# Advanced signal processing techniques for continuous variable quantum key distribution over optical fiber

François Roumestan

**THÈSE DE DOCTORAT DE**
**SORBONNE UNIVERSITÉ**

Spécialité

**Informatique**

École doctorale Informatique, Télécommunications et Électronique (Paris)

Présentée par

**François ROUMESTAN**

Pour obtenir le grade de
**DOCTEUR de SORBONNE UNIVERSITÉ**

Sujet de la thèse :

# Techniques avancées de traitement du signal pour les systèmes de distribution quantique de clés sur fibre optique basés sur des variables continues.

soutenue le 21 mars 2022

devant le jury composé de :

| | |
|---|---|
| M. Romain Alléaume | Rapporteur |
| M. Andreas Poppe | Rapporteur |
| Mme Paulette Gavignet | Examinatrice |
| M. Thierry Debuisschert | Examinateur |
| M. Philippe Grangier | Invité |
| Mme Eleni Diamanti | Directrice de thèse |
| M. Amirhossein Ghazisaeidi | Co-encadrant de thèse |

*À mon épouse. À mon fils que j'ai hâte de rencontrer.*

# Remerciements

Je souhaite dans ces quelques mots d'introduction exprimer mes remerciements les plus chaleureux aux différentes personnes qui m'ont entouré et soutenu durant les trois années de ma thèse, et on rendu possible la réalisation de ce manuscrit.

Je souhaite remercier en premier lieux Romain Alléaume, Andreas Poppe, Paulette Gavignet et Thierry Debuisschert qui ont accepté de faire partie de mon jury de thèse, et qui m'ont remis le titre de docteur de Sorbonne Université. Merci à eux pour leur relecture minutieuse, leur écoute attentive lors de ma soutenance et leurs nombreuses questions pertinentes.

Je souhaite ensuite exprimer toute ma reconnaisance à Philippe Grangier, Eleni Diamanti et Amirhossein Ghazisaeidi pour leur constant engagement à mes cotés durant ces trois dernières années. C'est grâce à nos nombreuses discussions, et nos rencontres à Nokia ou Jussieu, que j'ai pu progressivement lever les différents obstacles qui séparaient Alice et Bob ! Je veux aussi les remercier pour leur humanité et leur bienveillance. Ce fut un immense plaisir de travailler avec eux.

Durant ces trois dernières années, j'ai passé le plus clair au sein du département de recherche sur les transmissions optique de Nokia Bell Labs, dans les laboratoires de Nozay. Merci à Jérémie Renaudier de m'avoir accueilli dans son équipe. J'ai eu la chance d'y rencontrer des collègues formidables. Au fil de nos passionnantes discussion, durant les pauses déjeuner ou les cafés virtuel en confinement, nous avons pu nouer de véritables amitiés. Merci à eux tous pour cela, ainsi que pour l'aide qu'ils m'ont bien souvent apportée.

Je souhaite aussi remercier les différentes personnes qui ont contribué à cette recherche et qui n'ont pas encore été citées. Je pense en particulier à Luis Trigo-Vidarte qui posé les premières bases de ce travail et avec qui j'ai eu la chance de collaborer au début de ma thèse. Je pense aussi à Anthony Leverrier, dont le regard de théoricien a permis de fructueux développements.

Enfin, je profite de ces dernières lignes pour remercier ma famille. Merci à mon épouse Albane, qui a été mon meilleur soutien du premier au dernier jour, dans les meilleurs moments comme dans les plus difficiles. Merci à mes parents qui ont cultivé en moi la curiosité et le goût pour la science, et qui m'ont soutenu durant toutes mes études, dont le doctorat est en quelque sorte l'achèvement. Merci enfin à ma sœur qui m'a régulièrement exprimé son soutien, et surtout bon courage à elle pour ses étude qui commencent.

*François Roumestan*

# Contents

# Résumé en français

Le projet Quantum Flagship lancé à l'initiative de la Commission européenne, ainsi que l'élaboration d'une stratégie nationale sur les technologies quantiques en France, sont deux exemples de l'intérêt que ces technologies suscitent auprès des pouvoirs publics. En particulier, les travaux présentés dans cette thèse s'inscrivent dans le cadre du projet européen CiViQ, membre du Quantum Flagship. L'ambition de ce projet est de développer des services de sécurité de la couche physique améliorés par la physique quantique et pouvant être combinés avec des techniques cryptographiques modernes. Plus particulièrement, ce projet s'intéresse aux technologies de distribution quantiques de clés à variables continues.

## Chapitre 1 : De la cryptographie classique à la cryptographie quantique avec des variables continues

Dans ce premier chapitre, on prend soin de motiver le travail que nous allons présenter. On commence par décrire les principes fondamentaux de la cryptographie moderne. Le mot cryptographie est dérivé des mots grecs kruptos, caché, et graphein, écrire. Cette idée d'écriture cachée décrit bien ce qu'est la cryptographie, un ensemble de techniques qui permettent à des utilisateur de communiquer à distance sans compromettre la confidentialité de leurs échanges. La grande majorité de ces techniques reposent sur l'existence de données secrètes, appelées clés, connues des seuls utilisateurs. Ces protocoles sont rassemblés sous le nom de cryptographie à clés secrètes, ou à clés symétriques. Leur inconvénient est précisément la nécessité de distribuer le secret à priori. En 1976, les cryptologues Whitfield Diffie et Martin Hellman proposent un paradigme fondamentalement différent. Leur idée est de générer deux clés dont les rôles sont asymétriques. La première clé est publique et permet de réaliser l'action de cryptage. La seconde est secrète, connue d'un seul utilisateur, et permet de décrypter les messages cryptés. Pour que la sécurité soit garantie, il faut que deviner la clé secrète à partir de la clé publique soit impossible. En pratique, les protocoles à clés asymétriques s'assurent que ce calcul ne soit pas réalisable dans un temps raisonnable. Cela repose en général sur une hypothèse mathématique de difficulté algorithmique, et sur la puissance de calcul disponible aux potentiels attaquants. Cependant, les progrès théoriques et technologiques pourraient rendre caduc ces hypothèses. Dans la pratique, ces protocoles sont souvent utilisés pour générer les clés secrètes nécessaire à la cryptographie à clés symétriques. L'enjeu est alors de proposer des méthodes de distribution de clés qui ne reposent pas sur de pareilles suppositions.

Les bases de la distribution quantique de clé ont été posées en 1984 par le physicien Charles Bennett et le cryptologue Gilles Brassard dans un article scientifique proposant un nouveau protocole, baptisé BB84 depuis. Le principe général de la distribution quantique est le suivant. Une première utilisatrice, appelée Alice par convention, génère des états quantiques qu'elle transmet à un second utilisateur, appelé Bob. Alice et Bob possèdent alors des données corrélées dont ils vont pouvoir extraire une clé secrète. La sécurité repose sur le théorème de non clonage, qui énonce l'impossibilité de cloner parfaitement un état quantique. Une conséquence est que toute attaque d'une potentielle espionne, appelée Ève, introduit nécessairement des erreurs de communication. Alice et Bob peuvent compter ces erreurs, et ainsi borner la quantité d'information qu'Ève possède sur leurs données. En utilisant des méthodes d'amplification de confidentialité, ils extraient ensuite une clé plus petite, dont la confidentialité est garantie avec un probabilité proche de 1.

La plupart des protocoles de distribution quantique de clé utilisent des grandeurs physiques discrètes comme l'état de polarisation d'un photon. Cependant, cette thèse s'intéresse plus particulièrement à un autre type de protocoles appelés à variables continues, introduits en 2002 par les physiciens Frédéric Grosshans et Philippe Grangier. Dans de tels protocoles, Alice transmet à Bob de l'information aléatoire qu'elle module sur la phase et l'amplitude de la lumière issue d'un laser, c'est à dire sur les quadratures d'états cohérents. Cette manière de faire est similaire en plusieurs aspects aux techniques modernes de transmission d'information sur fibre optique. Cela présente l'intérêt majeur de pouvoir utiliser les nombreux équipements et algorithmes développés pour ces dernières dans l'implémentation pratique des protocoles de distribution quantique de clés à variables continues.

## Chapitre 2 : Sécurité des protocoles de distribution quantique de clés à variables continues

Le second chapitre est consacré à l'analyse théorique d'un protocole à distribution de clés à variables continues. On commence par définir le protocole étudié, dans lequel Alice génère des états cohérents $|\alpha_k\rangle$, avec $\alpha_k = \frac{1}{2}(q_k + jp_k)$, dont les quadratures $p_k$ et $q_k$ sont tirées aléatoirement selon une certaine loi de probabilité. Elle transmet ces états à Bob à travers un canal quantique. On distingue le cas d'une modulation Gaussienne, où $q_k$ et $p_k$ sont indépendantes et distribuées selon une loi normale, du cas d'une modulation discrète, où $q_k$ et $p_k$ peuvent prendre un nombre fini de valeurs. Notons que le cas d'une modulation discrète est à ne pas confondre avec les protocoles à variables discrètes, pour lesquels c'est bien la grandeur physique qui est discrète.

L'analyse théorique se décompose en plusieurs étapes de simplification. Tout d'abord, on se ramène à protocole équivalent dans lequel Alice possède plusieurs copies d'un état intriqué $\rho_{AB}$, dont elle conserve un mode et transmet le second mode à Bob. Ensuite, on se limite à l'étude de la sécurité asymptotique, c'est à dire lorsque le nombre de symboles transmis tend vers l'infini. Dans ce cadre, on peut se ramener au cas d'attaques collectives, c'est à dire que l'on suppose qu'Ève réalise la même attaque pour chaque état, et que ces attaques sont indépendantes. On peut alors utiliser la formule de Devetak-Winter qui donne le nombre $r$ de bits secrets

par état cohérent transmis,

$$r = \beta I_{AB} - \chi_{EB} \tag{1}$$

où $I_{AB}$ est l'information mutuelle classique entre les données d'Alice et Bob, $\beta$ l'efficacité de la réconciliation, c'est à dire de la correction d'erreurs, et $\chi_{EB}$ est la borne de Holevo sur la quantité d'information possédée par Eve sur les états quantiques de Bob. Ensuite, on utilise un théorème d'optimalité qui affirme qu'on peut calculer $\chi_{EB}$ pour un état Gaussien dont la matrice de covariance $\Gamma_{AB}$ est égale à celle de l'état intriqué $\rho_{AB}$ après transmission du second mode à Bob. On peut alors exprimer $\chi_{EB}$ comme une fonction de cette matrice.

L'enjeu est maintenant le calcul de la matrice $\Gamma_{AB}$. Celui n'est pas immédiat car l'état $\rho_{AB}$ est un intermédiaire de calcul qui n'existe pas expérimentalement. $\Gamma_{AB}$ ne peut donc pas être expérimentalement évaluée. Le cas d'une modulation Gaussienne est plus facile à traiter parce que l'attaque optimale est alors une attaque Gaussienne. C'est à dire qu'on peut supposer que le canal est Gaussien, avec une certaine atténuation $T$ et un excès de bruit de variance $\xi$. La borne $\chi_{EB}$ s'exprime finalement comme une fonction de $T$ et $\xi$, qu'Alice et Bob peuvent expérimentalement mesurer. Le cas d'une modulation discrète est plus délicat et a fait l'objet d'un article publié en 2021 par Aurélie Denys, Peter Brown et Anthony Leverrier, dont nous donnons les résultats principaux. La méthode passe par la résolution d'un problème d'optimisation semi définie, et donne $\chi_{EB}$ en fonction de trois nouvelles quantités expérimentalement observables, notées $c_1$, $c_2$ et $n_B$.

Enfin, le calcul de $\chi_{EB}$ se décline en fonction du modèle considéré pour le récepteur de Bob. On distingue d'abord le cas d'un détecteur homodyne, c'est à dire qui ne mesure qu'une seule des deux quadratures, et d'un détecteur hétérodyne, qui mesure les deux quadratures simultanément. Enfin, un récepteur réel ne peut pas détecter tous les photons, il présente donc une certaine efficacité quantique $\eta < 1$, et introduit un bruit additionnel. On décrit la méthode qui permet de prendre en compte ces imperfections dans le calcul de $\chi_{EB}$. Autrement, ces imperfections sont attribuées au canal, et donc aux attaques de Ève.

L'enseignement théorique essentiel de ce chapitre se trouve dans le résultat des calculs numériques de taux de clés. On y apprend en effet que les taux de clés de certaines modulation discrètes approchent ceux d'une modulation Gaussienne, qui reste optimale. Ces modulations discrètes sont en fait des Gaussiennes discrétisées. Dans la suite de cette thèse, on décrira la réalisation expérimentale d'un système de distribution de clés à variables continues qui utilise de telles modulations discrètes.

On a ainsi calculé le taux de clés dans le cas asymptotique. En pratique, Alice ne transmet qu'un nombre fini d'états cohérents. La dernière section présente une méthode simplifiée pour prendre en compte les conséquences des tailles finies. Une de ces conséquences est que les quantités nécessaires au calcul du taux de clé sont estimées avec un nombre fini d'échantillons, c'est à dire avec des erreurs. C'est pour cela que pour chacune de ces grandeurs, on introduit un estimateur du pire cas, qui est la borne supérieure, ou inférieure, d'un intervalle de confiance. L'estimateur du pire cas est tel que la vraie valeur de la quantité estimée lui est inférieure, ou supérieure, avec une probabilité proche de 1. On présente une méthode générale pour calculer de tels estimateurs, et on fait référence à l'Appendice B pour les détails de calcul.

## Chapitre 3 : Principe fondamentaux des transmissions sur fibre optique modernes

Dans ce chapitre, on donne les notions de transmissions numériques sur fibre optique qui sont pertinentes pour la mise en œuvre expérimentale d'un système de distribution quantique de clés à variables continues. On commence par rappeler les concepts essentiels en communications numériques. Le modèle fondamental se compose d'un transmetteur et d'un récepteur séparés par un canal physique. Le transmetteur encode une source d'information binaire sur un signal physique en utilisant des techniques de modulation numérique. La technique qui nous intéresse est celle de la modulation en phase et en amplitude, dont les exemples essentiels sont les formats de modulation $2^m$-QAM (quadrature amplitude modulation) : des mots de $m$ bits sont modulés par $2^m$ points dans le plan de phase, qui sont répartis selon une grille carrée. Ces formats présentent cependant une pénalité, la quantité d'information qu'ils portent ne peut pas approcher la capacité du canal donnée par Claude Shannon. Pour s'approcher de cette capacité, il est possible de modifier la distribution de probabilité des mots binaires, afin que la distribution de probabilité sur la grille soit celle d'une Gaussienne discrétisée. Ces formats de modulation sont appelés PCS $2^m$-QAM (probabilistic constellation shaping). Ils correspondent aux modulations discrètes dont la bonne performance pour la distribution quantique de clés a été démontrée au Chapitre 2.

On décrit ensuite le fonctionnement d'un modulateur optique IQ, qui permet de moduler les quadratures d'une onde de lumière cohérente. Le principe repose sur deux interféromètres Mach-Zehnder. On ne garde qu'une sortie de chaque, qu'on fait passer dans un troisième Mach-Zehnder. En appliquant une tension pour contrôler la longueur des bras des interféromètres, on est capable de convertir un signal électrique en un signal optique modulé. Il est aussi possible de générer un signal multiplexé en polarisation en combinant deux modulateurs optiques.

On s'intéresse ensuite au principe de fonctionnement de la détection cohérente, permettant de mesurer les quadratures d'un signal cohérent. L'idée est de faire battre le signal optique reçu avec un signal non modulé de même fréquence, appelé oscillateur local. Avec une photo-diode, on mesure alors directement le cosinus de la phase relative entre les deux champs, c'est à dire une quadrature. De plus, l'utilisation de photo-détecteurs balancés permet d'améliorer la détection en supprimant la composante DC. En combinant les récepteurs, on peut retrouver les deux quadratures du signal, ainsi que mesurer un signal multiplexé en polarisation. Enfin, on donne des détails sur le bruit quantique associé à la détection cohérente, dont l'origine se trouve dans le principe d'incertitude de Heisenberg.

La transmission d'un signal lumineux à travers une fibre optique est soumise à diverses distorsions. Nous résumons celles qui sont pertinentes pour notre application. Il s'agit tout d'abord de l'atténuation de puissance le long de la fibre, principalement causée par l'absorption de photons. On cite aussi la dispersion chromatique qui induit un étalement spectral causé par la dépendance de l'indice de réfraction, et donc de la vitesse de transmission, à la longueur d'onde. Un des effets les plus important est causé la biréfringence de la fibre, qui fait que deux modes de polarisation ne se propagent pas à la même vitesse. Cette biréfringence étant aléatoire le

long de la fibre, l'effet cumulé est une rotation de l'état de polarisation dépendant de la longueur d'onde.

