Theoretical study of continuous-variable quantum key distribution

Anthony Leverrier

École Doctorale
d'Informatique,
Télécommunications
et Électronique de Paris

Thèse

présentée pour obtenir le grade de docteur

de l'Ecole Nationale Supérieure des Télécommunications

Spécialité : Informatique et Réseaux

Anthony LEVERRIER

Etude théorique de la distribution quantique de clés à variables continues.

Soutenue le 20 novembre 2009 devant le jury composé de

Pr. Joseph Boutros	Examinateur
Pr. Nicolas Cerf	Examinateur
Pr. Jean Dalibard	Examinateur
Pr. Philippe Grangier	Directeur de thèse
Pr. Renato Renner	Rapporteur
Pr. Jean-Pierre Tillich	Rapporteur
Pr. Gilles Zémor	Directeur de thèse

École Doctorale
d'Informatique,
Télécommunications
et Électronique de Paris

PhD THESIS

prepared and presented at

Graduate School of Telecom ParisTech

A dissertation submitted in partial fulfillment of the requirements for the degree of

DOCTOR OF SCIENCE

Specialized in Network and Computer Science

Anthony LEVERRIER

Theoretical study of continuous-variable quantum key distribution.

Prof. Joseph Boutros	Examiner
Prof. Nicolas Cerf	Examiner
Prof. Jean Dalibard	Examiner
Prof. Philippe Grangier	Advisor
Prof. Renato Renner	Reviewer
Prof. Jean-Pierre Tillich	Reviewer
Prof. Gilles Zémor	Advisor

A ma famille.

Abstract

This thesis is concerned with quantum key distribution (QKD), a cryptographic primitive allowing two distant parties, Alice and Bob, to establish a secret key, in spite of the presence of a potential eavesdropper, Eve. Here, we focus on continuous-variable protocols, for which the information is coded in phase-space. The main advantage of these protocols is that their implementation only requires standard telecom components.

The security of QKD lies on the laws of quantum physics: an eavesdropper will necessary induce some noise on the communication, therefore revealing her presence.

A particularly difficult step of continuous-variable QKD protocols is the "reconciliation" where Alice and Bob use their classical measurement results to agree on a common bit string. We first develop an optimal reconciliation algorithm for the initial protocol, then introduce a new protocol for which the reconciliation problem is automatically taken care of thanks to a discrete modulation.

Proving the security of continuous-variable QKD protocols is a challenging problem because these protocols are formally described in an infinite dimensional Hilbert space. A solution is to use all available symmetries of the protocols. In particular, we introduce and study a class of symmetries in phase space, which is particularly relevant for continuous-variable QKD. Finally, we consider finite size effects for these protocols. We especially analyse the influence of parameter estimation on the performance of continuous-variable QDK protocols.

Keywords: quantum cryptography, quantum key distribution, quantum optics, quantum communication, quantum bit commitment, phase-space representation, information theory, quantum information theory error correcting code.

Résumé

Cette thèse porte sur la distribution quantique de clés, qui est une primitive cryptographique qui permet à deux correspondants éloignés, Alice et Bob, d'établir une clé secrète commune malgré la présence potentielle d'un espion. On s'intéresse notamment aux protocoles "à variables continues" où Alice et Bob encodent l'information dans l'espace des phases. L'intérêt majeur de ces protocoles est qu'ils sont faciles à mettre en œuvre car ils ne requièrent que des composants télécom standards.

La sécurité de ces protocoles repose sur les lois de la physique quantique : acquérir de l'information sur les données échangées par Alice et Bob induit nécessairement un bruit qui révèle la présence de l'espion.

Une étape particulièrement délicate pour les protocoles à variables continues est la "réconciliation" durant laquelle Alice et Bob utilisent leurs résultats de mesure classiques pour se mettre d'accord sur une chaîne de bits identiques. Nous proposons d'abord un algorithme de réconciliation optimal pour le protocole initial, puis introduisons un nouveau protocole qui résout automatiquement le problème de la réconciliation grâce à l'emploi d'une modulation discrète.

Parce que les protocoles à variables continues sont formellement décrits dans un espace de Hilbert de dimension infinie, prouver leur sécurité pose des problèmes mathématiques originaux. Nous nous intéressons d'abord à des symétries spécifiques de ces protocoles dans l'espace des phases. Ces symétries permettent de simplifier considérablement l'analyse de sécurité. Enfin, nous étudions l'influence des effets de tailles finies, tels que l'estimation du canal quantique, sur les performances des protocoles.

Mots-clés : cryptographie quantique, distribution quantique de clés, optique quantique, communications quantiques, mise en gage quantique, représentation dans l'espace des phases, théorie de l'information, théorie de l'information quantique, code correcteur d'erreurs.

Contents

Remerciements

Ce manuscrit marque la fin de trois années fantastiques passées à essayer d'aider Alice et Bob à discuter tranquillement en utilisant des variables continues ... trois années passées à essayer d'améliorer les techniques existantes, et chose plus délicate, tenter de prouver que ces techniques étaient réellement sûres.

La première personne que je tiens à remercier chaleureusement est bien entendu Romain Alléaume, qui a rendu cette thèse possible : d'abord en m'aidant à trouver un stage chez MagiQ à Boston, qui m'a donné goût au sujet de la cryptographie quantique, puis bien sûr en réussissant à monter cette thèse ... et m'évitant ainsi de me retrouver à travailler dans quelque obscur ministère. Bref, je dois à Romain de m'avoir permis de me lancer dans le monde de la recherche, monde que je ne compte pas quitter de sitôt. Je dois bien avouer que Romain m'a beaucoup déstabilisé au cours de ces trois années. Je me souviens de ces journées où Romain passait boire un café dans mon bureau toutes les deux heures. A chaque nouvelle pause, Romain me racontait qu'il avait géré un projet européen, eu une idée pour monter un nouveau projet, avancé en ce qui concerne la création de sa start-up, ou même fait un peu de politique interne à l'école. De mon côté, je venais de passer deux heures à contempler une feuille désespéramment blanche en essayant d'avancer ma recherche. Et le pire était bien sûr que chaque action entreprise par Romain été couronnée de succès : que ça soit le projet SECOQC, la création de SeQureNet et la naissance de l'équipe quantique à l'école. Pas facile de travailler aux côtés de Romain, mais le moins que l'on puisse dire, c'est que ce fut une expérience pour le moins stimulante !

Je souhaite ensuite remercier Michel Riguidel, ainsi que son successeur Gérard Memmi, qui m'ont accueilli au sein du département Informatique et Réseaux de Télécom ParisTech, et m'ont offert des conditions exceptionnelles pour mener à bien mes travaux de thèse. Plus généralement, je remercie Télécom ParisTech pour les conditions idéales dans lesquelles j'ai pu travailler ces trois dernières années.

L'encadrement de cette thèse a été quelque peu particulier, il faut bien l'avouer ! Quelques mois avant le début de ma thèse, on s'était mis d'accord sur un co-encadrement entre Gilles Zémor, alors à Télécom ParisTech, et Philippe Grangier à l'Institut d'Optique. Cette organisation simple a très rapidement été mise à mal puisque Gilles est parti prendre un poste de professeur à Bordeaux le premier jour de ma thèse. Joseph Boutros a alors très gentiment proposé d'aider à m'encadrer. C'était bien sûr sans compter sur la propension de Joseph à aller découvrir des endroits aussi exotiques que Doha au Qatar, où il a choisi de s'établir un an après le début de ma thèse. Ainsi, pour une thèse effectuée à Paris, mon encadrant le plus proche géographiquement s'est retrouvé être Philippe Grangier qui a fait un effort pour se rapprocher de moi en déménageant son labo d'Orsay vers Palaiseau !

A distance ou non, chacun de mes trois directeurs de thèse m'a aidé, chacun avec son style particulier.

D'abord Gilles, avec qui j'ai trop peu travaillé à mon goût, mais ce n'est j'espère que partie remise. Je me souviens de quelques après-midi passés devant un tableau blanc à essayer de convaincre Gilles que diverses techniques de réconciliation ne révélaient pas d'information à notre espion favori, Eve. A chaque fois, je pensais avoir raison, et je désperais d'en convaincre Gilles, mais il faut bien avouer que ceci n'est pas chose facile, tout particulièrement quand on a tort !

Joseph ensuite, personnage pour le moins inimitable et inoubliable ! Joseph m'a fait découvrir beaucoup des subtilités qui accompagnent les codes correcteurs d'erreurs, tout particulièrement les codes LDPC. Je sais bien que Joseph a tenté de me convaincre de travailler sur les turbo-codes plutôt, mais ces codes et leur fonctionnement beaucoup trop compliqué à mon goût m'ont toujours effrayé, et j'ai trouvé le moyen de les éviter tout au long de ma thèse. Un des moments les plus marquants de ma thèse a certainement été la semaine passée à Doha dans la famille de Joseph. Je ne dirais pas que cette semaine ait été de tout repos ... je me souviens d'un moment où une certaine Mareva s'était enfermée dans le bureau où Joseph et moi avions laissé nos ordinateurs, et avoir craint pour la survie de ces-dits ordinateurs (surtout du mien en fait !). Ces craintes n'étaient bien sûr pas justifiées. Cette semaine a également était une révélation pour moi car j'y ai découvert pour la première fois la véritable cuisine libanaise dont je suis immédiatement tombé amoureux.

Enfin Phillipe, avec qui j'ai le plus interagi, et qui m'a ouvert les portes du monde de la physique, et de la communauté de l'information quantique. Philippe m'a beaucoup appris ces dernières années, que ce soit au cours de discussions tardives à l'Institut d'Optique ou à travers de longs échanges d'emails, en particulier pendant les week-ends. Je dois avouer que ma thèse a réellement démarré le jour où je me suis délocalisé entre Télécom ParisTech et l'Institut d'Optique.

Hormi mes directeurs de thèse, je ne peux pas oublier Nicolas Cerf, avec qui j'ai beaucoup travaillé, et que je remercie pour l'accueil chaleureux qu'il m'a réservé à de nombreuses reprises dans son groupe à Bruxelles, ainsi que pour sa généreuse invitation à Boston.

Merci également à Renato Renner et Valerio Scarani qui m'ont invité respectivement à

Zürich et à Singapour, ainsi qu'à Iordanis Kerenidis qui m'a permis de découvrir Tokyo. Renato, ainsi que Johan Åberg à l'ETH, ont toujours fait preuve d'une très grande disponibilité pour répondre à mes nombreuses questions.

Je remercie bien évidemment les membres de l'équipe crypto quantique de l'Institut d'Optique : Simon Fossier et Eleni Diamanti qui m'ont accueilli dans leur bureau et avec qui j'ai partagé des discussions passionnantes, sur la physique quantique ou sur n'importe quel autre sujet. Merci également à Rosa Tualle-Brouri ainsi qu'à Thierry Debuisschert, et plus généralement à toute l'équipe du groupe d'optique quantique. Je remercie tous les membres du QuiC pour leur accueil, et plus particulièrement Loïck Magnin avec qui on s'est amusé plus longtemps que prévu sur un certain théorème d'impossibilité, Raúl García-Patrón transfuge au MIT, et bien sûr Evgueni Karpov qui s'est attelé à m'aider à montrer la sécurité inconditionnelle de nos protocoles. Enfin, du côté de Télécom ParisTech, j'ai beaucoup apprécié l'ambiance de l'équipe quantique que j'ai vu se monter sous mes yeux sous l'impulsion de Romain. Je pense à Damian Markham, qui m'a fait découvrir les joies du karaoké, à Aurélien Bocquet, plus récemment aux nouvelles recrues de SeQureNet, Paul Jouguet et Sébastien Kunz-Jacques, et enfin aux nouveaux doctorants qui prennent le relais et à qui je souhaite bonne chance, Anne Marin et Zizhu Wang.

Je remercie enfin les membres de mon jury, en particulier les rapporteurs Jean-Pierre Tillich et Renato Renner qui ont accepté la lourde charge de décortiquer ce manuscrit de thèse, ainsi que Jean Dalibard, qui m'a enseigné la mécanique quantique à l'X, et qui n'a pas hésité à abandonner quelque temps les condensats de Bose Einstein pour venir découvrir les péripéties d'Alice et Bob.

Un dernier mot pour remercier ma famille qui m'a encouragé tout au long de mes interminables études. Un grand merci pour leur soutien sans faille !

List of Publications

Papers in Peer-Reviewed Scientific Journals

1. A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, P. Grangier, *Multidimensional reconciliation for continuous-variable quantum key distribution*, Physical Review A 77, 042325 (2008).

2. A. Leverrier, P. Grangier, *Unconditional security proof of long-distance continuous-variable quantum key distribution with a discrete modulation*, Physical Review Letters, 102, 180504 (2009).

3. A. Leverrier and N.J. Cerf. *Quantum de finetti theorem in phase-space representation*, Physical Review A, 80, 010102 (2009).

4. A. Leverrier, E. Karpov, P. Grangier, N.J. Cerf, *Security of continuous-variable quantum key distribution: exploiting symmetries in phase space*, New Journal of Physics, 11, 115009 (2009).

5. L. Magnin, F. Magniez, A. Leverrier, N.J. Cerf, *Strong No-Go Theorem for Gaussian Quantum Bit Commitment*, Physical Review A (2010).

6. R. Alléaume, J. Bouda, C. Branciard, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, A. Leverrier, N. Lütkenhaus, P. Painchault, M. Peev, A. Poppe, T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfürter, A. Zeillinger, *SECOQC White Paper on Quantum Key Distribution and Cryptography*, eprint arXiv: quant-ph/0701168 (submitted to Theoretical Computer Science).

Conferences Proceedings

1. A. Leverrier, R. Alléaume, J.J. Boutros, G. Zémor, P. Grangier, *Multidimensional reconciliation for continuous-variable quantum key distribution*, Proc. 2008 IEEE International Symposium on Information Theory, pages 1020-1024, July 2008.

2. D. Elkouss, A. Leverrier, R. Alléaume, J.J. Boutros, *Efficient reconciliation protocol for discrete-variable quantum key distribution*, Proc. 2009 IEEE International Symposium on Information Theory, pages 1879-1883, July 2009.

Résumé en français

Cette thèse s'intéresse à la distribution quantique de clés, et plus particulièrement à certains aspects théoriques liés à l'utilisation de variables continues.

La distribution quantique de clés, souvent appelée de façon abusive *cryptographie quantique*, est une primitive cryptographique[1] qui permet à deux correspondants éloignés, traditionnellement prénommés Alice et Bob, d'établir une clé secrète commune. Cette clé secrète peut ensuite être utilisée pour chiffrer des communications à l'aide de protocoles de cryptographie symétrique. En particulier, combiner distribution quantique de clés avec le code de Vernam, qui est le seul protocole de chiffrage inconditionnellement sûr, permet d'obtenir une sécurité absolue pour les communications. Rappelons rapidement le fonctionnement du code de Vernam: Alice et Bob disposent initialement d'une clé secrète C de longueur n. Si Alice veut envoyer un message M de longueur n à Bob[2], elle calcule le "ou exclusif" entre le message et la clé pour obtenir le message chiffré $MC = M \oplus C$. Ensuite, Bob décode ce message chiffré en appliquant simplement le "ou exclusif" avec la clé secrète pour obtenir le message secret envoyé par Alice : $M = MC \oplus C$. Il est simple de montrer qu'un espion, prénommé Eve[3], qui n'a accès qu'au message chiffré, ne peut obtenir aucune information sur le message secret : $H(M|MC) = H(M)$. Le problème, insoluble classiquement au sens de la théorie de l'information, du code de Vernam réside toutefois dans l'hypothèse qu'Alice et Bob disposent initialement d'une clé parfaitement secrète.

L'intérêt de la distribution *quantique* de clés est de fournir une solution *physique* au

[1] Une primitive cryptographique est un protocole cryptographique de bas niveau qui peut être intégré dans un système de cryptographie. Une autre primitive est par exemple l'*autentification* qui consiste à établir ou confirmer l'identité de quelqu'un (ou quelque chose).

[2] En fait, afin d'optimiser le protocole, Alice commence en général par compresser son message de façon à ce qu'il ait une entropie maximale.

[3] le choix du prénom Eve vient de l'anglais "eavesdropper", qui réfère à un espion, ou plus généralement, à quelqu'un qui écoute aux portes.

problème de la distribution de clés. L'idée de base est pour Alice et Bob d'échanger des systèmes quantiques sur lesquels est encodée de l'information. Ensuite, les relations d'incertitude d'Heisenberg garantissent que dans une certaine mesure, si Eve venait à écouter la conversation quantique d'Alice et Bob, elle induirait des perturbations sur les systèmes quantiques échangés, perturbations qui seraient suffisantes pour révéler sa présence. A contrario, en l'absence de telles perturbations, Alice et Bob sont certains que leur conversation n'a pas été écoutée, et peuvent utiliser leurs données respectives pour établir une clé secrète. Bien sûr, cette présentation est simplifiée à l'extrême, et les scientifiques travaillent depuis 25 ans, la date de l'invention de la distribution quantique de clés par Bennett et Brassard [10], à la rendre plus rigoureuse. En particulier, même en l'absence d'espion, les données d'Alice et Bob sont toujours plus ou moins bruitées, simplement parce que les transmissions optiques ne sont jamais parfaites: les fibres optiques (comme n'importe quel autre medium de transmission) présentent toujours des pertes, les détecteurs ne sont jamais parfaits, etc. En pratique, ces défauts existent donc toujours et sont *a priori* indiscernables de l'action malveillante d'un espion. Néanmoins, si ces défauts sont suffisamment faibles, intuitivement, on sent que les données d'Alice et Bob peuvent être utiles pour distiller des clés secrètes. La question théorique qui se pose alors est de quantifier la taille de la clé secrète qu'Alice et Bob peuvent extraire à partir de leurs données. En fait, la méthode d'extraction d'une clé d'une longueur donnée à partir de données corrélées est bien établie. On procède typiquement en deux étapes. D'abord, Alice et Bob transforment leurs données corrélées en données identiques, c'est l'étape de correction d'erreurs, ou de *réconciliation*. Ensuite, ils utilisent une fonction de hachage pour transformer leur chaîne de données commune en une clé parfaitement sûre. La question est donc de savoir de combien il faut diminuer la taille de la chaîne initiale pour obtenir une clé véritablement secrète.

Bien entendu, le but est de mettre au point un protocole aussi pratique que possible, c'est-à-dire facile à mettre en œuvre expérimentalement, qui permette de distribuer un débit maximum de clés secrètes. Aujourd'hui, en 2009, on ne sait pas toujours quel protocole est le meilleur. Répondre à cette question suppose d'abord d'avoir une définition de la qualité d'un protocole. La performance typique d'un protocole est de permettre de distribuer des clés tant qu'Alice et Bob ne sont pas trop éloignés. Plus précisément, le taux de clé secrète K que l'on peut distribuer est une fonction de la distance d entre Alice et Bob qui a généralement la forme suivante:

$$K(d) = \begin{cases} K_0 10^{-\eta d} & \text{pour} \quad d \leq d_{\max} \\ 0 & \text{pour} \quad d \geq d_{\max}. \end{cases} \tag{1}$$

Dans cette équation, η représente la perte linéique du medium de transmission, par exemple $\eta = 0.02$ pour une fibre optique classique qui présente 0.2 dB de pertes par kilomètre aux longueurs d'onde télécom. Le paramètre $d_{\max}$ représente une distance maximale au-dessus de laquelle le protocole en question ne permet plus de distribuer une clé secrète. L'ordre de grandeur typique pour cette distance maximale est de quelques dizaines de kilomètres, voire une centaine de kilomètres, et dépend de façon cruciale de la définition de sécurité utilisée.

Un but évident est donc d'essayer de trouver les protocoles qui permettent de distribuer des clés sur des distances aussi grandes que possibles. Toutefois, cette question est plus délicate qu'il n'y paraît car établir le taux secret d'un protocole donné est une tâche compliquée. En effet, l'intérêt de la cryptographie quantique est de ne faire aucune hypothèse sur l'espion, qui n'est contraint que par les lois de la mécanique quantique. Ainsi, les stratégies possibles pour l'espion sont innombrables et déterminer laquelle est optimale constitue un problème généralement insoluble, en dehors de quelques protocoles de distribution quantiques assez simples. Heureusement, ces protocoles assez simples pour pouvoir être étudiés (et mis en œuvre) apparaissent comme très robustes, et sont probablement meilleurs que d'autres protocoles trop compliqués pour être étudiés théoriquement ou réalisés expérimentalement.

La plupart de ces protocoles à la fois simples et robustes sont inspirés du protocole BB84 introduit par Bennett et Brassard et ont la particularité d'encoder l'information sur des systèmes quantiques à deux niveaux, par exemple la polarisation de photons uniques. Le fait que ces systèmes, décrits dans des espaces de Hilbert de dimension 2, soient particulièrement bien connus théoriquement grâce à la multitude de problèmes physiques où ils interviennent, a pour conséquence de simplifier l'analyse théorique des protocoles cryptographiques en question. L'inconvénient de ces protocoles, toutefois, est que le support de l'information, un photon unique, est difficile à générer et plus encore à détecter. En fait, l'absence de vraies sources de photons uniques ne constitue pas un trop gros handicap pour la cryptographie quantique car de simples sources d'états cohérents atténués remplacent avantageusement les sources de photons uniques : elles sont beaucoup, beaucoup plus simples à mettre en œuvre et ont un impact limité en termes de sécurité[4]. L'autre problème de ces protocoles est que Bob est obligé de détecter des photons uniques, ce qui est une tâche technologiquement délicate. En fait, les détecteurs de photons uniques ont généralement une efficacité quantique limitée à quelque 10 ou 20%[5]. Comme ces détecteurs de photons uniques n'ont qu'une application limitée, l'industrie ne finance pas d'importants travaux de recherche et développement pour les améliorer, et les progrès technologiques sont de ce fait assez lents.

Pour ces raisons, une alternative a été proposée au début des années 2000 : encoder l'information dans l'espace des phases plutôt que dans un système quantique à deux niveaux. L'intérêt est alors que la détection n'est plus faite par un détecteur de photons, mais par une technique interférométrique appelée *détection homodyne* qui peut être réalisée à l'aide de photodiodes PIN standard. Comme ces photodiodes sont massivement utilisées par l'industrie télécom, elles sont comparativement bien plus performantes que les détecteurs de photons de la cryptographie quantique *à la BB84*. La distribution quantique de clés où l'information est encodée dans l'espace des phases est dite "à variables continues" par opposition aux traditionnels protocoles "à variables discrètes".

Technologiquement, encoder l'information sur des variables continues, les quadratures de l'espace des phases, semble être une bonne alternative aux protocoles à variables

[4] c'est-à-dire qu'on arrive à intégrer aux preuves de sécurité le fait que l'on utilise des sources d'états cohérents atténués au lieu de vrais photons uniques.

[5] aux longueurs d'onde télécom, 1550 nm, pertinentes pour la cryptographie quantique.

discrètes. Cependant, parce qu'espace des phases est synonyme d'espace de Hilbert de dimension infinie, l'analyse théorique des protocoles de cryptographie quantique à variables continues est assez délicate.

Au début de ma thèse, en 2006, des protocoles à variables continues avaient déjà été proposés et étudiés. A cette époque, ces protocoles avaient été prouvés sûrs contre une classe d'attaques restreintes appelées "attaques collectives", dans le cas asymptotique où les caractéristiques du canal gaussien[6] liant Alice à Bob sont parfaitement connues. Malheureusement, les protocoles à variables continues, bien que sûrs, ne semblaient alors fonctionner que pour de courtes distances : 30 kilomètres maximum. La cause de cette limitation était alors identifiée comme étant l'efficacité limitée de la réconciliation des variables corrélées d'Alice et Bob. Améliorer cette réconciliation était donc une condition *sine qua non* à l'augmentation de la portée des protocoles à variables continues.

L'objectif de cette thèse était double. D'abord, proposer de nouveaux algorithmes pour améliorer la réconciliation, et ainsi augmenter la portée des protocoles à variables continues. Ensuite, il s'agissait d'étendre les preuves de sécurité aux attaques les plus générales, en prenant notamment en compte les effets de tailles finies.

Le premier objectif a été rempli doublement. Il fait l'objet de la Partie II de ce manuscrit. D'une part, un algorithme de réconciliation spécifique a été proposé afin d'améliorer l'efficacité de la réconciliation à faible rapport signal à bruit (voir chapitre 4). L'utilisation de cet algorithme permet, sans rien changer à l'implémentation expérimentale du protocole à variables continues initial, de faire passer la portée du protocole de 30 à 50 km. Ensuite, un nouveau protocole à variables continues utilisant une modulation discrète a été proposé. Cet algorithme a été prouvé aussi sûr que l'algorithme initial qui utilise une modulation gaussienne, et permet de distribuer des clés secrètes sur des distances supérieures à la centaine de kilomètres[7]. Ce protocole est donc tout-à-fait compétitif vis-à-vis des traditionnels protocoles de distribution quantique de clés à variables discrètes (voir chapitre 5).

Le second objectif –étudier la sécurité des protocoles à variables continues face aux attaques les plus générales– était nettement plut délicat. Pendant ma thèse, la question a en partie été résolue par Renner et Cirac [127] qui ont montré que les attaques collectives étaient optimales dans la limite asymptotique. En revanche, la méthode qu'ils emploient n'utilise pas les symétries naturelles des protocoles de distribution quantique de clés à variables continues, et il est donc plausible que les bornes qu'ils obtiennent puissent être substantiellement améliorées (voir chapitre 6). Ensuite, nous avons étudié spécifiquement les effets de tailles finies pour les protocoles à variables continues (voir chapitre 7). Les résultats obtenus sont assez pessimistes, mais sont conformes à ce que l'on pouvait attendre suite aux récentes études sur les effets de tailles finies pour les protocoles à variables discrètes. Enfin, dans le chapitre 8, on étudie d'autres problèmes liés à la cryptographie quantique avec des variables continues, différents de la distribution quantique de clés. En particulier, on s'intéresse aux mesures optimales pour distinguer

[6] un canal gaussien est défini par deux grandeurs : sa transmission et son niveau de bruit.

[7] dans l'hypothèse d'un régime asymptotique où le canal gaussien reliant Alice à Bob est complètement caractérisé.

des états cohérents. Ensuite, on s'intéresse à une autre primitive cryptographique : la mise en gage. On prouve en particulier que la mise en gage quantique est impossible avec des états gaussiens et des opérations gaussiennes uniquement.

Les différentes parties de ce manuscrit sont maintenant décrites en détail.

Partie I : Rappels généraux sur l'information quantique, les variables continues et la cryptographie quantique

La première partie de ce manuscrit (chapitres 1 à 3) consiste en une présentation des outils nécessaires à l'étude de la distribution quantique de clés à variables continues. Trois chapitres peuvent sembler beaucoup pour présenter cette thématique, mais la distribution quantique de clés à variables continues est à l'intersection de diverses disciplines : mécanique quantique, théorie de l'information, optique quantique, cryptographie, etc, et son étude requiert une bonne connaissance de toutes ces disciplines.

Chapitre 1 : Information et communication quantiques

Le premier chapitre pose les fondations de la jeune discipline scientifique qu'est la théorie de l'information quantique. Ce champ de recherche, vieux d'une vingtaine d'années, vise à comprendre les liens entre la mécanique quantique et la théorie de l'information développées respectivement dans les années 20 et les années 50. Il est troublant que la théorie de l'information quantique ait mis si longtemps à émerger puisqu'elle constitue le prolongement naturel de la théorie de l'information de Shannon. En effet, toute information est codée de façon ultime sur un support quantique puisque la description de la nature est quantique.

Le premier chapitre présente donc successivement les bases de la mécanique quantique, en particulier les axiomes mathématiques qui la caractérisent, puis la théorie de l'information de Shannon avec ses deux théorèmes centraux qui décrivent le codage de source et le codage de canal, et naturellement les quantités qui leur sont associées : l'entropie, et l'information mutuelle. Enfin, on décrit comment les notions d'entropie et d'information mutuelle sont généralisées dans un contexte quantique. On introduit en particulier le concept de "smooth min-entropy" qui est particulièrement pertinent pour l'analyse théorique de protocoles cryptographiques quantiques.

Chapitre 2 : Information quantique avec des variables continues

Le deuxième chapitre s'intéresse aux spécificités de la théorie de l'information quantique avec des variables continues. D'abord, on présente le domaine de l'optique quantique, et la représentation dans l'espace de phases. Ensuite, on introduit les états gaussiens et les opérations gaussiennes. Ces états et transformations sont incontournables en optique quantique car ils correspondent exactement à ce qu'il est relativement facile de faire expérimentalement, tout en disposant d'un formalisme théorique qui permet leur étude. Ce deuxième point est essentiel car l'optique quantique est en général décrite dans un espace de Hilbert de dimension infinie, ce qui rend les analyses théoriques infaisables dans la plupart des cas, à l'exception notable des états gaussiens et opérations gaussiennes.

Enfin, on décrit les spécificités des variables continues par rapport aux outils de l'information quantique. Il est intéressant de noter qu'alors que les variables continues posent de nombreux problèmes en théorie *classique* de l'information, ce n'est plus nécessairement le cas en théorie quantique de l'information où les entropies par exemple

restent bien définies pour les variables continues. On insiste également sur les propriétés des états gaussiens qui se trouvent être extrémaux vis-à-vis de diverses fonctionnelles telles que l'entropie par exemple. Ces propriétés font que les états gaussiens, outre le fait qu'ils soient facilement décrits de manière théorique, sont en fait souvent les états les plus adaptés à diverses tâches de communications quantiques, et tout particulièrement pour la distribution quantique de clés.

Chapitre 3 : Distribution quantique de clés

Le troisième chapitre présente finalement la distribution quantique de clés. Le chapitre commence par une discussion sur la notion de sécurité d'un protocole. En particulier, la sécurité d'une clé est une notion qui n'est décrite de manière satisfaisante que depuis très récemment[8]. Un protocole générique de distribution quantique de clés est ensuite décrit, et le principe général de l'étude de la sécurité de cette primitive cryptographique est détaillé. En particulier, la plupart des preuves de sécurité font appel à la notion d'intrication virtuelle. La fin du chapitre s'intéresse plus particulièrement aux protocoles à variables continues, et aux preuves de sécurité (contre les attaques collectives) qui les concernent.

En conclusion, cette première partie ne contient quasiment pas de recherche originale. C'est une partie d'introduction qui présente les outils théoriques nécessaires à l'étude de protocoles de distribution quantique de clés.

[8]La thèse de Renato Renner [124] fait généralement autorité en ce qui concerne la définition et l'étude de la sécurité de la distribution quantique de clés.

Partie II : Améliorer la portée des protocoles à variables continues

La seconde partie de ce manuscrit présente des travaux de recherche dont le but était d'augmenter la portée des protocoles de distribution quantique de clés à variables continues. Au début de ma thèse, en 2006, les protocoles à variables continues pouvaient distribuer des clés sur des distances inférieures à 30 km. La raison de cette limitation était alors déjà bien identifiée comme étant l'efficacité insuffisante de la réconciliation des données corrélées d'Alice et Bob.

Deux solutions ont été apportées à ce problème. D'abord, un nouvel algorithme de réconciliation a été introduit. Cet algorithme, conçu spécifiquement pour la réconciliation de variables gaussiennes corrélées à faible rapport signal à bruit, permet d'augmenter la portée du protocole de 30 à 50 km. La présentation détaillée de cet algorithme fait l'objet du chapitre 4 de ce manuscrit.

Ensuite, afin de résoudre totalement les problèmes liés à la réconciliation, un nouveau protocole de distribution quantique de clés a été proposé. L'idée de ce protocole est d'utiliser une modulation discrète au lieu de la traditionnelle modulation gaussienne. Ce nouveau protocole est présenté dans le chapitre 5. Les performances de ce protocole sont très intéressantes car elles sont comparables à celles des meilleurs protocoles à variables discrètes en termes de portée. Pour être plus précis, dans la limite asymptotique de clés infiniment longues, des distances nettement supérieures à 100 km peuvent être atteintes avec les implémentations expérimentales actuelles[9]. Par ailleurs, on prouve dans le chapitre 5 que les preuves de sécurité du protocole à modulation gaussienne habituel peuvent être adaptées pour le nouveau protocole à modulation discrète. Ainsi, ce nouveau protocole est aussi sûr que le précédent, mais présente de bien meilleures performances en termes de portée.

Chapitre 4 : Réconciliation de variables gaussiennes corrélées

Dans le chapitre 4, on s'intéresse au problème de l'amélioration du protocole de distribution quantique de clés à variables continues basé sur une modulation gaussienne. Ce protocole fonctionne de la façon suivante. Alice tire deux variables aléatoires (q_A, p_A) qui suivent une distribution normale centrée de variance V_A, et envoie à Bob un état cohérent centré au point (q_A, p_A) de l'espace des phases. Bob reçoit cet état après qu'il a traversé le canal quantique, typiquement une fibre optique, et choisit aléatoirement de mesurer l'une ou l'autre des deux quadratures. Son résultat de mesure est noté y. Bob informe alors Alice de son choix de quadrature. Alice ne conserve que la variable q_A ou p_A correspondante et la note x. Alice et Bob répètent cette opération un grand nombre n de fois (typiquement n prend des valeurs de l'ordre de 10^5 ou 10^6. Alice et Bob stockent

[9] Il faut toutefois relativiser ces résultats en tenant compte des effets de taille finie. Ces effets sont décrits au chapitre 7 et mettent en doute la capacité de distribuer des clés secrètes sur des distances nettement supérieures à 100 km. Toutefois, ce problème n'est pas du tout spécifique aux protocoles à variables continues, et aucun protocole actuel n'est en mesure de distribuer des clés secrètes sur 100 km si l'on tient compte de ces effets de taille finie.

leurs variables dans deux vecteurs $X = (x_1, \cdots, x_n)$ et $Y = (y_1, \cdots, y_n)$. On suppose ici qu'Alice et Bob connaissent parfaitement le canal gaussien qui les lie, qui est caractérisé par sa transmission et son excès de bruit[10]. En fait, on suppose juste que les variances d'Alice et Bob, ainsi que la covariance entre leurs données sont parfaitement connues. A une normalisation près, le modèle pertinent pour leurs données est le suivant :

$$y_i = x_i + z_i, \tag{2}$$

où les x_i (resp. les z_i) sont des variables gaussiennes centrées indépendantes et identiquement distribuées de variance 1 (resp. σ^2).

Le problème pour Alice et Bob est alors de transformer ces données en une clé secrète. Deux étapes sont nécessaires :

- la *réconciliation* consiste pour Alice et Bob à utiliser leurs données corrélées pour se mettre d'accord sur une chaîne de bits identiques,
- l'*amplification de confidentialité* consiste à utiliser une fonction de hachage pour transformer leur chaîne commune en une clé secrète.

L'amplification de confidentialité ne pose pas de problème particulier, et on s'intéresse ici uniquement à la réconciliation. Pour rendre les choses un peu plus compliquées, la réconciliation doit être *inverse*[11], c'est-à-dire que Bob doit calculer une chaîne U à partir de son vecteur Y et qu'Alice doit déterminer cette chaîne U. A cette fin, Bob va envoyer de l'information à Alice[12] pour l'aider à retrouver U à partir de son vecteur X.

Le problème de la réconciliation est en fait très proche d'un problème de codage de canal. La seule différence tient dans le fait que Bob reçoit une donnée aléatoire qu'il doit faire retrouver à Alice, alors que dans un problème de codage de canal classique, Alice envoie un *mot de code* à Bob qui doit le retrouver. Le moyen de transformer le problème de la réconciliation en problème de codage de canal est de travailler avec un *code coset*. Supposons qu'Alice et Bob utilisent des données binaires et que le canal qui les relie soit un canal binaire symétrique. Dans ce cas, Alice et Bob choisissent un code correcteur d'erreurs linéaire adapté au canal, et Bob peut simplement définir le code coset qui contient Y en informant Alice du syndrome de Y pour le code en question.

En fait, le problème de la réconciliation de données binaires est presque trivial dans le sens où il se ramène immédiatement à un problème bien connu de codage de canal. Les choses se compliquent singulièrement pour des données continues. Dans ce cas, Bob

[10] En réalité, cette hypothèse est trop forte, et Alice et Bob doivent échanger $N = n + m$ signaux, dont m sont utilisés pour l'estimation du canal. Toutefois, l'hypothèse faite ici que le canal est bien caractérisé correspond à une hypothèse très répandue dans le domaine de la cryptographie quantique. Les effets liés à la taille finie, et en particulier le problème de l'estimation de paramètres, sont traités dans le chapitre 7.

[11] l'alternative qu'est la réconciliation *directe* est en effet incompatible avec des pertes supérieures à 3 dB, et n'est donc pas intéressante pour distribuer des clés à grande distance puique 3 dB représentent seulement 15 km de fibre.

[12] sur un canal classique authentifié sans erreur. En fait l'espion Eve a accès à ce canal qu'elle peut écouter, mais elle ne peut pas modifier les communications qui y transitent.

reçoit un vecteur réel qui n'appartient pas clairement à un code coset donné. La solution à ce problème est pourtant d'essayer de définir un code pour lequel Y appartienne à un coset. L'idée de base est de voir que Y n'est pas distribué uniformément dans $\mathbb{R}^n$ mais que le vecteur normalisé $Y/||Y||$ a une distribution uniforme sur la sphère unité, $\mathcal{S}^{n-1}$, de $\mathbb{R}^n$. Le problème est maintenant de définir de bons codes correcteurs d'erreurs sur cette sphère. Une façon naturelle de définir de bons codes sur la sphère $\mathcal{S}^{n-1}$ est d'utiliser l'isomorphisme suivant entre $\mathbb{F}_2^n = \{0;1\}^n$ et $\mathcal{S}^{n-1}$:

$$\begin{array}{rccc} \Phi & : & \mathbb{F}_2^n & \longrightarrow & \mathcal{S}^{n-1} \\ & & b & \longmapsto & \frac{(-1)^b}{\sqrt{n}}. \end{array} \tag{3}$$

On choisit donc de bons codes correcteurs pour le canal bi-AWGN (modulation binaire $\pm A$ suivie d'un canal additif à bruit blanc gaussien). Soit C un tel code, c'est-à-dire un ensemble de points de $\Phi(\mathbb{F}_2^n)$. Le problème est maintenant de faire correspondre à chaque point possible $Y/||Y||$ de la sphère un élément de C. La méthode que nous proposons est la suivante. Bob choisit un point U de $\Phi(\mathbb{F}_2^n)$ avec une distribution uniforme. Ce point U est le vecteur binaire que doit retrouver Alice. Pour cela, Bob calcule $\alpha = U \cdot Y^{-1}$ où la multiplication et l'inversion sont les lois d'un groupe que l'on va préciser. Ensuite, Bob envoie à Alice la valeur du vecteur α ainsi que le syndrome du mot U pour le code C. Alice calcule $\hat{U} = \alpha \cdot X = U \cdot Y^{-1} \cdot X$. Si le groupe est bien choisi, $\hat{U}$ correspond à une version bruitée de U telle que le bruit $||\hat{U} - U||$ soit égal au bruit $||Z|| = ||Y - X||$. Enfin, Alice décode $\hat{U}$ dans le code coset de C défini par le syndrome de U et retrouve la valeur de U (avec une probabilité d'erreur négligeable).

Pour que cette stratégie fonctionne, on voit qu'on a besoin de mettre une structure de groupe sur la sphère $\mathcal{S}^{n-1}$. En fait, une conséquence d'un théorème d'Adams est que les sphères avec une structure de groupe (en fait, les sphères qui sont des algèbres de division) sont les sphères unité dans $\mathbb{R}, \mathbb{R}^2, \mathbb{R}^4$ et $\mathbb{R}^8$. Ces sphères correspondent respectivement aux unités des réels, des complexes, des quaternions et des octonions. Dans notre cas, on cherche à travailler dans la plus grande dimension possible, c'est-à-dire en dimension 8. A cette fin, les vecteurs X, Y et U sont divisés en sous-vecteurs de longueur 8, et identifiés aux octonions correspondants. Pour ces octonions, Bob calcule simplement la division de U par Y pour former α. Cette division correspond en fait à une rotation dans $\mathbb{R}^8$, c'est-à-dire une isométrie qui préserve les distances, ce qui assure que $||\hat{U} - U|| = ||X - Y||$ pour la norme 2.

La stratégie décrite ci-dessus est optimale dans le sens que la dimension 8 est la dimension maximale qui ait les propriétés requises. L'algorithme de réconciliation ainsi défini présente de bonnes performances, spécialement à faible rapport signal à bruit, par exemple pour une variance du bruit gaussien $\sigma^2 = 2$. En conséquence, l'utilisation de cet algorithme dans le protocole de distribution quantique de clé à variables continues permet d'améliorer notablement les performances de ce dernier. En particulier, la distance maximale du protocole est portée à 50 km contre 30 km en utilisant l'ancien algorithme de réconciliation où les données sont quantifiées en dimension 1 plutôt qu'en dimension 8.

Chapitre 5 : Distribution quantique de clés à longue distance : protocoles à variables continues et modulation discrète

Dans le chapitre 4, on a décrit une technique de réconciliation permettant d'accroître significativement la portée du protocole de distribution quantique de clé à modulation gaussienne. Malheureusement, cette technique reste impuissante quand le rapport signal à bruit se dégrade trop, ce qui arrive inévitablement lorsque l'on essaie de distribuer des clés à longue distance.

Comme le problème vient de la réconciliation imparfaite des variables gaussiennes, l'idée naturelle est de considérer un problème plus simple que l'on sait bien résoudre. Ce problème est celui de la correction d'erreurs pour un canal bi-AWGN. En particulier, on sait bien corriger les erreurs pour ce canal, même pour des rapports signal à bruit arbitrairement proches de zéro[13]. L'idée est donc de faire en sorte que le problème de réconciliation qui apparaît dans le protocole de distribution quantique de clés puisse se ramener à une question de codage de canal pour un canal bi-AWGN. Ceci est facile à réaliser si on utilise une modulation quaternaire dans l'espace des phases au lieu d'une modulation gaussienne. Aussi Alice va-t-elle maintenant envoyer des états cohérents centrés sur l'un des 4 points suivants de l'espace des phases : $(q_A, p_A) = (\pm A, \pm A)$. Bob procède ensuite comme dans le protocole habituel : il choisit de mesurer l'une ou l'autre des quadratures et obtient un résultat de mesure y. Bob informe Alice de son choix, et celle-ci détermine la valeur de x correspondante. Ainsi, la relation entre x et y est donnée par :

$$y = x + z, \tag{4}$$

où à une normalisation près, x est une variable de Bernoulli prenant les valeurs ± 1 avec probabilité $\frac{1}{2}$ et z est un bruit blanc gaussien de variance σ^2.

L'intérêt de ce schéma de modulation est que les problèmes de réconciliation directe, et de réconciliation inverse (où Bob envoie de l'information supplémentaire à Alice) sont identiques. Comme le problème de réconciliation directe est un problème classique et bien résolu en théorie de l'information, le problème inverse l'est également. Montrons maintenant que le problème de réconciliation inverse est également un problème de codage de canal avec une modulation binaire et un canal AWGN. Bob reçoit la variable y et définit les variables (u, t) de la façon suivante :

$$(u, t) \equiv (y/|y|, |y|). \tag{5}$$

Bob indique la valeur de t à Alice en utilisant le canal classique authentifié, et conserve la valeur de u qui correspond à la variable qu'Alice doit déterminer. Alice calcule alors la nouvelle variable v définie par

$$v \equiv t \cdot \text{signe}(x). \tag{6}$$

Il est facile de voir que v et u sont liés par

$$v = u + w \tag{7}$$

[13]Ici, le rapport signal à bruit est simplement défini comme le rapport de la variance de modulation du signal et de la variance du bruit.

où u est une variable de Bernoulli et w est un bruit blanc gaussien de variance σ^2. Ainsi, le problème de réconciliation inverse est identique au problème de réconciliation directe.

L'intérêt de la modulation binaire est que l'on peut facilement trouver de très bons codes correcteurs d'erreurs qui fonctionnent à très faible rapport signal à bruit. En effet, il suffit par exemple de considérer la concaténation d'un bon code correcteur d'erreur à bas rendement (par exemple, un code LDPC multi-edge) avec un simple code à répétition. Cette technique produit des codes presque optimaux à très faible rapport signal à bruit, qui sont en plus très facilement décodables.

En utilisant ce type de codes, on obtient un algorithme de réconciliation qui reste efficace pour des rapports signal à bruit arbitrairement faibles. Pour prouver que le protocole quaternaire surpasse le protocole à modulation gaussienne, il ne reste qu'à montrer que la sécurité du protocole n'est pas dégradée quand la modulation devient discrète au lieu de gaussienne.

Les preuves de sécurité des protocoles à variables continues sont basées sur des propriétés d'optimalité des états quantiques gaussiens. Pour cette raison, il est facile de prouver la sécurité du protocole de distribution quantique de clé basé sur une modulation gaussienne car ce protocole peut être interprété en termes d'états gaussiens. Ceci n'est a priori plus possible pour un protocole quaternaire. En revanche, si la modulation sur protocole quaternaire est suffisamment faible, cette modulation devient presque identique à une modulation gaussienne de même variance. Cela peut être précisé en termes d'états quantiques, et il existe ainsi un régime de variance où le protocole quaternaire peut distribuer des clés secrètes avec une sécurité identique à celle du protocole à modulation gaussienne.

Ainsi, à condition de travailler avec une variance de modulation suffisamment faible (ce qui est requis afin d'atteindre des distances importantes), on peut prouver la sécurité du protocole quaternaire, tout en disposant d'un algorithme de réconciliation efficace. La conjonction de ces deux éléments a pour conséquence que le protocole quaternaire permet de distribuer des clés secrètes sur des distances nettement plus importantes que le protocole gaussien initial. En particulier, des distances supérieures à la centaine de kilomètres sont possibles, à la condition de rester dans le régime asymptotique où l'on fait l'hypothèse que le canal gaussien qui lie Alice et Bob est parfaitement connu. Cette hypothèse est discutée dans le chapitre 7.

Partie III : Etude de la sécurité des protocoles à variables continues

Dans la troisième partie de ce manuscrit, on aborde plus spécifiquement l'étude de la sécurité des protocoles cryptographiques. En effet, un protocole quantique donné est caractérisé par deux éléments : sa performance d'une part, mais également sa sécurité. N'oublions pas que l'intérêt majeur de la cryptographie quantique par rapport à la cryptographie classique est justement que l'on peut prouver qu'un protocole donné est sûr, sans avoir besoin de recourir à des hypothèses sur la difficulté de tel ou tel problème mathématique.

De ce point de vue, le choix du plan de ce manuscrit peut sembler un peu incongru : pourquoi commencer par étudier les performances d'un protocole sans avoir d'abord établi qu'il était sûr ? La raison est historique et tient à la jeunesse du champ de recherche dédié à la cryptographie quantique. En fait, jusqu'à très récemment, aucun protocole n'était prouvé complètement sûr, la question se révélant être hautement non triviale. Pour pallier à ce problème, il était courant (et c'est toujours le cas aujourd'hui) de commencer à étudier la sécurité des protocoles face à des familles d'attaques restreintes, la famille la plus emblématique de ce point de vue étant celle des *attaques collectives*. Une attaque collective est telle que l'on peut supposer le canal quantique reliant Alice à Bob sans mémoire[14]. Faire l'hypothèse d'une attaque collective simplifie donc considérablement l'analyse théorique des protocoles. Par ailleurs, pour de nombreux protocoles, la meilleure attaque possible est souvent une attaque collective, prouvant ainsi que faire cette hypothèse n'est pas seulement pratique, mais également légitime. La sécurité des protocoles à variables continues étant pour des raisons (principalement) techniques, plus délicate à établir que celle des protocoles à variables discrètes, il apparaît naturel de faire dans un premier temps l'hypothèse d'attaques collectives et d'étudier leurs performances dans ce contexte. Ceci fait l'objet de la deuxième partie de ce manuscrit.

Dans la troisième partie, on adresse donc la question de la sécurité des protocoles de cryptographie quantique à variables continues, dans le cas le plus général.

Dans le chapitre 6, on cherche à déterminer si les attaques collectives sont optimales dans le cas des protocoles à variables continues. Un résultat récent de Renner et Cirac en 2009 prouve que c'est bien le cas dans le régime asymptotique, et fournit des bornes très conservatrices en régime non asymptotique. L'objet du chapitre 6 est de proposer une approche différente de celle de Renner et Cirac, qui pourrait aboutir à des bornes significativement meilleures en régime non asymptotique.

Le chapitre 7 est consacré justement aux effets de taille finie qui apparaissent dans n'importe quelle implémentation expérimentale d'un protocole de distribution quantique de clé. En particulier, le problème de l'estimation du canal (qui est supposé parfaitement connu en régime asymptotique) est étudié. Les résultats trouvés sont assez pessimistes

[14]Plus précisément, faire l'hypothèse d'une attaque collective signifie que l'état quantique ρ_{AB} à n modes partagé par Alice et Bob peut s'écrire sous la forme $\rho_{AB} = \int p(\sigma)\,\sigma^{\otimes n} \mathrm{d}\sigma$ où σ est un état bipartite et $p(\sigma)$ est une distribution de probabilité. Cet état est dit *identique et indépendamment distribué*.

mais sont en accord avec les résultats récemment obtenus dans la littérature pour les protocoles à variables discrètes. En particulier, les expériences actuelles, qui prennent rarement en compte ces effets de taille finie, sont souvent beaucoup trop optimistes dans les résultats qu'elles affichent.

Enfin, le chapitre 8 s'intéresse à des primitives cryptographiques quantiques autres que la distribution de clé. On adresse en particulier la question de la discernabilité des états cohérents, états qui constituent le support de l'information dans les protocoles de distribution quantique de clé à variables continues. Ensuite, on étudie la primitive qu'est la *mise en gage quantique* du point de vue des variables continues. La spécificité de la mise en gage est que c'est une primitive impossible à réaliser classiquement, mais également quantiquement (à la différence de la distribution de clé). Ici, on montre qu'elle reste impossible même si l'on restreint les participants à utiliser uniquement des états gaussiens et des opérations gaussiennes.

Chapitre 6 : Preuves de sécurité, les attaques collectives sont-elles optimales?

Dans le chapitre 6, on étudie les attaques les plus générales qu'un espion puisse effectuer contre un protocole de distribution quantique de clé à variables continues. Un des avantages de la cryptographie quantique est qu'une attaque peut être décrite, sans perte de généralité, par l'état quantique ρ_{AB} décrivant les systèmes d'Alice et Bob. Cet état appartient à l'espace de Hilbert $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n}$ correspondant à n produits tensoriels des espaces de Hilbert individuels $\mathcal{H}_A$ d'Alice et $\mathcal{H}_B$ de Bob. L'état d'Alice et Bob décrit complètement l'attaque de Eve car on peut toujours considérer que l'état d'Eve purifie l'état d'Alice et Bob, c'est-à-dire que $\rho_{AB} = \mathrm{tr}_E |\Psi_{ABE}\rangle$ où $|\Psi_{ABE}\rangle$ décrit le système joint d'Alice, Bob et Eve. Ainsi, l'état ρ_E de Eve est défini à une transformation unitaire près.

Etudier un état $\rho_{AB} \in (\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n}$ est en général simplement impossible car l'espace de Hilbert considéré est beaucoup trop gros. L'idéal de ce point de vue serait de pouvoir se ramener au cas d'une attaque collective car l'état quantique d'Alice et Bob prend alors la forme simple suivante $\int \mathrm{d}\sigma\, p(\sigma)\sigma^{\otimes n}$ où $\sigma \in \mathcal{H}_A \otimes \mathcal{H}_B$. Une telle réduction n'est pas toujours possible directement. La stratégie que l'on va donc adopter comprend deux étapes.

Dans un premier temps, on utilise un argument de symétrie pour simplifier l'état quantique qu'Alice et Bob ont besoin de considérer. Traditionnellement, l'argument est que le protocole de distribution quantique de clé est invariant si Alice et Bob réordonnent de façon coordonnée leurs n états quantiques respectifs (ceci est vrai pour la grande majorité des protocoles de cryptographie quantique, y compris pour les protocoles à variables continues). Ceci permet de montrer que l'état d'Alice et Bob peut toujours être supposé symétrique, c'est-à-dire invariant par rapport à n'importe quelle permutation de ses sous-systèmes[15]. L'intérêt de cette symétrisation est qu'elle réduit considérablement

[15]En fait, faire l'hypothèse d'un état symétrique peut juste amener Alice et Bob à sous-estimer leur taux secret réel, et à surestimer la puissance de l'espion.

la taille de l'espace à considérer : dans le cas où la dimension de $\mathcal{H}_A \otimes \mathcal{H}_B$ prend une valeur finie, la taille du sous-espace symétrique de $\mathcal{H}_A \otimes \mathcal{H}_B$ est polynomiale en n et non pas exponentielle. Malheureusement, si l'espace initial est de dimension infinie comme c'est la cas pour les protocoles à variables continues, la réduction apportée par cette symétrisation n'est pas aussi spectaculaire.

Dans un deuxième temps, on étudie les propriétés des états symétriques, et on essaie de montrer que ces états partagent beaucoup de propriétés avec les états indépendants et identiquement distribués (i.i.d.) qui correspondent à une attaque collective. Historiquement (depuis 2007 !), la technique employée dans ce but était la version exponentielle du théorème de de Finetti établie par Renner. Ce théorème montre qu'à condition de tracer un nombre négligeable de sous-systèmes, un état symétrique est très proche d'un état i.i.d.[16]. Cette technique donne des bornes particulièrement conservatrices sur le taux de clé finale (en particulier pour les protocoles à variables continues pour lesquelles une version spéciale du théorème a été établie en 2009 par Renner et Cirac). Une technique proposée plus récemment par Christandl, König et Renner, appelée technique de *post-sélection* permet de s'affranchir du théorème de de Finetti, et permet d'obtenir de meilleures bornes pour le taux secret. Cette technique est pour le moment limitée aux espaces de Hilbert de dimension finie et exclut donc le cas des protocoles à variables continues.

L'idée développée dans le chapitre 6 est que l'invariance par permutation n'est pas la symétrie la plus adaptée pour les protocoles à variables continues. Pour être plus précis, on va considérer un groupe de symétrie significativement plus gros, qui va conduire à une diminution plus importante de la taille de l'espace symétrique final qu'il sera nécessaire d'étudier. Pour cela, la remarque importante est que dans les protocoles à variables continues à modulation gaussienne, les données classiques $X, Y \in \mathbb{R}^n$ obtenues par Alice et Bob vérifient la relation suivante

$$Y = X + Z, \tag{8}$$

où Z est un vecteur i.i.d; gaussien centré. Le protocole à variables continues est par conséquent bien invariant par permutation de ses sous-systèmes car la loi jointe des vecteurs (X, Y) est invariante par permutation. Mais cette loi est également invariante sous l'action du groupe orthogonal. Plus précisément, pour toute transformation orthogonale $R \in O(n)$, la loi du couple (RX, RY) est la même que celle du couple (X, Y). Retranscrit au niveau des états quantiques, cela signifie que le protocole de distribution quantique est invariant si Alice et Bob appliquent tous les deux des opérations conjuguées dont l'action dans l'espace des phases est décrite par une transformation orthogonale.

L'étude de cette invariance est critique pour la sécurité de protocole à variables continues car elle correspond à la symétrie naturelle du protocole. Toutefois, nous n'avons pas encore été en mesure d'achever cette étude. Des résultats préliminaires intéressants ont toutefois été obtenus. En particulier, un théorème de de Finetti dans l'espace des phases a pu être prouvé. Ce théorème dit en substance que si un état quantique à n modes est invariant par transformation orthogonale dans l'espace des phases, alors en

[16] En fait un état i.i.d. sur la grande majorité de ses sous-systèmes.

traçant de plus en plus de modes, l'état devient de plus en plus proche d'un état thermique multimodal. Ce théorème constitue une généralisation quantique d'un résultat de Diaconis et Freedman qui dit que la distribution marginale des k premières coordonnées d'une distribution uniforme sur la sphère unité dans $\mathbb{R}^n$ devient normale quand n tend vers l'infini.

L'approche proposée au chapitre 6 n'a pas encore abouti à une preuve de sécurité pour les protocoles à variables continues pour la raison que les états bipartites qui respectent la symétrie décrite plus haut sont encore mal caractérisés. La façon naturelle d'obtenir une preuve consiste donc à caractériser ces états bipartites puis à leur appliquer une version adaptée à l'espace des phases de la technique de post-sélection de Christandl, König et Renner.

Chapitre 7 : Analyse des effets de taille finie dans la sécurité des protocoles de distribution quantique de clés

Dans le chapitre 7, on s'intéresse aux effets de taille finie, et à leurs conséquences en termes de sécurité. Jusqu'à très récemment, la sécurité des protocoles de distribution quantique de clé était étudiée le plus souvent dans le régime asymptotique. La principale hypothèse faite dans le cadre asymptotique est qu'Alice et Bob ont une connaissance parfaite du canal quantique. Dans sa thèse, Renner a développé un cadre théorique qui permet d'étudier les effets de taille finie. L'objet du chapitre 7 est d'appliquer ce cadre, initialement développé pour les protocoles à variables discrètes, aux protocoles de distribution quantique de clé à variables continues.

La première spécificité liée aux effets de taille finie est qu'une clé donnée n'est jamais complètement sûre. En fait, la sécurité d'une clé peut être caractérisée par un paramètre petit ϵ qui correspond à la probabilité que le protocole de distribution quantique n'ait pas fonctionné comme il devait : on parle alors d'une clé ϵ-sûre. *Grosso modo*, cela signifie que la clé distribuée par le protocole est complètement sûre, sauf avec une probabilité ϵ. Un ordre de grandeur possible pour ϵ est 10^{-10}.

En régime non-asymptotique, ϵ est la somme de quatre termes, qui sont liés à quatre effets distincts

$$\epsilon = \epsilon_{\mathrm{EC}} + \bar{\epsilon} + \epsilon_{\mathrm{PA}} + \epsilon_{\mathrm{PE}}. \tag{9}$$

On détaille maintenant la signification de chacun de ces termes.

Le premier terme ϵ_{EC} est lié à la correction d'erreurs (ou plutôt réconciliation dans le cas des variables continues). Il quantifie la probabilité qu'à l'issue de la réconciliation, Alice et Bob obtiennent des chaînes de bits différentes et qu'ils ne s'en aperçoivent pas. Dans un tel cas, ils poursuivent le protocole en procédant à l'amplification de confidentialité et le protocole aboutit à deux clés potentiellement secrètes, mais malheureusement différentes. Ce scénario correspond évidemment à un échec du protocole de distribution quantique de clé et doit donc être évité. La façon de remédier à ce problème est assez simple. A l'issue de l'étape de réconciliation, Alice et Bob choisissent une fonction de hachage et calculent l'image de leur chaîne de bits respective avec cette fonction. Ils comparent ensuite publiquement leur résultat. L'intérêt de cette méthode que les fonctions de

hachage ont la propriété d'amplifier les différences : si deux chaînes données ne diffèrent que d'un bit, avec grande probabilité, leurs images par une fonction de hachage seront très différentes. En particulier, la probabilité de ne pas détecter une différence entre les deux chaînes décroît exponentiellement avec la longueur de la fonction de hachage. La correction d'erreurs a un deuxième effet sur le taux secret final : l'efficacité de la réconciliation n'atteint en effet jamais la borne maximale prédite par la théorie de Shannon. Cet effet est loin d'être négligeable pour les protocoles à variables continues, et c'est pour le combattre que les stratégies présentées dans la partie II de ce manuscrit ont été développées.

Le deuxième terme, $\bar{\epsilon}$, correspond au fait que la "smooth min-entropy" (d'un état i.i.d.) qui caractérise la longueur de la clé n'est égale à l'entropie de von Neumann que dans la limite asymptotique. De même, le troisième terme ϵ_{PA} correspond à la probabilité d'échec de l'amplification de confidentialité. Ces deux termes ne sont pas des données observables pour un protocole donné, mais correspondent à des variables virtuelles, qu'il s'agit d'optimiser sous la contrainte imposée par l'équation 9, afin de maximiser le taux de clé secrète final.

Le dernier terme ϵ_{PE} correspond à la probabilité que l'estimation de paramètre échoue, et constitue de loin l'effet de taille finie avec les plus grandes conséquences en termes de diminution du taux de clé secrète par rapport au taux asymptotique. Pour être plus précis, dans le protocole de distribution quantique de clé à variables continues, deux paramètres doivent être estimés pour caractériser le canal quantique qui peut être supposé gaussien : la transmission du canal, et la variance du bruit ajouté par le canal. Ces deux grandeurs, que l'on peut supposer parfaitement connues dans le régime asymptotique, doivent en réalité être mesurées. La façon de procéder à cette estimation est la suivante : Alice et Bob échangent une nombre $N = n + m$ de signaux quantiques pendant le protocole. Parmi ces N signaux, m sont choisis aléatoirement et révélés publiquement, tandis que les n autres servent à extraire une clé secrète comme précédemment. On note déjà que le taux secret final est affecté d'un coefficient égal à n/N qui correspond au nombre de signaux utiles comparé au nombre de signaux échangés. Par ailleurs, les m paires de données dévoilées servent à construire deux estimateurs correspondant respectivement à la transmission et à la variance de bruit sur le canal. Ces estimateurs sont tels que l'on peut définir une région de confiance pour ce couple. On définit ainsi une région de confiance paramétrée par ϵ_{PE} qui signifie que la vraie valeur des deux estimateurs est située dans cette région, sauf avec une probabilité ϵ_{PE}. Ensuite, le taux de clé secrète est calculé en prenant les valeurs situées dans cette région qui *minimisent* le taux final. Ainsi est-on sûr que l'on considère bien la pire erreur statistique possible[17], compatible avec les m couples de données sacrifiées, sauf avec une probabilité ϵ_{PE}.

Notons ici que l'on se restreint aux attaques collectives. Pour certains protocoles très symétriques comme BB84, les attaques collectives sont optimales, même en régime non asymptotique. Dans le cas des protocoles à variables continues, le même résultat n'a pas été établi et est seulement conjecturé pour le moment. Quoi qu'il en soit, si on souhaitait prendre en compte les attaques les plus générales, il faudrait également ajouter un terme

[17] c'est-à-dire celle qui minimise la taille de la clé finale

correctif apporté par l'application du théorème de de Finetti établi par Renner et Cirac. Cette correction malheureusement conduirait à un scénario extrêmement pessimiste. Ce fait montre clairement l'importance que revêt l'étude des symétries spécifiques du protocole à variables continues suggérée au chapitre 6 car elle pourrait permettre d'améliorer significativement les bornes de sécurité pertinentes face à des attaques générales.

La prise en compte de ces différents effets conduit à un taux secret nettement plus pessimiste que le taux asymptotique généralement considéré. En particulier, le problème réside dans le fait que le nombre N de signaux qui doivent être échangés avant de pouvoir extraire une clé secrète est de plusieurs ordres de grandeurs supérieur à ce qui est habituellement mis en œuvre expérimentalement. Par exemple, pour un nombre de signaux échangés égal à un million, aucune clé secrète ne peut être distribuée, même avec un montage expérimental de grande qualité. Il semble qu'il faille des quantités de signaux de l'ordre du milliard pour atteindre la cinquantaine de kilomètres et de l'ordre de 10^{14} pour atteindre la centaine de kilomètres.

Dans ces conditions, les effets de taille finie, loin d'être négligeables, constituent à présent l'obstacle majeur pour le déploiement de la distribution quantique de clés à grande distance.

Chapitre 8 : Autres primitives cryptographiques quantiques à variables continues

Le dernier chapitre de ce manuscrit adresse des questions qui ne sont pas directement liées à la distribution quantique de clé à variables continues. En effet, les variables continues, avec leur technique de mesure spécifique qu'est la détection homodyne, peuvent être utilisées pour réaliser d'autres primitives cryptographiques que la distribution de clé. Dans le chapitre 8, on aborde deux problèmes distincts. Le premier problème est assez générique et s'intéresse à la discernabilité des états cohérents. En effet, deux états cohérents ne sont jamais orthogonaux et ne peuvent donc jamais être distingués de façon parfaite. On donne ici quelques bornes sur la probabilité d'erreur lorsque l'on cherche à distinguer parmi 2 ou 4 états cohérents. Ensuite, on introduit ce qui est probablement la primitive cryptographique la plus étudiée après la distribution de clé : la mise en gage. Bien entendu, on étudie ici la mise en gage quantique avec des variables continues, et on s'intéresse plus particulièrement au cas où les participants sont restreints à utiliser uniquement des états gaussiens et des opérations gaussiennes. On montre que dans ce cas, la mise en gage est interdite par les lois de la mécanique quantique.

L'idée à la base de la cryptographie quantique est qu'encoder de l'information sur des états quantiques non orthogonaux empêche un éventuel espion d'obtenir cette information sans laisser de traces. En effet, deux états non orthogonaux ne peuvent jamais être distingués parfaitement. Les états de prédilection pour la cryptographie à variables continues sont les états cohérents car ils sont extrêmement faciles à produire puisqu'ils correspondent simplement aux états générés par n'importe quel laser de bonne qualité. Les états cohérents, étant des états gaussiens, ne sont jamais orthogonaux entre eux.

Plus précisément, la *fidélité* de deux états cohérents $|\alpha\rangle$ et $|\beta\rangle$ ne s'annule jamais:

$$|\langle\alpha|\beta\rangle|^2 = e^{-|\alpha-\beta|^2} > 0. \tag{10}$$

Dans le cadre de la distribution quantique de clé, deux ensembles d'états gaussiens sont particulièrement intéressants : les ensembles $\mathcal{S}_2$ et $\mathcal{S}_4$ comprenant respectivement 2 et 4 états cohérents définis par

$$\mathcal{S}_2 = \{|\alpha\rangle, |-\alpha\rangle\}, \tag{11}$$
$$\mathcal{S}_4 = \{|\alpha\rangle, |i\,\alpha\rangle, |-\alpha\rangle, |-i\,\alpha\rangle\}, \tag{12}$$

où $\alpha > 0$. Le problème que l'on étudie au chapitre 8 est le suivant : pour l'un ou l'autre des deux ensembles $\mathcal{S}_2$ et $\mathcal{S}_4$, on génère aléatoirement l'un des états cohérents avec une probabilité uniforme, et on cherche à déterminer, de manière optimale, quel état a effectivement été généré. La notion d'optimalité peut être définie d'au moins deux façons distinctes suivant que l'on utilise une technique de discrimination ambiguë ou non-ambiguë. Une discrimination *non-ambiguë* signifie que pour chaque état, on applique un technique qui donne un résultat de mesure, quitte à se tromper. L'objectif est alors de minimiser cette probabilité d'erreur. Pour une discrimination *ambiguë*, en revanche, on interdit la possibilité d'une erreur, et on autorise en contrepartie le fait que la technique ne donne pas toujours de réponse. Ici, on considère le cas d'une discrimination non-ambiguë et on étudie deux types de mesures différents : la mesure optimale autorisée par la mécanique quantique, mesure qui donne la borne la plus générale, mais qui est souvent difficile à implémenter, et la mesure homodyne (ou hétérodyne) qui est simple à mettre en oeuvre, mais qui n'est pas optimale. Enfin, on considère dans les deux cas l'information mutuelle entre la source qui produit les états aléatoirement et le récepteur qui essaie de discriminer ces états de manière non-ambiguë.

Dans la deuxième partie du chapitre 8, on aborde un sujet très différent, celui de la mise en gage quantique. L'idée de la mise en gage est assez simple : Alice s'engage sur un certain bit vis-à-vis de Bob. L'image classique de cette primitive est la suivante : Alice écrit son bit[18] sur un morceau de papier, qu'elle place dans un coffre-fort. Elle remet ensuite ce coffre-fort à Bob sans lui donner la clé. Plus tard, quand Alice décide de révéler son bit, elle donne simplement la clé à Bob, qui peut donc prendre connaissance de la valeur du bit mis en gage par Alice. Deux caractéristiques sont attendues d'un bon protocole de mise en gage : Bob ne doit pas être en mesure d'obtenir de l'information sur le bit d'Alice avant que celle-ci ne le souhaite, et Alice ne doit pas pouvoir changer la valeur du bit sur lequel elle s'est engagée.

Classiquement, le problème de la mise en gage ne peut pas être résolu de manière parfaite : si Bob est dans l'incapacité d'ouvrir le coffre, cela signifie qu'Alice peut tricher. La différence notable avec la distribution de clé est que la mise en gage reste impossible dans un contexte quantique.

[18] En général, la mise en gage peut concerner n'importe quel type de message, mais par simplicité, on peut toujours se ramener au cas d'un bit, 0 ou 1.

En effet, un protocole de mise en gage quantique peut toujours être réduit au protocole suivant. Alice utilise deux états bipartites $|\Psi_0\rangle$ et $|\Psi_1\rangle$ pour encoder les bits respectifs 0 et 1. Dans la première phase du protocole, Alice remet à Bob la trace partielle de ces états, c'est-à-dire $\rho_0 = \mathrm{tr}_A |\Psi_0\rangle$ ou $\rho_1 = \mathrm{tr}_A |\Psi_1\rangle$. Dans la deuxième partie du protocole, quand Alice veut révéler la valeur de son bit, elle donne à Bob la seconde moitié de son état. Malheureusement, si on veut interdire à Bob de tricher, il ne doit pas pouvoir distinguer ρ_0 et ρ_1, ce qui signifie que les traces partielles des états $|\Psi_0\rangle$ et $|\Psi_1\rangle$ doivent être égales. Dans ce cas, il est possible de montrer qu'Alice peut agir localement sur la moitié de l'état qu'elle a conservé pour transformer à sa guise $|\Psi_0\rangle$ en $|\Psi_1\rangle$, et *vice versa*.

Le fait que la mise en gage quantique soit impossible de manière générale ne signifie pas qu'elle ne puisse pas devenir possible si l'on restreint astucieusement Alice et Bob. Un modèle possible est de supposer qu'Alice et Bob ne disposent que de mémoires quantiques bornées. Dans ce cas (très réaliste), on peut montrer qu'il est possible de faire de la mise en gage quantique. En fait, le fait d'avoir une mémoire quantique bornée force Alice ou Bob à faire une mesure qui l'empêche ensuite d'utiliser la technique de triche quantique.

Ici, on s'intéresse à la mise en gage quantique avec des variables continues, et une restriction naturelle dans ce cadre consiste à autoriser Alice et Bob à utiliser uniquement des états gaussiens et des états gaussiennes, ce qui correspond effectivement à ce qu'il est possible d'implémenter "facilement" dans un laboratoire. On montre toutefois que ces restrictions ne permettent pas de réaliser la mise en gage quantique. Plus précisément, si les états $|\Psi_0\rangle$ et $|\Psi_1\rangle$ sont gaussiens avec une trace partielle identique, il existe une transformation gaussienne locale qui permette à Alice de passer d'un état à l'autre.

Une conséquence intéressante de ce résultat est qu'elle fournit un contre-exemple à une conjecture formulée par Brassard et Fuchs qui espéraient que la mécanique quantique puisse être caractérisée de manière unique par le fait qu'elle permet la distribution de clé, mais interdit la mise en gage. Le résultat démontré au chapitre 8 montre que la mécanique quantique gaussienne, qui est un sous-ensemble strict de la mécanique quantique[19], vérifie ces mêmes propriétés.

[19] le fait que la mécanique quantique gaussienne soit strictement comprise dans la mécanique quantique résulte par exemple du fait qu'elle ne permet pas de violer les inégalités de Bell.

Introduction

The advent of Quantum Information Theory

Quantum Mechanics is a description of Nature that has been consistently tested and challenged for 100 years without ever being proven wrong. It describes very accurately[20] how Nature behaves at microscopic scales. However, despite its great success, it seems yet unachieved as it does not stand on clear physical principles, in contrast for instance with Special Relativity which can be derived from two very appealing principles: physics laws are the same in all inertial frames, and the velocity of light is identical in vacuum for all inertial frames. Quantum Mechanics, on the other hand, is presently based on a series of mathematical axioms whose physical significance is very unclear.

A challenging goal for physicists would certainly be to reformulate these axioms in more physical, and natural, terms. A possible way towards this ambitious objective is to study the connections between Quantum Mechanics and Information Theory. Information Theory was arguably discovered by Claude Shannon in the forties[21] and his seminal work [141] opened a new field of research that lead in particular to the society of information we live in today. This development was also made possible thanks to the technological possibilities offered by Quantum Mechanics without which the transistor, the integrated circuit or the laser for instance would not have been invented. In a sense, it is interesting to notice that our society of information and communication where the Internet or intercontinental communications seem obvious and where the planet has become a *small village* is a consequence of two scientific fields, Quantum Mechanics and Information Theory, working separately instead of combining their efforts. Indeed, Quan-

[20] the most famous example for its accuracy comes from quantum electrodynamics and is concerned with the value of the electron magnetic moment for which theoretical prediction and experimental precision agree with a precision of better than one part in a trillion [111].

[21] Although notions like entropy were familiar to physicists since the development of Statistical Mechanics, Shannon was the first to formalize the concept of information.

tum Mechanics was necessary to build the tools making all this possible and Information Theory tells us how to use these tools to achieve our goals, but the two theories certainly do not work hand in hand to give us their best!

What would it mean for Quantum Mechanics and Information Theory to work together? Quite astonishingly, Quantum Mechanics was already well established when the field of Information Theory took off fifty years ago. Therefore, it could (and maybe should) have been obvious back then that the ultimate support of information was necessary quantum and not classical. Unfortunately, this thought only came to scientists much later, in the early seventies, when Stephen Wiesner suggested a method to make money unforgeable by using properties of Quantum Mechanics. At that time (and still now quite frankly), the idea appeared quite impractical and did not catch the attention of the scientific world[22]. A second attempt was made a few years later by Charles Bennett and Gilles Brassard who introduced quantum protocols for two cryptographic primitives: the distribution of secret keys among distant parties and bit commitment. Although their paper also encountered difficulties to get published[23], it became the seminal paper that gave birth to the now very prolific field of Quantum Cryptography [10].

Quantum Cryptography, and particularly its most emblematic primitive, Quantum Key Distribution, is now the first real application of the combined efforts of Quantum Mechanics and Information Theory working hand in hand. For more than twenty years, the new field of *Quantum Information* has been expanding quite rapidly. The goal of this new scientific field is ambitious: it is to determine the fundamental limits Nature imposes concerning the storage of information, the rate at which communication can be performed between distant parties and also the ultimate limits on computation capabilities. The first two questions concern the subfield of *Quantum Information and Communication*, whereas the third question is emblematic of the younger *Quantum Information Processing* subfield[24]. Apart from being raising arguably very interesting questions, Quantum Information appears as a possible way towards finding the Physical grounds for Quantum Mechanics that scientists are still desperately looking for at the beginning of the twenty-first century. Indeed, many proposals have been made along this path. For instance, a conjecture made by Fuchs and Brassard suggests that the following two principles are sufficient to rederive Quantum Mechanics: Nature allows Key Distribution but Nature forbids Bit commitment.

The field of Quantum Information is still very young and exciting developments occur with a much more rapid pace than in other more established research fields[25]. Moreover,

[22] it actually took more than 10 years for the work of Wiesner to get published [156].

[23] it finally appeared in an obscure conference in India where the authors were invited and could submit their unorthodox results.

[24] the real groundbreaking result that stirred the interest of scientists for Quantum Computing was the unexpected polynomial algorithm for factoring integers [142] that clearly showed that a quantum computer was apparently strictly more powerful than a classical computer, thus apparently violating the celebrated Church-Turing thesis stating that all computation model are equivalent. However, before Shor's algorithm, the possible computational power of a quantum computer had already been touched upon in a visionary paper of Feynman [46].

[25] Among the recent surprising new developments of Quantum Information, one can certainly think of the various additivity conjectures for capacities of Quantum Channels that were proven wrong in 2008

not only is the theoretical effort really impressive in the field, but experimenters also play a major role. Indeed, the achievements of experiments in Quantum Optics for instance are truly amazing: one can literally create and observe Schrödinger cats [115, 114], witness the birth and death of a photon [55], developments that would certainly have seen as impossible by the fathers of Quantum Mechanics[26]. There is also reasonable hope to expect that Quantum computers will exist in the next few decades. At least, since the invention of Quantum Error Correcting Codes [22] and the threshold theorem [121], there does not seem to be any fundamental reason forbidding the existence of Quantum computers. This gives hope that we are only at the beginning of Quantum Information Theory and that much, much more is yet to be discovered.

Quantum key distribution

Cryptography has for main objective to make secure communication possible between distant parties. Let us call these two parties without originality Alice and Bob, and let us assume that they want to communicate secretly, even in the presence of a potential eavesdropper that we shall name Eve. To achieve their goal, Alice and Bob will use keys to encrypt and decrypt their messages. There are basically two types of cryptographic protocols: *symmetric* cryptography where the *encryption* key is identical to the *decryption* key and *asymmetric* cryptography both keys differ. Only symmetric cryptography can be proven *unconditionally secure* meaning that the eavesdropper cannot learn anything about the message except with an exponentially small probability. This means in particular that no assumption needs being made concerning the capabilities of Eve. This is in sharp contrast with the situation of asymmetric cryptography for which security relies on the fact that there exist one-way functions, that is functions are are easy to compute but hard to invert[27]. The security of symmetric schemes, on the other hand, is easy to establish: as soon as the key shared by Alice and Bob is secret, Alice can simply compress her message and XOR it with the key. She then sends the result to Bob who XOR it again with the key to recover the compressed message. This is the so-called *one-time pad*. A simple entropic argument shows that Eve cannot learn anything concerning the message from the ciphered text. Unfortunately, there is a catch to this too simple protocol: how can Alice and Bob proceed to share a secret key in the first place? This is the problem of the *distribution of secret key*. While there are different classical ways to realize this task, none is completely satisfying. This is where Quantum Key Distribution enters the game: Quantum Mechanics indeed provides an unexpected but elegant solution to the problem of key distribution. It is indeed possible for Alice and Bob to perform a protocol that allows them to share an unconditionally secure key [136].

[66, 147]!

[26] indeed, the question whether Schrödinger cats could really happen in Nature or if they were only a Gedanken Experiment was not fully resolved by the time the mathematical foundations of Quantum Mechanics were established.

