optic modulators : Two-photon beats and bell experiments with moving beam splitters. *Phys. Rev. A*, 67:042115/1–13, 2003.

[95] Jean-Marc Merolla, Yuri Mazurenko, Jean-Pierre Goedgebuer, Laurent Durrafourg, Henri Porte et William T. Rhodes : Quantum cryptographic device using single photon phase modulation. *Phys. Rev. A*, 60(3):1899–1905, September 1999.

[96] Jean-Marc Merolla, Yuri Mazurenko, Jean-Pierre Goegebuer et William T. Rhodes : Single-Photon Interference in Sidebands of Phase-Modulated Light for Quantum Cryptography. *Phys. Rev. Lett.*, 82(8):1656–1659, February 1999.

[97] Jean-Marc Merolla, Yuri Mazurenko, Jean-Pierre Goegebuer et William T. Rhodes : Phase-modulation transmission system for quantum cryptography. *Opt. Lett.*, 24(2):104–106, January 1999.

[98] Govind P. Agrawal : *Fiber-Optic Communication Systems*. Wiley-Interscience, 3rd édition, 2002.

[99] Amnon Yariv : *Optical Electronics in Modern Communications*, chapitre 20. Oxford University Press, 1997.

[100] Alessandro Zavatta, Marco Bellini, Pier Luigi Ramazza, Francesco Marin et Fortunato Tito Arecchi : Time-domain analysis of quantum states of light : noise characterization and homodyne tomography. *JOSA B*, 19(5):1189–1194, May 2002.

[101] Frédéric Grosshans : *Communication et cryptographie quantiques avec des variables continues*. Thèse de doctorat, Université Paris XI, December 2002.

[102] K. J. Blow, Rodney Loudon et Simon J. D. Phoenix : Continuum fields in quantum optics. *Phys. Rev. A*, 42(7):4102–4114, October 1990.

[103] F. Grosshans et P. Grangier : Effective quantum efficiency in the pulsed homodyne detection of a n-photon state. *The European Physical Journal D*, 14(1):119–125, April 2001.

[104] Horace P. Yuen et Vincent W. S. Chan : Noise in homodyne and heterodyne detection. *Opt. Lett.*, 8(3):177–179, March 1983.

[105] Jerald G. Graeme : *Photodiode Amplifiers : OP AMP Solutions*. McGraw-Hill Professional, 1st édition, December 1995.

[106] Kim-Chi Nguyen, Gilles Van Assche et Nicolas J. Cerf : Side-Information Coding with Turbo Codes and its Application to Quantum Key Distribution. *In Proc. International Symposium on Information Theory and its Applications*, 2004.

[107] Giuseppe Caire, Giorgio Taricco et Ezio Biglieri : Bit-interleaved Coded Modulation. *IEEE Trans. Inf. Theory*, 44(3):927–946, May 1998.

[108] Stephan ten Brink : Iterative demapping and decoding for multilevel modulation. *In Proc. IEEE Globecom Conference*, volume 1, pages 579–584, Sydney, November 1998.

[109] Udo Wachsmann, Robert F. H. Fischer et Johannes B. Huber : Multilevel Codes : Theoretical Concepts and Practical Design Rules. *IEEE Trans. Inf. Theory*, 45(5):1361–1391, July 1999.

[110] T. Wörz et J. Hagenauer : Iterative decoding for multilevel codes using Reliability information. *In Proc. IEEE Globecom Conference*, Orlando, December 1992.

[111] Robert G. Gallager : *Low Density Parity Check Codes*. Thèse de doctorat, Massachusetts Institute of Technology, Cambridge, MA, 1963.

[112] Angelos D. Liveris, Zixiang Xiong et Costas N. Georghiades : Compression of Binary Sources With Side Information at the Decoder Using LDPC Codes. *IEEE Comm. Lett.*, 6(10):440–442, October 2002.