Enfin, la dernière partie de ce chapitre est consacrée aux techniques de traitement numérique du signal utilisées pour les transmissions sur fibre optique. On discute d'abord de la forme d'impulsion du signal, et on énonce le critère de Nyquist. Celui-ci conduit à l'utilisation de filtres RRC (root-raised cosine), qui permet d'implémenter un filtre adapté, ou "matched filter". On présente ensuite un égaliseur adaptatif basé sur des filtres à réponse impulsionnelle finie. Ce dernier réalise une opération inverse du canal approchée. En particulier, il corrige l'état de polarisation du signal, la dispersion chromatique, ainsi que la synchronisation à postériori de l'horloge du récepteur à celle du transmetteur. Enfin, on décrit l'algorithme de récupération de la phase du signal, qui se décompose en deux étapes. Une première étape corrige les variations rapide de la phase qui sont dues à un écart de fréquence entre le signal et l'oscillateur local. Une seconde étape implémente un égaliseur de maximum de vraisemblance pour corriger les variations lente de la phase, causées par la largeur de raie des deux sources lasers du système.

Pour conclure ce chapitre, on présente l'intuition de notre travail. Celle ci consiste à utiliser des équipements commerciaux utilisés pour les transmissions optiques, ainsi que les techniques de traitement numérique du signal, pour concevoir un système de distribution de clés à variables continues à haut débit.

## Chapitre 4 : Système expérimental et résultats

Ce chapitre présente la contribution principale de notre travail. On y décrit le système expérimental que nous avons mis en œuvre ainsi que les résultats obtenus.

Le système expérimental se compose d'équipements commerciaux. Le système d'Alice se compose d'un laser à faible largeur de raie, d'un modulateur IQ pour multiplexage de polarisation, dont les quatre entrées analogiques sont connectées aux sorties d'un générateur de formes de signaux arbitraires qui assure la fonction de conversion numérique-analogique. Un puissance-mètre optique et un atténuateur permettent de régler la puissance optique de sortie, un paramètre qui doit être optimisé pour maximiser le taux de clé secrète. Le système de Bob se compose pour sa part d'un laser identique comme oscillateur local, d'un récepteur cohérent, et d'un oscilloscope pour la conversion analogique-numérique. Un interrupteur optique est inséré entre l'entrée optique et le récepteur, pour éteindre régulièrement le signal entrant afin de calibrer le bruit de grenaille du récepteur, un autre paramètre essentiel pour le calcul du taux de clés. On détaille le principe de cette calibration et pourquoi elle nécessite d'appliquer aux échantillons du bruit les mêmes opérations de traitement numérique que celles subies par le signal.

Les premières utilisations du systèmes expérimental ont permis d'observer une source d'excès de bruit basse fréquence qui empêche la distribution de clés. Par conséquent, on décale le spectre du signal dans les fréquences positives de sorte qu'il n'ait pas de composantes basse fréquence et ne soit pas affecté par ce bruit.

Le traitement numérique du signal présenté au chapitre précédent doit être adapté pour permettre le fonctionnement d'un système de distribution quantique de clés. En effet, le rapport signal sur bruit est plus faible que dans le cadre des

transmissions classiques. Par conséquent, nous proposons d'ajouter des symboles pilotes tirés d'un format de modulation QPSK (quadrature phase shift keying), intercalés en temps, et dont l'amplitude est plus élevée que celle des symboles du protocole. On adapte alors le traitement numérique. Il utilise ainsi l'information connue sur ces pilotes pour corriger les distorsions du canal et retrouver le signal. Enfin, on optimise les paramètres des pilotes, leur amplitude et leur taux, afin de minimiser la variance de l'excès de bruit.

Les premiers résultats expérimentaux publiés ont été obtenus avant que ne soit disponible une preuve pour les modulations discrètes. Nous avions alors utilisé des modulations PCS 1024-QAM, dont la forme était optimisée pour minimiser la distance à une modulation Gaussienne. Cette distance portait sur les matrices densité des états quantiques. On supposait alors que la modulation était suffisamment proche d'une Gaussienne pour utiliser la preuve de sécurité de cette dernière. On vérifie maintenant la conformité de cette approximation avec la preuve de sécurité pour une modulation discrète.

On présente ensuite ses premiers résultats. Avec une distance de 9.5 km de fibre mono-mode (SMF, single mode fiber), une variance d'Alice de 8.22 SNU (unité de bruit de grenaille, ou shot noise unit), un taux de symboles de 400 MBaud, on mesure un excès de bruit moyen de 0.012 SNU. Cela donne taux de clé secrète moyen de 45.5 Mbps, calculés sur 100 acquisitions de 5 ms. On estime la distance maximale atteignable dans ces conditions à 17 km. Les expériences ont été réalisées avec un récepteur optique cohérent intégré. En caractérisant ce récepteur, nous avons observé certains comportement problématiques pour notre application. En particulier, on observe que la variance du bruit de grenaille n'est pas une fonction linéaire de la puissance optique de l'oscillateur local. Cela fausse l'estimation des paramètres nécessaire au calcul du taux de clés. Dans la suite, on utilise un nouveau récepteur cohérent, composé d'un mixeur optique et de 4 photo-détecteurs balancés, pour lequel on a vérifié l'absence de ces comportement problématiques.

Les deuxièmes résultats expérimentaux publiés utilisent la preuve de sécurité pour une modulation discrète. On a donc pu considérer des formats de modulation avec un cardinal plus faible, les formats PCS 64-QAM et PCS 256-QAM. Toujours pour une distance de 9.5 km, avec un taux de symboles de 600 MBaud, on mesure un excès de bruit moyen de 0.006 SNU et 0.011 SNU respectivement. On obtient alors des taux de clés moyens de 67.6 Mbps et 66.8 Mbps respectivement. On estime que l'on pourrait obtenir des taux de clés positifs jusqu'à une distance de 22 km avec cet état du système.

Pour aller plus loin, nous avons optimisé plus finement les paramètres du traitement numérique du signal. En particulier les deux paramètres du filtre adaptatif. Pour ce faire, on lance le traitement du signal avec différentes valeurs de ces paramètres, pour une dizaines d'acquisitions du signal. On choisit enfin les valeurs de paramètres qui minimisent l'excès de bruit. Après cette optimisation, on présente des résultats d'acquisitions avec 9.5 km de SMF et 25 km de fibre EX3000 (0.17 dB d'atténuation par km). On obtient respectivement 117.7 Mbps et 35.6 Mbps pour PCS 64-QAM, 138.8 Mbps et 44.0 Mbps respectivement pour PCS 256-QAM.

Cependant, ces derniers taux de clés ont été calculés à partir des paramètres atténuation $T$ et excès de bruit $\xi$. On a donc calculé les paramètres $c_1$, $c_2$ et $n_B$

de la preuve de sécurité pour une modulation discrète, en fonction de $T$ et $\xi$, les formules étant données pour un canal Gaussien. Une approche plus rigoureuse est d'estimer directement $c_1$, $c_2$ et $n_B$ à partir des données expérimentales, et de calculer le taux de clés avec ces valeurs. Cela donne des résultats asymptotique très proches. En revanche, les estimateurs de $c_1$, $c_2$ et $n_B$ sont plus sensibles aux fluctuations statistiques. Ainsi, en utilisant les estimateurs du pire cas pour prendre en compte les effets de taille finie, on obtient des taux de clés qui sont moins bons. Pour PCS 64-QAM, on obtient 60.2 Mbps à 9.5 km, et 0 Mbps à 25 km. Pour PCS 256-QAM, 91.9 Mbps à 9.5km et 24.0 Mbps à 25 km. Bien que plus pessimistes, cette méthode est plus rigoureuse. Ce sont donc ces taux de clés que l'on retient dans notre conclusion.

Une dernière expérience s'intéresse à la faisabilité de multiplexer en fréquence plusieurs canaux de distribution de clés. On remplace le laser d'Alice par quatre lasers dont les fréquences sont séparées de 4 GHz, qu'on assemble en un seul faisceaux modulé par le modulateur optique. Ainsi, on obtient un signal composé de quatre canaux PCS 256-QAM multiplexés en fréquence. On mesure les canaux les uns après les autres en faisant varier la longueur d'onde de l'oscillateur local. On obtient alors un taux de clés moyen de 63.7 Mbps pour chaque canal, avec 13.5 km de fibre monomode. Cette première expérience de multiplexage fréquentielle n'est cependant pas totalement satisfaisante puisqu'un vrai système utiliserait un modulateur différent pour chaque canal. Remarquons que ces calculs ont été faits à partir de $T$ et $\xi$ pour un canal Gaussien.

## Chapitre 5 : Discussion sur les expériences et leurs limitations

Ce chapitre rassemble différentes discussions sur des limitations de l'expérience et sur des pistes d'amélioration.

À cause de l'utilisation d'un oscilloscope, le mode de fonctionnement du système expérimental est actuellement lent. L'acquisition de 20 ms de signal prend environ 20 s. De plus, la moitié de la durée de l'acquisition sert à la calibration du bruit de grenaille. Cela ne remet pas en cause nos résultats qui ont permis de confirmer la possibilité d'utiliser des modulations discrètes avec un taux de clés de plusieurs dizaines de Mbps. En revanche, un système commercial devrait prendre en compte ces contraintes. En raisonnant sur le taux de symbole et la capacité des systèmes actuels de transmission optique, on argumente en faveur de la possibilité pratique d'une acquisition et d'un traitement du signal en temps réel.

On discute aussi de l'hypothèse d'un canal Gaussien pour le calcul du taux de clés avec une modulation discrète. On constate expérimentalement que le canal se comporte bien comme un canal Gaussien. Cependant il reste nécessaire d'estimer directement les paramètres $c_1$, $c_2$ et $n_B$ dont les estimateurs du pire cas donnent des valeurs du taux de clé plus pessimistes que les estimateurs du pire cas de $T$ et $\xi$.

On se penche ensuite sur l'estimation des paramètres pour le calcul du taux de clés. En théorie, la variance des symboles d'Alice $V_A$ est fixée par Alice et parfaitement connue, et $T$ est contrôlé par Ève et doit être estimé. En pratique, $V_A$ est dépendant de la puissance optique du laser d'Alice, ainsi que du réglage du

modulateur. En revanche, $T$ est fixé par la longueur de la fibre et ne varie pas. Pour mettre en conformité la pratique et la théorie, on commence par estimer $V_A$ en utilisant la valeur connue de $T$. On peut ensuite utiliser la valeur moyenne de $V_A$ comme une valeur fixe.

Enfin, on termine en parlant du décalage fréquentiel du signal. Ce dernier peut causer des fuites du signal sur la bande symétrique par rapport à la porteuse, à cause d'imperfections de modulation. Nous avons négligé l'impact de ces fuites sur la sécurité. Pour améliorer le système, il est possible de concevoir un signal multiplexé en fréquence numériquement. Cela permet de doubler le taux de symboles, tout en évitant ces potentielles fuites.

# Introduction

The Quantum Flagship project launched at the initiative of the European Commission, as well as the elaboration of a national strategy on quantum technologies in France, are two examples of the interest that these technologies are arousing among public authorities. In particular, the work presented in this thesis is part of the European project CiViQ, member of the Quantum Flagship. The ambition of this project is to develop quantum-enhanced physical layer security services that can be combined with modern cryptographic techniques. More specifically, this project focuses on continuous variable quantum key distribution technologies.

An important part of cryptographic protocols, called symmetric, rely on the existence of a secret pre-shared string of bits between users, called the key. Introduced in 1984 by Charles Bennett and Gilles Brassard, quantum key distribution (QKD) enables the generation of such secret keys between two distant parties [1]. Their security is based on the laws of quantum physics, in particular the no-cloning theorem. Therefore, it cannot be compromised by theoretical or technological advances, unlike other methods that rely on mathematical assumptions regarding computational complexity. The first protocol and most of the proposed variants encode the key information on discrete physical quantities, like the polarization of a photon. We refer to such techniques as discrete variable QKD (DV-QKD).

The idea of continuous variables QKD (CV-QKD) was proposed in 2002 by Frederic Grosshans and Philippe Grangier [2]. In their proposal, the information is encoded on the quadratures of the electromagnetic field of a coherent light source, which are in fact continuous quantities. In many ways, this protocol evokes techniques used in modern fiber optic transmissions. In particular, off-the-shelf equipment and digital signal processing (DSP) algorithms developed for the latter can be used for the practical implementation of CV-QKD. The work presented in this thesis deals precisely with the experimental realization of a CV-QKD system.

The security of QKD protocols relies on mathematical proofs that provide a bound on the amount of information available to a potential eavesdropper, without making any assumptions about their capabilities. However, these security proofs do make certain assumptions that must be verified to ensure their validity. In CV-QKD, the most common assumption is that the quadratures are modulated according to a Gaussian probability distribution. This assumption makes the theoretical analysis much easier, but does not reflect practical conditions. Indeed, the generation of a true Gaussian is not feasible.

Other proofs have emerged for certain discrete modulations, i.e. with a finite number of possible values [3, 4]. A very recent proof proposes a new method to

establish the security for any modulation [5]. In particular, it provides an analytical expression for the secret key rate, and establishes that asymptotic rates of discretized Gaussian modulations are very close to continuous Gaussian modulations.

The main contribution of the work presented in this thesis is to provide an experimental implementation of this proof, using discretized Gaussian modulations. The experimental system is built from commercially available equipment, and takes advantage of DSP techniques used in digital optical transmissions. In particular, we demonstrate the feasibility of a high-speed system, capable of generating several tens of Megabits per second of secret key, through a few tens of kilometers of optical fiber. Although subject to more restrictive security assumptions, the performance of our experiment compares favorably with the state of the art.

Here is an outline of the content of this manuscript :

**Chapter 1** We introduce essential concepts of modern cryptography and motivate the use of QKD technologies. The differences between DV-QKD and CV-QKD are explained, and a state of the art of the performance of CV-QKD experimental systems is provided.

**Chapter 2** A CV-QKD protocol is presented in detail, and the essential steps of the theoretical security proof are summarized. We insist on the particularities of a discrete modulation compared to a Gaussian modulation. We also describe how to take into account the imperfections of a practical receiver, as well as the statistical errors of measurement.

**Chapter 3** This chapter presents the fundamental principles of coherent optical communication that are relevant to the design of CV-QKD systems. More specifically, the operation of the optical modulator and receiver, the physical impairments of an optical fiber, and the conventional DSP algorithms to correct them are described.

**Chapter 4** We describe the experimental implementation of a CV-QKD system based on discrete modulations and using modern digital signal processing techniques. Finally, we present the obtained results, which conclude to the feasibility of such a system with key rates of several tens of Mbps with a range of a few tens of km.

**Chapter 5** This last chapter proposes a discussion on the experiments carried out, their limitations and possible improvements.

# Chapter 1

# From classical to quantum cryptography using continuous variables

Techniques for securing communication processes have long played an essential role in the protection of private data. They allow individuals to ensure the confidentiality of their personal data, companies to protect their sensitive documents, and are used by the military and intelligence services to ensure public security. The first elementary techniques have gradually given way to new and more sophisticated ones, up to the modern techniques which rely in particular on electronics and computers. In this chapter, we briefly present the latter and introduce the concept of quantum cryptography which is the subject of this thesis.

## 1.1 Cryptography or "hidden writing"

The word cryptography comes from the Greek word kruptos meaning hidden and the verb graphein meaning to write. The word carries the idea of a writing whose meaning would remain hidden from any unauthorized reader. In fact, cryptography refers to techniques that allow two distant parties communicating to make the content of their exchange inaccessible to a potential spy. A very common convention in literature is to name Alice and Bob the two trusted users, and Eve the spy.

The common basis for most cryptographic systems is as follows. Bob wants to transmit to Alice the private message $m$, called the *plaintext*. He has at his disposal an encryption cipher $E$, i.e. a function which outputs the encrypted message $c = E(m)$. This encrypted message $c$, called ciphertext, is transmitted to Alice by means of a communication channel that can be eavesdropped by Eve. Alice has for her part a decryption cipher $D$, such that $D(c) = D(E(m)) = m$.