[27] the most emblematic asymmetric protocol is certainly the scheme introduced by Rivest, Shamir and Adleman RSA which bases its security on the assumption that factoring integers is hard [133].

For a more detailed discussion on the advantages on QKD over classical schemes, the interested reader is encouraged to consult the SECOQC White Paper and the references therein [5].

Even if QKD is arguably a very interesting solution to the problem of key distribution for symmetric cryptography, the question of whether QKD has a bright future in terms of being implemented on a large scale is not yet solved. A positive answer will certainly not come before standardization and certification efforts are made by the proponents of QKD. In particular, the crucial problem of the unavoidable discrepancies between theoretical models and technological implementations of QKD has to be addressed. Obviously, theoretical models include already an accurate description of the quantum channel between the two protagonists Alice and Bob, but still fail to take into account all implementation imperfections. Those can be coined by the generic name of *side channels*. A spectacular result in this direction, however, has recently been obtained by Antonio Acín and collaborators [2, 1, 119] where they prove the security of a device-independent QKD protocol. Hence, apart if the classical memories of Alice and Bob leak information to a potential eavesdropper[28], their protocol is actually resistant to completely faulty implementations. The bottleneck of the protocol is that key distribution can only be achieved if Alice and Bob are able to perform a loophole-free Bell test, which, is still out of reach today (but seems possible in a foreseeable future). Anyway, the fact that such a protocol exists is truly intriguing development which generalizes the idea of Artur Ekert who proved that QKD could be performed even if the source of entangled particles was in the possession of the eavesdropper [43]. The result by Acín and collaborators goes one step further: not only can Eve distribute the photons, but she can also sell their equipment to Alice and Bob! Quantum Key Distribution is therefore possible in principle even if you purchase your equipment from an evil company!

For experts of the field, the result by Acín and coworkers was not a shocking revelation: indeed it is intuitively clear that if Alice and Bob can violate Bell's inequalities (in a loophole-free manner), then their quantum states must be entangled in such a way that they almost completely factorize from the environment, that is, from any eavesdropper. The real *tour de force* was to be able to compute a bound on the accessible information for an eavesdropper depending on a parameter stating measuring the violation of Bell's inequality. This is actually the recurring problem of QKD: being able to relate the correlations between Alice and Bob's data to the amount of information an eavesdropper can acquire. This task appears tantamount as one needs to consider every possible eavesdropping strategy allowed by Nature (that is, not forbidden by Quantum Mechanics). The difficulty of this problem explains why most QKD protocols studied today are very simple, in the sense that they display a lot of symmetries for instance. An interesting feature is that the most simple protocols also seem to be very competitive both in terms of secret key rate and distance over which the distribution of secret key is possible.

The device-independent QKD proposal is one way to answer to the problem of side channels. Unfortunately, however elegant, one must admits that it is far from being a very practical solution, especially compared with the current level of technological

[28] in which case no secret communication can ever be expected ...

implementations of QKD protocols which, it turns out, are not that complicated. The first demonstration was performed in IBM labs in 1989[29] and complete systems can already be bought today for less than 100 000 euro. This is not so bad as the perspectives of getting any useful quantum computer for that price are far out of reach at present time. If the device-independent protocol is not a practical solution against side channels, what is? Well, one can proceed the other way around: instead of first considering all possible side channels as in the case of a loophole-free Bell test, one can list all possible side channels, and start addressing each of them, one by one. No need to say that this solution appears far less appealing than the elegant device-independent proposal, but it is fair to say that this is a much more realistic option, and that this work has to be carried out as comprehensively as possible before QKD can really reach the market and appear as a viable alternative to classical cryptography.

In this thesis, we do not consider the study of side channels. Indeed, our primary focus is an alternative to the historical QKD protocols such as BB84 and is called *continuous-variable QKD*. This alternative proposal which basically gets rid of single photon counters is quite recent. The idea of encoding information on the continuous variables of the Electro-Magnetic field has been introduced by Tim Ralph in 2000 [122] and the first realistic proposals involving using coherent states along with homodyne detection were developed in 2002 [64, 144]. Because of this very young age, continuous-variable (CV) QKD is not as well established as its discrete-variable (DV) counterpart. In particular, at the beginning of my thesis in September 2006, it was not clear what the good CV QKD protocols were to achieve long-distance, and security proofs were not complete. The goal of this thesis is to address these questions.

Outline of the thesis

The manuscript is divided into three parts. The first part introduces the material which is necessary to understand quantum key distribution with continuous variables. The second part deals with the problem of the range of continuous-variable quantum key distribution, and gives solutions to improve it significantly. The third part finally discusses the security of quantum cryptography with continuous variables.

Part I: From Quantum information to Quantum Key Distribution

Chapter 1: Quantum information and communication. In Chapter 1, we introduce the field of quantum information theory. We first give a quick overview of Quantum Mechanics whose difficulty lies more in its counter-intuitive predictions than in its formalism which is surprisingly quite simple. Then we present the basics of classical information theory and concentrate on the definitions and properties of relevant quantities such as entropy and mutual information. We finally end Chapter 1 by explaining how the concepts

[29] it is interesting to note that this first demonstration was burdened with obvious side channels. In particular, Alice's modulator made a different noise for the two encoding bases. The key distribution was therefore theoretically secure only against deaf eavesdroppers!

of entropy and mutual information are generalized to the quantum setting.

Chapter 2: Quantum information with continuous variables. In Chapter 2, we focus on the use of continuous variables for quantum information theory. The main interest of continuous variables is that the relevant quantum states can be produced and measured experimentally with quantum optics techniques. In particular, the states that are relevant for our purpose in this thesis, that is continuous-variable QKD, are very easy to produce: they are simply the coherent states that any good laser will output, and can be measured with a high efficiency thanks to an interferometric detection technique called *homodyne detection*. In Chapter 2, we introduce the formalism for the study of continuous variables in phase space. A notable feature of continuous variables is that, whereas being poorly suited for classical information theory[30], they are actually well-defined in the quantum setting where the Hilbert spaces have an infinite but countable dimension.

Chapter 3: Quantum Key Distribution. In Chapter 3, we finally present quantum key distribution. We first discuss the notion of security for a QKD protocol. We also detail the general structure of a typical QKD protocol before explaining how most security proofs are derived. An important concept from this point of view is *virtual entanglement*, which is used to prove the security of a given protocol by studying an equivalent entangled protocol. Then, we introduce continuous-variable QKD protocols as well as their security proof against the restricted class of attacks called *collective attacks*. This proof is specific to continuous-variable protocols and is based on the extremality of Gaussian states.

Part II: Increase the range of continuous-variable QKD

At the beginning of my thesis in 2006, CV QKD did not yet appear as a true alternative to DV QKD protocols. Of course, the theoretical key rates at short distances were quite high, but the main problem was that CV QKD seemed limited to short distances: back then, it could not distribute secret keys beyond 30 km with state of the art technology, a quite modest distance compared to more than 100 km (and now close to 200 km) for DV QKD protocols. The main objective of my thesis was to address this specific question. In 2006 already, the reason why CV QKD had such a limited range was well identified: the answer lied in the classical post-processing of Alice and Bob's data. It indeed turned out that continuous variables were much more difficult to handle than the classical bits one got in DV QKD protocols. The so-called *reconciliation* algorithms were then limiting both the range and the speed of CV QKD protocols! Unfortunately, at that time already, the best classical error correcting codes (LDPC codes) where used for this reconciliation procedure and there was not much hope one could do much better...

Chapter 4: Reconciliation of correlated Gaussian random variables. In the first part of my doctoral work, I worked on the problem of the reconciliation of correlated Gaussian

[30] where the entropy of a continuous variable needs to be replaced by the notion of *differential entropies* which can take negative values...

random variables. This study is described in Chapter 4 of this thesis. The problem can be stated quite easily and is in fact very interesting from a purely mathematical point of view. Alice and Bob are given correlated Gaussian random variables: for instance, Alice has a vector $\mathbf{x} = (x_1, x_2, \cdots, x_n)$ where the x_i are independent and identically distributed (i.i.d.) normal variables: $x_i \sim \mathcal{N}(0, 1)$ and Bob is given the vector $\mathbf{y} = (y_1, y_2, \cdots, y_n)$ where $y_i = x_i + z_i$ with the variables z_i being also i.i.d. Gaussian variables with a variance σ^2: $z_i \sim \mathcal{N}(0, \sigma^2)$. Their goal is then, through a one-way reconciliation (where only Alice is authorized to send classical information to Bob[31]) to extract a common bit string U, as long as possible, with the constraint that the classical communication should not reveal any information about U to a potential eavesdropper. In Chapter 4, we give an explicit solution for this problem and prove its optimality for the relevant range of parameters (that is $\sigma \geq 1$). This solution is quite effective since the new reconciliation algorithm allows to distribute secret key over 50 km instead of the previous 30 km, without any change in the hardware implementation and without any increase of the complexity of the reconciliation algorithm. Therefore this new scheme greatly enhances the performance of CV QKD, improving the range of the protocol without any added complexity.

Chapter 5: Long distance CVQKD: protocols with a discrete modulation. Unfortunately, the algorithm presented in Chapter 4 is not a completely satisfying answer to the problem of the limited range of CV QKD. It arguably improves the situation, but the latter remains desperately less brilliant than for DV QKD protocols which do not seem to be affected at all by reconciliation (or error correction) problems. In Chapter 5, we address this question by proposing a new CV QKD protocol for which the reconciliation problem can be solved efficiently and is not a obstacle anymore to the perspective of long distance distribution of secret keys. The main feature of the new protocol is that the modulation scheme involves now only a finite number of possible states (either two or four states) instead of the previous Gaussian modulation. The new modulation scheme is actually designed on purpose to solve the problem of reconciliation and manages to do so quite efficiently. However, this is only one half of the problem. Indeed, as for any other new QKD protocol, one must prove its security or it will be soon forgotten. The problem was that previous security proofs for CV QKD were explicitly requiring a Gaussian modulation. A new approach was therefore required here. A method for proving the security of discrete-modulation against the so-called *collective* attacks, which are thought to be optimal, is given in Chapter 5 and a lower bound on the secret key rate is derived. The performances of the protocols are then analyzed. The protocols introduced turn out to be able to perform QKD over large distances comparable to DV QKD protocols. This puts at rest the question of whether CV QKD is intrinsically restricted to short distances: the short answer is "No!"

[31] Actually, the situation of interest is when only Bob can send information to Alice, but in the case of a Gaussian modulation, both problems are equivalent.

Part III: Security of continuous-variable quantum cryptography

As we mentioned before, the task of analyzing the security of any QKD protocol might appear quite daunting because of the size of the space of possibilities for the attacks of an eavesdropper. Fortunately, a general framework for the study of the security of QKD was recently developed by Renato Renner [124]. This framework provides a way to prove the security of QKD against general attacks. This framework, however, is mainly concerned with finite dimensions, that is, discrete-variable QKD and the techniques developed by Renner cannot be directly applied to CV QKD which is described with an infinite-dimensional Hilbert space. Moreover, even in the case of collective attacks[32], there are a number of subtleties that need to be taken into account, the main one being finite size effects. Again, a framework for their study was recently developed by Valerio Scarani and Renato Renner [137]. However, they again only focus on DV protocols and it turns out that one more time, CV QKD presents some specificities that makes the problem less easy. Finally, although we essentially considered QKD until now, it should be noted that QKD is by no means the only quantum cryptographic primitive. An other very important primitive is bit commitment, which is remarkable because it is forbidden both in the classical and in the quantum frameworks.

Chapter 6: Are collective attacks optimal? As we said, there now exists a framework to establish the unconditional security of QKD protocols. Among the nice features of this framework is the use of a theorem, de Finetti's theorem, which proves that collective attacks are asymptotically optimal [125]. Therefore one only needs proving the security of a QKD protocol against collective attacks. This is rather fortunate as these attacks are much more restricted and easy to analyze than general attacks. Unfortunately, de Finetti's theorem explicitly depends on the dimension of the Hilbert space used to describe the protocol, and, as a consequence, it cannot apply directly to continuous-variable protocols. Recently Renner and Cirac [127] found a way to generalize de Finetti's theorem to make it work for reasonable CV QKD protocols. Their proof, however, do not exploit all the symmetry properties of CV QKD, and one can hope that tighter bounds could be obtained in the non-asymptotic regime.

The goal of chapter 6 is to study the symmetries of CV QKD protocols and to suggest approaches that would take advantage of them. For instance, it is worth noting that the security proof for the BB84 protocol does not require advanced tools such as the exponential de Finetti theorem: considerations of symmetry are indeed sufficient to establish the security of the protocol against general attacks. In some sense, CV QKD also appears as a very symmetric protocol in phase space and one might hope that symmetry considerations can be used in a more intensive way than in the approach by Renner and Cirac to prove the security of the protocol.

[32]There are generally three types of attack considered in Quantum Key Distribution: general (or coherent) attacks, collective attacks and individual attacks (see [53] and references therein for a detailed description of the different attacks). Collective attacks turn out to be optimal (that is the best possible attack for an eavesdropper) in the asymptotic setting for most QKD protocols.

This line of research, involving specific symmetries in phase space, has not be completely successful yet as it has not lead to a new complete proof of security of CV QKD protocols against general attacks, but partial results have already been established. This is the case of a new de Finetti-type result considering *orthogonally invariant* states in phase space.

Chapter 7: Finite size analysis. Until very recently, security of QKD was mainly studied in the asymptotic regime where Alice and Bob exchange an infinite number of quantum states and one is interested in the secret key rate. Reality, however, is quite different: Alice and Bob only exchange a finite number N of quantum signals, and the question is to determine the length of the secret key that can be distilled from these N quantum signals. Various finite size effects need to be taken into account, that all lead to deviations from the asymptotic key rate.

Without any doubt, the most crucial finite size effect is the imperfect parameter estimation. Whereas in the asymptotic regime, Alice and Bob are assumed to know perfectly the quantum channel, this is not true anymore in a real experiment. This turns out to be quite problematic, especially for continuous-variable protocols, and leads to very pessimistic results. In particular, most experimental implementations today use a number N of quantum signals which is incompatible with unconditional security in a finite size context.

Chapter 8: Other continuous-variable cryptographic primitives. The primary focus of this thesis is Quantum Key Distribution. However, it is important to note that QKD is not the only cryptographic primitive of interest in the Quantum world.

In Chapter 8, we first study the question of the distinguishability of coherent states. This is a rather general problem which is interesting for most quantum cryptographic primitives with continuous variables since coherent states are by far the most practical support of information in this context.

Then we study quantum bit commitment, for which a no-go theorem was established [103, 96]. More exactly, quantum bit commitment is impossible if the participants are only restricted by the laws of quantum mechanics. However, it does not mean that there cannot exist any secure protocol if one puts stronger restrictions on the capabilities of the different players. In Chapter 8, we prove that the no-go theorem for bit commitment still holds for continuous-variable protocols where both players are restricted to Gaussian states and operations.

Part I

From Quantum information to Quantum Key Distribution

CHAPTER 1

Quantum information and communication

The goal of this chapter is to present the main tools of Quantum Mechanics and Information Theory that will be useful for the study of quantum key distribution (QKD). The reader already familiar with the topic of quantum information may skip the first part of this chapter. Note, however, that if most of the content of this chapter can be found already in Nielsen and Chuang's textbook [109], the very last section 1.3.3 dealing with operational entropic quantities introduces more recent concepts which play an important role for proving the security of QKD against general attacks.

1.1 A rapid presentation of Quantum Mechanics

The object of this section is certainly not to give a comprehensive description of Quantum Mechanics as one would really have a hard time summarizing it in a single book. However, for our purpose, this is not at all a problem, as we only need to know the postulates of the theory to be able to talk sensibly about quantum information theory and its application to QKD. Note that is true because we mainly focus on the theoretical aspects of QKD in

this thesis, and not too much on its implementation. In the same spirit, the knowledge of Quantum Mechanics required to investigate the power of quantum computation is rather limited, and a good grasp on the axioms of the theory is practically sufficient to achieve this goal. This is obviously not the case anymore if one wants to be able to physically build a quantum computer or even only consider possible implementations of such a computer: in this case, one needs a very deep (and broad) understanding of the physics involved. This low barrier to entry explains why the relatively young field of *quantum information and computation* has attracted not only physicists but also many mathematicians and computer scientists in the recent years.

The axioms of Quantum Mechanics really define a mathematical framework. They give the playground that can be used to describe physical phenomena, but, by themselves, they do not provide a complete description of Nature. This would require additional theories such as the celebrated Quantum ElectroDynamics (QED) which has displayed tremendous success in the description of the interaction between light and matter. Again, it is important to distinguish between the axioms of Quantum Mechanics that are simply a mathematical framework and the effective Physical theories that allow to understand Physical phenomena.

The axioms of Quantum Mechanics aim at answering two basic questions: what is the general description of a physical (quantum) system, and how does this system evolve with time?

1.1.1 Description of a quantum physical system.

The first postulate of Quantum Mechanics gives the mathematical structure relevant for the description of a physical system.

Postulate 1. Associated to any isolated physical system is a Hilbert space (*i.e.* a complex vector space with inner product) known as the *state space* of the system. The system is completely described by its *state vector*, which is a unit vector in the system state's space[1].

Following the Dirac bra-ket notation, we refer to a state vector with the *ket* $|\psi\rangle$, while its transpose is described by the *bra* $\langle\psi|$. The inner product between state vectors $|\psi\rangle$ and $|\phi\rangle$ is $\langle\psi|\phi\rangle$ and the normalization condition reads $\langle\psi|\psi\rangle = 1$.

An alternative description of the first postulate is *the superposition principle*: if $|\psi\rangle$ and $|\phi\rangle$ are two states, any superposition $\alpha|\psi\rangle + \beta|\phi\rangle$ (such that $|\alpha|^2 + |\beta|^2 = 1$) is a legitimate state authorized by Quantum Mechanics. Even if any superposition is allowed in principle[2], some can be very fragile and are never observed in Nature. This is the case

[1] More exactly, a state is a *ray* in a Hilbert space, that is, an equivalence class of vectors that differ by multiplication by a nonzero complex scalar. We usually choose a representative of a particular class to have unit norm. Two vectors differing by a global phase describe the same physical system.

[2] although some physicists argue that the superposition principle should not be taken too literally, and that the superposition principle might fail for macroscopic systems. Up until now, however, the superposition principle has never been experimentally falsified. For instance, photonic kittens, which are

of Schrodinger's cat which is in the superposition of the state $|\text{alive}\rangle$ and the state $|\text{dead}\rangle$.

The second postulate aims at describing a composite system.

Postulate 2. The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n, and system i is prepared in the state $|\psi_i\rangle$, then the joint state of the total system is $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$.

Let us now apply this second postulate to the case of a bipartite state. If the individual systems are described by the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, the Hilbert space $\mathcal{H}_{AB}$ of interest for the bipartite quantum system is the *tensor product* of $\mathcal{H}_A$ and $\mathcal{H}_B$:

$$\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B. \tag{1.1}$$

In particular, if $\mathcal{B}_A = \{u_1, u_2, \cdots\}$ and $\mathcal{B}_B = \{v_1, v_2, \cdots\}$ are respectively orthogonal bases for $\mathcal{H}_A$ and $\mathcal{H}_B$, then an orthogonal basis for $\mathcal{H}_{AB}$ is given by $\mathcal{B}_{AB} = \{u_1 \otimes v_1, u_1 \otimes v_2, \cdots, u_1 \otimes v_n, \cdots, u_2 \otimes v_1, u_2 \otimes v_2, \cdots, u_m \otimes v_n, \cdots\}$. If both $\mathcal{H}_A$ and $\mathcal{H}_B$ are finite-dimensional Hilbert spaces with respective dimensions d_A and d_B, the tensor product $\mathcal{H}_{AB}$ is finite-dimensional with dimension $d_{AB} = d_A\, d_B$.

From this tensor structure, and a simple dimension analysis, one can infer that all physical systems cannot be described by vectors, that is, pure states. Indeed if the subsystems A and B could always be described by state vectors $|\psi\rangle_A \in \mathcal{H}_A$ and $|\phi\rangle_B \in \mathcal{H}_B$, then the bipartite system could always be described by elements of the set $\text{Sep}_{AB} = \{|\psi\rangle_A \otimes |\phi\rangle_B : |\psi\rangle_A \in \mathcal{H}_A, |\phi\rangle_B \in \mathcal{H}_B\}$ whose dimension is only $d_A + d_B \leq d_A d_B$ (for $d_A, d_B \geq 2$). In fact, Sep_{AB} corresponds to the set of *separable states*. Any state of $\mathcal{H}_{AB}$ that does not belong to Sep_{AB} is called an *entangled state*, meaning that its subsystems A and B cannot be considered separately.

In the case of a bipartite state $|\psi\rangle_{AB}$, the description of the system A (resp. B) is given by the *partial trace* of $|\psi\rangle_{AB}$ over the Hilbert space $\mathcal{H}_B$ (resp. $\mathcal{H}_A$), that is the trace-one nonnegative operator:

$$\rho_A = \text{tr}_B |\psi\rangle\langle\psi|_{AB} \quad \text{and} \quad \rho_B = \text{tr}_A |\psi\rangle\langle\psi|_{AB}. \tag{1.2}$$

If $|\psi\rangle_{AB} = \sum_{i,j} \lambda_{i,j} |u_i\rangle_A \otimes |v_j\rangle_B$, the partial trace over B is given by:

$$\begin{aligned}
\rho_A &= \text{tr}_B |\psi\rangle\langle\psi|_{AB} && (1.3)\\
&= \text{tr}_B \sum_{i,j,k,l} \lambda_{i,j} \lambda^*_{k,l} |u_i\rangle\langle u_k|_A \otimes |v_j\rangle\langle v_l|_B && (1.4)\\
&= \sum_{i,j,k,l} \lambda_{i,j} \lambda^*_{k,l} |u_i\rangle\langle u_k|_A \otimes \langle v_j|v_l\rangle && (1.5)\\
&= \sum_{i,j,k} \lambda_{i,j} \lambda^*_{k,j} |u_i\rangle\langle u_k|_A \quad \text{if} \quad \langle v_j|v_l\rangle = \delta_{j,l} && (1.6)
\end{aligned}$$

very small Schrödinger cats, have already been experimentally demonstrated [115].

Such an operator ρ is referred to as a *mixed state* by opposition to the rank-one *pure state* $|\psi\rangle\langle\psi|$. We note $\mathcal{S}(\mathcal{H})$ the set of trace-one nonnegative operators on the Hilbert space $\mathcal{H}$. The partial trace over a subsystem of a pure entangled state is a genuine mixed state, meaning that it cannot be intrinsically described by any pure state. An apparently different kind of mixed states corresponds to the case where only *partial information* about the state is available. For instance, consider a source generating randomly either the state $|\psi\rangle$ with probability p or the state $|\phi\rangle$ with probability $1-p$. The correct description ρ of the *random* state generated by the source is a mixture of both pure states: $\rho = p|\psi\rangle\langle\psi| + (1-p)|\phi\rangle\langle\phi|$.

Therefore it seems as if there were two kinds of mixed states: the ones obtained by taking the partial trace of a pure multipartite quantum state, and the ones due to an incomplete knowledge about the state. In fact, the concept of *purification* shows that this distinction is only apparent. For any mixed state ρ_A in a Hilbert space $\mathcal{H}_A$, one can define a reference system R and a Hilbert space $\mathcal{H}_R$ (isomorphic to $\mathcal{H}_A$) such that there exists a pure state $|\psi\rangle_{AR}$ verifying $\rho_A = \mathrm{tr}_R|\psi\rangle\langle\psi|_{AR}$. The state $|\psi\rangle_{AR}$ is called a *purification* of ρ_A.

1.1.2 Evolution of a physical system

The first two postulates of Quantum Mechanics described the mathematical framework of the theory. The last two are concerned with the dynamics of quantum states: how do they evolve with time and what is the effect of a measurement? What is surprising is that two distinct postulates are required to answer these questions whereas a measurement could legitimately be seen as a regular evolution of a quantum system[3] . The special status of the measurement process among all the temporal evolutions is referred to as the *measurement problem* and partly explains why physicists have been looking for higher-level interpretations of Quantum Mechanics, hoping to get rid of this need for two distinct axioms governing the dynamics of pure quantum systems.

The third postulate we introduce describes the *normal* evolution of a quantum system, in contrast with a measurement process.

Postulate 3. The evolution of a closed quantum system is described by a unitary transformation, that is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2,

$$|\psi'\rangle = U|\psi\rangle. \tag{1.7}$$

Note that Quantum Mechanics does not a priori give the form of the unitary U. An alternate formulation of this postulate is the Schrödinger equation which states that the

[3]It should be noted that this need for two distinct postulates is true in the Copenhagen interpretation of Quantum Mechanics discussed here. Other interpretations such as the *Many-Worlds interpretation* introduced by Hugh Everett are explicitly based on the idea that the wavefunction collapse should be abandoned [45]. Unfortunately, this comes at a rather high price, namely, accepting the existence of an infinity of parallel universes!

state vector temporal evolution is governed by:

$$i\hbar\frac{\mathrm{d}|\psi\rangle}{\mathrm{d}t} = H|\psi\rangle, \tag{1.8}$$

where H is the Hamiltonian of the system. Both equations are in fact equivalent and their respective advantage depends on whether one is actually interested in the physical process involved or not.

The fourth and last postulate gives a description of the measurement process.

Postulate 4. Quantum measurements are defined by a collection $\{M_n\}$ of *measurement operators*. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\psi\rangle$ immediately before the measurement, then the probability $p(m)$ that the result m occurs is given by

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle, \tag{1.9}$$

and the state of the system after the measurement is

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}. \tag{1.10}$$

The measurement operators satisfy the *completeness equation*

$$\sum_m M_n^\dagger M_n = \mathbb{1}. \tag{1.11}$$

The measurement process is really where the Quantum weirdness crystallizes. The other postulates describe a totally deterministic theory where states evolve under a deterministic and reversible (unitary) evolution. As soon as a measurement is involved, both these properties appear to be lost: the evolution becomes intrinsically probabilistic and non-reversible. The probabilistic aspect is clear from the statement of the postulate: Quantum Mechanics can only predict probabilities, and not which outcome will actually be observed (except in the case where there is an outcome of probability 1!). The fact that a measurement makes the evolution non-reversible is a simple consequence that the information of what the state was prior to the measurement is definitely lost. If one starts with a state $|\psi\rangle$ in a random superposition of $|0\rangle$ and $1\rangle$, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and measures it in the basis $\{|0\rangle, |1\rangle\}$, then the measurement will yield either 0 or 1 but all information concerning α and β will be lost, except that $\alpha \neq 0$ (resp. $\beta \neq 0$) if the outcome is 0 (resp. 1)[4].

[4]However, one must be careful when talking of a non-deterministic theory as the Many Worlds interpretation for instance argues that the theory is deterministic: the universe is attributed a state vector $|\psi_{\text{universe}}\rangle$ which undergoes a unitary (reversible) evolution. Each measurement then corresponds to a splitting of the universe into parallel universes. As all branches exist in parallel, meaning that all possible outcomes of a measurement do occur, the theory is deterministic. However, even though the evolution of the universe is deterministic, the observer (scientist or not), being part of the universe, cannot do better than making probabilistic predictions.

Projective measurement versus POVM. In the version of the measurement postulate given above, one considers general measurements, also referred to as *Positive Operator Valued Measures* (POVM) in contrast with the more familiar *projective measurements* which display a supplementary condition, that is, that a projective measurement is defined by a set $\{\Pi_1, \cdots, \Pi_n\}$ of projectors such that $\Pi_i\Pi_j = \delta_{i,j}\Pi_i$ and $\sum_{i=1}^{n}\Pi_i = \mathbb{1}$. It turns out, however, that requiring the operators to be projectors is unnecessary. In fact, a consequence of Neumark's dilation theorem is that a POVM element can always be seen as a projective measurement on a larger Hilbert space .

As we saw previously, not all physical systems can be described by a state vector. More general quantum systems are described by a density matrix. The same line of argument shows that not all evolution is unitary. In fact, the evolution of a density matrix is expressed by a Completely Positive Trace Preserving (CPTP) map. A characterization of such CPTP maps is given by the Kraus decomposition (or operator-sum decomposition) theorem:

Theorem 1.1 (Kraus decomposition)**.** *Every CPTP map $T : \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{H})$ can be given the form*

$$T(\rho) = \sum_{k=1}^{K} t_k \rho t_k^\dagger \tag{1.12}$$

for all $\rho \in \mathcal{S}(\mathcal{H})$. The $K \leq dim^2\mathcal{H}$ Kraus operators $t_k : \mathcal{H} \to \mathcal{H}$ satisfy the completeness relation $\sum_{k=1}^{K} t_k^\dagger t_k = \mathbb{1}$.

An alternative to the Kraus decomposition is to go to *the Church of the Larger Hilbert Space*, which makes use of the Stinespring's dilation theorem that roughly states that any quantum channel can be described as a unitary evolution in a larger Hilbert space. Basically, any quantum channel, that is any CPTP map, can be decomposed in three operations:

- tensoring with a second system, the *ancilla*,
- unitary evolution on the joint system,
- reduction to a subsystem.

The Stinespring's dilation theorem gives a bound on the dimension of the Hilbert space of the ancilla, and states that the representation is unique up to unitary equivalence.

Theorem 1.2 (Stinespring's dilation)**.** *Let $T : \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{H})$ be a CPTP map on a finite-dimensional Hilbert space $\mathcal{H}$. Then there exists a Hilbert space $\mathcal{K}$ and a unitary operation U on $\mathcal{H} \otimes \mathcal{K}$ such that:*

$$T(\rho) = \mathrm{tr}_{\mathcal{K}} U(\rho \otimes |0\rangle\langle 0|)U^\dagger \tag{1.13}$$

for all $\rho \in \mathcal{S}(\mathcal{H})$. The ancilla space $\mathcal{K}$ can be chosen such that $\mathrm{dim}\mathcal{K} \leq \mathrm{dim}\mathcal{H}^2$. This representation is unique up to unitary equivalence.

Then, when considering the evolution of a general quantum system described by its density matrix under a CPTP map, one can always instead study the problem, in a non ambiguous way, by looking at a purification of the system that undergoes a unitary evolution. Switching from one point of view to the other is merely a question of taste and of simplicity. These two points of view are especially important in the case of QKD for instance as one can either consider that Alice sends quantum states ρ_A to Bob which are partially (or totally) intercepted by the eavesdropper Eve, that is, they evolve under a CPTP map, or that Alice, Bob and Eve share a tripartite pure state $|\psi\rangle_{ABE}$ which follows a unitary evolution. These two scenarios correspond respectively to the *Prepare and Measure* and the *Entanglement-Based* descriptions of the protocol. Both give a complete and equivalent description of the real protocol, but one approach might be easier to analyze. In practice, it turns out that the entanglement-based description is often easier to handle from a theoretic point of view.

For the sake of completeness, let us note that the equivalence between the Prepare and Measure and the Entanglement-Based versions of the protocol is only true when the protocol is well-defined. In particular, this means that the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, and especially its dimension, should be known. This is always the case when discussing QKD protocols from a theoretical perspective. However, it becomes more problematic when analyzing experimental implementations. In this case, it is in general very difficult to prove that the effective Hilbert space describing the experimental protocol has the right dimension. This leads for instance to the so-called problem of *side channels*, where the relevant information is encoded in degrees of freedom not explicitly considered by the theoretical protocol, meaning that the experimental Hilbert space is larger than the one considered for proving the security of the protocol. A way to avoid this problem is for instance to use properties which are independent of the dimension of the Hilbert space considered: this has lead to the concept of *device-independent* QKD where the security of the protocol can be linked to the violation of a Bell inequality, meaning that no assumption one the dimension of the Hilbert space is necessary. This will be discussed in more details in Chapter 3.

After this brief summary of the axioms of Quantum Mechanics, and before considering quantum information theory, let us recall the basics of classical information theory. This is the object of the following section.

1.2 Information theory: the classical picture

At the end of the forties, Claude Shannon proved two theorems that gave birth to the field of Information Theory: the *source coding* and the *noisy-channel coding* theorems which are respectively concerned with the limits for data compression of a source and information transfer rate of a channel.

Here we only give a rapid overview of information theory. A more detailed presentation can be found for instance in the textbooks "Elements of information theory" by Cover and Thomas [33] and "Information theory, inference and learning algorithms" by MacKay [100].

1.2.1 Shannon entropy

A natural measure of the uncertainty of a random variable X is its (Shannon) *entropy* $H(X)$ defined as follows:

$$H(X) = -\sum_{x\in\mathcal{X}} p(x)\log_2 p(x) \tag{1.14}$$

where $\mathcal{X}$ is the support of X and $p(x)$ is the probability associated with each realization. This notion can be generalized to n-uples of random variables $X_1, \cdots, X_n$ with the *joint entropy*:

$$H(X_1, \cdots, X_n) = -\sum_{x_1\in\mathcal{X}_1} \cdots \sum_{x_n\in\mathcal{X}_n} p(x_1, \cdots, x_n)\log_2 p(x_1, \cdots, x_n) \tag{1.15}$$

From this definition, one can immediately deduce the following properties:

Theorem 1.3 (Basic properties of the entropy [33])**.**

1. $H(X) \geq 0$*, with equality if and only if* X *is certain.*
2. H *is* subadditive*:* $H(X_1, \cdots, X_n) \leq H(X_1)+\cdots+H(X_n)$ *with equality if and only if the* X_i *are independent.*
3. *If* $\mathcal{X}$ *is finite,* $H(X) \leq \log_2 |\mathcal{X}|$ *with equality if and only if* X *is uniformly distributed over* $\mathcal{X}$*.*

Besides being a useful tool for the study of probability distributions, the entropy also has an operational interpretation. The *source coding theorem* relates the entropy of a random variable to the optimal compression rate one can achieve for this variable. Before stating this theorem, let us introduce the notion of *source code*. A binary *source code* C for a random variable X is a mapping from $\mathcal{X}$, the range of X, to the set of finite-length bit strings. A source code should allow one to recover the source symbol x from $C(x)$. The *expected length* of the code C is

$$L(C) = \sum_{x\in\mathcal{X}} p(x)l(x) \tag{1.16}$$

where $l(x)$ is the length of $C(x)$. The source coding theorem gives a lower bound on the expected length of a code.

Theorem 1.4 (Source coding theorem [100])**.** N *independent and identically distributed (i.i.d.) random variables each with entropy* $H(X)$ *can be compressed into more than* $NH(X)$ *bits with negligible risk of information loss, as* $N \to \infty$*; conversely if they are compressed into fewer than* $NH(X)$ *bits it is virtually certain that information will be lost.*

Roughly speaking, the entropy of a random variable measures the number of bits necessary to describe faithfully this variable.

1.2.2 Generalization of the Shannon entropy

The Shannon entropy is not the only entropic quantity of interest for a random variable. One can define the *Rényi entropy of order* α of the random variable X as:

$$H_\alpha(X) = \frac{1}{1-\alpha} \log_2 \sum_{x \in \mathcal{X}} p(x)^\alpha. \tag{1.17}$$

Among the values of α of interest, one can find:

- $H_0(X) = \log_2 |\mathcal{X}|$, the *max-entropy* of X,
- $H_1(X) = H(X)$, which is simply the Shannon entropy of X,
- $H_2(X) = -\log_2 \sum_{x \in \mathcal{X}} p(x)^2$, the *collision entropy* which plays a role for *privacy amplification* protocols for instance [11].
- $H_\infty(X) = -\log_2 \sup_{x \in \mathcal{X}} p(x)$, the *min-entropy* of X, which is related to the maximal probability of guessing the value of X.

For a given random variable X, $(\alpha \mapsto H_\alpha(X))$ is a decreasing function of α. All the Rényi entropies are *additive*, meaning that $H_\alpha(X,Y) = H_\alpha(X) + H_\alpha(Y)$ for independent random variables X and Y. However, if X and Y are not independent, only in the case of the Shannon entropy can one separate out the variables X and Y and write:

$$H(X,Y) = H(X) + \mathbb{E}_{p(x)} H(Y|X=x), \tag{1.18}$$

where $\mathbb{E}_{p(x)}$ refers to the expectation under the law $p(x)$. This leads to the definition of the *conditional entropy* $H(Y|X)$ of the random variable Y given X:

$$H(Y|X) = -\sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x,y) \log_2 p(y|x) \tag{1.19}$$

with the following property (*chain rule*):

$$H(X,Y) = H(X) + H(Y|X). \tag{1.20}$$

A fundamental property of conditioning is that it reduces the entropy:

$$H(X|Y) \leq H(X), \tag{1.21}$$

with equality if and only if X and Y are independent random variables. One then defines the *mutual information* $I(X;Y)$ between the random variables X and Y:

$$I(X;Y) = -\sum_{(x,y) \in \mathcal{X} \times \mathcal{Y}} p(x,y) \log_2 \frac{p(x,y)}{p(x)p(y)} \tag{1.22}$$

with the property that

$$\begin{aligned} I(X;Y) &= H(X) + H(Y) - H(X,Y) && (1.23)\\ &= H(X) - H(X|Y) = H(Y) - H(Y|X). && (1.24) \end{aligned}$$

The mutual information between two random variables is a measure of their correlation. In particular, one has $I(X;Y) = 0$ for independent variables. It should be noted that equation 1.21 also holds for conditional entropies

$$H(X|Y,Z) \leq H(X|Y) \tag{1.25}$$

which is called the *strong subadditivity property*. This property can equivalently be written:

$$H(X,Y) + H(Y,Z) \geq H(X,Y,Z) + H(Y). \tag{1.26}$$

1.2.3 Operational interpretation: Shannon's noisy-channel theorem

One of the great insights of Shannon was to give a very simple but universal model for the transmission of data [141], consisting of five parts and depicted on Figure 1.1:

- an *information source* produces a message to be communicated to the *destination*,
- a *transmitter* operates on the message to produce a signal suitable for the transmission over the *channel*,
- the *channel* is the physical medium used to transmit the signal,
- the *receiver* recovers the message from the received signal,
- the *destination* is the person for whom the message is intended.

Let us now give a mathematical definition of a communication channel. A *discrete channel* is a system consisting of an input alphabet $\mathcal{X}$, an output alphabet $\mathcal{Y}$ and a probability transition matrix $p(y|x)$ that expresses the probability of observing the output y given the input x. The channel is said to be *memoryless* if the probability distribution of the output only depends on the input at that time. One defines the *capacity* C of a discrete memoryless channel (DMC) as

$$C = \max_{p(x)} I(X,Y) \tag{1.27}$$

where the maximum is taken over all possible input distributions $p(x)$.

The *Binary Symmetric Channel* (BSC) is the simplest example of channels. The input and output alphabet both are $\mathcal{X} = \mathcal{Y} = \{0,1\}$ and the probability transition matrix is given by

$$p(y|x) = \begin{cases} 1-p & \text{if} \quad y = x \\ p & \text{if} \quad y \neq x \end{cases} \tag{1.28}$$

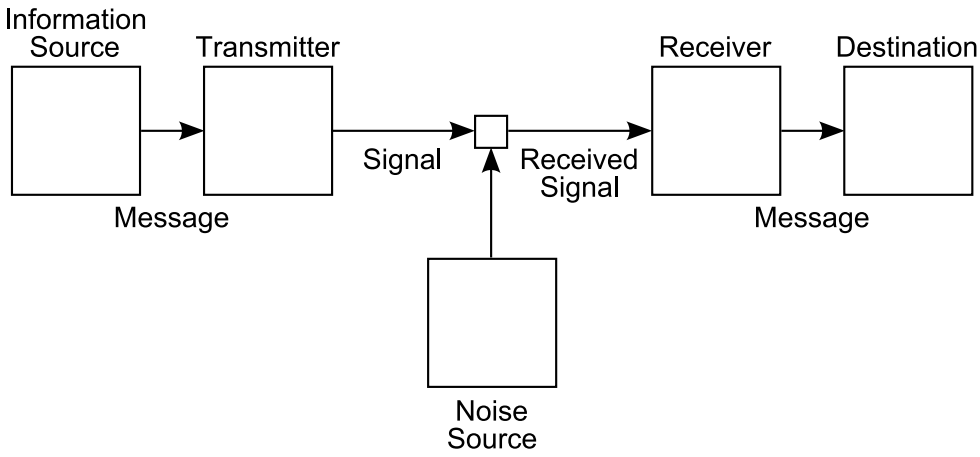

Figure 1.1: Shannon's model for the transmission of a message

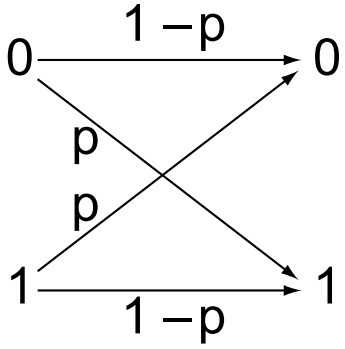

Figure 1.2: Binary symmetric channel

This means that an error will occur with probability p and that both possible errors are equally probable (see Figure 1.2).

Let us now prove that the capacity of the BSC is given by:

$$C_{\mathrm{BSC}} = 1 - h(p), \tag{1.29}$$

where $h(p) = -p \log_2 p - (1-p) \log_2 (1-p)$ is the binary entropy function.

Proof. The mutual information between the input X and the output Y of the BSC is

such that:

$$\begin{aligned} I(X;Y) &= H(Y) - H(Y|X) && (1.30)\\ &= H(Y) - \sum_{x\in\{0,1\}} p(x)H(Y|X=x) && (1.31)\\ &= H(Y) - \sum_{x\in\{0,1\}} p(x)h(p) && (1.32)\\ &= H(Y) - h(p) && (1.33)\\ &\leq 1 - h(p) && (1.34) \end{aligned}$$

since the entropy of a binary random variable is upper bounded by 1. Equality is achieved when the input distribution is uniform. □

An example of continuous alphabet channel of significant interest (especially for QKD with continuous variables) is the *Additive White Gaussian Noise* (AWGN) channel where the input X and the output Y are related through $Y = X + Z$ where Z is a Gaussian noise of variance σ^2, $Z \sim \mathcal{N}(0, \sigma^2)$, independent of the input. This means that the probability transition is given by:

$$p(y|x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(y-x)^2}{2\sigma^2}}. \tag{1.35}$$

If no restriction is imposed on the input, the capacity of the AWGN channel is infinite. Usually, however, a energy constraint is imposed meaning that the variance of X is upper bounded by some maximal energy Σ^2. In that case, the capacity of the AWGN channel is given by:

$$C_{\text{AWGN}} = \frac{1}{2}\log_2(1 + \text{SNR}), \tag{1.36}$$

where the signal-to-noise ratio (SNR) is defined as $\text{SNR} = \Sigma^2/\sigma^2$.

Proof. In order to compute the capacity of the AWGN channel, we need a generalization of the notion of entropy for continuous variables as the input and output alphabets are now a priori continuous: $\mathcal{X} = \mathcal{Y} = \mathbb{R}$. The *differential entropy* $h(X)$[5] is defined as

$$h(X) = -\int_{x\in\mathcal{X}} p(x)\log_2 p(x), \tag{1.37}$$

which, unlike the entropy, can be negative. The differential entropy of a normal distri-

[5] which is not to be mistaken with the binary entropy function $h(p)$ of a probability p

bution $\phi(x) = \frac{1}{\sqrt{2\pi}\sigma} \exp(-\frac{x^2}{2\sigma^2})$ is easily computed:

$$\begin{aligned} h(\phi) &= -\int \phi \log_2 \phi && (1.38)\\ &= -\int \mathrm{d}x\, \phi(x) \left(-\frac{x^2}{2\sigma^2} + \frac{1}{2} \log_2(2\pi\sigma^2) \right) && (1.39)\\ &= \frac{1}{2} + \frac{1}{2} \log_2 2\pi\sigma^2 && (1.40)\\ &= \frac{1}{2} \log_2 2\pi e\sigma^2. && (1.41) \end{aligned}$$

This allows us to compute the mutual information $I(X;Y)$ between the input and output of an AWGN channel:

$$\begin{aligned} I(X;Y) &= h(Y) - h(Y|X) && (1.42)\\ &= h(Y) - h(X+Z|X) && (1.43)\\ &= h(Y) - h(Z|X) && (1.44)\\ &= h(Y) - h(Z) && (1.45) \end{aligned}$$

because X and Z are independent random variables. Since $Z \sim \mathcal{N}(0, \sigma^2)$, $h(Z) = \frac{1}{2} \log_2 2\pi e\sigma^2$. The independence of X and Z and the fact that $\mathbb{E}Z = 0$ show that:

$$\begin{aligned} \mathbb{E}Y^2 &= \mathbb{E}X^2 + \mathbb{E}Z^2 && (1.46)\\ &\leq \Sigma^2 + \sigma^2 && (1.47) \end{aligned}$$

We now use the fact that the normal distribution maximizes the entropy for a given variance[6] to bound $h(Y)$:

$$h(Y) \leq \frac{1}{2} \log_2 2\pi e(\Sigma^2 + \sigma^2). \tag{1.48}$$

Finally, one gets an upper bound for $I(X;Y)$:

$$I(X;Y) \leq \frac{1}{2} \log_2 \left(1 + \frac{\sigma^2}{\Sigma^2} \right). \tag{1.49}$$

This inequality is saturated when the input follows a normal distribution, which concludes the proof. □

Error-correcting codes. Source coding is a way to remove redundancy in order to compress data. We are now interested with the converse problem, that is adding some redundancy in order to protect data from noise. This protection is achieved thanks to an *error correcting code* C which is also a mapping from the source alphabet $\mathcal{X}$ to the

[6] We do not give a proof of this statement (Theorem 8.6.5 of [33]) here, as we will derive a generalization of this result for the quantum setting in Chapter 3.

set of N-bit strings (for a code of length N). The encoded information $C(x)$ is then sent through the communication channel, where it can be affected by noise. The goal of the error correcting code is for the output of the channel to be sufficient to recover x. As one can define the expected length for a source code, one defines the *rate* of an error correcting code as the ratio between $\log_2 |\mathcal{X}|$ and the length N of the code:

$$R = \frac{\log_2 |\mathcal{X}|}{N}. \tag{1.50}$$

The rate R is a measure of the quantity of information sent per use of the communication channel. The *channel coding theorem* gives an upper bound for the rate at which information can be *reliably* sent through a channel.

Theorem 1.5 (Channel coding theorem [33])**.** *All rates below capacity C are achievable, and all rates above capacity are not; that is, for all rates $R < C$, there exists a sequence of codes of length n with 2^{nR} elements with probability of error $p_e^{(n)} \to 0$. Conversely, for rates $R > C$, $p_e^{(n)}$ is bounded away from 0.*

Roughly speaking, the channel coding theorem states that one can send information reliably on a noisy channel up to a rate corresponding to the capacity of the channel. One important remark is that this theorem does not provide a construction of a code achieving the capacity of the channel. More exactly, the proof of the theorem uses the fact that a random code will achieve the capacity, but such a code suffers important short-comings, namely that both encoding and decoding will be very complex tasks that are therefore not practical. Indeed, to any error-correcting code are associated two functions:

- an *encoding function* which associates every source signal $x \in \mathcal{X}$ to a bit-string $C(x) \in \{0,1\}^N$ (which is itself mapped to a physical signal to be sent on the communication channel),
- a *decoding function* which maps the output of the channel to an estimated value for x: $\hat{x}$.

MacKay [100] suggested the following classification for error-correcting codes:

- *Very good codes* which achieve arbitrary small probability of error for any communication rate up to the capacity of the channel.
- *Good codes* which achieve arbitrary small probability of error for any communication rate up to some maximum rate which is less than the capacity of the channel.
- *Practical codes* which can be encoded and decoded on time and space polynomial in the block length. As it turns out, the practical codes of interest are even more constrained as one would rather have a complexity linear (or almost linear) in the block length.

Unfortunately, practical very good codes are still unknown at the time of writing of this manuscript. However, for the AWGN channel, two families of practical good codes are known, *turbo codes* [13] and *LDPC codes* [132].

1.3 Information theory in the quantum age

Let us now turn to quantum information theory. This field was born with the idea that the physical support of information is ultimately quantum. The main topics of interest for quantum information theory are the transmission of information (classical or quantum) over quantum channels, and the tradeoff between acquisition of information about a quantum state and disturbance of the state. This second topic, specific to the quantum setting, is of primary importance for the study of cryptographic primitives such as quantum key distribution for which the action of an eavesdropper will be detected thanks to the disturbance of the state it induces.

Comprehensive expositions of quantum information theory can be found in John Preskill's lecture notes [73] or in Nielsen and Chuang's "Quantum computation and quantum information" [109].

1.3.1 Encoding quantum information

The fundamental support of quantum information is the *qubit*, that is a quantum state in a two-dimensional Hilbert space spanned by the orthogonal basis $\{|0\rangle, |1\rangle\}$. A qubit $|\psi\rangle$ can be written as:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1.51}$$

where α and β are complex amplitudes such that $|\alpha|^2 + |\beta|^2 = 1$. Whereas it seems as if an infinite amount of information is required to defined the state $|\psi\rangle$ (in order to describe α and β), we will see later that, if fact, only one bit of classical information can be stored in a qubit.

More generally, given a Hilbert space of dimension d spanned by the orthogonal basis $\{|0\rangle, \cdots, |d-1\rangle\}$, one can define the notion of *qudit* as an generic element $|\psi\rangle$ of this Hilbert space:

$$|\psi\rangle = \alpha_0|0\rangle + \cdots \alpha_{d-1}|d-1\rangle \tag{1.52}$$

where $|\alpha|^2 + \cdots + |\alpha_{d-1}|^2 = 1$. A quantum state can even be defined in an infinite dimensional Hilbert space, such as the Fock basis $\{|0\rangle, \cdots, |n\rangle, \cdots\}$. For instance, a *qumode* describes the quantum state associated with a mode of the quantized electromagnetic field, and is central to the study of quantum information with continuous variables (see Chapter 2).

Distance between quantum states. Before even talking of encoding information on quantum states, one needs to realize that contrary to the classical case, not all states are perfectly distinguishable. We are thus interested in answering the following question: "how close are two quantum states"? There is not any universal answer but two quantities, the *trace distance* and the *fidelity*, which are generalizations of the classical concepts, display some interesting properties.

Trace distance

The trace distance between quantum states ρ and σ is defined as

$$D(\rho,\sigma) \equiv \frac{1}{2}||\rho-\sigma||_1, \tag{1.53}$$

where $||A||_1 = \mathrm{tr}|A| = \mathrm{tr}\sqrt{A^\dagger A}$. D is a genuine distance in the mathematical sense of the term, meaning that the triangle inequality holds: for all states ρ,σ,τ,

$$D(\rho,\tau) \leq D(\rho,\sigma) + D(\sigma,\tau). \tag{1.54}$$

The quantum trace distance is a generalization of the classical trace distance $D(p_x,q_x) \equiv 1/2\sum_x |p_x - q_x|$ between two classical probability distributions $\{p_x\}$ and $\{q_x\}$. This is shown by the following theorem [109]:

Theorem 1.6. *Let $\{E_m\}$ be a POVM, with $p_m \equiv \mathrm{tr}(\rho E_m)$ and $q_m \equiv \mathrm{tr}(\sigma E_m)$ as the probabilities of obtaining a measurement outcome labeled by m. Then*

$$D(\rho,\sigma) = \max_{\{E_m\}} D(p_m,q_m), \tag{1.55}$$

where the maximization is over all POVMs $\{E_m\}$.

We will see later that a consequence of this theorem is that the trace distance is related to the probability of distinguishing two quantum states. Because it only depends on the spectrum of $\rho-\sigma$, the trace distance between ρ and σ is invariant under unitary operations, that is, for any unitary U,

$$D(U\rho U^\dagger, U\sigma U^\dagger) = D(\rho,\sigma). \tag{1.56}$$

In the case of two pure states $\rho = |\psi\rangle\langle\psi|$ and $\sigma = |\phi\rangle\langle\phi|$, the expression of the trace distance takes a simple form:

$$D(|\psi\rangle,|\phi\rangle) = \sqrt{1-|\langle\psi|\phi\rangle|^2}. \tag{1.57}$$

Fidelity

The fidelity between quantum states ρ and σ is defined as

$$F(\rho,\sigma) \equiv \mathrm{tr}\sqrt{\rho^{1/2}\sigma\rho^{1/2}}. \tag{1.58}$$

In the case where ρ and σ commute, they are diagonal in the same basis,

$$\rho = \sum_k r_k|k\rangle\langle k| \quad \text{and} \quad \sigma = \sum_k s_k|k\rangle\langle k|, \tag{1.59}$$

and

$$F(\rho,\sigma) = \sum_k \sqrt{r_k s_k} \tag{1.60}$$

meaning that F reduces to the classical fidelity between the distributions $\{r_k\}$ and $\{s_k\}$. If one of the states is pure, then the fidelity between $|\psi\rangle$ and ρ is simply given by

$$F(|\psi\rangle, \rho) = \sqrt{\langle\psi|\rho|\psi\rangle}, \tag{1.61}$$

and if both states are pure, the fidelity corresponds to their overlap. As the trace distance, the fidelity is invariant under unitary operations, that is, for all unitary U, one has

$$F(U\rho U^\dagger, U\sigma U^\dagger) = F(\rho, \sigma). \tag{1.62}$$

The fidelity is a practical measure of closeness for two quantum states because of Uhlmann's theorem:

Theorem 1.7 (Uhlmann's theorem)**.** *For any states ρ and σ, and any purification $|\psi\rangle$ of ρ, there exists a purification $|\phi\rangle$ of σ such that*

$$F(\rho, \sigma) = |\langle\psi|\phi\rangle|. \tag{1.63}$$

Therefore, the fidelity between two mixed states can always be interpreted as the maximal overlap between two purifications of these states.

The trace distance and the fidelity are related through the following inequalities [109]:

$$1 - F(\rho, \sigma) \leq D(\rho, \sigma) \leq \sqrt{1 - F(\rho, \sigma)^2}. \tag{1.64}$$

Therefore, for most purposes, these two measures of distance between quantum states are equivalent, and one should choose the most practical one for some practical application.

Distinguishing quantum states. A consequence of the linearity of quantum mechanics is the *no cloning theorem* stating that there cannot exist an operation that clones an arbitrary quantum state since the operation $|\psi\rangle \longmapsto |\psi\rangle|\psi\rangle$ is not unitary. A corollary to this result is that one cannot distinguish perfectly between non orthogonal quantum states.

The general question of how well could two quantum states ρ_0 and ρ_1 be distinguished was addressed by Helström [69]:

Theorem 1.8. *Let ρ_0 and ρ_1 be two quantum states prepared with probability q and $1-q$. The probability to correctly identify the state is at most:*

$$p_{\text{guess}} = \frac{1}{2}[1 + ||q\rho_0 - (1-q)\rho_1||_1]. \tag{1.65}$$

The measurement saturating this bound is the POVM $\{M_0, M_1 = \mathbb{1} - M_0\}$, where M_0 is the projector on the positive eigenspace of $q\rho_0 - (1-q)\rho_1$.

This theorem explains why the trace distance is often chosen as an operational measure of the distance between quantum states: it gives the maximal probability of distinguishing two quantum states prepared with the same probability, given the best possible

measurement[7]. In particular, in the case of any operational task (such as quantum key distribution for instance), one is often interested in comparing the performance of the actual protocol producing a state ρ_{protocol} with an ideal realization of the task ρ_{ideal}[8]. If $D(\rho_{\text{protocol}}, \rho_{\text{ideal}}) \leq \epsilon$ for some small value of the parameter ϵ, it then means that the outcome of protocol is indistinguishable from the one of an ideal protocol except with probability ϵ.

There is a vast literature concerned with the problem of distinguishing quantum states (see for instance [28] and references therein). It should be noted that this problem (which is nothing more than an optimization problem) is often too complicated to be solved explicitly. In the case where the number of states is greater than two, it can however be solved if the states display important symmetry as we show now.

Let us consider the following problem of distinguishing between N states $\{|\psi_1\rangle, \cdots, |\psi_N\rangle\}$ prepared with uniform probability with the goal to minimize the probability of errors. Let us assume moreover that the states are symmetric, in the sense that there exists a unitary U such that

$$|\psi_k\rangle = U|\psi_{k-1}\rangle = U^{k-1}|\psi_1\rangle, \tag{1.66}$$

$$U|\psi_N\rangle = |\psi_1\rangle. \tag{1.67}$$

The optimum measurement for these states is known as the *square-root measurement* [28] given by the POVM $\{\Pi_k = |\omega_k\rangle\langle\omega_k|\}_{1\leq k\leq N}$ where

$$|\omega_k\rangle = \Psi^{-1/2}|\psi_k\rangle \tag{1.68}$$

with the operator Ψ defined as

$$\Psi = \sum_{k=1}^{N} |\psi_k\rangle\langle\psi_k|. \tag{1.69}$$

For a uniform probability distribution for the $\{|\psi_k\rangle\}_{1\leq k\leq N}$, this measurement attains the minimum possible error probability p_e:

$$p_e = 1 - \frac{1}{N}\sum_{k=1}^{N} |\langle\psi_k|\Psi|\psi_k\rangle|^2. \tag{1.70}$$

[7] A related but different problem is concerned with *unambiguous discrimination* of quantum states where the goal is not to minimize the error probability but to never make a wrong prediction about which state was measured. Since this cannot be achieved in general because of the previous theorem, one has to authorize a third kind of answer in addition to 0 and 1: in particular, the measurement result labelled '?' corresponds to the case where the measurement could not discriminate between states ρ_0 and ρ_1.

[8] For instance, in the case of a quantum key distribution protocol, the ideal protocol should produce a state $\rho_{\text{ideal}} = \rho_K \otimes \rho_E$ where ρ_K is the completely mixed uniform state shared by Alice and Bob and corresponding to the key and ρ_E is the state of the eavesdropper which is completely uncorrelated with the value of the key.

Distinguishing quantum channels. A quantum channel is a *completely positive trace-preserving* (CPTP) map transforming the state ρ_A of a system A at time t to ρ'_A, the state of a system A' at time t'. In a similar way that one may be interested in distinguishing two quantum states, one might also want to distinguish two quantum maps, for instance the map describing an ideal realization of some operational task with the map of an actual implementation of a protocol. For such a purpose, one needs to define a measure of distance between CPTP maps. A possibility is to use the *diamond norm* $||.||_\diamond$ of a transformation[9] $\mathcal{T}$ defined by

$$||\mathcal{T}||_\diamond \equiv \sup_{k\in\mathbb{N}} ||\mathcal{T}\otimes \mathrm{id}_k||_1, \tag{1.71}$$

where

$$||\mathcal{S}||_1 \equiv \sup_{||\sigma||_1\leq 1} ||\mathcal{S}(\sigma)||_1 \tag{1.72}$$

and id_k denotes the identity map on states of a k-dimensional quantum system. The suprema in both definitions are reached for positive σ and k equal to the dimension of the input of $\mathcal{T}$ [79]. The diamond norm allows for the definition of the *diamond distance* between two CPTP maps $\mathcal{E}$ and $\mathcal{F}$:

$$D_\diamond(\mathcal{E},\mathcal{F}) \equiv ||\mathcal{E}-\mathcal{F}||_\diamond. \tag{1.73}$$

As the trace distance, the diamond distance has an operational interpretation in the following sense: if one is asked to distinguish between two physical processes respectively described by the CPTP maps $\mathcal{E}$ and $\mathcal{F}$, the maximal probability p_{guess} of a correct guess, if the player is allowed to observe the process once, with an input of his choice, possibly correlated with a reference system, is given by [31]:

$$p_{\mathrm{guess}} = \frac{1}{2}\left(1 + D_\diamond(\mathcal{E},\mathcal{F})\right). \tag{1.74}$$

von Neumann entropy. The *von Neumann entropy* is the quantum information theoretic generalization of the Shannon entropy. The von Neumann entropy $S(\rho)$ of a quantum state ρ is defined as

$$S(\rho) = -\mathrm{tr}\rho\log_2\rho. \tag{1.75}$$

In the orthogonal basis $\{|k\rangle\}$ that diagonalizes ρ, one has

$$\rho = \sum_k \lambda_k |k\rangle\langle k|, \tag{1.76}$$

and $S(\rho) = -\sum_k \lambda_k \log_2\lambda_k$ simply reduces to the Shannon entropy of the distribution $\{\lambda_k\}$. In the following, the entropy of a density matrix ρ_A associated with a quantum system A is written either $S(A)$ or $S(\rho_A)$.

We now list some properties of the von Neumann entropy (their proof can be found in [109]):

[9] such a transformation can be a difference between two CPTP maps $\mathcal{E}$ and $\mathcal{F}$: $\mathcal{T} = \mathcal{E} - \mathcal{F}$

Theorem 1.9 (Basic properties of S). *1. $S(\rho) \geq 0$, with equality if and only if ρ is pure*[10].

2. *In a finite dimensional Hilbert space $\mathcal{H}$ of dimension d, $S(\rho) \leq \log_2 d$, with equality if and only if $\rho = \mathbb{1}_{\mathcal{H}}/d$.*

3. *S is invariant under unitary operations: for any unitary U, $S(U\rho U^\dagger) = S(\rho)$.*

4. *If a composite system AB is in a pure state, then $S(A) = S(B)$.*

5. *If $\rho = \sum_k p_k \rho_k$ where the ρ_k have support on orthogonal subspaces, then*

$$S(\rho) = H(p_k) + \sum_k p_k S(\rho_k). \tag{1.77}$$

6. *S is* subadditive*: $S(\rho_{AB}) \leq S(\rho_A) + S(\rho_B)$ with equality if and only if $\rho_{AB} = \rho_A \otimes \rho_B$*[11].

As is the case for classical information theory, one can defines quantum joint and conditional entropies as well as quantum mutual information for composite systems. Let a quantum state of a composite system AB be represented by the density matrix ρ_{AB}, one defines

- the *joint entropy* of the system AB as

$$S(A, B) = -\mathrm{tr}\, \rho_{AB} \log_2 \rho_{AB}, \tag{1.78}$$

- the *conditional entropy* of A given B as

$$S(A|B) = S(A, B) - S(B), \tag{1.79}$$

- the *quantum mutual information* between systems A and B as

$$\begin{aligned} S(A : B) &= S(A) + S(B) - S(A, B) && (1.80)\\ &= S(A) - S(A|B) = S(B) - S(B|A). && (1.81) \end{aligned}$$

An important difference with the classical setting is that the conditional von Neumann entropy can be negative [24].

An non trivial property of the von Neumann entropy is given by the following theorem:

Theorem 1.10 (Strong subadditivity). *For any three quantum systems, A, B and, C, one has:*

$$S(A, B, C) + S(B) \leq S(A, B) + S(B, C). \tag{1.82}$$

[10] A pure state therefore corresponds to a state of maximal knowledge, which is the quantum generalization of a classical probability distribution when one event has probability 1.

[11] The tensor product structure is therefore the quantum generalization of the notion of independence for classical random variables.

Corollaries of this result are:

1. *Conditioning reduces entropy*: $S(A|B,C) \leq S(A|B)$.
2. *Discarding quantum systems never increases mutual information*: $S(A:B) \leq S(A:B,C)$.
3. *Quantum operations never increase mutual information*: if the system AB is mapped to $A'B'$ through a quantum operation, then $S(A':B') \leq S(A:B)$. Here, a *quantum operation* refers to a linear completely positive trace non-increasing map.

1.3.2 Communication over a quantum channel

After having considered various entropic measures for composite quantum states, let us look more closely at some quantum information theoretic tasks, such as communicating over a quantum channel. In particular, in the context of quantum key distribution, we are especially interested in the problem of sending *classical information* on a quantum channel.

An important result of quantum information theory is given by the *Holevo bound* which implies that one cannot send more than n bits of information in n qubits.

Theorem 1.11 (Holevo bound)**.** *Suppose Alice prepares a state ρ_X where $X = 0, \cdots, n$ with probabilities $p_0, \cdots, p_n$. Bob performs a measurement described by POVM elements $\{E_y\} = \{E_0, \cdots, E_m\}$ on that state with measurement outcome Y. Then, for any such measurement,*

$$I(X;Y) \leq S(\rho) - \sum_{x \in X} p_x S(\rho_x), \tag{1.83}$$

where $\rho = \sum_x p_x \rho_x$.

The *Holevo information* of the ensemble $\mathcal{E} = \{\rho_x, p_x\}$ is noted $\chi(\mathcal{E}) = S(\rho) - \sum_x p_x S(\rho_x)$. In general, the Holevo bound is not tight, and the *accessible information* which is the supremum over Bob's measurements of $I(X;Y)$ cannot reach the Holevo bound. In fact, the accessible information reaches the Holevo bound if and only if the states $\{\rho_x\}_{x \in X}$ have orthogonal supports. Despite this, the Holevo bound is very useful as it is much easier to compute than the accessible information which computation amounts to an optimization problem over the set of POVMs that Bob can perform. The Holevo bound is however reachable if Alice sends n-letter words (with $n \longrightarrow \infty$) and Bob is allowed to perform a *collective* measurement instead of *individual* (product) measurements. This is the reason why it is used to quantify the information potentially accessible to an eavesdropper performing a collective attack against a QKD protocol (see [38] and Chapter 3).

1.3.3 Operational entropic quantities for quantum protocols

The Shannon entropy H as well as its quantum generalization, the von Neumann entropy S, are both relevant in the asymptotic limit of n independent instances of a same process.

In the case where either one of these assumptions does not hold (infinite number of signals or independence), one needs to consider more general entropic quantities.

Such a quantity is the *conditional min-entropy*. Following the notations of [83], we introduce the generalization of the *relative entropy*[12] of two states ρ and σ as:

$$D_\infty(\rho||\sigma) \equiv \inf\{\lambda \in \mathbb{R} : \rho \leq 2^\lambda \sigma\}. \tag{1.85}$$

For a bipartite state $\rho = \rho_{AB}$, one defines the min-entropy of A conditioned on B as

$$H_{\min}(A|B)_\rho \equiv -\inf_{\sigma_B} D_\infty(\rho_{AB}||\mathrm{id}_A \otimes \sigma_B) \tag{1.86}$$

where id_A is the identity on the subsystem A. As pointed out in [83], it is interesting to note that the conditional von Neumann entropy can be written in a similar way:

$$S(A|B)_\rho := -\inf_{\sigma_B} D(\rho_{AB}||\mathrm{id}_A \otimes \sigma_B) \tag{1.87}$$

where D is the relative entropy.

Operational meaning of min-entropy. An interesting case is when a classical system is conditioned on a quantum system B. For instance, let us consider the state

$$\rho = \rho_{XB} = \sum_x P_X(x)|x\rangle\langle x| \otimes \rho_B^x, \tag{1.88}$$

where $\{|x\rangle\}_x$ is a family of mutually orthogonal vectors representing the classical values of X. Let us now consider the task of guessing the value of the classical variable X given the knowledge of the system B. In general, such a strategy can always be described by a POVM $\{E_x\}$ on B and the corresponding probability of success $p_{\mathrm{guess}}(X|B)_{\{E_x\}}$ is given by:

$$p_{\mathrm{guess}}(X|B)_{\{E_x\}} = \sum_x P_X(x)\mathrm{tr}(E_x \rho_B^x). \tag{1.89}$$

We now define the *guessing probability* as the probability obtained for the optimal measurement:

$$p_{\mathrm{guess}}(X|B) := \max_{\{E_x\}} p_{\mathrm{guess}}(X|B)_{\{E_x\}} \tag{1.90}$$

In [83], it was proved that the min-entropy of X conditioned on B was linked to the guessing probability through the following equality:

$$p_{\mathrm{guess}}(X|B) = 2^{-H_{\min}(X|B)_\rho}. \tag{1.91}$$

[12] The relative entropy between the states ρ and σ is given by

$$D(\rho||\sigma) \equiv \mathrm{tr}\left(\rho(\log_2 \rho - \log_2 \sigma)\right). \tag{1.84}$$

Smooth min and max-entropies. For various reasons, it is fruitful to consider a slightly generalized version of the min-entropy called the *smooth min-entropy* which corresponds to the min-entropy of an *optimal* state in the neighborhood of the quantum state considered. More precisely, let $\rho = \rho_{AB}$ be a bipartite quantum state and ϵ a positive number, the *smoothness parameter*. The smooth min-entropy of A conditioned on B is given by:

$$H_{\min}^{\epsilon}(A|B)_{\rho} \equiv \sup_{\rho'} H_{\min}(A|B)_{\rho'}, \tag{1.92}$$

where the supremum ranges over all the density operators ρ' which are ϵ-close of ρ for the trace-distance, that is such that $||\rho - \rho'||_1 \leq \epsilon$. The smooth min-entropy is a generalization of the von Neumann entropy as can be seen by the following result [124]:

$$S(A|B)_{\rho} = \lim_{\epsilon \to 0} \lim_{n \to \infty} \frac{1}{n} H_{\min}^{\epsilon}(A^n|B^n)_{\rho^{\otimes n}}. \tag{1.93}$$

The smooth min-entropy shares some properties with the von Neumann entropy. In particular, it is strongly subadditive:

$$H_{\min}^{\epsilon}(A|B) \geq H_{\min}^{\epsilon}(A|BC). \tag{1.94}$$

Alternatively, one can also define the *conditional smooth max-entropy* of A given B:

$$H_{\max}^{\epsilon}(A|B)_{\rho} := \inf_{\rho'} H_{\max}(A|B)_{\rho'}, \tag{1.95}$$

where the supremum ranges over all the density operators ρ' which are ϵ-close of ρ for the trace-distance, and where the *max-entropy* is defined by:

$$H_{\max}(A|B)_{\rho} \equiv -H_{\min}(A|C)_{\rho}, \tag{1.96}$$

where the min-entropy on the right hand side is evaluated for any purification ρ_{ABC} of ρ_{AB}.

Both smooth min and max-entropies have an operational meaning, and can be used to quantify operational tasks such as data compression, channel coding and privacy amplification.

Data compression. A random variable X is given, and we note $l_{\text{compr}}^{\epsilon}(X)$ the minimum length of an encoding of X such that X can be perfectly recovered except with probability ϵ. In the case of an arbitrary long sequence of independent realizations of X, the source coding theorem states that the right measure is given by the entropy of X, i.e.,

$$\lim_{\epsilon \to 0} \lim_{n \to \infty} \frac{1}{n} \, l_{\text{compr}}^{\epsilon}(X_1, \cdots, X_n) = S(X). \tag{1.97}$$

If one of the assumptions is relieved, the right compression measure becomes the smooth max-entropy [128]:

$$l_{\text{compr}}^{\epsilon}(X) = H_{\max}^{\epsilon'}(X) + O(\log 1/\epsilon) \tag{1.98}$$

for some $\epsilon' \in [\frac{1}{2}\epsilon, 2\epsilon]$. Here the term $O(\log 1/\epsilon)$ is independent of the size of X and becomes negligible in the asymptotic limit.

Channel coding. Let us note $l^{\epsilon}_{\text{transm}}(X \to Y)$ the maximum amount of bits that can be reliably transmitted in one use of a classical channel $X \to Y$. It was proven in [129] that:

$$l^{\epsilon}_{\text{transm}}(X \to Y) = \max_{P_X} \left(H^{\epsilon'}_{\min}(X) - H^{\epsilon'}_{\max}(X|Y) \right) + O(\log 1/\epsilon) \tag{1.99}$$

for some $\epsilon' \in [\frac{1}{2}\epsilon, 2\epsilon]$. Again one easily recover the noisy-channel theorem as a special case of an infinite sequence of independent realizations of the channel:

$$\lim_{\epsilon \to 0} \lim_{n \to \infty} \frac{1}{n} l^{\epsilon}_{\text{transm}}(X^n \to Y^n) = \max_{P_X} I(X:Y). \tag{1.100}$$

Privacy amplification. Finally, of utmost importance in the case of quantum key distribution, is the task of *privacy amplification* (also known as *randomness extraction*). Let X be a classical random variable and B some side information. In a secret key establishment protocol, one wants to distill a key $f(X)$ from X which appears completely random from the point of view of an adversary having access to the system B. Let us note $l^{\epsilon}_{\text{extr}}(X|B)$ the maximum length of a bit string $f(X)$ which is ϵ-close to a string perfectly uniform and independent of B. One has [124, 82]:

$$l^{\epsilon}_{\text{extr}}(X|B) = H^{\epsilon'}_{\min}(X|B) + O(\log 1/\epsilon) \tag{1.101}$$

for some $\epsilon' \in [\frac{1}{2}\epsilon, 2\epsilon]$. This result is crucial as it gives the general secure key rate of a QKD protocol. Unfortunately, the value of $H^{\epsilon'}_{\min}(X|B)$ is often difficult to compute. For this reason, one usually consider the case of the so-called *collective attacks* which means that X corresponds to an i.i.d. variable. Then equation 1.93 allows to express the key rate as a conditional von Neumann entropy, which turns out to be much easier to handle.

CHAPTER 2

Quantum information with continuous variables

The goal of this chapter is to present the formalism specific to the study of quantum information with the continuous variables of a bosonic system, for instance, the electromagnetic field.

2.1 Phase space representation

2.1.1 Canonical quantization

In classical Hamiltonian mechanics, the state of a particle is specified by its position x and momentum p. Hamiltonian mechanics is formulated in terms of *Poisson brackets* where one defines the Poisson bracket $\{f, g\}$ of two functions $f(x_i, p_i, t)$ and $g(x_i, p_i, t)$ of N particles by:

$$\{f, g\} = \sum_{i=1}^{N} \left[\frac{\partial f}{\partial x_i} \frac{\partial g}{\partial p_i} - \frac{\partial f}{\partial p_i} \frac{\partial g}{\partial x_i} \right] \tag{2.1}$$

In particular, the canonical variables x_i and p_i satisfy the following relations:

$$\{x_i, x_j\} = 0, \quad \{x_i, p_j\} = \delta_{i,j}, \quad \{p_i, p_j\} = 0. \tag{2.2}$$

Finally, the only transformations allowed in Hamiltonian mechanics are the ones that leave the Poisson bracket invariant. This characterizes the *symplectic* (or *canonical*) structure of classical mechanics.

Generalizing this framework to quantum mechanics can be done through the process of *canonical quantization*. In this case, the canonical variables are replaced by operators $\hat{x}_i$ and $\hat{p}_i$ and the Poisson bracket is replaced by the commutator. In this context, the relations between the canonical variables become

$$[\hat{x}_i, \hat{x}_j] = 0, \quad [\hat{x}_i, \hat{p}_j] = i\delta_{i,j}, \quad [\hat{p}_i, \hat{p}_j] = 0, \tag{2.3}$$

in units where Plank's constant $\hbar$ is set to 1 (which is always possible through a proper rescaling of physical units). These commutation relations immediately lead to the Heisenberg uncertainty relation

$$\Delta\hat{x}\Delta\hat{p} \geq |\langle[\,\hat{x}, \hat{p}\,]\rangle| = \frac{1}{2}. \tag{2.4}$$

More formally, an N-mode continuous-variable quantum system (think of N modes of the electromagnetic field) is described in the infinite-dimensional Hilbert space

$$\mathcal{H} = \bigotimes_{k=1}^{N} \mathcal{H}_k \tag{2.5}$$

which is the tensor product of N *Fock spaces* $\mathcal{H}_i$. Each Fock space $\mathcal{H}_i$ describes a particular mode (characterized by its polarization, its energy and its spatial and temporal wavefunction) and is spanned by a particular basis, the *Fock basis* $\{|0\rangle, |1\rangle, \cdots, |n\rangle, \cdots\}$ where the *Fock state* $|n\rangle$ describes the state of n (indistinguishable) photons present in the mode[1]. The *annihilation* and *creation* operators respectively noted $\hat{a}_i$ and $\hat{a}_i^\dagger$ for the mode i are defined as:

$$\left\{ \begin{array}{rcl} \hat{a}_i|n\rangle_i & = & \sqrt{n}\,|n-1\rangle_i \\ \hat{a}_i^\dagger|n\rangle_i & = & \sqrt{n+1}\,|n+1\rangle_i. \end{array} \right. \tag{2.6}$$

In the remaining of this manuscript, we shall omit the subscript i referring to a particular mode when there is no ambiguity.

The annihilation and creation operators are linked to the *quadrature operators* $\hat{x}$ and $\hat{p}$ through

$$\hat{x} = \frac{1}{\sqrt{2}}\left(\hat{a} + \hat{a}^\dagger\right) \quad \text{and} \quad \hat{p} = -\frac{i}{\sqrt{2}}\left(\hat{a} - \hat{a}^\dagger\right) \tag{2.7}$$

[1]The Fock space is built in such a way that the symmetry aspects of the wavefunction of a system of N identical bosons are automatically taken care of. Hence the notation $|n\rangle$ is quite pragmatic as it allows to describe the unique symmetric state of n bosons in a very compact form, without useless references on how this symmetry is actually enforced.

and thus follow the same commutation rules as $\hat{x}$ and $\hat{p}$:

$$[\hat{a}_i, \hat{a}_j] = 0, \quad [\hat{a}_i, \hat{a}_j^\dagger] = \delta_{i,j}, \quad [\hat{a}_i^\dagger, \hat{a}_j^\dagger] = 0. \tag{2.8}$$

As we will see in the following, these commutation rules give rise to a *symplectic* structure for transformations of continuous-variable quantum systems.

The *vacuum state* of the global Hilbert space $\mathcal{H}$ is noted $|0\rangle \equiv |0, 0, \cdots, 0\rangle$ and corresponds to the ground state of the interaction-free Hamiltonian $\hat{H}$ of a system of N harmonic oscillators:

$$\hat{H} = \sum_{i=1}^{N} \left[\hat{a}_i^\dagger \hat{a}_i + \frac{1}{2} \right]. \tag{2.9}$$

The Fock basis of the global Hilbert space $\mathcal{H}$ is obtained by tensoring the Fock bases of the individual Fock spaces and its generic element is given by

$$|n_1, \cdots, n_N\rangle, \tag{2.10}$$

where $n_i \in \mathbb{N}$ for $i \in \{1, \cdots, N\}$. This state is formally obtained by adding n_i photons in the mode i to the vacuum state:

$$|n_1, \cdots, n_N\rangle = \frac{1}{\sqrt{n_1!\, n_2! \cdots n_N!}}\, \hat{a}_1^{\dagger n_1} \hat{a}_2^{\dagger n_2} \cdots \hat{a}_N^{\dagger n_N} |0\rangle. \tag{2.11}$$

At this point, there are two possibilities to study quantum systems in the Fock space. One can proceed with the standard density operator description, as for finite dimensional Hilbert spaces. In particular, states can be described by infinite-dimensional density matrices:

$$\rho = \sum_{\mathbf{m},\mathbf{n}=0}^{\infty} \rho_{\mathbf{m},\mathbf{n}} |m_1, \cdots, m_N\rangle\langle n_1, \cdots, n_N|, \tag{2.12}$$

where $\mathbf{m} = (m_1, \cdots, m_N)$ and $\mathbf{n} = (n_1, \cdots, n_N)$. However, whereas the density matrix formalism is very useful and handy for small dimensions, it is no longer the case for infinite-dimensional Hilbert spaces as its mathematical manipulation becomes intractable in most cases. For this reason, it might be convenient to work in the *phase space representation*. Formally, this is done by working with the quadratures operators of the state instead of its density operator. The idea is really to exploit the most convenient mathematical formalism, just as N particles might be easier to describe in phase space in classical mechanics.