[113] F.R. Kschischang, B.J. Frey et H.-A. Loeliger : Factor graphs and the sum-product algorithm. *IEEE Trans. Inf. Theory*, 47(2):498–519, Feb 2001.

[114] Thomas J. Richardson, M. Amin Shokrollahi et Rdiger L. Urbanke : Design of Capacity-Approaching Irregular Low-Density Parity-Check Codes. *IEEE Trans. Inf. Theory*, 47(2):619–637, February 2001.

[115] Alexandre de Baynast, Predrag Radosavljevic, Joe Cavallaro et Ashutosh Sabharwal : Turbo-schedule for ldpc decoding. *In Proc. 43rd Allerton Conference*, September 2005.

[116] Sae-Young Chung, Jr. G. David Forney, Thomas J. Richardson et Rdiger Urbanke : On the Design of Low-Density Parity-Check Codes within 0.0045 dB of the Shannon Limit. *IEEE Comm. Lett.*, 5(2):58–60, February 2001.

[117] LTHC, Communications Theory Lab.

[118] Stephan ten Brink : Convergence Behavior of Iteratively Decoded Parallel Concatenated Codes. *IEEE Trans. Comm.*, 49(10):1727–1737, October 2001.

[119] Jinghu Chen, Ajay Dholakia, Evangelos Eleftheriou, Marc P. C. Fossorier et Xiao-Yu Hu : Reduced-Complexity Decoding of LDPC Codes. *IEEE Trans. Comm.*, 53(8):1288–1299, August 2005.

Résumé

Longtemps considérée comme une curiosité de laboratoire, la distribution quantique de clés s'est aujourd'hui imposée comme une solution viable de sécurisation des données. Les lois fondamentales de la physique quantique permettent en effet de garantir la sécurité inconditionnelle des clés secrètes distribuées.

Nous avons proposé un système de distribution quantique de clés par photons uniques exploitant un véritable codage en fréquence de l'information. Cette nouvelle méthode de codage permet de s'affranchir de dispositifs interférométriques et offre donc une grande robustesse. Un démonstrateur basé sur des composants optiques intégrés standard a été réalisé et a permis de valider expérimentalement le principe de codage. Nous avons ensuite étudié un système mettant en œuvre un protocole de cryptographie quantique par « variables continues », codant l'information sur l'amplitude et la phase d'états cohérents. Le dispositif proposé est basé sur un multiplexage fréquentiel du signal porteur d'information et d'un oscillateur local.

Les débits atteints par les systèmes de distribution de clés ne sont pas uniquement limités par des contraintes technologiques, mais aussi par l'efficacité des protocoles de réconciliation utilisés. Nous avons proposé un algorithme de réconciliation de variables continues efficace, basé sur des codes LDPC et permettant d'envisager de réelles distributions de clés à haut débit avec les protocoles à variables continues.

Mots clés

cryptographie quantique, distribution quantique de clé, variables continues, algorithme de réconciliation, codes LDPC

Abstract

Despite being long regarded as merely an amusement for researchers, quantum cryptography has now been accepted has a viable solution for secure communications. In fact, the fundamental laws of quantum mechanics guarantee the unconditionnal security of the distributed secret keys.

We proposed a quantum key distribution system based on single-photons, exploiting genuine frequency-coded quantum states. This new coding technique removes the need for interferometric devices and therefore offers high intrinsic robustness. We implemented a system based on integrated off-the-shelf optical devices and validated the coding technique. We then investigated a system based on continuous variables, in which information is encoded in the amplitude and phase of coherent states. The proposed setup is based on frequency multiplexing of the information signal with a local oscillator.

The communication rates achievable by quantum key distribution systems are not only limited by technological constraints, but also by the efficiency of the reconciliation protocols. We developed an efficient reconciliation algorithm for continuous variables based on LDPC codes, which enables high-rate key distributions with continuous variable protocols.

Key words

quantum cryptography, quantum key distribution, continuous variables, reconciliation algorithms, LDPC codes