One of the most elementary examples is the Caesar cipher, named after Julius Caesar, who claimed to use this technique to encrypt his private correspondence. The encryption principle is illustated in Figure 1.1. In the Caesar cipher, each letter of the plaintext is replaced by a letter located at a fixed number of positions down the alphabet. For instance, with an upshift of 2, the plaintext "ALEA JACTA EST"

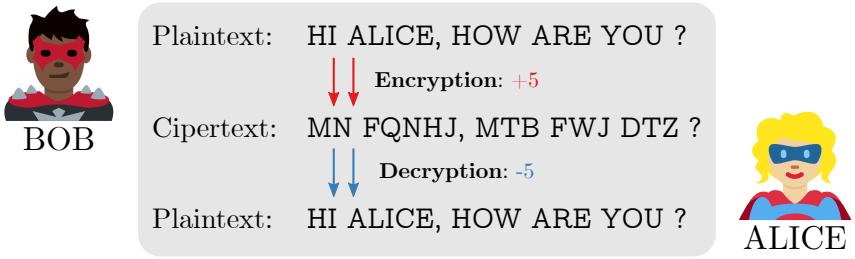



Figure 1.1: Caesar cipher. The key of the protocol is the shift value: +5.

gives the ciphertext "CNGC LCEVC GUV". To decrypt the cipher text, Alice needs to know the type of shift used and simply apply the reverse shift. Note that in this example, the encryption and decryption functions depend on a parameter, the relative integer $k$ of the shift. Assuming that Eve is able to read and copy the ciphertext, the security relies on the fact that she doesn't know the method used. Otherwise, she can easily guess $k$ by doing a simple exhaustive research. The security of the Caesar cipher is poor...

### 1.1.1 Symmetric key cryptography

When the encryption and decryption ciphers $E_k$ and $D_k$ depend on the same parameter $k$, we talk about *symmetric key* cryptography. The parameter $k$ is called the *key* of the protocol. Relying on the secrecy of ciphers is not recommended because the attacker can learn how they work, as was the case for the Allies and the Enigma machine during World War II. This is why most systems rely on the secrecy of the key and the difficulty of finding it.

The most common example of a symmetric key protocol is the one-time pad. It was Frank Miller who first came up with the idea in 1882 [6], to secure telegraphic communications, although Gilbert Vernam's contribution is more generally remembered. Vernam developed a one-time pad system using perforated paper tape, which he patented in 1919 [7]. In the one-time pad cipher, ciphertext $c$ is obtained as a XOR operation between the plaintext $m$ and the key $k$, which is a string with as many characters as $m$.

Claude Shannon proved in 1945 that the one-time pad protocol is secure regardless of the attacker's computing resources if and only if the following three conditions are met [8]:

- the key and message are strings of the same length and are kept secret,
- the key is completely random,
- the key is used only once.

The one-time pad opens up the possibility of long-term security, since security is not challenged by the improvement over time of computing systems. However, its practical implementation is made challenging by the need to share between Alice and Bob a very large amount of keys, which must be generated by a true random source.

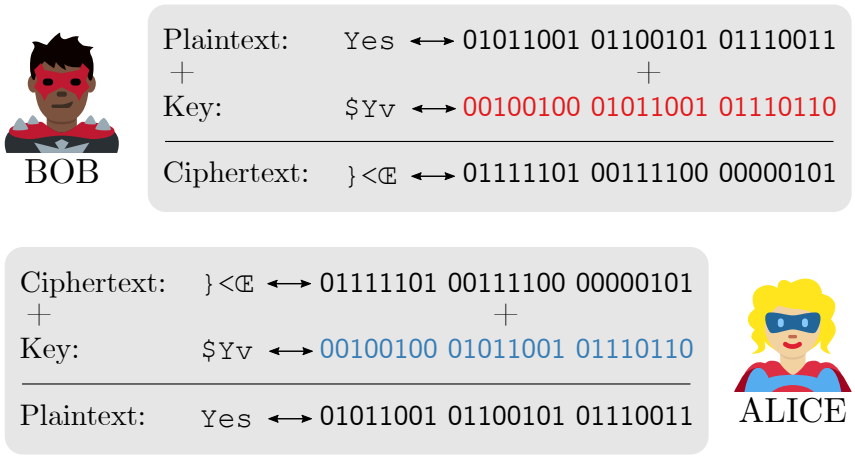



Figure 1.2: One time pad. The key must be random, and used only once: in this case, the security of the coding is demonstrated.

If one of the three conditions formulated by Shannon is not verified, security cannot be formally demonstrated. On the other hand, it is still possible to establish security under certain assumptions, within the framework of a certain number of attacks. In particular, the protocols must ensure that the key is long enough to prevent so-called exhaustive attacks, consisting in testing all possible keys. The security is then computational: the protocol is considered secure if the minimal time to determine the key is unreasonably long.

Many other examples of symmetric encryption protocols could be given. One of the most famous is the Data Encryption Standard (DES) [9], although it is no longer used because its 56-bit key allows for a very fast exhaustive attack. Nowadays, a key of 80 bits is considered a minimum, but a key of 128 or even 256 bits is recommended. Among the most widely used algorithms are Blowfish [10] and the Advanced Encryption Standard (AES) [11].

### 1.1.2 Asymmetric key cryptography

Symmetric key encryption requires that Alice and Bob share a key that must remain secret and be regularly updated. This requires a physical distribution of the key which is often impractical. W. Diffie and M. Hellman proposed in 1976 the idea of asymmetric encryption which was to revolutionize the way cryptography is done [12]. In this paradigm, Alice generates two keys k and k'. She stores k, which is the decryption key, also called the private key. She makes k', the encryption key, public on an authenticated server. When Bob wants to send a message to Alice, he takes note of the public key on the server, and uses it to encrypt his message. Alice can then easily use her private key to decrypt the message. There is currently no formal proof that such protocols are secure. The security is in fact computational, relying on the difficulty to find the private key from the message and the public key in a reasonable amount of time.

Protocols of this type are commonly used to secure Internet navigation. Indeed, they do not require a priori contact to transmit a message. On the other hand, the

keys must be much longer than for symmetric encryption. It is commonly considered that for long term security (typically 40 years), the key must be at least 4096 bits long, which is very rarely the case in practice. Among the best-known algorithms are RSA (for Rivest, Shamir and Adleman) [13], and the Digital Signature Standard (DSS) [14].

The security of asymmetric protocols is essentially based on a small family of assumptions about the computational difficulty of certain simple mathematical problems. For example, decrypting RSA requires factoring a very large integer into prime factors, a problem for which no efficient classical algorithm is known. Thus, an unexpected breakthrough, in mathematics or in algorithms, can brutally compromise the security of asymmetric systems. Moreover, the development of quantum computers would allow to solve some problems faster. For example, Shor's algorithm allows to factor large numbers in polynomial time [15]. The RSA assumption therefore does not offer very likely long-term security guarantees. Indeed, an attacker always has the possibility to store all communications until such a device is available.

The set of bounded-error quantum polynomial time (BQP) is the class of decision problems solvable with high probability by a quantum computer in polynomial time. If the NP(nondeterministic polynomial time) is not strictly contained is the BQP, it is then possible to design cryptographic systems that cannot be easily broken by a quantum computer. The post-quantum cryptography field is currently addressing this issue. Note that the boundary between BQP and NP is not well established and that the existence of NP problems outside BQP has not been demonstrated yet. For the moment it is only possible to use problems for which no algorithm with quantum advantage has been found.

## 1.2 Quantum Key Distribution

Let us now introduce the main object of this thesis, quantum key distribution. This term covers all the methods for distributing keys between two distant parties, whose security can be demonstrated by arguments from the theory of quantum mechanics. They offer a long-term secure alternative to asymmetric cryptography.

### 1.2.1 The no-cloning theorem

In a paper published in 1970, J. L. Park demonstrated the impossibility of designing a measurement device, even a theoretical one, which does not disturb the quantum states being measured [16]. In 1982, this same result was independently re-demonstrated in a slightly different context by W. H. Zurek and W. K. Wootters in reference [17] and by D. Dieks in reference [18]. The authors demonstrated the impossibility of creating an identical and independent copy of an arbitrary unknown quantum state. This fundamental result for quantum key distribution is called the *no-cloning theorem*. It should be noted that the 1982 articles were published in response to an article by Nick Herbert published the same year, proposing a hypothetical technique of superluminal communication [19], i.e. at a speed exceeding the speed of light. In fact, evidence shows that the theorem was actually proved 18 months prior by G. Ghirardi, in a referee report to Herbert's proposal [20].

In the 1970s, Stephen Wiesner devised a protocol to prevent banknote forgery [21], introducing the idea of using quantum mechanics for security. In a generalization of his proposal, the bills are issued by the bank with a serial number and a set of quantum states, known only to the bank. The quantum states are chosen randomly among four different values, forming conjugate observables. If a user wants to exchange the banknote, they must transmit the quantum states to the bank for verification. If the banknote is cloned, the forgery is detected with probability $1 - (3/4)^N$, where $N$ is the number of states in the set. As $N$ becomes large, the probability of detecting counterfeit money approaches 1. This same idea is at the origin of the first quantum key distribution protocol, which we will describe in the next subsection.

### 1.2.2 A QKD protocol: BB84

Charles Bennett and Gilles Brassard proposed in 1984 the first key distribution protocol with security based on quantum mechanical theory. The founding idea is based on the non-cloning property of a quantum state. In short, Alice sends to Bob polarized photons on a quantum channel. The eavesdropper cannot perfectly clone or divide the photons. She has to measure them, and generate new ones to send to Bob with the measured polarization. In doing so, she introduces errors in the protocol, that betray her presence. The protocol assumes that Alice and Bob also have access to an authenticated classical channel, to monitor the protocol and identify if the channel is being eavesdropped.

As already mentioned, one of the possible physical quantities to implement the BB84 protocol is the polarization of photons. Alice transmits random bits to Bob by encoding them on an orthonormal basis. For example a horizontal polarization, noted $|\leftrightarrow\rangle$, encodes a 0, and a vertical polarization, noted $|\updownarrow\rangle$, a 1. Alice has at her disposal a second basis inclined by a 45° angle: a polarization of 45° to the left, noted $|\nwarrow\!\!\searrow\rangle$, encodes a 0, and a polarization of 45° to the right, noted $|\swarrow\!\!\nearrow\rangle$, encodes a 1. For each bit to be transmitted, Alice randomly chooses the encoding basis and the bit with uniform probability. Bob is not informed of her choice. For his measurement, he chooses arbitrarily one of the two basis. If his choice does not coincide with Alice's, the polarization he measures is random, and the information is unusable. Using the authenticated channel, Alice and Bob communicate to each other their basis choices and dismiss the bits measured with incompatible bases. This step of the protocol is called *sifting*.

What if Eve tries to eavesdrop the channel? Since she cannot clone or divide a photon, any action will introduce errors. For instance, she can measure the polarization, and then generate a new photon to send to Bob corresponding to her measurement. This basic attack is called intercept-and-resend. Like Bob, she has to decide on the basis to use, with probability 1/2 of making a mistake. This induces a 1/4 error probability in the bit read by Bob. Thus, if Alice and Bob reveal a fraction of their bits on the authenticated channel to estimate the bit error rate, they are able to estimate the quantity of information leaked to Eve. In fact, Eve is capable of subtle attacks consisting in imperfect cloning of the photons. In this case, she still introduces an error rate of 11%. Figure 1.3 illustrates the principles of BB84 protocol that we have just described.

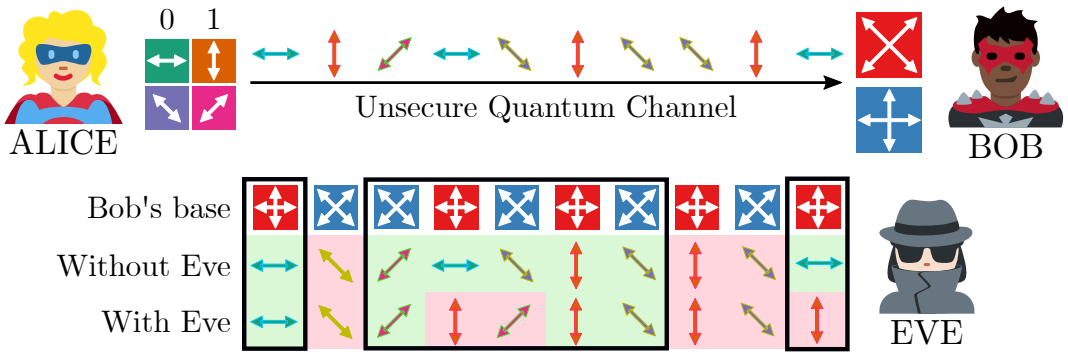



Figure 1.3: Illustration of the BB84 protocol, where Alice encodes random bit on the polarization of a photon, using either one of two orthogonal basis. Alice and Bob dismiss the bits for which Bob chose the wrong basis. In the presence of Eve, they observe an increase of the bit error rate.

Thus, Alice and Bob can calculate a bound on the amount of Eve's information, regardless of the attack. They can use this knowledge to extract a secret from their correlated data. To do so, they have first to correct the errors by using error-correcting codes to obtain a common error-less key, in a step called *information reconciliation*. Then, using *privacy amplification* techniques, they generate from their shared data a smaller key, which is unknown to the eavesdropper with high probability.

**Remarks** In the following, we propose some useful remarks on the BB84 protocol as well as QKD in general...

- In a practical system, the various sources of noise we have to deal with introduce measurement errors. Thus, a non-zero bit error rate is always observed, even when there is no eavesdropper. In the absence of additional information on the noise, it is necessary for security to attribute the observed errors to a potential attack.

- In fact, the amount of information actually obtained by Eve is generally inaccessible. We rather try to obtain an upper bound on this quantity. As no hypothesis is made on Eve's abilities, we must assume that she makes the most advantageous attack among the ones compatible with Alice and Bob's information. Bounding Eve's information knowing Alice and Bob's observables is actually the object of so-called mathematical security proofs.

- The BB84 protocol assumes the use of a single photon source with perfect modulation of the polarization, and of a single photon detector. If these assumptions are not met, the security proof cannot be applied to the system.

- Power losses due to dispersion in a practical channel like an optical fiber limit the range of QKD. In fact, a maximum reachable distance can be calculated independently of the considered protocol [22].

- The assumption of an authenticated channel implies that some security protocol is used, which requires that Alice and Bob already have a key at their disposal. Therefore, QKD requires a pre-shared secret. In a way, it is a key amplification process.

### 1.2.3 Some developments in QKD

Since the publication of BB84, many other QKD protocols were proposed. They typically follow the same outline:

1. **Prepare and measure.** Quantum states are generated by Alice and transmitted to Bob for measurement through a quantum channel.

2. **Parameter estimation.** Communicating on the authenticated channel, Alice and Bob estimate the relevant quantities to derive a bound on the information accessible to Eve.

3. **Information reconciliation.** Typically using error correcting codes, Alice and Bob extract from the measurement a common data string that is still unsafe.

4. **Privacy amplification** techniques are used to generate a private key from the shared data, using the result of step 2.

Let's note that only the first two steps of the protocols involve quantum mechanics. That is why most experimental proof-of-principle works do not implement the last two steps. They usually exchange the quantum states and estimate the achievable length of the secret key using security proofs.

Some protocols follow a slightly different approach, based on entangled states. In these protocols, Alice prepares two entangled states, sends one of them to Bob and measures the other one. Steps 2, 3 and 4 remain conceptually unchanged. The first protocol of this type, E91, was proposed in 1991 by Artur Ekert and makes use of entangled photons [23]. Other protocols were then proposed on the same model, like BBM92 [24]. We might think that the world is divided between *entanglement-based* (EB) and *prepare-and-measure* (PM) protocols, but in fact it was realized that EB protocols have PM equivalents and conversely. PM protocol are more practical in general, while their EB equivalent offers more convenient theoretical tools for security analysis.

The practical use of entangled states in QKD remains promising as it would allow to use *quantum repeaters* [25]. Indeed, channel attenuation is one of the main limiting factors in quantum communication and cryptography and the use of conventional optical repeaters such as erbium-doped fiber amplifiers (EDFA) is not possible because they would irreversibly alter the quantum states. On their part, quantum repeaters rely on quantum teleportation to distribute entanglement between two distant parties. The development of such devices is a considerable challenge that would permit in particular to improve the reach distance of QKD systems, but would also serve for the implementation of other quantum communication systems. The family of *twin-field protocols* (TF-QKD) is another way to extend the reach of QKD, where

both Alice and Bob generate quantum states which interfere at an intermediate untrusted place [26]. This scheme is in a fact a simplification of quantum repeaters than can be built using current technology [27]. A recent field-test reported the feasibility of key exchange on a 511 km optical fiber between two distant cities [28].

As mentioned earlier, the security of a QKD system relies on the validity of certain assumptions, some of which on the equipment used. Thus, there is a concern that an accidental or malicious malfunction of one of the components in the system could jeopardize its security. In 1998, D. Mayers and A. Yao proposed the use of self-testing quantum systems to reduce this device dependence [29]. It was ten years later that the use of Bell tests in this context was proposed by R. Colbeck [30]. The interest of these protocols is that their security is not based on an assumption of trust in the devices used, this is why they are known as device independent protocols. On the other hand, they have the disadvantage of requiring a loophole-free Bell test measurement, which is impractical to implement for the moment [31]. To simplify this approach, one can assume that only measuring devices are unreliable. Protocols following this approach are referred to as measurement device independent (MDI-QKD) [32]. The practical implementation of the latter is easier than that of DI-QKD protocols [33].