For an N-mode system, the quadratures can be grouped together in a vector $\hat{r}$:

$$\hat{r} = (\hat{r}_1, \hat{r}_2 \cdots, \hat{r}_{2N})^T = (\hat{x}_1, \hat{p}_1, \hat{x}_2, \hat{p}_2, \cdots, \hat{x}_N, \hat{p}_N)^T. \tag{2.13}$$

This allows us to write the bosonic canonical commutation relations in a more compact form:

$$[\hat{r}_k, \hat{r}_l] = i\Omega_{kl}, \tag{2.14}$$

where Ω is the symplectic form

$$\Omega = \bigoplus_{i=1}^{N} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}. \tag{2.15}$$

A real-valued operator S is said to be *symplectic* if it leaves the symplectic form invariant:

$$S\Omega S^T = \Omega. \tag{2.16}$$

The set of symplectic operators has the structure of a group, and is noted $\mathrm{Sp}(2N, \mathbb{R})$. Note that a consequence of the Stone - von Neumann theorem is that each element of this group can be associated to a transformation corresponding to a quadratic Hamiltonian. In the phase space representation, the Fock states become less relevant, and two sets of states turn out to play a more central role: the *quadrature eigenstates* and the *coherent states*, that we describe now.

Quadrature eigenstates. The quadrature eigenstates states are defined (not surprisingly) as the eigenstates of the position and moment operators:

$$\hat{x}|x\rangle = x|x\rangle \tag{2.17}$$
$$\hat{p}|p\rangle = p|p\rangle. \tag{2.18}$$

With these notations, $|x\rangle$ is a position eigenstate whereas $|p\rangle$ is a momentum eigenstate. Since the operators $\hat{x}$ and $\hat{p}$ are Hermitian, their respective family of eigenstates form two orthonormal bases of the Fock space

$$\langle x \,|\, x' \rangle = \delta(x - x'), \tag{2.19}$$
$$\langle p \,|\, p' \rangle = \delta(p - p') \tag{2.20}$$

that give two resolutions of the identity

$$\int_{-\infty}^{\infty} |x\rangle\langle x| \mathrm{d}x = \mathbb{1}, \tag{2.21}$$
$$\int_{-\infty}^{\infty} |p\rangle\langle p| \mathrm{d}p = \mathbb{1}. \tag{2.22}$$

Both bases are related by Fourier transform:

$$|p\rangle = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \mathrm{d}p \, e^{ixp} |x\rangle, \tag{2.23}$$
$$|x\rangle = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \mathrm{d}x \, e^{-ixp} |p\rangle. \tag{2.24}$$

The main interest of the quadrature eigenstates is that they are related to the wave function of the state and to its Fourier transform: the wave function $\psi(x)$ of a state $|\psi\rangle$ and its Fourier transform $\psi(p)$ read

$$\psi(x) = \langle x \,|\psi\rangle, \tag{2.25}$$
$$\psi(p) = \langle p \,|\psi\rangle. \tag{2.26}$$

Because of their link with the wave functions, the quadrature eigenstates are useful theoretical tools. However, it should be noted that they do not correspond to physical states as their energy diverges.

Coherent states. A more interesting class of quantum states both from the theoretical and the experimental point of view, the *coherent states*, can be easily described in the phase space formalism. Formally, they are defined as the eigenstates of the annihilation operator: the state $|\alpha\rangle$ is such that

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle, \tag{2.27}$$

where α is a complex number. Note that because the annihilation operator $\hat{a}$ is not Hermitian, the states $|\alpha\rangle$ are not orthogonal.
Coherent states have a practical interest as they correspond to the output of (good) lasers. For this reason, they are very easy to generate experimentally, in sharp contrast with the Fock states[2] or quadrature eigenstates (which are unphysical).
In order to study coherent states, it is useful to introduce the so-called *displacement operator* $\hat{D}(\alpha)$ defined as:

$$\hat{D}(\alpha) = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}, \tag{2.28}$$

which is a unitary operator since $i(\alpha\hat{a}^\dagger - \alpha^*\hat{a})$ is Hermitian. Applying the Hadamard lemma for two operators X and Y such that X commutes with $[X, Y]$,

$$e^X Y e^{-X} = Y + [X, Y] \tag{2.29}$$

to $X = -\alpha\hat{a}^\dagger + \alpha^*\hat{a}$ and $Y = \hat{a}$, one gets:

$$\hat{D}^\dagger(\alpha)\hat{a}\hat{D}(\alpha) = \hat{a} + \alpha, \tag{2.30}$$
$$\hat{D}^\dagger(\alpha)\hat{a}^\dagger\hat{D}(\alpha) = \hat{a}^\dagger + \alpha^*. \tag{2.31}$$

Let us now apply the annihilation operator to a displaced vacuum $\hat{D}(\alpha)|0\rangle$. This gives:

$$\hat{a}\hat{D}(\alpha)|0\rangle = \hat{D}(\alpha)(\hat{a} + \alpha)|0\rangle \tag{2.32}$$
$$= \alpha\,\hat{D}(\alpha)|0\rangle, \tag{2.33}$$

which means that $\hat{D}(\alpha)|0\rangle$ is an eigenstate of the annihilation operator with eigenvalue α. As a consequence, $\hat{D}(\alpha)|0\rangle = |\alpha\rangle$, and one can thus conclude that coherent states are displaced vacuums.
In order to derive the expansion of $|\alpha\rangle$ in the Fock basis, one can use the Baker-Hausdorff formula,

$$\hat{D}(\alpha) = e^{-|\alpha|^2/2} e^{\alpha\hat{a}^\dagger} e^{-\alpha^*\hat{a}}, \tag{2.34}$$

[2] the vacuum state $|0\rangle$ is by definition easy to generate, but while single photons can be generated with relatively good quality, the situation becomes more complicated with higher number states. It should be noted, however, that generating such number states is the subject of intense ongoing experimental efforts. For instance, the creation of a two-photon Fock state of free propagating light and Fock states up to 7 photons in a cavity were reported in [116] and [20], respectively.

to write

$$|\alpha\rangle = e^{-|\alpha|^2/2} e^{\alpha \hat{a}^\dagger} e^{-\alpha^* \hat{a}} |0\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n \hat{a}^{\dagger n}}{n!} |0\rangle, \tag{2.35}$$

which gives the well-known expression[3]:

$$|\alpha\rangle = e^{-|\alpha^2|/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \tag{2.36}$$

From the action on the displacement operator on the annihilation and creation operators, one can immediately deduce its action on the quadrature operators, namely,

$$\hat{D}^\dagger(\alpha) \hat{x} \hat{D}(\alpha) = \hat{x} + \sqrt{2}\,\mathrm{Re}(\alpha) \tag{2.37}$$

$$\hat{D}^\dagger(\alpha) \hat{p} \hat{D}(\alpha) = \hat{p} + \sqrt{2}\,\mathrm{Im}(\alpha), \tag{2.38}$$

where $\mathrm{Re}(\alpha)$ and $\mathrm{Im}(\alpha)$ refer respectively to the real and imaginary part of α. This means that the coherent state $|\alpha\rangle$ can be interpreted as a vacuum state displaced by the quantity $d_x = \sqrt{2}\,\mathrm{Re}(\alpha)$ along the quadrature $\hat{x}$ and the quantity $d_p = \sqrt{2}\,\mathrm{Im}(\alpha)$ along the quadrature $\hat{p}$ in phase space.

Coherent states are often referred to as *quasi-classical states* since the saturate the Heisenberg uncertainty principle. Let us indeed compute the variance of the quadrature operators for a coherent state:

$$\langle \hat{x}^2 \rangle = \frac{1}{2} \langle \alpha | \hat{a}^2 + [\hat{a}, \hat{a}^\dagger + 2\hat{a}^\dagger \hat{a} + \hat{a}^{\dagger 2} | \alpha \rangle = \frac{1}{2} \left(1 + (\alpha + \alpha^*)^2\right) = \langle \hat{x} \rangle^2 + \frac{1}{2}, \tag{2.39}$$

which gives $\Delta^2 \hat{x} = \langle \hat{x}^2 \rangle - \langle \hat{x} \rangle^2 = \frac{1}{2}$ and similarly $\Delta^2 \hat{p} = \frac{1}{2}$. Thus, coherent states are the states with minimal uncertainty on their quadratures.

Finally, while the set of coherent states does not form an orthonormal basis since

$$\langle \alpha | \beta \rangle = e^{-(|\alpha|^2 + |\beta|^2)/2} \sum_{n=0}^{\infty} \frac{(\alpha^* \beta)^n}{n!} = e^{-\frac{1}{2}\left(|\alpha|^2 + |\beta|^2 - \alpha^* \beta\right)} \neq 0. \tag{2.40}$$

Two coherent states are never orthogonal, meaning that it is in principle impossible to distinguish perfectly between two coherent states. However, the probability

$$|\langle \alpha | \beta \rangle|^2 = e^{-|\alpha - \beta|^2} \tag{2.41}$$

rapidly falls to 0 when $|\alpha - \beta|$ exceeds a few shot noise units. A detailed study of the discrimination of coherent states can be found in Appendix B. Let us also note that the set of coherent states satisfies the completeness relation [139],

$$\frac{1}{\pi} \int_{\mathbb{C}} |\alpha\rangle\langle\alpha| \mathrm{d}^2 \alpha = \mathbb{1}. \tag{2.42}$$

[3]While Glauber was the first to provide a complete quantum-theoretic description of the coherence in the EM field [54], coherent states had already been studied for a long time, notably by Erwin Schrödinger who introduced them as the states of minimum uncertainty [138].

2.1.2 Measurements in phase space

As we saw in the first chapter, a measurement is characterized by a set of positive operators that form a resolution of the identity. For continuous-variable quantum systems, two types of measurements are mainly considered: photon counting and homodyne measurement which aim respectively at measuring the photon number and the quadrature operators of the field.

Photon number discrimination. This first type of measurement is described by the POVM corresponding to the Fock basis $\{|0\rangle\langle 0|, |1\rangle\langle 1|, \cdots, |n\rangle\langle n|, \cdots\}$. Such a measurement is extremely challenging from a experimental point of view, and actual photon counters really implement the much simpler POVM with two elements $\{|0\rangle\langle 0|, \mathbb{1} - |0\rangle\langle 0|\}$ which discriminates between the absence and presence of photons. Even such a simplified measurement turns out to be quite difficult to realize experimentally and all present implementations suffer of two sources of errors. First, the *quantum efficiency* of the detection η is significantly less than 1. Its current value is closer to 20% for single photon detectors working in the telecom regime (wavelength of 1550 nm). Second, detectors are also affected by *dark noise* meaning that they display spontaneous clicks in absence of a photon. The phenomenon of dark counts is actually quite problematic in applications such as quantum key distribution.

Homodyne detection. The goal of homodyne detection is to measure a quadrature of the state in phase space. It is an interferometric detection scheme where the mode to be measured $(\hat{x}_S, \hat{p}_S)$ interferes with a *local oscillator* which is (with a very good approximation) a classical state with quadratures $(E_{\mathrm{L}} \cos\theta, E_{\mathrm{L}} \sin\theta)$. The phase θ between the two modes can be easily adjusted with a piezoelectric transducer for instance (see Figure 2.1). Since the two modes are combined on a balanced beamsplitter, the outgoing modes $+, -$ are such that

$$\begin{aligned}
\hat{x}_+ &= (\hat{x}_S + E_{\mathrm{L}} \cos\theta)/\sqrt{2} && (2.43)\\
\hat{p}_+ &= (\hat{p}_S + E_{\mathrm{L}} \sin\theta)/\sqrt{2} && (2.44)\\
\hat{x}_- &= (\hat{x}_S - E_{\mathrm{L}} \cos\theta)/\sqrt{2} && (2.45)\\
\hat{p}_- &= (\hat{p}_S - E_{\mathrm{L}} \sin\theta)/\sqrt{2} && (2.46)\\
& && (2.47)
\end{aligned}$$

The intensities I_+ and I_- of modes $+$ and $-$ are measured with PIN detectors and are proportional to the photon numbers of each mode:

$$I_{+,-} = \hat{n}_{+,-} = \frac{1}{2}(\hat{x}^2_{+,-} + \hat{p}^2_{+,-} - 1) \tag{2.48}$$

where we take the proportionality constant equal to 1 for simplicity. Finally, we observe the difference ΔI between the two intensities:

$$\Delta I = I_+ - I_- = 2\left(\hat{x}_s E_{\mathrm{LO}} \cos\theta + \hat{p}_s E_{\mathrm{LO}} \sin\theta\right). \tag{2.49}$$

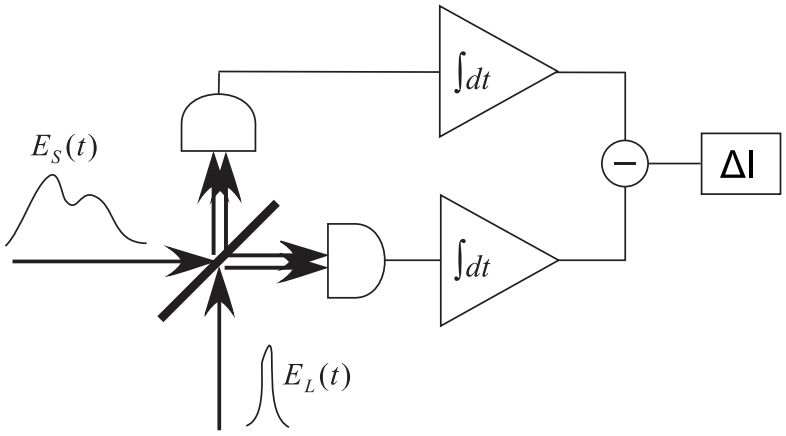

Figure 2.1: Homodyne detection setup (from Ref [99]).

Then, by fixing the value of θ to either 0 or $\pi/2$, one has access to the measurement of quadrature $\hat{x}_s$ or $\hat{p}_s$, respectively. More generally, any rotated quadrature $\hat{x}_\theta = \hat{x}_s \cos\theta + \hat{p}_s \sin\theta$ can be measured with a homodyne detection by applying the right dephasing θ between the signal mode and the local oscillator. The main interest of homodyne detection is that is quantum efficiency is much higher than the one of photon counting, and typically approaches 90% in state-of-the-art experiments.

2.1.3 Wigner function

Displacement operators can be generalized to the N-mode case with the *Weyl operator*:

$$\hat{D}(\xi) \equiv e^{-i\xi^T \Omega \hat{r}}, \tag{2.50}$$

where ξ is a vector in the $2N$-dimensional phase space. Then, instead of describing a quantum state ρ through its density matrix, one can work in phase space and use the *characteristic function* defined as

$$\chi_\rho(\xi) = \mathrm{tr}[\rho \hat{D}(\xi)]. \tag{2.51}$$

A state ρ is completely characterized by its representation in phase space as can be seen in the inversion formula:

$$\rho = \frac{1}{(2\pi)^N} \int \mathrm{d}^{2N}\xi \; \chi_\rho(-\xi)\hat{D}(\xi). \tag{2.52}$$

Finally, by taking the Fourier transform of the characteristic function, one obtains the *Wigner function* of the state

$$W(\xi) = \frac{1}{(2\pi)^N} \int \mathrm{d}^{2N}\zeta \; e^{i\xi^T \Omega \zeta} \chi_\rho(\zeta), \tag{2.53}$$

which corresponds to a quasi-probability distribution in phase space. For the interested reader, a comprehensive discussion about the Wigner function and its properties can be found in Reference [88].
Wigner's formula [157] relates the state ρ of an N-mode bosonic quantum system and its Wigner function in the $N-$dimensional phase space parametrized by the quadratures $(x_1, p_1, \ldots, x_N, p_N)$ through:

$$W(x_1, p_1, \cdots, x_N, p_N) = \frac{1}{\pi^N} \int_{\mathbb{R}^n} \mathrm{d}y_1 \cdots \mathrm{d}y_N \; e^{i(p_1 y_1 + \cdots + p_N y_N)} \langle x_1 - y_1, \cdots, x_N - y_N | \rho | x_1 + y_1, \cdots, x_N + y_N \rangle. \tag{2.54}$$

In this formula, the bra and ket refer to position eigenstates.

Whereas the Wigner function is not a genuine probability function since it can take negative values, it gives rise to such a genuine probability function in terms of homodyne measurement results. More specifically, let us consider an N-mode state described by its Wigner function $W(x_1, p_1, \cdots, x_N, p_N)$, the joint probability of the results of N homodyne measurements (one measurement per mode) is obtained by integrating the Wigner function over the quadratures that are not measured. For instance, the probability distribution for the variables x_1 and p_2 of a 2-mode state is given by:

$$\Pr(x_1, p_2) = \iint \mathrm{d}x_2 \mathrm{d}p_1 \, W(x_1, p_1, x_2, p_2). \tag{2.55}$$

For a single mode state ρ, one has:

$$\int_{-\infty}^{\infty} \mathrm{d}p \; W(x, p) = \mathrm{tr}\rho |x\rangle\langle x|, \tag{2.56}$$

$$\int_{-\infty}^{\infty} \mathrm{d}x \; W(x, p) = \mathrm{tr}\rho |p\rangle\langle p|, \tag{2.57}$$

and in the case of a pure state $\rho = |\psi\rangle\langle\psi|$, one recovers respectively $|\psi(x)|^2$ and $|\psi(p)|^2$. The Wigner function is a linear functional, meaning that the Wigner function of a mixed state $\rho = \sum_i p_i \rho_i$ is given by:

$$W_\rho(\xi) = \sum_i p_i \, W_{\rho_i}(\xi). \tag{2.58}$$

The integral of the Wigner function over the whole phase space is equal to the trace of the state:

$$\int_{\mathbb{R}^n} \mathrm{d}\xi \; W_\rho(\xi) = \mathrm{tr}\rho. \tag{2.59}$$

More generally, one can compute an operator $\hat{o}$ expectation as an average of its Wigner transform in phase space:

$$\langle \hat{o} \rangle = \int_{\mathbb{R}^n} \mathrm{d}\xi \; W_\rho(\xi) o(\xi). \tag{2.60}$$

One should keep in mind that the Wigner function formalism is completely equivalent to the more usual density operator formalism. One should choose the point of view which is the most practical for a specific application. In particular, Gaussian states that we introduce now are much easier to study in phase space than in Fock space.

2.2 Gaussian states and Gaussian operations

Among all possible sets of states of continuous-variable quantum systems, one turns out to be particularly relevant experimentally as well as quite tractable from a theoretical point of view: *Gaussian states* which are given this name because their Wigner function is Gaussian. For the same reasons, the class of *Gaussian operations*, that is quantum operations that map any Gaussian state to a Gaussian state, is also central for the study of quantum information with continuous variables.

2.2.1 Gaussian states

Definition and notations. Gaussian states are states whose characteristic function (and, equivalently, Wigner function) is Gaussian[4]. Thus, they are completely characterized by the first two moments of their characteristic function.
For a general state ρ, we define the *displacement vector* $d \in \mathbb{R}^{2N}$

$$d = \langle \hat{r} \rangle = \mathrm{tr}[\rho\, \hat{r}] \tag{2.62}$$

and the positive-semidefinite symmetric $2N \times 2N$ *covariance matrix* γ

$$\gamma_{ij} = \mathrm{tr}\left[\rho \left\{\hat{r}_i - d_i, \hat{r}_j - d_j\right\}\right], \tag{2.63}$$

where $\{\}$ is the anticommutator. With these notations, we define a generic Gaussian characteristic function to be

$$\chi_\rho(\xi) = \exp\left(-\frac{1}{4}\xi^T \Gamma \xi + iD^T \xi\right), \tag{2.64}$$

where $D = \Omega d$ and $\Gamma = \Omega\gamma\Omega$. Taking the Fourier transform of the characteristic function, one obtains the Wigner function of a Gaussian state:

$$W(r) = \frac{1}{\pi^{2N}\sqrt{\det\gamma}} e^{-(r-d)^T \gamma^{-1}(r-d)}. \tag{2.65}$$

The remarkable property of Gaussian states is that they are entirely described by their first two moments. This means that an N-mode Gaussian state is completely characterized by a number of parameters only quadratic in N (despite the infinite dimension

[4] An alternative definition is that a state is said to be Gaussian if and only if its density matrix ρ is the exponential of a quadratic function f on the canonical operators of the system,

$$\rho = \exp\left[-f(a_1, a_1^\dagger, \cdots, a_N, a_N^\dagger)\right]. \tag{2.61}$$

of the underlying Hilbert space). Such a compact description in phase space has many advantages. For instance, we use it in Chapter 6 to introduce a new type of quantum de Finetti theorem in phase space, despite the apparent restriction of de Finetti theorems to finite-dimensional Hilbert spaces.

Before we detail the most important families of Gaussian states, we would like to characterize admissible covariance matrices for a Gaussian states. Indeed, because of the Heisenberg uncertainty principle, it is clear that not all covariance matrices correspond to physical states. A necessary and sufficient condition that the covariance matrix γ has to satisfy is [146]:

$$\gamma + i\Omega \geq 0. \tag{2.66}$$

From the definition of Gaussian states, it is clear that the properties of a state are contained in the structure of its covariance matrix. We now introduce the notion of *symplectic invariants* that allow for a characterization of the covariance matrix of a Gaussian state.

Symplectic invariants and symplectic spectrum. Let us start by applying Williamson's theorem [145] to the the case of the covariance matrix γ. This theorem implies that for any covariance matrix γ, there exists a (non-unique) symplectic transformation S such that

$$S^T \gamma S = \nu, \tag{2.67}$$

where ν is a diagonal covariance matrix

$$\nu = \bigoplus_{k=1}^{N} \begin{bmatrix} \nu_k & 0 \\ 0 & \nu_k \end{bmatrix} \tag{2.68}$$

The quantities ν_k are referred to as *symplectic eigenvalues* and form the *symplectic spectrum* of the covariance matrix γ. The symplectic eigenvalues correspond to the eigenvalues of the operator $|i\Omega\gamma|$. The matrix ν is the *normal form* of the covariance matrix γ. The uncertainty principle 2.66 can be rewritten in terms of the symplectic eigenvalues as

$$\nu_k \geq 1 \quad \text{for} \quad k = 1, \cdots, N. \tag{2.69}$$

This bound is saturated only for pure Gaussian pure states with $\nu = \mathbb{1}$. This can be seen by noting that the *purity* μ of a Gaussian state ρ with covariance matrix γ is given by

$$\mu \equiv \mathrm{tr}\rho^2 = \frac{1}{\sqrt{\det \gamma}}. \tag{2.70}$$

It turns out that calculating the spectrum of $|i\Omega\gamma|$ is generally not the most practical way to determine the symplectic spectrum of a covariance matrix. An easier (and more elegant) way to proceed is to use symplectic invariants, that is, quantities that are invariant under the action of symplectic group $\mathrm{Sp}(2N, \mathbb{R})$. We now apply this method to the study of one-mode and two-mode states.

One-mode normal decomposition. Here, we are concerned with one-mode states characterized by their 2×2 covariance matrix γ_1. In order to determine the symplectic eigenvalue ν_1 of γ_1, we notice that the determinant is a symplectic invariant, that is for any covariance matrix γ, and any symplectic operator S, one has

$$\det(S\gamma S^T) = \det\gamma \tag{2.71}$$

since the determinant of a symplectic matrix S is necessary equal to 1[5]. As a consequence, one has in general

$$\prod_{k=1}^{N} \nu_k^2 = \det\,\gamma, \tag{2.72}$$

which reduces in the case of a single-mode system to

$$\nu_1 = \sqrt{\det\,\gamma_1}. \tag{2.73}$$

Two-mode normal decomposition. In order to compute the symplectic spectrum $\{\nu_1, \nu_2\}$ of a two-mode covariance matrix γ_{12}

$$\gamma_{12} = \begin{pmatrix} \gamma_1 & C_{12} \\ C_{12} & \gamma_2 \end{pmatrix}, \tag{2.74}$$

where γ_1, γ_2 and C_{12} are 2×2 real matrices, we need to use a second symplectic invariant Δ which is given by

$$\Delta = \det\,\gamma_1 + \det\,\gamma_2 + 2\det\,C_{12}. \tag{2.75}$$

This invariant corresponds to the *principal minor* of order 2 of the covariance matrix γ and is equal to $\nu_1^2 + \nu_2^2$. Hence, it is clear that ν_1^2 and ν_2^2 are the roots of the quadratic form

$$X^2 - \Delta X + \det\,\gamma_{12}, \tag{2.76}$$

that is

$$\nu_{1,2}^2 = \frac{1}{2}\left[\Delta \pm \sqrt{\Delta^2 - 4\det\,\gamma_{12}}\right]. \tag{2.77}$$

Generalization of higher numbers of modes. More generally, higher order principal minors can be used to define symplectic invariants of the covariance matrix γ. By noting $M_k(\alpha)$ the principal minor of order k of the matrix α, one obtains N symplectic invariants Δ_k^N $(k = 1 \cdots N)$ of an N-mode [140]:

$$\Delta_k^N \equiv M_{2k}(\Omega\gamma), \tag{2.78}$$

[5]It is easy to see that the determinant of a symplectic matrix is either 1 or -1 thanks to the relation $S\Omega S^T = \Omega$. The fact that it is necessary 1 can be proved with the identity $\mathrm{Pf}(S^T\Omega S) = \det S\,\mathrm{Pf}(\Omega)$ where $\mathrm{Pf}(\Omega) = 1$ is the Pfaffian of Ω.

which are known as *quantum universal invariants*. Note that $\Delta_N^N = \det \gamma$ and Δ_1^2 reduces to the quantity Δ defined in the previous paragraph. The invariants can easily be expressed as a function of the symplectic eigenvalues:

$$\Delta_k^N = \sum_{\mathcal{S}_k^N} \prod_{j \in \mathcal{S}_k^N} \nu_j^2, \tag{2.79}$$

where the sum runs over all the possible k-subsets $\mathcal{S}_k^N$ of the first N natural integers. Calculating the symplectic spectrum then amounts at solving a polynomial equation of degree N.

Principal families of Gaussian states.

One-mode Gaussian states. First, the *coherent states* are characterized by a displacement vector $d = (d_x, d_p)$ and a covariance matrix $\gamma = \mathbb{1}$. Note that $d = (0, 0)$ corresponds to the vacuum state.
A generalization of the coherent states is given by the *squeezed* coherent states which are characterized by a covariance matrix of the form

$$\gamma = \begin{pmatrix} e^{-2r} & 0 \\ 0 & e^{2r} \end{pmatrix} \tag{2.80}$$

where r is a squeezing parameter. For $r > 0$, the quadrature $\hat{x}$ is squeezed, meaning that its variance is less than the shot noise, whereas the quadrature $\hat{p}$ is anti-squeezed. A squeezed vacuum (with a displacement vector equal to $(0, 0)$) can be obtained by applying a squeezing operator $S(r)$ to the vacuum state. Its expansion in the Fock basis is given by

$$S(r)|0\rangle = \frac{1}{\sqrt{\cosh r}} \sum_{n=0}^{\infty} \frac{\sqrt{(2n)!}}{2^n n!} \tanh^n r \, |2n\rangle. \tag{2.81}$$

An interesting feature of the vacuum squeezed state is that, despite its name, it does contain photons. Let us indeed compute the mean photon number $\langle \hat{n} \rangle$ in the state $S(r)|0\rangle$:

$$\langle \hat{n} \rangle = \frac{1}{\cosh r} \sum_{n=0}^{\infty} 2n \frac{(2n)!}{2^{2n}(n!)^2} \tanh^n r = \sinh^2 r \tag{2.82}$$

which is positive for non zero squeezing.
Another interesting set of states are the *thermal states* for which the displacement vector is null and the covariance matrix is of the form

$$\gamma = \begin{pmatrix} V & 0 \\ 0 & V \end{pmatrix} \tag{2.83}$$

where V is related to the mean photon number through $V = 2\langle n \rangle + 1$.

Two-mode Gaussian states. A general two-mode Gaussian state is characterized by a displacement vector $d = (d_{x_1}, d_{p_1}, d_{x_2}, d_{p_2})$ and a covariance matrix γ_{12}:

$$\gamma_{12} = \begin{pmatrix} \gamma_1 & C_{12} \\ C_{12}^T & \gamma_2 \end{pmatrix}, \tag{2.84}$$

Note that the one-mode Gaussian state obtained by tracing out the second mode is described by the displacement vector $d_1 = (d_{x_1}, d_{p_1})$ and the covariance matrix γ_1.
The case where $C_{12} = 0$ corresponds, for a Gaussian state, to an absence of correlations between the two modes meaning that the Gaussian state ρ_{12} is such that

$$\rho_{12} = \rho_1 \otimes \rho_2, \tag{2.85}$$

where $\rho_1 = \mathrm{tr}_2\, \rho_{12}$ and $\rho_2 = \mathrm{tr}_1\, \rho_{12}$. More generally, an N-mode Gaussian state with a block-diagonal covariance matrix has a product-state structure.
An important class of two-mode Gaussian states are the *two-mode squeezed states* characterized by a covariance matrix γ_{TMS} of the form

$$\gamma_{\mathrm{TMS}} = \begin{pmatrix} \cosh 2r\, \mathbb{1}_2 & \sinh 2r\, \sigma_z \\ \sinh 2r\, \sigma_z & \cosh 2r\, \mathbb{1}_2 \end{pmatrix}, \tag{2.86}$$

where

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.87}$$

Since $\det \gamma_{\mathrm{TMS}} = 1$, a two-mode squeezed state is a pure state which plays a role in continuous-variable quantum information similar to the Bell state $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ in discrete-variable quantum information. This similarity becomes more obvious by noting that the expansion in the Fock basis of a two-mode squeezed vacuum (with a displacement vector $d = (0, 0, 0, 0)$) is given by:

$$|\mathrm{TMS}\rangle = \frac{1}{\cosh r} \sum_{n=0}^{\infty} \tanh^n r\, |n, n\rangle. \tag{2.88}$$

Note that tracing out the second mode of a two-mode squeezed vacuum gives a thermal state for the first mode. This gives a generic way to purify thermal noise as a thermal state can always be interpreted as one half of a pure two-mode squeezed vacuum.
While it is in general very difficult to characterize entanglement of arbitrary quantum states[6], a truly remarkable result is the existence of a simple necessary and sufficient condition for the separability of a general Gaussian state.

Theorem 2.1 (Separability of Gaussian states [41]). *A Gaussian state with covariance matrix γ is separable if and only if there exist covariance matrices γ_A and γ_B such that*

$$\gamma \geq \gamma_A \oplus \gamma_B. \tag{2.89}$$

Note, however, that this criterion is not always very practical as the matrices γ_A and γ_B can be difficult to exhibit.

[6] a notable exception being bipartite qubit systems for which the positivity of the partial transpose is a necessary and sufficient condition for separability [118],[71]

2.2.2 Gaussian operations

Gaussian operations are characterized by the fact that they correspond to all operations which can be performed on Gaussian states using linear optical elements (phase shifts, beam splitters and squeezers) together with homodyne measurements [52]. They are thus particularly relevant because these operations are exactly the ones that are easily implementable experimentally.

Because Gaussian operations are experimentally accessible with present technology, a crucial question in the field of quantum information with continuous variables is to characterize which tasks can be implemented with Gaussian states and Gaussian operations only. We will see later in this manuscript that quantum key distribution for instance is possible in this framework (see Chapters 3-7) but that bit commitment is impossible (see Chapter 8).

Symplectic transformations. Because a Gaussian map transforms every Gaussian state into a Gaussian state, it is entirely characterized by its action on the displacement vector d and the covariance matrix γ. In particular, to any Gaussian unitary transformation is associated a symplectic operation $S \in \mathrm{Sp}(2N, \mathbb{R})$ which preserves the canonical commutation relations [7]. Note that the inverse of S is given by $S^{-1} = \sigma S^T \sigma^{-1}$. As a consequence of the Stone-von Neumann theorem, there exists a *unique* unitary transformation U_S associated to the real symplectic transformation S such that the Weyl operators satisfy $U_S \hat{D}(\xi) U_S^\dagger = \hat{D}(S\xi)$ for all $\xi \in \mathbb{R}^{2N}$.

In particular, a Gaussian state with displacement vector d and covariance matrix γ is sent under the action of U_S to the Gaussian state with displacement vector d' and covariance matrix γ' given by

$$d' = Sd \tag{2.90}$$

and

$$\gamma' = S\gamma S^T. \tag{2.91}$$

An important subset of all symplectic transformations is formed by orthogonal transformations. They are described by the compact group $K(N) = \mathrm{Sp}(2N, \mathbb{R}) \cap O(2N)$ whose elements correspond to *passive* operations that preserve the total photon number. These transformations will be exploited in Chapter 6 of this manuscript where we introduce a quantum de Finetti theorem that applies to states invariant under the action of the group $K(N)$. The operations of $K(N)$ can be implemented with phase shifts, beam splitters and homodyne detection only, that is excluding squeezers.

Let us now quickly describe the symplectic transformations corresponding to the different operations.
A *phase shift* is a single-mode operation equivalent to a rotation in phase space. It is characterized by a phase θ and the corresponding symplectic transformation $S_{\mathrm{PS}}(\theta) \in \mathrm{Sp}(2, \mathbb{R})$

$$S_{\mathrm{BS}}(T) = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}. \tag{2.92}$$

A *beam splitter* operation of transmittance T makes a coherent combination of two modes and is described by the symplectic transformation $S_{\rm BS}(T) \in {\rm Sp}(4,\mathbb{R})$

$$S_{\rm BS}(T) = \begin{bmatrix} \sqrt{T}\,\mathbb{1}_2 & \sqrt{1-T}\,\mathbb{1}_2 \\ -\sqrt{1-T}\,\mathbb{1}_2 & \sqrt{T}\,\mathbb{1}_2 \end{bmatrix}. \tag{2.93}$$

A single-mode *squeezing* transformation is parametrized by its squeezing factor r and is described by the symplectic transformation $S_{\rm Sq}(r) \in {\rm Sp}(2,\mathbb{R})$ given by

$$S_{\rm Sq}(r) = \begin{bmatrix} e^{-r} & 0 \\ 0 & e^{r} \end{bmatrix}. \tag{2.94}$$

A two-mode *squeezing* transformation is parametrized by its squeezing factor r and is described by the symplectic transformation $S_{\rm Sq2}(r) \in {\rm Sp}(4,\mathbb{R})$ given by

$$S_{\rm Sq2}(r) = \begin{bmatrix} \cosh r\,\mathbb{1}_2 & \sinh r\,\sigma_z \\ \sinh r\,\sigma_z & \cosh r\,\mathbb{1}_2 \end{bmatrix}. \tag{2.95}$$

Finally, the *Euler decomposition* of symplectic transformations says that any $S \in {\rm Sp}(2N,\mathbb{R})$ can be decomposed into

$$S = K \bigoplus_{k=1}^{N} \begin{bmatrix} e^{-r_k} & 0 \\ 0 & e^{r_k} \end{bmatrix} L, \tag{2.96}$$

where $K, L \in K(N)$ and $r_k \in \mathbb{R}$. The interpretation of this theorem is that any Gaussian map can be implemented as a first passive transformation followed by a single-mode squeezing operation of each of the N modes finally followed by a second passive transformation. Another important class of transformations is becomes particularly interesting in the multiparticle scenario where N modes can be distributed among different locations: the class of *local* operations which corresponds to the subset ${\rm Sp}(2,\mathbb{R})^N$ of ${\rm Sp}(2N,\mathbb{R})$. A particular example is given by the *standard form* of a two-mode covariance matrix: any two-mode Gaussian state with covariance matrix

$$\gamma_{12} = \begin{bmatrix} \gamma_1 & C_{12} \\ C_{12} & \gamma_2 \end{bmatrix}, \tag{2.97}$$

can be transformed by local Gaussian operations into a Gaussian state with covariance matrix γ'_{12} in the standard form:

$$\gamma'_{12} = \begin{bmatrix} a & 0 & c_+ & 0 \\ 0 & a & 0 & c_- \\ c_+ & 0 & b & 0 \\ 0 & c_- & 0 & b \end{bmatrix}. \tag{2.98}$$

Completely Positive maps. The most general transformations that can be applied to a state (including measurements) forms the set of Completely Positive (CP) maps. Gaussian CP maps are characterized by two $2N \times 2N$ matrices X and Y [41] that transform the initial displacement vector d_{in} and covariance matrix γ_{in} into d_{out} and γ_{out} respectively, which are given by

$$d_{\text{out}} = X\, d_{\text{in}} \tag{2.99}$$

and

$$\gamma_{\text{out}} = X\gamma_{\text{in}}X^T + Y. \tag{2.100}$$

Matrix Y is symmetric and the positivity of the map imposes the condition

$$Y + i\Omega - iX\Omega X^T \geq 0. \tag{2.101}$$

Let us now describe some important Gaussian channels: the lossy, amplification and thermal noise channels.
A *lossy channel* of transmittance T corresponds to $X = \sqrt{T}\mathbb{1}$ and $Y = (1-T)\mathbb{1}$. It can be modeled by combining the signal with the vacuum on a beam splitter of transmittance T for which the second output mode is traced out.
An *amplification* channel with amplification factor $\eta \geq 1$ corresponds to $X = \sqrt{\eta}\mathbb{1}$ and $Y = (\eta - 1)\mathbb{1}$. It can be modeled by injecting the input signal into a two-mode squeezed with a squeezing factor such that $\eta = \cosh^2 r$ for which the second output (idler mode) is traced out.
A *thermal noise channel* of transmittance T and excess noise ϵ corresponds to $X = \sqrt{T}\mathbb{1}$ and $Y = T\chi\mathbb{1}$ where χ is the added noise referred to the input

$$\chi = \frac{1-T}{T} + \epsilon. \tag{2.102}$$

It can be modeled by combining the signal and a thermal state of variance $V = T\chi/(1-T)$ on a beamsplitter of transmittance T.

At this point, it is interesting to give a possible implementation for the displacement operator in phase space. Let us consider the case of a single-mode displacement $\hat{D}(\alpha)$ with $\alpha = (\alpha_1, \alpha_2)$. The idea is to combine the signal mode with a large amplitude coherent state centered on $(\alpha_1/\sqrt{1-T}, \alpha_2/\sqrt{1-T})$ on a beam splitter of transmittance $T \to 1$. The two-mode Gaussian state composed of the signal mode and of this large amplitude is characterized by its displacement vector $d_{12} = (d_x, d_p, \alpha_1/\sqrt{1-T}, \alpha_2/\sqrt{1-T})$ and its covariance matrix $\gamma_{12} = \gamma \oplus \mathbb{1}_2$ where the signal mode has a displacement vector (d_x, d_p) and a covariance matrix γ. Using the beamsplitter transformation $S_{\text{BS}}(T)$ and tracing out the second mode, one obtains

$$\begin{pmatrix} d'_x \\ d'_p \end{pmatrix} = \sqrt{T}\begin{pmatrix} d_x \\ d_p \end{pmatrix} + \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} \tag{2.103}$$

and

$$\gamma' = T\gamma + (1-T)\mathbb{1}, \tag{2.104}$$

which effectively implements the displacement $\hat{D}(\alpha)$ in the limit $T \to 1$. Note that this procedure can immediately be generalized to an arbitrary number of modes.

2.2.3 Partial measurements

We now consider the general situation of a bipartite $(N_A + N_B)$-mode Gaussian state ρ_{AB} with displacement vector $d = (d_A, d_B)$ and covariance matrix

$$\gamma = \begin{bmatrix} A & C \\ C^T & B \end{bmatrix}, \tag{2.105}$$

Homodyne measurement. Suppose we perform an homodyne measurement on the B part of the state, and that the results of this measurement are given by $m = (x_1, 0, x_2, 0, \cdots, x_{N_B}, 0)$, then this homodyne detection projected the state ρ_A on the Gaussian state ρ'_A characterized by its displacement vector

$$d'_A = d_A + C(XBX)^{\mathrm{MP}}(m - d_B), \tag{2.106}$$

and its covariance matrix

$$A' = A - C(XBX)^{\mathrm{MP}}C^T, \tag{2.107}$$

where $X = \mathrm{diag}(1, 0, 1, 0, \cdots, 1, 0)$ keeps track of which quadratures were measured (a entry equal to 1 corresponds to the quadrature measured, all position quadratures were measured in this example), and MP refers to the inverse on the range [41].
A property of Gaussian states is that the final covariance matrix A' does not depend on the measurement results.

Heterodyne measurement. An heterodyne measurement consists in sending the state to be measured on a balanced beam splitter and then performing a different homodyne measurement for each output mode. With the same notations as above, the state ρ_A is projected on the Gaussian state ρ'_A characterized by its displacement vector

$$d'_A = d_A + \sqrt{2}C(B + \mathbb{1}_{2N_B})^{-1}(m - d_B), \tag{2.108}$$

and its covariance matrix

$$A' = A - C(B + \mathbb{1}_{2N_B})^{-1}C^T, \tag{2.109}$$

where $m = (x_1, p_1, \cdots, x_{N_B}, p_{N_B})$ is the result of the heterodyne measurement. As in the case of the homodyne measurement, we note that the covariance matrix of ρ'_A does not depend on the measurement results.

2.3 Quantum information with continuous variables

2.3.1 von Neumann entropy

In classical information theory, many problems arise for continuous variables. In particular, the Shannon entropy becomes ill-defined, and one has to replace it by the concept of differential entropy which is defined up to some additive constant. In contrast, the

situation is actually more favorable in a quantum context as a continuous-variable system can always be described in an infinite, but *countable* Hilbert space. More specifically, any N-mode quantum state of a continuous-variable system is described by its density operator

$$\rho = \sum_{\mathbf{m},\mathbf{n}=0}^{\infty} \rho_{\mathbf{m},\mathbf{n}} |m_1, \cdots, m_N\rangle\langle n_1, \cdots, n_N|, \tag{2.110}$$

where $\mathbf{m} = (m_1, \cdots, m_N)$ and $\mathbf{n} = (n_1, \cdots, n_N)$. Then the definition of the von Neumann entropy can be applied directly to a continuous-variable quantum system as

$$S(\rho) = -\mathrm{tr}\rho \log \rho. \tag{2.111}$$

This quantity is well defined provided that the sum converges. Actually, it turns out that this quantity diverges for almost all states in the Fock space. But this is not that big a deal as it always takes a finite value on the compact set of states with bounded energy [41], which is the set of interest for quantum information theory.

2.3.2 Entropy of Gaussian states

Our goal here is to compute the von Neumann entropy of a Gaussian state. First, one shows that the entropy of a N-mode Gaussian state ρ_G does not depend on its first moment. To see this, one just need to note that the entropy is invariant under a displacement operation (since it is a unitary operation). As a consequence, the entropy of a Gaussian state is entirely determined by the covariance matrix γ of the state. To be more specific, we use the Williamson theorem stating the existence of a symplectic transformation S such that

$$S\gamma S^T = \bigoplus_{k=1}^{N} \begin{bmatrix} \nu_k & 0 \\ 0 & \nu_k \end{bmatrix} \tag{2.112}$$

where the $\{\nu_k\}_{k=1,\cdots,N}$ are the symplectic eigenvalues of the state. Hence, according to Williamson's theorem, there exists a unitary operation mapping the Gaussian state ρ_G to a product of N thermal states with $\bar{n}_k = \frac{1}{2}(\nu_k - 1)$ photons in the mode k. Noting $\rho_{\mathrm{th}}(\bar{n})$ the single mode thermal state with a mean photon number $\bar{n}$, one has:

$$S(\rho_G) = \sum_{k=1}^{N} S(\rho_{\mathrm{th}}(\bar{n}_k)). \tag{2.113}$$

Entropy of a thermal state. We now explicitly compute the von Neumann entropy of a thermal state. The density operator of a single-mode thermal state ρ_{th} is given by:

$$\rho_{\mathrm{th}} = \sum_{n=0}^{\infty} \frac{\bar{n}^n}{(\bar{n}+1)^{n+1}} |n\rangle\langle n|, \tag{2.114}$$

where $\bar{n} = \mathrm{tr}(\rho n)$ is the mean number of thermal photons in the state. Let us now compute the von Neumann entropy of this state ρ:

$$\begin{aligned} S(\rho_{\mathrm{th}}) &= -\mathrm{tr}\rho_{\mathrm{th}} \log_2 \rho_{\mathrm{th}} && (2.115)\\ &= -\frac{1}{\bar{n}+1} \sum_{k=0}^{\infty} \left(\frac{\bar{n}}{\bar{n}+1}\right)^k \log_2 \left[\frac{1}{\bar{n}+1}\left(\frac{\bar{n}}{\bar{n}+1}\right)^k\right] && (2.116)\\ &= -\frac{1}{\bar{n}+1} \sum_{k=0}^{\infty} \left(\frac{\bar{n}}{\bar{n}+1}\right)^k \left[-\log_2(\bar{n}+1) + k \log_2 \frac{\bar{n}}{\bar{n}+1}\right]. && (2.117) \end{aligned}$$

Then using the following identity,

$$\sum_{k=0}^{\infty} k x^k = \frac{x}{(1-x)^2}, \tag{2.118}$$

one finally gets:

$$S(\rho_{\mathrm{th}}) = (\bar{n}+1)\log_2(\bar{n}+1) - \bar{n}\log_2 \bar{n}. \tag{2.119}$$

2.3.3 Extremality of Gaussian states

We already saw that Gaussian states play a central role among continuous-variable quantum systems as they are at the same time relatively easy to generate experimentally, and easy to analyze. The main reason why they can be studied from a theoretical point of view is that they really are finite-dimensional systems in the sense that they are completely characterized by a number of parameters only quadratic in the number of modes N. For instance, the entropy of a Gaussian state can be computed from its covariance matrix only, as a function of the symplectic spectrum.

For most non Gaussian states, the situation is much more complicated and computing the von Neumann entropy implies to compute the spectrum of the infinite-dimensional density operator, which is almost always an intractable problem. Quite interestingly, Gaussian states are extremal with respect to various functionals. In particular, the state of maximal entropy for fixed first and second moments is Gaussian [76] (as in the classical case). This is a consequence of the following theorem:

Theorem 2.2 (Extremality of Gaussian states [158])**.** *Let $f : \mathcal{B}(\mathcal{H}^{\otimes N}) \to \mathbb{R}$ be a continuous functional, which is strongly sub-additive and invariant under local unitaries $f(U^{\otimes N}\rho U^{\dagger\otimes N}) = f(\rho)$. Then for every density operator ρ describing an N-partite system with finite first and second moments, we have that*

$$f(\rho) \leq f(\rho^G), \tag{2.120}$$

where ρ^G is the Gaussian state with the same first and second moments as ρ.

This theorem allows one to prove that Gaussian states are extremal for the von Neumann entropy as well as for various entanglement measures, or channel capacities [158]. In Chapter 3, we will show that, in the context of continuous-variable QKD, Gaussian states are extremal for the functional corresponding to the secret key rate secure against collective attacks.

2.3.4 Possible tasks and no-go theorems for Gaussian states with Gaussian operations

Quantum information theory began roughly 25 years ago when Bennett and Brassard noticed that quantum mechanics allowed us to perform a task impossible in the classical world, namely, distributing secret keys among distant parties with unconditional security. Since this striking discovery, the main goal of the field has been to study the frontier between the quantum and the classical worlds from an information theoretic point of view: what are the tasks impossible in the classical world that become possible in the quantum world, and *vice versa*?

In 2009, the frontier has not yet been completely uncovered or understood but quite a few differences have already been established. Key distribution and teleportation are compatible with quantum mechanics but not with any classical theory. It is the opposite situation for the task of *cloning* information: cloning classical information is not forbidden by any *physical* law, whereas cloning quantum information is. Bit commitment is impossible both for classical and quantum theories.

It is not known whether continuous-variable quantum mechanics is more or less powerful than discrete-variable quantum mechanics, but there probably are no differences between the two models. A much more interesting question, however, is to study what can or cannot be done with Gaussian states and Gaussian operations only. One of the main motivations for this question is that it concerns operations that could be relatively easily implemented, in sharp contrast with a generic operation on a continuous-variable quantum system. In this manuscript, we study two such questions, namely the possibility of Gaussian quantum key distribution and the impossibility of Gaussian quantum bit commitment. Note that put together, they give a convincing (and very natural) counter example for Brassard and Fuchs conjecture that quantum mechanics could be rederived from the principles that key distribution should be possible but not bit commitment [16]. We discuss these results in more details in Chapter 8.

Being more restricted that quantum mechanics, it is not surprising that several other no-go theorems have been established for Gaussian states and Gaussian operations. One could cite a no-go theorem for entanglement distillation [42] and a no-go theorem for quantum error correction [110]: this means that it is impossible to distill entanglement or to perform error correction in a context where one is restricted to Gaussian states and can only perform Gaussian operations.

Finally, one important feature of Gaussian states is that they are compatible with a *Local Hidden Variable* (LHV) model as their Wigner function is everywhere positive and thus corresponds to a genuine probability distribution. For this reason, it is impossible to violated a Bell inequality with Gaussian states and Gaussian operations only. As a consequence, there is not either any hope to devise a *device-independent* QKD scheme in this restricted context.

2.3.5 Gaussian states: Hilbert space versus phase space representation

As a conclusion for this chapter, we summarize the description of Gaussian states in Hilbert space and phase space representations on Table 2.1 (from [4]).

	Hilbert space $\mathcal{H}$	Phase space Γ
dimension	∞	2N
structure	$\otimes$	$\oplus$
description	ρ	γ
bona fide	$\rho \geq 0$	$\gamma + i\Omega \geq 0$
operations	$U : \begin{cases} U^\dagger U = \mathbb{1} \\ \rho \mapsto U\rho U^\dagger \end{cases}$	$S : \begin{cases} S^T \Omega S = \Omega \\ \gamma \mapsto S\gamma S^T \end{cases}$
spectra	$U\rho U^\dagger = \mathrm{diag}\{\lambda_k\}$ $0 \leq \lambda_k \leq 1$	$S\gamma S^T = \mathrm{diag}\{\nu_k\}$ $1 \leq \nu_k \leq \infty$
pure states	$\lambda_i = 1, \lambda_{j\neq i} = 0$	$\nu_j = 1, \forall j \in \{1, \cdots, N\}$
purity	$\mathrm{tr}\rho^2 = \sum_k \lambda_k^2$	$1/\sqrt{\det\gamma} = \prod_k \nu_k^{-1}$

Table 2.1: Gaussian states: Hilbert space versus phase space representation (from [4]).

CHAPTER 3

Quantum Key Distribution

Quantum key distribution (QKD) is a cryptographic primitive that allows two distant parties, Alice and Bob, to distill a secret key[1]. Key distribution is an essential primitive required to perform (classical) *symmetric cryptography*. Once solved, Alice and Bob, can communicate with unconditional security thanks to one-time pad[2]. Unconditional security, also referred to as *information-theoretic security* means that an adversary cannot learn anything about the message except with negligible probability. What makes QKD remarkable is that it has no classical equivalent.

[1] more importantly, as the first application of quantum information theory, it led to an impressive development of this new scientific research field, which might have been overlooked without the discovery of QKD.

[2] one-time pad, where the encryption and decryption simply consist in taking the XOR of the message and the secret key, is actually proven to be optimal as there does not exist any cryptographic scheme which requires a smaller key while guaranteeing perfect security. Note that in order to be optimal, the message M to be sent should first be compressed so that its length becomes equal to its entropy. Thus the minimal size of the key is given by the entropy of the message Alice and Bob want to exchange. In particular, a given key can only be used once.

3.1 Quantum Key Distribution

Our goal here is not to give a complete review of quantum key distribution. Such reviews can be found in the following books intended for general audience [87, 134] or in more technical review articles [53, 136] or books [153]. Let us however present the basic principle of a QKD protocol.

Two honest distant parties, usually referred to as Alice and Bob, wish to establish a key that remains secret from any adversary, usually named Eve. For this task, Alice and Bob have access to two channels: a quantum channel, *a priori insecure* and potentially completely controlled by Eve, and an *authenticated* classical channel. Authentication means that Eve can listen to the conversation on the classical channel but cannot participate to it: in other words, Eve cannot pretend to be either Alice or Bob. Such an assumption is not required concerning the quantum channel. A QKD protocol will be said to be *secure* if it does not generate non-secret keys. Hence, either the legitimate parties distill a secret key or they abort the protocol. Obviously, the trivial protocol that never generates any key is secure from this point of view, but not really interesting. Let us now give a more precise definition of the security of a key.

3.1.1 Security of a key

A key is a tool given to distant parties that they will use in an application, typically symmetric cryptography (not necessarily limited to one-time pad). As a consequence, one needs a definition for the security of the key that does not directly depend on the specific application it will be used for. This means that we require a *universal* definition of security. Such a definition was not available until recently[3]. The universal definition of security which we use in the following was introduced in Renato Renner's PhD thesis [124] and is characterized by the distance between the key S output by the protocol and a perfect key. Following the notations of [124], we describe the joint state of the classical key S and the adversary's quantum system[4] as

$$\rho_{SE} := \sum_{s\in\mathcal{S}} P_S(s)|s\rangle\langle s| \otimes \rho_E^s. \tag{3.1}$$

This expression means that the key S is a random variable following the probability distribution P_S, and that the state of the adversary given that $S = s$ is described by the density matrix ρ_E^s of the Hilbert space $\mathcal{H}_E$. The family $\{|s\rangle\}_{s\in\mathcal{S}}$ is an orthonormal basis for the Hilbert space $\mathcal{H}_S$ of the key[5]. Equipped with this description of the joint state of the key and the adversary, we can now define the security of a key: the key S is *ϵ-secure*

[3] until then, security was often characterized in terms of accessible information. This definition, however, was not *composable* [85] as a small accessible information is not a sufficient requirement to insure that the key can be securely used in one-time pad for instance.

[4] this is by no means a restriction as even a classical adversary can be described without loss of generality as a quantum adversary.

[5] the use of such an orthogonal basis is the usual way to represent a classical system in a quantum setting as we consider only mixtures (and never superposition) of the basis elements.

with respect to $\mathcal{H}_E$ if

$$\frac{1}{2}||\rho_{SE} - \rho_S \otimes \rho_E||_1 \leq \epsilon, \tag{3.2}$$

where $\rho_S = \sum_{s\in\mathcal{S}} \frac{1}{|\mathcal{S}|}|s\rangle\langle s|$ is the completely mixed state on the set S of possible final keys and ρ_E is any state of Eve. Put otherwise, a QKD protocol is ϵ-secure if the keys computed by Alice and Bob are

- identical,
- uniformly distributed,
- independent from the adversary's knowledge,

except with some small probability ϵ.

3.1.2 QKD protocols

A general QKD protocol consists of different steps:

- Alice and Bob start with the *quantum distribution*. This first step, which is at the core of the QKD protocol, will be detailed below, but the important point is that, at the end of it, we can assume that Alice and Bob share N bipartite quantum systems described in $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes N}$. More precisely, this is true in the *entanglement-based* version of the protocol. In practice, however, the distribution often consists for Alice to send N states to Bob through the quantum channel. In this case, the action of the quantum channel can be represented by a CPTP map on the states. As we saw in Chapter 1, the two pictures can be made equivalent, and it turns out that the analysis of a QKD protocol is often more simple in the entanglement-based version.
- Alice and Bob then sacrifice some $m \equiv N - n$ subsystems in order to perform a *parameter estimation*. This is achieved by performing measurements on m random subsystems and then publicly announcing the results on the authenticated public channel. At this point, Alice and Bob can estimate the level of correlation of their quantum subsystems, and decide either to proceed with the remaining of the protocol or to abort the protocol if the correlation is too low for a secret key to be distillable.
- Alice and Bob measure their n remaining quantum systems[6] and obtain a pair of *raw keys* X^n and Y^n. Typically, X^n and Y^n are only partially correlated and are not secure (i.e. they are not totally decoupled from the adversary quantum state). The rest of the QKD protocol aims at solving these two problems: first by letting Alice and Bob agree on an identical bit string, then by processing this bit string to establish a shorter string that will be secure.

[6] usually, this phase is performed at the same time as parameter estimation, but the data are only used once the parameter estimation is complete. This relieves the need for quantum memories which are still quite impractical with today's technology.

- Alice and Bob proceed with the *reconciliation* of their raw keys: using communication on the authenticated classical channel, they agree on a common bit-string U^n. Usually, for most discrete-variable (DV) QKD, schemes, Alice sends some side-information to Bob to help him recover the value of X^n[7]: in this case $U^n = X^n$. For continuous-variable (CV) protocols, the situation is a little bit more involved. First, it is advantageous to perform a *reverse reconciliation* [64] in place of a direct reconciliation, meaning that the classical communication only goes from Bob to Alice in the reconciliation phase. Then, Y^n is a random variable taking values on $\mathbb{R}^n$ and not on $\{0,1\}^n$. As the final key has to be a bit string, the output U^n of the reconciliation is also chosen to be a bit string[8]. Thus, for CV QKD, U^n is usually a bit string computed from Y^n, i.e, there exists a function $f : \mathbb{R}^n \to \{0,1\}^n$ such that $U^n = f(Y^n)$. Examples of such functions f will be described in Chapters 4 and 5.

- Finally, Alice and Bob need to turn U^n into a secure key of length l. This is achieved through *privacy amplification*. Typically, this is done thanks to two-universal hashing.

There exist two main families of QKD protocols whose distinction lies in the quantum distribution part: *Prepare and Measure* (P&M) protocols and *Entanglement-Based* (E-B) protocols. E-B protocols involve the actual distribution of N bipartite systems between Alice and Bob, whereas this distribution is only *virtual* for P & M protocols. More precisely, a quantum distribution is also required in P & M protocols, but only single-party systems are sent from Alice to Bob: no entanglement in particular is necessary in such a scenario.

P & M protocols are the easiest ones to implement, and were the first protocols introduced in the literature [10]. Alice prepares N random states and sends them to Bob through the quantum channel. Bob proceeds by measuring these states in a random basis. For a protocol to be secure, the family of states used by Alice and Bob should contain non-orthogonal states otherwise one can always find a measurement that allows to distinguish them perfectly. If there are non-orthogonal states however, one cannot deterministically distinguish them. In particular, an eavesdropper willing to measure the states sent by Alice to Bob will disturb them with a non-negligible probability. More precisely, there exists a trade-off between the information acquired by Eve on the state sent by Alice and the level of correlation between the states sent by Alice and the states received and measured by Bob. This trade-off, which is a purely quantum effect, is at the origin of the possibility of QKD. For a similar reason, it is also necessary for a QKD

[7] in reality Bob computes a guess $\hat{X}^n$ of X^n.

[8] choosing U^n to be a bit string is certainly a simplifying hypothesis. To our knowledge, alternatives where U^n would be described with a larger alphabet have not been considered in the literature and it is not clear whether there would be any potential advantage to do so. Anyway, it does not seem reasonable for U^n to be a truly continuous variable as the precision of the electronic equipment used in a CV QKD protocol is always finite and only a finite number of bits is required to describe Y^n. However, the question whether privacy amplification can be performed by taking real random values as an input might be an interesting theoretical question on its own right.

protocol to be secure that Bob performs randomly different measurements. Indeed, if Bob were always to perform the same (projective) measurement, Eve could just apply the same measurement and send back to Bob the state she measured. In this case, Bob and Eve would share exactly the same data, and no secret key could be extracted this way.

In an E-B protocol, the situation is a little bit different. A source of quantum bipartite states is used to distribute correlations to Alice and Bob. This idea was first formulated by Ekert in [43]. Alice and Bob proceed with measuring the states they receive with random measurements. Again, it is crucial that Alice and Bob use at least two incompatible measurements in order to prevent Eve to always apply the correct measurement. Such an E-B protocol is clearly less practical than a P & M protocol as a source of entangled states is required for the protocol to work. Note that entanglement is necessary and that bipartite separable states are not sufficient to perform QKD with an E-B protocol.

While being conceptually quite different, it appears that E-B and P & M protocols are in fact equivalent from a theoretical point of view. In particular, they are (theoretically) equally secure. We now prove that any P&M protocol can be associated with an equivalent E-B protocol. Let us consider a generic P&M protocol where Alice sends the (pure) state $|\phi_k\rangle_B$ to Bob with probability p_k for $k \in \{1, \cdots, K\}$. This is equivalent to an E-B protocol where Alice produces the following state $|\psi\rangle_{AB}$:

$$|\psi\rangle_{AB} = \sum_{k=1}^{K} \sqrt{p_k}|k\rangle_A|\phi_k\rangle_B \tag{3.3}$$

where the family $\{|k\rangle\}_{k\in\{1,\cdots,K\}}$ forms an orthogonal basis of the Hilbert space $\mathcal{H}_A$. Then Alice can simply perform the projective measurement $\{|1\rangle\langle 1|, \cdots, |K\rangle\langle K|\}$ on $\mathcal{H}_A$. She will obtain the result k with probability p_k, thus effectively preparing the second half of the state in $|\phi_k\rangle_B$. From Eve and Bob's points of view, this E-B scheme is genuinely undistinguishable from the original P&M protocol. For this reason, the two protocols share the same security properties and the security of the P&M protocol can be established by considering the one of the E-B protocol.

However, the practical implementations of both schemes are rather different, and E-B protocols *might* be more resistant to potential side-channels, which are basically discrepancies between the theoretical model and the practical implementation. More precisely, a *side-channel* is present each time that some information about the raw key is encoded in degrees of freedom not considered in the theoretical model. This amounts to wrongly assess the dimension of the relevant Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ describing the protocol. For instance, if different lasers are used to generate the different states sent by Alice in a P&M protocol, these lasers should be in principle rigorously identical. It might unfortunately be the case that they have a slightly different wavelength, in which case the eavesdropper can use a grating to distinguish the different wavelengths and acquire a complete information about the state sent by Alice without destroying information in a noticeable way for Alice and Bob. Other potential side-channels exist besides frequency, for instance the timing of the detectors. Usually, there exists a counter-measure for each side-channel, but it is difficult to be sure that every possible side-channels are taken into

account in a given implementation (see the "Black paper of quantum cryptography" [135] for a more detailed discussion). The bottom-line is that one cannot in principle prove that all side-channels are taken into account in a P&M protocol whereas it might be the case in some E-B protocols, in particular, for device-independent protocols [1, 119].

Hence, one should be careful when using the equivalence between P&M and E-B protocols. A fundamental hypothesis in order to write $|\psi\rangle_{AB}$ is that the number of different states sent by Alice in the P&M version is indeed K. This hypothesis is unfortunately not valid as soon as there are side-channels not accounted for. In this case, the state given by Eq. 3.3 does not correspond to an effective purification of the experimental P&M protocol, and the security proof becomes consequently invalid. The idea behind device-independent cryptography is to use properties that are independent of the dimension of $\mathcal{H}_A \otimes \mathcal{H}_B$ to prove that the correlations of Alice and Bob can be use to extract some secret. Such a dimension-independent property is for instance given by the violation of a Bell inequality.

To summarize the principle of a QKD protocol, Alice and Bob exchange non orthogonal quantum states, thus preventing an adversary from measuring them without introducing some errors, that is, some noise. If this noise level is sufficiently low (as determined in the parameter estimation phase), then with high probability, Alice and Bob quantum states (or data) or more correlated than with the eavesdropper quantum states. In information-theoretic terms, this means roughly that the mutual information between Alice and Bob is provably higher than the mutual information between Eve and either Alice or Bob. Then, using a reconciliation procedure and a privacy amplification step, it is possible to distill a secret key (i.e. a bit string shared by Alice and Bob which appears to be uniform from anybody else's point of view, except with a probability ϵ for an ϵ-secure key). For this reason, any sensible QKD protocol works for a certain regime of noise[9], which is in sharp contrast with the situation of cryptographic protocols such as bit commitment for instance where no scheme can actually work (see Chapter 8 for a discussion about quantum bit commitment). Obviously, the real challenge is to link the correlations between Alice and Bob to an upper bound on the eavesdropper information. For this reason, only a few QKD protocols have be proven unconditionally secure[10]. Quite fortunately, these protocols turn out to be efficient and practical. The formalism used to prove the security of QKD was mainly introduced by Renato Renner [124]. We now give a quick overview of this formalism.

3.2 Security analysis of QKD

Here we briefly present the general formalism which allows for a derivation of the secret key rate of a given QKD protocol. We use the same notations than before and note l the size of a secret key and N the number of quantum signal exchanged during the protocol.

[9] In fact, it was proven by Bennett [12] that any two non-orthogonal states were sufficient to allow for secure QKD.

[10] In general, these are very simple protocols displaying a fair amount of symmetries.

Thus, the *secret key rate* K is just the ratio between these two quantities:

$$K \equiv \frac{l}{N}. \tag{3.4}$$

Note that this convention is as general as possible, and is compatible with a *finite-size analysis*. A more restricted scenario is concerned with *asymptotic analysis* for with one can define an asymptotic secret key rate K^{asympt}:

$$K^{\text{asympt}} \equiv \frac{l}{n}, \tag{3.5}$$

where n is the size of the raw key (that is once parameter estimation and possibly sifting[11] have been done).

Here, we restrict the analysis to *one-way post-processing* consisting of *reconciliation* and *privacy amplification*. In such protocols, the reconciliation scheme must be unidirectional[12]: it can be either *direct*, in which case Alice will help Bob correct his errors and guess the value of X^n which will be used for privacy amplification, or *reverse* in which case Alice and Bob's roles are inverted. In the following, we use the notations for reverse reconciliation as it is the one relevant for continuous-variable QKD.

The formula for the number of ϵ-secure secret key bits l was established in [124] and is given by

$$l = H_{\min}^{\bar{\epsilon}}(Y^n|E^n) - \text{leak}_{\text{rec}} - 2\log_2 \frac{1}{2(\epsilon - \bar{\epsilon} - \epsilon_{\text{rec}})}, \tag{3.6}$$

for some $\bar{\epsilon} \geq 0$. In this expression, leak_{rec} corresponds to the number of bits carrying information about Y^n that need to be transmitted over the public channel during the reconciliation procedure, and ϵ_{rec} is the failure probability of the reconciliation, that is, the probability that Alice makes a wrong guess about Y^n.

Thus, the secret key rate of a QKD protocol is known as soon as one can estimate the smooth min-entropy $H_{\min}^{\bar{\epsilon}}(Y^n|E^n)$. Unfortunately, this turns out to be a rather complicated task, and one usually prefers to consider the much simpler problem where one restricts the adversary to perform *collective attacks*. For such a collective attack, the bipartite state $\rho_{A^N B^N} \in (\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes N}$ takes a simple form:

$$\rho_{A^N B^N} = \int \mathrm{d}\sigma_{AB}\, p(\sigma_{AB})\, \sigma_{AB}^{\otimes N}, \tag{3.7}$$

[11] *Sifting* corresponds to the action of discarding the data that have been measurement in incompatible bases by Alice and Bob.

[12] Note that one-way post-processing, which simplifies the security proofs of most QKD protocols, and is even required for some continuous-variable schemes, was not used in early implementations of QKD protocols. In particular, the reconciliation step would often be *interactive* meaning that Alice and Bob would alternatively send information to each other to correct the discrepancies between their classical data. Such a reconciliation protocol used the algorithm "Cascade" developed in 1994 by Brassard and Salvail [19]. One-way reconciliation protocols were introduced more recently, especially in the context of continuous-variable QKD [14, 91, 89] and make an intensive use of powerful error correction techniques such as low-density parity-check (LDPC) codes [132]. Such codes can also be of benefice for discrete-variable QKD as they perform better than Cascade for most relevant situations [44].

where $p(\sigma_{AB})$ is a probability distribution on $\mathcal{H}_A \otimes \mathcal{H}_B$. Such a state is called an *independent and identically distributed* (i.i.d.) state. It turns out that the assumption of collective attacks, in addition to be mathematically convenient, is actually quite reasonable from the security point of view. It can indeed be shown that for most QKD protocols, collective attacks are *optimal* in the asymptotic regime. The interested reader is referred to Chapter 6 for a more detailed description of the relation between general (coherent) attacks and collective attacks.

In the case of a collective attack, the quantity $H_{\min}^{\bar{\epsilon}}(Y^n|E^n)$ can be lower bounded by [124]:

$$H_{\min}^{\bar{\epsilon}}(Y^n|E^n) \geq n \left(\min_{\sigma_{\bar{Y}\bar{E}} \in \Gamma} S(\bar{Y}|\bar{E}) - (2H_{\max}(\rho_Y) + 3)\sqrt{\frac{\log_2(2/(\bar{\epsilon} - \bar{\epsilon}')/2)}{n}} \right), \quad (3.8)$$

for any $\bar{\epsilon} \geq \bar{\epsilon}'$. In this formula, Γ is a set of quantum states compatible with the statistics obtained during the parameter estimation procedure, except with probability $\bar{\epsilon}'$. Characterizing the set Γ is the challenging task required for a finite-size analysis of the security of QKD. Until recently, people preferred to consider the asymptotic analysis where Γ is a set of measure 0 supposed to be perfectly known. Unfortunately, this assumption is quite strong and not justified for actual implementations. This has led to pessimistic results concerning the real security of QKD implementations [137]. A finite-size analysis of continuous-variable QKD can be found in Chapter 7 of this manuscript.

Let us now consider the security of QKD against collective attacks in the asymptotic limit. In this case, the leakage $\text{leak}_{\text{rec}}/n$ per symbol can become arbitrarily close from the Shannon limit $H(Y|X)$ given by the channel coding theorem. As a consequence, in this scenario, one recovers the result of Devetak and Winter [38]:

$$K_{\text{coll}}^{\text{asymp}} = S(Y|E) - H(Y|X), \quad (3.9)$$

which can also be written as

$$K_{\text{coll}}^{\text{asymp}} = I(X;Y) - S(Y;E) \quad (3.10)$$

where $S(Y;E)$ is the Holevo information between the classical variable Y and the quantum state ρ_E if the adversary.

With the exception of Chapters 6 and 7, we are mainly interested in the asymptotic secret key rate secure against collective attacks in the manuscript. For this reason, when the context is clear, we shall note this quantity K instead of $K_{\text{coll}}^{\text{asymp}}$. Another remark concerning notations is that the classical variable resulting from Alice's (resp. Bob's) measurement is noted either X or a (resp. Y or b).

3.3 Continuous-variable QKD

The idea of continuous-variable QKD is to use a different support of information to encode the key: instead of working in the Bloch sphere of a two-level system[13], one

[13] or any low-dimensional generalization

prefers to exploit degrees of freedom in *phase space*. The main consequence of this choice is that CV QKD and DV QKD involve different measurement stages: homodyne (or heterodyne[14]) for continuous-variable protocols instead of photon counting techniques for discrete-variable protocols. The main advantage of CV QKD is thus to use only standard telecom components (such as PIN photodiodes) that are much more mature from a technological point of view than single photon detectors whose primary use is QKD. A review on continuous-variable QKD can be found in [26].

3.3.1 General presentation of continuous-variable protocols

The idea of CV QKD is to encode information in phase space. To do so, Alice and Bob will exchange quantum states whose Wigner functions are peaked near specific values in phase space. Indeed, in a Prepare & Measure protocol, Alice will send states from a family $\{|\phi_1\rangle, \cdots, |\phi_K\rangle\}$ with K possibly equal to $+\infty$ such that the Wigner function of $|\phi_k\rangle$ is peaked around the complex value $\alpha_k \in \mathbb{C}$. Depending on whether Bob performs an homodyne or an heterodyne detection, he will have access to an estimate of $\mathrm{Re}(\alpha_k)$, $\mathrm{Im}(\alpha_k)$ or both values. Many families of quantum states satisfy this condition. However, an important requirement for a QKD protocol is to be practical. In particular, the quantum states $|\phi_k\rangle$ should be easy to generate. For this reason, the states usually considered are *Gaussian* states:

- *coherent* states $|\alpha\rangle$ which are the states of minimum uncertainty around their mean $\alpha \in \mathbb{C}$,
- *squeezed* states which can be chosen to have a well-defined quadrature (at the expense of the other quadrature).

It would seem that squeezed states are well suited for protocols involving a homodyne detection whereas coherent states are more natural for protocols with a heterodyne detection. Fortunately, it turns out that coherent states (that are much easier to generate than squeezed states) are also compatible with protocols involving only a homodyne detection (which is at least twice as easy to implement than a heterodyne detection!). Historically, squeezed states were considered for CV QKD as they were facilitating the derivation of security proofs, but they are not used anymore as QKD schemes based on squeezed states are not practical enough. For this reason, in the following, we only consider QKD protocols encoding information on coherent states.

There are two families of CV QKD protocols (using coherent states) but the distinction between them somewhat drifted during the last few years. To be more precise, a *family* of CV QKD protocols is characterized by a specific theoretical framework that can be used to study the security of the protocols in question. In particular, some proof

[14] in the context of CV QKD, an heterodyne detection refers to a simultaneous measurement of both quadratures of an optical mode in phase space. Obviously, such a measurement is forbidden by quantum mechanics, but can nevertheless be implemented at the cost of adding 3 dB of noise: a balanced beamsplitter is used to send the two halves of the signal to two homodyne detection stages, each of which measuring a different quadrature.

techniques can be used to compute the secret key rates of some but not all CV QKD protocols. Until recently, the border between the two classes of CV QKD protocols was concerned with the modulation: some protocols use a Gaussian modulation whereas other use a discrete modulation[15]. The reason for it is that a specific framework had been developed to study protocols with a Gaussian modulation, and that protocols with a discrete modulation did not seem to be compatible with this framework. However, we recently managed to analyze protocols with a discrete modulation within this framework (see [93] and Chapter 5 of this manuscript for details), thus erasing the frontier between the two kinds of protocols. It is interesting to note that not all CV QKD protocols can yet be analyzed within this framework. This thus gives rise to a new distinction, specifically between protocols using or not a postselection procedure[16]. In this manuscript, we will restrict ourselves to protocols without postselection.

Before going further in the description of CV QKD protocols, let us emphasize that there are two types of results (or bounds) one could be interested in:

- lower bounds on the secret key rate: such bounds are the most pessimistic and give a conservative estimate of the secret key rate.

- upper bounds on the secret key rate which are derived for a specific attack. Such bounds study the security against particular attacks, and do not guarantee unconditional security.

The ultimate goal is obviously to have the two kinds of bounds coincide. This would mean that the optimal attack against a protocol is known and that tight bounds on the secret key rate are established. In the case of CV QKD with a Gaussian modulation, an heterodyne detection and without postselection procedure for instance, the (known) upper and lower bounds only coincide in the case of individual attacks [98, 151].
In this manuscript, we are mainly concerned with lower bounds on the secret key rate.

3.3.2 A brief history of CV QKD protocols: from EPR states to coherent states

Before starting the study of CV QKD and especially its security, it is interesting to give an historical perspective.

The first QKD protocols were all designed to work with single photons. However, as such states are not very easy to produce, they were quickly replaced by attenuated coherent states as a first approximation. An interesting question was then to see if specific QKD protocols could be built to intrinsically work with such states. Because

[15] obviously, for any practical implementation, any modulation scheme only uses a finite number of states. This is due to the limited precision of both the random number generators and the modulators. However, in this case, the number of possible inputs is much larger than the one for a discrete-modulation scheme which usually requires 2 or 4 different coherent states.

[16] *Postselection* refers to the fact that Alice and Bob might discard some of their data in the case where they fail to satisfy some condition. Such a condition might be that the result of Bob's homodyne detection should have an absolute value greater than some predetermined threshold.

coherent states are not orthogonal, it was known that the answer was positive [12], but how practical such schemes might be was unknown.

The first proposals for continuous-variable QKD were based on EPR-like entanglement [122], [123] [9], [107], [143] and consequently not very practical. Other ideas concerned P&M protocols [70], [58] which used a discrete modulation and [27] with a Gaussian modulation. Note that [27] was the first paper to introduce a protocol where Bob performs an homodyne detection and uses the variance of the excess noise to upper bound Eve's information thanks to Shannon information theory with continuous variables. This technique was using results concerning cloning machines for continuous variables [25]. Unfortunately, these protocols were all relying on squeezed states which are still significantly harder to generate than coherent states. In particular, the secret key rate of the protocol [27] drops to 0 in the limit where the squeezing disappears.

The first protocol which made used of coherent states was introduced in 2002, and the main new idea consisted in modulating both quadratures simultaneously [64]. In this protocol, Alice sends coherent states modulated with a Gaussian distribution to Bob who chooses randomly to perform an homodyne detection on either one of the quadratures.

This protocol, while being much more practical than previous proposals, still suffered from an important drawback: it was limited to losses below 3 dB. Indeed, for higher losses, Eve's knowledge concerning Alice's state is necessary higher than Bob's knowledge, thus preventing the distillation of any secret. This 3 dB limit was beaten the following year by two new proposals: reverse reconciliation [60], [61] and postselection [144]. Reverse reconciliation means that the secret key is derived from Bob's measurement results instead of Alice's. Postselection consists for Alice and Bob to discard some data that are too noisy, and thus only keep the data for which Eve was unsuccessful to acquire more information than Bob.

3.3.3 The GG02 protocol

There are many continuous-variable QKD protocols being studied today. These protocols can all be seen as variations around the GG02 protocol, which was the first protocol using coherent states only. In the following, we call GG02 the protocol where reverse reconciliation is used. We now give a detailed description of this protocol.

The GG02 protocol

1. Alice draws $2N$ random variables according to a centered normal distribution with variance V_A:
$$q_1, p_1, \cdots, q_N, p_N \sim \mathcal{N}(0, V_A). \tag{3.11}$$
Then, she sends the N coherent states $|q_1 + ip_1\rangle, \cdots, |q_n + ip_N\rangle$ to Bob through the quantum channel.