## 1.3 Continous variable QKD

Our experimental work focuses on the class of continuous variable QKD protocols (CV-QKD). In this section, we present this type of protocols, their advantages and the latest experimental advances.

### 1.3.1 DV-QKD vs CV-QKD

Most available QKD protocols use quantum states taken in a finite-dimensional Hilbert space. For example, the states in the BB84 protocol are actually qubits in a two-dimensional Hilbert space. This context allows for simple security analysis but typically requires complex practical implementation. Such protocols are referred to as discrete variable (DV-QKD). Another way to proceed is to consider a Hilbert space of infinite dimension, in which the observables have continuous eigenspectra. Typical example of such observables are the quadratures in the phasor diagram of the electromagnetic field of a light beam. Such protocols are called continuous variable (CV-QKD). Their theoretical analysis is more difficult than that of DV-QKD. However, their practical implementation is greatly simplified by their proximity to classical communications. Indeed, the most efficient systems in optical communication use phase and amplitude modulation of coherent light beams. It is therefore possible to benefit from the state-of-the-art equipment available as well as from modern digital processing techniques.

The first CV-QKD protocol proposals involved squeezed-states, with discrete modulation in phase space [34, 35, 36], and then Gaussian modulation [37]. F. Grosshans and P. Grangier proposed in 2002 a protocol, called GG02, that used coherent states with Gaussian modulation [2]. The use of coherent states allowed to avoid the practical difficulty of technological generation of squeezed states, allowing

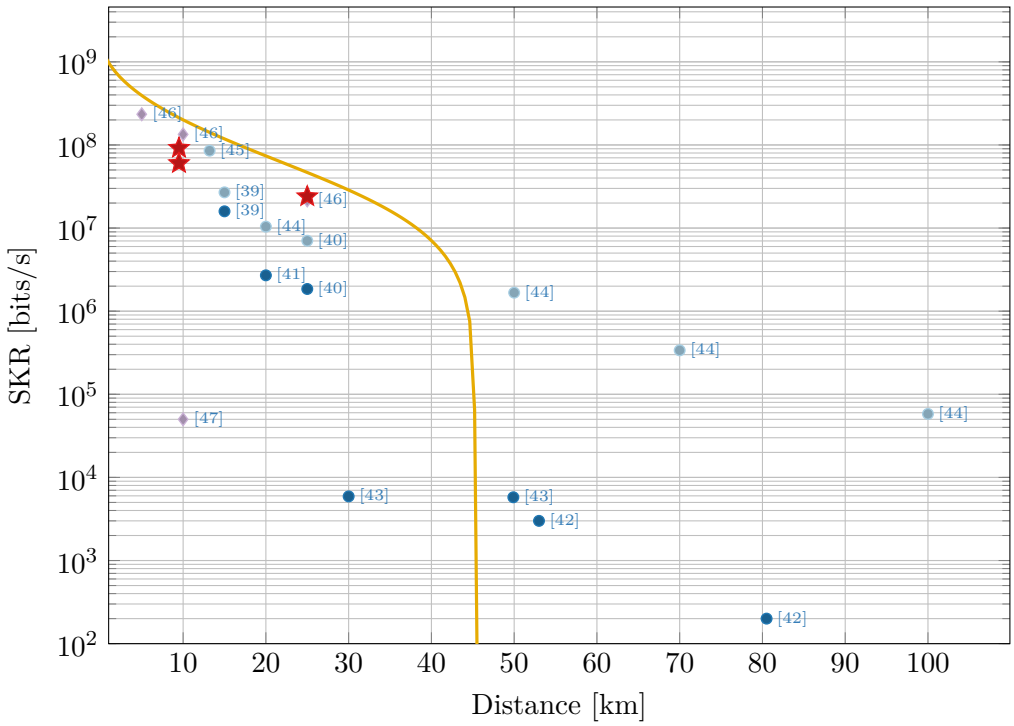



Figure 1.4: Comparison of the final experimental result of this thesis, given by red stars, to state of the art publications. Blue circles denote Gaussian modulation results while purple diamond are discrete modulation results. Asymptotic and finite size results are distinguished by light and dark colors respectively (see text for explanation). The yellow curve is a theoretical curve for an optimal Gaussian modulation with similar conditions as in our experiments: a symbol rate of 600 MBaud, an excess noise variance $\xi_B = 0.0005$, for an optical fiber link with 0.172 dB loss per km.

a fast experimental validation [38].

In the GG02 QKD protocol, Alice generates coherent states $|\alpha_\rangle, |\alpha_2\rangle, \ldots$ with $\alpha_1, \alpha_2, \ldots$ chosen independently at random from a complex circular Gaussian distribution. The quantity of interest to detect the presence of Eve, similar to the bit error rate in BB84, is the covariance matrix between Alice's and Bob's data. The quadratures of a coherent state present a fundamental noise called shot noise, or vacuum noise. The presence of Eve is typically betrayed by the presence of an additional noise, called excess noise. In the next chapter, we will present the steps for computing the secret key rate from the quantities measurable by Alice and Bob.

### 1.3.2 Experimental state of the art

Figure 1.4 shows the most recent key rates obtained with experimental CV-QKD systems on optical fiber, as a function of the considered channel distance.

The rates are divided into two categories. The light points are asymptotic rates, i.e. those that would be obtained for a stable protocol of infinite duration. This

asymptotic hypothesis allows to have a first idea of the performance of a system. However, it is not realistic. The dark points are rates calculated by taking into account some consequences of the finite duration of the protocol. It should be noted, however, that no formal proof of the safety of a finite protocol is available at this time, although progress in this direction has been made [48]. These rates are therefore more realistic than the asymptotic ones, but are not yet sufficient.

Most protocols in the figure are implemented with Gaussian modulation [41, 42, 45, 39, 44, 40, 43]. They are represented by circles. This corresponds to the GG02 protocol, for which the theoretical security is the most established. However, Gaussian modulation has the disadvantage of making post-processing more complex. Moreover, the practical realization of a true Gaussian modulation is not possible since the hardware necessarily introduces quantization.

Other systems implement discrete modulation, such as quadrature phase shift keying (QPSK) [46, 47, 49], or 8-PSK modulation [50]. They are represented by diamonds. Their use facilitates the practical realization of the modulation and post-processing. However, the theoretical proofs for such modulations have much lower secret bit per transmitted coherent state than Gaussian modulation.

The main contribution of this thesis is to consider discrete Gaussian modulation formats, inspired by the latest technologies developed in optical communications. The modulation formats are probabilistic constellation shaping (PCS) quadrature amplitude modulation (QAM) formats. By analyzing their security using the latest theoretical advances [5], we obtain very promising results. Our work in reference [51] established a first result with a PCS 1024-QAM format. Then, we consolidated our results in Reference [52], with PCS 64 and 256-QAM. The final results are represented by red stars on the figure. The resulting key rates are similar or even better than the state-of-the-art experiments with Gaussian modulation, but have the advantage of coming from discrete modulation formats. To our knowledge, they are the first experimental implementation of the theoretical advance of Reference [5].

# Chapter 2

# Security of continuous variable QKD

In this chapter, we summarize the main arguments to establish the theoretical security of a QKD protocol. The considered protocol is a little more general than GG02, since it does not assume a Gaussian modulation. The reader is expected to be familiar with quantum information theory and the Gaussian state formalism. Appendix A provide a summary of the main concepts and results necessary to understand this chapter.

## 2.1 A QKD protocol using coherent states

### 2.1.1 The GG02 prepare and measure protocol

The following is a brief theoretical description of a general CV-QKD protocol using coherent states. It is in fact a variant of the widely used GG02 protocol proposed in 2002 by Frédéric Grosshans and Philippe Grangier [2]. The basic assumptions are that Alice and Bob have two channels at their disposal, a quantum one and a classical one. It is assumed that Eve has full access and control of the quantum channel. Her interactions with the channel are ruled by quantum mechanics. Eve can also listen to the classical channel. However, it is assumed that the classical channel is *authenticated*, i.e. Eve cannot modify the messages, or pretend to be Alice or Bob. Figure 2.1 gives a schematic view of the protocol.

**(i) Prepare** Alice draws samples $(q_1, p_1) \dots, (q_N, p_N)$ from independent and identically distributed random vectors $(Q_1, P_1), \dots, (Q_N, P_N) \sim (Q, P)$. We assume that $\mathrm{Var}(Q) = \mathrm{Var}(P)$. Their common value is called Alice's variance, or *modulation variance*, and is denoted by $V_A$. Then, Alice prepares $N$ coherent states $|\alpha_1\rangle, \dots |\alpha_N\rangle$, with

$$\alpha_k = \frac{q_k + jp_k}{2} \tag{2.1}$$

for $i = 1, \dots, N$. As developed in Appendix A.3, the variance of the quadrature operators on the set of coherent states is

$$\mathrm{Var}(\hat{q}_A) = \mathrm{Var}(\hat{p}_A) = V_A + 1 \tag{2.2}$$

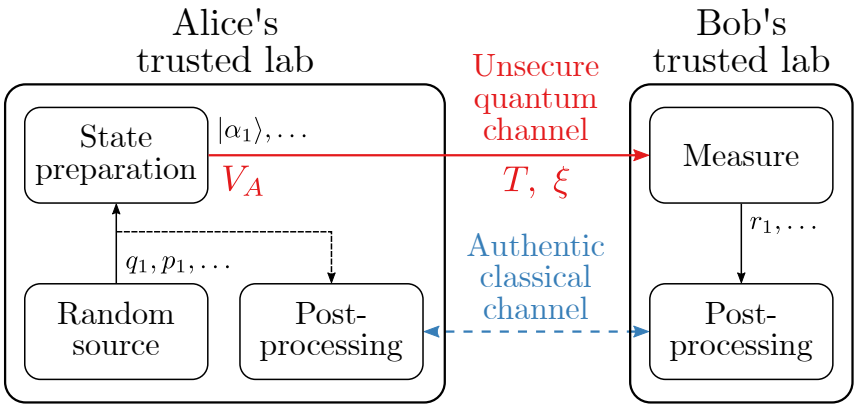



Figure 2.1: Schematic view of a the GG02 CV-QKD protocol, as described in 2.1.1.

where 1 can be interpreted as the variance of the vacuum fluctuation. Finally, Alice sends the coherent states to Bob through an insecure quantum channel. The quantum channel is formally represented by a map $\mathcal{N}$ between spaces of operators on Hilbert spaces.

**(ii) Measure** At the other side of the channel $\mathcal{N}$, Bob receives quantum states $\rho_1, \ldots, \rho_N$ where $\rho_k$ is a density matrix defined by

$$\rho_k = \mathcal{N}(|\alpha_k\rangle\langle\alpha_k|). \tag{2.3}$$

For each received state, he measures either one quadrature chosen at random or both quadrature simultaneously. For the latter, each state $\rho_k$ is split using a 50-50 beam splitter. Therefore, Bob obtains a string of either $N$ or $2N$ real values, which are noisy version of Alice's values $q_1, p_1, \ldots, q_N, p_N$. If Bob measured only one quadrature, he communicates to Alice his choice of basis and Alice keeps only the relevant values. At the end of step (ii), both Alice and Bob have a string of either $N$ or $2N$ real variables correlated to each other.

**(iii) Parameter estimation** Then, Alice and Bob communicate using an authenticated classical channel to obtain an estimation of the insecure quantum channel. Assuming that Eve is subject to the laws of quantum physics, they can obtain from this estimate a bound on the amount of information leaked to Eve. Thus, they are able to compute the length $l$ of the secret key that they can obtain after classical post-processing. Computing the key length from data measurable by Alice and Bob is the main focus of security proofs for CV-QKD. This chapter is intended to summarize the theoretical arguments of these proofs, as well as the practical calculation for obtaining the length $l$. Moreover, details on practical parameter estimation will be given in subsection 3.5.4.

**(iv) Classical post-processing** Finally, Alice and Bob apply classical post-processing techniques in order to extract a shared secret from their correlated data. The first step of this post processing, called *reconciliation*, is an error correcting

process at the end of which Alice and Bob share a common error-less bit string with a very high probability. However, it is not yet private, as Eve may have some information about the string. That's why Alice and Bob perform a *privacy amplification* protocol. They compress their bit string into a smaller one of length $l$, using 2-hashing functions in such a way that Eve's knowledge is reduced to a negligible amount [53].

There are actually two paradigms for reconciliation. On the one hand, *direct reconciliation* is close to classical error correction in that Bob attempts to correct detection errors to retrieve the actual data sent by Alice. Unfortunately, this scheme comes with the limitation that the channel attenuation cannot be greater than 3 dB [38]. On the other hand, *reverse reconciliation* doesn't exhibit this limitation and offers better performance, except for very short distances [54]. In this paradigm, the reference symbols are Bob's and Alice tries to guess their values. In fact, Alice and Bob have agreed on a linear error correcting code beforehand. Bob computes the syndromes of the received data, communicates them to Alice, who then performs classical error correction.

### 2.1.2 Similarities with classical optical transmissions

The first two steps of the protocol consist in sending information from Alice to Bob in the form of quadratures of a coherent light beam. In this respect, they are similar to digital transmission techniques using coherent optics. This similarity is a significant advantage of CV-QKD compared to DV-QKD. Indeed, it allows to take advantage of the considerable advances in the field of coherent optical transmission. In particular, CV-QKD can use commercially available equipment and state-of-the-art signal processing and coding techniques. Chapter 3 will provide more relevant details on modern coherent optical transmissions for CV-QKD.

Let's introduce some useful vocabulary. In coherent optical transmission, a source of bits is encoded in the form of points in the phasor diagram, called *symbols*, which are modulated onto a light wave. The symbols take their values from a certain subset of points, called the *constellation*. The statistical distribution of the symbols over the phasor diagram is called the *modulation format*, or modulation. In the previously described protocol, the symbols are the $(q_k + jp_k)$ and the modulation is the distribution of the random variable $(Q + jP)$.

Let's emphasize that the protocol presented in this section doesn't make any assumption on the probability distribution of the random vector $(Q, P)$, i.e. on the modulation format of the signal. In fact, modulation formats for CV-QKD are the main focus of this thesis. In the rest of this chapter, we analyze the security of the protocol under Gaussian modulation or arbitrary modulation with a finite number of points. The first case is the most studied and many security proofs are available in the asymptotic case [55, 56, 57]. Some progress has also been made towards realistic finite-size security [48]. The second case has been treated in a paper published in 2021, in the asymptotic case with the assumption of a collective attack [5]. Let's mention here the existence of security demonstrations for discrete modulation formats such as QPSK [3, 4, 58] or M-PSK [59].

### 2.1.3 Security assumptions

The security of a CV-QKD protocol is to be proven under given assumptions. Let's review some of the typical assumptions considered. As already mentioned, Eve can listen to and control the quantum channel. More precisely, it is assumed that Eve is able to prepare arbitrary ancillary states that can interact with the transmitted coherent states from Alice. Moreover, she may store the ancillary states in a quantum memory and measure them later in time. This way, she may take advantage of the information shared on the classical channel during the post-processing steps. In fact, three types of attacks are typically considered in the security analysis.

**Individual attack** Eve performs independent and identically distributed (i.i.d.) attacks on the coherent states, i.e. she prepares separable ancillary states, each of which interacts with only one transmitted coherent state. Then, Eve stores the ancillary states in a quantum memory until the end of step (ii). Finally, she measures the states independently from one another, before post-processing.

**Collective attack** Similarly, Eve performs an i.i.d. attack with separable ancillary states and stores the states in a quantum memory. However contrary to an individual attack, she performs optimal collective measurement on all ancillary states (not necessary i.i.d). Moreover, the measurement may be done after post-processing.

**Coherent attack** It is the most general attack. In fact, no additional assumption is made. In particular, Eve may prepare an optimal global ancillary state, with potentially mutual independent modes, interacting with the transmitted coherent states. Similarly to a collective attack, the modes are stored and an optimal collective measurement may be done after post-processing.

**Asymptotic security** In addition to the assumption on Eve's attack, we can analyze either the security in the *asymptotic* limit, i.e. with $N$ going to infinity, or with a more realistic *finite-size* hypothesis, i.e. assuming a finite number of transmitted coherent states. Even though unrealistic, the asymptotic security is simpler to derive and gives an upper bound on the length of the key with finite-size. In this thesis, we will derive calculation for asymptotic security. Moreover, we use a simple approach to finite-size using a statistical worst-case estimator for the excess noise. This method will be described in Section 2.7.