2. For each state, Bob randomly chooses a quadrature q or p and performs an homodyne detection along this quadrature. He obtains N classical variables $y_1, \cdots, y_N$. Bob informs Alice of his choice of quadratures. Alice keeps only the relevant data for each state, either q_i or p_i and notes it x_i. At this points, Alice and Bob share N couples of correlated classical variables $(x_1, y_1), \cdots, (x_N, y_N)$.

3. Alice and Bob randomly choose a subset of m indices $\{i_1, \cdots, i_m\} \in \{1, \cdots, N\}$ and reveal publicly there corresponding data $(x_{i_1}, y_{i_1}), \cdots, (x_{i_m}, y_{i_m})$. From these data, they perform a parameter estimation for the transmission T and the excess noise ξ of the quantum channel. More precisely, the parameter estimation allows Alice and Bob to upper bound Eve's information (see Chapter 7).

4. After the estimation phase, Alice and Bob still share two n-dimensional correlated vectors X and Y where $n = N - m$.

5. In the *reverse reconciliation phase*, the goal is for Alice and Bob to agree on a common bit string U. This reconciliation is achieved thanks to error correction techniques very similar to those that are widely used in the telecom industry. A subtlety here is that the reconciliation is *reverse*, meaning that only Bob can send classical information to Alice. This is precisely one of the difficulties of continuous-variable QKD. This problem is extensively addressed in Chapters 4 and 5.

6. After the reconciliation step, Alice and Bob share a common binary vector U. Obviously, U is not completely secret and does not constitute a secret key. The extraction of the key is done through the final step of the protocol which is the *privacy amplification*. This step is the same as for any other QKD protocol, thanks to two-universal hashing: Alice and Bob choose randomly a hashing function that takes U as input and outputs a secure key of size l (where l is the secret key size computed thanks to the parameter estimation).

Variations around the GG02 protocol. There are many ways to tweak the GG02 protocol in order to potentially improve performances. We now discuss such possible variations

Modulation. In the original GG02 protocol, Alice uses a Gaussian modulation. Some alternative protocols consider a discrete modulation. In Chapter 5, we will see that a dis-

crete modulation can be beneficial as the reconciliation procedure is simplified. However, the security proofs are specifically designed for a Gaussian modulation and generalizing these proofs for protocols with a discrete modulation was one of the achievements of this thesis (see Chapter 5 for details).

Detection. In the GG02 protocol, Bob performs an homodyne detection. However, the protocol can be easily modified to allow for an heterodyne detection where Bob measures both quadratures. Such an heterodyne detection is a slightly more involved to implement but can be beneficial in terms of performances (see Appendix B for details).

Postselection. An other possible variation around the GG02 protocol is to perform a postselection. Intuitively, it sounds as a good idea: Alice and Bob discard the data that are too noisy, and only keep the good data for which Eve has presumably only little information. Unfortunately, it is very difficult to establish general security proofs compatible with postselection. All proofs presently known require a complete tomography of the states received by Bob. This means that an infinity of parameters need to be estimated! In theory, this is always possible in the asymptotic limit, but it is clearly incompatible with any experiment which involves the exchange of only a *finite* number of quantum states. For this reason, we do not consider postselection in this thesis.

3.3.4 Security of CV QKD

The GG02 protocol is proven secure against collective attacks [51, 106] and the corresponding lower bound on the secret key rate has recently been shown to hold asymptotically against coherent attacks [127]. The security proof against collective attacks is based on the optimality property of Gaussian states and is reviewed here. Note that Gaussian attacks have always played a central role for continuous-variable QKD protocols. A first result showing that one only needed consider such attacks (in the case of protocols without postselection) could already be found in [63].

The idea is to use Theorem 2.2 to bound the Holevo information between Eve and Bob. As we saw in the previous Section, the secret key rate K_{coll} secure against collective attacks is given by:

$$K_{\text{coll}} = I(a;b) - S(b;E). \tag{3.12}$$

Here we use lowercase letters to describe classical variables (such as the measurement results a and b of Alice and Bob, respectively) and uppercase letters to describe quantum states (such as the quantum system E of Eve). As we will see in Chapter 4, the effect of an imperfect reconciliation procedure can be summarized by an additional parameter $\beta \leq 1$, the reconciliation efficiency, which modifies the secret key rate in the following way:

$$K_{\text{real}} = \beta I(a;b) - S(b;E). \tag{3.13}$$

In practice, the first term of the right side hand, $\beta I(a;b)$ is directly observed in a given implementation of the protocol. The real question is therefore to determine the value of

$S(b;E)$, or at least, to be able to find an upper bound for this quantity in order to derive a lower bound on the actual secret key rate of a given experiment.

Before explaining how this can be achieved, we would like to emphasize how counter-intuitive it is that this can be done at all. First, it is easy to see that $S(b,E)$ is a function of the quantum state ρ_{AB} shared by Alice and Bob in the equivalent entanglement-based protocol. Indeed, in such a protocol, Eve is without loss of generality supposed to hold a purifying system of ρ_{AB}, that is, the state ρ_{ABE} shared by Alice, Bob and Eve can be considered to be pure. That said, Eve's quantum state, $\rho_E = \mathrm{tr}_{AB}(\rho_{ABE})$ is defined up to a unitary operation on the system E. However, the quantity $S(b;E) = S(E) - S(E|b)$ is left invariant under such unitaries (this is a consequence of the fact that the von Neumann entropy is invariant under unitary operations). This means that there exists a function f such that $S(b;E) = f(\rho_{AB})$.
That fact being established, let us look more closely at our problem, that is evaluating $f(\rho_{AB})$ in a given experiment. There are actually two mains issues to be considered. First, we do not know how to compute f for a generic state ρ. f can only be computed (with today's knowledge) for a small class of states. The reason for that is that in general, the value of $f(\rho_{AB})$ is given by an optimization problem (in infinite dimension) that is intractable except for very specific families of states. For instance, if ρ_{AB} is the singlet state, then Eve's quantum state can be factorized from Alice and Bob's state, meaning that the quantity $S(b;E)$ is necessarily null in this case. Unfortunately, in practice, ρ_{AB} is never a pure entangled state. Another class of states for which f can be computed is Gaussian states, as we will see below. Unfortunately, proving that a given state is Gaussian is impossible in practice as it would in principle require an infinite number of copies of the state[17]. More generally, since we work in an infinite-dimensional Hilbert space, it is not reasonable for a proof to require a perfect tomography of the state of Alice and Bob[18]. Note however that the restriction to collective attacks considerably simplifies the analysis as the state ρ_{AB} describing Alice and Bob's respective N systems can be written as $\rho_{AB} = \int \mathrm{d}\sigma_{AB}\, p(\sigma_{AB})\, \sigma_{AB}^{\otimes N}$. Even with this restriction to collective attacks, it does not seem reasonable to assume that Alice and Bob have a perfect knowledge of the quantum state ρ_{AB} they share. In these conditions, it might appear quite lucky that we can indeed find an upper bound to the quantity $S(b;E)$, even considering an imperfect knowledge of ρ_{AB}.

The solution to our problem is brought by Theorem 2.2. It can indeed be shown that the function $f : \rho_{AB} \longmapsto f(\rho_{AB}) = S(b;E)$ satisfies the hypotheses of Theorem 2.2. Let us now check these different hypotheses.

(i) Continuity. First, for two quantum states ρ_{AB} and σ_{AB} such that $||\rho_{AB} - \sigma_{AB}||_1 \leq \epsilon$, there exist respective purifications ρ_{ABE} and σ_{ABE} such that $||\rho_{ABE} - \sigma_{ABE}||_1 \leq 2\sqrt{\epsilon}$.

[17] this is exactly the problem encountered when deriving the security of CV QKD protocols with postselection. Such security proofs always assume that the state ρ_{AB} is Gaussian [68] but this can never be completely checked in practice.

[18] the situation is different for discrete-variable QKD protocols where the Hilbert spaces considered usually have a small dimension, and where performing a tomography of the state is a reasonable demand. However, we will see in Chapter 7 that this task is not as benign as it looks in the case of a finite size analysis of the security.

Thus, since f does not depend on the choice of purification of ρ, it is sufficient to prove the continuity of $f(\rho_{ABE})$ to infer that of $f(\rho_{AB})$. Here, we keep the same notation to represent $S(b;E)$ whether we consider this Holevo information to be a function of ρ_{AB} or ρ_{ABE}. Since partial trace can only decrease the trace norm, it follows that $||\rho_{BE} - \sigma_{BE}||_1 \leq 2\sqrt{\epsilon}$ and $||\rho_E - \sigma_E||_1 \leq 2\sqrt{\epsilon}$. Moreover, the homodyne detection performed by Bob being a quantum operation, it can also only decrease the trace norm, meaning that $||\rho_{bE} - \sigma_{bE}||_1 \leq 2\sqrt{\epsilon}$. Finally, one needs to use a continuity argument for the von Neumann entropy. Unfortunately, it is known that the von Neumann entropy is discontinuous almost everywhere in an infinite dimensional Hilbert space. In order to restore the continuity of this functional, one can for instance bound the energy of the system in order to make the set of states compact (see for example Proposition 6.6 of [112]). Note that requiring the energy of the system to be bounded appears as a reasonable assumption. On the compact states of bounded energy, the von Neumann entropy is therefore continuous and so is the quantity $S(b;E) = S(E) - S(E|b)$. This concludes the proof of the continuity of f.

(ii) Strong sub-additivity. Here we follow the same steps as in [50, 51]. The goal is to show that $f(\rho_{A_1B_1} \otimes \rho_{A_2B_2}) = f(\rho_{A_1B_1}) + f(\rho_{A_2B_2})$ (additivity) and $f(\rho_{A_1B_1A_2B_2}) \leq f(\rho_{A_1B_1}) + f(\rho_{A_2B_2})$ where $\rho_{A_1B_1} = \mathrm{tr}_{A_2B_2}(\rho_{A_1B_1A_2B_2})$ and $\rho_{A_2B_2} = \mathrm{tr}_{A_1B_1}(\rho_{A_1B_1A_2B_2})$ (strong sub-additivity). Let us consider the case where Alice and Bob share a bipartite state $\rho_{A_1B_1A_2B_2}$ and Eve holds a purifying system E such that $\rho_{A_1B_1A_2B_2E}$ is pure. One has:

$$\begin{aligned} f(\rho_{A_1B_1A_2B_2}) &= S(b_1,b_2;E) && (3.14)\\ &= S(b_1,b_2) - S(b_1,b_2|E) && (3.15)\\ &= S(b_1,b_2) - S(b_1|b_2E) - S(b_2|b_1E) - S(b_1;b_2|E). && (3.16)\end{aligned}$$

Now, using the following basic properties of the von Neumann entropy,

$$\left\{\begin{array}{lcl} S(b_1,b_2) & \leq & S(b_1) + S(b_2) \\ S(b_1|b_2E) & \geq & S(b_1|A_2B_2E) \\ S(b_2|b_1E) & \geq & S(b_2|A_1B_1E) \\ S(b_1;b_2|E) & \geq & 0 \end{array}\right. \quad (3.17)$$

one gets:

$$f(\rho_{A_1B_1A_2B_2}) \leq S(b_1) - S(b_1|A_2B_2E) + S(b_2) - S(b_2|A_1B_1E). \quad (3.18)$$

Finally, observing that the system $E_1 \equiv A_2B_2E$ (resp. $E_2 \equiv A_1B_1E$) purifies A_1B_1 (resp. A_2B_2), one obtains

$$f(\rho_{A_1B_1A_2B_2}) \leq S(b_1;E_1) + S(b_2;E_2) = f(\rho_{A_1B_1}) + f(\rho_{A_2B_2}), \quad (3.19)$$

which is the strong sub-additivity. The additivity of f results from the additivity of the von Neumann entropy. This concludes the proof of the strong sub-additivity of f.

(iii) Invariance under unitaries. The crucial point here is that in order to prove Theorem 2.2, it is not necessary to show the invariance of f under any unitary U. It

is sufficient to consider the *Gaussification unitary* operation U_G which is the Gaussian operation acting on the quadratures $[x_1, \cdots, x_N]^T$ (with $N = 2^m$) in the following way:

$$\begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix}_{\text{out}} = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}^{\otimes m} \begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix}_{\text{in}} \tag{3.20}$$

Such a Gaussification unitary operation does not mix the different quadratures and thus commutes with the measurement process of the CV QKD protocol. Hence it leaves the quantity $S(b;E)$ invariant.

This concludes the proof that the quantity $f(\rho_{AB}) = S(b;E)$ satisfies the hypotheses of Theorem 2.2. As a consequence, one has:

$$f(\rho_{AB}) \leq f(\rho_{AB}^G), \tag{3.21}$$

which means that the quantity $S(b;E)$ can be bounded by the same quantity computed for the Gaussian state ρ_{AB}^G with the same first and second moments as ρ_{AB}. In fact, it turns out that the Holevo information between b and E computed for such a Gaussian state does not depend on the first moment of ρ_{AB}.

Two things are left to do in order to complete the security proof of the protocol against collective attacks. First, one needs to show how to compute $S(b;E)$ in the case where ρ_{AB} is Gaussian. Second, one needs to be able to derive the covariance matrix Γ_{AB} of the state ρ_{AB} from the data obtained in the Prepare and Measure version of the protocol.

Before addressing these two tasks, we would like to come back on the notion of *optimality of Gaussian attacks* often found in the literature. What we proved above is that is is always safe to assume the state ρ_{AB} to be Gaussian. This statement is equivalent to the optimality of Gaussian attacks, meaning that the quantum channel is Gaussian, only if the initial state is Gaussian. Obviously, this is the case in the GG02 protocol as Alice uses a Gaussian modulation (or equivalently, Alice uses two-mode squeezed states in the entanglement-based protocol). However, in the case where Alice does not use a Gaussian modulation, the result we proved is different from saying that the optimal attack is Gaussian. We will elaborate on this in Chapter 5 when we introduce and prove the security of a continuous-variable QKD protocol using a discrete (non Gaussian) modulation.

3.3.5 Estimation of the covariance matrix in the entanglement-based protocol from data observed in the Prepare and Measure protocol

The first link between the GG02 P&M protocol and its equivalent E-B protocol was established in [59]. The main idea is to describe two different protocols, which are completely identical from Bob and Eve's points of view: only the task performed by Alice differs, but her final classical data are the same for both protocols. For this reason, the protocols are indistinguishable and the secret key rate valid for one of them is also valid

for the other one. One of the protocols, the Prepare and Measure version, corresponds to GG02 as it is implemented in practice. However, its security analysis is rather involved. On the other hand, the Entanglement-Based version of the protocol is not implemented in practice, mostly because it is less practical, but turns out to be easier to analyze because it involves an entangled, bipartite state shared by Alice and Bob. Since both protocols are equivalent, there is no advantage to implement the E-B version, and it is sufficient to implement the P&M version.

In the P&M version of the GG02 protocol, Alice encodes information in the quadratures X and P of coherent states. The random variables X and P are drawn according to a Gaussian distribution of variance V_A: $X, P \sim \mathcal{N}(0, V_A)$.
In the E-B version, Alice starts with a two-mode squeezed state $|\psi\rangle$ with covariance matrix Γ given by

$$\Gamma = \begin{pmatrix} V\mathbb{1}_2 & \sqrt{V^2-1}\sigma_z \\ \sqrt{V^2-1}\sigma_z & V\mathbb{1}_2 \end{pmatrix} \tag{3.22}$$

where $V = V_A + 1$. Then she performs an heterodyne detection on the first half of the state, thus preparing a coherent state centered on $\frac{\sqrt{2(V^2-1)}}{V+1}(X_A, -P_A)$ if Alice's measurements were (X_A, P_A), according to equation 2.108.

At the end of the quantum exchange, Alice and Bob perform a parameter estimation which is done by analyzing m pairs of correlated data $(x_i, y_i)_{1\leq i\leq m}$ where y_i refers to the quadrature measurement of Bob and x_i refers to the corresponding value of Alice's quadrature. As we saw, for continuous-variable QKD, it is sufficient to estimate the covariance matrix Γ_{AB} of the state shared by Alice and Bob. In fact it turns out that only two parameters need being estimated:

- the variance on Bob's side $\langle y^2 \rangle$,
- the correlation between Alice and Bob's data $\langle xy \rangle$.

Why are these two parameters the only ones to be estimated? One could have expected to know the 10 parameters describing a general 4×4 covariance matrix. The answer is that Alice and Bob could add a *symmetrization procedure* to the protocol to ensure that Γ_{AB} is of the form

$$\Gamma_{AB} = \begin{pmatrix} V\mathbb{1}_2 & \sqrt{T(V^2-1)}\sigma_z \\ \sqrt{T(V^2-1)}\sigma_z & (1+T(V-1)+T\xi)\mathbb{1}_2 \end{pmatrix} \tag{3.23}$$

This symmetrization procedure is explained in more details in Chapter 6 as well as in Reference [90]. It is interesting to note that the assumption that only two parameters were required was done for many years without any theoretical justification. As we will see in Chapter 6, symmetrization is a very powerful tool for the security analysis of QKD protocols.

We directly wrote the matrix Γ_{AB} in the form of 3.23 because it makes the connection with the observed *transmission* T and *excess noise* ξ of the quantum channel. T and ξ

are linked to $\langle x^2 \rangle$, $\langle y^2 \rangle$ and $\langle xy \rangle$ through

$$\begin{cases} V & = & \langle x^2 \rangle + 1 \\ T & = & \frac{\langle xy \rangle^2}{\langle x^2 \rangle^2} \\ 1 + T(V-1) + T\xi & = & \langle y^2 \rangle \end{cases} \tag{3.24}$$

In order to compute the secret key rate of the continuous-variable QKD protocol, one needs to upper bound $S(b;E)$, which can be done by computing the value for the Gaussian state with the same covariance matrix. Therefore, one needs to compute $S(b;E)$ for the Gaussian state with covariance matrix Γ_{AB}:

$$S(b:E) = S(E) - S(E|b) \tag{3.25}$$
$$= S(AB) - S(AB|b), \tag{3.26}$$

since the system E can be considered without loss of generality to be a purifying system for AB. The quantities $S(AB)$ and $S(AB|b)$ can be easily computed from the symplectic eigenvalues ν_1, ν_2 of Γ_{AB} and ν_3 of $\Gamma_{AB|b}$ where $\Gamma_{AB|b}$ is the covariance matrix of Alice's mode, given Bob's result of the homodyne measurement of say, quadrature x:

$$\Gamma_{AB|b} = \begin{pmatrix} V - \frac{T(V^2-1)}{1+TV+T\xi} & 0 \\ 0 & V \end{pmatrix}. \tag{3.27}$$

The symplectic eigenvalues are given by:

$$\nu_1^2 = \frac{1}{2}\left[\Delta + \sqrt{\Delta^2 - 4D}\right] \tag{3.28}$$
$$\nu_2^2 = \frac{1}{2}\left[\Delta - \sqrt{\Delta^2 - 4D}\right] \tag{3.29}$$
$$\nu_3^2 = V\left(V - \frac{T(V^2-1)}{1+T(V-1)+T\xi}\right), \tag{3.30}$$

where one defines

$$\Delta = V^2 + (1+T(V-1)+T\xi)^2 - 2T(V^2-1) \tag{3.31}$$
$$D = \left((1+T(V-1)+T\xi)V - T(V^2-1)\right)^2. \tag{3.32}$$

Now, recall the expression the expression of the entropy of a Gaussian state as a function of its symplectic eigenvalues, one obtains:

$$S(b;E) = g\left(\frac{\nu_1 - 1}{2}\right) + g\left(\frac{\nu_2 - 1}{2}\right) - g\left(\frac{\nu_3 - 1}{2}\right), \tag{3.33}$$

where the function g is defined as

$$g(x) = (x+1)\log_2(x+1) - x\log_2 x. \tag{3.34}$$

3.3.6 Paranoid versus realistic mode

The derivation described above corresponds to the so-called *paranoid mode*, that is, all the sources of excess noise are attributed to a potential attack of the eavesdropper. In a particular implementation, however, the main source of excess noise is the electronic noise associated to the homodyne detection. Whereas this electronic noise can be made very low in state of the art experiments [48], it is still the main source of noise in a typical experiment. This is rather problematic as it considerably decreases the secret key rate associated the the QKD protocol, while at the same time, it seems very reasonable to suppose that this noise is not signature of a particular attack of an eavesdropper. The following question then naturally arises: can we consider that the electronic noise is legitimate, meaning that it is entirely caused by Bob's equipment and is therefore not associated with any leak of information to the eavesdropper? To answer positively to this question requires to be able to track perfectly any source of such legitimate noise. In particular, it means that Alice and Bob's devices should be *calibrated*. The question of paranoid versus realistic mode then boils down to the problem of calibrating the devices used for the QKD protocol. Here we can consider three possible scenarios:

- the *device independent* scenario, which is by far the most pessimistic one. In this case, Alice and Bob buy all there equipment from the eavesdropper and cannot trust it at all. The only assumptions necessary are hardly the obvious ones without which cryptography would not even make sense, that is, that the eavesdropper cannot read Alice and Bob's data, and does not have any influence on the choices of measurements performed by Alice and Bob. A more comprehensive discussion of these hypotheses can be found in [119]. For this scenario to work, one needs to rule out any local hidden variable model for the experiment performed by Alice and Bob. Quite astonishingly, this is possible at the (expensive) price of being able to perform a *loophole-free* Bell test. It is important to note that such a test has not yet been performed but it is reasonable to think that it should be doable in the next few years [113]. However, even if this is a fascinating theoretical scenario[19] , it is absolutely not practical! If only such a scenario existed, QKD would hardly be more than just a theoretical curiosity.

- the *uncalibrated* scenario, which is the scenario usually considered for most discrete-variable QKD protocols. In such a scenario, Alice and Bob trust their devices, meaning that they know what their device do, and measure. However, any imperfection of the devices is seen as the signature of the eavesdropper. For instance, the dark counts of a photon counter are seen as errors which are attributed to the malicious action of the eavesdropper. One should emphasize that when talking of calibrated or uncalibrated scenarios, one mostly refers to the behavior of the

[19] one should point out, however, that the unconditional security of device-independent QKD has not been established yet. So far, only security against collective attacks could be proven, and the usual tools (such as the exponential de Finetti theorem) to prove the asymptotic optimality of collective attacks do not work for such a scenario because one cannot easily bound the dimension of the Hilbert spaces relevant to describe the protocol.

detection stage, and not so much to Alice's device. The position of considering an uncalibrated scenario is therefore somewhat ambiguous as one does not completely trust the detection stage (meaning that some legitimate errors, induced by dark counts for instance, are conservatively attributed to Eve) but one trusts the preparation stage on Alice's side, in particular, ruling out various side-channels, that is relevant information encoded in degrees of freedom not explicitly relevant to a particular QKD protocol. Note also that an uncalibrated scenario does not make sense in the case of a continuous-variable QKD protocol[20] . The reason for that is that there is always a legitimate source of noise in a CV QKD protocol: *shot noise*. Moreover, this shot noise necessarily needs being calibrated, meaning that Bob always needs to perform *some* calibration of his detection stage.

- the *calibrated* scenario, in which Bob supposedly knows how his detection stage works. In particular, he knows the level of legitimate noise generated by his detectors. Therefore, there is no reason to attribute this noise to the action of an eavesdropper, and this allows for a significant improvement of the real performance of a QKD protocol. To be more precise, the secret key rate is roughly given by the difference between the mutual information between Alice and Bob and the information acquired by Eve on the key. In any of the three scenarios considered above, the mutual information between Alice and Bob is the same[21], but significant differences appear when evaluating Eve's information. This consequently greatly impacts the secret key rate of the protocol.

For a more comprehensive discussion concerning the calibrated versus uncalibrated scenarios, the interested reader is invited to consult the recent review by Scarani et al [136].

As we just saw, in the case of a continuous-variable QKD protocol, it does not make much sense to consider an uncalibrated scenario as one needs to calibrate the shot noise anyway, and this is why we can legitimately consider the calibrated scenario, that is the realistic one. In order to do that, one must be able to calibrate Bob's detectors and to model their imperfections in order to put an upper bound on Eve's information. For CV QKD, this can be done by modeling the homodyne detection with two parameters: its quantum efficiency η and its electronic noise V_{elec}. The derivation of the mutual information $S(b;E)$ between Eve and Bob's data can then be done in a rather straightforward way [97].
In the remaining of this manuscript, for the reasons pointed out above, we choose to consider the calibrated scenario.

It is also interesting to note that various assumptions are made while studying the security of QKD, and that it is not always clear how these assumptions compare to each other. Among these, we can cite

[20] at least for all the existing CV QKD protocol, which always consider *excess noise*. It might however be possible for instance to perform a loophole-free violation of a Bell inequality in the continuous-variable context, and therefore perform a device-independent, and thus uncalibrated, QKD protocol.

[21] More precisely, the size of the common bit string Alice and Bob agree on at the end of the reconciliation procedure is completely known.

- calibrated vs uncalibrated,
- with or without side-channels,
- asymptotic or finite-size security analysis,
- collective or coherent attacks[22].

The question of deciding which assumptions are more pertinent and can be safely be made has not yet been solved, and is clearly a prerequisite for any potential commercial application of QKD.

The problem of postselection. Here I would like to discuss rapidly CV QKD protocols using a postselection procedure, and in particular to argue that the security proofs presented above cannot directly be applied to them. A postselection procedure [144] has been suggested in the literature to help beat the 3dB limit that CV QKD was facing in 2002 before the concept of reverse reconciliation procedure was introduced. In a protocol with postselection, Bob basically announces the absolute value of his measurement result[23] and decides to throw away all the data for which this absolute value is smaller than some *threshold*. Typically this threshold is chosen so that

- measurements below the threshold correspond to data such that $I(a;b) \leq S(b;E)$,
- measurements above the threshold correspond to data such that $I(a;b) \geq S(b;E)$,

where the value $S(b;E)$ is computed for a certain class of attacks (usually Gaussian collective attacks). By only keeping the "good" data for which Eve has less information than Alice and Bob, one can significantly improve the performances of the QKD protocol, in particular, its range. However, one main drawback of this procedure is that it is not yet known to be secure, even against collective attacks. The security could only be established so far against Gaussian collective attacks, but it is not clear at all that such attacks should be optimal against protocols involving a postselection scheme (in contrast with protocols without such a postselection procedure).

I would now like to explain why the protocols with a postselection procedure cannot easily be analyzed in the framework described above. Roughly speaking, the reason is that the entanglement-based version of the protocol is not defined in an unambiguous way. More precisely, in order to use the same technique as before, one needs to know the covariance matrix of the bipartite state shared by Alice and Bob in the E-B version of the protocol, and especially, the covariance matrix corresponding to the postselected state that will be used to distill a key. Unfortunately, the relation between this covariance matrix Γ_{AB} in the entanglement-based protocol is not directly related to the data observed

[22] in this thesis, we do not discuss the so-called *individual* attacks. For a definition of these attacks, one can consult Reference [53].

[23] the raw key bit which corresponds to the sign of Bob's result, being independent of the absolute value of this result, is not compromised by this disclosure.

by Alice and Bob in the Prepare and Measure protocol, and in particular to the values of the second moments of these data: $\langle x^2 \rangle, \langle y^2 \rangle$ and $\langle xy \rangle$.

Indeed, if Bob postselects some states, he will have an influence on Alice's state in the entanglement-based version of the protocol. Therefore, the covariance matrix used to calculate the secret key rate might change. Now, this means that Eve has a way to influence the state of Alice in a protocol with postselection. Taking such effects into account does not appear possible with current analysis tools and one is restricted to study different class of attacks, without being capable to derive lower-bound for the secret key rate.

If one really wants to apply the optimality of Gaussian states to analyze the security of protocols with a postselection procedure, this can be done, but the price to pay is too high to prove the security of key distillation over reasonable distances. Indeed, one can upper bound the Holevo information between Eve and Bob's data, but this needs to be done on *all* the data. Unfortunately, because of the postselection, only some (typically small) fraction f of the data are used to make a raw key. This fraction f therefore appears as some new reconciliation efficiency coefficient, and the final secret key rate K_{PS} for a protocol with postselection reads

$$K_{\mathrm{PS}} = f\beta I(A;B) - S(b;E), \tag{3.35}$$

where β is the usual reconciliation efficiency for the postselected data. This key rate is secure against arbitrary collective attacks, but is equal to zero for any low value fraction f of postselected states, thus completely annihilating the purpose of postselection. Obviously, such a pessimistic secret key rate is not known to be tight, but has the main advantage to consider all collective attacks, in contrast with more optimistic proofs which only consider Gaussian attacks.

Let us conclude this section by emphasizing two points. First, the assumption of a Gaussian attack is quite problematic from a theoretical point of view as one can never prove that a particular *finite-size* attack is indeed Gaussian. This is why a theorem proving that such attacks are indeed optimal is indeed very useful. Second, when considering protocols with postselection, it is not at all clear (even intuitively) that Gaussian attacks should be optimal. Let us sketch a possible non-Gaussian attack: Eve can for instance use a noiseless *non-deterministic* amplifier to amplify the coherent states sent by Alice. Such an amplifier would perform the following transformation

$$|\alpha\rangle\langle\alpha| \longmapsto \rho(\alpha) \equiv P|g\alpha\rangle\langle g\alpha| + (1-P)|0\rangle\langle 0|, \tag{3.36}$$

where $|\alpha\rangle$ is a coherent state, $|g| > 1$ is the amplification factor and P is the probability of success of the amplification, and where a heralding signal identifies which term in the output density operator $\rho(\alpha)$ has been produced by any particular run of the device. Obviously, the laws of quantum mechanics forbid P to be equal to 1 as soon as $|g| > 1$ and the maximal allowed probability P is given by [160]

$$P \leq P_{\max} \equiv \frac{1 - e^{-|\alpha|^2}}{1 - e^{-|g\alpha|^2}} \tag{3.37}$$

Eve, when the amplification procedure worked, can keep part of the amplified state $|g\alpha\rangle$ in her quantum memory and send the rest of the state back to Bob. When the amplification procedure fails, Eve just sends to vacuum state $|0\rangle$ to Bob. If Alice and Bob are not careful enough, and for example discard all the data such that Bob's measurement has a too low absolute value, they might not realize that Eve has been spying as for successful amplification procedures, Eve did not add any noise to the state $|\alpha\rangle$. Such a type of attacks clearly indicates that even the states that fail the postselection sieve have to be closely monitored as they can be the only trace left by a possible eavesdropper. Thus, it is not possible to obtain any secure key rate by computing parameters only on the data that pass the postselection step.

Part II

Increase the range of continuous-variable QKD

CHAPTER 4

Reconciliation of correlated Gaussian random variables

The goal of this chapter is to provide a way to improve the reconciliation technique of the Grosshans-Grangier protocol (characterized by a Gaussian modulation of coherent states), referred to in the following as GG02 [64], in the low SNR regime in order to increase its range. Indeed, even with a state of the art experimental implementation, the protocol can only distribute secret keys over distances less than 30 km [97, 48, 117] and it turns out that this limitation is more a consequence of the imperfect reconciliation scheme, which is concerned with extracting all the available information from the correlated random variables shared by the legitimate parties at the end of the quantum part of the protocol, than of technological imperfections. To this end, we suggest a new reconciliation scheme adapted to the GG02 protocol, than can be applied without any modification of the hardware implementation, and without added complexity[1], that improves the range of the protocol from 30 km to 50 km[2].

[1] it is important to note that the reconciliation procedure currently also limits the rate of the protocol.

[2] this reconciliation scheme was the object of a publication in Physical Review A [91] and of a conference presentation at ISIT 2008 [89].

4.1 Figures of merit for a QKD system.

Two main technical figures of merit are usually considered for describing the performances of a QKD system: its secret rate (usually considered at zero distance), that is how many secret bits can be delivered by unit of time, and its range, that is the maximal distance between the legitimate parties compatible with a positive secret rate. In fact, both these figures of merit have been extensively used for advertising the performances of some protocols. However, such a picture is in fact too simple, and it is much more accurate to describe a QKD system by the entire function $K = f(d)$ giving the secret key rate as a function of the distance between Alice and Bob. Such a function is particularly relevant because the *working point* of a given QKD protocol is never at zero distance (where the key rate is maximum) nor at the distance where the key rate drops to zero. In practice, the working point is intermediate between these two extremes and can only be found when having access to the function $K = f(d)$. Such considerations are especially important if one wants to integrate several QKD systems in a network topology, which is arguably the next challenge for QKD[3]. Such a function can be measured experimentally for any implementation, but can also be estimated for a theoretical protocol. In order to perform such an estimation, one must know *a priori* the quantum channel, which is a bit counterintuitive as this quantum channel is usually assumed to be completely controlled by Eve. The solution to this problem is actually rather simple: the QKD protocols are compared for *normal conditions*, that is, in absence of an eavesdropper. This is rather natural as QKD is really a means to prove the security of the key distributed and does not allow the legitimate parties to do so in the case where an eavesdropper wants to prevent them for communicating. More precisely, QKD is helpless against an adversary who would cut the optical fiber between Alice and Bob for instance. The function of QKD is to distribute secret keys when possible or *to abort* if the security is not guaranteed. From this perspective, it is natural to compare QKD protocols in an optimal environment, as they are optimized for working in these conditions.

Hence, in the case of a fiber-optics implementation, it is usual to model the quantum channel as a typical fiber characterized by its transmission $T = 10^{-0.02d}$ where d is the distance in kilometers between Alice and Bob. This is compatible with regular telecom fibers which have losses of 0.2dB per kilometer. In the literature, the secret key rate is either given as a function of the transmission T or of the distance d. Whereas T appears more natural, especially because it does not depend on the specific performance of optical fibers which is subject to improvement with time, the distance d is in fact more used as it is more relevant for today's applications. Indeed, it is more meaningful[4] to say that quantum key distribution can be performed over 100 km than to say that it tolerates losses of 99%. For this reason, in this thesis, we will alway plot the *expected* secret key rate as a function of the distance, for an optical fiber with losses of 0.2dB per kilometer.

Even with the previous considerations, it is not quite clear how to measure the secret

[3]The question of topological optimization for QKD networks has just started being studied in the literature, and a first discussion can be found in [6].

[4]even if one can certainly argue that it is subjective

key rate as a function of the distance. In particular, the actual secret key rate generated in a real implementation is often much smaller than the secret key rate expected from the theoretical model.

As an example of this problem, let us consider typical performances of the GG02 protocol. The most recent data can be found in [48] and are summarized on Figure 4.1. There, it is shown that (at least) four different values of the secret key rate can be used:

- the maximum theoretical secret key rate of the protocol $K_{\max}$ given by

$$K_{\max} = I(A;B) - S(B;E)|_{\text{perf. impl.}} \tag{4.1}$$

  where "perf. impl." stands for *perfect implementation* meaning that Alice and Bob's boxes are ideal. In particular, the Bob's homodyne detection is supposed to be noiseless (absence of excess noise) and with a quantum efficiency of 100%,

- the theoretical secret key rate $K_{\max,\text{ noisy}}$ compatible with the non ideal characteristics of Bob's detection stage, but assuming an infinite amount of computational power, meaning that the reconciliation efficiency can be considered to be 100% (perfect reconciliation scheme) and that the post-processing of the data is instantaneous[5]

$$K_{\max,\text{ noisy}} = I(A;B) - S(B;E)|_{\text{noisy but fast impl.}}, \tag{4.2}$$

- the realistic secret key rate K_{real}, assuming noisy detectors, as well as realistic computing power and therefore a necessarily imperfect reconciliation scheme characterized by a finite reconciliation efficiency β, but for which the post-processing is still considered to be much faster than the optical treatment of data:

$$K_{\text{real}} = \beta I(A;B) - S(B;E), \tag{4.3}$$

- and finally, the secret key rate really $K_{\text{implementation}}$ observed in an experimental implementation of the protocol, where all the optical data cannot be processed in real-time. This implies to add a correction factor $\alpha < 1$ to the expression of K_{real} meaning that only the fraction α of the data can be processed:

$$K_{\text{implementation}} = \alpha\left(\beta I(A;B) - S(B;E)\right). \tag{4.4}$$

Actually, the situation is even more complicated than that. Indeed, we only considered here the asymptotic security of the protocol against collective attacks. Even if collective attacks have been proven optimal in the asymptotic regime against the GG02 protocol [127], it is in principle crucial to take into account the *finite-size effects*. Unfortunately, these effects appear to have important consequences when estimating the secret key rate. Preliminary results in this direction for CV QKD can be found in Chapter 7.

[5] in fact, it is sufficient to consider that the post-processing of the data is much faster than the optical repetition rate.

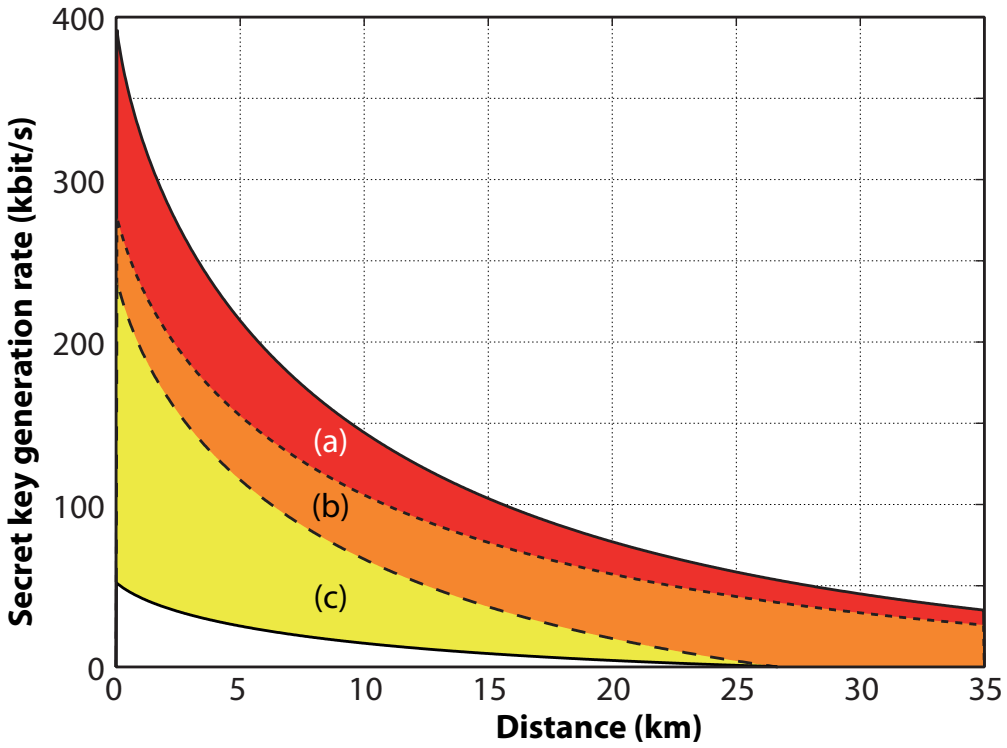

Figure 4.1: Various secret key rates corresponding to a given QKD protocol (This figure is taken from Reference [48]). The upper solid curve represents the maximum theoretical rate compatible with the protocol (perfect implementation, infinite computational resources). (a) Drop in rate due to a realistic implementation (here, effect of an excess noise of 4%). (b) Drop due to a realistic, imperfect reconciliation scheme (here, we take an efficiency of 90% for a signal-to-noise ratio of 3). (c) Drop due to the current impossibility to post-process all the data at the optical emission rate. The lower solid curve is the practical achievable secret key distribution rate.

A specificity of continuous-variable QKD protocols with a Gaussian modulation and without postselection is that taking into account the finite reconciliation efficiency has a great impact on the performances of the scheme. It is clear from Figure 4.1 that this is the main reason for the limited range of CVQKD. On the other hand, the effect of the slow post-processing compared to the optical rate as only a small impact: it limits the rate of the protocol, but this problem could easily be solved by giving a few supplementary computers to Bob. From this perspective, the reconciliation problem is very different: the computing power necessary to go from a finite reconciliation efficiency to a perfect reconciliation efficiency is clearly much more than a few additional computers[6]. Thus it

[6]The only known way to achieve a perfect reconciliation efficiency is to use a random code. Unfortunately, decoding such a random code appears to be a problem intractable with current technology: it is indeed an $\mathcal{NP}$-complete problem. If the celebrated $\mathcal{P} \neq \mathcal{NP}$ conjecture is true, then this decoding will always be out of reach of any classical (and even certainly quantum) technology.

appears reasonable to be interested in the effect of a non-ideal detection stage, as well as a non-ideal reconciliation efficiency, but the problem of the mismatch between the optical repetition rate and the post-processing power can safely be omitted. This is the scenario that we will consider in the rest of this manuscript.

4.2 The reconciliation problem for continuous-variable QKD

We now turn to the question of the reconciliation for a continuous-variable QKD protocol: more precisely, Alice and Bob are given correlated random vectors and they want to find a way to agree on a common bit string with the help of classical communication. Obviously, to make the task more interesting, this classical communication should be kept to a minimum as the classical channel is not private, meaning that Eve can in principle have access to it.

Two different approaches have been presented in the literature to extract binary information from Gaussian variables. *Slice reconciliation* [154, 108, 14, 153] consists in quantizing continuous variables and then correcting errors on the resulting discrete variables. It allows in principle to transmit more than 1 bit per pulse, and to extract all the information available, but only if the quantization takes place in $\mathbb{R}^d$ with $d \gg 1$, which results in an unacceptable increase of complexity in practice. Therefore the present protocols always use $d = 1$, resulting in finite efficiency, which limits the range of the QKD to about 30 km. The second approach uses the sign of the continuous variable to encode a bit, and it has the advantage of simplicity. It can also be efficient, at least in the case where the signal to noise ratio is low enough, so that less than 1 bit per pulse can be expected. But since the Gaussian distribution is centered around 0 and most of the data have a small absolute value, it becomes difficult to discriminate the sign when the noise is important. As a consequence, it has been proposed to use *postselection* [144] to get rid of the "low amplitude" data, and keep only the more meaningful "large amplitude" data[7]. However, this approach has a major drawback: since the optimal attack against such a postselected protocol is unknown, the secret key rate can be calculated only for certain types of *restricted* attacks [144, 68]. So the security is significantly weaker than the initial *non postselected* Gaussian-modulated protocol, where one can use the optimality of Gaussian attacks [51, 106] in order to prove that the protocol is secure against arbitrary general collective attacks.

Here we are interested in the problem of extending continuous-variable QKD over longer distances without postselection, but with proven security. This involves to keep unchanged the quantum distribution part. The main idea is as follows: whereas Gaussian random values are centered around 0, this is not the case for the norm of a Gaussian random vector. Such a vector lies indeed on a shell which gets thinner and thinner as the dimension of the space increases (see Fig. 4.2). Thus, if one performs a clever rotation

[7] To be more precise, the postselection idea was not introduced in order to specifically tackle the reconciliation problem. The goal was in fact to get rid of the noisy data as they are the one for which an eavesdropper might have more information than Bob. But it turns out that the postselection scheme also simplifies the reconciliation procedure.

(see Fig. 4.3) before encoding the key in the sign of the coordinates, one automatically gets rid of the small absolute value coordinates without postselection. Whereas this effect gets stronger and stronger for large dimensions, we will prove that we are intrinsically limited to performing such rotations in $\mathbb{R}^8$. As we will show below, this is related to the algebraic structure of octonions. For our purpose, working in $\mathbb{R}^8$ is already a significant improvement since it allows to exchange secure secret keys over more than 50 km, without postselection, and with a reasonable complexity for the reconciliation protocol[8].

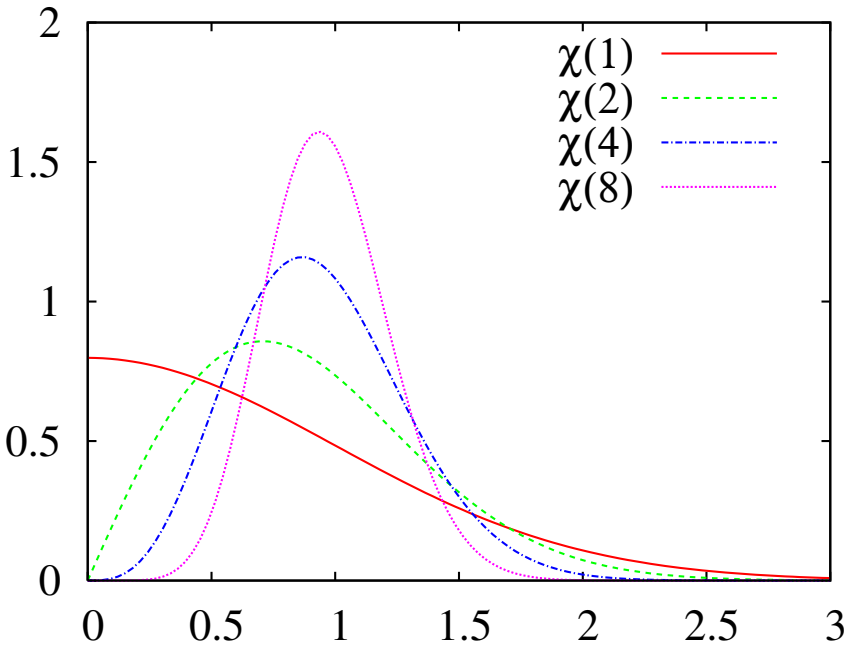

Figure 4.2: Probability distributions $\chi(1), \chi(2), \chi(4), \chi(8)$ of the radius of a Gaussian vector of dimension 1, 2, 4 and 8. When the dimension goes to infinity, the distribution gets closer to a Dirac distribution.

The rest of the chapter is organized as follows: Section 4.3 presents the link between the reconciliation and the security of the protocol, Section 4.4 describes the reconciliation in the case of discrete variables QKD protocols, Section 4.5 shows how to generalize this approach to Gaussian variables protocols. The performance of the scheme is finally analyzed in Section 4.6. The last section discusses some remaining open questions.

[8] in fact, there is actually a decrease of the complexity compared to slice reconciliation since here only one LDPC code needs being decoded against two codes for usual implementations of slice reconciliation [97].

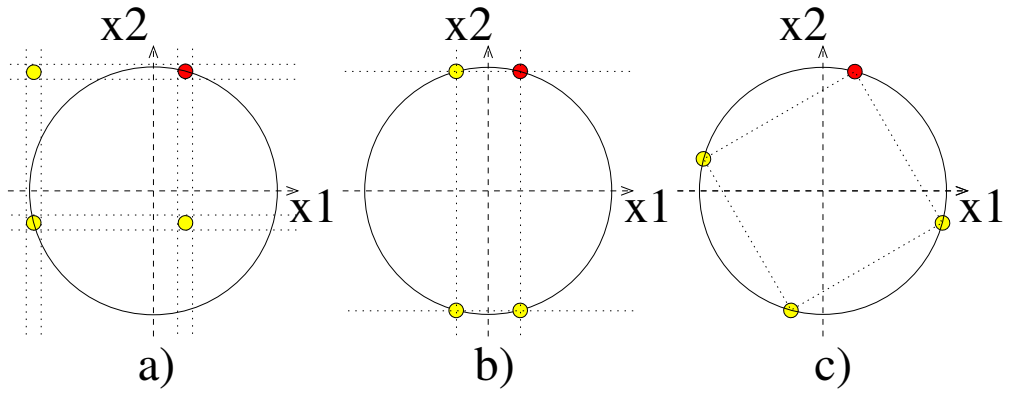

Figure 4.3: Consider two successive states x_1, x_2 sent by Alice: the states really sent correspond to $x_1 > 0, x_2 > 0$. Figures a), b) and c) show the four possible states Bob needs to discriminate after Alice has sent him some side information over the classical authenticated channel. a) corresponds to slice reconciliation [154, 14]: the four states are well separated but the Gaussian symmetry is broken, b) corresponds to the case where the information is encoded on the sign of the Gaussian value [144]: the symmetry of the problem is preserved but some states are very close and thus difficult to discriminate, c) corresponds to the approach presented in this paper where the states are well separated and the symmetry is preserved.

4.3 Reconciliation and security

The purpose of this section is to give a theoretical justification for the expression of the secret key rate K_{real} when taking into account the fact that the reconciliation procedure applied in practice is necessarily imperfect:

$$K_{\text{real}} = \beta I(A;B) - S(A;E). \tag{4.5}$$

More precisely, let x and y be the classical random variables associated with the measured quantities of the legitimate parties Alice and Bob, and let E refer to the quantum system of the eavesdropper. It has been shown [38] that the theoretical secret key rate K obtained using one-way reconciliation is bounded from below by

$$K \geq I(x;y) - S(x;E) \equiv K_{\text{th}} \tag{4.6}$$

if the adversary is limited to collective attacks[9]. Recall that $S(x;E)$ can also be seen as the Holevo quantity associated to the quantum measurements performed by Eve. This secret key rate is valid for one-way reconciliation: the classical communication between Alice and Bob is therefore restricted to be unidirectional, and not interactive. For the protocol described above, the quantum mutual information between Bob and Eve is smaller than between Alice and Eve. As a consequence, one will generally use

[9] but it was recently proven that this key rate remains valid against general attacks in the asymptotic limit [127].

reverse reconciliation [64]: the final key is extracted from Bob's data, and Bob sends extra information to Alice on the authenticated classical channel to help her correct her "errors". In this chapter, however, we are interested in describing a new reconciliation scheme. It turns out that this scheme works in the same manner for both direct and reverse reconciliations. Therefore, in order to simplify its description, we present it here in the context of direct reconciliation, but it could be applied without modification for a reverse reconciliation. However, the theoretical justification for the reverse reconciliation is slightly more involved and such complications are avoided here. In the next chapter, we will present a new CV QKD protocol, together with its specific reverse reconciliation, and will then elaborate on the differences between direct and reverse reconciliation.

The theoretical secret key rate K_{th} is only relevant in the case where one has access to a perfect reconciliation scheme, allowing Alice and Bob to extract all the information available in their correlated data. How should K_{th} be modified in the case of a real-world imperfect reconciliation scheme? In order to extract a secret from their data, Alice and Bob have access to a classical authenticated channel and have agreed on a particular code $\mathcal{C}_N$ whose size N is such that $\log_2(N) \leq I(x;y)$. The principle of the reconciliation protocol is the following: Alice chooses randomly an element $U \in \mathcal{C}_N$ and sends some information α to Bob who should be able to efficiently recover U from the knowledge of y and α, i.e., $H(U|y,\alpha) = 0$, the conditional entropy of U given y and α is null, or equivalently $I(U:y,\alpha) = H(U)$. In this case, Alice and Bob have extracted a common string U from their data, which they will be able to turn into a secret key thanks to privacy amplification, but they have also given the extra information α to the eavesdropper. As a consequence, the effective key rate after the reconciliation becomes:

$$K \geq H(U) - S(U:E,\alpha) \equiv K_{\text{real}}. \tag{4.7}$$

Unfortunately, one always has $K_{\text{real}} < K_{\text{th}}$ and K_{real} reaches 0 for a finite channel transmission. In other words, the range of the protocol is limited because of the imperfect reconciliation. It should be noted that this is one of the main differences with discrete variables protocols which are currently limited by technology, and more particularly by the dark counts of the photodetectors. A real difficulty lies in the estimation of $S(U:E,\alpha)$. One specificity of QKD is that it allows Alice and Bob to estimate an upper bound of $S(x:E)$ by comparing a subset of their data. However it is generally impossible to deduce $S(U:E,\alpha)$ from it. One exception is when U and α are independent[10], in which case the following lemma applies.

Lemma 4.1. *Let a and b be two classical random values, let E be a random quantum state. If a and b are independent, then $S(a:E,b) \leq S(a,b:E)$.*

[10]the independence of U and α is a crucial assumption here, which can easily be justified in the case of a direct reconciliation since the random variable x follows a genuine Gaussian modulation. In the case of a reverse reconciliation, this assumption is a priori more complicated to justify as Bob does not know a priori the distribution of the variable y. We will see in Chapter 5 that this issue can in fact be solved for a particular choice of U and α. Note also that this proof applies in the case of the reconciliation scheme presented in this chapter.

Proof. The chain rule for mutual quantum information reads:

$$S(a, b : E) = S(b : E) + S(a : E|b) \geq S(a : E|b) \tag{4.8}$$

where the inequality results from the non-negativity of mutual quantum information. Then, by definition of conditional mutual information,

$$\begin{aligned} S(a : E|b) &= S(a|b) - S(a|E, b) = S(a) - S(a|E, b) && (4.9) \\ &= S(a : E, b) && (4.10) \end{aligned}$$

where the second equality follows from independence of a and b. □

In the reconciliation protocol, U is chosen randomly by Alice, independently of x, meaning that $S(x, U : E) = S(x : E)$. Then, since α is a function of x and U, the data-processing inequality gives $S(U, \alpha : E) \leq S(x : E)$. In addition, in the case where α is independent of U, Lemma (4.1) gives: $S(U : E, \alpha) \leq S(x : E)$.
If one defines the efficiency of reconciliation

$$\beta = \frac{H(U)}{I(x : y)}, \tag{4.11}$$

one obtains finally

$$K_{\text{real}} \geq \beta I(x : y) - S(x : E), \tag{4.12}$$

which is the usual expression of the secret key rate taking into account the imperfect reconciliation protocol.

4.4 Reconciliation of binary variables

Reconciliation is a means for Alice and Bob to extract available common information from their correlated data. In the case when the data consists of binary strings, it is very similar to the problem of channel coding where the goal is for Alice to send information to Bob through a noisy channel. Channel coding is solved by appropriately choosing subsets of binary strings: codes. When Alice restricts her messages to codewords, Bob can recover them with high probability if the code size is not too large, given the channel noise. More precisely, Shannon's theorem [141] states that the size of the code $|\mathcal{C}|$ is bounded by the mutual information between Alice and Bob: $\log_2(|\mathcal{C}|) \leq I(x : y)$. The problem of channel coding has been extensively studied during the past 60 years, but only recently were discovered codes almost achieving Shannon's limit while being efficiently decoded thanks to iterative algorithms: turbocodes [13] and Low Density Parity Check (LDPC) codes [132].

The main difference between reconciliation and channel coding is that in the case of reconciliation, Alice does not choose what she sends and thus cannot restrict her messages to codewords of a given code. However, if one wants to take advantage of the code formalism, knowing what she sent, Alice can describe to Bob a code for which her

word is a codeword. Thus if Bob can guess what codeword Alice sent, they will effectively share a common sequence of bits. This is the method used for discrete QKD protocols. Indeed, given a linear code $\mathcal{C}$ and its parity check matrix H, the group $\mathbb{F}_2^n = \{0,1\}^n$ of possible states sent by Alice can be seen as the product of codewords and syndromes: if Alice sends x to Bob, she can tell him the syndrome of x which is $H \cdot x$ thus defining a coset code containing x. This coset code is the ensemble: $\{z \in \mathbb{F}_2^n | H \cdot z = x\}$. An equivalent solution is for Alice to randomly choose a codeword U from a given code and to send $U \oplus x = \alpha$ to Bob where $\oplus$ represents the addition in the group $\mathbb{F}_2^n$. Bob then computes $y \oplus \alpha$ which allows him to retrieve U if the code is well adapted to the channel between Alice and Bob. This coset coding scheme was initially suggested by Wyner [159].

In a way, the side information (information sent by Alice over the classical authenticated channel) corresponds to a change of coordinates allowing one to transform the initial reconciliation problem into the well-known problem of channel coding. Two properties are essential for this approach to work: first, the probability distribution of the states sent by Alice is uniform[11] over $\mathbb{F}_2^n$; second, the total space is a partition of the cosets of a linear code. Thus, any word can be seen as a unique codeword for a unique coset code and telling which coset code contains the word gives zero information about the codeword. The question is then whether or not it is possible to generalize this approach to continuous variables.

4.5 Reconciliation of Gaussian variables

4.5.1 Gaussian modulation

One of the main differences between discrete and continuous QKD protocols is the probability distribution of Alice's variables: the uniform distribution on $\mathbb{F}_2^n$ is changed into a *nonuniform* Gaussian distribution on $\mathbb{R}^n$. This is rather unfortunate since the uniformity of the distribution on $\mathbb{F}_2^n$ is an essential assumption in order to prove that the side information (e.g., the syndrome) Alice sends to Bob on the public channel does not give any relevant information to Eve about the codeword chosen by Alice. An interesting property of the Gaussian distribution $\mathcal{N}(0, \mathbb{1}_n)$ on $\mathbb{R}^n$ whose covariance matrix is the identity is that it has a spherical symmetry in $\mathbb{R}^n$. In other words, if the vector x follows such a distribution, then the normalized random vector $\frac{x}{|x|}$ has a uniform distribution on the unit sphere $\mathcal{S}^{n-1}$ of $\mathbb{R}^n$. Thus, spherical codes, codes for which all codewords lie on a sphere centered on 0, can play the same role for continuous-variable protocols as binary codes for discrete protocols. Some very good codes are known for binary channels: LDPC codes and turbocodes both almost achieve the Shannon limit and can be efficiently decoded thanks to iterative decoding algorithms. Are there codes with similar qualities among the spherical codes? The answer is almost. There is indeed a canonical way to convert binary codes into binary spherical codes and this can be achieved thanks

[11] In fact, this uniformity is not really required, but it greatly simplifies the theoretical analysis.

to the following mapping of $\mathbb{F}_2^n$ onto an isomorphic image in the n-dimensional sphere:

$$\mathbb{F}_2^n \to \mathcal{S}^{n-1} \subset \mathbb{R}^n, (b_1, \ldots, b_n) \mapsto \left(\frac{(-1)^{b_1}}{\sqrt{n}}, \ldots, \frac{(-1)^{b_n}}{\sqrt{n}} \right). \tag{4.13}$$

Then, as LDPC codes and turbocodes can both be optimized for binary symmetric channels, they can also be optimized for a binary phase shift keying (BPSK) modulation, where the bit 0 (1) is encoded into the amplitude $+A$ ($-A$), and where the channel noise is considered to be additive white Gaussian noise (AWGN). Thus, one has access to a family of very good codes (in the sense that they are very close to the Shannon limit) for which very efficient iterative decoding algorithms are available. It is important to note that there are actually two different Shannon limits considered here depending on the modulation, BPSK or Gaussian modulation, but these limits become asymptotically close when the signal-to-noise ratio (SNR) is small. Thus, at low SNR, a binary code optimized for a BPSK modulation can almost achieve the Shannon limit for a Gaussian modulation.

A remark is in order : the use of binary codes as described above limits the rate of the code to less than 1 bit per channel use, whereas one of the interests of a Gaussian modulation is precisely to get rid of this limit. Actually, one could use non-binary spherical codes, but their decoding is more complicated and thus slows down the reconciliation protocol. In addition, this is not really needed, since in the high loss scenario which interests us most here, the mutual information between Alice and Bob is always much less than 1 bit per channel use. Consequently the use of binary codes turns into an advantage, since they can be decoded very efficiently. In the low-loss case however, that is for short distances, one can hope to distill more than 1 bit per channel use, and the "usual" approach [97] will be more suitable than the one described in the present article (see also discussion in Sec. 4.6).

Now that we have a probabilistic space with a uniform probability distribution and a family of codes for this space, we need to see if the total space is a partition of a code and of its "generalized coset codes". First, the canonical hypercube of $\mathbb{R}^n$ (which is the image of $\mathbb{F}_2^n$ by the isomorphism defined above) is described as a partition of a linear code and its cosets. The question that remains to be solved is whether the unit sphere is a partition of such hypercubes. Another way to see this problem is the following: given a random point in $\mathcal{S}^{n-1}$, is there a hypercube inscribed in the sphere for which this point is a vertex? Surely there are such hypercubes, many in fact. Actually, the manifold of these hypercubes is a $[(n-1)(n-2)/2]$-dimensional manifold (this is the dimension of the subgroup of orthogonal group $\mathrm{O}(n)$ that transports the canonical hypercube onto the ensemble of hypercubes containing the point in question).

Yet another way to express the problem is the following: given two points $x, y \in \mathcal{S}^{n-1}$, is it possible to find an orthogonal transformation mapping x to y? One can immediately think of transformations such as the reflection across the mediator hyperplane of x and y. Unfortunately, such an orthogonal transformation gives some information about x and y as soon as $n > 2$ (this is linked to the phenomenon of concentration of measure for spheres in dimensions $n > 2$), and therefore cannot be used by Alice as legitimate side

information, which should be independent from the key in order to fulfill the hypothesis of Lemma 4.1.

A correct solution would then be to randomly choose an orthogonal transformation with uniform probability in the ensemble of orthogonal transformations mapping x to y. This can be done in the following way: one first draws a random orthogonal transformation mapping x to some random x'. Then one composes this transformation with the reflection across the mediator hyperplane of x' and y. Although theoretically correct, this procedure is not doable in practice for $n \gg 1$ since generating a random orthogonal transformation on $\mathbb{R}^n$ is a computational demanding task requiring to draw an $n \times n$ Gaussian random matrix and to calculate its QR decomposition (i.e., its decomposition into an orthogonal and a triangular matrix) which is an operation of complexity $O(n^3)$.

A practical solution involves the following scenario: for each word $x \in \mathcal{S}^{n-1}$ sent by Alice, for each codeword $U \in \mathcal{S}^{n-1}$ chosen by Alice (not necessarily a binary codeword), there should exist an continuous application M of the variables x and U such that $M(x,U) \in O_n$ and $M(x,U) \cdot x = U$. Then if Alice gives $M(x,U)$ to Bob, one has the continuous equivalent of $U \oplus x$ in the discrete protocol. The following theorem shows that the existence of such an application M restricts the possible values of n to be 1, 2, 4 or 8.

Theorem 4.1. *If there exists a continuous application*

$$\begin{array}{rccc} M: & \mathcal{S}^{n-1} \times \mathcal{S}^{n-1} & \longrightarrow & O_n \\ & (x,y) & \longmapsto & M(x,y) \end{array} \tag{4.14}$$

such that $M(x,y) \cdot x = y$ for all $x, y \in \mathcal{S}^{n-1}$, then $n = 1$, 2, 4 or 8.

The proof of this theorem uses a result from Adams [3], which quantifies the number of independent vector fields on the unit sphere of $\mathbb{R}^n$:

Theorem 4.2 (Independent vector fields on $\mathcal{S}^{n-1}$ (J.F. Adams, 1962))**.** *For $n = a \cdot 2^b$ with a odd and $b = c+4d$, one defines $\rho_n = 2^c + 8d$. Then the maximal number of linearly independent vector fields on $\mathcal{S}^{n-1}$ is $\rho_n - 1$.*

In particular, the only spheres for which there exist $(n-1)$ independent vector fields are the unit sphere of $\mathbb{R}$, $\mathbb{R}^2$, $\mathbb{R}^4$ and $\mathbb{R}^8$, which can respectively be seen as the units of the real numbers, the complex numbers, the quaternions and the octonions.

Proof of Theorem 4.1. The idea of the proof is to use the existence of such a continuous function M to exhibit a family of $(n-1)$ independent vector fields on S^{n-1}. Let $(e_1, e_2, \ldots, e_n)$ be the canonical orthonormal basis of $\mathbb{R}^n$. For $1 \leq i \leq n$, let $u_i(x) = M(e_n, x) \cdot e_i$. One has: $u_n(x) = x$ and

$$\begin{aligned} (u_i(x)|u_j(x)) &= e_i^T M(e_n,x)^T M(e_n,x) e_j & (4.15) \\ &= \delta_{i,j} \qquad \text{since } M(e_n,x) \in O_n. & (4.16) \end{aligned}$$

Then, for $x \in \mathcal{S}^{n-1}$, $u_1(x), u_2(x), \ldots, u_{n-1}(x)$ are $(n-1)$ independent vector fields on $\mathcal{S}^{n-1}$ and finally $n = 1, 2, 4$ or 8. □

4.5.2 Rotations on $\mathcal{S}^1$, $\mathcal{S}^3$ and $\mathcal{S}^7$

Now that we have proved that such an application M can only exist in $\mathbb{R}$, $\mathbb{R}^2$, $\mathbb{R}^4$ and $\mathbb{R}^8$, we need to answer three more questions: does it exist? Can Alice compute it efficiently? Does it leak any information about the codeword to Eve? Note that the trivial case of $\mathbb{R}$ for which the unit sphere is $\{-1, 1\}$ corresponds to the method where one encodes a bit in the sign of the Gaussian variable [144].

Existence. Let us start with the easiest case: $\mathbb{R}^2$. The existence of such an application M verifying $M(x, y) \cdot x = y$ for the unit circle is obvious: it is simply the rotation centered in O of angle $\mathrm{Arg}(y) - \mathrm{Arg}(x)$ where $\mathrm{Arg}(x)$ denotes the angle between x and the x-axis. An alternative way to see M is $M(x, y) = yx^{-1}$ where x and y are identified with complex numbers of modulus 1. The same is true for dimensions 4 and 8 where $\mathcal{S}^3$ and $\mathcal{S}^7$ can respectively be identified with the quaternion units and the octonion units, and for which a valid division exists.

Computation of $M(x, y)$. For $n = 2, 4$ and 8, there exists a (non-unique) family of n orthogonal matrices $\mathcal{A}_n = (A_1, \ldots, A_n)$ of $\mathbb{R}^{n\times n}$ such that $A_1 = \mathbb{1}_n$, and for $i, j > 1$, $\{A_i, A_j\} = -2\delta_{i,j}\mathbb{1}_n$ where $\{A, B\}$ is the anticommutator of A and B. An example of these families is explicitly given in Appendix A. The following lemma shows how to use such a family to construct a continuous function M with the properties described above.

Lemma 4.2. *$M(x, y) = \sum_{i=1\ldots n} \alpha_i(x, y)A_i$ with $\alpha_i(x, y) = (A_i x|y)$ is a continuous map from $\mathcal{S}^{n-1} \times \mathcal{S}^{n-1}$ to $O(n)$ such that $M(x, y)x = y$.*

Proof. First, because of the anticommutation property, one can easily check that the family $(A_1x, A_2x, \ldots, A_nx)$ is an orthonormal basis of $\mathbb{R}^n$ for any $x \in \mathcal{S}^{n-1}$. Then, for any $x, y \in \mathcal{S}^{n-1}$, $(\alpha_1(x, y), \ldots,$
$\alpha_n(x, y))$ are the coordinates of y in the basis $(A_1x, A_2x, \ldots, A_nx)$. This proves that $M(x, y)x = y$. Finally, the orthogonality of $M(x, y)$ follows from some simple linear algebra. □

Then $\alpha = (\alpha_1, \ldots, \alpha_n)$ is sufficient to describe $M(x, y)$ and the computation of α_i can be done efficiently since the matrices A_i are simply permutation matrices with a change of sign for some coordinates. In the QKD protocol, Alice chooses randomly u in a finite code and gives the value of $\alpha(x, u)$ to Bob, who is then able to compute $M(x, u)y$ which is a noisy version of u. One should note that the final noise is just a "rotated" version of the noise Bob has on x: in particular, both noises are Gaussian with the same variance.

No leakage of information. In order to prove that $\alpha = M(x, u)$ does not give any information about u, one needs to show that u and α are independent, in other words that: $Pr(u = u_i|M(x, u) = \alpha) = Pr(u = u_i) = \frac{1}{N}$ if one considers the spherical code

$\mathcal{C}_N = \{u_1, \ldots, u_N\}$. This is true because x and u have uniform distributions (on $\mathcal{S}^{n-1}$ and $\mathcal{C}_N$ respectively) and because the function:

$$\begin{array}{rccl} f_u: & \mathbb{R}^n & \longrightarrow & \mathbb{R}^n \\ & x & \longmapsto & f_u(x) = \alpha \text{ with } \alpha_i = (u|A_i x) \end{array} \tag{4.17}$$

has a constant Jacobian equal to 1 for each $u \in \mathcal{C}_N$. To see this, one should note that the lines of the Jacobian matrix of f_u are the $A_i^T u$ which form an orthonormal basis of $\mathbb{R}^n$.

Resulting channel capacity between Alice and Bob The channel between Alice and Bob is characterized by its signal-to-noise ratio (SNR). The capacity is achieved for a Gaussian modulation and is given by:

$$C = 1/2 \log_2(1 + \text{SNR}). \tag{4.18}$$

The reconciliation schemes presented above consist in the definition of a binary channel Q_X which results in a subcapacity for the channel. Figure 4.4 shows the subcapacities of the different cubes Q_X. First, if Q_X is a real n-dimensional cube (with width $2/\sqrt{n}$), then the channel defined by the reconciliation is the so-called BI-AWGN channel. It is the best binary channel one can hope for and corresponds to a rotation in $\mathbb{R}^n$ for $n \gg 1$. The subcapacities of the "sign coding" scheme [144] and of the rotations in $\mathbb{R}^8$ are also displayed, showing the improvement brought by the method presented in this paper for a signal-to-noise ratio around 1.

4.6 Application of the multi-dimensional reconciliation scheme to CVQKD

Now that we have explained how efficient reconciliation of correlated Gaussian variables can be achieved with rotations in $\mathbb{R}^8$, let us look at the implications in terms of performance for continuous-variable QKD.

At the end of the quantum part of the continuous-variable QKD protocol, Alice and Bob share correlated random values and their correlation depends on the variance of the modulation of the coherent states and on the properties of the quantum channel. The channel can safely be assumed to be Gaussian since it corresponds to the case of the optimal attack for Eve. This means that it can be entirely characterized by its transmission and excess noise. Both these parameters are accessible to Alice and Bob through an estimation step prior to the reconciliation [124]. Once these parameters are known, one can calculate the SNR of the transmission, which is the ratio between the variance of the signal (the variance of the Gaussian modulation of coherent states in our case) and the variance of the noise (noise induced by losses as well as excess noise). The SNR quantifies the mutual information between Alice and Bob when a Gaussian modulation is sent over a Gaussian channel:

$$I(A:B) = \frac{1}{2} \log_2(1 + \text{SNR}). \tag{4.19}$$

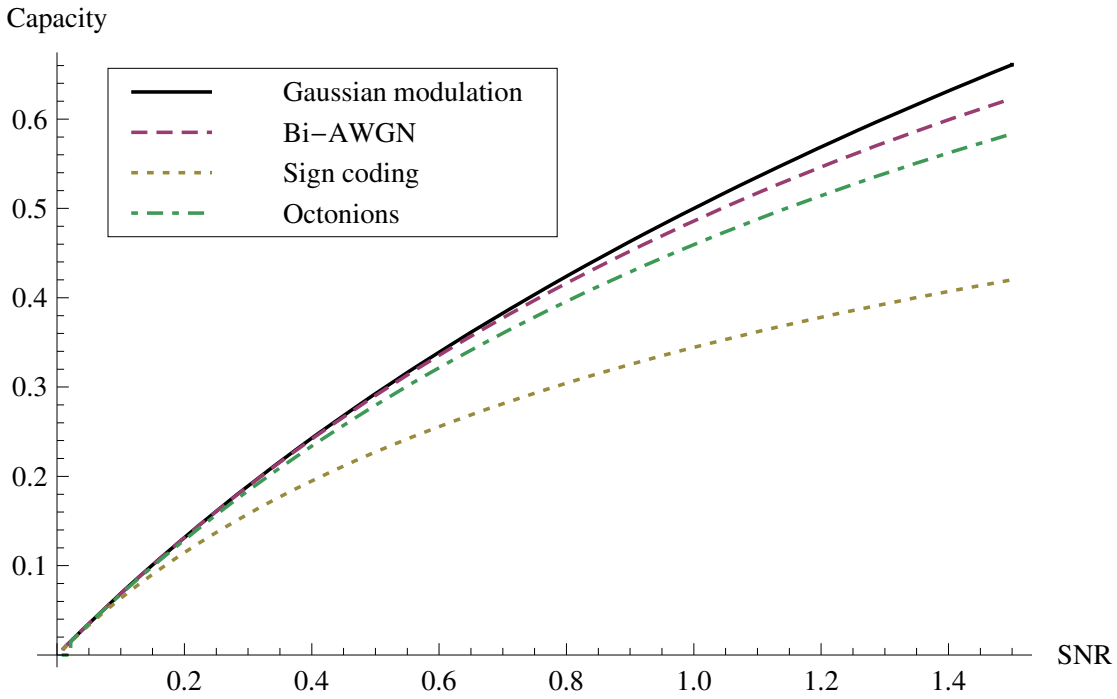

Figure 4.4: Capacity of the Gaussian channel and subcapacities for the different binary channels mentioned in the text: BI-AWGN channel (corresponding to a rotation in $\mathbb{R}^n$ for $n \gg 1$), "sign coding" [144] and the multidimensional reconciliation based on the properties of the octonions

Note also that the efficiency of the reconciliation only depends on the correlation between Alice's and Bob's data, that is, on the SNR. Thus, for a given transmission and excess noise, the secret key rate is a function of the SNR, which can be optimized by changing the variance of the modulation of the coherent states.

It is not easy to know exactly how the efficiency of reconciliation depends on the SNR. However, each reconciliation technique performs better for a certain range of SNR: slice reconciliation is usually used for a SNR around 3 [97] while rotations in $\mathbb{R}^8$ are optimal for a low SNR, typically around 0.5. Figure 4.5 shows the performance of rotations in $\mathbb{R}^8$ compared to slice reconciliation for typical experimental parameters [97, 48]. Both approaches achieve comparable reconciliation efficiencies (around 90%) but for different SNR. One can observe two distinct regimes: for low loss, i.e., short distance, slice reconciliation is better but only rotations in $\mathbb{R}^8$ allow QKD over longer distances (over 50 km with the current experimental parameters).

Concerning the complexity of the reconciliation, one should be aware that almost all the computing time is devoted to decoding the efficient binary codes, either LDPC codes or turbocodes. Compared to this decoding, the rotation in $\mathbb{R}^8$ only takes a negligible amount of time. Thus, the complexity of the reconciliation presented here is smaller than the one of slice reconciliation since the latter uses several codes (one code per slice).

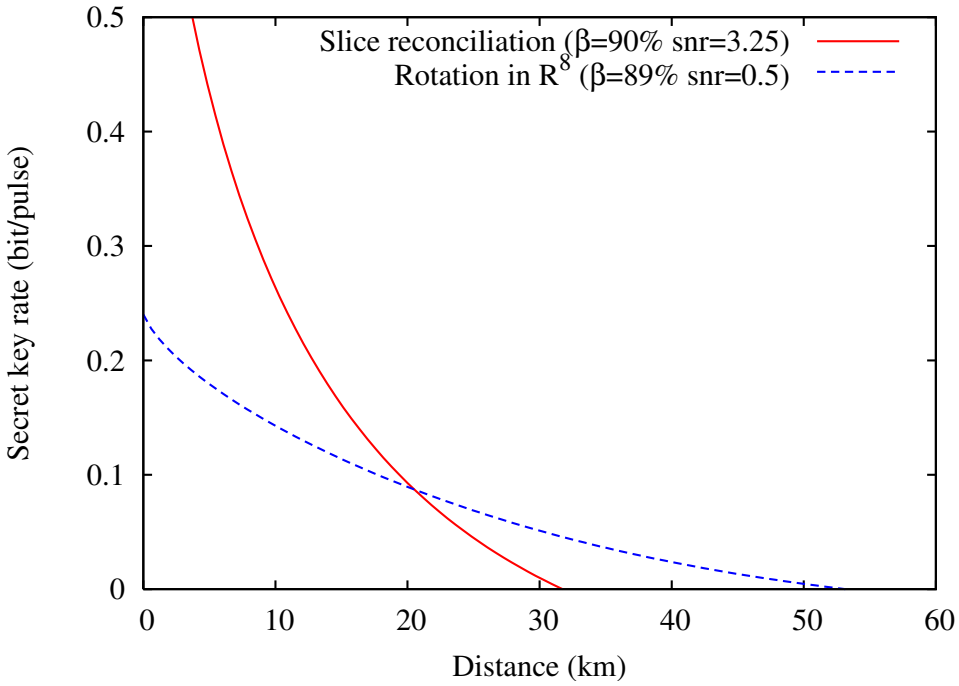

Figure 4.5: Performance of slice reconciliation vs rotation in $\mathbb{R}^8$. Experimental parameters: excess noise referred to the channel input $\xi = 0.005$, efficiency of Bob's detector $\eta = 0.606$ and electronic noise at Bob's side $V_{elec} = 0.041$ [97]. The reconciliation based on rotations in $\mathbb{R}^8$ uses a LDPC code of rate 0.26 [72]

4.7 Conclusion and open questions

We presented a protocol for the reconciliation of correlated Gaussian variables, which is is particularly well adapted for low signal-to-noise ratios. This turns out to be very interesting as it is exactly encountered when one wants to perform QKD over long distances. By taking into account current typical experimental parameters, one shows that this new reconciliation allows QKD over more than 50 km. Moreover, contrary to other protocols that have been proposed to increase the range of continuous-variable QKD, this protocol does not require any postselection. Hence, the security proofs based on the optimality of Gaussian attacks remain valid, meaning that the protocol is secure against general collective attacks, and even general attacks in the asymptotic limit.

If the mountain won't come to Muhammad. It should be pointed out that we deliberately chose a practical approach for the problem of the reconciliation of correlated Gaussian variables. Indeed, a maybe more natural approach would have been to see the problem as purely a coding problem. A possible solution for this problem is to design good spheric codes in n dimensions. Here, we did not follow such a path. On the

contrary, the motivation was to avoid designing new codes as there already exist very good codes (close to the Shannon limit, and with an efficient decoding algorithm) for a different but related channel, the BI-AWGN channel. The idea was then to see if these optimized codes could be used for the reconciliation problem and thus avoid to optimize specific codes for our problem. Our approach turned out to work rather well in practice, and had the additional advantage to be easily incorporated within existing security proofs. Indeed, in sharp contrast with regular channel coding, QKD is characterized by the presence of a potential adversary who can listen to all classical messages exchanged by Alice and Bob.

A few words concerning the optimal modulation variance, or equivalently the optimal signal-to-noise ratio. The security analysis of CV QKD (protocol GG02 as well as other protocols using squeezed states) has often been performed in the limit of an infinite modulation variance [62, 105]. However, it turns out that this regime is never interesting *in practice*. The reason it is not relevant is because it is an "unstable regime". Indeed, it is shown that the quantity $I(A;B)-S(B;E)$ tends to a finite limit when the modulation variance tends to infinity [62]. However, both $I(A;B)$ and $S(B;E)$ diverge in this case. This means that the realistic key rate $K_{\text{real}} \equiv \beta I(A;B) - S(B:E)$ becomes zero as soon as the reconciliation efficiency is strictly less than 1. To be fair, if one can ensure than the reconciliation efficiency is sufficiently close to 1 as the modulation variance increases, then the secret key rate might be positive. However, all the reconciliation schemes presently known seem to achieve a reconciliation efficiency which is less than 95 % for instance. Therefore, with the reconciliation techniques available today, considering the limit of large modulation variance is only an intellectual exercise without any practical relevance.

Is there a solution for the reconciliation problem for a Gaussian modulation? Even if the new reconciliation scheme described in this chapter brings a great improvement compared to previous known techniques, such as slice reconciliation, in the low SNR regime, it does not get rid of the problem. Efficient reconciliation (meaning that the reconciliation efficiency is at least 80%) is possible for signal-to-noise ratios greater that roughly 0.5, but unfortunately, the technique reaches its limits for lower SNR. This is problematic as it appears that one needs to work at very low SNR to reach longer distances. For this reason, even if the solution proposed here is a step in the right direction, it is not entirely satisfying as it does not completely solve the reconciliation problem for CV QKD with a Gaussian modulation. Solving this problem would mean (as is the case for most discrete-variable protocols) that the range of the protocol would be limited by noise in the detectors (dark counts for DV QKD, or excess noise for CV QKD). This is clearly not yet the case with continuous-variable QKD.

CHAPTER 5

Long distance CVQKD: protocols with a discrete modulation

The goal of this chapter is to improve the existing continuous-variable QKD protocols so that larger distances can be reachable[1]. Before this work, discrete-variable QKD seemed to achieve much more than one hundred kilometers[2] whereas continuous-variable QKD was only demonstrated over 30 km [97, 48] and theoretically possible over 50 km (see previous chapter and [91]). The question that we want to address here is whether this situation is accurate, meaning that 100 kilometers will always be out of reach of experimental CV QKD, as seems to be the case for the GG02 protocol which is limited by the reconciliation efficiency, despite using the best error correction techniques available. We will see in this chapter that continuous-variable QKD is not intrinsically limited to short distances, and that one can overcome the main limitation (reconciliation efficiency) by slightly modifying the original GG02 protocol, more specifically by switching from a

[1]The content of this chapter was the object of a publication in Physical Review Letters [93] and of a pending patent.

[2]although one should be careful when comparing performances of different protocols for which the security assumptions might significantly differ.

Gaussian modulation to a discrete modulation, but without including any postselection procedure which cannot be proved secure with any known technique. The main new idea is therefore to exploit a binary modulation in order to improve the reconciliation efficiency at very low SNR.

A comment on the realist mode and on typical values of the experimental parameters. In this chapter, one is interested in improving the current CV QKD protocols in order to increase their range. In accordance with what we wrote in Chapter 3, we consider here a realist mode where Bob's detection stage is calibrated. This calibration includes the quantum efficiency η as well as the electronic noise of the detector V_{elec}. It turns out that the exact value of the electronic noise has only a negligible impact on the final secret key rate. Moreover, distinguishing η from the total transmission T of the quantum channel also has a negligible impact on the final key rate. For these reasons, the secret key rate obtained in a realist mode with reasonable values for both parameters ($\eta \geq 0.5$ and V_{elec} around a few percent of the shot noise) is very close from the secret key rate obtained in a paranoid mode when the electronic noise is supposed to be null. Hence, in order to simplify the computations in this chapter, we will consider a paranoid mode where $V_{\text{elec}} = 0$ and the total transmission of the channel varies as

$$T = \eta 10^{-0.02d}, \tag{5.1}$$

where d is the distance between Alice and Bob in kilometers and $\eta = 0.6$ which corresponds to typical experimental implementations [48]. Therefore, the secret key rate only depends on the distance d, the reconciliation efficiency, and the excess noise ξ. A typical value for the excess noise is around one percent of the shot noise.

5.1 Longer distances mean lower SNR

A first important remark is that reconciliation efficiency is a crucial parameter to estimate the performance of a CV QKD protocol. Second, the reconciliation efficiency alone is not a sufficient criterium, one needs to know at which signal-to-noise ratio (SNR) a given reconciliation efficiency can be achieved. It is indeed pretty clear that, for a Gaussian quantum channel, or more precisely an additive white Gaussian noise (AWGN) channel[3], the reconciliation efficiency is a function of the SNR. Figure 5.1 displays the maximum distance that can be achieved by a CV QKD protocol (such as the GG02 protocol) as a function of the SNR of the channel. Three curves are displayed corresponding respectively to reconciliation efficiencies of 99%, 90% and 80%, meaning that such efficiencies are supposed to be achieved for the SNR considered. Note that these three values corresponds respectively to an ideal, but rather unrealist situation ($\beta = 99\%$), a very good reconciliation efficiency which can be attained with state-of-the-art coding

[3] an AWGN channel for the classical data shared by Alice and Bob corresponds to a quantum Gaussian channel that does not mix the quadratures and that has the same effect on both quadratures. Such a channel is completely described by its transmission T and excess noise ξ.

techniques[4] ($\beta = 90\%$), and finally to a more reasonable value of the reconciliation efficiency ($\beta = 80\%$). From Figure 5.1, one can infer that gaining a few percents for the reconciliation efficiency immediately translates into an increased range for the QKD protocol. However, the real insight brought by Figure 5.1 is that it is not the value of the reconciliation efficiency that really matters, but rather the signal-to-noise ratio at which such a value can be obtained. In particular, it is striking to note that the solution to increase the range of CV QKD is *not* to work to bring the reconciliation efficiency impossibly close to the maximum theoretical value of 100 % but rather to work to be able to get reasonable reconciliation efficiencies at *very low* SNRs.

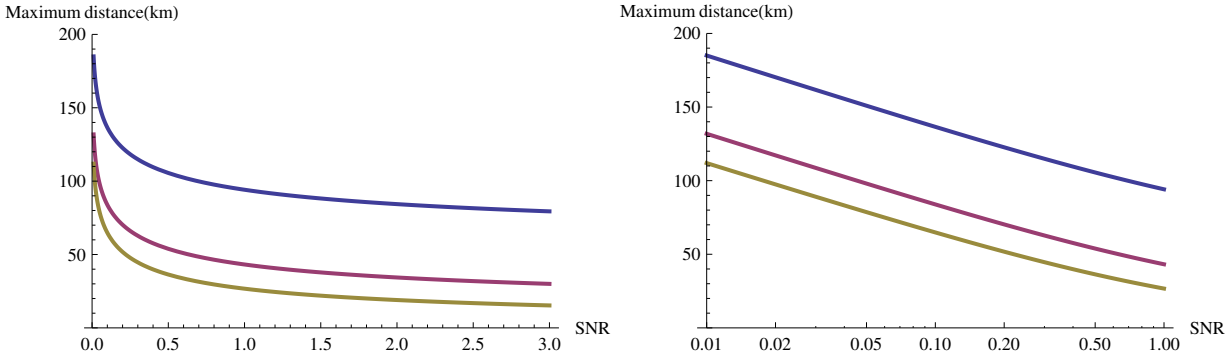

Figure 5.1: Maximal distance reachable for a CV QKD protocol as a function of the SNR. On the left, we use a linear scale for the SNR, on the right, we use a logarithmic scale in order to analyze the situation at very low SNR. The excess noise is 0.01 which is a typical value encountered in experiments (note the plots are almost the same for an excess noise of 0.001). From top to bottom, the reconciliation efficiency considered is 0.99, 0.9 and 0.8.

So far, the problem of obtaining good reconciliation efficiencies for a protocol with a Gaussian modulation has not been solved in a very satisfying manner. The *slice reconciliation* technique [154], even with the help of LDPC codes [14] is not capable to perform efficiently when the SNR is too low. The technique presented in the previous chapter improves things a little, but the SNR should not be much less than 0.5 in order to get an efficient reconciliation. Hence, both these strategies fail if one needs to work with a SNR of 1/100 for instance.

The goal of this chapter is therefore to investigate whether it is possible to modify the original GG02 protocol, in such a way that the reconciliation can be performed efficiently at low SNR, and that the security of the scheme can be proven.

[4] and a substantial amount of computing power, which might lead to a possible slow-down of the key distribution

5.2 Reconciliation at very low SNR

As we saw so far, reconciliation of correlated Gaussian variables is quite complicated at low SNR, and the present techniques are not efficient in this regime. A possible approach would be to keep searching for better and better reconciliation algorithms at low SNR, but the adversarial context of reconciliation where Alice and Bob should not publicly exchange any information that might help Eve (who is supposed to have access to an infinite amount of computational power) makes the task even more difficult.

Another strategy, that we choose to follow here, is to change the quantum protocol in a way that directly solves the reconciliation problem at (very) low SNR. This is achieved simply by switching from a Gaussian modulation to a discrete modulation. The idea is that the classical data that are used as input of the reconciliation scheme should be the same as those of a BI-AWGN channel, that is a classical binary modulation followed by an additive white Gaussian noise channel. To do this, Alice should send coherent states such that an homodyne detection of either one of the quadratures leads to a BI-AWGN classical channel. This can be done by either one of the two following modulation schemes:

- Alice sends randomly one of the two coherent states from the set

$$\mathcal{S}_2 = \{\alpha e^{-i\pi/4}, -\alpha e^{-i\pi/4}\}, \tag{5.2}$$

  where α is a positive number such that $2\alpha^2$ corresponds to Alice's modulation variance. This is the modulation used in our new *two-state protocol*.

- Alice sends randomly one of the four coherent states from the set

$$\mathcal{S}_4 = \{\alpha e^{i\pi/4}, \alpha e^{3i\pi/4}, \alpha e^{5i\pi/4}, \alpha e^{7i\pi/4}\}. \tag{5.3}$$

  This is the modulation used in our new *four-state protocol*.

For both modulation schemes, Bob will "see" an effective BI-AWGN channel for either choice of quadrature. Assuming that the quantum channel is known and is indeed Gaussian (which is the case in actual experiments), Alice and Bob can model their classical data respectively as $x = (x_1, \cdots, x_n)$ (with $x_i = \pm\alpha/\sqrt{2}$) and $y = (y_1, \cdots, y_n)$ (here we assume that $N - n$ data have already been used to estimate the parameters, transmission and excess noise, and that Bob has informed Alice of his choice of quadrature in the four-state protocol). Therefore, y_i corresponds to Bob's measurement result for the signal i (normalized with the transmission) and x_i corresponds to the corresponding quadrature for Alice's state. The Gaussian channel model reads:

$$y_i = x_i + z_i, \tag{5.4}$$

where z_i is a normal random variable with known variance σ^2 and x_i is simply an unbiased Bernoulli random variable (that we can assume takes values $+1$ or -1 up to a simple renormalisation). With these notations, the signal-to-noise ratio is given by:

$$\mathrm{SNR} = \frac{1}{\sigma^2}, \tag{5.5}$$

and we would like to find reconciliation scheme that perform well, say $\beta = 80\%$, for very small values of the SNR, for instance $1/100$, or even less.

Good low rate error correcting codes. First of all, the reconciliation procedure is necessarily based on good error correcting codes, such as low-density parity-check (LDPC) codes[5]. Despite their great performances, LDPC codes are not universal in the sense that they have not been optimized for every channel. For instance, they perform very well for the BI-AWGN channel when their rate is at least 0.2. The reason for this is that it is not profitable for the telecom industry to work with very noisy channels: it would cost too much to send reliable information. Therefore, there was no particular incentive to develop very good, very low rate LDPC codes. The situation is rather different in the context of quantum key distribution. Here, classical communications are considered as almost free, and requiring a large amount of error correction is not a problem. Quite on the contrary, classical noise is useful in a sense, as it helps to hide the information from the eavesdropper.

A special kind of LDPC codes was recently developed to work at reasonably low SNR: these are the *multi-edge* type LDPC codes [131]. These perform very well for rates as low as $1/10$. Even if they help working at low SNR, these codes do not solve our problem completely as we would like codes working at much lower rates. What rate do we need exactly? The rate R is linked to the reconciliation efficiency β through

$$\beta = \frac{R}{C_{\text{Gauss}}}, \tag{5.6}$$

where

$$C_{\text{Gauss}} = \frac{1}{2}\log_2(1+s) \tag{5.7}$$

is the capacity of the AWGN channel (which is achieved with a Gaussian modulation) and s is the SNR. Since in our protocol, we are restricted to a binary modulation, this capacity cannot be reached, and the maximal value of the mutual information between Alice and Bob is given by the capacity of the BI-AWGN channel, $C_{\text{BI-AWGN}}(s)$:

$$C_{\text{BI-AWGN}}(s) = -\int \phi_s(x)\log_2(\phi_s(x))dx - \frac{1}{2}\log_2(2\pi e) + \frac{1}{2}\log_2(s) \tag{5.8}$$

where

$$\phi_s(x) = \sqrt{\frac{s}{8\pi}}\left(e^{-s(x+1)^2/2} + e^{-s(x-1)^2/2}\right). \tag{5.9}$$

Quite interestingly, for small values of the SNR, both quantities C_{Gauss} and $C_{\text{BI-AWGN}}$ are almost equal as can be seen on Figure 5.2. However, the two quantities are obviously quite different for large SNR as the Gaussian capacity is unbounded whereas the capacity for a binary modulation is upper bounded by 1: one cannot send more than one bit of information per channel use with a binary modulation. With these notations, one can

[5]The history of LDPC codes is quite interesting. There were initially invented by Robert Gallager in 1963, but were impractical at that time [49]. They since were forgotten for more than 30 years and rediscovered in 1996 [101]. Now LDPC codes almost achieve the Shannon capacity of AWGN channels [132] and are therefore widely used in the telecom industry.

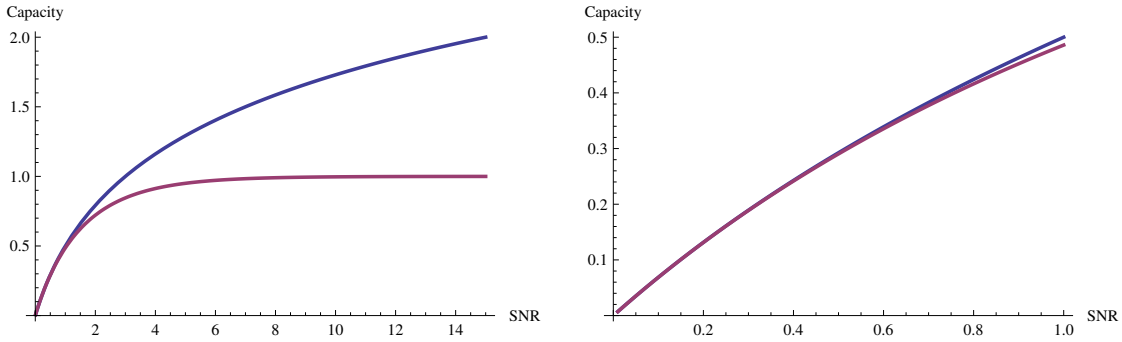

Figure 5.2: Channel capacities for an AWGN channel with a Gaussian modulation (upper curves) and a binary modulation (lower curves) as a function of the signal-to-noise ratio

rewrite the reconciliation efficiency as

$$\beta = \beta_{\text{modulation}} \frac{R}{C_{\text{BI-AWGN}}}, \tag{5.10}$$

where

$$\beta_{\text{modulation}} = \frac{C_{\text{Gauss}}}{C_{\text{BI-AWGN}}} \tag{5.11}$$

is a factor that rapidly tends to 1 as the signal-to-noise ratio tends to 0, and the second term $R/C_{\text{BI-AWGN}}$ directly reflects the performance of a given code of rate R on the BI-AWGN channel. In the limit of low SNR, we can approximate $\beta_{\text{modulation}} \approx 1$, meaning that the code rate that we require is given as a function of the SNR s by

$$R(s) \approx \frac{\beta}{2} \log_2(1+s) \tag{5.12}$$

$$\approx \frac{\log_2 e}{2} \beta\, s. \tag{5.13}$$

Since we want to fix the value of the reconciliation efficiency (for instance to 80%), we see that we need to find error correcting codes with a rate proportional to the signal-to-noise ratio. Hence, we would like to have a process such that if we know a code with rate R and efficiency β for a SNR s, we can construct a code with rate $R' = R/k$ (for some integer $k \geq 2$) which achieves an efficiency β' close to β at a SNR $s' = s/k$. This can be done quite simply with the idea of *repetition code*. Let us indeed consider the following scenario: instead of sending a random $x_i = \pm 1$ for each use of the channel, Alice sends k times the same value, that is, $x_{i_1} = x_{i_2} = \cdots = x_{i_k} \equiv X_i$. Hence Bob receives k noisy versions of X_i:

$$y_{i_1} = x_{i_1} + z_{i_1} \tag{5.14}$$

$$y_{i_1} = x_{i_1} + z_{i_1} \tag{5.15}$$

$$\cdots = \cdots \tag{5.16}$$

$$y_{i_k} = x_{i_k} + z_{i_k}, \tag{5.17}$$

where $z_{i_1}, z_{i_2}, \cdots, z_{i_k}$ are k independent and identically distributed random variables: $z_{i_j} \sim \mathcal{N}(0, \sigma^2)$ for $j \in \{1, \cdots, k\}$. Let us now consider the new random variables defined as:

$$X_i \equiv \frac{1}{k}\sum_{j=1}^{k} x_{i_j}, \quad Y_i \equiv \frac{1}{k}\sum_{j=1}^{k} y_{i_j}, \quad Z_i \equiv \frac{1}{k}\sum_{j=1}^{k} z_{i_j}. \tag{5.18}$$

One has

$$Y_i = X_i + Z_i, \tag{5.19}$$

with $X_i = \pm 1$, and $Z_i \sim \mathcal{N}(0, \frac{\sigma^2}{k})$. The new channel with input X_i and output Y_i is therefore also a BI-AWGN channel but with a signal-to-noise ratio k times higher than for the initial channel. Hence, if one knows a code with rate R achieving a reconciliation efficiency $\beta(s)$ for a BI-AWGN channel with SNR s, one can use a repetition scheme length k to build a code of rate $R' = R/k$ achieving a reconciliation efficiency $\beta'(s/k)$ for a SNR $s' = s/k$. The new reconciliation efficiency $\beta'(s/k)$ is given by

$$\beta'(s/k) = \beta(s)\,\frac{\log_2(1+s)}{k\,\log_2(1+s/k)}. \tag{5.20}$$

For small values of s, this gives $\beta'(s/k) \approx \beta(s)$ as expected. Unfortunately, as we said before, good codes are not known for very small values of s, and the best low rate codes presently available are the multi-edge type LDPC codes. In particular, the code of rate 1/10 described in [131] manages to decode reasonably well for a SNR of 0.17. This means that this code is such that $\beta(0.17) \approx 88\%$. Using equation 5.20, one observes that for all $k \geq 1$, $\beta'(0.17/k) \geq 80\%$. Hence, we can construct codes with arbitrarily low rate that have a reconciliation efficiency greater that 80%. We plot the performance of such codes on Figure 5.3 where we compare it with the reconciliation efficiency achieved with a Gaussian modulation. The difference is striking for low SNR: our concatenation of repetition codes with multi-edge type LDPC codes has a reconciliation efficiency alway greater than 80% when the SNR tends to zero, whereas the reconciliation efficiency is good (in the sense that in can be used in a CV QKD protocol) only for large enough SNR[6].

Specificities of the reverse reconciliation. Until now, we described a generic method to achieve a good reconciliation efficiency on channels with arbitrarily low SNR. Unfortunately, the approach we described is not directly compatible with QKD. The reason for this is two-fold:

- first, Alice cannot choose to send k times in a row the same quantum state, as this might give some information to the eavesdropper[7],

[6] Actually, using the multidimensional reconciliation presented in Chapter 4 improves things a little, but the conclusion is almost the same: there is a minimal value of the SNR below which the reconciliation scheme is not efficient enough to allow for the distillation of secret keys.

[7] in fact, this is not necessarily problematic as one could probably extend the security proof presented later in this chapter to the case where Alice sends many times the same quantum state.

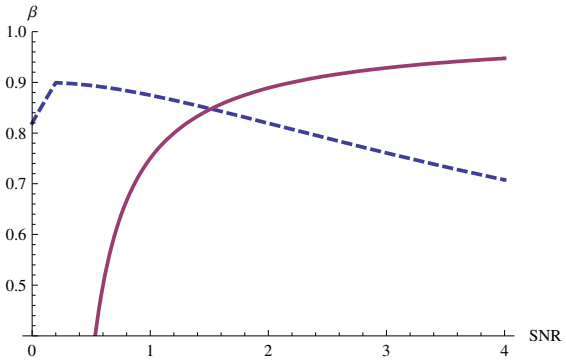

Figure 5.3: (Color online) Practical reconciliation efficiency for a binary modulation (dashed line) and for a Gaussian modulation (full line) [14].

- but, more importantly, continuous-variable QKD uses *reverse reconciliation*, meaning that Alice needs to guess Bob's measurement result, and not the other way around which would correspond to a direct reconciliation scheme. The problem here is that Bob cannot decide to measure k times in a row the same value. Moreover, it is not completely clear that the channel corresponding to the reverse reconciliation procedure is a BI-AWGN channel as well. We now proceed by answering these two points.

The reverse reconciliation channel. As we said, whereas the direct reconciliation channel is a BI-AWGN channel:

$$\text{input:} \quad x = \pm 1 \quad \longrightarrow \quad \text{output:} \quad y = x + z \quad \text{with} \quad z \sim \mathcal{N}(0, \sigma^2), \tag{5.21}$$

it is not clear what the reverse reconciliation channel is, simply because its input in real-valued (instead of binary), and that its output is binary instead of being real-valued! In fact, it turns out that this reverse reconciliation channel can be transformed into a BI-AWGN channel, if Bob sends some side-information to Alice. Our goal is to define two variables u for Bob and v for Alice such that the channel mapping u to v is a BI-AWGN channel. This can be done through the following procedure. First Bob computes two values u and the side-information t from his variable y. These two numbers are defined as

$$\left\{ \begin{array}{rcl} u & = & y/|y|, \\ t & = & |y| \end{array} \right. \tag{5.22}$$

Note that for an AWGN channel, the variables u and t are independent: the sign of y is independent from its absolute value since the distribution of y is symmetric. One can also note that u is a unbiased Bernoulli random variable, and therefore corresponds to a legitimate input for a BI-AWGN channel. Now, t is considered as a side-information and is sent by Bob to Alice, who can use it to compute a random variable v defined as

$$v = \left\{ \begin{array}{rcl} t & \text{if} & x = 1, \\ -t & \text{if} & x = -1. \end{array} \right. \tag{5.23}$$

One can check that u and v are related through

$$v = u + w, \tag{5.24}$$

where

$$\begin{aligned} w &= v - u && (5.25)\\ &= \mathrm{sgn}(x)|y| - \mathrm{sgn}(y) && (5.26)\\ &= \mathrm{sgn}(y)\,(\mathrm{sgn}(x)y - 1) && (5.27)\\ &= \mathrm{sgn}(y)\,(\mathrm{sgn}(x)(x+z) - 1) && (5.28)\\ &= \mathrm{sgn}(y)\,(1 + \mathrm{sgn}(x)\,z - 1) && (5.29)\\ &= \mathrm{sgn}(xy)\,z && (5.30) \end{aligned}$$

which means that $w \sim \mathcal{N}(0, \sigma^2)$ since $\mathrm{Prob}(\mathrm{sgn}(xy) = 1) = \mathrm{Prob}(\mathrm{sgn}(xy) = -1) = 1/2$. Hence, the channel corresponding to the reverse reconciliation scenario, taking u as input and v as output is a BI-AWGN channel.

Let us now show how one can apply the repetition trick to this channel. The main problem now is that one would want u_{i_1} to be equal to $u_{i_2}, \cdots, u_{i_k}$. Obviously, there is only one chance over 2^{k-1} for this to happen. The way to overcome this difficulty is in fact quite simple. In the direct reconciliation protocol, Bob would need to guess whether $(x_{i_1}, \cdots, x_{i_k})$ equals $(1, \cdots, 1)$ or $(-1, \cdots, -1)$. In the reverse reconciliation protocol, Bob will inform Alice of the signs of $y_{i_2}, \cdots, y_{i_k}$ relatively to the sign of y_{i_1} (which therefore encode the relevant information), that is, Bob will give Alice the following $(k-1)$ values: $\mathrm{sgn}(y_{i_1} y_{i_2}), \cdots, \mathrm{sgn}(y_{i_1} y_{i_k})$. Hence, in the reverse reconciliation protocol, Alice needs to guess whether $(y_{i_1}, \cdots, y_{i_k})$ equals $(1, y_{i_1} y_{i_2}, \cdots, y_{i_1} y_{i_k})$ or $(-(1, -y_{i_1} y_{i_2}, \cdots, -y_{i_1} y_{i_k})$. Clearly, this problem is completely equivalent to the direct reconciliation case. In fact, this solution exactly corresponds to Bob informing Alice of the syndrome of his bit string relative to the repetition code of length k.

To summarize, the reconciliation procedure starts with Alice and Bob having two correlated vectors of length $k \times m$: $(x_1, \cdots, x_{km})$ and $(y_1, \cdots, y_{km})$. Bob defines the vector $\mathbf{u} = (u_1, \cdots, u_{km})$ and sends some side information to Alice, namely the vector $\mathbf{t} = (t_1, \cdots, t_{km})$ as well as the m vectors $(1, \mathrm{sgn}(y_{ki+1} y_{ki+2}), \cdots, \mathrm{sgn}(y_{ki+1} y_{ki+k})$ so that Alice needs to guess the value of the vector $\mathbf{U} = (\mathrm{sgn}(u_1), \mathrm{sgn}(u_{k+1}), \mathrm{sgn}(u_{2k+1}), \cdots, \mathrm{sgn}(u_{(m-1)k+1}))$, which is a binary vector of length m. To do this, Alice and Bob first agree on a particular multi-edge type LPDC code C, and Bob sends the syndrome of $\mathbf{U}$ relative to C to Alice. Alice simply proceeds by decoding C in the coset code defined by the syndrome in question, and recovers $\mathbf{U}$.

To conclude, it is easy to adapt the error correction scheme to a reverse reconciliation procedure: it simply involves for Bob to send some well-chosen side-information to Alice through the authenticated classical channel. For a Gaussian channel, this side-information is useless to Eve as it does not contain any information on the vector U. A more detailed discussion on the potential role of this side-information for the security of the protocol can be found in Section 5.7 of this chapter.

The repetition scheme presented above provides a simple method to build a good code of rate R/k out of a code of rate R. This construction is not optimal compared to using a very good error correcting code at the considered signal-to-noise ratio but exhibits some interesting features. First, designing very good codes at low SNR is not easy, and has not been intensively studied so far, mainly because the telecom industry does not operate in this regime: this would not be economical since an important number of physical signals would be required to send one information bit. The problem is very different in QKD, where quantum noise is an advantage rather than a drawback. A second advantage of this repetition scheme lies in its simplicity. As we mentioned earlier, the main bottleneck of CV QKD is the reconciliation : it used to limit both the range and the rate of the protocol. In particular, the rate is limited by the complexity of decoding LDPC codes, which is roughly proportional to the size of the code considered (in fact $O(N \log N)$). If one uses a repetition scheme of length k, then the length of the genuine LDPC code becomes $m = N/k$ allowing a speedup of a factor k. The speed of the reconciliation is not proportional to the number of signals exchanged by Alice and Bob anymore, but to the mutual information they share, which is a major improvement for noisy channels, *i.e.*, long distance. Finally, the penalty in terms of reconciliation efficiency imposed by using this scheme instead of a dedicated low rate error correcting code is actually quite small, as soon as one knows a good low rate code. As we saw, a multi-edge type code of rate 1/10 is sufficient for our purpose.

Now that we have an efficient reconciliation algorithm available at (very) low SNR, let us introduce new continuous-variable QKD protocols that can make a good use of it.

5.3 Presentation of the new discrete-modulation protocols

5.3.1 CV QKD protocols with a discrete modulation

In the following, we consider two CV QKD protocols with a discrete modulation involving respectively two and four coherent states. In any such protocol, Alice sends N random states drawn from a specified set of coherent states, either $\mathcal{S}_2$ or $\mathcal{S}_4$. For instance, in the two-state protocol[8], the set of coherent states is $\mathcal{S}_2 = \{|\alpha e^{-i\pi/4}\rangle, |-\alpha e^{-i\pi/4}\rangle\}$ while the set corresponding to the four-state protocol is $\mathcal{S}_4 = \{|\alpha e^{i\pi/4}\rangle, |\alpha e^{3i\pi/4}\rangle, |\alpha e^{5i\pi/4}\rangle, |\alpha e^{7i\pi/4}\rangle\}$. As before, α is a positive number. Then Bob performs an homodyne measurement on a random quadrature x or p. He obtains a real random variable y_i for $i \in \{1, \cdots, N\}$. Alice and Bob use a reverse reconciliation, and the sign of y_i encodes the raw key bit, as described in the previous section. Alice then recovers the value of the sign of y_i. An alternative for the four-state protocol consists for Bob to perform an heterodyne measurement instead of an homodyne measurement. In this case, he measures both quadratures,

[8]It should be noted that a slight variation of this protocol was introduced in [67]. In this protocol, Alice sends either $|\alpha\rangle$ or $|-\alpha\rangle$ and Bob perform an heterodyne measurement on his received state. The security of this protocol against collective attacks was established in [163]. However, this security proof only holds in the asymptotic limit where Alice and Bob know perfectly the conditional probability distribution $p(y|x)$. This assumption, which is certainly problematic in the context of a finite-size analysis, is not required for the protocols presented in this chapter.

and obtains two measurement results y_i^x and y_i^p for each state sent by Alice. For the four-state protocol, the raw key now consists in both signs of y_i^x and y_i^p.

One should also note a supplementary step has to be added for channel estimation: Alice and Bob publicly reveal $(N-n)$ couples of their data and compute the covariance matrix of the state ρ_{AB} that they would share in an entanglement-based version of the protocol. This allows them to compute an upper bound on Eve's information on y, the Holevo information $S(y;E)$. If the error correcting code used by Alice and Bob has a rate R, the secret key rate against collective attacks (in the limit where the fraction of data revealed for parameter estimation becomes negligible) reads:

$$K = R - S(y;E). \tag{5.31}$$

R is upper bounded by the mutual information $I(x;y)$ between Alice and Bob and we saw in the previous section that R could be written $R = \beta I(x;y)$ with $\beta \approx 80\%$. for low SNR. Finally, one finds the more common expression for the secret key rate:

$$K = \beta I(x;y) - S(y;E). \tag{5.32}$$

The mutual information $I(x;y)$ refers here to the capacity of the Gaussian channel (and not to the mutual information in the case of a binary modulation) and is given by[9]

$$I(x;y) = \frac{1}{2}\log_2(1+\mathrm{SNR}) \tag{5.33}$$

where the SNR is linked to the parameters of the channel by

$$\mathrm{SNR} = \frac{TV_A}{1+T\xi}, \tag{5.34}$$

where $V_A = 2\alpha^2$ is Alice's modulation variance, T is the transmission of the channel and ξ is the excess noise. The variances are here expressed in shot noise units.

Hence the first term $\beta I(x,y)$ of the secret key rate can easily estimated for a given implementation (since V_A is chosen in advance, ξ is a characteristic of the experimental implementation, and T is linked to the distance d between Alice and Bob and the quantum efficiency η of the detection through $T = \eta 10^{-0.02d}$). Note that one can thus anticipate how an actual implementation will behave on a given distance, but that in a real distribution, Alice and Bob just observe the value $R = \beta I(x;y)$ that they get. On the contrary, Alice and Bob cannot directly observe the second term $S(y;E)$ in a given experiment[10], they need to upper bound its value. To give such an upper bound as a function of the measured parameters of an experiment (V_A, T and ξ) is precisely the role of the security proof that we detail now.

[9] since we are here only interested in very low signal-to-noise ratio, we prefer to consider C_{Gauss} instead of the capacity of the BI-AWGN channel $C_{\text{BI-AWGN}}$. The ratio between these two capacities β_{mod} is directly included in β. This has the advantage that the expression for C_{Gauss} is simpler that the one for $C_{\text{BI-AWGN}}$.

[10] this is actually a recurring problem for QKD: one cannot directly observe that the distribution was successful but always needs to trust the theoretical model that is used in order to prove that the key that is distributed is indeed secret.

5.3.2 General outline of security proofs against collective attacks

The security of the various protocols we consider here is studied through the entanglement-based versions of the protocols. In the *Prepare and Measure* version of the protocols that are used in practice, Alice randomly draws N binary or quaternary variables, each corresponding to a specific coherent state of $\mathcal{S}_2$ for the two-state protocol or of $\mathcal{S}_4$ in the case of the four-state protocol. Alice then prepares these N coherent states and sends them to Bob through the quantum channel. In the *entanglement-based* version of the protocol, Alice starts with a pure bipartite state $|\Phi_2\rangle$ (or $|\Phi_4\rangle$ depending on the protocol) and performs a projective measurement on the first half of this state. The second half is sent to Bob through the quantum channel. For instance, in the protocol with a Gaussian modulation [64], the initial bipartite state is a two-mode squeezed vacuum, and the projective measurement performed by Alice is an heterodyne measurement, which projects the second half of the state on a coherent state [59]. The covariance matrix Γ^{TMS} of the two-mode squeezed vacuum reads

$$\Gamma^{\text{TMS}} = \begin{pmatrix} (1+2\alpha^2)\mathbb{1}_2 & Z_G\sigma_z \\ Z_G\sigma_z & (1+2\alpha^2)\mathbb{1}_2 \end{pmatrix}, \tag{5.35}$$

where $\sigma_z = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and $Z_G = 2\sqrt{\alpha^4+\alpha^2}$. Rewriting Γ^{TMS} with a direct reference to Alice's modulation variance V_A in the prepare and measure protocol, one has:

$$\Gamma^{\text{TMS}} = \begin{pmatrix} (V_A+1)\mathbb{1}_2 & Z_G\sigma_z \\ Z_G\sigma_z & (V_A+1)\mathbb{1}_2 \end{pmatrix}. \tag{5.36}$$

As the second half of the state is sent through a quantum channel characterized by its transmission T and excess noise ϵ, one can write the covariance matrix $\Gamma^{\text{Gauss}}$of the state ρ_{AB} Alice and Bob share in the CV QKD protocol with a Gaussian modulation:

$$\Gamma^{\text{Gauss}} = \begin{pmatrix} (V_A+1)\mathbb{1}_2 & \sqrt{T}Z_G\sigma_z \\ \sqrt{T}Z_G\sigma_z & (TV_A+1+T\xi)\mathbb{1}_2 \end{pmatrix}. \tag{5.37}$$

Then the Holevo information between Eve and Bob's measurement result can be upper bounded by a function of Γ^{Gauss} (see Chapter 3).

For the protocols of interest here, that is the two-state and the four-state protocols, our goal is to apply the same proof technique. We therefore want to find a purification $|\Phi_2\rangle$ (resp. $|\Phi_4\rangle$) with a covariance matrix Γ_2 (resp. Γ_4) as close as possible as the covariance matrix Γ^{TMS} of a two-mode squeezed state. This covariance matrix has the following form:

$$\Gamma_{2,4} = \begin{pmatrix} (V_A+1)\mathbb{1}_2 & Z_{2,4}\sigma_z \\ Z_{2,4}\sigma_z & (V_A+1)\mathbb{1}_2 \end{pmatrix}, \tag{5.38}$$

and the goal is to find a bipartite state $|\Phi_2\rangle$ (resp. $|\Phi_4\rangle$) such that Z_2 (resp. Z_4) is as close as possible of Z_G. Because a Gaussian state is the state of maximum entropy for a given covariance matrix, and because the entropy of the two-mode squeezed state is null, we know that necessarily: $Z_2, Z_4 < Z_G$. Of course, in order to be a legitimate

entanglement-based version of the protocol, the bipartite initial state must be such that there exists a projective measurement that Alice can perform that projects the second half of the state onto the desired 2 (or 4) coherent states of the set $\mathcal{S}_2$ (or $\mathcal{S}_4$).

The main idea of the discrete modulation protocols we study here is that there exists a regime for V_A such that

$$\left\{ \begin{array}{lllll} I_2(x;y) & \approx & I_4(x;y) & \approx & I_G(x;y), \\ S_2(y;E) & \approx & S_4(y;E) & \approx & S_G(y;E) \end{array} \right. \tag{5.39}$$

but with $\beta_2 \approx \beta_4 \gg \beta_G$ where β_2, β_4 and β_G refer respectively to the reconciliation efficiencies for the binary modulation, the quaternary modulation and the Gaussian modulation. Here, the superscripts $2, 4$ and G refer respectively to the two-state, four-state and Gaussian protocols. The existence of such a regime allows for the secret key rates K_2, K_4 to be positive for distances where the secret key rate for a Gaussian modulation K_G is null.

In the next two sections, we introduce such states $|\Phi_2\rangle$ and $|\Phi_4\rangle$ and compute the correlation terms Z_2 and Z_4 of their covariance matrices.

5.4 Security of the two-state protocol

In the *prepare and measure* version of the two-state protocol, Alice sends the coherent states $|\beta\rangle = |\alpha e^{-i\pi/4}\rangle$ and $|-\beta\rangle = -|\alpha e^{-i\pi/4}\rangle$ with probability 1/2 to Bob. Hence Bob sees a mixture ρ_2 given by:

$$\begin{aligned} \rho_2 &= \frac{1}{2}\left(|\beta\rangle\langle\beta| + |-\beta\rangle\langle-\beta|\right) \\ &= \frac{1}{2}e^{-\alpha^2}\left(\sum_{m,n=0}^{\infty}\frac{e^{-i(n-m)\pi/4}\alpha^{n+m}}{\sqrt{n!}\sqrt{m!}}|n\rangle\langle m| + \sum_{m,n=0}^{\infty}(-1)^{n+m}\frac{e^{-i(n-m)\pi/4}\alpha^{n+m}}{\sqrt{n!}\sqrt{m!}}|n\rangle\langle m|\right) \\ &= e^{-\alpha^2}\sum_{m,n=0}^{\infty}\frac{e^{-i(n-m)\pi/2}\alpha^{2(n+m)}}{\sqrt{(2n)!(2m)!}}|2n\rangle\langle 2m| + \frac{e^{-i(n-m)\pi/2}\alpha^{2(n+m+1)}}{\sqrt{(2n+1)!(2m+1)!}}|2n+1\rangle\langle 2m+1| \\ &= \lambda_0|\phi_0\rangle\langle\phi_0| + \lambda_1|\phi_1\rangle\langle\phi_1|, \end{aligned}$$

where $\lambda_0 = e^{-\alpha^2}\cosh\alpha^2$, $\lambda_1 = e^{-\alpha^2}\sinh\alpha^2$ and

$$|\phi_0\rangle = \frac{1}{\sqrt{\cosh\alpha^2}}\sum_{n=0}^{\infty}\frac{(-i)^n(\alpha)^{2n}}{\sqrt{(2n)!}}|2n\rangle, \tag{5.40}$$

$$|\phi_1\rangle = \frac{1}{\sqrt{\sinh\alpha^2}}\sum_{n=0}^{\infty}e^{-i\pi/4}\frac{(-i)^n\alpha^{2n+1}}{\sqrt{(2n+1)!}}|2n+1\rangle. \tag{5.41}$$

In order to use the proof technique described in the previous section, we need to consider the *entanglement based* version on the protocol. In this version, Alice starts with a bipartite pure state $|\Phi_2\rangle$. She performs a projective measurement on one half of the

state and sends the other half to Bob through the quantum channel. Depending on the binary result of her measurement, the state sent to Bob is either $|\alpha e^{-i\pi/4}\rangle$ or $|-\alpha e^{-i\pi/4}\rangle$ with equal probabilities. Let us consider the following purification for ρ_2:

$$|\Phi_2\rangle = \sqrt{\lambda_0}|\phi_0^*\rangle|\phi_0\rangle + \sqrt{\lambda_1}|\phi_1^*\rangle|\phi_1\rangle \tag{5.42}$$

where $|\phi_0^*\rangle$ and $|\phi_1^*\rangle$ are simply defined as:

$$|\phi_0^*\rangle = \frac{1}{\sqrt{\cosh\alpha^2}}\sum_{n=0}^{\infty}\frac{(i)^n(\alpha)^{2n}}{\sqrt{(2n)!}}|2n\rangle, \tag{5.43}$$

$$|\phi_1^*\rangle = \frac{1}{\sqrt{\sinh\alpha^2}}\sum_{n=0}^{\infty}e^{i\pi/4}\frac{(i)^n\alpha^{2n+1}}{\sqrt{(2n+1)!}}|2n+1\rangle. \tag{5.44}$$

$|\Phi_2\rangle$ can also be rewritten as:

$$|\Phi_2\rangle = \frac{1}{\sqrt{2}}|\psi_0\rangle|\beta\rangle + \frac{1}{\sqrt{2}}|\psi_1\rangle|-\beta\rangle \tag{5.45}$$

with

$$\begin{cases} |\psi_0\rangle = \frac{1}{\sqrt{2}}\left(|\phi_0\rangle^* + |\phi_1\rangle^*\right) \\ |\psi_1\rangle = \frac{1}{\sqrt{2}}\left(|\phi_0\rangle^* - |\phi_1\rangle^*\right) \end{cases} \tag{5.46}$$

At this point, it is worthing noting that in the entanglement based version of the protocol, Alice simply applies the projective measurement $\{|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|\}$ to the first half of the state $|\Phi_2\rangle$ and that she therefore projects the second half either on the coherent state $|\beta\rangle$ or the coherent state $|-\beta\rangle$ with equal probabilities. The state $|\Phi_2\rangle$ can also be seen as a superposition of coherent states:

$$|\Phi_2\rangle = \mu_0|e_0\rangle + \mu_1|e_1\rangle \tag{5.47}$$

with

$$\mu_{0,1} = \sqrt{1+e^{-4\alpha^2}}\nu_{0,1} \tag{5.48}$$

and

$$|e_0\rangle = \frac{1}{\sqrt{2(1+e^{-4\alpha^2})}}\left(|\beta^*\rangle|\beta\rangle + |-\beta^*\rangle|-\beta\rangle\right) \tag{5.49}$$

$$|e_1\rangle = \frac{1}{\sqrt{2(1+e^{-4\alpha^2})}}\left(|-\beta^*\rangle|\beta\rangle + |\beta^*\rangle|-\beta\rangle\right). \tag{5.50}$$

Note that the states $|e_0\rangle$ and $|e_1\rangle$ are not orthogonal:

$$\langle e_0|e_1\rangle = \frac{2e^{-2\alpha^2}}{1+e^{-4\alpha^2}}. \tag{5.51}$$

We now proceed by evaluating the covariance matrix Γ_2 of $|\Phi_2\rangle$. Symmetry arguments show that it has the following form:

$$\Gamma_2 = \begin{pmatrix} X\mathbb{1}_2 & Z\sigma_z \\ Z\sigma_z & Y\mathbb{1}_2 \end{pmatrix}, \tag{5.52}$$

with

$$\begin{cases} X &= \langle\Phi_2|2a^\dagger a+1|\Phi_2\rangle \\ Y &= \langle\Phi_2|2b^\dagger b+1|\Phi_2\rangle \\ Z_2 &= \langle\Phi_2|ab+a^\dagger b^\dagger|\Phi_2\rangle \end{cases} \tag{5.53}$$

where $a, a^\dagger$ and $b, b^\dagger$ are respectively the annihilation and creation operators on Alice and Bob's modes of the state. In order to compute X, one can consider the state

$$\rho_A = \frac{1}{2}\left(|\beta^*\rangle\langle\beta^*| + |-\beta^*\rangle\langle-\beta^*|\right) \tag{5.54}$$

obtained by tracing over the second subsystem of $|\Phi\rangle$:

$$\begin{aligned} X &= \langle\Phi_2|2a^\dagger a+1|\Phi_2\rangle && (5.55)\\ &= \mathrm{tr}(2a^\dagger a+1)\rho_A && (5.56)\\ &= 1+\mathrm{tr}(a^\dagger a|\beta\rangle\langle\beta|)+\mathrm{tr}(a^\dagger a|-\beta\rangle\langle-\beta|) && (5.57)\\ &= 1+2\alpha^2 && (5.58) \end{aligned}$$

since $a|\pm\beta\rangle = \pm\beta\,|\pm\beta\rangle$. The symmetry of the state $|\Phi_2\rangle$ shows that

$$Y = \langle\Phi_2|2b^\dagger b+1|\Phi_2\rangle = X. \tag{5.59}$$

Finally, applying the operator ab on the state $|\Phi_2\rangle$ gives:

$$ab|\Phi_2\rangle = \alpha^2\mu_0|e_0\rangle - \alpha^2\mu_1|e_1\rangle \tag{5.60}$$

and:

$$\langle\Phi_2|ab|\Phi_2\rangle = \alpha^2(\mu_0^2-\mu_1^2) \tag{5.61}$$

and finally

$$\begin{aligned} Z_2 &= \langle\Phi_2|ab+a^\dagger b^\dagger|\Phi_2\rangle && (5.62)\\ &= 2\mathcal{R}e\langle\Phi_2|ab|\Phi_2\rangle && (5.63)\\ &= 2\alpha^2(\mu_0^2-\mu_1^2) && (5.64)\\ &= \frac{1+e^{-4\alpha^2}}{2\sqrt{\lambda_0\lambda_1}} && (5.65)\\ &= 2\alpha^2\frac{1+e^{-4\alpha^2}}{\sqrt{1-e^{-4\alpha^2}}} && (5.66) \end{aligned}$$

The quantity Z_2 is displayed on Figures 5.5 and 5.6. It is clear from these plots that for $\alpha \leq 0.15$, Z_2 is almost indistinguishable from Z_G thus suggesting that in this regime, $S^2(y;E) \approx S^G(y;E)$.

5.5 Security of the four-state protocol

In this section, we study the security of four-state protocol. More specifically, we introduce a state $|\Phi_4\rangle$ that can be used in an entanglement-based version of the protocol and for which we compute the covariance matrix.

In the *prepare and measure* version of the protocol, Alice sends the coherent states $|\beta\rangle = |\alpha e^{i\pi/4}\rangle, |\beta^*\rangle = |\alpha e^{3i\pi/4}\rangle, |-\beta\rangle = |\alpha e^{5i\pi/4}\rangle$ and $|-\beta^*\rangle = |\alpha e^{7i\pi/4}\rangle$ with probability $1/4$ to Bob. Hence Bob sees a mixture ρ_4 given by:

$$\begin{aligned} \rho_4 &= \frac{1}{4}\left(|\beta\rangle\langle\beta| + |\beta^*\rangle\langle\beta^*| + |-\beta\rangle\langle-\beta| + |-\beta^*\rangle\langle-\beta^*|\right) && (5.67)\\ &= \lambda_0|\phi_0\rangle\langle\phi_0| + \lambda_1|\phi_1\rangle\langle\phi_1| + \lambda_2|\phi_2\rangle\langle\phi_2| + \lambda_3|\phi_3\rangle\langle\phi_3|, && (5.68)\end{aligned}$$

where

$$\left\{ \begin{array}{rcl} \lambda_{0,2} &=& \frac{1}{2}e^{-\alpha^2}\left(\cosh(\alpha^2) \pm \cos(\alpha^2)\right) \\ \lambda_{1,3} &=& \frac{1}{2}e^{-\alpha^2}\left(\sinh(\alpha^2) \pm \sin(\alpha^2)\right) \end{array} \right. \tag{5.69}$$

and

$$|\phi_k\rangle = \frac{e^{-\alpha^2/2}}{\sqrt{\lambda_k}} \sum_{n=0}^{\infty} (-1)^n \frac{\alpha^{4n+k}}{\sqrt{(4n+k)!}} |4n+k\rangle \tag{5.70}$$

for $k \in \{0,1,2,3\}$. Applying the annihilation operator a to $|\phi_k\rangle$ gives:

$$a|\phi_k\rangle = \alpha \frac{\sqrt{\lambda_{k-1}}}{\sqrt{\lambda_k}} |\phi_{k-1}\rangle \tag{5.71}$$

for $k \in \{1,2,3\}$ and

$$a|\phi_0\rangle = -\alpha \frac{\sqrt{\lambda_3}}{\sqrt{\lambda_0}} |\phi_3\rangle. \tag{5.72}$$

Let us now introduce the following purification $|\Phi_4\rangle$ of the state ρ_4:

$$\begin{aligned} |\Phi_4\rangle &= \sqrt{\lambda_0}|\phi_0\rangle|\phi_0\rangle + \sqrt{\lambda_1}|\phi_1\rangle|\phi_1\rangle && (5.73)\\ &\quad + \sqrt{\lambda_2}|\phi_2\rangle|\phi_2\rangle + \sqrt{\lambda_3}|\phi_3\rangle|\phi_3\rangle && (5.74)\end{aligned}$$

This state can also be written as:

$$|\Phi_4\rangle = \frac{1}{2}\left(|\psi_0\rangle|\beta\rangle + |\psi_1\rangle|-\beta^*\rangle + |\psi_2\rangle|-\beta\rangle + |\psi_3\rangle|\beta^*\rangle\right) \tag{5.75}$$

where the states

$$|\psi_k\rangle = \frac{1}{2}\sum_{m=0}^{3} e^{i(1+2k)m\pi/4}|\phi_m\rangle \tag{5.76}$$

are orthogonal non-Gaussian states. These states are displayed on Figure 5.4. This makes apparent the projective measurement that Alice needs to perform in the entanglement-based version of the four-state protocol to project the second half of $|\Phi_4\rangle$ on one of the four coherent states of $\mathcal{S}_4$, namely $\{|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|, |\psi_2\rangle\langle\psi_2|, |\psi_3\rangle\langle\psi_3|\}$. Let us compute

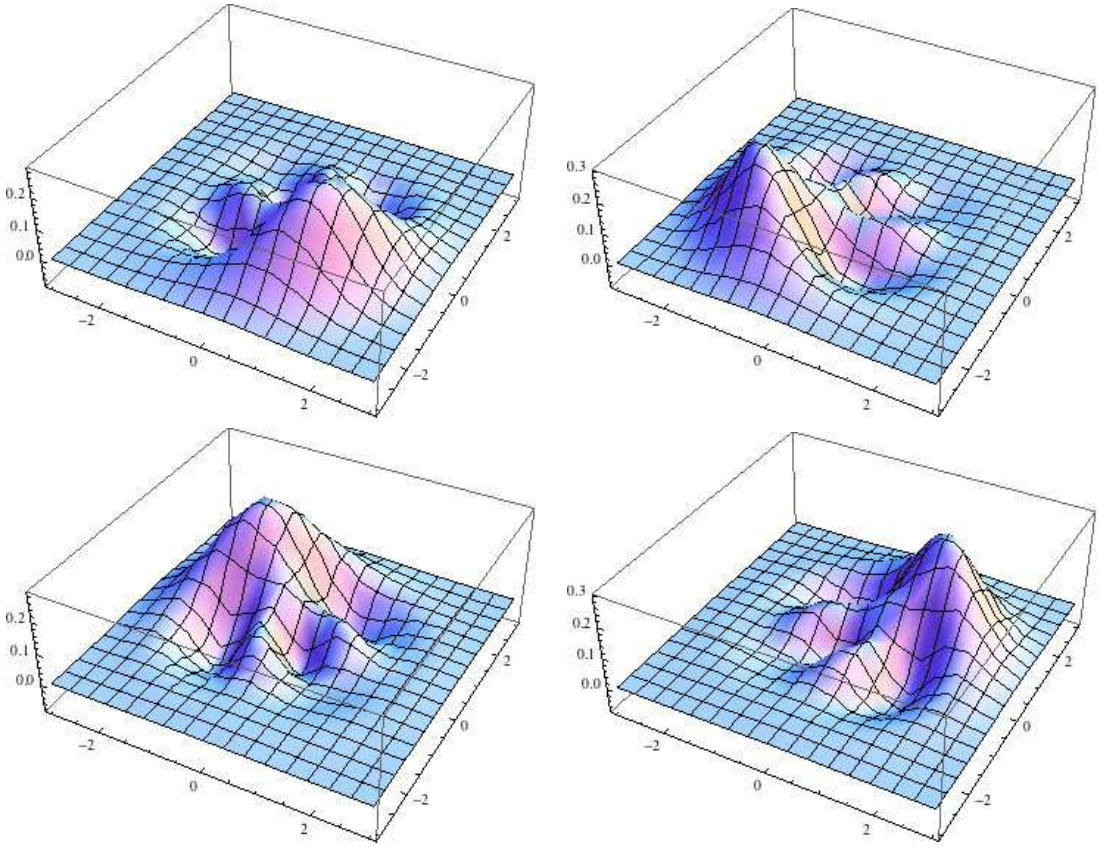

Figure 5.4: States $|\psi_0\rangle, |\psi_1\rangle, |\psi_2\rangle$ and $|\psi_3\rangle$ for $\alpha^2 = 0.5$ unit of shot noise.

the covariance matrix Γ_4 of the bipartite state $|\Phi_4\rangle$. Using symmetry arguments, it is clear again that Γ_4 has the following form:

$$\Gamma_4 = \begin{pmatrix} X\mathbb{1}_2 & Z_4\sigma_z \\ Z_4\sigma_z & X\mathbb{1}_2 \end{pmatrix}, \tag{5.77}$$

where

$$\begin{aligned} X = Y &= \langle\Phi_4|1 + 2a^\dagger a|\Phi_4\rangle = \Phi_4|1 + 2b^\dagger b|\Phi_4\rangle && (5.78)\\ &= \mathrm{tr}(1 + 2a^\dagger a\ \rho_4) && (5.79)\\ &= \mathrm{tr}(1 + \sum_{k=0}^{3} a^\dagger a\ \lambda_k|\phi_k\rangle\langle\phi_k|) && (5.80)\\ &= 1 + 2\sum_{k=0}^{3} \lambda_k\langle\phi_k|a^\dagger a|\phi_k\rangle && (5.81)\\ &= 1 + 2\alpha^2\sum_{k=0}^{3} \lambda_k\frac{\lambda_{k-1}}{\lambda_k} = 1 + 2\alpha^2\sum_{k=0}^{3}\lambda_{k-1} && (5.82) \end{aligned}$$

and finally

$$X = Y = 1 + 2\alpha^2. \tag{5.83}$$

We are now interested in the correlation term of the covariance matrix, that is

$$\begin{aligned} Z_4 &= \langle \Phi_4 | ab + a^\dagger b^\dagger | \Phi_4 \rangle & (5.84)\\ &= 2\mathcal{R}e\langle \Phi_4 | ab | \Phi_4 \rangle. & (5.85) \end{aligned}$$

One has:

$$\begin{aligned} ab|\Phi_4\rangle &= ab \sum_{k=0}^{3} \sqrt{\lambda_k} |\phi_k\rangle |\phi_k\rangle & (5.86)\\ &= \alpha^2 \sum_{k=0}^{3} \frac{\lambda_{k-1}}{\lambda_k} \sqrt{\lambda_k} |\phi_{k-1}\rangle |\phi_{k-1}\rangle & (5.87) \end{aligned}$$

where addition should be understood modulo 4. Finally, one obtains:

$$Z_4 = 2\alpha^2 \sum_{k=0}^{3} \frac{\lambda_{k-1}^{3/2}}{\lambda_k^{1/2}}. \tag{5.88}$$

The behavior of Z_4 is plotted on Figures 5.5 and 5.6. For $\alpha \leq 0.5$, Z_4 and Z_G are almost indistinguishable, meaning that in this regime, one has $S_4(y;E) \approx S_G(y;E)$. We confirm this intuition in the next section.

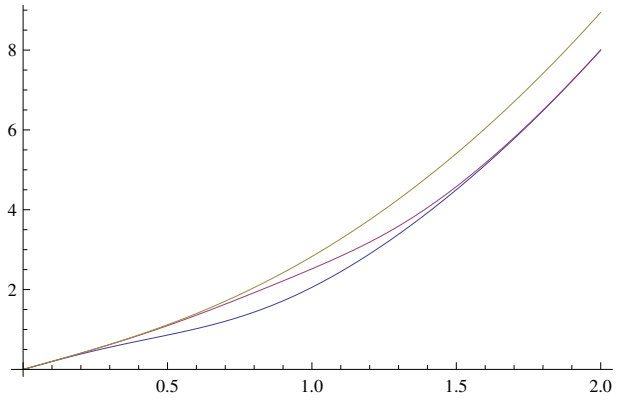

Figure 5.5: Comparison of the correlation Z_2 for the two-state protocol (lower curve), Z_4 for the four-state protocol (middle curve) and for the Gaussian modulation protocol Z_G (upper curve) as a function of α (for large values of α)

Already, Figures 5.5 and 5.6 suggest that the four-state protocol will be easier to implement than the two-state protocol since Z_4 is larger than Z_2. In particular, the covariance matrix of $|\Phi_4\rangle$ is almost indistinguishable from the one of the two-mode squeezed state for a much larger range of variances that the one of $|\Phi_2\rangle$.

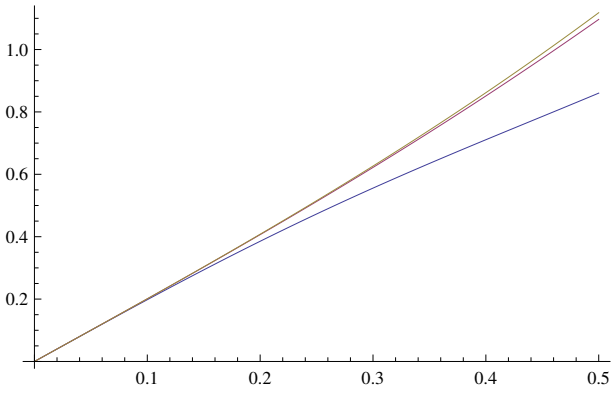

Figure 5.6: Comparison of the correlation Z_2 for the two-state protocol (lower curve), Z_4 for the four-state protocol (middle curve) and for the Gaussian modulation protocol Z_G (upper curve) as a function of α (for small values of α)

5.6 Performances of the protocols

For both protocols, the Holevo information between Eve and Bob's measurement result is upper bounded by the same quantity computed for a Gaussian state ρ_{AB}^G with the same covariance matrix as the state ρ_{AB} shared by Alice and Bob in an entanglement-based version of the protocol. Hence one can give a lower bound for both secret key rates K_2 and K_4:

$$\begin{cases} K_2 & \geq & \beta I_2(x;y) - S_2(y;E), \\ K_4 & \geq & \beta I_4(x;y) - S_4(y;E), \end{cases} \tag{5.89}$$

The expression for the upper bound on $S_2(y;E)$ (resp. $S_4(y;E)$) is computed from the symplectic eigenvalues ν_1, ν_2 of Γ_2 (resp. Γ_4) and from the eigenvalue ν_3 of the matrix $\Gamma_{2\,|y}$ (resp. $\Gamma_{4\,|y}$) corresponding to the covariance matrix of Alice's state given the result of Bob's homodyne measurement. The covariance matrix $\Gamma_{2,4}$ of the state shared by Alice and Bob is given by:

$$\Gamma_{2,4} = \begin{pmatrix} (V_A+1)\mathbb{1}_2 & \sqrt{T}Z_{2,4}\sigma_z \\ \sqrt{T}Z_{2,4}\sigma_z & (TV_A+1+T\xi)\mathbb{1}_2 \end{pmatrix}. \tag{5.90}$$

The reduced covariance matrix given Bob's measurement result depends on the type of measurement performed, either homodyne or heterodyne:

$$\Gamma_{2,4\,|y}^{\text{hom}} = \begin{pmatrix} V_A+1-\frac{(Z_{2,4})^2}{TV_A+1+T\epsilon} & 0 \\ 0 & V_A+1 \end{pmatrix}, \tag{5.91}$$

and

$$\Gamma_{2,4\,|y}^{\text{het}} = \begin{pmatrix} V_A+1-\frac{(Z_{2,4})^2}{TV_A+2+T\epsilon} & 0 \\ 0 & V_A+1-\frac{(Z_{2,4})^2}{TV_A+2+T\epsilon} \end{pmatrix}. \tag{5.92}$$

It is worth mentioning that the bounds for the Holevo information $S(y;E)$ that we derive from the covariance matrices of $|\Phi_2\rangle$ and $|\Phi_4\rangle$ are not proven to be tight. Indeed, even in the case where the quantum channel between Alice and Bob is perfect, that is $T = 1$ and $\xi = 0$, the bounds we compute do not give $S(b;E) = 0$ as we would expect, except in the limit of infinitely small modulation variances $\alpha \to 0$. This is because the states $|\Phi_2\rangle$ and $|\Phi_4\rangle$ are not Gaussian. However, the approximation becomes reasonably good for low modulation variances and one can expect the bounds not to be too loose. An intriguing question is whether the value of $S(y;E)$ computed for the Gaussian protocol is an upper bound for the same quantity computed for the discrete-modulation protocols. With the proof we presented, this is not the case (for instance, for a perfect quantum channel, $S_G(y;E) = 0$ as expected, whereas the bounds we found for $S_2(y;E)$ and $S_4(y;E)$ are positive). It is quite natural to expect the following relation to hold $S_2(y;E), S_4(y;E) < S_G(y;E)$ since a discrete modulation never maximizes the mutual information between Alice and Bob, and it is doubtful that it presents any advantage for a eavesdropper. However, our security proof cannot bring a definitive answer to this question.

The performances of the two-state protocol are displayed on Figure 5.7 corresponding to a perfect reconciliation efficiency and a perfect quantum efficiency for Bob's detector, and on Figure 5.8 corresponding to a realistic scheme where the reconciliation efficiency is only 80% and the quantum efficiency of Bob's detector is equal to 60%. One can

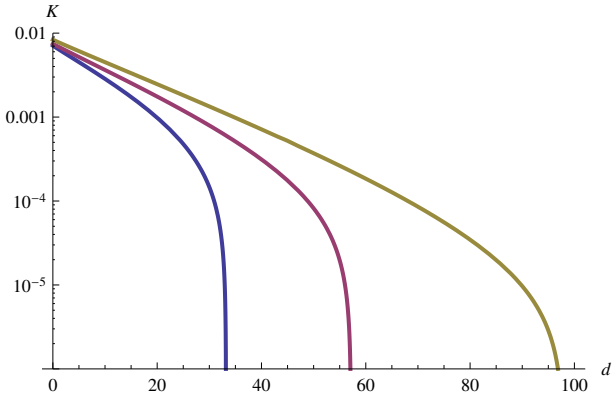

Figure 5.7: Secret key rate of the two-state protocol for a perfect reconciliation efficiency and a quantum efficiency of Bob's detection equal to 1. From top to bottom, excess noise is 0.001, 0.0015, 0.002. The respective optimized modulation variances (in number of photons) are 0.015, 0.018 and 0.23.

see from these figures that the two-state protocol can only work in a regime where the excess noise is very small: around 1/1000, which is compatible with the results obtained in [163] where the authors also study the security of a slightly different version of the two-state protocol (but where they need to assume the perfect knowledge of the probability distribution $p(y|x)$!).

The performance of the four-state protocol is presented on Figure 5.9 for an realistic reconciliation efficiency of 80% as well as a realistic quantum efficiency of 60% for Bob's

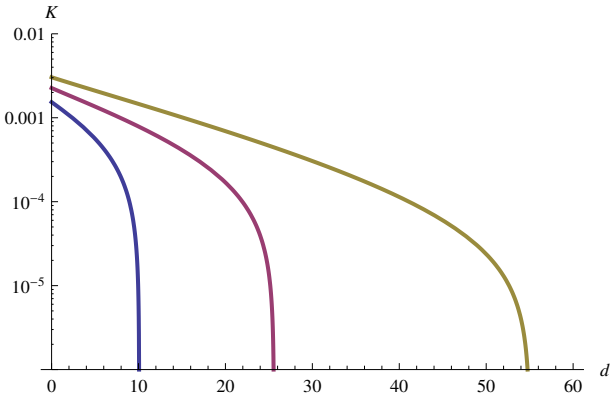

Figure 5.8: Secret key rate of the two-state protocol for a imperfect, realistic reconciliation efficiency of 80% and a quantum efficiency of Bob's detection equal to 0.6. From top to bottom, excess noise is 0.001, 0.0015, 0.002. The respective optimized modulation variances (in number of photons) are 0.015, 0.018 and 0.23.

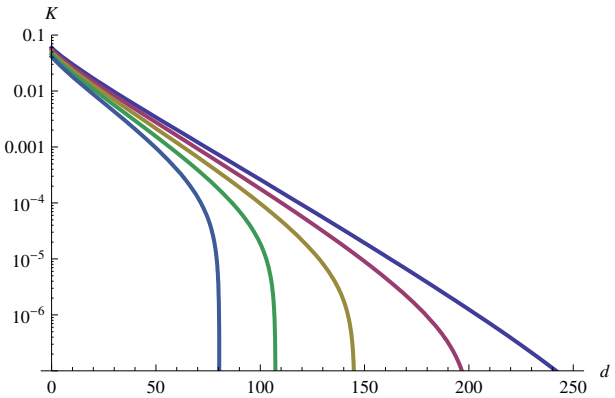

Figure 5.9: Secret key rate of the four-state protocol for a imperfect, realistic reconciliation efficiency of 80% and a quantum efficiency of Bob's detection equal to 0.6. From top to bottom, excess noise is 0.002, 0.004, 0.006, 0.008 and 0.01. The modulation variance (in number of photons) is 0.125, that is $V_A = 0.25$.

detector. One immediately notices that the four-state protocol performs much better than its two-state counterpart, that is, it allows for a distribution of secret keys over longer distances, and tolerates a much higher (and more reasonable) excess noise. This better resistance to excess noise is extremely important as we will see that the results presented so far are a little too optimistic in the sense that they assume a perfect knowledge of the transmission and excess noise (which is already infinitely less demanding that requiring a perfect knowledge of the quantum channel, which is described by an infinite number of parameters!). In practice, however, these parameters can never be perfectly known, and they can only be estimated with a precision depending on the number $N - n$ of data

used in the parameter estimation. The main consequence of this imperfect parameter estimation is to increase the effective excess noise, thus decreasing the actual performance of the protocols. We will come back on these aspects later in this manuscript, especially in Chapter 7.

5.7 Remaining issues

5.7.1 Potential issue with reverse reconciliation

In the case of discrete-variable QKD, the error correction messages exchanged by Alice and Bob during the reconciliation procedure always involve a finite number of bits. Then it is relatively easy to bound the amount of information that Eve can learn from Alice and Bob classical communication [124, 80]. Unfortunately, the situation is more involved for continuous-variable protocols as the reconciliation procedure might involve the exchange of continuous variables, that is, an a priori infinite amount of information. For instance, in the reconciliation scheme that we presented before, Bob needs to send the absolute value t of his measurement result to Bob. Intuitively, this is not a problem as t seems to be uncorrelated with the sign u of his measurement result. A rigorous proof of this intuition can be found in [163] and we reproduce it here.

Let us first recall the notations. Alice and Bob have access to correlated random variables x and y which corresponds respectively to the value of a quadrature of the coherent state sent by Alice and to Bob's result when measuring the corresponding quadrature on the state he received. Bob computes two values from y: its sign, $u = \mathrm{sgn}(y) = \pm 1$ which corresponds to the raw key element and its absolute value $t = |y|$ which is sent to Alice with the classical channel as side information. The result we want to prove is the following inequality:

$$S(u; E|t) \leq S(y; E). \tag{5.93}$$

This inequality means that Eve cannot learn any useful information about u from the knowledge of the side information t. The main idea of the proof is to use the concavity of the von Neumann entropy. First, the quantum state of Eve conditioned to Bob's outcome y can be written as

$$\rho_E^y = \sum_x \Pr(x|y)\rho_E^{x,y} \tag{5.94}$$

where $\Pr(y|x)$ is the probability of Alice's classical data being x given that Bob's measurement result is y and $\rho_E^{x,y}$ is Eve's quantum state conditioned on both Alice and Bob's classical variables. During the reconciliation procedure, Bob compute the variables t and u from y:

$$\rho_E^{t,u} = \sum_y \Pr(y|t,u)\rho_E^y. \tag{5.95}$$

Using these notations, one can lower bound the quantity $S(E|t,u)$ as follows:

$$\begin{aligned} S(E|t,u) &= \sum_u \int_t \mathrm{d}t \Pr(t,u) S\left(\rho_E^{t,u}\right) && (5.96)\\ &= \sum_u \int \mathrm{d}t \Pr(t,u) S\left(\int \mathrm{d}t \Pr(y|t,u)\rho_E^y\right) && (5.97)\\ &\geq \sum_u \int \mathrm{d}t \Pr(t,u) \int \mathrm{d}t \Pr(y|t,u) S\left(\rho_E^y\right) && (5.98)\\ &= \sum_u \Pr(y) S\left(\rho_E^y\right) && (5.99)\\ &= S(E|y), && (5.100) \end{aligned}$$

where the inequality is the direct application of the concavity of the entropy [109]. Now, one has

$$\begin{aligned} S(u;E|t) &= S(E|t) - S(E|u,t) && (5.101)\\ &\leq S(E) - S(E|y) && (5.102)\\ &\leq S(y;E), && (5.103) \end{aligned}$$

which is what we wanted.

5.7.2 Other potential issues for long distance CV QKD

So far, our results indicate that combining a discrete modulation together with a very efficient reconciliation procedure at low SNR allows to considerably increase the range of continuous-variable QKD. However, one might encounter other (technical) problems when trying to implement such a protocol. We list some potential problems below, together with possible approaches to solve them.

Statistical noise. Probably the main issue regarding long distance CV QKD is statistical noise. This is directly related to the problem of *finite-size effects* that we analyze in more details in Chapter 7. In fact, statistical noise relates to the specific problem of *parameter estimation*. As we stated before, the continuous-variable protocols we study are described by two main parameters that need to be known in order to compute the secret key rate: the transmission T and the excess noise ξ of the quantum channel between Alice and Bob. To be more precise, one also needs to know precisely the variance of Alice's modulation, but we can assume quite realistically, that this value is exactly known. Whereas the precise estimation of T is rather easy, the more crucial estimation of the excess noise appears quite involved, and the imperfect estimation has the immediate consequence of rather drastically reducing the range of the protocol even for quite long blocks ($N \approx 10^6 - 10^7$). Even if the problem of statistical noise is very relevant to continuous-variable protocol where one needs to precisely monitor the excess noise, it should be noted that the same issue also affects every discrete-variable QKD protocol.

Unfortunately, the solution to this problem is known. "Unfortunately" because the solution in question, whereas clear in theory, is rather complicated to implement. The solution is simply to increase the block length in such a way that the statistical noise becomes negligible. This seems straightforward, but is really problematic if this length must be in the order of a few billions (today, most implementations have block lengths of a few millions at most), and completely impossible if this length needs to be increased by a few more orders of magnitude. A more precise analysis in the case of CV QKD is detailed in Chapter 7.

Limited accuracy of the acquisition card. A second problem, that becomes highly relevant in the context of long distance where signals become very low, is the limited accuracy of the acquisition card used in Bob's homodyne detection. For long distances, one needs indeed to work at very low SNR meaning that the signal can easily be 10 or 100 times smaller than the noise. In these conditions, the signal is encoded in only a few bits of the (usually) 12 bits of the acquisition card. This implies that the data observed by Bob cannot be considered to be truly continuous, but rather discrete. The main consequence is that this digitization artifact behaves like some added noise. This is an issue for at least two reasons:

- the added noise might lead to a worse performance than anticipated for reconciliation efficiency since the reconciliation scheme is designated to fight Gaussian noise. This effect is difficult to precisely model theoretically, and one needs to test it in practice to see whether it is damaging or not. However, one might be confident that in certain regimes, this effect should not be too important thanks to the central limit theorem which states that adding many uncorrelated sources of random noise tends to a Gaussian noise. In particular, one can expect such a behavior from the use of the repetition codes at low SNR: one adds several weak and noisy signals to obtain a large and less noisy signal which is then corrected with standard LDPC codes.

- the second problem is that this new source of noise increases the excess noise, that is all the noise which is not the shot noise, nor the electronic noise. As a consequence, this noise will decrease the secret key rate of the protocol[11]. Fortunately, this noise is not caused by the eavesdropper and should be given a similar status than the electronic noise: it should decrease the mutual information between Alice and Bob, but not increase the Holevo information between Eve's quantum state and Bob's data. However, whereas modeling the source of electronic noise is rather easy (see [97]), modeling the noise due to the finite accuracy of the acquisition card is less obvious. This is because this modeling should be done by considering a purification of the quantum system shared by Alice and Bob: in these conditions, the Gaussian electronic noise is just modeled by an additional two-mode squeezed state, but the finite precision of the acquisition card probably cannot be modeled with a

[11] which is a decreasing function of the excess noise.

Gaussian state, which might make computations (as well as security proofs) much more tedious.

Sending the local oscillator far away. The third issue we would like to address when considering continuous-variable QKD over long distance is the problem of the local oscillator. Indeed, for the protocol to work, and more especially the homodyne detection to be possible, Bob needs a local oscillator perfectly synchronized with Alice's. Usually, for most CV QKD implementations (for instance [97] and [48]), the local oscillator is simply sent through the quantum channel (an optical fiber) along with the signal encoded the information. This is achieved by multiplexing the signal and the local oscillator, either in time, or in polarization, or both. Unfortunately, this system, which works very well over short distances, becomes problematic as the losses increase. The principal reason is that the local oscillator should be sufficiently intense on Bob's side in order to make the homodyne detection possible. However, amplifying the local oscillator (which is authorized in theory) is not possible if the local oscillator is sent in the same fiber than the quantum signal (which should not be amplified), and sending it in a distinct channel is not a very good solution as one will lose the synchronization between the oscillator and the quantum signal quite quickly. A possible solution would be to use clock recovery techniques, but it would imply a much more complicated setup than the ones used in current implementations.

5.8 Perspectives: convergence between DV and CV QKD at long distance

Whereas Alice usually sends coherent states with a few photons per pulse (between 3 and 10) in the Gaussian modulation protocol, here, the optimal number of photons per pulse typically ranges from 0.2 to 1. Therefore, the similitudes with discrete-variable QKD are important : the information is encoded onto low amplitude coherent states with generally less than 1 photon per pulse. The main difference is that an homodyne detection replaces photon counting. In the protocols we presented here, however, the error rate is not upper bounded (and can be as close as 0.5 as the reconciliation efficiency allows). This sounds in disagreement with security proofs for discrete-variable protocols that impose a maximum admissible quantum bit error rate (QBER). The reason for which this is nonetheless correct is that the error rate in our case in induced by both the noise added by Eve as well as the losses. This is in fact equivalent to a BB84 protocol where Bob would assign a random value to each pulse he did not detect. In this case, the QBER is arbitrarily high, but the security is still insured. In some sense, the main difference between the two schemes is that the vacuum noise is processed in two very different ways : whereas it creates "deletion errors" (which are ignored) in the photon counting scheme, it produces "real errors" (which have to be corrected) in the continuous-variable scheme.

Part III

Security of continuous-variable quantum cryptography

CHAPTER 6

Are collective attacks optimal?

Up until now, we have mainly focussed on the security of CV QKD against collective attacks. However, collective attacks correspond to a restriction on Eve's capabilities[1] and security against this class of attacks does not necessarily mean *unconditional security*.

Quite recently, Renner and Cirac generalized a method previously used for discrete-variable QKD to establish that collective attacks were asymptotically optimal also for CV QKD [127]. While being quite remarkable, this result presents a few drawbacks. First, it involves a *checking step* in order to verify that the Hilbert space relevant to describe the protocol is in fact finite-dimensional. Second, being an adaptation of the discrete-variable case, this technique does not fully take advantage of continuous-variable specificities (symmetries for instance), and consequently does not give the tightest bounds one could hope for in the non-asymptotic case, which is problematic for a finite-size analysis. Let us recall here that asymptotic results are useless in practice as one only has access to finite resources. First finite-size analyses are very pessimistic and suggest that asymptotic bounds become relevant only for very, very large block lengths, which are not achievable in practice. Therefore, one of the great challenges left for the theoretical study of QKD is to improve these non-asymptotic bounds. Whereas some components of

[1] and quite interestingly, a restriction on the limitations of theoretic physicists who find these attacks much easier to analyze than general attacks!

finite-size analysis, such as *parameter estimation* are already tight, it is not the case of the correction terms necessary to consider general attacks instead of collective attacks. These additional terms appear to be purely technical and without strong physical interpretation, and might disappear in future, with clever security proofs.

At this point, it is worth noting that symmetries of a QKD protocol can be exploited to derive security bounds, and it would seem that the more symmetric a protocol is, the simpler the optimal attack is. For instance, collective attacks are optimal against BB84, even for finite size [57, 86, 130]. Hence, in the case of BB84, there is no penalty to consider general attacks instead of collective attacks. In some sense, CV QKD protocols such as GG02 also appear to display important symmetries which could optimistically expected to be useful to derive tighter security proofs, and maybe to prove that collective attacks are always optimal, even in a non-asymptotic scenario.

The outline of this chapter is the following: we first review a general two-step strategy to prove the security of a QKD protocol, and we show how these two steps translate in the case of continuous-variable QKD. Then, we present preliminary results, in particular, a new de Finetti theorem in phase space representation. Unfortunately, these first results are not yet strong enough to prove the unconditional security of CV QKD. We conclude the chapter by exploring potential approaches for such a security proof.

6.1 Strategy for a proof

In this section, we start by defining the problem at hand: namely, how to reduce (when possible) the study of general (coherent) attacks to the study of the more easily handled collective attacks. We then explain a two-step strategy to solve this problem. Such a strategy will consist first in a symmetrization procedure, then on a proof that for our purpose (the security of QKD), symmetric states are reasonably close to i.i.d. states. Such closeness (in terms of the secret key rate distillable from a given state) can be established with at least two approaches: either an exponential version of the quantum de Finetti theorem[2] [125] or a postselection procedure [31][3].