### 2.1.4 Secret key rate

The security analysis of the protocol aims at giving the size $l$ of the secret key that Alice and Bob can generate. In the case of asymptotic security, rather than the size of the key, we are interested in the secret key rate $K$ (SKR), i.e. the number of secret bits per second that the protocol can produce. It is typically given by

$$K = f_S \times r \tag{2.4}$$

where $f_S$ is the symbol rate, that is the number of coherent states (or symbols) transmitted per second, and $r$ the *secret fraction*, that is the number of secret bits

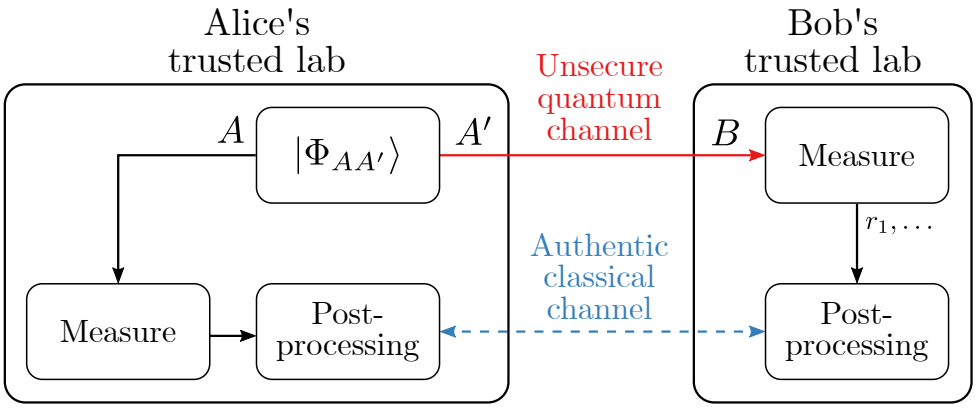



Figure 2.2: Schematic view of a the EB protocol based on a bipartite quantum state, theoretically equivalent to the PM protocol.

that can be extracted for each transmitted symbol. Let's note that, with notations from subsection 2.1.1, we have $r = \frac{l}{N}$. The rest of this chapter will detail the calculation of the secret fraction $r$.

## 2.2 Entanglement-based protocol

For security analysis, we introduce an equivalent protocol to the prepare and measure one described in subsection 2.1.1. In this equivalent protocol, in place of coherent states $|\alpha\rangle$, Alice prepares bipartite quantum states $|\Phi_{AA'}\rangle$. For each bipartite state, Alice measure the first mode $A$ and sends the second one $A'$ to Bob over the quantum channel $\mathcal{N}_{A'\to B}$ for measurement. For the two protocols to be equivalent, Alice's measurement must project the second mode A' into a statistical mixture of coherent states corresponding to the modulation format of the PM protocol. The bipartite state shared by Alice and Bob after each channel use is given by

$$\rho_{AB} = (\mathrm{Id}_A \otimes \mathcal{N}_{A'\to B})(|\Phi_{AA'}\rangle\langle\Phi_{AA'}|) \tag{2.5}$$

where $\mathrm{Id}_A$ stands for the identity operator on mode $A$. The quantum memory of Eve, denoted by E, is in a state $\rho_E$. We can assume without loss of generality that the state $\rho_{ABE}$ shared by the three parties is a purification of $\rho_{AB}$, and $\rho_E = \mathrm{Tr}_{AB}(\rho_{ABE})$. Figure 2.2 illustrates the EB protocol.

### 2.2.1 Devetak-Winter formula

We assume that Eve performs collective attacks. In other words, the bipartite states shared by Alice and Bob after each channel use are independent and identically distributed. In this framework, we can use the *Devetak-Winter formula* [60], which asserts that the asymptotic secret fraction $r$ is given by

$$r = I(X;Y) - \sup_{\mathcal{N}_{A'\to B}} S(E;Y). \tag{2.6}$$

Let's comment on this formula. $X$ and $Y$ are classical complex random variables corresponding to the random data of respectively Alice and Bob after their respective

measurements. The term $I(X;Y)$ refers to the classical mutual information between random variables $X$ and $Y$. It quantifies the amount of information shared by Alice and Bob before post-processing, in bits. The term $S(E;Y)$ is the Holevo information between Eve's quantum memory $E$ and the classical random variable $Y$. It quantifies the amount of information accessible to Eve on Bob's classical data. This quantity depends on the channel controlled by Eve, that's why the supremum in (2.6) is computed over all possible choices for $\mathcal{N}_{A'\to B}$. Since Alice and Bob detain some information on the channel, thanks to their respective measurements, the possible channels are those compatible with these measurements.

**Reconciliation efficiency** It is known that practical implementations of error correcting codes cannot retrieve the total of the mutual information $I(X;Y)$. A simple revision of the formula allows to take into account this limitation. We replace Equation (2.6) by

$$r = \beta I(X;Y) - \sup_{\mathcal{N}_{A'\to B}} S(E;Y), \tag{2.7}$$

where $\beta \in [0,1]$ is the *reconciliation efficiency* i.e. the ratio between the mutual information after error correction and $I(X;Y)$. Let's note that modern coding techniques allow to achieve reconciliation efficiency $\beta \geq 0.95$.

**Reduction to collective attacks** Arguments involving symmetry properties of the protocol or the use of a de Finetti representation theorem for infinite dimensions allows to reduce coherent attacks to collective attacks for asymptotic security [61, 62]. In other words, collective attacks are optimal in the asymptotic limit. This consideration justifies the assumption made at the beginning of this subsection.

### 2.2.2 Optimal property of Gaussian states

The calculation of the supremum of the Holevo information typically relies on the optimal property of Gaussian states [63, 64]. It asserts that $\sup_{\mathcal{N}_{A'\to B}} S(E;Y)$ is upper bounded by the Holevo information of a Gaussian state $\rho^G_{AYE}$ which is characterized by the same first moment and covariance matrix as those of the state $\rho_{AYE}$. With that in mind, we can replace Equation (2.7) by the following bound on the secret fraction,

$$r \geq \beta I(X;Y) - \chi(E;Y), \tag{2.8}$$

where $\chi(E;Y)$ is the Holevo information of the Gaussian state $\rho^G_{AYE}$, sometimes referred to as the Holevo bound. In the following subsection, we will see that $\chi(E;Y)$ is actually a function of the covariance matrix of the bipartite state $\rho_{AB}$ shared by Alice and Bob.

The optimal property of Gaussian states asserts that it is always safe to assume $\rho_{AB}$ to be a Gaussian state when computing the secret key rate. However, it isn't equivalent to saying that Gaussian attacks are optimal i.e. that the best choice of channel $\mathcal{N}_{A'\to B}$ is a Gaussian one. In fact, we will see that Gaussian attacks are optimal when the modulation is Gaussian, but not necessarily for finite size modulations.

### 2.2.3 An expression for the Holevo bound

In the following, we derive an expression of the Holevo bound $\chi(E;Y)$. We assume that Eve performs a Gaussian attack, such that all considered states are Gaussian. The Holevo bound $\chi(E;Y)$ is therefore the Holevo information $S(E;Y)$ of the quantum state $\rho_{AYE}$, which is given by

$$\chi(E;Y) = S(E) - S(E|Y) \tag{2.9}$$

where $S(E)$ is the von Neumann entropy of Eve's quantum register $E$ and $S(E|Y)$ the von Neumann entropy of $E$ after Bob's projective measurement. Since $\rho_{ABE}$ is assumed to be a purification of $\rho_{AB}$, the properties of the von Neumann entropy give that

$$\chi(E;Y) = S(AB) - S(AB|Y). \tag{2.10}$$

where $S(AB)$ and $S(AB|Y)$ are the von Neumann entropies of the quantum state shared by Alice and Bob respectively before and after Bob's measurement. They are both functions of the covariance matrix $\Gamma_{AB}$ of the state $\rho_{AB}$ before Bob's measurement. Symmetry arguments show that we can assume without loss of generality $\Gamma_{AB}$ to be of the following form [55],

$$\Gamma_{AB} = \begin{bmatrix} VI_2 & Z\sigma_z \\ Z\sigma_z & WI_2 \end{bmatrix}, \tag{2.11}$$

where $I_2$ is the identity matrix of size $2 \times 2$, $\sigma_z = \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$ is the third Pauli matrix and $V$, $W$ and $Z$ are real numbers given by

$$V = \frac{1}{2}(\langle \hat{q}_A^2 \rangle + \langle \hat{p}_A^2 \rangle) = 1 + 2\,\mathrm{Tr}(\rho_{AB}\hat{a}^\dagger \hat{a}) \tag{2.12}$$

$$W = \frac{1}{2}(\langle \hat{q}_B^2 \rangle + \langle \hat{p}_B^2 \rangle) = 1 + 2\,\mathrm{Tr}(\rho_{AB}\hat{b}^\dagger \hat{b}) \tag{2.13}$$

$$Z = \frac{1}{4}(\langle \{\hat{q}_A, \hat{q}_B\} \rangle - \langle \{\hat{p}_A, \hat{p}_B\} \rangle) = \mathrm{Tr}(\rho_{AB}(\hat{a}\hat{b} + \hat{a}^\dagger \hat{b}^\dagger)), \tag{2.14}$$

where $(\hat{a}, \hat{a}^\dagger)$ and $(\hat{b}, \hat{b}^\dagger)$ are respectively the annihilation and creation operators of modes $A$ and $B$, and $\{\hat{u}, \hat{v}\} = \hat{u}\hat{v} + \hat{v}\hat{u}$ denotes the anti-commutator between operators. $V$ and $W$ are the variances of the quadrature operators of respectively Alice's and Bob's states while $Z$ can be understood as quantifying their correlation. The von Neumann entropy of a Gaussian state can be expressed using the eigenvalues of its covariance matrix, as discussed in Appendix A.2. Using this property, we obtain the following expression for $\chi(E;Y)$,

$$\chi(E;Y) = g\Big(\frac{\nu_1 - 1}{2}\Big) + g\Big(\frac{\nu_2 - 1}{2}\Big) - g\Big(\frac{\nu_3 - 1}{2}\Big), \tag{2.15}$$

where $g$ is the function given by

$$g(x) = (x+1)\log_2(x+1) - x\log_2(x), \tag{2.16}$$

and $\nu_1$ and $\nu_2$ are symplectic eigenvalues of the matrix $\Gamma_{AB}$, and $\nu_3$ is the symplectic eigenvalue of $\Gamma_{AB|Y}$, the covariance matrix of $\rho_{AB}$ after Bob's projective

measurement. Since Bob's measurement is determined by the protocol, $\nu_3$ is actually a function of $\rho_{AB}$ which depends on the type of measurement involved. More details on Bob's projective measurements will be given in Section 2.5, including an introduction of trusted detection imperfections.

### 2.2.4 Practical evaluation of the Holevo bound

Equation (2.15) offers a convenient way to derive the Holevo bound $\chi(E;Y)$ when the covariance matrix $\Gamma_{AB}$ is known. If Alice and Bob are able to directly measure the values $V$, $W$ and $Z$, then they can infer $\chi(E;Y)$ and get a bound on the secret fraction $r$. First of all, the values $V$ and $W$ are expressed as the sum of the variances of the local quadrature operators. Therefore, they are both locally observable by Alice and Bob in their respective lab. In fact, $V = V_A + 1$ depends only on the modulation variance $V_A$ set by Alice. Recovering the quantity $Z$ is possible in the EB protocol, when Alice and Bob can perform coherent detection on their respective modes. The unfortunate truth is that practical protocols are generally PM, not involving any entangled state. The state $\rho_{AB}$ is more of a theoretical tool useful to establish the security. Therefore it is in general not possible to directly evaluate $Z$. We will see in Section 2.3 that the protocol with a Gaussian modulation is an exception, where $Z$ can be estimated by Alice's transmitted symbols and Bob's measured values. For arbitrary modulation with a finite constellation, A. Denys, P. Brown and A. Leverrier derived a practical lower bound $Z^* \leq Z$. This will be the subject of 2.4.

## 2.3 Protocol with a Gaussian modulation

In the following section, we provide details on the CV-QKD protocol with a Gaussian modulation format.

### 2.3.1 Gaussian PM and EB protocol

In the PM protocol with a Gaussian modulation, random variables $Q$ and $P$ are independent and both following a centered normal distribution with variance $V_A$. Equivalently, $\alpha = (Q + jP)/2$ follows a circular complex Gaussian probability distribution with variance $V_A/2$. The density operator $\tau$ representing the statistical mixture of coherent states prepared by Alice is actually a thermal state with average photon number $\langle n \rangle = V_A/2$,

$$\tau = \frac{1}{V_A \pi} \int_{\mathbb{C}} \exp\Big(-\frac{|\alpha|^2}{V_A}\Big) |\alpha\rangle\langle\alpha| d\alpha \tag{2.17}$$

$$= \sum_{m=0}^{+\infty} \frac{\langle n \rangle^m}{(1 + \langle n \rangle)^{m+1}} |m\rangle\langle m| \tag{2.18}$$

where $|m\rangle$ detones the Fock state with $m$ photons. In the equivalent EB protocol with a Gaussian modulation, the bipartite state $|\Phi_{AA'}\rangle$ prepared by Alice is a two-mode squeezed vacuum state, also called Einstein-Podolsky-Rosen (EPR) state. It

is a Gaussian state with covariance matrix $\Gamma_{AA'}$ given by

$$\Gamma_{AA'} = \begin{bmatrix} (V_A+1)I_2 & \sqrt{V_A^2+2V_A}\sigma_z \\ \sqrt{V_A^2+2V_A}\sigma_z & (V_A+1)I_2 \end{bmatrix}, \tag{2.19}$$

where $I_2$ is the identity matrix of size 2, and $\sigma_z = \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$ is the third Pauli matrix. The fact that $\rho_{AA'}$ is Gaussian simplifies the derivation of the Holevo bound and its experimental evaluation. The EB protocol with an EPR state has been extensively studied in the literature [57, 56]. Its security analysis typically relies on the study of Gaussian channels [65].

### 2.3.2 Gaussian attack and covariance matrix

The fact that the states prepared by Alice are Gaussian states drastically simplifies the security analysis and practical derivation of the secret key rate. In fact, the optimal property of Gaussian states used in subsection 2.2.2 implies that Gaussian attacks are optimal in that case. Therefore, we can bound $\chi(E;Y)$ by its value when considering a Gaussian attack. We model the channel by a thermal noise channel characterized by two parameters that will play a critical role in the following analysis:

- the *transmittance* $T$, which quantifies the attenuation of the channel (typically that of an optical fiber)
- the *excess noise* variance $\xi$, which is the variance of an additive white Gaussian noise introduced in the channel

After transmission of mode $A'$ through this thermal noise channel, the covariance matrix $\Gamma_{AB}$ is given by

$$\Gamma_{AB} = \begin{bmatrix} (V_A+1)I_2 & \sqrt{T(V_A^2+2V_A)}\sigma_z \\ \sqrt{T(V_A^2+2V_A)}\sigma_z & (TV_A+1+\xi)I_2 \end{bmatrix}. \tag{2.20}$$

We can compute its eigenvalues $\nu_1$ and $\nu_2$ as well as quantity $\nu_3$, and derive the Holevo bound using Equation (2.15). The main advantage of the covariance matrix in Equation (2.20) is that it can be directly evaluated using Alice's data and Bob's measured values. The practical evaluation of $\Gamma_{AB}$ in the PM protocol consists in estimating the transmittance $T$ and the excess noise variance $\xi$, while calibrating the shot noise variance. More details on this process will be given in subsection 3.5.4.

Let's emphasize that rather than estimating the covariance matrix Alice and Bob would obtain with an entangled state and the actual channel, they estimate the covariance matrix of such an entangled state but in the case of an optimal attack from Eve. Thus, they get an upper bound on the actual Holevo bound obtained with the optimal property of Gaussian states. In any case, their final estimation of the secret fraction $r$ is correct.

## 2.4 Protocol with an arbitrary finite-size constellation

### 2.4.1 Statement of the problem

In the following, we are interested in the security of the protocol for arbitrary finite-size constellations. We assume that the random vector $(Q, P)$ takes values $(q_k, p_k)_{k=1,\dots,M}$ with probability distribution $(\pi_k)_{k=1,\dots,M}$. Therefore, the states prepared by Alice in the PM protocol can be conveniently described by the density matrix

$$\tau = \sum_{k=1}^{M} \pi_k |\alpha_k\rangle\langle\alpha_k| \tag{2.21}$$

where $\alpha_k = (q_k + jp_k)/2$. The bipartite state $|\Phi_{AA'}\rangle$ of the EB protocol is a purification of the density matrix $\tau$. As mentioned in subsection 2.2.3, we are interested in evaluating the covariance matrix $\Gamma_{AB}$ of the bipartite state shared by Alice and Bob. The main challenge is the evaluation of the complex number $Z = \mathrm{Tr}(\rho_{AB}\hat{C})$ where

$$\hat{C} = \hat{a}\hat{b} + \hat{a}^\dagger\hat{b}^\dagger \tag{2.22}$$

This quantity cannot be directly evaluated in the PM protocol. Unlike for the Gaussian modulation protocol, Gaussian attacks are not optimal and we cannot obtain a practical bound on $\chi(E;Y)$ using a Gaussian channel assumption. However, we can obtain an upper bound on $\chi(E;Y)$ by replacing $Z$ with a more practical lower bound $Z^*$ in the covariance matrix of Equation (2.11), and using Equation (2.15).