6.1.1 Collective versus general attacks

Even if this claim has been made repeatedly since the proposal of the first QKD protocol in 1984 [10], it is only recently that complete security proofs have been rigorously established. Proving the security of a scheme without making any simplifying assumptions is indeed quite challenging: the legitimate parties, Alice and Bob, need to infer what is the most efficient attack that an eavesdropper, Eve, could perform. This can be achieved by considering all bipartite states ρ_{AB} compatible with Alice and Bob's data, but this quickly becomes almost intractable since the dimension of the Hilbert space $\mathcal{H}^{\otimes n}$ relevant

[2] in which case, one proves the closeness between the (partial trace of) symmetric states and the i.i.d. states in terms of trace-distance.

[3] Note that despite its name, such a postselection procedure is not linked to the procedure consisting in postselecting certain data in CV QKD, such as in [144].

to describe ρ_{AB} grows exponentially with the number n of quantum signals exchanged during the protocol. Here, we note $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ the tensor product of the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ which respectively describe Alice's and Bob's quantum systems. As a consequence, security proofs were often derived while restricting the adversary to the so-called *collective attacks*. For such attacks, the state ρ_{AB} is supposed to be *independent and identically distributed* (i.i.d.), meaning that there exists a state $\sigma_{AB} \in \mathcal{H}$ such that $\rho_{AB} = \sigma_{AB}^{\otimes n}$, or more exactly, ρ_{AB} should be a mixture of such i.i.d. states, that is, there exists a probability $p(\sigma)$ over all bipartite states $\sigma \in \mathcal{H}$ such that

$$\rho_{AB} = \int \mathrm{d}\sigma \, p(\sigma) \sigma^{\otimes n}. \tag{6.1}$$

As a consequence, the Hilbert space needed to analyze the protocol becomes $\mathcal{H}$ instead of $\mathcal{H}^{\otimes n}$: no need to emphasize that this "small" assumption considerably simplifies the analysis!

The question then is to know whether such a hypothesis limits the power of the adversary in a non trivial way, or, said otherwise, whether this leads to an unreasonably optimistic view of the security of QKD. Fortunately, this is not the case as collective attacks were recently proven asymptotically optimal against protocols described with a finite-dimensional Hilbert space [125]. In order to establish such a proof, two steps are usually necessary:

- first, one needs to show that the state ρ_{AB} can safely be assumed to be symmetric: this is done through the so-called *symmetrization* argument that we will detail below. The rough idea of this symmetrization is that if the QKD protocol displays some symmetries (for instance, the protocol is invariant under a reordering of the signals exchanged as in BB84, B92, GG02 and most QKD protocols), then Alice and Bob can always assume that the quantum state they share in the Entanglement-Based version of the protocol displays the same symmetries,

- then, it can be shown that, in general, such symmetric states are well-behaved with regard to QKD: this means that a symmetric state will allow one to distill roughly the same secret key rate than an i.i.d. state. Two methods can be used to prove this result. A brute-force approach consists in showing that up to some negligible operations (such as tracing out a negligible-sized subsystem[4]), a symmetric state is actually very close to a mixture of (almost) i.i.d. states for the trace distance: this is the content of the exponential version of de Finetti theorem [125]. The second approach works backwards: the idea is to show that if a protocol is ϵ-secure against collective attacks, then it is ϵ'-secure against coherent attacks where the ratio between ϵ' and ϵ is at most polynomial in the number of states exchanged by Alice and Bob. Since ϵ can be made exponentially small simply by shortening the length of the final key, this method can indeed be applied to show the unconditional security of a QKD protocol for which the security against collective attacks has been established. This second approach called *postselection* technique [31] turns out to

[4] in the asymptotic regime

be better than de Finetti theorem for proving security of QKD protocols as it gives much tighter bounds.

The challenge in the case of continuous-variable QKD is to adapt this general strategy to the case of infinite dimensional Hilbert spaces. Although this seems quite difficult with the usual symmetries considered for discrete-variable QKD, it might still be possible when using symmetries that are more specific to continuous-variable protocols.

6.1.2 Symmetrization

The goal of this section is to explain how symmetry considerations can simplify the theoretical analysis of quantum cryptography. In particular, we would like to provide a theoretical (but intuitive) justification to the common attitude of considering the state ρ_{AB} shared by Alice and Bob as being symmetric. Note that a more mathematical argument can be found in [31]. The symmetry which is usually considered is that the state $\rho_{AB} \in \mathcal{H}^{\otimes n}$ is invariant under any permutation of its n subsystems. Here we show that Alice and Bob can indeed always make this assumption, but that they are in fact not limited to the symmetric group $\mathcal{S}_n$, but can instead consider larger symmetry groups. Basically, the idea is that assuming any symmetry results in Alice and Bob underestimating the secret key rate they can extract from their data.

The secret key rate for a particular instance of a QKD protocol is a function of the state ρ_{AB} shared by the legitimate parties, Alice and Bob. The eavesdropper, Eve, is assumed to have the maximal information compatible with ρ_{AB} meaning that her state ρ_E is such that $\rho_E = \mathrm{tr}_{AB}(|\Psi_{ABE}\rangle)$ where $|\Psi_{ABE}\rangle$ is any purification of ρ_{AB}. Note that all purifications are equivalent up to a unitary operation applied on system E. More precisely, ρ_{AB} represents the *knowledge* that Alice and Bob have about the quantum state they share. For this reason, ρ_{AB} is subjective and inevitably depends on assumptions made by Alice and Bob[5]. A crucial observation is that Alice and Bob would like to ignore or forget the properties of ρ_{AB} they are not interested in, typically possible correlations between the N subsystems of their state, hence obtaining $\rho_{AB} = \sigma_{AB}^{\otimes n}$ for some prototype state $\sigma_{AB} \in \mathcal{H}$, which would exactly corresponds to the case of a collective attack. Unfortunately, this action of forgetting comes at a price, namely erasing some potentially useful information. The first idea to make the argument more rigorous is that Alice and Bob can actually *enforce* the symmetry they want. Let us for instance consider symmetry under permutations of the subsystems of ρ_{AB} which is the symmetry commonly used in various QKD security proofs (with the notable exception of protocols such as the Differential Phase Shift (DPS) [75] or the Coherent One-Way (COW) [150]). This symmetry can be enforced in the following way: Alice and Bob can perform the same random permutation π over their respective state, with π being chosen uniformly

[5]It must be emphasized that this cannot be avoided by performing a quantum tomography of the state since the latter is also subject to hypotheses, namely that one has access to an arbitrary large number of independent and identical copies of a single state.

over the symmetric group $\mathcal{S}_n$. This operation transforms ρ_{AB} into

$$\frac{1}{n!}\sum_{\pi\in\mathcal{S}_n} \mathrm{P}_\pi\,\rho_{AB}\,\mathrm{P}_\pi^\dagger \otimes |\pi\rangle\langle\pi|_C \tag{6.2}$$

where P_π is the unitary operator implementing the permutation π to both systems A and B, $\{|\pi\rangle\}_\pi$ is an orthogonal family of vectors and C is a classical auxiliary space whose sole purpose is to store the information concerning the permutation π that was applied. Then, tracing over system C (or equivalently giving this system to Eve), Alice and Bob obtain the state $\bar{\rho}_{AB}$

$$\bar{\rho}_{AB} \equiv \frac{1}{n!}\sum_{\pi\in\mathcal{S}_n} \mathrm{P}_\pi\,\rho_{AB}\,\mathrm{P}_\pi^\dagger, \tag{6.3}$$

which is symmetric by construction. Obviously, for any practical purpose, applying such a procedure is out of question as it would at least involve a quantum memory in order to store each subsystem while Alice and Bob wait for the total state ρ_{AB}. One may object, however, that applying such a permutation π to ρ_{AB} is equivalent to merely relabeling the indices of Alice and Bob's data, which is a much simpler task to perform. The key is that both procedures are indistinguishable, which is a clear consequence of the fact that the permutation of subsystems commutes with the measurement procedure and classical post-processing. This is true for most protocols, such as BB84 or continuous-variable protocols, but not for DPS or COW[6]. In order for the two procedures to be completely equivalent, Alice and Bob should completely forget which particular permutation was performed. A second crucial point is that, in reality, Alice and Bob do not even need to permute the labels of their data. What is really necessary is that they should never use any information related to the order of their data (the labeling of their data) in later parts of the QKD protocol (for instance during parameter estimation or reconciliation). If they do not use such potential information, then the protocol is exactly the same as if they would perform a random symmetry then forget which symmetry they applied.

It must be realized that enforcing such a symmetry can only decrease the secret key rate since Alice and Bob give additional information to Eve, or, equivalently, forget some *a priori* available information. This means that the quantity $S(b;E)$ can only be larger for the symmetrized state than for the initial state. On the other hand, while they are only throwing information that they do not use[7] in practice (the labeling of their data), this symmetrization step has no impact on $\beta I(a;b)$ which is the length of their raw key after the reconciliation procedure, but before the privacy amplification. Hence, the final secret key rate $\beta I(a;b) - S(b;E)$ can only be decreased during the symmetrization procedure. The point is to choose a symmetry which simplifies the analysis, but does not impact the secret key rate too much. Note than nothing forbids one to use such a technique in the study of the DPS and COW protocols. However, correlations between different subsystems are essential for these protocols to work and no key could be extracted if one was forgetting them. Essentially, if the usual symmetrization was applied

[6] for these protocols, the information is encoded onto successive signals, meaning that permuting the signals erases all the information, making the key distribution impossible.

[7] and do not know how to use

to these protocols, the resulting extracted mutual information $\beta I(a;b)$ would simply be null, which is certainly problematic as the secret key rate would be null as well, but then the protocols would still be theoretically secure, even if useless, as they do not produce insecure keys. In principle, any symmetrization is applicable to any QKD protocol, but some symmetrization procedures essentially erase all the relevant information and are consequently useless for the study of such protocols. Other symmetries have been investigated in the literature, for instance random bit-flip or phase-flip applied simultaneously by Alice and Bob, and have led to simplifications in the analysis of some protocols [86].

The above reasoning can easily be generalized to other symmetries. Let $\mathcal{G} = \mathcal{G}_A \otimes \mathcal{G}_B$ be a symmetry group in $\mathcal{H}^{\otimes n}$. More exactly, $\mathcal{G}$ is *local* in the sense that its elements g are of the form $g = g_A \otimes g_B$ where $g_A \in \mathcal{G}_A$ and $g_B \in \mathcal{G}_B$ are operations acting respectively on Alice and Bob's systems. If Alice and Bob perform a random $g = g_A \otimes g_B$ drawn from $\mathcal{G}$ and later forget about g, they effectively transform their ρ_{AB} into

$$\bar{\rho}_{AB}^{\mathcal{G}} \equiv \frac{1}{\#\mathcal{G}} \sum_{g_A \otimes g_B \in \mathcal{G}} (g_A \otimes g_B)\ \rho_{AB}\ \left(g_A^\dagger \otimes g_B^\dagger\right), \tag{6.4}$$

where $\#\mathcal{G}$ is the cardinal of $\mathcal{G}$. The group $\mathcal{G}$ can even be continuous (but still compact), in which case the discrete sum should simply be replaced by an integral over the Haar distribution of $\mathcal{G}$. This is actually what we will do for continuous-variable protocols.

6.1.3 Symmetric states versus i.i.d. states

Now that we have shown that the state ρ_{AB} shared by Alice and Bob in the Entanglement-Based version of the QKD protocol could be assumed to display some relevant symmetries, we need to establish that such a symmetrized state is almost as good as an i.i.d. state for the purpose of distilling a secret key. We will detail two approaches to this problem: the exponential version of de Finetti's theorem and the postselection procedure.

de Finetti's theorem. There has been a renewed interest in de Finetti's theorem [37] over the recent years, especially in the context of quantum information theory. In a classical setting, de Finetti's theorem addresses the statistics of large composite systems obeying some fundamental symmetry (e.g., invariance under permutations of its parts), stating that its parts can be well approximated by identical independent subsystems. In the language of probability theory, a permutation-invariant joint probability distribution of n random variables is shown to approach a probabilistic mixture of *independent and identically distributed* (i.i.d.) variables. In a quantum setting, the theorem makes the connexion between two types of n-mode states in $\mathcal{H}^{\otimes n}$: symmetric states, *i.e.*, states that are invariant under permutations of their subsystems (ρ such that $\rho = \pi\rho\pi^\dagger$ for any permutation $\pi \in \mathcal{S}_n$), and mixtures of i.i.d. states of the form $\sigma^{\otimes n}$ for some state $\sigma \in \mathcal{H}$. Whereas an i.i.d. state is obviously symmetric, the converse is not true in general. According to the quantum de Finetti theorem [74, 23], a symmetric state becomes increasingly close to a mixture of i.i.d. states as one traces out more of its parts. Attempts at characterizing the speed of convergence towards an i.i.d. state are more recent, both in

the classical case [39] and quantum case [81, 30]: the trace distance between the partial trace over $(n-k)$ parties of an n-partite symmetric state and a mixture of k-partite i.i.d. states is bounded from above by $2d^2k/n$, where d is the dimension of the Hilbert space.

Interestingly, a striking difference with the classical case is that the trace distance in the quantum case necessarily depends on the dimension of the Hilbert space. In particular, this rules out the possibility of a direct generalization of the theorem to an infinite-dimensional Hilbert space. This was proven in Ref. [30], where a counter-example was exhibited: the n-dimensional generalization of the singlet state $1/\sqrt{n!}\ \sum_\pi \mathrm{sign}(\pi)\ \pi(|0\rangle\otimes |1\rangle\otimes\cdots\otimes|n-1\rangle)$ is symmetric but any bipartite part, being a mixture of singlet states, cannot be approximated by a mixture of i.i.d. states. Even if a general quantum de Finetti theorem does not hold in infinite dimension, it is still possible to establish interesting versions of the theorem by restricting the set of states considered. For instance, such results can be obtained for coherent cat states [36] and Gaussian states [84].

Exponential de Finetti theorem. Unfortunately, the versions of de Finetti theorem mentioned above are useless for QKD. This is because the error in the approximation is proportional to k/n, which would make necessary to trace out most of the subsystems in order to get a "not so good" approximation. In particular, in the context of QKD, one requires the error to be exponentially small in the number n of subsystems. A way to obtain such an excellent approximation is to relax a little bit the i.i.d. property. This is the idea followed in Renner's exponential version of de Finetti theorem [125]. One introduces the notion of $\binom{n}{m}$-i.i.d. state: $\rho^{(n)}$ is called $\binom{n}{m}$-*i.i.d. (with prototype* σ*)* if there exists a permutation π and a state $\tilde{\rho}^{(n-m)}$ on $n-m$ subsystems such that

$$\rho^{(n)} = \mathrm{P}_\pi \left(\sigma^{\otimes m}\tilde{\rho}^{(n-m)}\right)\mathrm{P}_\pi^\dagger. \tag{6.5}$$

One recovers the usual i.i.d. property when $m = n$. The exponential de Finetti theorem then states that any n-partite part $\rho^{(n)}$ of an N-partite symmetric state $\rho^{(N)}$ is approximated by a probabilistic mixture of states $\rho_\sigma^{(n)}$ parametrized by σ, where each $\rho_\sigma^{(n)}$ is contained in the space spanned by $\binom{n}{n-r}$-i.i.d. states with prototype σ, for $r \ll n$. The remarkable property of this approximation is that its error is upper bounded by

$$\epsilon = 3e^{-r\frac{N-n}{N}+d\ln(N-n)}, \tag{6.6}$$

where d is the dimension of the subsystems, meaning that the error is exponentially small in r. By setting $r = N^\alpha$ and $n = N - N^\alpha$ for $1/2 < \alpha < 1$, one obtains that a symmetric state $\rho^{(N)}$ can be seen as a mixture of i.i.d. states (with an error exponentially small in N) if we ignore N^α subsystems and tolerate deviations in at most N^α of the subsystem, where N^α is sublinear in N.

This exponential version of de Finetti theorem can then be used in the context of QKD since it is known (see [124]) that the security of a QKD protocol in not affected by alterations of a small number of subsystems of $\rho^{(N)}$. Note, however, that is is only true in the asymptotic limit. In a finite-size analysis, correction terms depending on

$\epsilon = 3e^{-r\frac{N-n}{N}+d\ln(N-n)}$ must be taken into account[8].

In this present form, this theorem cannot be directly applied to CV QKD since the dimension d of the relevant Hilbert space is infinite, making the error ϵ in the approximation also infinite. This problem can be solved thanks to a generalization of the exponential version of de Finetti theorem to infinite dimensional quantum systems.

An exponential version for infinite-dimensional Hilbert spaces. As we mentioned earlier, a crucial difference between the classical and quantum versions of de Finetti theorem is that the latter makes an explicit reference to the dimension of the considered system while the former does not. In the case of continuous-variable QKD, the relevant Hilbert space is the Fock space which is infinite-dimensional. This would be an irremediable problem is there was not a subtlety, namely that the dimensions for continuous variables in fact correspond to energy levels. As a consequence, physical systems, which necessary have a finite energy, can be very well described with only a finite number of dimensions. This is because the populations in the very excited energy levels are always very small. Using this idea, Renner and Cirac were able to derive a generalization of the exponential de Finetti theorem for continuous variables, but restricted to the case where some property of the system can be checked, for instance that its energy is low enough [127]. Such a condition can be that the results of homodyne measurements performed on parts of the system should have a small absolute value. More precisely, the security proof of CV QKD protocols will work at the expense of an extra step in the protocol. This step is such that Alice and Bob will continue the protocol if the values z_i corresponding to results of homodyne measurements performed on random quadratures are such that $z_i^2 \leq \frac{n_0}{2}$ for some n_0, and abort otherwise. This verification step allows one to make sure, that with high probability, the relevant Hilbert space to describe the state ρ_{AB} is spanned by the eigenvectors of $\hat{X}_A + \hat{P}_A$ and $\hat{X}_B + \hat{P}_B$ with eigenvalues smaller than n_0. The quite involved technical part of the proof is detailed in [126].

Postselection procedure. The postselection technique recently introduced by Christandl, König and Renner in [31] gives a general method to upper bound the distance between to quantum channels, that is two completely positive trace-preserving (CPTP) maps, at the condition that the maps act symmetrically on an n-partite system with subsystems $\mathcal{H}$ of finite dimension. The distance between maps that we consider is the *diamond* distance which is derived from the diamond norm $||.||_\diamond$ introduced in Chapter 1: the norm of the CPTP map $\mathcal{T}$ is given by

$$||\mathcal{T}||_\diamond \equiv \sup_{k\in\mathbb{N}} ||\mathcal{T}\otimes \mathrm{id}_k||_1, \tag{6.7}$$

where

$$||\mathcal{S}||_1 \equiv \sup_{||\sigma||_1\leq 1} ||\mathcal{S}(\sigma)||_1 \tag{6.8}$$

[8] in such an analysis, an optimization procedure is applied to determine the best choice for the parameters r and n. This optimization also takes into account the parameter estimation phase. A more detailed presentation can be found in the next chapter of this manuscript.

and id_k denotes the identity map on states of a k-dimensional quantum system. The suprema in both definitions are reached for positive σ and k equal to the dimension of the input of $\mathcal{T}$ [79]. The postselection technique allows one to compute an upper bound on the distance $||\mathcal{E} - \mathcal{F}||_\diamond$ by only considering a *de Finetti* state, that is a state of the form[9]

$$\tau_{\mathcal{H}^{\otimes n}} \equiv \int \sigma_{\mathcal{H}}^{\otimes n} \mu(\sigma_{\mathcal{H}}), \tag{6.9}$$

where $\mu(.)$ is the measure on the space of states on $\mathcal{H}$.

In the context of QKD, the idea is to choose for $\mathcal{E}$ the map performed by the protocol: $\mathcal{E}$ takes $\rho_{AB} \in (\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n}$ as input and outputs the pair (S_A, S_B) corresponding to Alice and Bob's final keys as well as some classical communication C. The map $\mathcal{F}$ will be an ideal QKD protocol and takes ρ_{AB} as input but outputs the perfect keys (S, S) with the same length as S_A and S_B as well as the same classical communication C as $\mathcal{E}$. At the condition that $\mathcal{E}$ and $\mathcal{F}$ both act symmetrically on ρ_{AB}, one can bound the distance between the QKD protocol studied and the ideal protocol by the product of the same distance computed for a de Finetti state and a polynomial in n of degree $(\dim\mathcal{H})^2 - 1$. In particular, this means that if a QKD protocol is $\bar{\epsilon}$-secure against collective attacks, it is ϵ-secure against general attacks where

$$\epsilon \equiv (n+1)^{d^2-1}\, \bar{\epsilon}, \tag{6.10}$$

where $d = \dim(\mathcal{H}_A \otimes \mathcal{H}_B)$. It is crucial to note that such a polynomial ratio between the security parameters relative to collective attacks and general attacks is not a problem. Indeed, the parameter $\bar{\epsilon}$ can actually be chosen exponentially small, $\bar{\epsilon} \leq 2^{-c\delta^2 n}$ for some $c > 0$ at the cost of the of reducing the key size by an arbitrarily small fraction δ compared to the asymptotically optimal rate [31].

This postselection technique gives improved bounds for the secret key rate secure against coherent attacks compared to the results obtained from an application of the exponential version of de Finetti theorem. Unfortunately, the case of CV QKD cannot be treated directly through this approach as the final security parameter depends explicitly on the dimension of the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$.

6.2 Symmetries in phase space[10]

In this section, we introduce a new group of symmetry which is particularly important for continuous-variable QKD for at least two reasons:

- first, because the symmetry group introduced here is larger than the symmetric group $\mathcal{S}_n$, it is reasonable to think that its use will simplify the security analysis of continuous-variable QKD against general attacks. Indeed, this symmetry group allows for a new version of de Finetti theorem, which was shown to be impossible when considering the action of $\mathcal{S}_n$ in infinite dimensional Hilbert spaces [92].

[9] a de Finetti state corresponds to the state of n subsystems prepared as identical and independent copies of an unknown density operator $\sigma_{\mathcal{H}}$.

[10] The results of this section were published in New Journal of Physics [90].

- second, it allows us to justify the (usually assumed) form of the covariance matrix Γ_{AB} of the bipartite state ρ_{AB} shared by Alice and Bob in the Entanglement-Based version of the GG02 protocol when studying the security against coherent (or collective) attacks.

6.2.1 A symmetry group in phase space

The state ρ of an n-mode bosonic quantum system is completely characterized by its Wigner function in the $2n-$dimensional phase space parametrized by the quadratures $x_1, p_1, \ldots, x_n, p_n$, namely

$$W(x_1, p_1, \cdots, x_n, p_n) = \frac{1}{\pi^n} \int_{\mathbb{R}^n} \mathrm{d}y_1 \cdots \mathrm{d}y_n \, e^{i(p_1 y_1 + \cdots + p_n y_n)} \langle x_1 - y_1, \cdots, x_n - y_n | \rho | x_1 + y_1, \cdots, x_n + y_n \rangle \tag{6.11}$$

The Wigner function is well known to be a quasi-probability distribution, and not a genuine probability distribution as it can take negative values. However, by integrating it over one quadrature (x or p) for each mode, one obtains the n-variate probability distribution characterizing the outcomes of the n homodyne measurements (one performed on each mode).

One is of course not restricted to measuring quadratures x_k or p_k, but can also measure rotated quadratures with any angle θ_k in phase space. Thus, from a Wigner function, one can always construct a genuine probability distribution $p(r_1, \cdots, r_n)$, where r_k corresponds to a particular rotated quadrature of the k^{th} mode. In addition, one can also mix several modes with the help of a passive linear interferometer before performing the homodyne measurements, which means that the variables r_k become (normalized) linear combinations of the quadratures $x_1, p_1, \ldots, x_n, p_n$. In summary, starting with an arbitrary Wigner function, one can always construct a family of n-variate probability distributions $p(r_1, \cdots, r_n)$ using the following procedure: first, one process the n modes through a passive linear interferometer (a network of beamsplitters and phase shifters), and then one measures one fixed quadrature for each output mode. This exactly corresponds to passive Gaussian operations.

Let us now consider possible symmetries of the joint probability distribution characterizing the n random variables r_k. A first symmetry, which is standard in the context of de Finetti's theorem, is the invariance under permutations of the variables. This means that $p(r_1, \cdots, r_n) = p(r_{\pi(1)}, \cdots, r_{\pi(n)})$ for any permutation $\pi \in \mathcal{S}_n$, which denotes the group of permutations on $\{1, \ldots, n\}$. Another symmetry, which has not been explored so far in the quantum context, emerges naturally if one considers the real-valued random vector $\mathbf{r} = (r_1, \cdots, r_n) \in \mathbb{R}^n$. Note that the previous permutation symmetry simply means that the distribution probability is not affected by reordering the coordinates. As we work in $\mathbb{R}^n$, however, it seems more appropriate to substitute a discrete symmetry group such as $\mathcal{S}_n$ with a continuous symmetry group. A natural choice in this respect is

the orthogonal group $O(n)$, that is, the group of orthogonal transformations (or isometries) acting on vector $\mathbf{r}$. Note that applying an orthogonal transformation on $\mathbf{r}$ precisely corresponds to inserting an n-mode passive linear interferometer before performing the n homodyne measurements.

In classical probability theory, distributions that are invariant under orthogonal transformations are referred to as *orthogonally invariant* distributions. It has long been known that such probability distributions tend to mixtures of i.i.d. Gaussian distributions in the limit $n \to \infty$, or, more formally, that the first k coordinates of a random point that is uniformly distributed on the n-dimensional sphere are asymptotically normal. (An historical perspective of this property, going back to Poincaré, Borel, and Maxwell, can be found in Ref. [40], where the authors also derive a sharp bound for the theorem). In what follows, we consider the natural quantum counterpart of these distributions, namely n-mode states ρ for which the probability distribution $p(r_1, \cdots, r_n)$ that results from measuring n quadratures of ρ is unaffected by an n-mode passive interferometer preceding the measurement. This is equivalent to the condition that the state ρ is itself invariant under passive symplectic transformations, or, more physically, that ρ remains unchanged after being processed via any n-mode passive linear interferometer. In what follows, we will refer to these states as *orthogonally invariant* in phase space.

This orthogonal invariance in phase space clearly encompasses the permutation invariance in state space since permuting the coordinates in phase space is just a special case of an orthogonal transformation. Since we are considering a continuous instead of a discrete symmetry group, this invariance in phase space might appear quite restrictive, and we may question whether there exist interesting orthogonally invariant states. This is fortunately the case as, for example, any multimode thermal state is orthogonally invariant. This can be readily checked by considering its Wigner function which is given by a $2n$-partite Gaussian distribution with variance σ^2,

$$W_{\text{th}}(x_1, p_1, \cdots, x_n, p_n) = \frac{1}{(2\pi\sigma^2)^{n/2}} e^{-\left(x_1^2+p_1^2+\cdots+x_n^2+p_n^2\right)/2\sigma^2} \tag{6.12}$$

which is clearly invariant under orthogonal transformations of the coordinates. Note that such a multimode thermal state is nothing but a product of identical thermal states, which, in fact, plays the same role for the invariance under orthogonal transformations as i.i.d. states for the usual invariance under permutations. Another class of orthogonally invariant states is, for example, the multimode extension of Fock states that we will consider in the following.

6.2.2 Single-party case: main properties of orthogonal invariance in phase space

Let us now give two alternative characterizations of the set of orthogonally invariant states. The most natural one relies on phase space representation, since this is how the symmetry is expressed. In order to be invariant under orthogonal transformations in phase space, these states must simply have a Wigner function that only depends on one

single parameter, namely the modulus $||\mathbf{r}|| = (x_1^2 + p_1^2 + \cdots + x_n^2 + p_n^2)^{1/2}$. The characterization of this set of states in the Fock state representation is slightly more involved. We note that this set is convex as any mixture of orthogonally invariant states remains invariant under orthogonal transformations. It is, therefore, completely characterized by its extremal points, which can be shown to be the states

$$\sigma_p^n = \frac{1}{a_p^n} \sum_{\substack{p_1 \cdots p_n \\ \text{s.t. } \sum_i p_i = p}} |p_1 \cdots p_n\rangle\langle p_1 \cdots p_n| \tag{6.13}$$

with $a_p^n = \binom{n+p-1}{n-1}$. These extremal states are the multimode generalization of number states $|p\rangle$, that is, they correspond to the (normalized) projectors onto the various eigenspaces of the total number operator $\hat{n} = \hat{n}_1 + \ldots + \hat{n}_n$. For instance, σ_p^n, which is proportional to the projector onto the eigenspace of $\hat{n}$ with eigenvalue p, physically corresponds to a state with p photons distributed over n modes. The normalization factor a_p^n simply coincides with the number of ways of distributing p photons over n modes. These extremal states σ_p^n form a discrete infinite set of mixed states parametrized by p (or pure states for $n = 1$ as $\sigma_p^1 = |p\rangle\langle p|$). Importantly, any pure eigenstate chosen in the eigenspace corresponding to a given total photon number p is generally not orthogonally invariant; Schur's lemma insures that only the uniform mixture of them fulfills this invariance, which is why the extremal states σ_p^n are mixed for $n > 1$.

Finally, any state ρ that is invariant under orthogonal transformations in phase space can be written as

$$\rho = \sum_{k=0}^{\infty} c_k \sigma_k^n \tag{6.14}$$

where the weights c_k satisfy $0 \leq c_k \leq 1$ and $\sum_k c_k = 1$.

6.2.3 Bipartite case: application to continuous-variable QKD

One of the nice features of continuous-variable QKD is that the security against collective attacks is entirely characterized by the covariance matrix of ρ_{AB} (see Chapter 3 for details). Let us first restrict our analysis to collective attacks, so that one has $\rho_{AB} = \sigma_{AB}^{\otimes n}$, and the covariance matrix γ of σ_{AB} is usually assumed to be of the form:

$$\gamma_{\text{sym}} = \begin{pmatrix} X\mathbb{1}_2 & Z\sigma_z \\ Z\sigma_z & Y\mathbb{1}_2 \end{pmatrix}, \tag{6.15}$$

where $\sigma_z = \text{diag}(1, -1)$. Note that this form can easily be understood from an experimental point of view since the quantum channel is not supposed to induce correlations between different quadratures, for instance, but no theoretical justification has been given so far[11]. Here, we use a specific symmetry in phase space to prove that γ can indeed be supposed to take this simple form.

[11] in an implementation, the parameters X, Y and Z are linked to the experimental parameters V_A (Alice's modulation variance), T (the channel transmission) and ξ (the excess noise) through $X = V_A + 1, Y = 1 + TV_A + T\xi$ and $Z = \sqrt{T(V_A^2 + 2V_A)}$.

Since we make the assumption of a collective attack, the covariance matrix γ is well defined and can be estimated by Alice and Bob. The most general form for γ is:

$$\gamma = \begin{pmatrix} X_{11} & X_{12} & Z_{11} & Z_{12} \\ X_{12} & X_{22} & Z_{21} & Z_{22} \\ Z_{11} & Z_{21} & Y_{11} & Y_{12} \\ Z_{12} & Z_{22} & Y_{12} & Y_{22} \end{pmatrix}. \tag{6.16}$$

The idea is that Alice and Bob can perform some symmetrization operation, which transforms γ into the symmetrized covariance matrix γ_{sym}. First, note that their classical data are two strings $x, y \in \mathbb{R}^n$, which correspond to the results of homodyne measurements of the various quadratures of ρ_{AB}[12]. The reconciliation is always optimized for a Gaussian channel, meaning that the random variable y is modeled as $y = tx + z$ [91] where t is a (constant) transmission factor and z is a random variable modeling the added (isotropic) noise and characterized by its variance σ^2. Therefore, the reconciliation procedure would not be affected if Alice and Bob both performed the same random orthogonal transformation $R \in O(n)$ to their respective data, since one would then have $Ry = tRx + z'$, where z' is a rotated (isotropic) noise with the same variance σ^2 (that is, z and z' are two random variables with the same law). If Alice and Bob apply such a random orthogonal transformation and forget which one was performed, their data become "symmetric" in the sense that the matrix γ takes the form of γ_{sym} where $X = (X_{11} + X_{22})/2, Y = (Y_{11} + Y_{22})/2$ and $Z = (Z_{11} - Z_{22})/2$. The fact that the covariance matrix γ_{sym} features $Z\sigma_z$ instead of $Z\mathbb{1}_2$ simply reflects the fact that γ_{sym} is not the covariance matrix of the classical data of Alice and Bob in the Prepare & Measure scenario, but the covariance matrix of ρ_{AB} in the equivalent Entanglement-Based version. In the latter case, Alice and Bob would actually apply *conjugate* orthogonal transformations to their respective share of the state instead of the same transformation. Conjugate transformation here means the transformation whose corresponding $2n \times 2n$ matrix in phase space is obtained from the original one by flipping the sign of all rows whose label corresponds to a p quadrature and then flipping the sign of all columns whose label corresponds to a p quadrature. This can be understood by considering a two-mode squeezed vacuum, which is the state characterizing the inherent symmetry of continuous-variable QKD: this state has a covariance matrix Γ_{sym} where $Y = X$ and $Z = \sqrt{X^2 - 1}$, and is invariant under conjugate orthogonal transformations performed by Alice and Bob[13].

[12] more exactly, here x and y refers to Alice and Bob's classical data in the Prepare & Measure version of the protocol.

[13] To be more precise, there are orthogonal transformations that Alice and Bob can apply to their classical data which do not have a true physical equivalent in phase space. Such a transformation is the change of coordinates

$$\begin{cases} x & \leftarrow & x, \\ p & \leftarrow & -p. \end{cases} \tag{6.17}$$

Such an operation corresponds to a phase conjugation in phase space or to a time reversal. Even if such an operation appears difficult to genuinely implement, it can be easily simulated if Alice and Bob simply agree to perform the change of coordinates 6.17. This operation is crucial for our purpose as it allows us to set the values of X_{12}, Y_{12} and Z_{12} to zero.

In fact, using the notations of Section 6.1.2, Alice and Bob can safely replace their state ρ_{AB} by the state $\bar{\rho}_{AB}^{\mathcal{G}}$ given by

$$\bar{\rho}_{AB}^{\mathcal{G}} \equiv \int_{U\in\mathcal{G}} (U\otimes U^*)\ \rho_{AB}\ \left(U^\dagger\otimes U^T\right) \mathrm{d}U, \tag{6.18}$$

where $\mathcal{G}$ is the group of Gaussian unitary operators corresponding to a real symplectic orthogonal in phase space, and where $\mathrm{d}U$ refers to the Haar measure over $\mathcal{G}$. Note that this symmetrization procedure is very similar to a *twirling* operation[14]. For this reason, the state $\bar{\rho}_{AB}^{\mathcal{G}}$ can be seen as isotropic in phase space.

Hence starting with any state ρ_{AB}, this symmetrization outputs a state $\bar{\rho}_{AB}^{\mathcal{G}}$ with the property that its covariance matrix Γ_{sym} is given by

$$\Gamma_{\mathrm{sym}} = \begin{pmatrix} \gamma_{\mathrm{sym}} & 0 & \cdots & & 0 \\ 0 & \gamma_{\mathrm{sym}} & & & \\ \vdots & & \ddots & & \vdots \\ & & & \gamma_{\mathrm{sym}} & 0 \\ 0 & & \cdots & 0 & \gamma_{\mathrm{sym}} \end{pmatrix}, \tag{6.19}$$

with

$$\gamma_{\mathrm{sym}} = \begin{pmatrix} X\mathbb{1}_2 & Z\sigma_z \\ Z\sigma_z & Y\mathbb{1}_2 \end{pmatrix}. \tag{6.20}$$

The new symmetry group we introduce is therefore immediately useful as it allows to justify us an old (and until now unproven) assumption about the structure of the covariance matrix of ρ_{AB}. Moreover, we will argue in the following that this new symmetrization procedure (based on orthogonal transformations in phase space instead of permutations in state space) also gives a much simpler structure for the state ρ_{AB}. In particular, it makes possible the existence of a de Finetti theorem in phase space for instance.

6.3 de Finetti theorem and postselection procedure in phase space

The goal of this section is to give some insights on the structure of the states which are invariant under orthogonal transformations in phase space such as the state $\bar{\rho}_{AB}^{\mathcal{G}}$ described in the previous section. Ultimately, our goal would be to be able to derive an exponential version of de Finetti theorem for such states, or to be able to use them with the postselection technique introduced in [31]. Unfortunately, we still need to restrict ourselves to the case of single-party systems, instead of bipartite systems which would be directly relevant for their application in CV QKD, because the characterization of the

[14] for a twirling operation, the group $\mathcal{G}$ is the unitary group, and one would apply U on both systems A and B.

latter is more complicated and not yet well understood. This means that we will mainly consider states of the form $\rho = \mathrm{tr}_B\, \bar{\rho}_{AB}$, that is

$$\rho = \sum_{k=0}^{\infty} c_k \sigma_k^{(n)} \tag{6.21}$$

where the weights c_k satisfy $0 \leq c_k \leq 1$ and $\sum_k c_k = 1$.

6.3.1 de Finetti theorem in phase space representation[15]

As mentioned above, a classical de Finetti's theorem exists for classical orthogonally invariant probability distributions. The theorem states that, in the limit of infinite sequences $X_1, \cdots, X_n$ with $n \to \infty$, the first k variables are exactly mixtures of i.i.d. Gaussian distributions.

This result only holds approximately for finite sequences [40]: if the distribution of $X_1, \cdots, X_n$ is invariant under orthogonal transformations in $\mathbb{R}^n$, then the marginal distribution of the first k coordinates $X_1, \cdots, X_k$ is close to a mixture of i.i.d. Gaussian distributions. Here, the "closeness" is measured in the sense that the variation distance is bounded from above by $2(k+3)/(n-k-3)$ for $1 \leq k \leq n-3$.

In the following, we establish the quantum counterpart of the previous result.

Theorem 6.1. *If ρ^n is a n-mode orthogonally invariant quantum state, its partial trace over any $(n-k)$ modes $tr_{n-k}(\rho^n)$ can be approximated in the sense of the trace-norm distance by a mixture of k-mode thermal states $\rho_{th}^k(x)$, that is,*

$$\left|\left| tr_{n-k}(\rho^n) - \int \rho_{th}^k(x)\, \mu(dx) \right|\right|_1 \leq 2\left(\frac{n^2}{(n-k-1)(n-k-2)} - 1 \right), \tag{6.22}$$

where $\rho_{th}^k(x)$ is the tensor product of k thermal states with a mean number of x photons per mode, and μ is a probability measure.

The idea of the proof is inspired from that of the classical version of the theorem for geometric probability distributions, as described in [40]. If $X_1, \cdots, X_n$ are integer classical random variables whose joint distribution is invariant under transformations that keep the sum $X_1 + \cdots + X_n$ constant, then the marginal law of the first k coordinates $X_1, \cdots, X_k$ is close, in the sense of the variation distance, to a mixture of i.i.d. geometric distributions. The link with the quantum problem comes from the fact that in the Fock basis, any passive linear interferometer redistributes the photons among the modes in such a way that the total photon number is kept constant, since the energy is conserved. The invariance under orthogonal transformations in phase space therefore translates into the invariance under transformations that keep the total photon number constant in the Fock basis. As a consequence, the asymptotic state in our theorem is characterized by a geometric distribution in the Fock basis, which precisely is the signature of a thermal state. The proof will thus consist in bounding the convergence of an n-mode state that

[15] The results of this section were published in Physical Review A [92].

is invariant under a redistribution of photons among the n modes (with a constant total photon number) towards a mixture of thermal states.

Proof. First, any $n-$mode orthogonally invariant state ρ^n can be written as a convex mixture of the multimode number states σ_p^n, namely

$$\rho^n = \sum_{p=0}^{\infty} c_p \, \sigma_p^n \tag{6.23}$$

with arbitrary weights c_p satisfying $0 \leq c_p \leq 1$ and $\sum_p c_p = 1$. Now, using the convexity of the trace-norm distance

$$\left|\left| \mathrm{tr}_{n-k}(\rho^n) - \int \rho_{\mathrm{th}}^k(x) \, \mu(dx) \right|\right|_1 \leq \sum_{p=0}^{\infty} c_p \, \left|\left| \mathrm{tr}_{n-k}(\sigma_p^n) - \int \rho_{\mathrm{th}}^k(x) \, \mu(dx) \right|\right|_1 \tag{6.24}$$

we see that it is sufficient to prove the theorem for the extremal states σ_p^n, that is, it is enough to prove

$$\left|\left| \mathrm{tr}_{n-k}(\sigma_p^n) - \rho_{\mathrm{th}}^k(p/n) \right|\right|_1 \leq 2 \left(\frac{n^2}{(n-k-1)(n-k-2)} - 1 \right), \tag{6.25}$$

for any p. Note that we have arbitrarily reduced the mixture of thermal states to one single term, which is natural since we start with an extremal state σ_p^n. Note also that we have taken $x = p/n$ for this single term, that is, we characterize the convergence of the reduced state towards a k-mode thermal state with a mean number of p/n photons per mode.

The reduced state $\mathrm{tr}_{n-k}(\sigma_p^n)$ is obviously orthogonally invariant in the remaining space of k modes, which implies that it can be written as a mixture of k-mode number states,

$$\mathrm{tr}_{n-k}(\sigma_p^n) = \sum_{l=0}^{p} f(l) \, \sigma_l^k \tag{6.26}$$

where a simple combinatorial argument shows that:

$$f(l) = \frac{a_l^k \; a_{p-l}^{n-k}}{a_p^n}. \tag{6.27}$$

The k-mode thermal state $\rho_{\mathrm{th}}^k(x)$ is defined as the product of k single-mode thermal states with x photons per mode, namely $\rho_{\mathrm{th}}^k(x) = \rho_{\mathrm{th}}(x)^{\otimes k}$ with

$$\rho_{\mathrm{th}}(x) = \sum_{l=0}^{\infty} \frac{x^l}{(1+x)^{l+1}} \, |l\rangle\langle l| \tag{6.28}$$

A straightforward calculation shows that it can be written as a mixture of k-mode number states

$$\rho_{\mathrm{th}}^k(x) = \sum_{l=0}^{\infty} g(l) \, \sigma_l^k, \tag{6.29}$$

with

$$g(l) = a_l^k \frac{x^l}{(1+x)^{l+k}} \tag{6.30}$$

which confirms that it is also orthogonally invariant.

We now prove Eq. (6.25) using the fact that both $\mathrm{tr}_{n-k}(\sigma_p^n)$ and $\rho_{\mathrm{th}}^k(x)$ are diagonal in basis of k-mode number states. This implies that their trace-norm distance is given by the variation distance between the classical probability distributions f and g, that is

$$\begin{aligned}
\left|\left|\mathrm{tr}_{n-k}(\sigma_p^n) - \rho_{\mathrm{th}}^k(p/n)\right|\right|_1 &= \sum_{l=0}^{\infty} |f(l) - g(l)| && (6.31)\\
&= 2\sum_{l=0}^{\infty} \left(\frac{f(l)}{g(l)} - 1\right)^+ g(l) && (6.32)\\
&\leq 2\left(\sup_l \frac{f(l)}{g(l)} - 1\right) && (6.33)
\end{aligned}$$

where the function $(x)^+$ is equal to x if $x \geq 0$ and vanishes otherwise. Using the notation

$$h(l) \equiv \frac{f(l)}{g(l)} = \frac{a_{p-l}^{n-k}\ (1+p/n)^{l+k}}{a_p^n\ (p/n)^l}, \tag{6.34}$$

the rest of the proof consists in upper bounding the supremum of $h(l)$ as tightly as possible. Expanding the binomials in a_{p-l}^{n-k} and a_p^n, the function $h(l)$ can be rewritten as:

$$\begin{aligned}
h(l) &= \frac{(n-1)!}{n^k\ (n-k-1)!} \frac{(p-1)!}{p^{l-1}\ (p-l)!} \frac{(n+p)^{k+l}\ (n+p-k-l-1)!}{(n+p-1)!} && (6.35)\\
&= \frac{\prod_{t=1}^{k}(1-\frac{t}{n}) \prod_{t=1}^{l-1}(1-\frac{t}{p})}{\prod_{t=1}^{k+l}(1-\frac{t}{n+p})}. && (6.36)
\end{aligned}$$

The logarithm of $h(l)$ can be expressed as

$$\log h(l) = -S(n,k) - S(p,l-1) + S(n+p,k+l), \tag{6.37}$$

where $S(n,k)$ is defined as

$$S(n,k) \equiv -\sum_{t=0}^{k} \log\left(1 - \frac{t}{n}\right). \tag{6.38}$$

The function $x \mapsto -\log(1-x)$ being monotonically increasing on $[0,1[$, one has

$$n\,J\left(\frac{k}{n}\right) \leq S(n,k) \leq n\,J\left(\frac{k+1}{n}\right), \tag{6.39}$$

where

$$J(x) \equiv -\int_0^x \log(1-t)\,dt \tag{6.40}$$
$$= x + (1-x)\log(1-x). \tag{6.41}$$

Let us introduce the two reduced variables $u = k/n$ and $v = l/p$, which both belong to the interval $[0,1[$. Since the function $J(x)$ is convex on $[0,1[$, we have

$$J(\alpha\, u + (1-\alpha)\, v) \leq \alpha J(u) + (1-\alpha) J(v), \tag{6.42}$$

where $0 \leq \alpha \leq 1$. If we choose $\alpha = n/(n+p)$, this equation translates into

$$(n+p)\, J\left(\frac{k+l}{n+p}\right) \leq n\, J\left(\frac{k}{n}\right) + p\, J\left(\frac{l}{p}\right). \tag{6.43}$$

By using Eq. (6.39), we can lower (upper) bound the left- (right-) hand side term of Eq. (6.43), which yields

$$S(n+p, k+l-1) \leq S(n,k) + S(p,l). \tag{6.44}$$

Substituting k with $k+2$ and l with $l-1$, we get the equivalent inequality

$$S(n+p, k+l) \leq S(n, k+2) + S(p, l-1), \tag{6.45}$$

which can be used to upper bound the quantity of interest obtained in Eq. (6.37), namely

$$\log h(l) \leq S(n, k+2) - S(n,k). \tag{6.46}$$

We conclude that

$$h(l) \leq \frac{n^2}{(n-k-1)(n-k-2)}, \tag{6.47}$$

which, using Eq. (6.33), concludes the proof of the theorem.

□

Towards a security proof based on a de Finetti theorem in phase space. So far, we only discussed single-partite orthogonally-invariant states. Obviously, in order to use this approach to the study of QKD security, one needs a bipartite generalization. Let us consider the case of a $2n$-mode bipartite state ρ_{AB}, meaning that Alice and Bob each have n modes. Such a state ρ_{AB} is termed *invariant under conjugate orthogonal transformations* in phase space if, for any Gaussian unitary operation U corresponding to a real symplectic orthogonal transformation in Alice's $2n$-dimensional phase space, it satisfies

$$U \otimes U^*\; \rho_{AB}\; U^\dagger \otimes U^T = \rho_{AB} \tag{6.48}$$

where U^* is the Gaussian unitary operation corresponding to the conjugate orthogonal transformation in Bob's phase space. Physically, this invariance means that ρ_{AB} remains unchanged when Alice processes her n modes into any passive linear interferometer while

Bob processes his n modes into the passive linear interferometer effecting the conjugate rotation in phase space.

Ideally, one should have a quantum de Finetti theorem for bipartite orthogonally invariant states since this is the case which is directly relevant for proving the security of continuous-variable QKD. The reason is that, following the arguments in Section 6.2, Alice and Bob can indeed assume their bipartite state ρ_{AB} to be invariant under conjugate orthogonal transformations. Thus, a bipartite quantum de Finetti theorem would rigorously prove that ρ_{AB} is "close to" a product of Gaussian states. Note, however, that an *exponential* version of the theorem would actually be required to address the security of continuous-variable QKD, meaning that it is enough to trace over only an exponentially small number of modes in order to get a good approximation by a Gaussian state. Then, such a Gaussian state would be the product of n i.i.d. Gaussian states, and the security against collective attacks would therefore imply the security against arbitrary attacks.

Finding a bipartite version of this quantum de Finetti theorem is the subject of further work. Although we do not have a rigorous proof yet, the fact that a bipartite version of the theorem holds is very likely. In particular, both partial traces $\rho_A = \mathrm{tr}_B \rho_{AB}$ and $\rho_B = \mathrm{tr}_A \rho_{AB}$ are single-partite orthogonally-invariant states, for which the theorem applies. Hence, locally, we already know that a state ρ_{AB} that is invariant under conjugate orthogonal transformations in phase space becomes asymptotically Gaussian. One only needs to prove that the correlations between Alice and Bob also behave according to the bipartite version of the theorem.

6.3.2 Postselection technique in phase space

We now are interested in generalizing the postselection technique introduced in [31] to continuous variables. In [31], the authors show that they can start with an i.i.d. state of the form

$$\tau_{\mathcal{H}^{\otimes n}} \equiv \int \sigma_{\mathcal{H}}^{\otimes n} \, \mu(\sigma_{\mathcal{H}}), \tag{6.49}$$

where $\mu(.)$ is the measure on the space of states on $\mathcal{H}$, and generate an arbitrary symmetric state on $\mathcal{H}^{\otimes n}$ with a success probability decreasing only polynomialy in n. Roughly speaking, in the context of QKD, this means that if one can prove the security of a protocol against collective attacks, then the protocol has to be secure against general attacks with a security parameter only polynomialy larger.

Here we would like to prove a generalization of this postselection technique in phase space. As in the previous section, we restrict ourselves to the single-party case here. The natural generalization of the purification of i.i.d. state $\tau_{\mathcal{H}^{\otimes n}}$ will be the n-mode continuous-variable EPR pair:

$$|\Phi_{\mathrm{EPR}}^{n}(x)\rangle \equiv |\Phi_{\mathrm{EPR}}(x)\rangle^{\otimes n} \tag{6.50}$$

$$= \sum_{k=0}^{\infty} \sqrt{\lambda_k} \, |\psi_k^n\rangle \tag{6.51}$$

where $\lambda_k \equiv \binom{n+k-1}{n-1} \frac{x^k}{(1+x)^{k+n}}$ and

$$|\psi_k^n\rangle \equiv \frac{1}{\sqrt{a_k^n}} \sum_{\substack{k_1 \cdots k_n \\ \text{s.t. } \sum_i k_i = k}} |k_1, \cdots, k_n\rangle |k_1, \cdots, k_n\rangle. \tag{6.52}$$

A generalization of the postselection technique to continuous variables aims at computing the probability of success p_{succ} of producing any orthogonally-invariant state $\rho = \sum_{k=0}^{\infty} c_k \, \sigma_k^n$ by performing a measurement on one half of the state $|\Phi_{\text{EPR}}^n(x)\rangle$ for a well chosen value of x. Our goal here is to find the smallest value of p_{succ}. A convexity argument shows that this value is necessarily obtained when the orthogonally invariant state considered is an extremal state σ_k^n. We will consider the following procedure to create an arbitrary orthogonally invariant state: one just applies the POVM $\{\mathbb{1}_A \otimes M_B, \mathbb{1}_A \otimes (\mathbb{1}_B - M_B)\}$ to the state $|\Phi_{\text{EPR}}^n(x)\rangle$ where $M = \sum_{k=0}^{\infty} \mu_k^n \sigma_k^n$ and the parameters μ_k are such that $0 \leq \mu_k \leq 1$. This measurement produces the state

$$\rho_{\text{succ}} \equiv \frac{\text{tr}_B(\mathbb{1}_A \otimes M_B)|\Phi_{\text{EPR}}^n(x)\rangle\langle\Phi_{\text{EPR}}^n(x)|}{\text{tr}(\mathbb{1}_A \otimes M_B)|\Phi_{\text{EPR}}^n(x)\rangle\langle\Phi_{\text{EPR}}^n(x)|}, \tag{6.53}$$

with a success probability

$$p_{\text{succ}}(n) = \text{tr}(\mathbb{1}_A \otimes M_B)|\Phi_{\text{EPR}}^n(x)\rangle\langle\Phi_{\text{EPR}}^n(x)|. \tag{6.54}$$

One gets:

$$\rho_{\text{succ}}(n) = \frac{\sum_{k=0}^{\infty} \lambda_k \mu_k \sigma_k^n}{\sum_{k=0}^{\infty} \lambda_k \mu_k}, \tag{6.55}$$

and

$$p_{\text{succ}} = \sum_{k=0}^{\infty} \lambda_k \mu_k. \tag{6.56}$$

If one wants to produce the state σ_k^n, then one should choose the POVM element $M = \sigma_k^n$ together with the initial EPR state with a mean photon number x equal to k/n. This gives the probability of success

$$p_{\text{succ}}(n) = \lambda_k = \binom{n+k-1}{n-1} \frac{(k/n)^k}{(1+k/n)^{k+n}}. \tag{6.57}$$

The binomial coefficient can be approximated thanks to Stirling's formula:

$$\binom{n+k-1}{n-1} \sim \sqrt{\frac{1+1/x}{nx}} \, 2^{n\,G(x)}, \tag{6.58}$$

where $G(z) = (z+1)\log_2(z+1) - z\log_2(z)$ is the von Neumann entropy of a thermal state with z photons. Hence, one finally obtains

$$p_{\text{succ}}(n) \approx \sqrt{\frac{1+1/x}{nx}}, \tag{6.59}$$

which is a behaviour compatible with the use of the postselection theorem to prove the security of continuous-variable QKD against arbitrary attacks. Obviously, once again, a complete proof would concern bipartite orthogonally invariant states and not only single-party state as here. However, the fact that the probability of success decreases only as the inverse of the square-root of the number of modes considered and not exponentially with this number, is a good indication that the post-selection technique might apply for symmetries in phase space.

6.4 Possible approaches to prove the unconditional security of CVQKD

In this chapter, we discussed strategies to prove the unconditional security of continuous-variable QKD protocols. As we already mentioned, such a proof already exists [127] but the bounds it gives are only interesting in the asymptotic regime where collective attacks are optimal. We think that using the symmetries in phase space specific to continuous-variable QKD protocols such as GG02 would allow for the derivation of tighter bounds. Indeed, GG02 is in a sense the continuous-variable equivalent of BB84, meaning that it is very (maximally?) symmetric in the relevant Hilbert space, and it is known that for BB84, the secret key rate secure against general attacks is exactly the same as the one secure against collective attacks (the proof for this result explicitly uses the symmetries of BB84). Therefore it is reasonable for keep looking for security proofs for GG02 relying explicitly on the symmetries of the protocol in phase space.

Such a security proof has not been established yet. In this section, we review the challenges that need to be met in order to derive such a proof, and discuss other possible approaches to prove the unconditional security of QKD.

6.4.1 Characterization of isotropic states in phase space

The key element that is still missing is a complete characterization of the bipartite states of interest for continuous-variable QKD. These are the states obtained from any initial state ρ_{AB} through a twirling-like operation mapping ρ_{AB} to $\bar{\rho}_{AB}$ defined as

$$\bar{\rho}_{AB} \equiv \int_{U\in\mathcal{G}} (U \otimes U^*)\ \rho_{AB}\ \left(U^\dagger \otimes U^T\right) \mathrm{d}U, \tag{6.60}$$

where $\mathcal{G}$ is the group of Gaussian unitary operators corresponding to a real symplectic orthogonal transformation in phase space, and where $\mathrm{d}U$ refers to the Haar measure over $\mathcal{G}$.

Note that $\bar{\rho}_{AB}$ is very close to what one could call an isotropic continuous-variable state. Indeed, in a d-dimensional Hilbert space, one defines the projector P_{iso} which projects ρ onto the *isotropic state* as

$$P_{\mathrm{iso}}\,\rho \equiv \int_{U\in U(d)} U \otimes U^*\,\rho\,(U \otimes U^*)^\dagger \mathrm{d}U, \tag{6.61}$$

where $U(d)$ is the group of d-dimensional unitary matrices. Isotropic states correspond to maximally entangled states mixed with white noise.

In the case of continuous-variable systems, this definition does not directly hold for various reasons. First of all, such an operator would be ill-defined simply because the group $U(\infty)$ of unitary operators is not compact, with the consequence that one cannot define a Haar measure for this group. This is a mathematical reason, but there is a least one physical reason for why the definition fails in the case of infinite-dimensional Hilbert spaces: the energy of the resulting state would indeed be infinite, which is a serious problem.

What is worth noting, is that in the case of continuous-variable quantum systems, not all dimensions play a similar role, in contrast with what happens for d-dimensional Hilbert spaces. In finite dimension, a basis of the Hilbert space is typically noted $\{|0\rangle, \cdots, |d-1\rangle\}$, but the labels of the basis elements are not really meaningful and could be exchanged without any consequence. This is not true anymore in continuous-variable systems. In that case, the infinite basis $\{|0\rangle, |1\rangle, |2\rangle, \cdots\}$ refers to the Fock basis, and the index of the various vectors is not merely an index: it characterizes the state as being the vacuum for the state labeled $|0\rangle$ and corresponds to k bosonic excitations for the state $|k\rangle$. Importantly, the index is directly linked to the energy of the state. From this perspective, when discussing potential continuous-variable isotropic states, it is reasonable to ask that the group of operators used in the twirling-like operation should conserve the energy of the initial state. This is what justifies the choice of the group $\mathcal{G}$ of Gaussian unitary operators corresponding to a real symplectic orthogonal transformation in phase space.

The characterization of the set of states $\bar{\rho}_{AB}$ is clearly a required preliminary to a potential security proof based on symmetries in phase space. Unfortunately, this set appears to be more complicated that one set of single-party orthogonally invariant states which is a polytope with simple extremal vertices (the n-mode generalizations of number states).

6.4.2 Further than symmetrization and postselection

Let us recall once more the general strategy to prove the security of a particular QKD protocol against coherent attacks. The first idea is to characterize the natural symmetries of the protocol. These symmetries are described by a symmetry group $\mathcal{S}$ acting on density matrices. Then Alice and Bob can always replace their initial state ρ_{AB} (in the entanglement-based version of the protocol) to be replaced by $\bar{\rho}_{AB}^{\mathcal{S}}$ defined as:

$$\bar{\rho}_{AB}^{\mathcal{S}} \equiv \int_{U \in \mathcal{S}} (U \otimes U^*) \ \rho_{AB} \ \left(U^\dagger \otimes U^T\right) \mathrm{d}U. \tag{6.62}$$

Then the second step is to prove that this state is close enough to a mixture of i.i.d. states, either through an exponential version of de Finetti theorem, or through a postselection procedure.

A question that arises is whether one can go a little bit further with the first step. Indeed, the second step becomes more and more easier as the relevant state becomes more and more "symmetric". A maximally symmetric state, in this sense, would be a

mixture of i.i.d. states and one can see that if Alice and Bob could assume their state to be i.i.d., then this would immediately prove that collective attacks are optimal among general attacks. Unfortunately, this is not possible in general as a symmetrization that would make the state i.i.d. would typically consist in erasing all the correlations relevant for the QKD protocol.

Usually the relevant symmetry group used in the symmetrization procedure is such that is leaves invariant the parameters of the protocol:

- for discrete-variable protocols such as BB84, the symmetry group preserves the quantum bit error rate (QBER), hence leaving the mutual information between Alice and Bob, as well as Eve's information unchanged. A typical symmetry group leaving the QBER unchanged is the symmetric group consisting of permutations of the labels of Alice and Bob's data.

- for continuous-variable QKD, the parameters that should be invariant are the transmission T and the excess noise ξ of the quantum channel between Alice and Bob. It turns out that Gaussian unitary operations corresponding to real orthogonal symplectic transformations in phase space exactly leave T and ξ invariant.

A possibility would be to consider a symmetry group that leaves the parameters in question invariant *asymptotically* (and only almost invariant in a finite-size setting). For instance, in the case of continuous variables, one would like the state shared by Alice and Bob to be as close as possible from a Gaussian state. An idea would therefore be for Alice and Bob to apply operations on a small subset of their subsystems (for instance) such that the overall state becomes more Gaussian but in such a way that T and ξ would not be too affected.

The idea for example would be to define a group $\mathcal{S}^\epsilon$ (containing $\mathcal{S}$) such that the state

$$\bar{\rho}_{AB}^{\mathcal{S}^\epsilon} \equiv \int_{U\in\mathcal{S}^\epsilon} (U\otimes U^*)\ \rho_{AB}\ \left(U^\dagger\otimes U^T\right) \mathrm{d}U, \tag{6.63}$$

would not be too degraded compared to $\bar{\rho}_{AB}^{\mathcal{S}}$ concerning its potential usage in the QKD protocol. For a CV QKD protocol, this means that the transmission T^ϵ and the excess noise ξ^ϵ of the new state should not be too different from the initial values of T and ξ. A possible way to characterize this difference is to consider the secret key rate secure against collective attacks $K_{\mathrm{coll}}(T,\xi)$ compatible with the parameters T and ξ and impose that T^ϵ and ξ^ϵ should be such that

$$|K_{\mathrm{coll}}(T,\xi) - K_{\mathrm{coll}}(T^\epsilon,\xi^\epsilon)| \leq \epsilon. \tag{6.64}$$

The idea is that the state $\bar{\rho}_{AB}^{\mathcal{S}^\epsilon}$ will be much easier to use for the postselection technique for instance, and would lead to an improved overall security parameter than the one obtained while using $\bar{\rho}_{AB}^{\mathcal{S}}$.

An example of such a larger symmetry group $\mathcal{S}^\epsilon$ for continuous-variable protocols would include for instance Alice and Bob applying random squeezing operations on part of their subsystems. This obviously leads to a change of the parameters T and ξ as a

squeezing operation does not conserve the total energy for instance. However, applying such random squeezing operators symmetrizes the state ρ_{AB}. An other possibility would be for Alice and Bob to mix their states with additional (classically correlated) modes.

More generally, Alice and Bob could apply a local Hamiltonian to their respective state that would drive their bipartite state closer to an i.i.d. state. The question of which Hamiltonian would be the most effective with the respect of the final key rate is still unsolved.

6.4.3 Links with Statistical Mechanics

Our goal ultimately is to show that there exists a procedure allowing Alice and Bob to transform their initial state ρ_{AB} into a state which is as close as possible to a Gaussian state. Such a procedure could be to couple their respective n modes with a heat reservoir, so that their respective states could be described by the canonical ensemble and then converge to Gaussian states.

A possible procedure would be the following. Alice and Bob start with a N-mode state which they first symmetrize using the technique detailed in the previous section. Then they define n particular modes that will be used in the raw key while the other $N - n \ll N$ are used for a procedure close to the parameter estimation. More precisely, if $N - n \ll n$, then the n modes act like a heat reservoir for the $N - n$ modes. One can therefore proceed with measurements on these $N - n$ modes to obtain information concerning the other n modes. More specifically, if the state considered was simply ρ_A instead of ρ_{AB}, the parameter of interest would be the temperature of the system A (or equivalently, its energy). Here we consider a bipartite system, so the parameters of interest are the energies for both Alice and Bob's systems as well as the level of correlation between these systems. With this information, Alice and Bob could prepare two heat reservoirs with the appropriate temperature and couple them with their respective n modes. If this coupling is done appropriately (not sure how ...), the correlation between Alice and Bob should remain the same (in total, not per mode!), and the secure key rate one could obtain would be necessarily equal or less than the initial key rate. However, now, the new state shared by Alice and Bob would be much closer to a Gaussian state.

These ideas are still preliminary and should be the object of future investigation.

CHAPTER 7

Finite size analysis

So far in this manuscript, we mostly (exclusively?) focused on the problem of the security of continuous-variable QKD protocols in the *asymptotic* limit and not on the ultimately necessary *finite size* analysis. This choice can be justified by different reasons. The main reason is historical. When, in 1984, Bennett and Brassard came up with the idea of a quantum key distribution protocol, they only had a hint to believe that their protocol had to be secure in some appropriate regime (for instance in the unrealistic case where Alice and Bob's data are perfectly correlated) but could not establish any security proof for a realistic setup at that time. During the last 25 years, security proofs have steadily improved by including more and more effects: what happens if the quantum channel is lossy or noisy, what happens if Alice uses weak coherent pulses instead of true single photons for discrete-variable protocols, etc. Some questions are still not answered today: for instance, there is still no convincing theoretical framework allowing to deal with side-channels[1]. Among the questions that have been solved quite recently (at least in the discrete-variable case) is the one of finite size effects: how does the key rate depend on

[1] An extreme solution in order to avoid this problem is to use device-independent QKD [1] but this is highly unpractical! In fact, if one cannot prove the security of more practical protocols, taking into account imperfect implementations, then quantum key distribution will probably have no future, except from a completely (fascinating) theoretical perspective.

the number of signals exchanged by Alice and Bob? This question was first addressed by Renner in his PhD thesis [124] and subsequently detailed in [137] and [21] where the authors published very pessimistic results. In particular, it is not totally unreasonable to think that the security of all QKD implementations realized until now was jeopardized due to the (way) too short length of the blocks exchanged by Alice and Bob.

The goal of this chapter is to extend the framework of finite size analysis to continuous-variable QKD protocols. We do not solve this problem completely here, and we mainly consider the finite size effects on the parameter estimation procedure. Despite the fact that all questions are certainly not yet answered, we will be able to give an estimation of the secret key rate of the protocols described in the previous chapters for a finite size analysis. As expected, these results are considerably more pessimistic than the ones presented in Chapters 4 and 5 where we were only interested in the asymptotic regime.

7.1 The general framework for finite size analysis

The formalism developed in Renner's thesis allows for the following generalization of the secret-key rate of a discrete-variable QKD protocol which is secure against collective attacks[2] [137]:

$$k = \frac{n}{N}\left(S_{\epsilon_{\mathrm{PE}}}(x|E) - \Delta - \frac{\mathrm{leak}_{\mathrm{EC}}}{n}\right). \tag{7.1}$$

This key rate has to be compared to the asymptotic key rate K given by

$$K = S(x|E) - H(x|y), \tag{7.2}$$

and four differences can be noticed:

- only n signals are used for the establishment of the key, out of the N signals exchanged. This is due to the fact that $N - n$ signals are used for parameter estimation. This leads to the presence of the prefactor n/N in front of the secret key rate.

- the parameter estimation has a finite precision characterized by the parameter ϵ_{PE}, which is the probability that the true values of the parameters are not inside the

[2] If one was to consider general security, it would be necessary to add a correction term linked to the use of the exponential version of de Finetti theorem [125], or to the postselection technique [31] and this would give an even more pessimistic key rate. However, in the case of BB84 for instance, collective attacks are optimal, even in the case of finite size analysis, and such terms are therefore not required. For CV QKD protocols, it is also conjectured but not yet proven that collective attacks are always optimal. Therefore, it makes sense to consider the finite size analysis when the eavesdropper is restricted to collective attacks. Without the proof of the optimality of collective attacks, one can certainly use the bound derived in [127] for the application of an exponential version of de Finetti theorem for infinite-dimensional Hilbert spaces. However, this bound leads to very, very pessimistic results, and it is not believed that this bound is tight.

confidence region computed from the parameter estimation procedure[3]. There exists a clear trade-off between the level of precision desired and the number of signals that need being used to this end, and that would be useless for the distillation of the key. In [21], the authors suggest that in the limit where N tends to infinity, the optimal number of samples $N - n$ used for the parameter estimation should be on the order of $\sqrt{N}$. However, for reasonable values of the block length N, the number of samples certainly needs to be much larger than $\sqrt{N}$, especially in the case of continuous-variable protocols.

- the parameter Δ accounts for the security parameter of the privacy amplification and will be detailed below.

- finally, leak_{EC} corresponds to the amount of information which needs to be exchanged by Alice and Bob during the reconciliation phase. This quantity is necessarily equal or larger than the conditional entropy $H(x|y)$ due to Shannon theorem, but in practice, it always turns out out be strictly larger than the optimal value.

A few remarks are in order. First, we would like to emphasize that the effect of an imperfect reconciliation, which is parameterized by leak_{EC} here, was already taken into account for the study of continuous-variable QKD through the term β that corresponds to the so-called *reconciliation efficiency* (the reader is referred to Chapters 4 and 5 for a precise definition of β). This effect has indeed been for a long time the cause of the limited range of CV QKD protocols. In the case of discrete-variable QKD protocols, leak_{EC} is typically modeled as:

$$\text{leak}_{\text{EC}} \approx f_{\text{EC}} H(x|y) + \frac{1}{n} \log_2(2/\epsilon_{\text{EC}}), \tag{7.3}$$

where $f_{\text{EC}} > 1$ is a parameter characterizing the reconciliation efficiency (in a slightly different way than β for continuous-variable reconciliation[4]) and ϵ_{EC} is the probability that the reconciliation fails and that this failure goes undetected by Alice and Bob[5].

[3]Note there is never unicity of such a confidence region, but one is free to optimize his choice among all possible regions compatible with the failure probability ϵ_{PE}. This choice can be based on the easiness of the description of the region (for instance the Cartesian product of n_{PE} intervals if n_{PE} independent parameters need to be estimated), or on an optimization maximizing the final secret key rate, in which case the confidence region is a very general region in the n_{PE}-dimensional space of the parameter space. Unfortunately, such an optimization is often rather complicated to perform, and in general, one chooses confidence regions with very simple shapes.

[4]In fact, f_{EC} and β are related to each other (for binary variables) through the following equation

$$(f_{\text{EC}} - 1) H(x|y) = (1 - \beta) I(x; y). \tag{7.4}$$

Using the fact that $I(x; y) = H(x) - H(x|y) = 1 - H(x; y)$ for symmetric binary variables, one obtains

$$f_{\text{EC}} = \frac{1 - \beta(1 - H(x|y))}{H(x|y)}. \tag{7.5}$$

[5]In practice, this probability can be made arbitrarily small. The idea is for Alice and Bob to compute a hash of their respective bit strings after the reconciliation and to publicly compare it. This method is

Second, the factor n/N due to the fact that $N - n$ data are used for parameter estimation is not very critical: it would maybe be very relevant if a QKD protocol were to be implemented and commercialized as it limits the rate of the protocol, but in practice, it has very little effect on the final rate, say a factor 1/2 if 50% of the data are used for parameter estimation. Indeed, the real theoretical problem today is certainly to decide when a given QKD protocol is secure, more precisely, in which conditions (of losses and noise) it can be used to distill a secret key. From this point of view, optimizing every possible parameter in order to maximize the secret key rate seems a little bit premature[6].

Let us now turn to the new finite size effect that is Δ. As we said, Δ is linked to the security of the privacy amplification procedure. Its value is given by

$$\Delta \equiv (2\dim \mathcal{H}_X + 3)\sqrt{\frac{\log_2(2/\bar{\epsilon})}{n}} + \frac{2}{n}\log_2(1/\epsilon_{\mathrm{PA}}), \tag{7.6}$$

where $\mathcal{H}_X$ is the Hilbert space corresponding to the variable x used in the raw key, $\bar{\epsilon}$ is a *smoothing* parameter and ϵ_{PA} is the failure probability of the privacy amplification procedure. Both the smoothing parameter $\bar{\epsilon}$ and ϵ_{PA} are intermediate parameters which should be optimized numerically. The first term of Δ, that is the square-root term, actually corresponds to the speed of convergence of the smooth min-entropy of an i.i.d. state (remember that we consider collective attacks here) towards the von Neumann entropy. Indeed, only in the asymptotic limit is the smooth min-entropy of an independent and identically distributed quantum state to its von Neumann entropy. The second term is directly linked to the failure probability ϵ_{PA} of the privacy amplification procedure. The parameter ϵ_{PA} should also be optimized numerically.

Finally, the last finite size effect is the finite precision of the parameter estimation. For BB84, only one parameter needs be estimated[7]: the quantum bit error rate (QBER). Using Hoeffding's inequality for instance, one can find a confidence interval (parameterized by ϵ_{PE}) for this parameter such that the true value of the parameter (here the QBER) is inside the interval with probability $1 - \epsilon_{\mathrm{PE}}$. In the case where several parameters must be estimated (for instance in continuous-variable QKD protocols), the notion of confidence interval should be replaced by a confidence region[8] such that the true value

very interesting because computing a hash acts like an error amplification: even if the original strings only differ for a few bits out of several millions, their hash will be different with a very high probability. Hence Alice and Bob can check that they share a common bit-string while sacrificing only a negligible quantity of data.

[6]For a given QKD protocol, the important (still unsolved because of side-channel effects for instance) question is clearly to determine the two regions (parametrized by the distance between Alice and Bob, and the level of noise in the channel for instance) where the protocol can be used and where it is useless. From a theoretical point of view, a factor 2 on the final secret key rate is therefore almost meaningless. But this would however not be the case anymore if quantum key distribution were to be deployed for real-world applications.

[7]actually, depending on the implementation, more parameters might need being estimated especially if weak coherent states are sent instead of true single photons, for instance in the case where the decoy-state technique [95] is applied.

[8]when two parameters have to be estimated, the confidence region can be a rectangle or an ellipse for example.

of the parameters lies in the region with a probability at least $1 - \epsilon_{\mathrm{PE}}$. Then one needs to compute the minimum value of the conditional entropy $S(x|E)$ compatible with the confidence interval: this gives $S_{\epsilon_{\mathrm{PE}}}(x|E)$. Whereas this procedure is relatively straightforward for the QBER (which is a bounded parameter since $0 \leq \mathrm{QBER} \leq 1$), we will see in the following that the question is more involved for continuous-variable QKD protocols where one needs to estimate *a priori* unbounded parameters such as the excess noise. In the following, we will consider two parameters to be estimated in continuous-variable QKD: the transmission T and the excess noise ξ. In principle, these are not the only parameters to be estimated in a real implementation as one also needs to know Alice's modulation variance[9], but one can reasonably assume that this parameter is relatively well known, in comparison to T and ξ.

In the end, one needs to fix an overall security parameter ϵ for the quantum key distribution protocol. This parameter corresponds to the failure probability of the whole protocol, meaning that the protocol is assured to performed as is supposed to[10] except with a probability at most ϵ. This failure probability can be computed from the various parameters described above, and in the limit of small parameters[11], one has

$$\epsilon = \epsilon_{\mathrm{EC}} + \bar{\epsilon} + \epsilon_{\mathrm{PA}} + \epsilon_{\mathrm{PE}}. \tag{7.7}$$

Note that all parameters $\epsilon_{\mathrm{EC}}, \bar{\epsilon}, \epsilon_{\mathrm{PA}}$ and ϵ_{PA} can independently be fixed at arbitrarily low values:

- ϵ_{EC} can be decreased simply by increasing the length of the hash Alice and Bob compute from their raw keys. Indeed, the larger the length of the hash, the smaller the probability that their raw keys differ.

- $\bar{\epsilon}$ and ϵ_{PA} are virtual parameters that can be optimized in the computation. They must simply satisfy both equalities 7.6 and 7.7.

- ϵ_{PE} can also be made as low as desired simply by increasing the size of the sample used for parameter estimation (and therefore not used for establishing a key).

As a consequence, the overall security parameter ϵ can be chosen arbitrarily small, to a value corresponding to the users wishes. Obviously, this comes at the cost of decreasing the final secret key size.

Note also that an additional (experimental) parameter needs to be taken into account in order to compute the real secret key rate (in bits per second), that is the *detection rate* which quantifies the rate at which Alice and Bob exchange quantum signals. Here however, we do not consider such a parameter and always express the secret key rate in bits per channel use.

[9] as well as the electronic noise if one considers a scenario where Bob's detection is calibrated.

[10] here, we do not consider problems due to an imperfect implementation, which might lead to the existence of side-channels that can be used by an eavesdropper.

[11] in general, one has $1 - \epsilon = (1 - \epsilon_{\mathrm{EC}})(1 - \bar{\epsilon})(1 - \epsilon_{\mathrm{PA}})(1 - \epsilon_{\mathrm{PE}})$, which gives equation 7.7 for $\epsilon \ll 1$.

7.2 Outline of the CV QKD protocol in a finite size context

Traditionally, in the asymptotic regime, one knows perfectly the quantum channel, even before the experiment is actually performed. Hence the optimization of the various free parameters can be made before the exchange of data, and even the final secret key rate is known in advance.

In the finite-size scenario, the situation is rather different. In particular, one does not know in advance the characteristics of the quantum channel. To be fair, even after the exchange of quantum signals, the quantum channel is only partially known: more precisely, a few relevant parameters (QBER for qubit channels[12], transmission and excess noise for continuous-variable channels) are known to lie inside some confidence regions, except with probability ϵ_{PE}.

Even if Alice and Bob do not know in advance the properties of the quantum channel they will use, they can guess them with a reasonable accuracy, making the assumption that no eavesdropper will actually try to control the quantum channel. Note that this guess is only used in order to *a priori* optimize various parameters of the protocols and consequently maximize the expected secret key rate, under a "normal use" of the quantum channel. If an eavesdropper is present, the guess made by Alice and Bob might not be very good, hence leading to an non optimized use of the quantum channel, but the security of the key distribution will not be affected.

For a continuous-variable QKD protocol, the secret key rate depends (in the asymptotic limit) on three main physical parameters: Alice's modulation variance V_A, the transmission of the channel T and the excess noise ξ. The idea is to optimize V_A in order to maximize the expected secret key rate. To do that, Alice and Bob can guess the values of T and ξ. Indeed, the value of ξ depends on the quality of the setup and turns out to be fairly stable from one experimental run of the QKD protocol to the next. Typically, for state-of-the-art implementations, its value is around 1% of the shot noise [48]. The transmission can also be evaluated quite precisely with $T \approx \eta 10^{-0.02d}$ where η is the known quantum efficiency of Bob's detection (typically around 60%) and d is the distance in kilometers between Alice and Bob. Here, we assume an optical fiber with losses of 0.2dB per kilometer. In practice, Alice and Bob generally have a good estimate of the transmission of the quantum channel before they even start the quantum key distribution protocol.

At the beginning of the protocol, Alice and Bob agree on a particular value of the overall security parameter ϵ. They also agree on a reconciliation protocol, meaning that they know the parameter ϵ_{EC} in advance. Since both $\bar{\epsilon}$ and ϵ_{PA} are virtual parameters

[12] In general, as many as three different QBER could be considered depending on the polarization choice σ_X, σ_Y or σ_Z. For BB84, two such polarizations are relevant but one can apply random bit-flips and phase-flips in order to need to consider only one (symmetrized) QBER. Remember that in a finite-size scenario, the fewer parameters to consider, the better, which is in sharp contrast with the situation encountered in the case of asymptotic analysis where the better the quantum channel is characterized, the higher the secret key rate [155]. This is consistent with the results of Chapter 6 where it is shown that Alice and Bob can always consider symmetrized versions of the quantum channel, without overestimating their secret key rate.

that have to be optimized afterwards. The rest of the initial (that is before the quantum distribution) optimization consists in studying the parameter ϵ_{PE} which quantifies the failure probability of the parameter estimation. This parameter depends on the number $N-n$ of samples used for this parameter estimation as well as on some properties of the quantum channels such as the expected true values of the parameters[13]. Therefore, given the expected behavior of the quantum channel, one can infer the value of $N-n$ required to obtain a particular value of the parameter ϵ_{PE}. This in turn puts a lower bound on the block size N.