### 2.4.2 Lower bound on $Z$

S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier proposed a way to find a lower bound on $Z$ by expressing it as the objective function of a semidefinite program [3]. They established such a bound in the case of a QPSK modulation. Finally, A. Denys, P. Brown, and A. Leverrier solved a similar semidefinite program to obtain a practical bound $Z^* \leq Z$ for any finite size modulation [5]. The lower bound is given by

$$Z^* := 2c_1 - 2w^{\frac{1}{2}}\Big(n_B - \frac{c_2^2}{\langle n\rangle}\Big)^{\frac{1}{2}} \tag{2.23}$$

where $w$ and $\langle n\rangle$ are defined by the protocol, and $n_B$, $c_1$ and $c_2$ are quantities experimentally accessible to Bob in the PM protocol. Let's provide the definition of these quantities. First of all, $\langle n\rangle$ is simply the average number of photons of the states prepares by Alice, $\langle n\rangle = \sum_k \pi_k|\alpha_k|^2$, and $w$ is a parameter depending only on the density matrix $\tau$, given by

$$w := \pi_k\big(\langle\alpha_k|a_\tau^\dagger a_\tau|\alpha_k\rangle - |\langle\alpha_k|a_\tau|\alpha_k\rangle|^2\big), \tag{2.24}$$

where $\hat{a}_\tau$ is the operator defined by

$$\hat{a}_\tau := \tau^{\frac{1}{2}}\hat{a}\tau^{-\frac{1}{2}}. \tag{2.25}$$

The expression of $Z^*$ also introduces three experimental parameters. The first one is linked to the second moment of the received state,

$$n_B := \langle\hat{n}_B\rangle = \mathrm{Tr}(\rho_{AB}\hat{b}^\dagger\hat{b}), \tag{2.26}$$

and the other ones are linked to the first moment of the received states,

$$c_1 := \frac{1}{2}\,\mathrm{Tr}\Big(\rho_{AB}\big(\sum_k \overline{\langle\alpha_k|\hat{a}_\tau|\alpha_k\rangle}|\psi_k\rangle\langle\psi_k|\otimes\hat{b}+\mathrm{h.c.}\big)\Big), \tag{2.27}$$

$$c_2 := \frac{1}{2}\,\mathrm{Tr}\big(\rho_{AB}\big(\sum_k \bar{\alpha}_k|\psi_k\rangle\langle\psi_k|\otimes\hat{b}+\mathrm{h.c.}\big)\big), \tag{2.28}$$

where h.c. denotes the Hermitian conjugate operator and $(|\psi_k\rangle)_{k=1,\dots,M}$ is an orthonormal basis of Alice's mode $A$ such that

$$|\phi_{AA'}\rangle = \sum_{k=1}^{M}\sqrt{\pi_k}|\psi_k\rangle\otimes|\alpha_k\rangle. \tag{2.29}$$

### 2.4.3 Experimental evaluation of the parameters

In the PM protocol, Bob can experimentally evaluate the first moment of the received states when Alice has sent coherent state $|\alpha_k\rangle$,

$$\beta_k := \mathrm{Tr}(\rho_k\hat{b}), \tag{2.30}$$

where $\rho_k = \mathcal{N}_{A'\to B}(|\alpha_k\rangle\langle\alpha_k|)$, as well as the second moment $n_B$. In fact, for each coherent state $|\alpha_k\rangle$ in the modulation format, Bob measure $N$ values $\beta_{k,i} = \frac{1}{2}(q_{k,i} + jp_{k,i})$ where $q_{k,i}$ and $p_{k,i}$ are measured values of the quadratures of mode $B$ (before beam-splitting for heterodyne detection). Then Bob can estimate $\beta_k$ and $n_B$ using the following consistent estimators,

$$\frac{1}{N}\sum_{k,i}\beta_{k,i} \xrightarrow[N\to+\infty]{} \beta_k, \tag{2.31}$$

$$\frac{1}{N}\sum_{k,i}\pi_k|\beta_{k,i}|^2 \xrightarrow[N\to+\infty]{} n_B+1 \tag{2.32}$$

Finally, the quantities $c_1$ and $c_2$ can be experimentally estimated as in the following,

$$c_1 = \mathrm{Re}\big(\sum_k \pi_k\overline{\langle\alpha_k|\hat{a}_\tau|\alpha_k\rangle}\beta_k\big), \tag{2.33}$$

$$c_2 = \mathrm{Re}\big(\sum_k \pi_k\bar{\alpha}_k\beta_k\big). \tag{2.34}$$

### 2.4.4 For a Gaussian channel

Finally, we provide the values of $Z^*$ for a thermal noise channel, introduced in subsection 2.3.2, with transmittance $T$ and excess noise variance $\xi$. In that case, the $\beta_{k,i}$ are given by

$$\beta_{k,i} = \sqrt{T}\alpha_k + \gamma_{k,i} \tag{2.35}$$

where $(\gamma_{k,i})$ is an additive white Gaussian noise with variance $1 + T\xi/2$ accounting for both the shot noise and excess noise. Then, we obtain the values for $c_{1,2}$ and $n_B$,

$$c_1 = \sqrt{T}\,\mathrm{Tr}(\bar{\tau}^{\frac{1}{2}}\hat{a}\bar{\tau}^{\frac{1}{2}}\hat{a}^\dagger), \tag{2.36}$$

$$c_2 = \sqrt{T}\langle n\rangle, \tag{2.37}$$

$$n_B = T\langle n\rangle + T\frac{\xi}{2}, \tag{2.38}$$

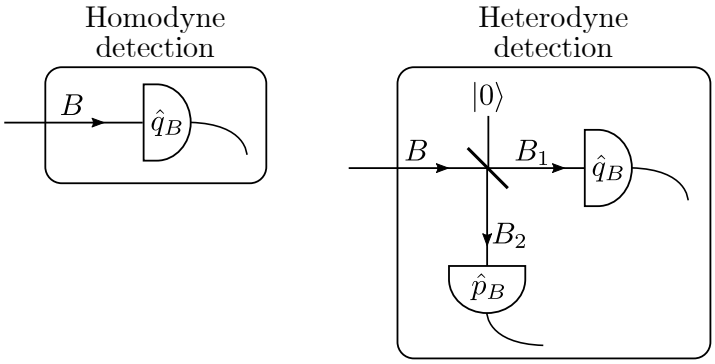



Figure 2.3: Schematic views of homodyne and heterodyne detection of Bob's received mode $B$.

and consequently the bound $Z^*$ is given by

$$Z^* = 2\sqrt{T}\,\mathrm{Tr}(\bar{\tau}^{\frac{1}{2}}\hat{a}\bar{\tau}^{\frac{1}{2}}\hat{a}^\dagger) - \sqrt{2T\xi w}. \tag{2.39}$$

## 2.5 Projective measurement and trusted imperfections

### 2.5.1 Homodyne and heterodyne detection

Depending on the protocol, Bob may measure only one quadrature or both quadratures for each received state. In quantum information, the former is called homodyne detection and the latter heterodyne detection. Figure 2.3 illustrates these two types of detection. For homodyne detection, Bob directly performs a projective measurement, either $\hat{q}_B$ or $\hat{p}_B$ on the received mode. For heterodyne detection, Bob splits mode $B$ into $B_1$ and $B_2$ using a 50-50 beam splitter and performs a projective measurement on each output mode. Section 3.3 will provide details on the practical implementation of these measurements.

In this subsection, we are interested in their description in terms of quantum mechanics, and their impact on the secret key rate. We remind that the covariance matrix $\Gamma_{AB}$ of the state $\rho_{AB}$ shared by Alice and Bob before the measurement is given in Equation (2.11), and that the Holevo bound $\chi(E;Y)$ is given by Equation (2.15). In particular, it involves the quantity $\nu_3$ which is in fact the symplectic eigenvalue of the covariance matrix $\Gamma_{A|Y}$ of Alice's state after Bob's detection, either homodyne or heterodyne. If Bob performs a homodyne measurement, then $\Gamma_{A|Y}$ is given by

$$\Gamma_{A|Y}^{hom} = \begin{bmatrix} V - \frac{Z^2}{W} & 0 \\ 0 & W \end{bmatrix}, \tag{2.40}$$

and its symplectic eigenvalue is,

$$\nu_3^{hom} = \sqrt{W\Big(V - \frac{Z^2}{W}\Big)} \tag{2.41}$$

In the case of a heterodyne measurement, Bob splits the received states using a 50-50 beam splitter and performs a measurement on each output. The resulting

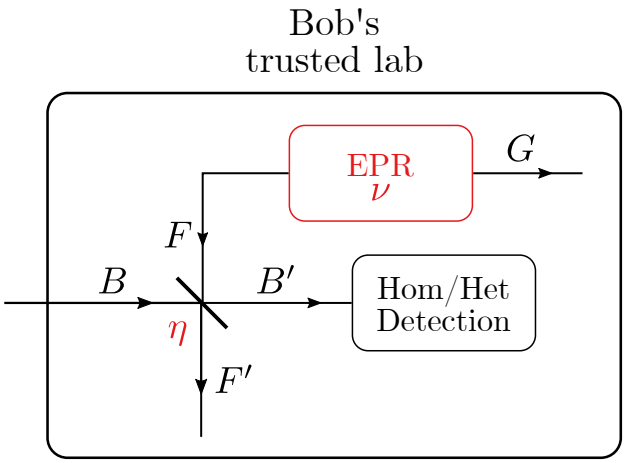



Figure 2.4: Schematic view of a the EPR model for a noisy and inefficient detector.

covariance matrix is

$$\Gamma_{A|Y}^{hom} = \begin{bmatrix} V - \frac{Z^2}{W+1} & 0 \\ 0 & V - \frac{Z^2}{W+1} \end{bmatrix}. \tag{2.42}$$

and its symplectic eigenvalue is

$$\nu_3^{het} = V - \frac{Z^2}{W+1}. \tag{2.43}$$

The calculation details of these covariance matrices can be found in Section 7 of reference [57].

### 2.5.2 Noisy and inefficient detectors

The above analysis assumed that Bob was able to do a perfect measurement of the quadratures. However, real detectors cannot detect all photons, their quantum efficiency is strictly lower than 1. Moreover, the electronical parts of the detectors are sensible to thermal noise, introducing an additional noise with variance $V_{el}$ in shot noise unit (SNU). In this subsection we are presenting a model to take into account these imperfections for the calculation of the Holevo bound. In fact, the covariance matrix $\Gamma_{AB}$ and its eigenvalues $\nu_1$ and $\nu_2$ are left unchanged, since they are given for the quantum state before measurement. The changes are on the value of $\Gamma_{A|Y}$ and its eigenvalue $\nu_3$.

The model for Bob's imperfect detector is illustrated in Figure 2.4. The loss of the detector is modeled by a beam splitter with transmittance $\eta$ between received mode $B$ and output $B'$. The quantity $\eta$, without unit, is typically the quantum efficiency of the photodetectors. The additional electronic noise is modeled using an EPR state $\rho_{FG}$ of variance $\nu$. Its first mode, denoted $F$, interacts with the received mode $B$ in the beamsplitter. The variance $\nu$ is such that the additive noise on the measurement has variance $V_{el}$. For a homodyne detection, $\nu = 1 + V_{el}/(1-\eta)$, and for a heterodyne detection, $\nu = 1 + 2V_{el}/(1-\eta)$. Note that Eve cannot interact with this state which is generated in Bob's lab; it is then said to be trusted. This model is often called the *trusted receiver* scenario.

The EPR state $\rho_{FG}$ has covariance matrix

$$\Gamma_{FG} = \begin{bmatrix} \nu I_2 & \sqrt{\nu^2-1}\sigma_z \\ \sqrt{\nu^2-1}\sigma_z & \nu I_2 \end{bmatrix}, \tag{2.44}$$

It is independent of the state $\rho_{AB}$, such that the covariance matrix of $\rho_{AB} \otimes \rho_{FG}$ is given by $\Gamma_{AB} \oplus \Gamma_{FG}$. The action of the beam splitter on the covariance matrix of modes $B$ and $F$ reads

$$Y_{BF}^{bs} = \begin{bmatrix} \sqrt{\eta} I_2 & \sqrt{1-\eta} I_2 \\ -\sqrt{1-\eta} I_2 & \sqrt{\eta} I_2 \end{bmatrix}. \tag{2.45}$$

We extend its action on $\rho_{AB} \otimes \rho_{FG}$ as $Y^{bs} = I_2 \oplus Y_{BF}^{bs} \oplus I_2$. Therefore, the output of the beamsplitter is the state $\rho_{AB'F'G}$ with covariance matrix

$$\Gamma_{AB'F'G} = (Y^{bs})^T (\Gamma_{AB} \oplus \Gamma_{FG}) Y^{bs} \tag{2.46}$$

By rearranging the columns and the rows, we obtain the covariance matrix

$$\Gamma_{AF'GB'} = \left[\begin{array}{c|c} \Gamma_{AF'G} & \sigma_{AF'GB'}^T \\ \hline \sigma_{AF'GB'} & \Gamma_{B'} \end{array}\right]. \tag{2.47}$$

We extract the $6 \times 6$ covariance matrix $\Gamma_{AF'G}$ and compute the projection $\Gamma_{AF'G|Y}$ after Bob's measurement (homodyne or heterodyne). The 3 eigenvalues of $\Gamma_{AF'G|Y}$ are denoted $\nu_3$, $\nu_4$ and $\nu_5$, with $\nu_5 = 1$. Finally, the Holevo bound $\chi(E;Y)$ is given by

$$\chi(E;Y) = g\Big(\frac{\nu_1 - 1}{2}\Big) + g\Big(\frac{\nu_2 - 1}{2}\Big) - g\Big(\frac{\nu_3 - 1}{2}\Big) - g\Big(\frac{\nu_4 - 1}{2}\Big). \tag{2.48}$$

The use of this trusted receiver scenario typically gives better secret key rate in experimental conditions. In fact, if we do not assume the receiver to be trusted, the attenuation and electronic noise are attributed to Eve. We have to consider a transmittance $T^{\text{untrusted}} = \eta T$, and an excess noise $\xi_B^{\text{untrusted}} = \xi_B + V_{el}$, leading to worse secret key rates. In a way, the trusted receiver scenario allows to distinguish between trusted attenuation $\eta$ and untrusted attenuation $T$, trusted excess noise $V_{el}$ and untrusted excess noise $\xi$.

## 2.6 Numerical results

As an illustration, let's provide some theoretical curves for the secret fraction obtained with the equations detailed in this chapter. More specifically, we are interested in the dependence of the secret fraction on the modulation variance $V_A$, or the distance between Alice and Bob for an optical fiber. Moreover we wish to compare the performance of the Gaussian modulation to finite size constellations. In fact, we expect the Gaussian modulation to provide the best secret key rates. Therefore, it is natural to introduce a discretized Gaussian modulation. An example of such discrete Gaussian modulations are probabilistically shaped QAM formats, or PCS-QAM, which are used in digital communications to approach the Shannon capacity. For a description of PCS-QAM modulation formats, the reader may refer to the first section of Chapter 3.

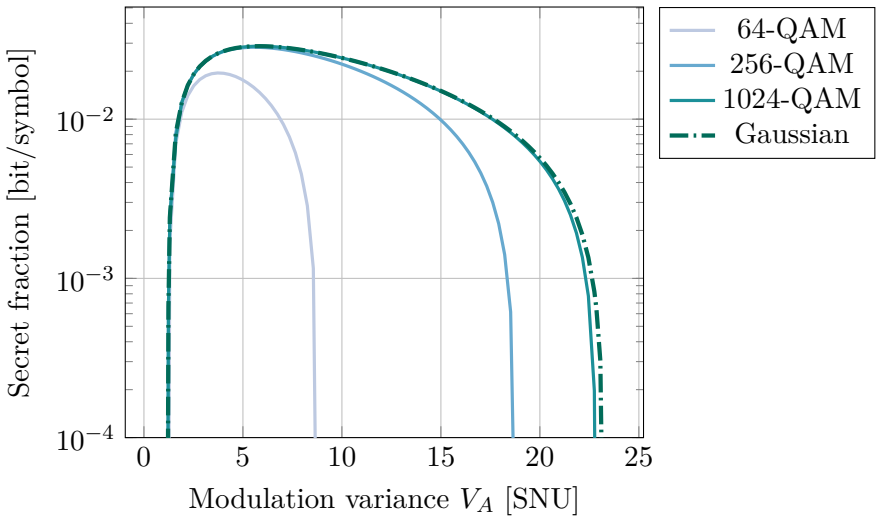



Figure 2.5: Secret fraction [bit/symbol] vs modulation variance $V_A$ [SNU] for a Gaussian channel with transmittance $T = -5\,\text{dB}$, corresponding to 25 km of single mode fiber, and excess noise variance $\xi_B = 0.01\,\text{SNU}$, trusted receiver with quantum efficiency $\eta = 0.65$ and electronic noise variance $V_{el} = 0.1\,\text{SNU}$, and reconciliation efficiency $\beta = 0.95$.

**Secret fraction vs modulation variance** Figure 2.5 shows the asymptotic secret fraction as a function of the modulation variance $V_A$, for a Gaussian channel with transmittance $T = -5\,\text{dB}$ and excess noise variance $\xi_B = 0.01\,\text{SNU}$, in the trusted receiver scenario for heterodyne detection with quantum efficiency $\eta = 0.65$ and electronic noise variance $V_{el} = 0.1\,\text{SNU}$, and assuming reverse reconciliation with efficiency $\beta = 0.95$. The excess noise variance $\xi_B$ is the variance observed by Bob during his measurement. In that case, it is linked to the excess noise variance $\xi$ of the Gaussian channel through $\xi_B = \frac{\eta T}{2}\xi$. The asymptotic secret fraction is given for a Gaussian modulation format, using the equations described in Section 2.3, and for PCS 64-QAM, PCS 256-QAM and PCS 1024-QAM, using the bounds derived in Section 2.4 and the formulas for a Gaussian channel.

We observe that the secret fraction for a PCS-QAM modulation tends to approach that of Gaussian modulation as the number of points in the constellation increases. Furthermore, for each modulation format, there is a modulation variance for which the secret fraction is maximum. As a practical consequence, Alice must be able to adjust the modulation variance of the protocol, and optimize it depending on the context. In fact, this optimal value depends on the parameters of the channel.

Let's note that the probability distribution of a PCS-QAM is defined for a given parameter $\nu \geq 0$, as defined in subsection 3.1.3. For each point of Figure 2.5, this parameter was chosen to maximize the secret fraction. Figure 2.6 illustrates with one example the dependence of the secret key rate on parameter $\nu$, for $V_A = 5\,\text{SNU}$. We observe that the function is in fact concave. Thus, an optimal value of the parameter clearly stands out.

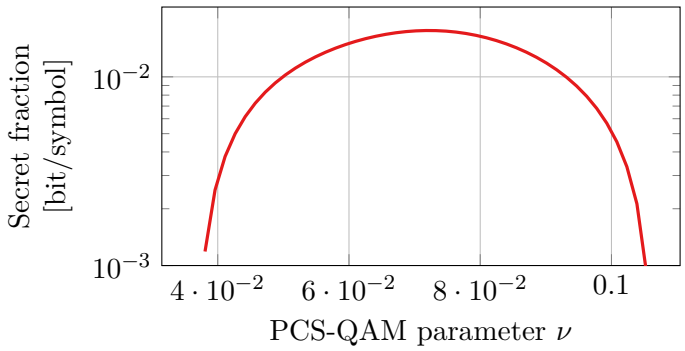



Figure 2.6: Secret fraction [bit/symbol] vs PCS-QAM parameter $\nu$ for a PCS 64-QAM at $V_A = 5\,\text{SNU}$ with parameters of Figure 2.5.

**Secret fraction vs distance** Figure 2.7 shows the asymptotic secret fraction as a function of the distance in km, for a single mode fiber with 0.2 dB/km loss. We assume a Gaussian channel with excess noise variance $\xi_B = 0.01\,\text{SNU}$, trusted receiver scenario for heterodyne detection with quantum efficiency $\eta = 0.65$ and electronic noise variance $V_{el} = 0.1\,\text{SNU}$, and reverse reconciliation with efficiency $\beta = 0.95$. Moreover, for each point in the Figure, the modulation variance $V_A$ is set to maximize the secret fraction.

We observe that the secret fraction decreases as the distance increases, with a maximum distance beyond which no secret fraction can be extracted during the protocol. Moreover, we observe that the secret fraction of the PCS 256-QAM is very close to that of the Gaussian modulation. That is because the modulation variance $V_A$ was optimized for each distance.

**Secret fraction vs excess noise** Figure 2.8 shows the asymptotic secret fraction as a function of the excess noise $\xi_B$, for a Gaussian channel with transmittance $T = -5\,\text{dB}$, in the trusted receiver scenario for heterodyne detection with quantum efficiency $\eta = 0.65$ and electronic noise variance $V_{el} = 0.1\,\text{SNU}$, and assuming reverse reconciliation with efficiency $\beta = 0.95$. For each point in the figure, the modulation variance $V_A$ is set to maximize the secret fraction.

When $\xi_B$ tends to 0, we observe that the secret fraction saturates to a maximum value. When $\xi_B$ increases, the secret fraction decreases until it drops to zero. We also observe that the performance of the PCS 256-QAM is almost indistinguishable from that of the Gaussian modulation.

## 2.7 Finite size analysis of parameter estimation

### 2.7.1 Parameter estimation for a Gaussian channel

Parameter estimation is used to measure the quantities useful for the calculation of the secret fraction. In this section, we give some practical considerations on how to estimate these parameters. We restrict ourselves to the hypothesis of a Gaussian channel, which is simpler to analyze in the non-asymptotic case. Moreover, we

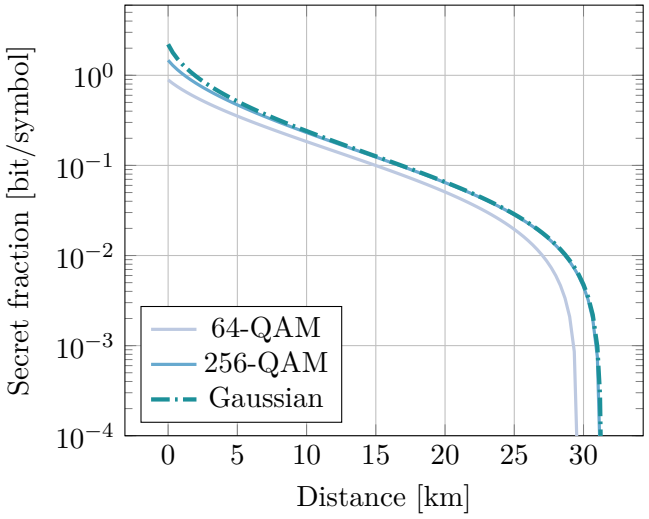



Figure 2.7: Secret fraction vs distance for a single mode fiber with 0.2 dB/km loss, assuming a Gaussian channel with excess noise variance $\xi_B = 0.01$ SNU, trusted receiver with quantum efficiency $\eta = 0.65$ and electronic noise variance $V_{el} = 0.1$ SNU, and reconciliation efficiency $\beta = 0.95$.

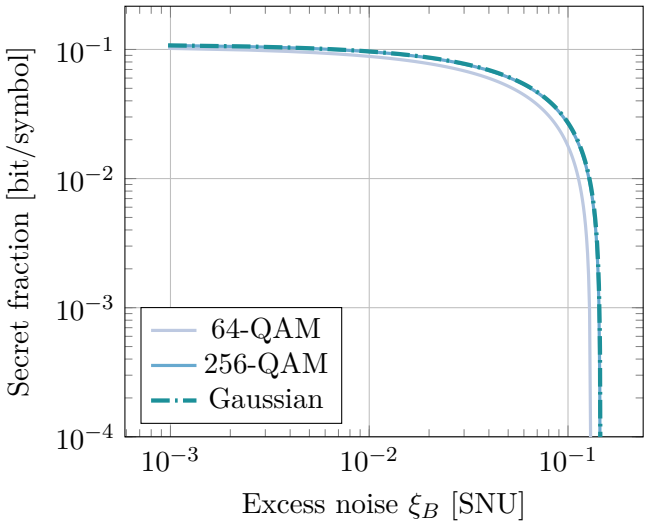



Figure 2.8: Secret fraction [bit/symbol] vs excess noise variance $\xi_B$ for PCS 64-QAM for Gaussian channel with transmittance $T = -5$ dB, trusted receiver with quantum efficiency $\eta = 0.65$ and electronic noise variance $V_{el} = 0.1$ SNU, and reconciliation efficiency $\beta = 0.95$.

place ourselves in the case of a trusted receiver and heterodyne detection, which will correspond to our experiments. Therefore, Bob measures both quadratures of each received state $\rho_k$. For each quadrature, he measures real numbers $(y_k)$,

$$y_k = \sqrt{\frac{\eta T}{2}} x_k + w_k \tag{2.49}$$

where $(x_k)$ are the corresponding transmitted real symbols with variance $V_A$ and $(w_k)$ is additive white Gaussian noise (AWGN) with variance $1 + V_{el} + \frac{\eta T}{2}\xi$. We assume that the the quantum efficiency $\eta$ has been calibrated before the protocol.

**Shot noise calibration** In fact, Bob measures values in [V] that are proportional to the quadrature values in shot noise units. Therefore, he needs to calibrate the variance of the shot noise in [V$^2$]. In practical systems, Bob typically disconnects the output of the channel from Alice and measures vacuum states $|0\rangle$ to obtain $N$ iterations of the detection noise $\tilde{w}_k$ accounting for both the shot noise and the electronic noise. Then, he records $N$ iterations of the electronic noise $\tilde{n}_k$. Using these measured values, he can estimate $N_0$ as well as $V_{el}$,

$$\hat{N}_0 = \widehat{\mathrm{Var}}(\tilde{w}) - \widehat{\mathrm{Var}}(\tilde{n}) \tag{2.50}$$

$$\hat{V}_{el} = \frac{1}{\hat{N}_0}\widehat{\mathrm{Var}}(\tilde{n}) \tag{2.51}$$

where $\widehat{\mathrm{Var}}(\cdot)$ stands for the unbiased consistent estimator of the variance. Let's remind that for $N$ samples $\{a_1, \ldots, a_N\}$, $\widehat{\mathrm{Var}}(a)$ is defined by

$$\widehat{\mathrm{Var}}(a) = \frac{1}{N-1}\sum_{k=1}^{N}(a_k - \bar{a})^2 \tag{2.52}$$

where $\bar{a} = \frac{1}{N}\sum_{k=1}^{N} a_k$ is the sample mean.

**Parameter estimation** Alice reveals $N$ symbols for parameter estimation. For the sake of simplicity, lets assume that she reveals the $N$ first symbols. Then, the transmittance $T$ can be estimated as

$$\hat{T} = \frac{2}{\eta}\frac{\sum_{k=1}^{N} x_k y_k}{\sum_{k=1}^{N} x_k^2}. \tag{2.53}$$

Moreover, the total noise $w_k$ can be decomposed as

$$w_k = s_k + n_k + \epsilon_k \tag{2.54}$$

where $(s_k)$, $(n_k)$ and $(\epsilon_k)$ are AWGN corresponding to respectively the shot noise, the electronic noise and the excess noise. Bob can estimate the variance $\sigma = \mathrm{Var}(w_k)$ of the total noise, and the variance $\sigma_0 = \mathrm{Var}(s_k + n_k) = \mathrm{Var}(\tilde{w}_k)$ of the trusted noise,

$$\hat{\sigma}^2 = \widehat{\mathrm{Var}}\Big(y - \sqrt{\frac{\eta\hat{T}}{2}}x\Big) \tag{2.55}$$

$$\hat{\sigma}_0^2 = \widehat{\mathrm{Var}}(\tilde{w}) \tag{2.56}$$

Finally, the excess noise estimator is given by

$$\hat{\xi}_B = \frac{\hat{\sigma}^2 - \hat{\sigma}_0^2}{\hat{N}_0}. \tag{2.57}$$

### 2.7.2 Worst case excess noise

A first simple approach to take into account finite size effects is to consider a worst case estimator for the excess noise variance $\xi_B$. We call worst-case excess noise a value $\hat{\xi}_B^{wc}$ such that the actual variance of the excess noise $\xi_B$ is lower than $\hat{\xi}_B^{wc}$ with probability $1-\epsilon$, where $\epsilon$ is the security parameter. It is derived as the upper bound of a statistical confidence interval of the form $]-\infty, \hat{\xi}_B^{wc}]$.

To simplify the derivation of the worst case estimator, we can assume that,

$$\hat{\sigma}^2 \approx \frac{1}{N}\sum_{k=1}^{N} w_k^2 \tag{2.58}$$

$$\hat{\sigma}_0^2 \approx \frac{1}{N}\sum_{k=1}^{N} \tilde{w}_k^2 \tag{2.59}$$

Therefore, the random variables $N\hat{\sigma}^2/\sigma^2$ and $N\hat{\sigma}_0^2/\sigma_0^2$ follow chi-squared distributions with $N$ degrees of freedom. Moreover, we assume that the true electronic variance $V_{el}$ is known. Therefore, $\hat{N}_0 \approx \sigma_0/(1+V_{el})$, and

$$\hat{\xi}_B \approx (1+V_{el})\frac{\hat{\sigma}^2}{\hat{\sigma}_0^2} - 1 - V_{el}. \tag{2.60}$$

This way, $\hat{\xi}_B$ is expressed with the random variable $\sigma_0\hat{\sigma}^2/(\sigma\hat{\sigma}_0^2)$ which follows a F-distribution with parameter $(N,N)$. As written above, $\sigma$ and $\sigma_0$ are the actual values of the variances estimated by $\hat{\sigma}$ and $\hat{\sigma}_0$. A $(1-\epsilon)100\%$ confidence interval for $\sigma_0\hat{\sigma}^2/(\sigma\hat{\sigma}_0^2)$ is given by

$$\frac{\sigma_0\hat{\sigma}^2}{\sigma\hat{\sigma}_0^2} \in \left]-\infty, F_{N,N}^{-1}(1-\epsilon)\right] \tag{2.61}$$

where $F_{N,N}^{-1}$ is the inverse cumulative distribution function of the F-distribution with parameter $(N,N)$. Finally, we obtain the confidence interval for $\xi_B$,

$$\xi_B \in \left]-\infty, \hat{\xi}_B + \left(F_{N,N}^{-1}(1-\epsilon) - 1\right)\frac{\hat{\sigma}^2}{\hat{N}_o}\right] \tag{2.62}$$

Then, the worst case excess noise is given by

$$\hat{\xi}_B^{wc} = \hat{\xi}_B + \left(F_{N,N}^{-1}(1-\epsilon) - 1\right)\frac{\hat{\sigma}^2}{\hat{N}_o}. \tag{2.63}$$

We can use $\hat{\xi}_B^{wc}$ as the variance of the excess noise at Bob's, when considering Gaussian attacks, to take into account statistical finite-size effects on parameter estimation.

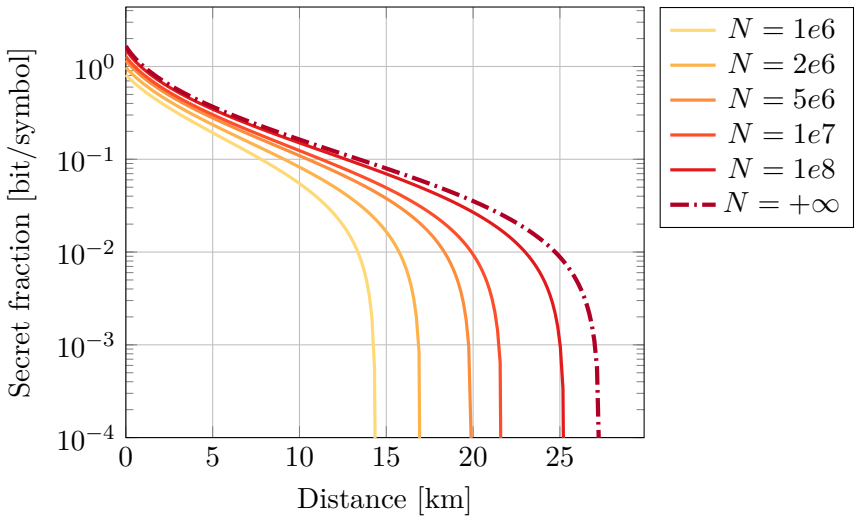



Figure 2.9: Theoretical finite-size secret fraction vs fiber link distance (with 0.2 dB loss per km), for a Gaussian modulation, with $\hat{\xi}_B = 0.01$, $\beta = 0.95$, $\eta = 0.5$, $V_{el} = 0.1$. The curves are computed using worst case excess noise $\xi_B^{wc}$ with $N$ symbols, with $N$ between $10^6$ and $+\infty$, and security parameter $\epsilon = 10^{-10}$.