At this point, still before the actual start of the quantum key distribution protocol, Alice and Bob can optimize the values of the total number N of signal exchanged, the length of the raw key n as well as the optimal value for Alice's modulation variance V_A in order to maximize the expected secret key rate compatible with a overall security parameter ϵ. The values of N, n and V_A can be considered to be fixed at this stage.

Then, Alice and Bob proceed with the quantum exchange part of the QKD protocol: Alice sends N random coherent states (modulated with a variance V_A) who measures them with a homodyne (or heterodyne) detection. Bob informs Alice of his measurement choices (that is, for each state, Bob tells Alice whether he measured the X or the P quadrature, or both) and Alice discards the data that Bob did not measure. They publicly compare $N-n$ of their correlated data in order to estimate the true values of the transmission and excess noise of the quantum channel. They can therefore compute the value of $S_{\epsilon_{\mathrm{PE}}}(y|E)$, the conditional von Neumann entropy of Bob's data (which will be used to form the key in a reverse reconciliation procedure) given Eve's quantum state, which is compatible with the estimated parameters except with probability ϵ_{PE}. If this value is compatible with a positive secret key rate, Alice and Bob continue with the reconciliation procedure, otherwise they abort the protocol. At the end of the reconciliation procedure, Alice and Bob compute the hash of their respective bit strings (for some well chosen hash function, that is a randomly chosen hash function from a family such that the equality of both hashs guarantees that the reconciliation procedure worked except with probability ϵ_{EC}). If their strings differ (because their hashs differ), Alice and Bob abort the protocol[14]. If their hashs are identical, Alice and Bob compute the final key size compatible with the security parameter ϵ (by optimizing over $\bar{\epsilon}$ and ϵ_{PA}) and perform the privacy amplification, that is, they randomly pick a hash function from a two-universal family of hash functions from $\{0,1\}^n$ to $\{0,1\}^l$ where $l=kN$ is the size of the ϵ-secure secret key that they can extract from their data.

In the remaining of the chapter, we try to adapt the framework presented in the previous section to the case of continuous-variable QKD protocols. More precisely, in Section 7.3, we present various issues that are specific to continuous-variable QKD, linked in particular to the problem of the infinite dimension of the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. Then, in Section 7.4, we study the procedure which is at the heart of finite-size analysis, that

[13] Actually, the general situation is rather involved for continuous-variable QKD and in this manuscript, we will have to make the assumption of a Gaussian quantum channel in order to deal with the parameter estimation problem, especially in order to derive the confidence region.

[14] Note however, that Alice and Bob might try to continue with the protocol by exchanging more classical information in order to complete the reconciliation procedure.

is, *parameter estimation*. Finally, we present the results of this finite-size analysis for the 4-state protocol as well as the GG02 protocol in section 7.5. Note that in this chapter, we only address the security of CV QKD protocols which do not involve a postselection procedure[15].

7.3 Various issues specific to continuous variables

First of all, we would like to insist on the fact that we are only considering here collective attacks and not general attacks. This decision can be motivated by the fact that the optimality of collective attacks has been proven asymptotically and that it is conjectured that this optimality could hold in a finite-size setting. Moreover, the correction terms computed in [127] are quite large and probably not tight. Therefore, using the proof of [127] to study the behavior of CV QKD in a finite-size scenario would appear quite pessimistic and might hide interesting effects (such as the dependence of the key rate on parameter estimation) behind purely technical details such as (temporary?) bounds linked to a particular mathematical proof (exponential version of de Finetti theorem for infinite dimensional Hilbert spaces).

7.3.1 Dimensionality

The main difference between discrete-variable and continuous-variable QKD protocols is obviously the infinite dimensionality of the Hilbert space required to describe CV QKD protocols. This is in general rather problematic when studying the security of CV QKD but it becomes even more annoying when one considers finite size effects. In particular, if one is only interested in asymptotic key rates, the dimension problem can be solved by saying that in the end, everything in the experiment is discrete (even the homodyne detection since the local oscillator has a finite energy). Therefore, one can always theoretically bound the dimension of the relevant Hilbert space by a number large enough and prove that the correction terms due to this large dimension all go to zero in the asymptotic limit. Unfortunately, for a finite-size scenario, such an approach fails as the convergence towards the asymptotic rate is very (very) slow.

For that reason, it is important to come up with security proofs that are as dimension-independent as possible. When this is not possible, one should be able to replace the real dimension of the system (for instance of the order of 2^{12} if one uses 12-bit analog-to-digital converters) by its *effective dimension*. Such an effective dimension is generally much smaller than the real dimension and is sufficient to capture the relevant features of the continuous-variable system. Different definitions for this effective dimension can be proposed. Generally however, one defines the effective dimension d_1^{eff} of a mixed system

[15] Remember that protocols with a postselection procedure are only proved to be secure against Gaussian attacks. Unfortunately, in a finite-size context, it is impossible to prove rigorously that an attack is indeed Gaussian. One can probably upper-bound the probability that it is not the case but this is not a trivial task, and it is quite certain that the final secret key rate one could compute would be very small.

ρ as [120]

$$d_1^{\text{eff}}(\rho) \equiv \frac{1}{\text{tr}\rho^2}, \tag{7.8}$$

which quantifies the number of states over which ρ is spread. For instance, a totally mixed state over N orthogonal states has $d^{\text{eff}} = N$. A more speculative variant would be to remember that according to [83], the proper max-entropy $H_{\max}$ of a state is not the Rényi entropy of order 0 (which diverges for any quantum state of a CV system) but the Rényi entropy of order 1/2. Therefore one could also define the effective dimension d_2^{eff} as the exponential of this entropy, that is

$$d_2^{\text{eff}}(\rho) \equiv (\text{tr}\sqrt{\rho})^2. \tag{7.9}$$

The advantage of the first definition is that it relates to the energy of the state, and that it is automatically bounded, for any state ρ.

In any case, it is intuitively clear that ultimately, it is such effective dimensions that should appear in security proofs of CV QKD protocols. This question certainly needs to be investigated further. We stress again that such a problem, which is rather benign in the asymptotic limit, plays a crucial role in a finite-size analysis.

7.3.2 Ill-defined entropies for continuous variables

Another specificity of CV QKD is that classical entropies are ill-defined for continuous variables: the Shannon entropy has to be replaced by a differential entropy, which is not a practical quantity to analyze secret key rates. For this reason, the expression

$$S_{\epsilon_{\text{PE}}}(y|E) - \frac{\text{leak}_{\text{EC}}}{n} \tag{7.10}$$

is inadequate for CV QKD. The solution is to rewrite the different quantities in terms of mutual information instead of relative entropies. Hence, the previous expression can be replaced by

$$\beta I(x:y) - S_{\epsilon_{\text{PE}}}(y:E) \tag{7.11}$$

in the case of a CV protocol. Here $\beta I(x:y)$ gives the amount of mutual information Alice and Bob were effectively capable to extract through the reconciliation phase: β is the so-called *reconciliation efficiency* which ranges from 0 when no information was extracted to 1 for a perfect reconciliation scheme. While $S_{\epsilon_{\text{PE}}}(y|E)$ is defined as the minimum conditional entropy compatible with the statistics given by the parameter estimation except with probability ϵ_{PE}, $S_{\epsilon_{\text{PE}}}(y:E)$ is naturally defined as the *maximum* of the Holevo information compatible with the statistics except with probability ϵ_{PE}. Hence, in the case of a continuous-variable QKD protocol, the secret key rate obtained for a finite size analysis reads:

$$k = \frac{n}{N}\left(\beta I(x:y) - S_{\epsilon_{\text{PE}}}(y:E) - \Delta\right). \tag{7.12}$$

7.3.3 Reconciliation efficiency

Whereas the question of error-correction has never been a crucial issue for DV protocols where it just implied a small correction term, the same is not true for CV protocols *without postselection*. For these schemes, Alice and Bob need to be able to extract their mutual information very efficiently. The absence of efficient reconciliation protocols working in the low Signal-to-Noise Ratio (SNR) regime was, for a long time, the reason why CV protocols could not distribute secret keys as far as their DV counterparts. To be more precise, a reconciliation protocol is considered efficient if β is larger than roughly 80%. For such efficiencies, the correction term appears quite negligible and has a limited impact on the QKD protocol. For a Gaussian modulation, the best known protocols achieve efficiencies higher than 80 % only for SNR larger than 1 [91]. For lower SNR (relevant to increase the range of the protocol), no good protocol is known for the reconciliation of correlated Gaussian variables. Fortunately, this problem can be solved in this regime by switching to a discrete modulation where efficient protocols are available for all SNR lower than 1 [93].

To summarize, both modulation schemes (Gaussian and discrete) are useful depending on the working distance of the protocol. When working at short distances, a Gaussian modulation should be chosen whereas a discrete modulation is more adapted to reach longer distances. In both cases, the effect of imperfect reconciliation can be taken care of by taking $\beta = 0.8$ which is a conservative value consistent with state of the art reconciliation schemes.

7.4 Parameter estimation

For discrete-variable QKD protocols, it turns out that the principal finite-size effect, in terms of its consequences on the secret key rate, is the parameter estimation. A similar situation is expected for continuous-variable protocols, the main problem being without any doubt, the estimation of the excess noise.

In this section, we study the parameter estimation procedure for continuous-variable protocols, without postselection. Quite fortunately, despite being described in an infinite dimensional Hilbert space, there are only a few parameters that need to be estimated: these are the parameters characterizing the covariance matrix of the state shared by Alice and Bob in the entanglement-based version of the protocol. On the positive side, this covariance matrix can be symmetrized through the approach explained in Chapter 6, and that the symmetrized version is described by only two unknown parameters[16]. On the negative side, in order to be able to estimate the two relevant parameters, it seems that one still has to make the assumption of a Gaussian channel. This does not look as a very

[16]Of course, if one is interested in the asymptotic secret key rate (secure against collective attacks), one should not proceed with the symmetrization as it can only decrease the secret key rate. However, without such a symmetrization, the covariance matrix is described by 10 real parameters against only two for the symmetrized covariance matrix. It will be clear at the end of this chapter (if it is not yet the case) that when considering finite-size analysis, one should really consider the symmetrized state instead of the non-symmetric one.

constraining assumption as it is known that Alice and Bob can always assume their state to be Gaussian (see results in Chapter 5). However, this result has only been established in the asymptotic limit, and one cannot yet rigorously exclude the (improbable) situation where this result does not hold in general.

A non-Gaussian attack that would exploit such a possible loophole would have to be quite subtle. Indeed, the usual security proof stating that Gaussian states are the ones which minimize the secret key rate cannot be used here because the proof implicitly assumes the knowledge of the covariance matrix. For a *given* covariance matrix, the state maximizing Eve's information is Gaussian. The only possible loophole would be that because the covariance matrix is not perfectly known in a finite-size scenario, there might exist a non-Gaussian state, compatible with the estimated covariance matrix computed with a Gaussian assumption, that would be better for Eve than the Gaussian state estimated by Alice and Bob. Let us detail things a little. Let us note $\mathcal{S}^g_{\epsilon_{\text{PE}}}$ the set of states compatible with the results of the parameter estimation, under a Gaussian model, except with probability ϵ_{PE}. Let us $\mathcal{S}^{ng}_{\epsilon_{\text{PE}}}$ the set of states compatible with the results of the parameter estimation, under a general, non-Gaussian model, except with probability ϵ_{PE}. It is not easy to compare the two sets a priori, but one can imagine that they probably get closer and closer as ϵ_{PE} goes to 0 (we typically consider $\epsilon_{\text{PE}} = 10^{-10}$). In the following, because we make the Gaussian assumption, we consider the Gaussian state $\rho^g \in \mathcal{S}^g_{\epsilon_{\text{PE}}}$ which maximizes Eve's information (note that $\mathcal{S}^g_{\epsilon_{\text{PE}}}$ is not only composed of Gaussian states, but we know that the worst case from Alice and Bob's point of view is Gaussian). However, it is not yet possible to exclude the existence of a non-Gaussian state $\rho^{ng} \in \mathcal{S}^{ng}_{\epsilon_{\text{PE}}}$ such that the secret key rate obtained for ρ^{ng} is strictly lower that the one obtained for ρ^g. This is however quite unlikely.

For this reason, we conjecture that the Gaussian optimality still holds in a non-asymptotic scenario, and in the following, the make the assumption of a Gaussian channel. Again we insist on the point that even if this conjecture were proven wrong, the bounds computed here would still be quite accurate.

Our goal here is to compute $S_{\epsilon_{\text{PE}}}(y:E)$, the maximal value of the Holevo information between Eve and Bob's classical variable compatible with the statistics except with probability ϵ_{PE}. The nice property of CV protocols without postselection is that $S(y:E)$ can be bounded from above by a function of two parameters only. More precisely, this function depends on the covariance matrix Γ_{AB} of the state ρ_{AB} shared by Alice and Bob in the entanglement-based version of the protocol [106, 51]. One can always suppose that Γ_{AB} take the following form (see Chapter 6):

$$\Gamma = \begin{pmatrix} (V_A+1)\mathbb{1}_2 & \sqrt{T}Z\sigma_z \\ \sqrt{T}Z\sigma_z & (TV_A+1+T\xi)\mathbb{1}_2 \end{pmatrix}, \tag{7.13}$$

where V_A is the variance of Alice's modulation in the *prepare and measure* scheme and T and ξ refer to the experimentally estimated effective transmission and excess noise of the channel. The parameter Z is a function of V_A which depends on the modulation scheme. For instance, one has: $Z_{\text{Gauss}} = \sqrt{V_A^2 + 2V_A}$ in the case of a Gaussian modulation. For a discrete modulation, Z has a more complicated expression but turns out to be almost

equal to Z_{Gauss} for small variances (see Chapter 5): for the two-state protocol, one has

$$Z_2 = V_A \frac{1+e^{-2V_A}}{\sqrt{1-e^{-2V_A}}}, \tag{7.14}$$

and for the four-state protocol, one has

$$Z_4 = V_A \left(\frac{\lambda_0^{3/2}}{\lambda_1^{1/2}} + \frac{\lambda_1^{3/2}}{\lambda_2^{1/2}} + \frac{\lambda_2^{3/2}}{\lambda_3^{1/2}} + \frac{\lambda_3^{3/2}}{\lambda_0^{1/2}} \right), \tag{7.15}$$

where

$$\left\{ \begin{array}{rcl} \lambda_{0,2} & = & \frac{1}{2} e^{-V_A/2} \left(\cosh(V_A/2) \pm \cos(V_A/2) \right) \\ \lambda_{1,3} & = & \frac{1}{2} e^{-V_A/2} \left(\sinh(V_A/2) \pm \sin(V_A/2) \right) \end{array} \right. \tag{7.16}$$

In order to compute $S_{\epsilon_{\text{PE}}}(y:E)$, one simply needs to evaluate $\Gamma_{\epsilon_{\text{PE}}}$, the covariance matrix compatible with the data except with probability ϵ_{PE} which maximizes the Holevo information between Eve and Bob's classical data.

The estimation of $\Gamma_{\epsilon_{\text{PE}}}$ is made through the sampling of $m \equiv N - n$ couples of correlated variables $(x_i, y_i)_{i=1\cdots m}$. As we said before, we consider here a normal model for these variables. Within this model, Alice and Bob's data are linked through the following relation[17]:

$$y = tx + z \tag{7.17}$$

which is a normal linear model parametrized by $t = \sqrt{T} \in \mathbb{R}$ and where z follows a centered normal distribution with unknown variance $\sigma^2 = 1 + T\xi$. The random variable x can be either a normal random variable with variance V_A in the case of the CV QKD protocol with a Gaussian modulation, or an unbiased Bernoulli random variable taking values $\pm\sqrt{V_A}$ in the case of the two- and four-state protocols. At this point, it is worth considering the dependence of $S(y:E)$ in the variables t and σ^2. One can in particular check numerically that the following inequalities hold for any value of the modulation variance V_A and for both modulation schemes (discrete and Gaussian):

$$\left. \frac{\partial S(y:E)}{\partial t} \right|_{\sigma^2} < 0 \quad \text{and} \quad \left. \frac{\partial S(y:E)}{\partial \sigma^2} \right|_{t} > 0. \tag{7.18}$$

This means that one can find the covariance matrix $\Gamma_{\epsilon_{\text{PE}}}$ which minimizes the secret key rate with a probability at least $1 - \epsilon_{\text{PE}}$:

$$\Gamma_{\epsilon_{\text{PE}}} = \begin{pmatrix} (V_A+1)\mathbb{1}_2 & t_{\min} Z \sigma_z \\ t_{\min} Z \sigma_z & (t_{\min}^2 V_A + \sigma_{\max}^2)\mathbb{1}_2 \end{pmatrix}, \tag{7.19}$$

where $t_{\min}$ and $\sigma^2_{\max}$ correspond respectively to the minimal value of t and the maximal value of σ^2 compatible with the sampled data, except with probability $\epsilon_{\text{PE}}/2$. Note that this means that the confidence region we consider here is simply a two-dimensional rectangle. One could obviously study more complicated regions that might slightly improve

[17] the simplicity of this relation comes from the fact that the state ρ_{AB} and consequently the quantum channel are symmetrized.

the final key rate. However, here, we prefer to study this simpler solution which has the advantage of displaying the same features as a more complicated model, but without drowning them under too technical mathematical details.

Maximum-Likelihood estimators $\hat{t}$ and $\hat{\sigma}^2$ are known for the normal linear model [104]:

$$\hat{t} = \frac{\sum_{i=1}^{m} x_i y_i}{\sum_{i=1}^{m} x_i^2} \quad \text{and} \quad \hat{\sigma}^2 = \frac{1}{m}\sum_{i=1}^{m}(y_i - \hat{t}x_i)^2. \tag{7.20}$$

Moreover, $\hat{t}$ and $\hat{\sigma}^2$ are independent estimators with the following distributions:

$$\hat{t} \sim \mathcal{N}\left(t, \frac{\sigma^2}{\sum_{i=1}^{m} x_i^2}\right) \quad \text{and} \quad \frac{m\hat{\sigma}^2}{\sigma^2} \sim \chi^2(m-1), \tag{7.21}$$

where t and σ^2 are the true values of the parameters. This allows us to compute $t_{\min}$, a lower bound for t, and $\sigma^2_{\max}$, an upper bound for σ^2 in the limit of large m[18]:

$$\begin{cases} t_{\min} & \approx & \hat{t} - z_{\epsilon_{\mathrm{PE}}/2}\sqrt{\frac{\hat{\sigma}^2}{m\,V_A}} \\ \sigma^2_{\max} & \approx & \hat{\sigma}^2 + z_{\epsilon_{\mathrm{PE}}/2}\frac{\hat{\sigma}^2\sqrt{2}}{\sqrt{m}} \end{cases} \tag{7.22}$$

where $z_{\epsilon_{\mathrm{PE}}/2}$ is such that $(1 - \mathrm{erf}(z_{\epsilon_{\mathrm{PE}}/2}/\sqrt{2})/2 = \epsilon_{\mathrm{PE}}/2$.

In a given experiment, one can simply compute the values of both estimators $\hat{t}$ and $\hat{\sigma}^2$ and plug them in the previous equation in order to get the values of $t_{\min}$ and $\sigma^2_{\max}$ and finally the value of $S_{\epsilon_{\mathrm{PE}}}(y : E)$. In order to keep analyzing the protocol from a theoretical point of view, we take for $\hat{t}$ and $\hat{\sigma}^2$ their expected values:

$$\begin{array}{rcl} \mathbb{E}[\hat{t}] & = & \sqrt{T}, \\ \mathbb{E}[\hat{\sigma}^2] & = & 1 + T\xi. \end{array} \tag{7.23}$$

Using these values, one can compute $t_{\min}$ and $\sigma^2_{\max}$:

$$\begin{cases} t_{\min} & \approx & \sqrt{T} - z_{\epsilon_{\mathrm{PE}}/2}\sqrt{\frac{1+T\xi}{m\,V_A}} \\ \sigma^2_{\max} & \approx & 1 + T\xi + z_{\epsilon_{\mathrm{PE}}/2}\frac{(1+T\xi)\sqrt{2}}{\sqrt{m}}. \end{cases} \tag{7.24}$$

Finally, one gets the covariance matrix $\Gamma_{\epsilon_{\mathrm{PE}}}$ which should be used to compute the expected secret key rate $S_{\epsilon_{\mathrm{PE}}}(y : E)$ in the finite case:

$$\mathbb{E}[\Gamma_{\epsilon_{\mathrm{PE}}}] = \Gamma + \begin{pmatrix} 0 & \Delta_Z\sigma_z \\ \Delta_Z\sigma_z & \Delta_B\mathbb{1}_2 \end{pmatrix}, \tag{7.25}$$

with

$$\begin{cases} \Delta_Z & = & -z_{\epsilon_{\mathrm{PE}}/2}\sqrt{\frac{1+T\xi}{m\,V_A}} \\ \Delta_B & = & \frac{z_{\epsilon_{\mathrm{PE}}/2}}{\sqrt{m}}((1+T\xi)\sqrt{2} - 2\sqrt{TV_A}) + z^2_{\epsilon_{\mathrm{PE}}/2}\frac{1+T\xi}{m}. \end{cases} \tag{7.26}$$

[18]Indeed, for large m, the χ^2 distribution converges to a normal distribution. The approximation is almost exact in our case as we consider values of m (much) larger than 10^6.

At the first order, for long distances, the main effect is clearly the uncertainty on the excess noise. The *effective* excess noise $\Delta_m\xi$ due to the imprecision of the estimation is given by:

$$\Delta_m \xi \approx \frac{z_{\epsilon_{\rm PE}/2}\sqrt{2}}{T\sqrt{m}}. \tag{7.27}$$

We will display in the next section the effect of the parameter estimation on the secret key rate, but we can already give a hint about what kind of block length will generally be required for a given distance. Indeed, one has

$$m \approx \frac{2z^2_{\epsilon_{\rm PE}/2}}{T^2\Delta_m\xi^2}. \tag{7.28}$$

For $\epsilon_{\rm PE} = 10^{-10}$, one has $z_{\epsilon_{\rm PE}/2} \approx 6.5$, and if one requires $\Delta_m\xi \approx 1/100$, which is a typical value for the true excess noise [48], then the number of samples required scales as a function of the transmission as

$$m \propto \frac{10^6}{T^2}. \tag{7.29}$$

For instance, if the distance between Alice and Bob is 50 km, then $T = 10^{-1}$ which means that one expects the block length[19] to be on the order of 10^8, which is barely realistic. If the distance is 100 km, then the block length should be on the order of 10^{10}, which is much more complicated. We will see in Section 7.5 that the reality is even worse than that ...

Expected secret key rate or most probable secret key rate. For a given experiment, the secret key rate can be computed and is a function of the observed values of the estimators $\hat{t}$ and $\hat{\sigma}^2$ (but not only). One can write $K_{\rm exp} = f(\hat{t}, \hat{\sigma}^2)$. From a theoretical point of view, that is without performing the actual experiment, there are two different secret key rates that can be computed.

The first possibility, considered for instance in [21], in to compute the secret key rate K_1 obtained for the expected values of the parameters:

$$K_1 \equiv f(\mathbb{E}[\hat{t}], \mathbb{E}[\hat{\sigma}^2]). \tag{7.30}$$

In some sense, this corresponds to what one could call the most probable secret key rate. However, this interpretation is not correct.

In any case, the correct theoretical secret key rate K_2 is the expected value of the secret key rate, that is

$$K_2 \equiv \mathbb{E}[f(\hat{t}, \hat{\sigma}^2)]. \tag{7.31}$$

Obviously, this value is much more difficult to evaluate in general as one needs to know the probability distributions of both estimators $\hat{t}$ and $\hat{\sigma}^2$, whereas in the case of K_1, one just needs to know the expected values. We will see in Section 7.5 that in fact both values are remarkably close, meaning that one can always safely use K_1 as the secret key size.

[19] as a first approximation, the block length is comparable to the number m of samples used in the parameter estimation.

More economical parameter estimation procedure. An interesting characteristics of continuous-variable QKD protocols is that it might be possible to perform the parameter estimation without sacrifing any data. This is obviously something impossible in discrete-variable QKD where estimating the quantum bit error rate (QBER) requires for Alice and Bob to disclose part of their data.

In continuous-variable QKD however, the bit used for the raw key is encoded in only a part of Bob's classical data. Let us take the example of the four-state protocol for instance [93]. In this case, Bob's data $\{y_i\}_{1\leq i\leq N}$ are real numbers and the raw key elements are simply given by the sign of the variables y_i. The absolute value is sent to Alice through the public, authenticated channel, and Alice uses it to perform the reverse reconciliation procedure.

In the parameter estimation procedure that we described above, Alice and Bob would agree on a certain subset of their data and completely disclose their data in this subset. This means that the absolute values of the rest of Bob's data are not used for this parameter estimation, whereas it manifestly contains information concerning the covariance matrix of the state shared by Alice and Bob. One could certainly use this information to improve the accuracy of the parameter estimation, or equivalently, obtain the same accuracy while using less samples, therefore increasing the final secret key rate. However, the statistics techniques necessary for this study are beyond the scope of this manuscript, and we do not address this question more extensively here.

Before concluding this section, we give another possible way to improve upon the parameter procedure presented here. For continuous-variable QKD protocols, it is clear that the critical parameter to estimate is the excess noise. The transmission on the other hand is less critical for two reasons: first, it can be estimated more precisely than the excess noise with the same amount of data (in particular, the relative uncertainty for the transmission is smaller than the one for the excess noise), and second, the secret key rate is much more sensitive to variations in the excess noise than in the transmission. Therefore, one could use the following method in order to estimate the transmission and the parameters:

- the transmission is estimated through the same procedure as before, with m samples,
- Bob uses the totality of his data to compute an estimation of the variance of his data. Then using the relation $\langle y^2\rangle = 1 + TV_A + T\xi$ and his estimation of T, Bob infers an estimation for the excess noise.

This approach seems better than the one studied above. However, it involves computing two *dependent* estimators and the probability distributions of the estimators (necessary to compute confidence regions) are not known.

Therefore, in this chapter, we use a probably suboptimal procedure to perform the parameter estimation, but this procedure allows for the computation of explicit bounds. The question of what is the best parameter estimation procedure in the case of continuous-variable QKD is still open, and is certainly worth investigating further, as it turns out

that the parameter estimation is an important problem if one wants to distribute secret keys over long distance, while using realistic block lengths.

7.5 Results

7.5.1 Influence of Δ

On Figure 7.1, we plot the value of the parameter Δ as a function of n, the size of the raw key. Here, we take $\dim \mathcal{H}_Y = 2$ since for all continuous-variable protocols we considered in this thesis, the raw key is encoded on bits. Among notable features, one sees that the value of Δ does not depend to much on the parameters $\bar{\epsilon}$ and ϵ_{PA} which need to be optimized in theory. The important lesson is the large value of Δ, even for (seemingly)

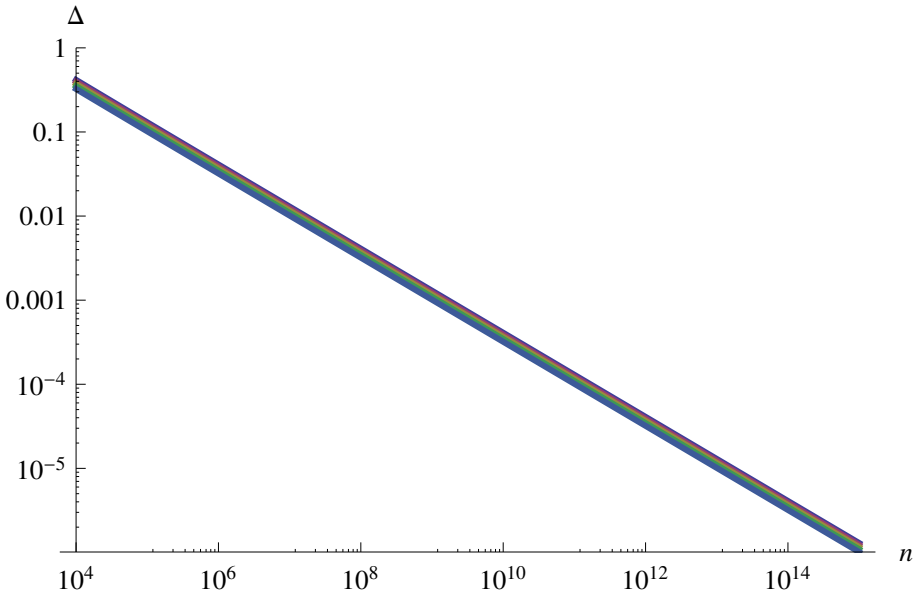

Figure 7.1: Parameter Δ as a function of n for various values of $\bar{\epsilon}$ and ϵ_{PA}. From top to bottom,$\bar{\epsilon} = \epsilon_{\mathrm{PA}} = 10^{-6}, 10^{-7}, 10^{-8}, 10^{-9}, 10^{-10}$.

quite large sizes of the raw key. In particular, one observes that Δ is larger than 0.01 for raw key sizes smaller than 10^7. In practice, this means that if the asymptotic secret key rate is below 0.01 bit per channel use, then if one wants to take into account finite-size effects, one has to use block lengths larger than 10 million in order to be able to claim to have truly distributed a secret key among distance parties. No need to say that secret key rates well below 0.01 bit per channel use have been repeatedly claimed to be achieved in the literature whereas it is doubtful any experiment actually used raw key lengths larger than 10 million!

7.5.2 Influence of the parameter estimation

Here, we focus on the value of the *effective* excess noise $\Delta_m\xi$ due to the finite precision of the parameter estimation. On Figure 7.2, we display this effective excess noise as a function of m, the number of samples used in the parameter estimation. From Figure

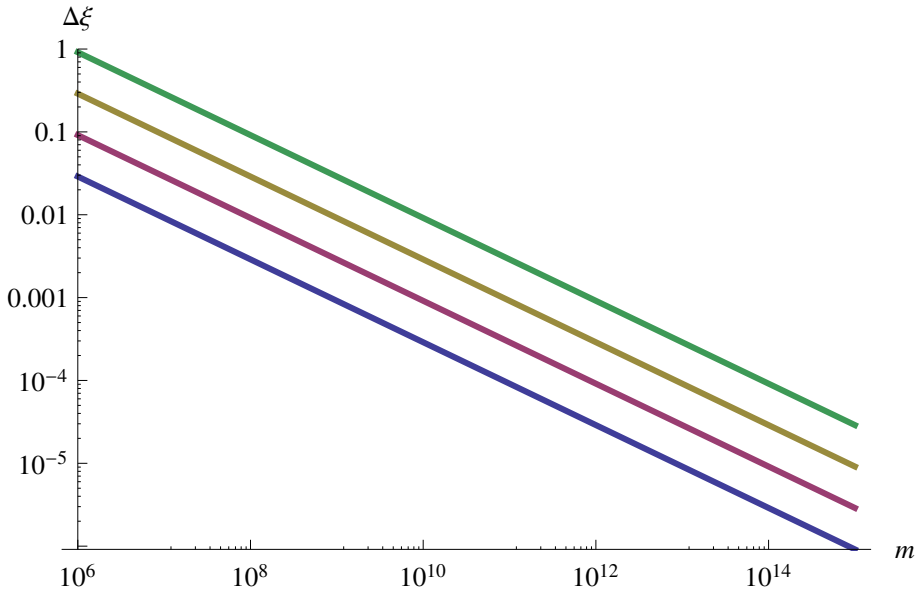

Figure 7.2: Parameter $\Delta_m\xi$ as a function of m for $\epsilon_{\mathrm{PE}} = 10^{-10}$ (in fact, $\Delta_m\xi$ does not depend too critically of the precise value of ϵ_{PE}, and one obtains almost similar plots for $\epsilon_{\mathrm{PE}} = 10^{-5}$ for instance). From bottom to top, we consider channel losses of 5 dB, 10 dB, 15 dB and 20 dB. With a perfect homodyne detection (quantum efficiency equal to 1), this is equivalent to distances of 25, 50, 75 and 100 km.

7.2, it is clear that the parameter estimation has a major impact on the final secret key rate. Indeed, the four-state protocol for instance, which can achieve remarkably long distances in the asymptotic limit, requires very low values of the excess noise, typically less than one percent in order to distribute key over distances close to 100 km. Here we see that such parameters require to sample 10 billion couples of correlated data! For this reason, it is doubtful that continuous-variable QKD is very practical over distances much larger than 100 km.

7.5.3 Secret key rate in the finite-size scenario

Here, we first consider the secret key rate K_1 which is the one obtained if the estimators $\bar{t}$ and $\bar{\sigma}^2$ are equal to their expected values. We do not proceed to a complete optimization of the various parameters since it will not fundamentally change the results and instead

take the following values:

$$\begin{cases} \epsilon_{\mathrm{EC}} = \bar{\epsilon} = \epsilon_{\mathrm{PA}} = \epsilon_{\mathrm{PE}} = 10^{-10} \\ \epsilon \approx 10^{-10} \\ m = n = N/2 \\ \beta = 80\% \\ \eta = 0.6. \end{cases} \tag{7.32}$$

The choice for ϵ is a very conservative choice, but it turns out that the secret key rate does not depend very critically on ϵ (a similar observation was made in [137]). The choice to use half of the data for the parameter estimation procedure results from the fact that the block size is almost entirely decided by the number of data actually sampled. The reconciliation efficiency of 80% is a conservative value (see Chapters 4 and 5). Finally, we consider the quantum efficiency of the homodyne detection to be 60% which corresponds to a typical experimental parameter [48]. Moreover, as we explained before in this manuscript, we consider the paranoid mode were the electronic noise is null. As a first approximation, this is equivalent (in the asymptotic regime) with the case of a realistic mode where the electronic noise is non negligible but is not supposed to be caused by the action of an eavesdropper. In the finite-size regime, one can always make the assumption that Bob's detection is very well calibrated and that there is virtually no uncertainty on the value of the electronic noise. As a consequence, in order to avoid too many technical details, we present here results obtained in the paranoid scenario without electronic noise. Note that this solution was also chosen in the review by Scarani et al [136].

The secret key rates displayed on Figure 7.3 correspond to the key rate one can expect if the estimators give the true value of the parameters. As we argued above, a more relevant secret key rate corresponds to the *expected* value computed for the probability distributions of the estimators $\hat{t}$ and $\hat{\sigma}^2$.

As we already explained, the most important parameter for the final secret key rate is the excess noise. This means that one should mainly consider the probability distribution of the estimator $\hat{\sigma}^2$. According to Equation 7.21, one has:

$$\frac{m\hat{\sigma}^2}{\sigma^2} \sim \chi^2(m-1). \tag{7.33}$$

For large m, the χ^2 distribution tends to a normal distribution, which translates into

$$\hat{\sigma}^2 \sim \mathcal{N}\left(\sigma^2, \frac{2\sigma^4}{m}\right), \tag{7.34}$$

where as before, σ^2 corresponds to the true value of the parameter. Here, we can therefore compute an approximate value of the expected secret key rate K_2 as

$$K_2 = \mathbb{E}[f(\hat{t}, \hat{\sigma}^2] \approx \mathbb{E}[f(t, \hat{\sigma}^2] \tag{7.35}$$

since $\hat{t}$ has a probability distribution peaked around the true value of the parameter t and because f does not depend critically on the value of t. Using the normality of the

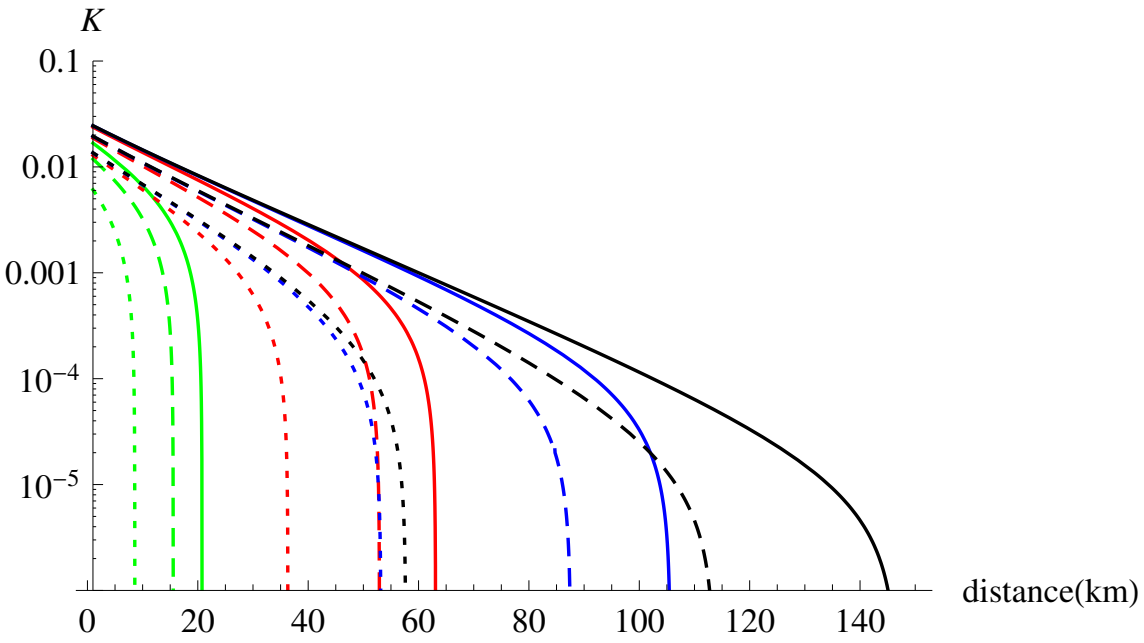

Figure 7.3: Secret key rate for the four-state protocol. The green red, blue and black curves correspond respectively to block lengths of $N = 10^8, 10^{10}, 10^{12}$ and 10^{14}. Full lines, dashed lines and dotted lines correspond respectively to an expected value of the excess noise of 0.001 (optimistic), 0.005 (realistic), 0.01 (conservative). The secret key rate is null for a block length of 10^6.

random variable $\hat{\sigma}^2$, one obtains

$$K_2 = \int_{-\infty}^{\infty} \frac{1}{2\sigma^2}\sqrt{\frac{m}{\pi}} \exp\left(-m\frac{(s-\sigma^2)^2}{4\sigma^4}\right) f(t,s)\mathrm{d}s. \tag{7.36}$$

From the relation $\sigma^2 = 1 + T\xi$, one concludes that the observed value of the excess noise $\hat{\xi}$ has the following probability distribution

$$\hat{\xi} \sim \mathcal{N}\left(\xi, \frac{2}{T^2 m}\right), \tag{7.37}$$

in the limit where $T\xi \ll 1$. Here, ξ represents the true value of the excess noise (typically between 10^{-3} and 10^{-2}) and $\hat{\xi}$ is the observed value of the excess noise.

It turns out that the behavior of K_2 is numerically indistinguishable from the value of K_1. For this reason, we do not display it here. The main consequence is that one can in very good approximation compute the final key rate by considering the expected values of the parameters being estimated. This is rather fortunate as computing K_2 is much more demanding from a computing point of view than computing K_1.

Finally, on Figure 7.4, we display the secret key rate obtained when the failure probability ϵ_{PE} of the parameter estimation procedure is set at 10^{-5} instead of 10^{-10} as in

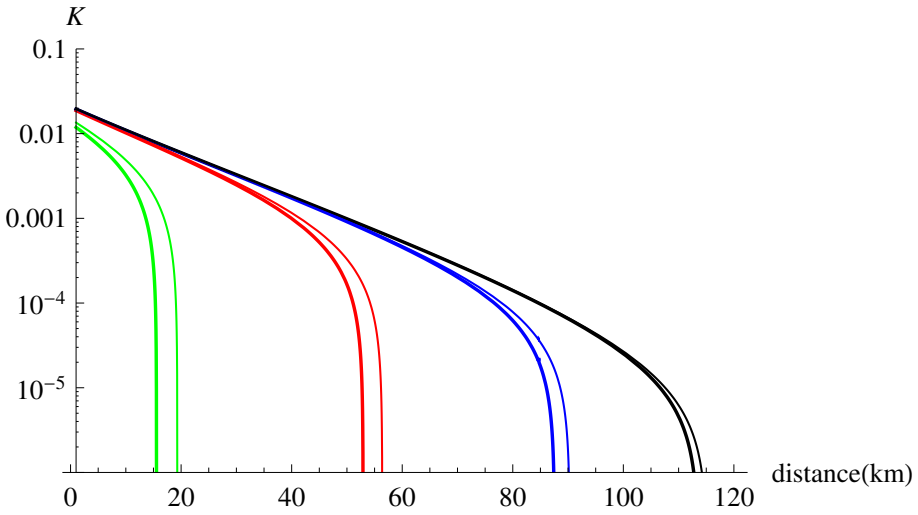

Figure 7.4: Secret key rate for the four-state protocol obtained for an expected realistic value of the excess noise of 0.005, and for $\epsilon_{\mathrm{PE}} = 10^{-5}$ (thin curves) or $\epsilon_{\mathrm{PE}} = 10^{-10}$ (thick curves). From top to bottom, the block length N is equal to $10^{14}, 10^{12}, 10^{10}$ and 10^{8}. The secret key rate is null for a block length of 10^{6}.

the previous plots. As expected, the final secret key rate is not significantly impacted by the precise value of ϵ_{PE} and increasing its value from 10^{-10} to 10^{-5} merely results in an improvement of a couple of kilometers for the range of the continuous-variable QKD protocol.

7.6 Perspectives

As we saw in this chapter, the problem of finite-size analysis of continuous-variable QKD protocols is still not completely solved. Several problems remain open and should be addressed in further studies:

- first, one should prove whether or not collective attacks are optimal in the finite-size setting. If this is the case, then all is for the best and the bounds derived here are accurate. But is collective attacks are not optimal, then one needs to come up with bounds as tight as possible. On this subject, it would seem that adapting the postselection technique from [31] to continuous variables (using for instance symmetries in phase space as explained in Chapter 6) would lead to much tighter bounds that the one currently available through an exponential version of de Finetti theorem for infinite dimensional Hilbert spaces [127].

- Second, one still needs to make the assumption of a Gaussian attack (if one restricts the adversary to collective attacks). Whereas this is completely legitimate in the asymptotic regime [51, 106], it is not so clear in a finite-size scenario, where very

subtle (and highly improbable) attacks might perform slightly better. Such attacks would have to be based on the idea of fooling Alice and Bob by having them make wrong assumptions in the parameter estimation procedure.

Despite the fact that there are still open problems concerning the finite size analysis of continuous-variable quantum key distribution, some lessons can already be learned. The main lesson is that, as is the case for discrete-variable QKD protocols, the most important finite-size effect is the limited accuracy of the parameter estimation[20]. The results presented here are very pessimistic for that matter, but the worst part is certainly that there is only one solution to fight this effect, namely increasing up to presently unrealistic values the block length. A possible alternative approach might be to give up Prepare and Measure protocols and replace them with Entanglement-based protocols. This seems to work relatively well in the case of discrete-variable QKD where entanglement-based protocols clearly outperform their Prepare and Measure alternatives in the finite-size regime (but not in the asymptotic limit) [21].

[20]In fact, this is true because the reconciliation is no longer a problem for continuous-variable QKD protocols such as the four-state protocol presented in Chapter 5. Before this protocol, the imperfect reconciliation efficiency at low SNR was preventing to distribute secret keys over distances larger than 30 or 50 km. Hence, at that time, the reconciliation efficiency was (temporarily) the most important finite-size effect (remember that the asymptotic limit can be understood as a situation where the reconciliation efficiency is equal to 100%.

CHAPTER 8

Other continuous-variable cryptographic primitives

In this chapter, I would like to investigate questions that are not directly related to continuous-variable QKD without postselection. In particular, I will first study the problem of the optimal measurement to distinguish coherent states as this is directly relevant for the security of CV QKD *with* postselection (and maybe also as an alternative approach to prove the security of the protocols already discussed in this manuscript). This problem is actually quite general and might be of importance for various cryptographic schemes with continuous variables. Then, I explain the results we obtained in collaboration with Loïck Magnin, Frédéric Magniez and Nicolas Cerf concerning quantum bit commitment: more precisely, we established a no-go theorem for quantum bit commitment with Gaussian states and Gaussian operations [102]. A nice consequence of this result is that is falsifies a conjecture formulated by Gilles Brassard and Christopher Fuchs concerning the possibility of deriving quantum mechanics from operational principles such as the possibility of secure key distribution and the impossibility of bit commitment [16].

8.1 Distinguishing coherent states

In this section, we study the problem of the discrimination of coherent states. In particular, we consider the cases of two and four coherent states described by the sets $\mathcal{S}_2$ and $\mathcal{S}_4$ which are relevant respectively for the two- and the four-state protocols presented in Chapter 5. Let us recall the definition of these sets[1]:

$$\mathcal{S}_2 = \{|\alpha\rangle, |-\alpha\rangle\}, \tag{8.1}$$
$$\mathcal{S}_4 = \{|\alpha e^{i\pi/4}\rangle, |\alpha e^{3i\pi/4}\rangle, |\alpha e^{5i\pi/4}\rangle, |\alpha e^{7i\pi/4}\rangle\}. \tag{8.2}$$

Since the different elements of $\mathcal{S}_2$ and $\mathcal{S}_4$ are not orthogonal to each other, it is impossible to distinguish them perfectly. The question that logically arises is how well they can be distinguished. There is not a unique answer to this question, as it depends how distinguishability is defined.

There are two main notions of distinguishability studied in the literature [28]:

- *ambiguous discrimination*, where the goal is to maximize the probability of success,
- *unambiguous discrimination* where errors are not authorized, at the expense of getting inconclusive results.

Both notions are relevant to the security of QKD: unambiguous discrimination for attacks where Eve does not introduce any error (or noise), and ambiguous discrimination when she introduces noise on the quantum channel.

In the following, we focus on ambiguous discrimination and consider two different probabilities of success: the maximal probability authorized by quantum mechanics, $p_{\mathrm{QM},2}$ or $p_{\mathrm{QM},4}$ for the sets $\mathcal{S}_2$ or $\mathcal{S}_4$, and the probability achievable with homodyne (or heterodyne) measurements, p_{hom} or p_{het}.

8.1.1 Case of two coherent states

Optimal measurement. The general question of distinguishing two quantum states ρ_0 and ρ_1 has been addressed by Helström [69]:

Theorem 8.1. *Let ρ_0 and ρ_1 be two quantum states prepared with probability q and $1-q$. The probability to correctly identify the state is at most:*

$$p_{\mathrm{QM},2} = \frac{1}{2}[1 + ||q\rho_0 - (1-q)\rho_1||_1]. \tag{8.3}$$

The measurement saturating this bound is the POVM $\{M_0, M_1 = \mathbb{1} - M_0\}$, where M_0 is the projector on the positive eigenspace of $q\rho_0 - (1-q)\rho_1$.

[1] Note that we slightly change the definition of $\mathcal{S}_2$ compared to Chapter 5. This is without consequence as the distinguishability of two coherent states in phase space depends only on the euclidean distance between their displacement vectors.

In our case, since we consider the set $\mathcal{S}_2$, we have $\rho_0 = |\alpha\rangle\langle\alpha|$, $\rho_1 = |-\alpha\rangle\langle-\alpha|$ and $q = 1/2$. Let us define $\rho = \frac{1}{2}\left(|\alpha\rangle\langle\alpha| + |-\alpha\rangle\langle-\alpha|\right)$. As we saw in Chapter 5, one has:

$$\rho = \lambda_0|\phi_0\rangle\langle\phi_0| + \lambda_1|\phi_1\rangle\langle\phi_1| \tag{8.4}$$

where $\lambda_0 = e^{-\alpha^2}\cosh\alpha^2$, $\lambda_1 = e^{-\alpha^2}\sinh\alpha^2$ and:

$$|\phi_0\rangle = \frac{1}{\sqrt{\cosh\alpha^2}}\sum_{n=0}^{\infty}\frac{\alpha^{2n}}{\sqrt{(2n)!}}|2n\rangle, \tag{8.5}$$

$$|\phi_1\rangle = \frac{1}{\sqrt{\sinh\alpha^2}}\sum_{n=0}^{\infty}\frac{\alpha^{2n+1}}{\sqrt{(2n+1)!}}|2n+1\rangle. \tag{8.6}$$

Let us also define $|\omega_0\rangle$ and $|\omega_1\rangle$:

$$|\omega_0\rangle = \frac{1}{\sqrt{2}}\left(|\phi_0\rangle + |\phi_1\rangle\right) \tag{8.7}$$

$$|\omega_1\rangle = \frac{1}{\sqrt{2}}\left(|\phi_0\rangle - |\phi_1\rangle\right). \tag{8.8}$$

The following lemma states that the projective measurement on the states $|\omega_0\rangle$ and $|\omega_1\rangle$ corresponds to the optimal measurement for distinguishing between $|\alpha\rangle$ and $|-\alpha\rangle$.

Lemma 8.1. *The optimal measurement for distinguishing the coherent states $|\alpha\rangle$ and $|-\alpha\rangle$ is the POVM $\{M_0 = |\omega_0\rangle\langle\omega_0|, M_1 = |\omega_1\rangle\langle\omega_1|, M_2 = \mathbb{1} - M_0 - M_1\}$. When obtaining result 0 (resp. 1), we infer that the coherent state was $|\alpha\rangle$ (resp. $|-\alpha\rangle$). Note that result 2 never occurs when measuring ρ.*

Proof. First, note that $\{M_0, M_1, M_2\}$ forms a legitimate POVM as one has $0 \leq M_2 \leq \mathbb{1}$ since M_0 and M_1 have orthogonal supports. The probability of success of this POVM is:

$$p_{\text{succ}} = \frac{1}{2}\text{tr}(M_0|\alpha\rangle\langle\alpha|) + \frac{1}{2}\text{tr}(M_1|-\alpha\rangle\langle-\alpha|) \tag{8.9}$$

$$= \frac{1}{2}|\langle\omega_0|\alpha\rangle|^2 + \frac{1}{2}|\langle\omega_1|-\alpha\rangle|^2. \tag{8.10}$$

One has:

$$\langle\omega_0|\alpha\rangle = \frac{e^{-\alpha^2}}{\sqrt{2}}\left(\frac{1}{\sqrt{\cosh\alpha^2}}\sum_{n=0}^{\infty}\frac{(\alpha^2)^{2n}}{(2n)!} + \frac{1}{\sqrt{\sinh\alpha^2}}\sum_{n=0}^{\infty}\frac{(\alpha^2)^{2n+1}}{(2n+1)!}\right) \tag{8.11}$$

$$= \frac{1}{\sqrt{2}}\left(\sqrt{\lambda_0} + \sqrt{\lambda_1}\right) \tag{8.12}$$

$$= \langle\omega_1|-\alpha\rangle. \tag{8.13}$$

Therefore, it follows that

$$p_{\text{succ}} = \frac{1}{2}\left(\sqrt{\lambda_0} + \sqrt{\lambda_1}\right)^2 = \frac{1}{2}\left(1 + \sqrt{1 - e^{-4\alpha^2}}\right). \tag{8.14}$$

Let us now compute the Helström bound:

$$p_{QM,2} = \frac{1}{2}\left(1 + \frac{1}{2}\,||\,|\alpha\rangle\langle\alpha| - |\alpha\rangle\langle\alpha|\,||_1\right). \tag{8.15}$$

One needs to compute the trace norm of $\sigma = \frac{1}{2}\left(|\alpha\rangle\langle\alpha| - |-\alpha\rangle\langle-\alpha|\right)$:

$$\begin{aligned} ||\sigma||_1 &= \mathrm{tr}|\sigma| = \mathrm{tr}\sqrt{\sigma^2} && (8.16)\\ &= \mathrm{tr}\left(\lambda_0\lambda_1\left(|\phi_0\rangle\langle\phi_0| + |\phi_1\rangle\langle\phi_1|\right)\right) && (8.17)\\ &= 2\sqrt{\lambda_0\lambda_1}. && (8.18) \end{aligned}$$

Therefore, one gets the Helström bound:

$$p_{\mathrm{QM},2} = \frac{1}{2}\left(1 + \sqrt{1 - e^{-4\alpha^2}}\right). \tag{8.19}$$

This proves that the POVM $\{M_0, M_1, M_2\}$ saturates the Helström bound.

□

Homodyne detection. Unfortunately, the POVM described above is not very practical. A much easier way to discriminate the two coherent states $|\alpha\rangle$ and $|-\alpha\rangle$ is to perform an homodyne measurement. In this case, we assign the state $|\alpha\rangle$ for positive results and $|-\alpha\rangle$ for negative results. This procedure, homodyne measurement followed by the post-processing assigning a different state for each sign of the result, can also be seen as a POVM $\{M_0^{\mathrm{hom}}, M_1^{\mathrm{hom}}\}$ with

$$M_0^{\mathrm{hom}} = \int_0^\infty |x\rangle\langle x|\,\mathrm{d}x \quad \text{and} \quad M_1^{\mathrm{hom}} = \mathbb{1} - M_0^{\mathrm{hom}} = \int_{-\infty}^0 |x\rangle\langle x|\,\mathrm{d}x. \tag{8.20}$$

The probability of success of this strategy is obtained by integrating the square of the wavefunction of $|\alpha\rangle$ (resp. $|-\alpha\rangle$) over the positive (resp. negative) real numbers:

$$\begin{aligned} p_{\mathrm{hom}} &= \int_0^\infty |\langle x|\alpha\rangle|^2 \mathrm{d}x && (8.21)\\ &= \int_0^\infty |\phi(x)|^2 \mathrm{d}x && (8.22)\\ &= \frac{1}{\sqrt{\pi}}\int_0^\infty e^{-(x-\alpha)^2}\mathrm{d}x && (8.23)\\ &= \frac{1}{2}\left(1 + \mathrm{erf}\left(\sqrt{2}\alpha\right)\right). && (8.24) \end{aligned}$$

This probability is strictly smaller than the Helström bound but turns out to be almost optimal for very low values[2] of the parameter α (see Figure 8.1). Note also that the homodyne detection has recently been proven to be optimal among Gaussian measurements [152].

[2] as well as for large values of α since both states than become almost orthogonal.

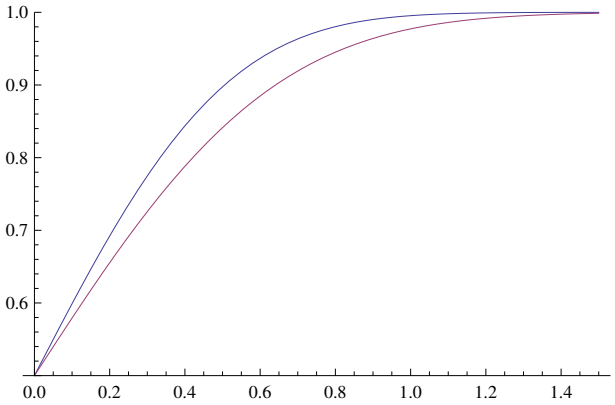

Figure 8.1: Probability of success of distinguishing $\{|\alpha\rangle, |-\alpha\rangle\}$ with an optimal measurement (upper curve), and an homodyne detection (lower curve), as a function of α.

8.1.2 Case of four coherent states

We now consider the four coherent states $\{|\alpha_0\rangle, |\alpha_1\rangle, |\alpha_2\rangle, |\alpha_3\rangle\}$ of the set $\mathcal{S}_4$ are prepared with probability 1/4, $|\alpha_k\rangle = |e^{i(2k+1)\pi/4}\alpha\rangle$ for $k \in \{0,1,2,3\}$. Let us consider the mixed state σ defined as:

$$\sigma = \frac{1}{4}\left(|\alpha_0\rangle\langle\alpha_0| + |\alpha_1\rangle\langle\alpha_1| + |\alpha_2\rangle\langle\alpha_2| + |\alpha_3\rangle\langle\alpha_3|\right). \tag{8.25}$$

The state σ is a rank 4 operator that can be diagonalized as follows:

$$\sigma = \sum_{k=0}^{3} \mu_k |\phi_k\rangle\langle\phi_k| \tag{8.26}$$

where

$$\mu_{0,2} = \frac{1}{2}e^{-\alpha^2}(\cosh(\alpha^2) \pm \cos(\alpha^2)), \tag{8.27}$$

$$\mu_{1,3} = \frac{1}{2}e^{-\alpha^2}(\sinh(\alpha^2) \pm \sin(\alpha^2)) \tag{8.28}$$

and

$$|\phi_k\rangle = \frac{e^{-\alpha^2/2}}{\sqrt{\lambda_k}} \sum_{n=0}^{\infty} \frac{\alpha^{4n+k}}{\sqrt{(4n+k)!}}(-1)^n |4n+k\rangle \tag{8.29}$$

for $k \in \{0,1,2,3\}$.

The idea now is to determine the optimal POVM $\{M_0, M_1, M_2, M_3\}$ for the ambiguous discrimination of the four coherent states. To our knowledge, such a POVM, specifically concerned with the discrimination of coherent states, has not yet been studied in the literature.

Optimal measurement. The states $\{|\alpha_0\rangle, |\alpha_1\rangle, |\alpha_2\rangle, |\alpha_3\rangle\}$ are pure and *symmetric*, in the sense that

$$|\alpha_k\rangle = U|\alpha_{k-1}\rangle = U^k|\alpha_0\rangle \tag{8.30}$$
$$U|\alpha_3\rangle = |\alpha_0\rangle, \tag{8.31}$$

where $U = \exp(i\frac{\pi}{4}a^\dagger a)$. For such states, the measurement that maximizes the probability of success for the discrimination is known: it is the so-called *square-root measurement* [28]: the optimal measurement operators are M_0, M_1, M_2 and M_3 defined as

$$M_k = \frac{1}{4}\sigma^{-1/2}|\alpha_k\rangle\langle\alpha_k|\sigma^{-1/2}. \tag{8.32}$$

Note that these operators form a genuine POVM as they are positive operators which sum to $\mathbb{1}$. Then, the maximal probability of success allowed by Quantum Mechanics is:

$$p_{\mathrm{QM},4} = \frac{1}{16}\sum_{k=0}^{3}|\langle\alpha_k|\sigma^{-1/2}|\alpha_k\rangle|^2. \tag{8.33}$$

In order to make this explicit, we first notice that the states $|\alpha_k\rangle$ are linear combinations of the $|\phi_k\rangle$:

$$|\alpha_k\rangle = \sum_{m=0}^{3}\sqrt{\mu_m}e^{im(2k+1)\pi/4}|\phi_m\rangle. \tag{8.34}$$

Therefore, one has $M_k = |\omega_k\rangle\langle\omega_k|$ with:

$$|\omega_k\rangle = \sigma^{-1/2}|\alpha_k\rangle \tag{8.35}$$
$$= \sum_{p,q=0}^{3}\mu_p^{-1/2}|\phi_p\rangle\langle\phi_p|\sqrt{\mu_q}e^{iq(2k+1)\pi/4}|\phi q\rangle \tag{8.36}$$
$$= \sum_{p=0}^{3}e^{ip(2k+1)\pi/4}|\phi_p\rangle, \tag{8.37}$$

and

$$p_{\mathrm{QM},4} = \frac{1}{16}\sum_{k=0}^{3}|\langle\alpha_k|\omega_k\rangle|^2 \tag{8.38}$$
$$= \frac{1}{4}\left(\sum_{k=0}^{3}\sqrt{\mu_k}\right)^2. \tag{8.39}$$

Heterodyne measurement. The natural generalization of the homodyne detection in the case of four coherent states is an hererodyne measurement. It consists in sending the state on a balanced beamsplitter and proceeding with homodyne detections along two different quadratures for the two output modes. Sending the state $|\alpha_k\rangle$ through a

balanced beamsplitter outputs the bimodal state $|\alpha_k/\sqrt{2}\rangle_1|\alpha_k/\sqrt{2}\rangle_2$. Then one proceeds with the heterodyne measurement of this bimodal state which can be seen as a POVM measurement $\{M_0^{\rm het}, M_1^{\rm het}, M_2^{\rm het}, M_3^{\rm het}\}$ where:

$$M_0^{\rm het} = \int_0^\infty |x\rangle\langle x|_1 \,{\rm d}x \otimes \int_0^\infty |p\rangle\langle p|_2 \,{\rm d}p \tag{8.40}$$

$$M_1^{\rm het} = \int_{-\infty}^0 |x\rangle\langle x|_1 \,{\rm d}x \otimes \int_0^\infty |p\rangle\langle p|_2 \,{\rm d}p \tag{8.41}$$

$$M_2^{\rm het} = \int_{-\infty}^0 |x\rangle\langle x|_1 \,{\rm d}x \otimes \int_{-\infty}^0 |p\rangle\langle p|_2 \,{\rm d}p \tag{8.42}$$

$$M_3^{\rm het} = \int_0^\infty |x\rangle\langle x|_1 \,{\rm d}x \otimes \int_{-\infty}^0 |p\rangle\langle p|_2 \,{\rm d}p. \tag{8.43}$$

The success probability of the heterodyne measurement can immediately be inferred from the one of an homodyne measurement:

$$p_{\rm het} = \frac{1}{4}\left(1 + {\rm erf}\left(\frac{\alpha}{\sqrt{2}}\right)\right)^2. \tag{8.44}$$

This probability is again strictly smaller than the optimal bound but turns out to be almost optimal for very low values of the parameter α (see Figure 8.2). It is not known whether the heterodyne detection is optimal among Gaussian measurements, but this appears to be quite a reasonable conjecture.

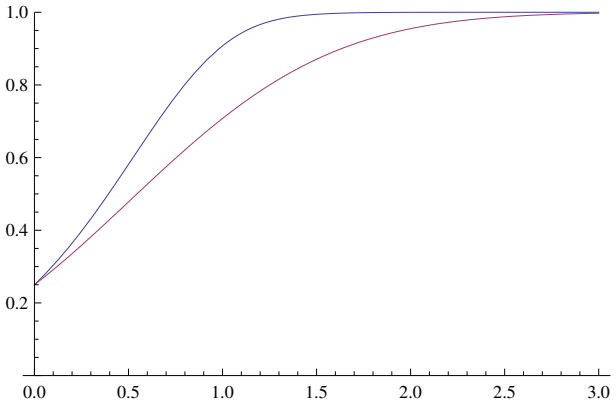

Figure 8.2: Probability of success of distinguishing $\{|e^{i\pi/4}\alpha\rangle, |e^{3i\pi/4}\alpha\rangle, |e^{5i\pi/4}\alpha\rangle, |e^{7i\pi/4}\alpha\rangle\}$ with an optimal measurement (upper curve), and an heterodyne detection (lower curve), as a function of α.

8.1.3 Mutual information, Holevo information

Here we consider another figure of merit of the different measurement schemes, that is, the mutual information between the source (generating either a mixture of $|\alpha\rangle$ and $|-\alpha\rangle$,

or of $|\alpha_0\rangle, |\alpha_1\rangle, |\alpha_2\rangle$ and $|\alpha_3\rangle$) and the output of the measurement. Yet another measure is the Holevo information which gives an upper bound (not tight since the different states do not have orthogonal supports) of this mutual information.

Case of two coherent states. Let us first compute the different mutual informations relative to an optimal measurement and to an homodyne detection. The protocol which consists in generating a random coherent state with probability 1/2 and measuring it, can be seen as a classical binary symmetric (BSC) channel. The mutual information we are interested in then corresponds to the classical capacity of the BSC channel, which is known to be $C_{\rm BSC} = 1 - h(p_{\rm succ})$ where h is the binary entropy function defined as $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$. Therefore, the mutual information corresponding to an optimal measurement $I_{\rm QM,2}$ and to an homodyne detection $I_{\rm hom}$ are given by:

$$I_{\rm QM,2} = 1 - h(p_{\rm QM,2}) \tag{8.45}$$
$$I_{\rm hom} = 1 - h(p_{\rm hom}). \tag{8.46}$$

The other quantity of interest, especially in the case of an application to quantum key distribution (QKD), is the Holevo information which is defined for an ensemble of states $\{\rho_i\}_{i=1,\cdots,n}$ with probabilities $\{p_i\}_{i=1,\cdots,n}$ as

$$\chi(\{\rho_i, p_i\}) = S(\sum_i p_i\rho_i) - \sum_i p_i S(\rho_i), \tag{8.47}$$

where $S(\rho) = -{\rm tr}\rho\log_2\rho$ is the von Neumann entropy of the state ρ. The Holevo

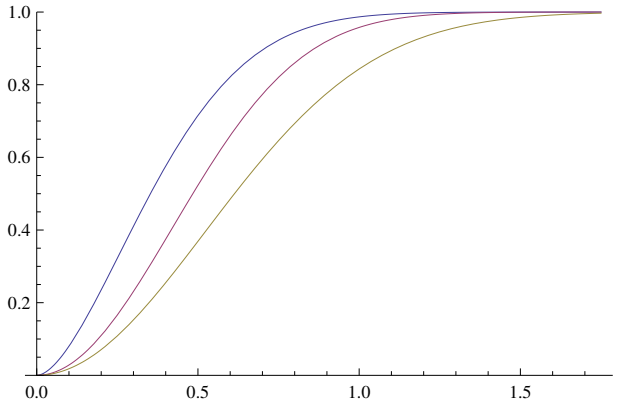

Figure 8.3: Case of 2 coherent states: mutual information between encoding and the measurement result, for an optimal measurement (middle curve), and an homodyne detection (lower curve), as a function of α. The upper curve represents the Holevo information of the state.

information is known to be an upper bound to the accessible information of a quantum state [109]. However, this bound is only tight when the states $\{\rho_i\}$ commute, which is

not the case of any coherent state. In our case, the Holevo information can be easily computed:

$$\chi_2 = S(\rho) - \frac{1}{2}S(|\alpha\rangle) - \frac{1}{2}S(|-\alpha\rangle) \tag{8.48}$$
$$= -\lambda_0 \log_2 \lambda_0 - \lambda_1 \log_2 \lambda_1 \tag{8.49}$$

since the von Neumann entropy of coherent states, which are pure states, is zero. It turns out that this bound is much larger that the mutual information computed above, as can be seen on Figure 8.3. In fact, in the case of two coherent states, the maximal accessible information is known under the name *Levitin bound* [94] which turns out to be equal to $I_{\mathrm{QM},2}$. Interestingly, in the context of quantum key distribution, the accessible information and the Holevo information relate respectively to individual and collective attacks.

Case of four coherent states. Here the situation is a little bit more complicated as different types of errors have to be taken into account. In particular, if the state $|\alpha_0\rangle$ has been generated, the measurement might indicate either state $|\alpha_1\rangle$ or $|\alpha_3\rangle$ with the same error probability p_1 or the state $|\alpha_2\rangle$ with error probability p_2. Here again, the mutual information we are interested in can be seen as the classical capacity of a classical communication channel with four inputs and transition probabilities defined as:

$$\begin{array}{lcll} |\alpha_k\rangle & \longrightarrow & |\alpha_k\rangle & \text{with probability } p_{\mathrm{succ}}, \\ |\alpha_k\rangle & \longrightarrow & |\alpha_{k-1}\rangle & \text{with probability } p_1, \\ |\alpha_k\rangle & \longrightarrow & |\alpha_{k+1}\rangle & \text{with probability } p_1, \\ |\alpha_k\rangle & \longrightarrow & |\alpha_{k+2}\rangle & \text{with probability } p_2. \end{array} \tag{8.50}$$

where all additions must be understood modulo 4.
The corresponding capacity reads:

$$C_4 = 2 + p_{\mathrm{succ}} \log_2 p_{\mathrm{succ}} + 2p_1 \log_2 p_1 + p_2 \log_2 p_2. \tag{8.51}$$

This capacity is achieved when the four input states are emitted with uniform probability, and is therefore equal to the mutual information we are looking for.

Optimal measurement. The probability of the first type of error is given by:

$$p_1 = \frac{1}{16}\sum_{k=0}^{3} |\langle \alpha_k | \omega_{k+1} \rangle|^2 \tag{8.52}$$
$$= \frac{1}{4}\left|\sqrt{\mu_0} + i\sqrt{\mu_1} - \sqrt{\mu_2} - i\sqrt{\mu_3}\right|^2. \tag{8.53}$$

The probability of the second type of error is likewise computed in the following way:

$$p_2 = \frac{1}{16}\sum_{k=0}^{3} |\langle \alpha_k | \omega_{k+2} \rangle|^2 \tag{8.54}$$
$$= \frac{1}{4}\left|\sqrt{\mu_0} - \sqrt{\mu_1} + \sqrt{\mu_2} - \sqrt{\mu_3}\right|^2. \tag{8.55}$$

Heterodyne detection. The first type of errors occurs when one of the homodyne detections is successful while the second leads to an error. Its probability is:

$$p_1^{\text{het}} = \frac{1}{4} - \frac{1}{4}\left(\text{erf}\left(\frac{\alpha}{\sqrt{2}}\right)\right)^2. \tag{8.56}$$

Finally, the probability of the second type of error is given by:

$$p_2^{\text{het}} = \frac{1}{4}\left(1 - \text{erf}\left(\frac{\alpha}{\sqrt{2}}\right)\right)^2. \tag{8.57}$$

Holevo information. The Holevo information has the same form as in the case of two coherent states, namely:

$$\chi_4 = S(\sigma) - \frac{1}{4}\sum_{k=0}^{3} S(|\alpha_k\rangle\langle\alpha_k|) \tag{8.58}$$

$$= -\sum_{k=0}^{3} \mu_k \log_2 \mu_k. \tag{8.59}$$

Discussion. The comparison between the different mutual information and the Holevo information can be found on Figure 8.4. As before, one should notice that the Holevo information is much larger that the other 2 quantities. In the case of four coherent states, the maximal accessible information is not known, but it seems natural to conjecture that it is equal to the quantity:

$$I_{\text{QM},4} = 2 + p_{\text{QM},4} \log_2 p_{\text{QM},4} + 2p_1 \log_2 p_1 + p_2 \log_2 p_2. \tag{8.60}$$

8.2 A no-go theorem for Gaussian quantum bit commitment

Cryptography is not at all limited to key distribution. Among other important primitives, one can cite *bit commitment* and *oblivious transfer*. Similarly to key distribution, both these tasks are impossible classically. But it turns out that they are also impossible in a quantum framework, in sharp contrast with key distribution. The fact that they are impossible in general, that is, if the players are only limited by quantum mechanics, does not mean that their study is not interesting. In this section, we consider quantum bit commitment with continuous variables. In particular, we prove a no go theorem for bit commitment where both parties are restricted to using Gaussian states and operations.

The results presented in this section where obtained in collaboration with Loïck Magnin, Frédéric Magniez and Nicolas Cerf. Loïck was the main architect of the proof. This work was presented in Ref. [102].

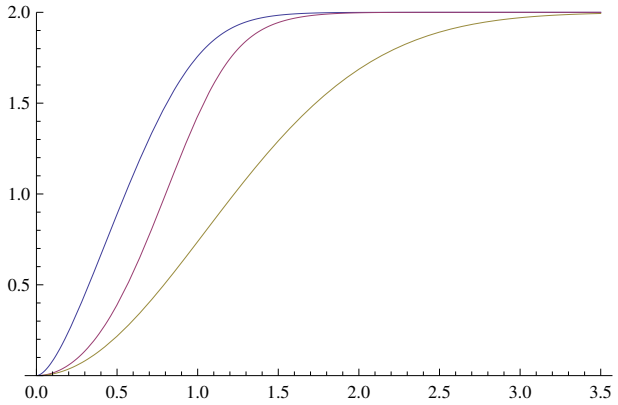

Figure 8.4: Case of 4 coherent states: mutual information between encoding and the measurement result, for an optimal measurement (middle curve), and an heterodyne detection (lower curve), as a function of α. The upper curve represents the Holevo information of the state.

8.2.1 Quantum bit commitment

Bit commitment is a cryptographic involving only two players, Alice and Bob, who distrust each other. The basic idea is that Alice should commit to a bit, either 0 or 1, and commit to it. To make the task more interesting, Bob should not be able to guess the value of the bit before Alice tells him, but Alice should not be able to change her mind once she committed to a certain bit. A more imaged (classical) description is the following: Alice writes down a bit on a piece of paper that she puts in a safe. She then hands the safe over to Bob. Obviously, with a good safe, Bob cannot learn the value of the bit at that point, and Alice cannot change her mind anymore. When Alice decides to reveal her bit, she just gives the key of the safe to Bob, who can open it and read the value of the committed bit.

Let us now give some terminology. Bit commitment is a two-step protocol:

- in the *committing phase*, Alice chooses a bit and informs Bob that she has made a commitment,
- in the *revealing phase* (also called *opening* phase), she reveals her choice to Bob.

The time interval between the two phases is sometimes referred to as *holding phase*: it is when Alice and Bob can both try to cheat.

Obviously, a good bit commitment primitive should be secure against either a dishonest Alice or a dishonest Bob. A protocol secure against Alice cheating is called *binding* as it prevents Alice to change her mind after the committing phase. A protocol secure against Bob cheating is called *concealing*, meaning that Bob cannot learn anything concerning the value of the bit before the revealing phase. This concept of bit commitment scheme was first formalized by Brassard, Chaum and Crépeau in 1988 [17].

In a similar way as key distribution is a primitive for secure communication between distant parties, bit commitment is a primitive for various cryptographic applications. For instance, bit commitment can be used for

- *coin flipping*: Alice and Bob flip a *fair* coin,
- *secure computation*: Alice and Bob have respective secret data x and y and they wish to compute the value of a function f for these data in such a way that neither the computation not the value of $f(x, y)$ can give Alice (resp. Bob) any information about y (resp. x) [161],
- *zero-knowledge proofs* are interactive protocols where one party wishes to prove to the other that a mathematical statement is true without revealing any other information except that the statement is true [56]. Roughly speaking, one wishes to show that he knows the mathematical proof of a theorem, without revealing the proof in question.

In the classical setting, a bit commitment protocol can never be unconditionally secure, that is perfectly binding and concealing at the same time [78]. One therefore needs to make extra assumptions on the hardness of certain tasks, and can only achieve *computational* security. Unfortunately, even with such restrictions, known bit commitment protocols are only either computationally binding or computationally concealing (see Ref. [35] and references therein for more details). A natural question is to ask whether there exist secure *quantum* bit commitment schemes. Remember that secure key distribution is impossible classically but allowed by the laws of quantum mechanics.

Actually, this question was asked a long time ago since it was indirectly addressed (but not solved) in the seminal paper of Bennett and Brassard that introduced the BB84 QKD protocol [10]. In this article, the authors proposed a quantum bit commitment QBC protocol (more precisely, a version adapted from coin tossing) but suggested a cheating attack for Alice where she would use an EPR pair. The basic idea is that the committing phase will consist for Alice to send one half of an EPR pair to Bob, while keeping the other half. The cheating strategy then simply amounts to performing the right operation on the second half of the pair. In 1993, Brassard, Crépeau, Jozsa and Langlois introduced a new QBC scheme [18] where the players are forced to perform measurements and communicate classically during the protocol in order to avoid the loophole of Bennett and Brassard's scheme. This scheme was believed to be secure until 1996 when Mayers [103] and independently Lo and Chau [96] showed that all previous QBC schemes were vulnerable to a generalized EPR attack and proved the impossibility of QBC in general: this is the celebrated *no-go theorem for quantum bit commitment*.

However, the story does not end here. The proofs for the no-go theorem are based on a reduction of any QBC protocol to a purified protocol, and it was not clear at that time that such a reduction encompassed all QBC protocols. For this reason, the no-go theorem was not universally accepted (see for instance Ref. [162] and subsequent works by the same author). More recently, the question was arguably put to rest by d'Ariano and collaborators in Refs [35] and [29].

Again, the fact that the no-go theorem of QBC is now widely accepted by the scientific community is still not the end of the story. Indeed, one should stress that the no-go theorem only applies to *unconditionally* secure protocols, that is, protocols where Alice and Bob are only limited by the laws of quantum mechanics. This does not mean that there are no other (more restricted) contexts where QBC could be interesting. A classical analogy would be to consider protocols computationally secure in the hypothesis where one could establish results about the hardness of certain computations (remember that such results are only conjectured today). For instance, in a reasonable scenario, Alice and Bob only have access to limited quantum memories, this is the so-called *bounded storage model* (which is a quantum version of the model introduced in Ref. [8]). Quantum bit commitment can be made secure within this model[34]: the idea is that, due to their finite-size quantum memories, Alice and Bob have to measure their quantum states at some point, hence preventing them from applying unitary cheating strategies on their whole quantum system. Another way around the no-go theorem is to use the constraints imposed by special relativity to achieve unconditional security [77]. However, this last proposal is far from being practical as Alice and Bob should be space-like separated and need to synchronize their communication quite precisely!

The conclusion of this preamble is two-fold. First, there exists a general no-go theorem for quantum bit commitment. Second, it is possible to put reasonable constraints on Alice and Bob capabilities to allow them to perform secure quantum bit commitment. We now introduce such reasonable constraints, namely that Alice and Bob are restricted to use Gaussian states and Gaussian operations only. Then we prove that in this framework, secure *Gaussian* quantum bit commitment is impossible.

8.2.2 Bit commitment with Gaussian states and Gaussian operations

A reasonable restriction for continuous variables. In this section, we introduce QBC schemes with continuous variables, and study more particularly the restriction to Gaussian states and Gaussian operations. Indeed, as is the case for QKD, most protocols were initially considered in finite-dimensional Hilbert spaces. In this chapter, there is no need to argue one more time that continuous variables can represent a valid alternative to qubits (or low dimensional systems) to encode quantum information.

There are various reasons to justify the restriction to Gaussian states and Gaussian operations we impose to Alice and Bob. First, the obvious reason is that one needs to impose a restriction, otherwise the usual no-go theorem applies and there is nothing more to say. The question then is to find a reasonable restriction. The Gaussian restriction we consider is reasonable from two perspectives. First, it has the great advantage of considerably simplifying the theoretical analysis of the protocol: this is because Gaussian states and Gaussian operations can entirely be described by their first two moments in phase space. In fact, the analysis boils down to considering covariance matrices, which have the nice property of being finite-dimensional. Therefore, the Gaussian restriction is already convincingly justified as it allows for a tractable theoretical description of the problem. A second point of view is the experimental perspective. We saw in Chapter 2 that Gaussian operations exactly correspond to what is easily performed in a lab. They

can indeed be implemented with linear optical elements (phase shifts, beam splitters and squeezers) together with homodyne detection [52]. The fact that Gaussian operations are easily implementable experimentally is crucial for QBC: indeed, the general no-go theorem tells us that there always exists a cheating strategy for Alice or Bob, but in practice, one wants to know whether such a strategy can be implemented or not. From this perspective, Gaussian cheating strategies are relatively "easy" to implement. In the following, we will prove that if Alice and Bob are both restricted to Gaussian states and Gaussian operations, then there always exists a Gaussian cheating strategy.

Notations and main theorem. Before proving this no-go theorem for Gaussian QBC, we need to recall some definitions and notations. To do this, we detail the generic description of any (reduced) QBC protocol. Alice starts by choosing a bit b which she encodes into a bipartite pure state $|\psi_b\rangle$. She then sends one half of her state, $\rho_b = \mathrm{tr}_A|\psi_b\rangle\langle\psi_b|$ to Bob and keeps the second half. The QBC protocol is said ϵ-concealing if $D(\rho_0, \rho_1) \leq \epsilon$ (where D is the trace distance defined in Chapter 1). Because of the Helström bound, this means that Bob cannot learn the value of b, except with probability at most ϵ. The second part of the protocol, the revealing phase, consists for Alice to send the second half of $|\phi_b\rangle$ to Bob. We now define the notion of δ-cheating strategy (for Alice[3]): Alice sends a state $\rho^\sharp$ to Bob in the committing phase and decides later whether her bit should be 0 or 1, corresponding respectively to final states $|\psi_0^\sharp\rangle$ or $|\psi_1^\sharp\rangle$. Such a strategy is said to be a *δ-cheating strategy* if Bob cannot distinguish it from a honest strategy with a probability greater that δ. This implies the following conditions:

$$D(\rho^\sharp, \rho_b) \leq \delta \quad \text{and} \quad D(|\psi_b^\sharp\rangle, |\psi_b\rangle) \leq \delta \quad \text{for} \quad b \in \{0, 1\}. \tag{8.61}$$

As it is sufficient to exhibit one cheating strategy to prove a no-go theorem, here, we only need to consider the slightly simpler scenario where $\rho^\sharp = \rho_0$ and $|\psi_0^\sharp\rangle = |\psi_0\rangle$. Therefore, in the case we study, Alice always commits to 0 but can later decide to switch to 1. This will allow us to prove the following no-go theorem for Gaussian QBC:

Theorem 8.2. *Given any ϵ-concealing Gaussian quantum bit commitment protocol, there exists a Gaussian $\sqrt{2\epsilon}$-cheating strategy for Alice.*

Note that removing the word "Gaussian" from this statement gives the usual no-go theorem for QBC [35].

Proof of the main theorem. For QBC in finite dimension, the core of the proof of the no-go theorem is Uhlmann's theorem (see Theorem 1.7 in Chapter 1). For any two states ρ_0 and ρ_1, this theorem guarantees the existence of two respective purifications $|\psi_0\rangle$ and $|\psi_1\rangle$ such that $F(|\psi_0\rangle, |\psi_1\rangle) = F(\rho_0, \rho_1)$. Because Uhlmann's theorem is independent of the dimension of the Hilbert space, it also works for continuous-variable quantum systems and the general no-go theorem remains valid for continuous-variable QBC. However, it

[3] in fact, it is sufficient to establish the existence of a cheating strategy for Alice to prove a no-go theorem for QBC.

does not give anymore explicitly the purifications $|\psi_0\rangle$ and $|\psi_1\rangle$ in infinite dimension[4]. In particular, one does not know any explicit cheating strategy, in contrast with the finite-dimensional case. Here, we cannot use the usual Uhlmann's theorem as we require the purifications to be Gaussian and the theorem does not say anything about Gaussianity. Moreover, we could not yet prove a conjectured Uhlmann's theorem for Gaussian states which is that if ρ_0 and ρ_1 are Gaussian states, then there exist *Gaussian* purifications $|\psi_0\rangle$ and $|\psi_1\rangle$ such that $F(|\psi_0\rangle, |\psi_1\rangle) = F(\rho_0, \rho_1)$ (where F is the fidelity between two states). In the absence of such a result, we will need to find explicit Gaussian purifications that almost reach Uhlmann's bound. The existence of such purifications is the object of the following lemma:

Lemma 8.2. *Given two (n-mode) states ρ_0 and ρ_1, there exist (2n-mode) purifications $|\hat{\psi}_0\rangle$ of ρ_0 and $|\hat{\psi}_1\rangle$ of ρ_1 such that*

$$D(|\hat{\psi}_0\rangle, |\hat{\psi}_1\rangle) \leq \sqrt{2D(\rho_0, \rho_1)}. \tag{8.62}$$

Moreover, if ρ_0 and ρ_1 are Gaussian states, so are their purifications $|\hat{\psi}_0\rangle$ and $|\hat{\psi}_1\rangle$.

In order to prove this lemma, we introduce the concept of *intrinsic purification* [102], which we explain below. First, remember that an n-mode Gaussian state ρ is characterized by its Gaussian Wigner function (see Chapter 2):

$$W_\rho(r) = \frac{1}{\pi^n \sqrt{\det\gamma}} \exp\left\{-(r-\mu)^T \gamma^{-1} (r-\mu)\right\}, \tag{8.63}$$

where $\mu \in \mathbb{R}^{2n}$ is the displacement vector and $\gamma \in \mathbb{R}^{2n} \times \mathbb{R}^{2n}$ is the covariance matrix of ρ.

Where Gaussian states and Gaussian operations are very nice, is that everything can be described easily in phase space. In particular, a Gaussian map $\mathcal{E}$ is entirely characterized by a displacement vector d and a symplectic matrix S such that for all states ρ, one has [7]

$$W_{\mathcal{E}(\rho)}(r) = W_\rho(S^{-1}r - d). \tag{8.64}$$

The Williamson decomposition theorem states that for any covariance matrix γ, there exists a symplectic transformation S such that

$$S\gamma S^T = \bigoplus_{k=1}^{n} \nu_k \mathbb{1}_2, \tag{8.65}$$

where $\{\nu_1, \cdots, \nu_n\}$ is the symplectic spectrum of γ. For a Gaussian state ρ, this means that there exists a Gaussian operation V, a Williamson unitary, such that

$$V\rho V^\dagger = \sum_{\mathbf{i}} \left(\prod_{k=1}^{n} (1-x_k) x_k^{i_k} \right) |\mathbf{i}\rangle\langle\mathbf{i}|, \tag{8.66}$$

[4]more precisely, one would need to prove the existence of a polar decomposition for non-invertible bounded linear operators.

where $x_k = (\nu_k - 1)/(\nu_k + 1)$ and $|\mathbf{i}\rangle = |i_1\rangle \cdots |i_n\rangle$ is the Fock basis of the n-mode Hilbert space that describes ρ. This means that any Gaussian state can be mapped to a tensor product of thermal states via a Gaussian operation.

We now introduce the concept of *intrinsic purification*. Let ρ be an n-mode state and U be a diagonalization of ρ in the Fock basis, that is a unitary operator such that

$$\langle \mathbf{i}|U^\dagger \rho U|\mathbf{j}\rangle = p_i \delta_{ij}, \tag{8.67}$$

where δ_{ij} is the Kronecker delta. A purification $|\hat{\psi}\rangle$ of ρ will be said *intrinsic* if it can be written as

$$|\hat{\psi}\rangle = (U^* \otimes U) \sum_{\mathbf{i}} \sqrt{p_i}\, |\mathbf{i}\rangle|\mathbf{i}\rangle, \tag{8.68}$$

where A^* (resp. A^T) denotes the complex conjugate (resp. the transpose) of any linear operator A relatively to the Fock basis, that is

$$\langle \mathbf{i}|A^*|\mathbf{j}\rangle = \langle \mathbf{i}|A|\mathbf{j}\rangle^* \quad \text{and} \quad \langle \mathbf{i}|A^T|\mathbf{j}\rangle = \langle \mathbf{j}|A|\mathbf{i}\rangle. \tag{8.69}$$

For a Gaussian state, one simply obtains a Gaussian intrinsic purification by choosing $U = V$. To see that, it is sufficient to show that the purification is indeed Gaussian. First, the state $\sum_{\mathbf{i}} \sqrt{p_{\mathbf{i}}}|\mathbf{i}\rangle|\mathbf{i}\rangle$ is Gaussian in this case since it is the tensor product of two-mode squeezed states. Therefore, all is left to do is to show that $U \otimes U^*$ is Gaussian. Since U is Gaussian, one only needs to prove that its complex conjugate U^* is also Gaussian. Let us note d and S the displacement vector and the symplectic matrix associated with the Gaussian map U. It can be shown [102] that for any state state σ,

$$W_{U^*\sigma U^{*\dagger}}(r) = W_\sigma(\Sigma_z^n S^{-1} \Sigma_z^n r - \Sigma_z^n d), \tag{8.70}$$

where

$$\Sigma_z^n = \bigoplus_{k=1}^{n} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{8.71}$$

This shows that U^* is a Gaussian map characterized by the displacement vector $\Sigma_z^n d$ and the symplectic matrix $\Sigma_z^n S^{-1} \Sigma_z^n$.

Proof of Lemma 8.2. We take for $|\hat{\psi}_0\rangle$ and $|\hat{\psi}_1\rangle$ the intrinsic purifications of ρ_0 and ρ_1. A straightforward calculation shows that

$$\mathrm{tr}\sqrt{\rho_0}\sqrt{\rho_1} = \sqrt{F(|\hat{\psi}_0\rangle, |\hat{\psi}_1\rangle)}. \tag{8.72}$$

Using the Battacharyya bound (second part of Eq. 1.64), one gets

$$1 - D(\rho_0, \rho_1) \leq \sqrt{F(|\hat{\psi}_0\rangle, |\hat{\psi}_1\rangle)}. \tag{8.73}$$

Then, the relation between fidelity and trace distance (first part of Eq. 1.64) gives

$$D(|\hat{\psi}_0\rangle, |\hat{\psi}_1\rangle) \leq \sqrt{2D(\rho_0, \rho_1) - D(\rho_0, \rho_1)^2}, \tag{8.74}$$

which concludes the proof of Lemma 8.2. □

In order to prove our no-go theorem for Gaussian QBC, we need a second lemma:

Lemma 8.3. *Let $|\psi_0\rangle$ and $|\psi_1\rangle$ be two $2n$-mode Gaussian states such that $tr_A|\psi_0\rangle\langle\psi_0| = tr_A|\psi_1\rangle\langle\psi_1|$, there exists a Gaussian unitary operator U acting on n modes such that $(U \otimes \mathbb{1})|\psi_0\rangle = |\psi_1\rangle$, where $\mathbb{1}$ is the identity on n modes.*

Note that without the Gaussian property, the lemma is a consequence of the Schmidt decomposition of $|\psi_0\rangle$ and $|\psi_1\rangle$. In the Gaussian case, one needs to work in phase space, and this lemma results from the normal mode decomposition [15]. The complete proof of Lemma 8.3 can be found in [102].

With Lemmas 8.2 and 8.3, we can finally prove the no-go theorem for Gaussian QBC.

Proof of Theorem 8.2. We consider an ϵ-concealing protocol where Alice prepare the state $|\psi_0\rangle$ and sends $\rho_0 = \mathrm{tr}_A|\psi_0\rangle\langle\psi_0|$ to Bob. If Alice wants to reveal the bit 0, she just sends the second half of $|\psi_0\rangle$ to Bob. If she wants to cheat and to switch her bit to 1, she applies a local Gaussian unitary operation to her half of $|\psi_0\rangle$ which maps the pure state to $|\psi_1^\sharp\rangle$ and she sends her half of the state to Bob. In order to prove the existence of a $\sqrt{2\epsilon}$-cheating strategy for Alice, we only need to show that there exists such a state $|\psi_1^\sharp\rangle$ which is $\sqrt{2\epsilon}$-close to $|\psi_1\rangle$.
According to Lemma 8.2, there exist purifications $|\hat{\psi}_0\rangle$ of ρ_0 and $|\hat{\psi}_1\rangle$ of ρ_1 such that

$$D(|\hat{\psi}_0\rangle, |\hat{\psi}_1\rangle) \leq \sqrt{2D(\rho_0, \rho_1)}. \tag{8.75}$$

Since $|\psi_b\rangle$ and $|\hat{\psi}_b\rangle$ are two Gaussian purifications of the same state ρ_b with $b \in \{0, 1\}$, Lemma 8.3 ensures the existence of two local Gaussian unitaries U_0 and U_1 such that

$$(U_0 \otimes \mathbb{1})|\psi_0\rangle = |\hat{\psi}_0\rangle \quad \text{and} \quad (U_1 \otimes \mathbb{1})|\psi_1\rangle = |\hat{\psi}_1\rangle \tag{8.76}$$

We define $|\psi_1^\sharp\rangle$ as

$$|\psi_1^\sharp\rangle = (U_1^{-1}U_0 \otimes \mathbb{1})|\psi_0\rangle = (U_1^{-1} \otimes \mathbb{1})|\hat{\psi}_0\rangle. \tag{8.77}$$

Since the trace distance is invariant under unitaries, one has:

$$\begin{aligned} D(|\psi_1^\sharp\rangle, |\psi_1\rangle) &= D(|\hat{\psi}_0\rangle, |\hat{\psi}_1\rangle) && (8.78)\\ &\leq \sqrt{2D(\rho_0, \rho_1)} && (8.79)\\ &\leq \sqrt{2\epsilon}, && (8.80) \end{aligned}$$

for ϵ-concealing protocols, which concludes the proof of the no-go theorem for Gaussian quantum bit commitment. □

8.3 Deriving Quantum Mechanics from information theory axioms

As we already mentioned in the introduction, although the predictions of quantum mechanics have not been falsified yet[5], it still lacks a derivation from basic postulates.

[5]despite an important experimental effort during the last hundred years

Whether this situation is definitive or not is impossible to say right now, but it certainly did not stop people from trying to derive quantum mechanics from a few operational principles. Such a situation applies for both special relativity (the physical laws, as well as the velocity of light, are the same for all inertial frames) and general relativity (equivalence between a gravitational field and an accelerated frame in absence of a gravitational field). Yet, quantum mechanics is currently described by mathematical axioms that are not derived from fundamental physical postulates.

With the rapid development of quantum information theory in the last two decades, people started to wonder if quantum mechanics was not in the end only concerned with information, and consequently if it could not be derived from information theory axioms. Such a possibility became even more interesting with the development of quantum cryptography, and more precisely with the discovery of differences between the classical world and quantum mechanics concerning cryptography. Among notable results, one should cite the fact that *key distribution* is allowed in a quantum world but not in a classical world whereas *bit commitment* is forbidden in both situations. Christopher Fuchs and Gilles Brassard suggested that quantum mechanics could be derived from these two axioms [16]:

1. possibility of perfect confidentiality,
2. impossibility of bit commitment.

However, it was soon proven that these two axioms were not sufficient to rederive quantum mechanics as toy models could be invented such that they satisfy these two properties while being incompatible with quantum mechanics [148] (although this counter-example might suffer some physical pathologies [65]). At the same time, Bub, Clifton and Halvorson suggested to replace the possibility of key distribution with two more fundamental postulates [32], namely,

- the *no-signaling property*, that is, that no manipulations occurring at some point in space can have an instantaneously (faster than what is authorized by special relativity) observable effect at some remote location,
- the *no-cloning theorem*.

Quite remarkably, from the three no-go theorems that are no-signaling, no-cloning and no bit commitment, Bub, Clifton and Halvorson were able[6] to rederive some genuine features of quantum mechanics: interferences, non-commutativity of measurements and the existence of space-like separated entanglement.

However, despite this success, we argue here that their three axioms cannot be sufficient to completely rederive quantum mechanics. The reason for this is that we have exhibited a theory compatible with the three information theoretic axioms of Bub, Clifton

[6]to be more precise, they also had to assume that the laws of physics can be described in the mathematical framework of $C^\star$-algebras, that is complex algebras of linear operators on a complex Hilbert space which are closed for the norm topology of operators as well as under the operation of taking adjoints of operators.

and Halvorson that is strictly different from quantum mechanics. This theory is the theory of Gaussian states and Gaussian operations, or more simply *Gaussian quantum theory*.

It is indeed easy to see that Gaussian quantum theory satisfies all three axioms of Bub, Clifton and Halvorson:

- being contained within quantum theory, it obviously respects the no-signaling property,
- the argument concerning the no-cloning property is a little more elaborate since classical mechanics is superseded by quantum mechanics but does not satisfy the no-cloning theorem. If fact, the no-cloning theorem is valid within Gaussian information theory since there exist non orthogonal Gaussian states. Actually, there cannot exist orthogonal Gaussian states at all since their Wigner functions, being Gaussian distributions, necessary overlap.
- the impossibility of Gaussian quantum bit commitment was just established in the previous section.

To complete our argument, we also need to establish that Gaussian quantum theory is strictly different from quantum theory. This can be seen, for instance, by noting that Wigner functions never take negative values for Gaussian state. A particular consequence of this fact is that there always exists a local hidden-variable model that describes a Gaussian quantum system. Hence, one cannot violate any Bell inequality with Gaussian states and Gaussian operations[7] only. Since Bell inequalities violations are theoretically allowed by quantum mechanics (and even experimentally demonstrated), Gaussian quantum theory forms a strict subset of quantum theory.

It must be pointed out that a previous counter-example, that is, satisfying the three axioms suggested by Bub, Clifton and Halvorson but strictly different from Quantum Mechanics, was exhibited by Spekkens [149]. However, his counter-example is really an *ad hoc* toy model, and we might argue that Gaussian states and Gaussian operations give a much more physically motivated counter-example. The reason why the argument of Bub, Clifton and Halvorson fails in both cases is that they cannot be described with C^*-algebras.

Interestingly, the C^*-algebra assumption which seemed rather benign to begin with turns out to be in fact quite strong. Therefore, it would be nice to formulate axioms where such a mathematical structure was not imposed *a priori*. Answering such a question is clearly out of the scope of this thesis.

[7] meaning, for example, homodyne or heterodyne detection

Part IV

Conclusion and perspectives

Conclusion and perspectives

In this thesis, we studied continuous-variable quantum key distribution from a theoretical point of view. However, "theoretical" here does not mean disconnected from any experimental consideration. Quite the opposite actually! Indeed, the first half of our work was directly concerned with improving the current continuous-variable QKD protocols in order to make them more robust to losses, and consequently increase their range. This lead us to introduce new protocols which clearly outperform the historical protocol involving coherent states sent with a Gaussian modulation. A striking feature of these new protocols is that they look suboptimal on the paper, but turn out to be more efficient in practice. In the second half of our work, we investigated the security of continuous-variable QKD. In particular, we suggested approaches to prove its security against general attacks. The goal here is to obtain bounds as tight as possible so that they can be used, even when taking into account finite size effects.

We now discuss some perspectives concerning these two issues:

- What are the best continuous-variable QKD protocols, and do they represent a viable alternative to discrete-variable protocols?

- What are the remaining open questions concerning the security of continuous-variable protocols?

Better continuous-variable QKD protocols?

The history of continuous-variable quantum key distribution is interesting. The first protocols that were suggested involved squeezed states and were consequently quite hard to implement. Later, it was proven that coherent states were indeed sufficient to guarantee security. This was a great step as coherent states are much easier to produce than

squeezed states. At that moment, it was possible to implement continuous-variable QKD with only standard telecom components.

However, the story was not quite finished yet as a Gaussian modulation was still required in order for the security proofs (against collective attacks) to hold. The next improvement was to extend the security proofs to a discrete modulation. Such a modulation combines two advantages. First, it allows for a simpler experimental scheme as only one modulator is required instead of two for a truly Gaussian modulation. Second, a quaternary modulation allows for much more efficient reconciliation algorithms, which results in an drastically increased range for the key distribution.

Can one do even better? There are two possible paths to improve a QKD protocol. One can simplify its experimental setup in order to make it as practical as possible. This is clearly what one might want to achieve in order to eventually sell QKD. The other consists in improving the performances of the protocol, especially its range. Concerning the experimental setup, one can hardly hope for a much simpler scheme than the four-state protocol presented in Chapter 5. Indeed, only one modulator is required on Alice's side, and a (simple) homodyne detection is performed on Bob's side. There does not seem to be much room for improvement. On the performance aspect, one might wonder whether the four-state protocol can be improved. For instance, one could add quantum memories to the scheme in order to significantly increase its range, but this would represent a real technological step. Another (more modest) possibility is to change the detection scheme and to allow Bob to perform an heterodyne measurement instead of an homodyne detection. This would actually open the door for new modulation schemes that would perform as well as the quaternary modulation in terms of reconciliation efficiency, but would lead to an improved secret key rate (because one could derive tighter bounds on the eavesdropper information). Such a new protocol based on an heterodyne detection, and a continuous modulation is presented in Appendix B. This protocol is shown to outperform the four-state protocol (at the price of an heterodyne detection). Because this is less practical than an homodyne detection, it might not be relevant for an eventual commercial application. Time will tell.

Concerning the historical battle between discrete variables and continuous variables, it is difficult to make a definitive opinion already. However, whereas 5 years ago, discrete variables clearly outperformed continuous variables, it is not the case anymore: the performances and the security proofs are now similar, only the experimental implementations differ significantly for the detection stage. From the experimental point of view, continuous variables have the great advantage of only requiring off-the-shelf telecom equipment compared to discrete variables which need specific single photon detectors. All considered, continuous variables certainly appear as a credible alternative to discrete variables.

Remaining issues concerning the security of continuous-variable QKD

In Chapters 6 and 7 of this thesis, we investigated some questions linked to the security of continuous-variable QKD protocols. Three years ago, their security was only established against collective attacks in the asymptotic regime. Since then, Renner and Cirac have proved that the security bounds still held against general attacks, in the asymptotic limit.

In Chapter 6, we suggested a possible approach to improve Renner and Cirac's result, in particular, in the context of finite size effects. This approach has not been successful yet, but we conjecture that collective attacks should be optimal, even in the non-asymptotic regime. A natural approach to tackle this problem consists in exploiting the symmetries in phase space that are specific to continuous-variable QKD protocols. Given the power of symmetries in physics in general, and QKD in particular, it is quite clear that such an approach should be fruitful as it has already been in the past . A symmetry argument is indeed used to reduce the security against general attacks to the security against collective attacks (permutation invariance). An other symmetry argument is used to prove that collective attacks are optimal against BB84 (invariance under bit-flips and phase-flips). The remaining question is what the symmetries in phase space can tell about the security of continuous-variable QKD.

In Chapter 7, we investigated finite-size effects for continuous-variable QKD. An intriguing question on that matter is the status of the dimension in security proofs. Indeed, many bounds referring to discrete-variable QKD protocols involve the dimension of the Hilbert space that describes the protocol. Such bounds are not applicable for continuous-variable protocols as the Hilbert space of interest become infinite dimensional. At the same time, it is clear that this infinite dimension is not relevant for a given protocol when only a few photons are exchanged between Alice and Bob. One then expects that a notion of *effective dimension* should replace the usual dimension in the various security proofs. How to define such an effective dimension? Can it simply be related to the energy of the quantum states considered for instance, or does one need to consider more complicated quantities? This is still an open question.

Finally, I would like to recall that the problem of the side-channels was not at all addressed in this thesis. The reason for this choice is that there is not yet any satisfying theoretical framework to study them. This, however, is not a question that one can easily discard: side-channels are indeed present in any physical implementation, and certainly need to be included in the security proofs before claiming unconditional security. At the time of writing, two approaches are suggested to take care of the side-channels. The first solution, not very exciting from a theoretical point of view, but in the end probably unavoidable, consists in painstakingly listing as exhaustively as possible, all known side-channels and finding a practical solution for every one of them. Device-independent QKD certainly appears as a much more exciting alternative. However, because it involves a loophole-free Bell test, it is not at all practical. A fascinating question is to determine whether their exists a middle ground between these two extreme solutions.

APPENDIX $\mathcal{A}$

Examples of families $\mathcal{A}_2$, $\mathcal{A}_4$ and $\mathcal{A}_8$

We give here examples of families $\mathcal{A}_2$, $\mathcal{A}_4$ and $\mathcal{A}_8$ which are used in the reconciliation procedure for correlated Gaussian variables presented in Chapter 4. These families respectively correspond to matrix representations of the complex numbers, the quaternions and the octonions in dimension 2, 4 or 8.

Notations

Let us introduce the following 4 2×2 matrices:
$K_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, K_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, K_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $K_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and the tensor product $K_{i_1,..,i_l} = K_{i_1} \otimes .. \otimes K_{i_l}$.

Examples

Family $\mathcal{A}_2$: $\{K_0, K_2\}$

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Family $\mathcal{A}_4$: $\{K_{00}, K_{32}, K_{20}, K_{12}\}$

$$A_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, A_2 = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix},$$

$$A_3 = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, A_4 = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Family $\mathcal{A}_8$: $\{K_{000}, K_{332}, K_{320}, K_{312}, K_{200}, K_{102}, K_{123}, K_{121}\}$

$$A_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

$$A_2 = \begin{pmatrix} 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix},$$

$$A_3 = \begin{pmatrix} 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \end{pmatrix},$$

$$A_4 = \begin{pmatrix} 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \end{pmatrix},$$

$$A_5 = \begin{pmatrix} 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$A_6 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$A_7 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$A_8 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

APPENDIX *B*

Long distance CV QKD with large modulation variance

B.1 Yet another continuous-variable QKD protocol

Here, we introduce a new continuous-variable QKD protocol specifically designed to allow for larger modulations variances than the two- and four-state protocols presented in Chapter 5. This protocol displays improved performances compared to all previous protocols, at the price of requiring an heterodyne detection instead of an homodyne detection.

One might wonder whether a new protocol is needed since the four-state protocol already displays nice performances over long distances. However, as was argued in Chapter 7, finite-size effects considerably worsen the behaviour of the protocol compared to the asymptotic scenario. Actually, even without taking into account all finite-size effects, in an experimental implementation, one needs to perform a reliable parameter estimation in order to compute a secret key rate. This parameter estimation, unfortunately, turns out to be quite challenging if the signal-to-noise ratio (SNR) is very low. More generally, from an experimental perspective, when possible, it is more convenient to work with

reasonably large SNR. As a rough estimate, the SNR is approximately equal to TV_A for small transmissions, where T is the channel transmission and V_A is Alice's modulation variance expressed in shot noise units[1]. Since there is nothing that can be done to increase T for a given distance (except developing better optical fibers!), the only way to work at higher SNR is to allow for a larger modulation variance. A specificity of the four-state protocol, however, is to only work with low modulation variances: this is a consequence of the security proof which uses the extremality of Gaussian states. Indeed, the entanglement-based version of the four-state protocol is actually very close to the entanglement-based version of the CV protocol with a Gaussian modulation, but only for small variances[2]. A typical modulation variance for the four-state protocol is around 0.5 units of shot noise. While this is perfectly alright from a theoretical point of view, the experimental implementation is rather tricky as soon as the distance considered is larger than a few tens kilometers. Hence, it would be nice to have a protocol allowing for larger modulation variances. We now introduce such a protocol.

As we already discussed at length, one critical step in a CV QKD protocol is the reconciliation phase: the reconciliation efficiency must be large enough at low SNR, otherwise the range of the protocol gets drastically limited. In this manuscript, we studied two different modulation schemes:

- a Gaussian modulation which allows for tight security bounds, but unfortunately suffers of inefficient reconciliation algorithms at low SNR,
- discrete modulations (with either two or four elements) for which efficient reconciliation algorithms exist, but which work only for low modulation variances.

Let us say a few words concerning the reconciliation procedure. A necessary condition in order to achieve long distances is to be able to have an efficient reconciliation at low SNR. The main difficulty here lies in the fact that we need a reverse reconciliation. Indeed, if we only considered a direct reconciliation, we could take advantage of the arsenal of solutions typically used in digital communication problems and choose an adapted quadrature amplitude modulation in order to get a good reconciliation efficiency for various values of the SNR. This, however, seems to be incompatible with a reverse reconciliation as the side information sent by Bob must help Alice without giving Eve any information. The only schemes where side information seems to have these properties are the Gaussian modulation where side information describes rotations in $\mathbb{R}^8$ (see Chapter 4) and the binary and quaternary modulations where side information consists in the absolute value of Bob's measurement result.

[1]To be more precise, in the case of an homodyne detection, one has

$$\mathrm{SNR} = \frac{TV_A}{1 + T\xi}, \tag{B.1}$$

where ξ is the excess noise. This relation can indeed be well approximated with $\mathrm{SNR} \approx TV_A$ when the excess noise is on the order of a few percents.

[2]The situation is even worse for the two-state protocol where the approximation holds only for even lower variances.

In Chapter 4, we considered a Gaussian modulation, and the reconciliation scheme was based on the algebraic properties of the octonions in $\mathbb{R}^8$. This reconciliation scheme was not optimal as successive vectors in $\mathbb{R}^8$, whose coordinates were eight successive measurement results for Bob, did not have a constant norm. More precisely, the norm of Alice's corresponding vector was following a χ distribution with 8 degrees of freedom. If those vectors had had a constant norm, the reverse reconciliation problem could have been reduced to a channel coding problem for a bi-AWGN channel, hence allowing for an efficient reconciliation procedure, even at arbitrary low SNR.

The protocol we introduce solves the previous problem in the following way. Alice sends $4n$ coherent states to Bob such that the coordinates of all quadruples

$$\{|\alpha_{4k}\rangle, |\alpha_{4k+1}\rangle, |\alpha_{4k+2}\rangle, |\alpha_{4k+3}\rangle\}_{k=1,\cdots,n}$$

are drawn with the uniform probability on the seven-dimensional sphere of radius 2α in phase space (where α is a positive number characterizing the modulation variance):

$$|\alpha_{4k}|^2 + |\alpha_{4k+1}|^2 + |\alpha_{4k+2}|^2 + |\alpha_{4k+3}|^2 = 4\alpha^2. \tag{B.2}$$

Then Bob proceeds with an *heterodyne measurement*. Here, it is crucial that both quadratures are measured in order to use the property of Eq. B.2. Then, the reconciliation procedure is a mix between the reconciliation using the octonions presented in Chapter 4 and the one described in Chapter 5 using the concatenation of good error correcting codes with a repetition code in order to be able to work at very low SNR. It goes at follows. Bob first puts together his n 8-dimensional real vectors and choose randomly n 8-bit strings. He then computes the n rotations in $\mathbb{R}^8$ as described in Chapter 4 and sends them to Alice with the authenticated classical channel. He also sends the norm of each of his n vectors. Alice applies the same n rotations to her data. At this point, Bob computes the syndrome of his $8n$-bit string for a code C he and Alice agreed on beforehand and sends this syndrome to Alice. Finally, Alice simply decodes in the correct coset code of C. The efficiency of this procedure is the same as the one of the reconciliation of the four state protocol.

Why working with 8 dimensions? The key in order to be able to perform an efficient reconciliation is that all Alice's data corresponding to Bob's measurements should have the same amplitude: this allows us to map the reconciliation problem to a channel coding problem for a BI-AWGN channel, which we know how to solve at arbitrarily low SNR. If Bob is restricted to homodyne detection, then both quadratures should have the same amplitude for Alice's state, restricting her to send coherent states among the sets $\mathcal{S}_2$ or $\mathcal{S}_4$ defined in Chapter 5. If Bob performs an heterodyne measurement instead, it gives Alice more freedom for the coherent states she can send. In particular, she can now send any coherent state $|\alpha\rangle$ such that $|\alpha|$ is constant. If now, Bob can perform rotations in $\mathbb{R}^n$ and inform Alice of such a rotation without leaking any relevant information to a potential eavesdropper, this gives even more freedom for Alice's modulation. It was established in Chapter 4 that the only allowed values for n were $n \in \{1, 2, 4, 8\}$ if we

require that Bob should be able to efficiently compute the rotation in question[3]. The case $n = 2$ corresponds to Alice sending one-mode coherent states with the same amplitude, the case $n = 8$ corresponds to Alice sending four-mode coherent states which lie on a 7-dimensional real sphere in $\mathbb{R}^8$.

From the point of view of the reconciliation efficiency, all these strategies work equally well, but the higher the dimension considered, the closer Alice's modulation is from a Gaussian modulation. Hence, in order to get the maximal secret key rate (using a security proof based on the optimality of Gaussian states), one should work with the highest possible dimension, that is dimension 8.

B.1.1 $\beta I(A;B)$ *versus* $S(b;E)$

The secret key rate K for continuous-variable QKD protocols has the following general expression:

$$K = \beta I(A;B) - S(B;E). \tag{B.3}$$

In order to increase this secret key rate, one needs to find the best possible balance between a large value of $\beta I(A;B)$ and a small value of $S(B;E)$. From this perspective, the initial GGO2 protocol with a Gaussian modulation and the four-state protocol introduced in Chapter 5 appear to be at the two ends of the spectrum:

- the protocol with a Gaussian modulation insures the lowest possible value of $S(B;E)$, but unfortunately, the quantity $\beta I(A;B)$ is also quite small, and one cannot distill secret keys over large distances with this protocol[4],
- the four-state protocol is designed specifically to maximize the quantity $\beta I(A;B)$ at the cost of increasing $S(B;E)$. Indeed, the bound on $S(B;E)$ computed from the Gaussian optimality theorem is less tight for the four-state protocol than for the GG02 protocol, because the mixture of four coherent states only roughly approximate a genuine Gaussian modulation.

In Chapter 4, we saw how one could use rotations in $\mathbb{R}^8$ in order to improve the reconciliation of Gaussian variables. The idea was that such rotations made the Gaussian modulation closer from a binary modulation, hence facilitating the reconciliation problem. However, as the modulation was still Gaussian, the bound on $S(B;E)$ remained valid. The use of the algebraic properties of the octonions helped to increase the quantity $\beta I(A;B)$ while leaving $S(B;E)$ constant, and consequently improved the performances

[3]Indeed, with infinite computational power, Bob could just pick a random orthogonal transformation in $\mathbb{R}^n$ with n arbitrarily high. However, such a scheme would not be at all practical. In the hypothesis where Alice and Bob are given infinite computational power, it would be much simpler to conclude that Alice and Bob can perform a perfect reconciliation for correlated Gaussian variables, using for instance random spherical codes. In this manuscript, however, we are only interested in procedures that can be performed with realistic computational capabilities.

[4]In theory, however, this protocol also maximizes the quantity $I(A;B)$, making it probably the best *theoretical* continuous-variable QKD protocol. In practice, unfortunately, because of the very small efficiency β at low SNR, this protocol does not work as well as one could expect from theory.

of the QKD protocol.
Here, we would like to use the octonions the other way around. We start with the four-state protocol, for which the reconciliation problem is solved[5]. The goal, now, is to decrease the bound on $S(B;E)$. To this end, Alice will used a rotated modulation in $\mathbb{R}^8$, which is much closer from a Gaussian distribution than is the four-state modulation. Thanks to the properties of the octonions in $\mathbb{R}^8$, this can be achieved without degrading the reconciliation efficiency $\beta I(A;B)$. Hence, with this new protocol, the quantity $S(B;E)$ is decreased compared to the one of the four-state protocol, while leaving $\beta I(A;B)$ unchanged. As a consequence, the performance of this new QKD protocol is significantly improved compared to the four-state protocol.

B.2 Security of the protocol

Before computing the Holevo information between Bob and Eve, let us first consider the mutual information between Alice and Bob. This mutual information differs from the one of the usual protocol as Bob performs an heterodyne detection instead of an homodyne detection.

B.2.1 Mutual information between Alice and Bob

In the case of an heterodyne detection, Alice and Bob share twice as many data that in the case of an homodyne detection. However, the data are noisier as the heterodyne detection is implemented by splitting the pulses with a balanced beamsplitter before measuring both modes on a different quadrature with an homodyne de detection. This amounts to 3 supplementary decibels of noise, compared to an homodyne detection. The mutual information $I(A;B)$ therefore reads [47]:

$$\begin{aligned} I(A;B) &= I(x_1;y_1) + I(x_2;y_2) && \text{(B.4)} \\ &= 2 \times \frac{1}{2}\log_2(1+\mathrm{SNR}) && \text{(B.5)} \\ &= \log_2\left(1+\frac{TV_A}{2+T\xi}\right). && \text{(B.6)} \end{aligned}$$

On the other hand, the reconciliation efficiency is exactly the same as for the four-state protocol (this new protocol is indeed designed specifically with this property in mind).

B.2.2 Holevo information between Bob and Eve: entanglement-based version of the protocol

In order to compute the Holevo information between Bob and Eve, we proceed along the same lines as in the case of the discrete modulation protocols presented in Chapter 5 and we first need to consider the entanglement-based version of our new QKD protocol.

[5] meaning that we are satisfied with the value of $\beta I(A;B)$

Entanglement-based version of the protocol. Because of the choice of modulation, the mixed state ρ^4 sent by Alice corresponds to four successive coherent states uniformly distributed on a real 7-dimensional sphere and is given by

$$\rho^4 \equiv \iiint_{\mathcal{S}_\alpha} |\alpha_1\rangle\langle\alpha_1| \otimes |\alpha_2\rangle\langle\alpha_2| \otimes |\alpha_3\rangle\langle\alpha_3| \otimes |\alpha_4\rangle\langle\alpha_4| \mathrm{d}S \tag{B.7}$$

where the sphere $\mathcal{S}_\alpha$ is defined as

$$\mathcal{S}_\alpha \equiv \{(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \in \mathbb{C}^4 : |\alpha_{4k}|^2 + |\alpha_{4k+1}|^2 + |\alpha_{4k+2}|^2 + |\alpha_{4k+3}|^2 = 4\alpha^2\}, \tag{B.8}$$

and $\mathrm{d}S$ is the Haar measure on $\mathcal{S}_\alpha$. Because ρ^4 is a four-mode orthogonally invariant state (by construction), we saw in Chapter 6 that one can write

$$\rho^4 = \sum_{k=0}^{\infty} \lambda_k \, \sigma_k^4, \tag{B.9}$$

where

$$\sigma_k^4 = \frac{1}{\binom{k+3}{3}} \sum_{\substack{k_1 \cdots k_4 \\ \text{s.t. } \sum_i k_i = k}} |k_1, k_2, k_3, k_4\rangle\langle k_1, k_2, k_3, k_4|. \tag{B.10}$$

In order to determine the $\{\lambda_k\}_{k=0,\cdots,\infty}$, we use again the symmetry invariance of ρ^4. Let us compute the probability $\Pr(k)$ of finding k photons in the four-mode state ρ^4:

$$\begin{aligned} \Pr(k) &= \mathrm{tr}(\rho^4 \sigma_k^4) && \text{(B.11)} \\ &= \langle 2\alpha|\langle 0|\langle 0|\langle 0| \, \sigma_k^4 \, |2\alpha\rangle|0\rangle|0\rangle|0\rangle, && \text{(B.12)} \end{aligned}$$

since $|2\alpha\rangle|0\rangle|0\rangle|0\rangle \in \mathcal{S}_4$. Because the coherent state $|0\rangle$, which refers to the vacuum, does not contain any photon, one has:

$$\begin{aligned} \Pr(k) &= \langle 2\alpha|\sigma_k^4|2\alpha\rangle && \text{(B.13)} \\ &= e^{-4\alpha^2} \frac{(2\alpha)^{2k}}{k!} && \text{(B.14)} \\ &= \lambda_k. && \text{(B.15)} \end{aligned}$$

We therefore get the expression of ρ^4:

$$\rho^4 = e^{-4\alpha^2} \sum_{k=0}^{\infty} \frac{(2\alpha)^{2k}}{k!} \, \sigma_k^4. \tag{B.16}$$

The natural purification of ρ^4 which should be considered in the entanglement-based version of the QKD protocol is $|\Psi^4\rangle$ defined as:

$$|\Psi^4\rangle \equiv e^{-2\alpha^2} \sum_{k=0}^{\infty} \frac{(2\alpha)^k}{\sqrt{k!}} \, |\psi_k^4\rangle, \tag{B.17}$$

where

$$|\psi_k^4\rangle = \frac{1}{\sqrt{\binom{k+3}{3}}} \sum_{\substack{k_1 \cdots k_4 \\ \text{s.t. } \sum_i k_i = k}} |k_1, k_2, k_3, k_4\rangle|k_1, k_2, k_3, k_4\rangle. \tag{B.18}$$

Covariance matrix of $|\Psi^4\rangle$. Now that we know the pure state used in the entanglement-based of the protocol, all is left to do is to compute its covariance matrix, in particular the following values

$$X \equiv \langle\Psi^4|1+2a^\dagger a|\Psi^4\rangle = \langle\Psi^4|1+2b^\dagger b|\Psi^4\rangle \quad \text{(B.19)}$$
$$Z \equiv \langle\Psi^4|ab+a^\dagger b^\dagger|\Psi^4\rangle \quad \text{(B.20)}$$

where a and b refer to Alice and Bob's annihilation operators relative to the first mode. Indeed, because of the symmetry of $|\Psi^4\rangle$, its covariance matrix, Γ^4, reads,

$$\Gamma^4 = \bigoplus_{i=1}^{4} \begin{pmatrix} X\mathbb{1}_2 & Z\sigma_z \\ Z\sigma_z & X\mathbb{1}_2 \end{pmatrix}. \quad \text{(B.21)}$$

First, the partial trace ρ_k^1 of $|\psi_k^4\rangle$ over the first mode is given by:

$$\rho_k^1 = \frac{1}{\binom{k+3}{3}} \sum_{l=0}^{k} \binom{k-l+2}{2} |l,l\rangle\langle l,l|. \quad \text{(B.22)}$$

One immediately has:

$$\mathrm{tr}(a^\dagger a\rho_k^1) = \frac{1}{\binom{k+3}{3}} \sum_{l=0}^{k} l\binom{k-l+2}{2} = \frac{k}{4}. \quad \text{(B.23)}$$

Then,

$$\mathrm{tr}(a^\dagger a\rho^4) = \sum_{k=0}^{\infty} e^{-4\alpha^2} \frac{(2\alpha)^{2k}}{k!}\frac{k}{4} \quad \text{(B.24)}$$
$$= \alpha^2, \quad \text{(B.25)}$$

as expected. Finally $X = 1+2\alpha^2$.
Let us now compute $Z = \langle\Psi^4|ab+a^\dagger b^\dagger|\Psi^4\rangle$. First, one notes that $\langle\phi_l^4|ab|\psi_k^4\rangle = 0$ except if $l = k-1$. Some combinatorics shows that

$$\langle\phi_{k-1}^4|ab|\psi_k^4\rangle = \frac{1}{\sqrt{\binom{k+3}{3}\binom{k+2}{3}}} \sum_{l=0}^{k} l\binom{k-l+2}{2} \quad \text{(B.26)}$$
$$= \frac{1}{4}\sqrt{k(k+3)}. \quad \text{(B.27)}$$

Using the expression of $|\Psi^4\rangle$, one obtains

$$\langle\Psi^4|ab|\Psi^4\rangle = \frac{1}{4}e^{-4\alpha^2} \sum_{k=0}^{\infty} \frac{\sqrt{k+4}}{k!}(2\alpha)^{2k+1}, \quad \text{(B.28)}$$

and finally

$$Z = \frac{1}{2} e^{-4\alpha^2} \sum_{k=0}^{\infty} \frac{\sqrt{k+4}}{k!} (2\alpha)^{2k+1}. \tag{B.29}$$

Now, using the same procedure as in Chapter 5, we can compute the secret key rate as a function of the transmission T and the excess noise ξ. We address this question in the next section, directly in the finite size framework.

The fact that $Z < Z_G \equiv 2\sqrt{\alpha^4 + \alpha^2}$ leads to an increase of the upper bound on $S(y;E)$ one can derive from a Gaussian optimality argument. In particular, the value of $S(y;E)$ one obtains corresponds to the value one would obtain for a Gaussian modulation protocol with a quantum channel characterized by it transmission T_G and excess noise ξ_G which are given by $T_G = T/F \approx T$ and $\xi_G = F\xi + (F-1)V_A \approx \xi + (F-1)V_A$, where $F \equiv (Z_G/Z)^2$. Since one has $F \approx 1$ for reasonable values of V_A, the main effect of the non-Gaussian is the *equivalent excess noise* $\Delta\xi = (F-1)V_A$. Figure B.1 displays this equivalent excess noise in the case of the protocol presented here as well as for the 4-state protocol. In state-of-the-art implementation, the excess noise is typically less than a few

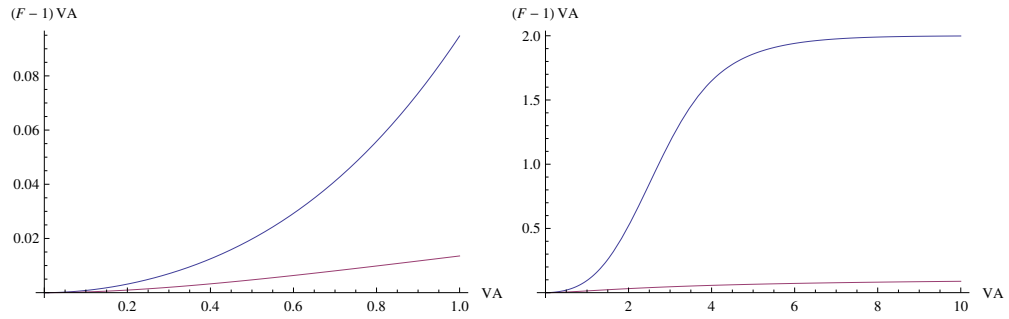

Figure B.1: (Color online) Equivalent excess noise due to the non-Gaussian modulation. Upper curve refers to the 4-state protocol [93], lower curve to the new continuous-modulation protocol. An excess noise of two units of shot noise corresponds to an entanglement-breaking channel, therefore no security is possible with such a level of noise.

percent of the shot noise. This gives a approximate limit for the value of the equivalent excess noise that is acceptable. In particular, for the 4-state protocol, one needs to work with modulation variances below 0.5 units of shot noise. On the contrary, it becomes possible to work with much higher variances in the case of our new protocol.

This can be seen on Figure B.2 where we display the asymptotic secret key rate for a distance of 50 km for the new protocol as well as for the 4-state protocol as a function of Alice's modulation variance. The various parameters are chosen conservatively: a quantum efficiency of 60% and an excess noise of 0.01. Both plots correspond respectively to a reconciliation efficiency of 80% and a more optimistic value of 90%. The superiority of the new protocol is quite clear: the secret key rate is higher by nearly an order of magnitude, and one can work with significantly larger modulation variances.

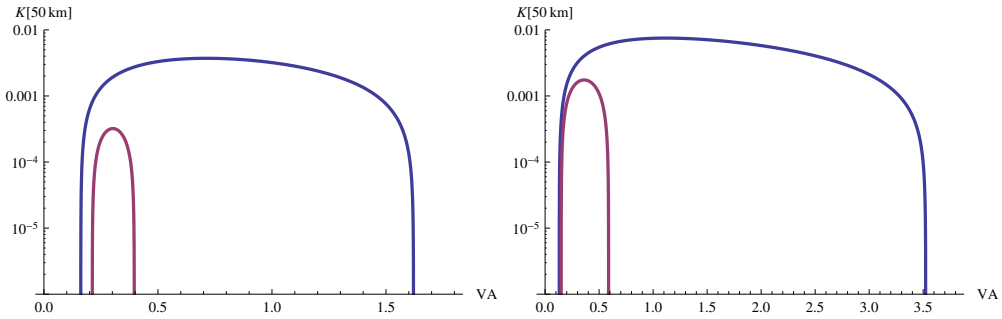

Figure B.2: (Color online) Asymptotic secret key rate for the new protocol and the four-state protocol (heterodyne detection) for a distance of 50 km, as a function of Alice's modulation variance. The various parameters are an excess noise of 0.01 and quantum efficiency of the detectors is $\eta = 60\%$. Reconciliation efficiency is supposed to be a conservative 80% on the left Figure, and an optimistic 90% on the right Figure.

B.2.3 Finite size performance

On Figure B.3, we display the secret key rate of the new protocol where finite sizes are taken into account. This finite size analysis is similar to the one described in Chapter 7. One should note that the secret key rate is computed against collective attacks, and not general attacks. The reason for this is that the optimality proof of Ref. [127] is only valid asymptotically and that the finite size corrections lead to very pessimistic results. However, the bounds of Ref. [127] are not believed to be tight. In particular, these might be improved by considering specific symmetries in phase space [90]. Among various finite size effects [137], the most crucial ones for continuous-variable protocols are clearly the imperfect reconciliation efficiency (which prevents the protocol with a Gaussian modulation to achieve key distribution over large distances) and parameter estimation. While the reconciliation efficiency is taken care of with our 8-dimensional continuous modulation, the parameter estimation is quite sensitive for continuous-variable protocols. In fact, the real problem lies in the estimation of the excess noise ξ, which is an extremely small in comparison to the shot noise. In Figure B.3, all finite size effects are taken into account. The protocol is now slightly modified as Alice and Bob exchange N quantum states, and use $m = N/2$ for the parameter estimation, while the other half is used for the key distillation. The results of the finite size analysis are quite pessimistic, but remember that the same situation is also true for all discrete-variable protocols [21]. While exchanging 10^{14} quantum signals is rather unrealistic, exchanging 10^8 or even 10^{10} signals can be done with today's technology. Hence, our new protocol allows for the distribution of secret keys over distances of the order of 50 km, while taking into account all finite-size effects.

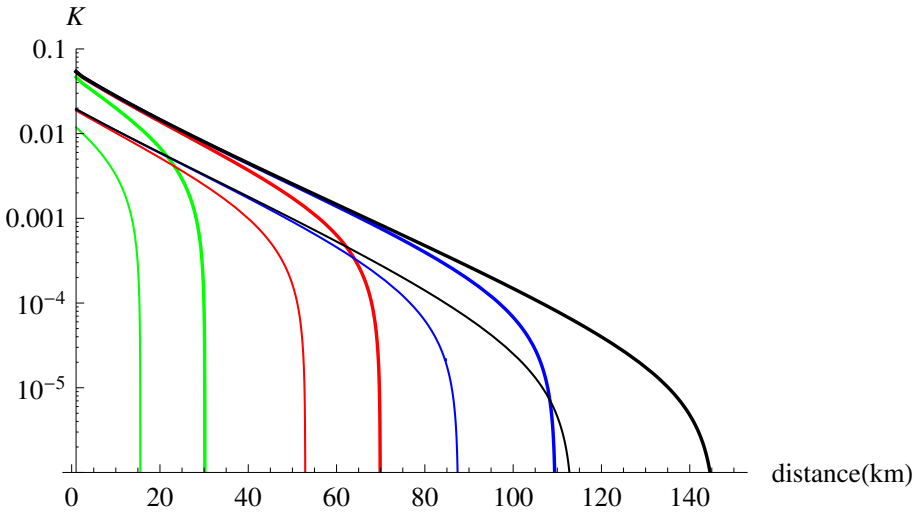

Figure B.3: (Color online) Secret key rate for the new protocol (thick lines) and the four-state protocol (thin lines) obtained for an expected realistic value of the excess noise of 0.005, and for $\epsilon_{\mathrm{PE}} = 10^{-10}$. Quantum efficiency of the detectors is $\eta = 60\%$. Reconciliation efficiency is supposed to be 80% for the bi-AWGN channel. The number of samples used for the parameter estimation is $m = n = N/2$. From top to bottom, the block length N is equal to $10^{14}, 10^{12}, 10^{10}$ and 10^{8}.

B.2.4 Perspectives

As a conclusion, we presented a new unconditionally secure continuous-variable QKD protocol based on a continuous but non-Gaussian modulation. The use of a specific reconciliation procedure allows for the distribution of secrets keys over long distances, which was impossible with a Gaussian modulation. Moreover, this protocol clearly outperforms all known practical continuous-variable, with a secret key rate an order of magnitude higher than for the four-state protocol.

Bibliography

[1] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-Independent Security of Quantum Cryptography against Collective Attacks. *Physical Review Letters*, 98(23):230501, 2007.

[2] Antonio Acín, Nicolas Gisin, and Lluis Masanes. From Bell's Theorem to Secure Quantum Key Distribution. *Physical Review Letters*, 97(12):120405, 2006.

[3] J.F. Adams. Vector Fields on spheres. *Ann. of Math*, 75(3):603–632, 1962.

[4] G. Adesso and F. Illuminati. Entanglement in continuous-variable systems: recent advances and current perspectives. *Journal of Physics A-Mathematical and Theoretical*, 40(28):7821–7880, 2007.

[5] R. Alléaume, J. Bouda, C. Branciard, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, A. Leverrier, et al. SECOQC White Paper on Quantum Key Distribution and Cryptography. *Arxiv preprint quant-ph/0701168*, 2007.

[6] R. Alléaume, F. Roueff, E. Diamanti, and N. Lütkenhaus. Topological optimization of quantum key distribution networks. *New Journal of Physics*, 11(7), 2009.

[7] B.D. Arvind, N. Mukunda, and R. Simon. The real symplectic groups in quantum mechanics and optics. *Pramana*, 45:471, 1995.

[8] Y. Aumann and M.O. Rabin. Information theoretically secure communication in the limited storage space model. *Lecture Notes in Computer Science*, pages 65–79, 1999.

[9] K. Bencheikh, T. Symul, A. Jankovic, and JA Levenson. Quantum key distribution with continuous variables. *Journal of Modern Optics*, 48(13):1903–1920, 2001.

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

[11] C.H. Bennett, G. Brassard, C. Crepeau, and U.M. Maurer. Generalized privacy amplification. *Information Theory, IEEE Transactions on*, 41(6):1915–1923, Nov 1995.

[12] Charles H. Bennett. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 68(21):3121–3124, May 1992.

[13] C. Berrou, A. Glavieux, and P. Thitimajshima. Near Shannon limit error-correcting coding and decoding: Turbo-codes. In *IEEE International Conference on Communications, 1993. ICC 93. Geneva. Technical Program, Conference Record*, volume 2, 1993.

[14] M. Bloch, A. Thangaraj, S.W. McLaughlin, and J.M. Merolla. LDPC-based Gaussian key reconciliation. In *IEEE Information Theory Workshop, 2006. ITW'06 Punta del Este*, pages 116–120, 2006.

[15] Alonso Botero and Benni Reznik. Modewise entanglement of Gaussian states. *Physical Review A*, 67(5):052311, May 2003.

[16] G. Brassard. Is information the key? *Nature Physics*, 1(1):2–4, 2005.

[17] G. Brassard, D. Chaum, and C. Crépeau. Minimum disclosure proofs of knowledge. *J. Comput. Syst. Sci.*, 37(2):156–189, 1988.

[18] G. Brassard, C. Crepeau, R. Jozsa, and D. Langlois. A quantum bit commitment scheme provably unbreakable by both parties. In *Foundations of Computer Science, 1993. Proceedings., 34th Annual Symposium on*, pages 362–371, 1993.

[19] G. Brassard and L. Salvail. Secret key reconciliation by public discussion. *Lecture Notes in Computer Science*, 765:410–423, 1994.

[20] M. Brune, J. Bernu, C. Guerlin, S. Deléglise, C. Sayrin, S. Gleyzes, S. Kuhr, I. Dotsenko, J. M. Raimond, and S. Haroche. Process tomography of field damping and measurement of fock state lifetimes by quantum nondemolition photon counting in a cavity. *Physical Review Letters*, 101(24):240402, 2008.

[21] Raymond Y. Q. Cai and Valerio Scarani. Finite-key analysis for practical implementations of quantum key distribution. *New Journal of Physics*, 11(4), 2009.

[22] A.R. Calderbank and P.W. Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54(2):1098–1105, 1996.

[23] C.M. Caves, C.A. Fuchs, and R. Schack. Unknown quantum states: The quantum de Finetti representation. *Journal of Mathematical Physics*, 43:4537, 2002.

[24] N. J. Cerf and C. Adami. Negative Entropy and Information in Quantum Mechanics. *Physical Review Letters*, 79(26):5194–5197, Dec 1997.

[25] N. J. Cerf, A. Ipe, and X. Rottenberg. Cloning of continuous quantum variables. *Physical Review Letters*, 85(8):1754–1757, Aug 2000.

[26] N.J. Cerf and P. Grangier. From quantum cloning to quantum key distribution with continuous variables: a review (Invited). *Journal of the Optical Society of America B*, 24(2):324–334, 2007.

[27] NJ Cerf, M. Levy, and G.V. Assche. Quantum distribution of Gaussian keys using squeezed states. *Physical Review A*, 63(5):52311, 2001.

[28] A. Chefles. Quantum state discrimination. *Contemporary Physics*, 41(6):401–424, 2000.

[29] G. Chiribella, G.M. D'Ariano, P. Perinotti, DM Schlingemann, and R.F. Werner. A short impossibility proof of Quantum Bit Commitment. *Arxiv preprint arXiv:0905.3801*, 2009.

[30] M. Christandl, R. König, G. Mitchison, and R. Renner. One-and-a-half quantum de Finetti theorems. *Communications in Mathematical Physics*, 273(2):473–498, 2007.

[31] Matthias Christandl, Robert König, and Renato Renner. Postselection Technique for Quantum Channels with Applications to Quantum Cryptography. *Physical Review Letters*, 102(2):020504, 2009.

[32] R. Clifton, J. Bub, and H. Halvorson. Characterizing quantum theory in terms of information-theoretic constraints. *Foundations of Physics*, 33(11):1561–1591, 2003.

[33] T.M. Cover and J.A. Thomas. *Elements of information theory*. Wiley-Interscience, 2006.

[34] I.B. Damgard, S. Fehr, L. Salvail, and C. Schaffner. Cryptography in the bounded quantum-storage model. In *Foundations of Computer Science, 2005. FOCS 2005. 46th Annual IEEE Symposium on*, pages 449–458, 2005.

[35] Giacomo Mauro D'Ariano, Dennis Kretschmann, Dirk Schlingemann, and Reinhard F. Werner. Reexamination of quantum bit commitment: The possible and the impossible. *Physical Review A*, 76(3):032328, 2007.

[36] Christian D'Cruz, Tobias J. Osborne, and Rüdiger Schack. Finite de Finetti Theorem for Infinite-Dimensional Systems. *Physical Review Letters*, 98(16):160406, 2007.

[37] B. De Finetti. La prévision: Ses lois logiques, ses sources subjectives. *Annales de l'institut Henri Poincaré (B) Probabilités et Statistiques*, 7:1–68, 1937.

[38] I. Devetak and A. Winter. Distillation of secret key and entanglement from quantum states. In *Proc. R. Soc. A*, volume 461, pages 207–235, 2005.

[39] P. Diaconis and D. Freedman. Finite Exchangeable Sequences. *The Annals of Probability*, 8(4):745–764, 1980.

[40] P. Diaconis and D. Freedman. A dozen de Finetti-style results in search of a theory. *Ann. Inst. Henri Poincare*, 23(2):397–423, 1987.

[41] J. Eisert and M.B. Plenio. Introduction to the basics of entanglement theory in continuous-variable systems. *Arxiv preprint quant-ph/0312071*, 2003.

[42] J. Eisert, S. Scheel, and M.B. Plenio. Distilling Gaussian states with Gaussian operations is impossible. *Physical review letters*, 89(13):137903, 2002.

[43] A.K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6):661–663, 1991.

[44] David Elkouss, Anthony Leverrier, Romain Alléaume, and Joseph J. Boutros. Efficient reconciliation protocol for discrete-variable quantum key distribution. In *IEEE International Symposium on Information Theory*, pages 1879–1883, 2009.

[45] Hugh Everett. "Relative State" Formulation of Quantum Mechanics. *Review of Modern Physics*, 29(3):454–462, Jul 1957.

[46] R.P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6):467–488, 1982.

[47] S Fossier, E Diamanti, T Debuisschert, R Tualle-Brouri, and P Grangier. Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers. *Journal of Physics B: Atomic, Molecular and Optical Physics*, 42(11):114014 (10pp), 2009.

[48] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier. Field test of a continuous-variable quantum key distribution prototype. *New Journal of Physics*, 11(4), 2009.

[49] R.G. Gallager. Low density parity check codes, 1963.

[50] R. Garcia-Patron. *Quantum information with optical continuous variables: from Bell tests to key distribution*. Phd thesis, Université Libre de Bruxelles, 2007.

[51] Raúl García-Patrón and Nicolas J. Cerf. Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution. *Physical Review Letters*, 97(19):190503, 2006.

[52] Géza Giedke and J. Ignacio Cirac. Characterization of Gaussian operations and distillation of Gaussian states. *Physical Review A*, 66(3):032316, Sep 2002.

[53] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. *Reviews of Modern Physics*, 74(1):145–195, 2002.

[54] R.J. Glauber. Coherent and incoherent states of the radiation field. *Physical Review*, 131(6):2766–2788, 1963.

[55] S. Gleyzes, S. Kuhr, C. Guerlin, J. Bernu, S. Deléglise, U.B. Hoff, M. Brune, J.M. Raimond, and S. Haroche. Quantum jumps of light recording the birth and death of a photon in a cavity. *Nature*, 446(7133):297–300, 2007.

[56] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof-systems. In *Proceedings of the seventeenth annual ACM symposium on Theory of computing*, pages 291–304. ACM New York, NY, USA, 1985.

[57] D. Gottesman and H.K. Lo. Proof of security of quantum key distribution with two-way classical communications. *IEEE Transactions on Information Theory*, 49(2):457–475, 2003.

[58] D. Gottesman and J. Preskill. Secure quantum key distribution using squeezed states. *Physical Review A*, 63(2):22309, 2001.

[59] F. Grosshans, N.J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. *QUANTUM INFORMATION & COMPUTATION*, 3(Sp. Iss. SI):535–552, OCT 2003.

[60] F. Grosshans and P. Grangier. Reverse reconciliation protocols for quantum cryptography with continuous variables. *Arxiv preprint quant-ph/0204127*, 2002.

[61] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N.J. Cerf, and P. Grangier. Quantum key distribution using Gaussian-modulated coherent states. *Nature*, 421(6920):238–241, 2003.

[62] Frédéric Grosshans. Collective Attacks and Unconditional Security in Continuous Variable Quantum Key Distribution. *Physical Review Letters*, 94(2):020504, Jan 2005.

[63] Frédéric Grosshans and Nicolas J. Cerf. Continuous-Variable Quantum Cryptography is Secure against Non-Gaussian Attacks. *Physical Review Letters*, 92(4):047905, Jan 2004.

[64] Frédéric Grosshans and Philippe Grangier. Continuous Variable Quantum Cryptography Using Coherent States. *Physical Review Letters*, 88(5):057902, Jan 2002.

[65] H. Halvorson and J. Bub. Can quantum cryptography imply quantum mechanics? Reply to Smolin. *QUANTUM INFORMATION & COMPUTATION*, 5(2):170–175, MAR 2005.

[66] M.B. Hastings. Superadditivity of communication capacity using entangled inputs. *Nature Physics*, 5(4):255–257, 2009.

[67] Matthias Heid and Norbert Lütkenhaus. Efficiency of coherent-state quantum cryptography in the presence of loss: Influence of realistic error correction. *Physical Review A*, 73(5):052316, 2006.

[68] Matthias Heid and Norbert Lütkenhaus. Security of coherent-state quantum cryptography in the presence of Gaussian noise. *Physical Review A*, 76(2):022313, 2007.

[69] C.W. Helström. Quantum detection and estimation theory. *Journal of Statistical Physics*, 1(2):231–252, 1969.

[70] M. Hillery. Quantum cryptography with squeezed states. *Physical Review A*, 61(2):22309, 2000.

[71] P. Horodecki. Separability criterion and inseparable mixed states with positive partial transposition. *Physics Letters A*, 232:333–339, February 1997.

[72] http://ltchwww.epfl.ch/research/ldpcopt.

[73] http://www.theory.caltech.edu/people/preskill/ph229/.

[74] R.L. Hudson and G.R. Moody. Locally normal symmetric states and an analogue of de Finetti's theorem. *Probability Theory and Related Fields*, 33(4):343–351, 1976.

[75] Kyo Inoue, Edo Waks, and Yoshihisa Yamamoto. Differential Phase Shift Quantum Key Distribution. *Physical Review Letters*, 89(3):037902, Jun 2002.

[76] E.T. Jaynes. Information Theory and Statistical Mechanics. *Physical Review*, 106(4):620–630, May 1957.

[77] Adrian Kent. Unconditionally Secure Bit Commitment. *Physical Review Letters*, 83(7):1447–1450, Aug 1999.

[78] J. Kilian. Founding crytpography on oblivious transfer. In *Proceedings of the twentieth annual ACM symposium on Theory of computing*, pages 20–31. ACM New York, NY, USA, 1988.

[79] A.Y. Kitaev. Quantum Computation: Algorithms and Error Correction. *Russian Mathematical Surveys*, 52(6):1191–1249, 1997.

[80] R. König, U. Maurer, and R. Renner. On the power of quantum memory. *IEEE Transactions on Information Theory*, 51(7):2391–2401, 2005.

[81] R. König and R. Renner. A de Finetti representation for finite symmetric quantum states. *Journal of Mathematical Physics*, 46:122108, 2005.

[82] R. König and R. Renner. Sampling of min-entropy relative to quantum knowledge. In *Workshop on Quantum Information Processing (QIP 2008)*, volume 480, 2007.

[83] R. König, R. Renner, and C. Schaffner. The operational meaning of min-and max-entropy. *arXiv*, 807, 2008.

[84] R. König and M.M. Wolf. On exchangeable continuous variable systems. *Journal of Mathematical Physics*, 50:012102, 2009.

[85] Robert König, Renato Renner, Andor Bariska, and Ueli Maurer. Small Accessible Quantum Information Does Not Imply Security. *Physical Review Letters*, 98(14):140502, 2007.

[86] B. Kraus, N. Gisin, and R. Renner. Lower and Upper Bounds on the Secret-Key Rate for Quantum Key Distribution Protocols Using One-Way Classical Communication. *Physical Review Letters*, 95(8):080501, Aug 2005.

[87] M. Le Bellac. *A short introduction to quantum information and quantum computation*. Cambridge University Press, 2006.

[88] U. Leonhardt. *Measuring the quantum state of light*. Cambridge University Press, 1997.

[89] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier. Multidimensional reconciliation for continuous-variable quantum key distribution. In *IEEE International Symposium on Information Theory*, pages 1020–1024, 2008.

[90] A. Leverrier, E. Karpov, P. Grangier, and N.J. Cerf. Security of continuous-variable quantum key distribution: towards a de Finetti theorem for rotation symmetry in phase space. *New Journal of Physics*, 11(11):115009, 2009.

[91] Anthony Leverrier, Romain Alléaume, Joseph Boutros, Gilles Zémor, and Philippe Grangier. Multidimensional reconciliation for a continuous-variable quantum key distribution. *Physical Review A*, 77(4):042325, 2008.

[92] Anthony Leverrier and Nicolas J. Cerf. Quantum de Finetti theorem in phase-space representation. *Physical Review A*, 80(1):010102, 2009.

[93] Anthony Leverrier and Philippe Grangier. Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation. *Physical Review Letters*, 102(18):180504, 2009.

[94] L.B. Levitin. Optimal quantum measurements for two pure and mixed states. In *Quantum Communications and Measurement: Proceedings of an International Workshop Held in Nottingham, England, July 11-16, 1994*, page 439. Plenum Publishing Corporation, 1995.

[95] H.K. Lo, X. Ma, and K. Chen. Decoy state quantum key distribution. *Physical Review Letters*, 94(23):230504, 2005.

[96] Hoi-Kwong Lo and H.F. Chau. Is Quantum Bit Commitment Really Possible? *Physical Review Letters*, 78(17):3410–3413, Apr 1997.

[97] Jérôme Lodewyck, Matthieu Bloch, Raúl García-Patrón, Simon Fossier, Evgueni Karpov, Eleni Diamanti, Thierry Debuisschert, Nicolas J. Cerf, Rosa Tualle-Brouri, Steven W. McLaughlin, and Philippe Grangier. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Physical Review A*, 76(4):042305, 2007.

[98] Jérôme Lodewyck and Philippe Grangier. Tight bound on the coherent-state quantum key distribution with heterodyne detection. *Physical Review A*, 76(2):022332, 2007.

[99] A. I. Lvovsky and M. G. Raymer. Continuous-variable optical quantum-state tomography. *Reviews of Modern Physics*, 81(1):299, 2009.

[100] D.J.C. MacKay. *Information theory, inference and learning algorithms*. Cambridge University Press, 2003.

[101] D.J.C. MacKay and R.M. Neal. Near Shannon limit performance of low density parity check codes. *Electronics letters*, 33(6):457–458, 1997.

[102] L. Magnin, F. Magniez, A. Leverrier, and N.J. Cerf. Strong No-Go Theorem for Gaussian Quantum Bit Commitment. *Arxiv preprint arXiv:0905.3419*, 2009.

[103] Dominic Mayers. Unconditionally Secure Quantum Bit Commitment is Impossible. *Physical Review Letters*, 78(17):3414–3417, Apr 1997.

[104] Alain Montfort. *Cours de statistique mathématique*. Economica, 1997.

[105] Miguel Navascués and Antonio Acín. Security Bounds for Continuous Variables Quantum Key Distribution. *Physical Review Letters*, 94(2):020505, Jan 2005.

[106] Miguel Navascués, Frédéric Grosshans, and Antonio Acín. Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography. *Physical Review Letters*, 97(19):190502, 2006.

[107] P. Navez. Statistical confidentiality tests for a quantum transmission using continuous variables. *The European Physical Journal D*, 18(2):219–228, 2002.

[108] K.-C. Nguyen, G. Van Assche, and N.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.

[109] M.A. Nielsen and I.L. Chuang. *Quantum computation and quantum information*. Cambridge Univ Pr, 2000.

[110] Julien Niset, Jaromír Fiurášek, and Nicolas J. Cerf. No-Go Theorem for Gaussian Quantum Error Correction. *Physical Review Letters*, 102(12):120501, 2009.

[111] B. Odom, D. Hanneke, B. D'Urso, and G. Gabrielse. New Measurement of the Electron Magnetic Moment Using a One-Electron Quantum Cyclotron. *Physical Review Letters*, 97(3):030801, 2006.

[112] M. Ohya and D. Petz. *Quantum entropy and its use*. Springer Verlag, 2004.

[113] S. Olmschenk, DN Matsukevich, P. Maunz, D. Hayes, L.M. Duan, and C. Monroe. Quantum Teleportation Between Distant Matter Qubits. *Science*, 323(5913):486, 2009.

[114] A. Ourjoumtsev, H. Jeong, R. Tualle-Brouri, and P. Grangier. Generation of optical Schrödinger cats from photon number states. *Nature*, 448(7155):784–786, 2007.

[115] A. Ourjoumtsev, R. Tualle-Brouri, J. Laurat, and P. Grangier. Generating Optical Schrödinger kittens for quantum information processing. *Science*, 312(5770):83–86, 2006.

[116] Alexei Ourjoumtsev, Rosa Tualle-Brouri, and Philippe Grangier. Quantum Homodyne Tomography of a Two-Photon Fock State. *Physical Review Letters*, 96(21):213601, 2006.

[117] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Furst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hubel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorunser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger. The SECOQC quantum key distribution network in Vienna. *New Journal of Physics*, 11(7), 2009.

[118] Asher Peres. Separability Criterion for Density Matrices. *Physical Review Letters*, 77(8):1413–1415, Aug 1996.

[119] Stefano Pironio, Antonio Acin, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, 11(4), 2009.

[120] S. Popescu, A.J. Short, and A. Winter. Entanglement and the foundations of statistical mechanics. *Nature Physics*, 2(11):754–758, 2006.

[121] J. Preskill. Reliable quantum computers. *Proceedings: Mathematical, Physical and Engineering Sciences*, pages 385–410, 1998.

[122] T.C. Ralph. Continuous variable quantum cryptography. *Physical Review A*, 61(1):010303, Dec 1999.

[123] MD Reid. Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations. *Physical Review A*, 62(6):62308, 2000.

[124] R. Renner. Security of quantum key distribution. *Arxiv preprint quant-ph/0512258*, 2005.

[125] R. Renner. Symmetry of large physical systems implies independence of subsystems. *Nature Physics*, 3(9):645–649, 2007.

[126] R. Renner and J.I. Cirac. A de Finetti representation theorem for infinite dimensional quantum systems and applications to quantum cryptography. *Arxiv preprint arXiv:0809.2243*, 2008.

[127] R. Renner and J.I. Cirac. de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography. *Physical Review Letters*, 102(11):110504, 2009.

[128] R. Renner and S. Wolf. Smooth Renyi entropy and applications. In *Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on*, pages 233–, June-2 July 2004.

[129] R. Renner, S. Wolf, and J. Wullschleger. The Single-Serving Channel Capacity. In *IEEE International Symposium on Information Theory*, pages 1424–1427, July 2006.

[130] Renato Renner, Nicolas Gisin, and Barbara Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Physical Review A*, 72(1):012332, Jul 2005.

[131] T. Richardson and R. Urbanke. Multi-Edge Type LDPC Codes. *Workshop honoring Prof. Bob McEliece on his 60th birthday*, pages 24–25, 2002.

[132] T.J. Richardson, M.A. Shokrollahi, and R.L. Urbanke. Design of capacity-approaching irregular low-density parity-checkcodes. *IEEE Transactions on Information Theory*, 47(2):619–637, 2001.

[133] R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[134] V. Scarani. *Quantum physics: a first encounter: interference, entanglement, and reality*. Oxford University Press, 2006.

[135] V. Scarani and C. Kurtsiefer. The black paper of quantum cryptography: real implementation problems . *Arxiv preprint 0906.4547*, 2005.

[136] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81(3):1301, 2009.

[137] Valerio Scarani and Renato Renner. Quantum Cryptography with Finite Resources: Unconditional Security Bound for Discrete-Variable Protocols with One-Way Postprocessing. *Physical Review Letters*, 100(20):200501, 2008.

[138] E. Schr
"odinger. Der stetige
"Ubergang von der Mikro-zur Makromechanik. *Naturwissenschaften*, 14(28):664–666, 1926.

[139] M.O. Scully and M.S. Zubairy. *Quantum optics*. Cambridge Univ. Press, 1997.

[140] Alessio Serafini. Multimode Uncertainty Relations and Separability of Continuous Variable States. *Physical Review Letters*, 96(11):110402, 2006.

[141] Claude E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423 and 623–656, 1948.

[142] P.W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. *Proc. 35nd Annual Symposium on Foundations of Computer Science (Shafi Goldwasser, ed.)*, pages 124–134, 1994.

[143] C. Silberhorn, N. Korolkova, and G. Leuchs. Quantum key distribution with bright entangled beams. *Physical review letters*, 88(16):167902, 2002.

[144] Ch. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs. Continuous Variable Quantum Cryptography: Beating the 3 dB Loss Limit. *Physical Review Letters*, 89(16):167901, Sep 2002.

[145] R. Simon, S. Chaturvedi, and V. Srinivasan. Congruences and canonical forms for a positive matrix: Application to the Schweinler-Wigner extremum principle. *JOURNAL OF MATHEMATICAL PHYSICS*, 40(7):3632–3642, JUL 1999.

[146] R. Simon, N. Mukunda, and B. Dutta. Quantum-noise matrix for multimode systems: U(n) invariance, squeezing, and normal forms. *Physical Review A*, 49(3):1567–1583, Mar 1994.

[147] G. Smith and J. Yard. Quantum communication with zero-capacity channels. *Science*, 321(5897):1812, 2008.

[148] J.A. Smolin. Can quantum cryptography imply quantum mechanics? *QUANTUM INFORMATION & COMPUTATION*, 5(2):161–169, MAR 2005.

[149] Robert W. Spekkens. Evidence for the epistemic view of quantum states: A toy theory. *Physical Review A*, 75(3):032110, 2007.

[150] D. Stucki, R. Thew, V. Scarani, N. Brunner, N. Gisin, J.D. Gautier, and C. Barreiro. Fast and Simple Quantum Key Distribution. *Appl. Phys. Lett*, 87:194108, 2005.

[151] J. Sudjana, L. Magnin, R. García-Patrón, and N.J. Cerf. Tight bounds on the eavesdropping of a continuous-variable quantum cryptographic protocol with no basis switching. *Physical Review A*, 76(5):052301, 2007.

[152] Masahiro Takeoka and Masahide Sasaki. Discrimination of the binary coherent signal: Gaussian-operation limit and simple non-Gaussian near-optimal receivers. *Physical Review A*, 78(2):022320, 2008.

[153] G. Van Assche. *Quantum cryptography and secret-key distillation*. Cambridge Univ Pr, 2006.

[154] G. Van Assche, J. Cardinal, and N.J. Cerf. Reconciliation of a quantum-distributed Gaussian key. *IEEE Transactions on Information Theory*, 50(2):394–400, 2004.

[155] Shun Watanabe, Ryutaroh Matsumoto, and Tomohiko Uyematsu. Tomography increases key rates of quantum-key-distribution protocols. *Physical Review A*, 78(4):042316, 2008.

[156] S. Wiesner. Conjugate coding. *ACM Sigact News*, 15(1):78–88, 1983.

[157] E. Wigner. On the quantum correction for thermodynamic equilibrium. *Physical Review*, 40(5):749–759, 1932.

[158] Michael M. Wolf, Geza Giedke, and J. Ignacio Cirac. Extremality of Gaussian Quantum States. *Physical Review Letters*, 96(8):080502, 2006.

[159] A.D. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54(8):1355–1387, 1975.

[160] G.Y. Xiang, T.C. Ralph, A.P. Lund, N. Walk, and G.J. Pryde. Noiseless Linear Amplification and Distillation of Entanglement. *Arxiv preprint arXiv:0907.3638*, 2009.

[161] A.C. Yao. Protocols for secure computations. In *Foundations of Computer Science, 1982. SFCS'08. 23rd Annual Symposium on*, pages 160–164, 1982.

[162] H.P. Yuen. Unconditionally secure quantum bit commitment is possible. *Arxiv preprint quant-ph/0006109*, 2000.

[163] Yi-Bo Zhao, Matthias Heid, Johannes Rigas, and Norbert Lütkenhaus. Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks. *Physical Review A*, 79(1):012307, 2009.