**Discussion** Clearly, this method does not meet the standards required for a rigorous proof of the finite size case. However, in the absence of such a proof, it offers a simple and practical way to validate the possibility of a QKD protocol in finite size. The results provided by this method are more severe and realistic than those obtained with an asymptotic assumption. To illustrate this, Figure 2.9 gives theoretical curves for the secret fraction vs the fiber link distance (with 0.2 dB loss per km), for a Gaussian modulation, with $\epsilon = 10^{-10}$ and $\hat{\xi}_B = 0.01\,\text{SNU}$.

However, this approach can only be used for Gaussian attacks. For an arbitrary modulation format, using the calculation described in Section 2.4, the finite-size analysis should use worst-case estimators for the experimental parameters $\hat{c}_1$, $\hat{c}_2$ and $\hat{n}_B$. In fact, we have to derive the Holevo bound with $\hat{c}_1^{\min}$, $\hat{c}_2^{\min}$ and $\hat{n}_B^{\max}$ such that [5],

$$P(\hat{c}_1^{\min} \leq c_1) \geq 1 - \frac{\epsilon}{3}$$
$$P(\hat{c}_2^{\min} \leq c_2) \geq 1 - \frac{\epsilon}{3}$$
$$P(\hat{n}_B^{\max} \geq n_B) \geq 1 - \frac{\epsilon}{3}.$$

The following subsection presents a general method to derive a worst-case estimator.

### 2.7.3 General method to derive worst-case estimators

We first remark that, in addition to the estimators for $c_1$, $c_2$ and $n_B$, it can also be useful to derive a worst-case estimator for the transmittance $\hat{T}$, which is a lower bound in this case. Let us now introduce a general method to derive a worst-case estimator for an estimator $\hat{\theta}$. A typical estimator is expressed as the sum of a large

number $N$ of independent and identically distributed random variables. Therefore, it can be safely approximated by a normal distribution. Then, we can use the quantiles of the normal distribution. To use this method, we have to:

- Check that $\hat{\theta}$ is close to a normal distribution, using either the central limit theorem, or by Monte-Carlo simulations and normality tests.
- Compute the expected value of the estimator, typically given by a function $g(\theta)$ of the estimated quantity $\theta$. Make sure that $g(\theta)$ is strictly monotonic, either increasing or decreasing.
- Compute the variance $\sigma^2$, or obtain a numerical approximation using Monte-Carlo estimation.

Then, assuming that $g$ is strictly increasing, the worst-case estimators are given by

$$\hat{\theta}^{\max} = g^{-1}(\hat{\theta} + \sigma Q_{1-\epsilon}) \tag{2.64}$$

$$\hat{\theta}^{\min} = g^{-1}(\hat{\theta} - \sigma Q_{1-\epsilon}) \tag{2.65}$$

$$\tag{2.66}$$

where $Q_{1-\epsilon}$ is the $(1-\epsilon)$ quantile of the normal distribution with expected value 0 and variance 1. We have that

$$P(\hat{\theta}^{\max} \geq \theta) \geq 1 - \epsilon$$
$$P(\hat{\theta}^{\min} \leq \theta) \geq 1 - \epsilon.$$

If $g$ is decreasing, we have to invert the expressions for $\hat{\theta}^{\max}$ and $\hat{\theta}^{\min}$. In Appendix B, we propose to study statistical estimators of $T$, $c_1$, $c_2$ and $n_B$, to use with this method.

# Chapter 3

# Fundamentals of coherent optical transmissions for CV-QKD

This chapter deals with implementations (as well as possible impairments) of coherent optical communication that are relevant to the design of a CV-QKD system. The reader should be comfortable with fundamental concepts of digital communications. The newcomer will find a rigorous introduction to this topic in the textbook by A. Lapidoth [66].

## 3.1 Digital communication basics

### 3.1.1 Digital communication model

Digital communication consists in the transmission of messages in the form of bit strings between a sender and a receiver, regardless of the nature of the information (video, text, ...). The message is carried by a signal that travels through a physical medium, be it a copper wire, the air or an optical fiber. Physical transmission introduces signal distortion and noise whose impact on the message is modeled by a communication channel. Figure 3.1 gives a schematic view of such a digital communication system [67]. A source generates a string of bits that gets converted into a suitable signal thanks to a transmitter. After transmission through the communi-

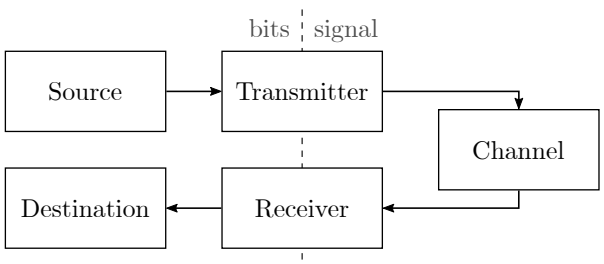



Figure 3.1: Schematic view of a general digital communication system.

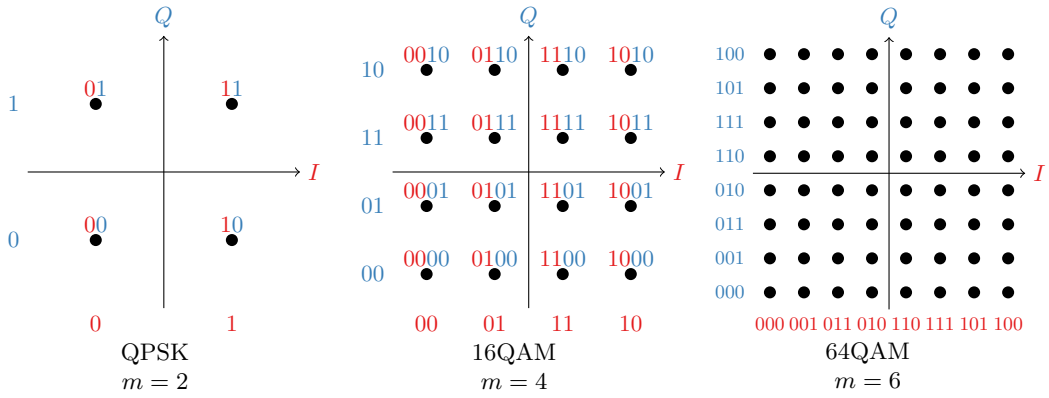



Figure 3.2: Regular $2^m$QAM constellations, for $m = 2$ (QPSK), $m = 4$ (16QAM) and $m = 6$ (64QAM)

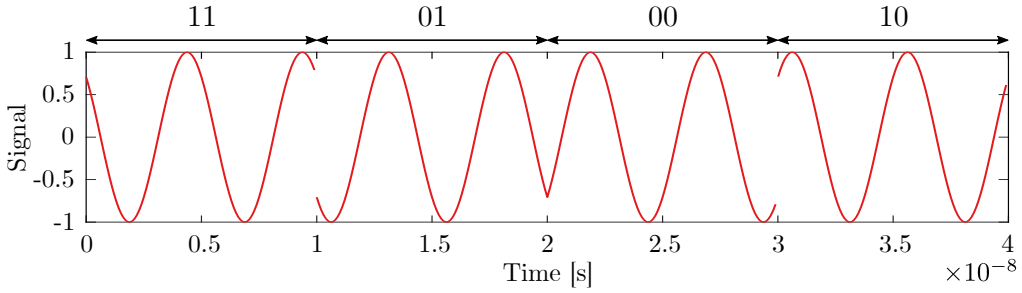



Figure 3.3: QPSK modulation of a 100 MBaud signal over a 200 MHz carrier.

cation channel, a receiver reads the noisy and distorted signal and converts it back into a string of bits. The transmitter and receiver typically include error correcting codes and digital signal processing to compensate for channel distortion and noise.

### 3.1.2 Digital modulation

The conversion from bits to a physical signal relies on digital modulation. Modulation is the process of encoding information in the physical properties of a periodic waveform, the signal *carrier*. Digital modulation typically encodes bits into discrete values of the phase and amplitude of the carrier. The process divides the bit string into codewords of size $m$. Each possible code word $x \in \{0,1\}^m$ is attributed to a given phase and amplitude, which can be represented by a point in the phasor diagram. The set of all points attributed to a codeword is called the constellation. Figure 3.2 gives several examples of classical constellations called Quadrature Phase Shift Keying (QPSK) and Quadrature Amplitude Modulation (QAM). Figure 3.3 illustrates the principle of QPSK modulation. The codewords 11, 01, 00, 10 are attributed to respectively phases $\pi/4$, $3\pi/4$, $5\pi/4$ and $7\pi/4$. The phase of a 200 MHz carrier waveform is changed every nanosecond, corresponding to symbol rate 100 MBaud.

The mapping of codewords to constellation points should be set to minimize the bit error rate. This is done by minimizing the Hamming distance between codewords

associated with neighboring points. Such mapping can be obtained using Gray codes [68]. A Gray code is a binary code such that two successive integers differ in only one bit. For instance, the standard binary representation associates 0, 1, 2, 3, etc, to binary numbers 000, 001, 010, 011, etc, while a Gray code can give 000, 001, 011, 010, etc. Figure 3.2 shows that each quadrature I and Q is coded with a Gray code. The final mapping is simply the concatenation of each quadrature. We can see that codewords associated to neighboring points only differ in one bit.

### 3.1.3 Approaching the Shannon capacity using probabilistic constellation shaping

Since the bits are encoded into points in the phase space, the channel can be modeled with a discrete input of complex numbers $(x_k)$ and output $(y_k)$. A classical model for the communication channel is the additive white Gaussian noise (AWGN) channel, where the output is given by

$$y_k = x_k + w_k, \tag{3.1}$$

where $(w_k)$ are independent and identically distributed random variables following a complex circular normal distribution. Claude Shannon demonstrated that the maximal information rate that such a channel can transmit, its capacity, is achieved when the $(x_k)$ are themselves independent and identically distributed random variables following a complex circular normal distribution. In that case, the mutual information $I(X;Y) = H(X) - H(Y|X)$ is equal to the well known Shannon capacity, expressed in $\mathrm{bit\,s^{-1}}$,

$$C = B \log_2(1 + SNR) \tag{3.2}$$

where $B$ is the bandwidth of the channel and $SNR$ the signal to noise power ratio.

Unfortunately, when the $(x_k)$ are independent and identically distributed with uniform distribution over a QAM constellation, the mutual information $I(X;Y)$ suffers a penalty with respect to the Shannon capacity [69]. Probabilistic constellation shaping was introduced to tackle this limitation. The idea is to use a non-uniform distribution over a QAM lattice, with a discrete Gaussian-like shape. The probability distribution of a PCS $M^2$-QAM is given by

$$p_\nu(x, y) \propto \exp(-\nu(x^2 + y^2)) \tag{3.3}$$

where $x, y \in \{-M+1, -M+3, \ldots, M-1\}$ and $\nu$ is a free parameter. Figure 3.4 illustrates the probability distribution of several PCS QAM constellations. Intuitively, $\nu$ allows to change the spread of the Gaussian-like distribution over the constellation. When $\nu = 0$, the constellation is a standard QAM with uniform distribution. When $\nu$ tends to $+\infty$, the PCS QAM converges to a QPSK. For a given value of the SNR, $\nu$ can be set such that the mutual information $I(X;Y)$ closely approaches the Shannon capacity.

Practical implementation of PCS QAM requires that the distribution of the Gray mapping codewords matches the distribution $p_\nu(x, y)$. This is ensured by a distribution matcher, which maps the source bit string to another bit string with the right properties. Distribution matching is performed together with forward error correction coding [69]. Both distribution matching and error correcting can be safely

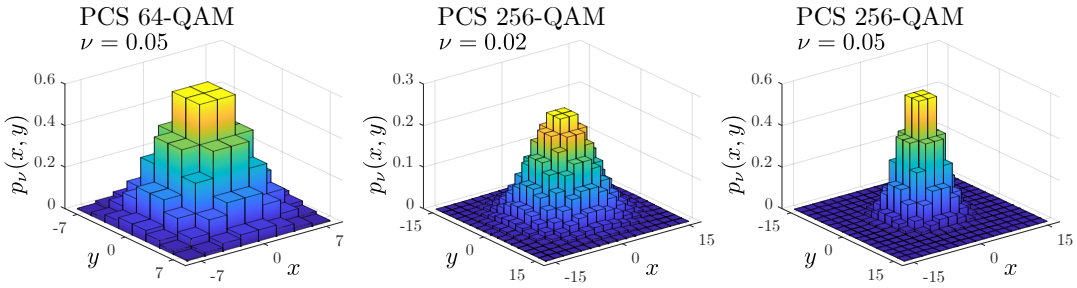



Figure 3.4: Probability distribution of PCS 64-QAM with $\nu = 0.5$, and PCS 256-QAM with $\nu = 0.2$ and $\nu = 0.5$.

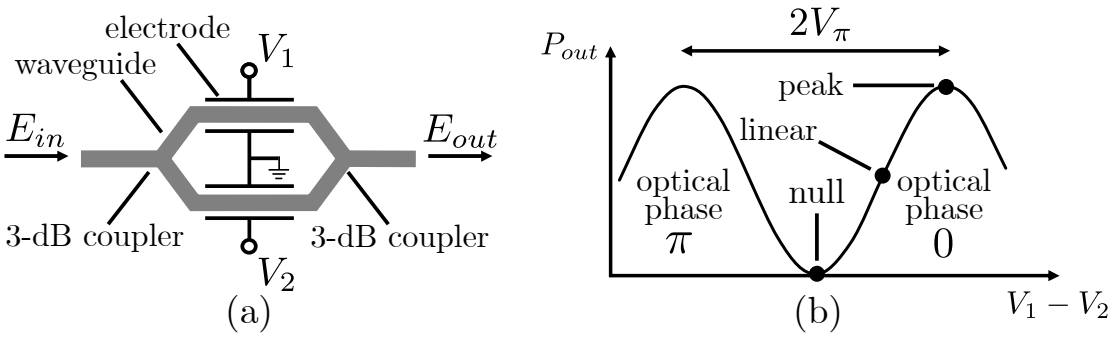



Figure 3.5: (a) Mach-Zehnder modulator scheme and (b) output optical power vs voltage difference.

neglected in this work because the symbols ($x_k$) are directly generated using random number generators.

## 3.2 Description of the optical IQ modulator

The purpose of optical modulation is to convert electrical signals into optical signals. Its most basic principle relies on the Pockels effect, also known as linear electro-optic effect, which changes the refractive index of an optical medium proportionally to the electric field. This effect occurs only in crystals that lack inversion symmetry, such as lithium niobate $LiNbO_3$. Using such linear electro-optical cells enables *phase modulation* of an optical signal, by controlling the applied voltage. Amplitude modulation is made possible by using Mach-Zehnder (MZ) interferometers, named after their inventors Ludwig Zehnder and Ludwig Mach [70, 71]. A MZ interferometer is composed of two 3-dB couplers and two optical waveguides called arms, disposed as outlined in Figure 3.5(a). One or both arms includes a linear electro-optical cell. Depending on the applied voltages $V_1$ and $V_2$, a phase shift is introduced between the optical signals of both arms. When combined, the interference results in *amplitude modulation* as the relationship between the input and output fields, respectively $E_{in}$ and $E_{out}$ is given by

$$E_{out} \propto E_{in} \cos\left(\pi \frac{V_1 - V_2}{2V_\pi}\right), \tag{3.4}$$

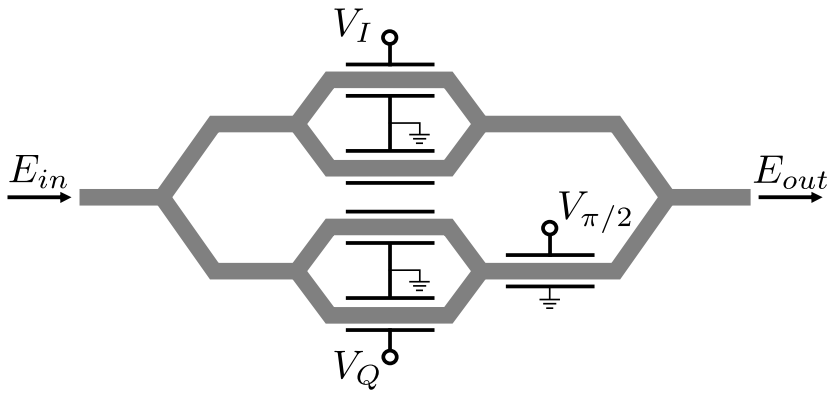



Figure 3.6: Nested Mach-Zehnder modulators scheme for IQ optical modulation.

where a voltage difference of $V_\pi$ leads to destructive interference. Figure 3.5(b) illustrates the output optical power $P_{out}$ given by

$$P_{out} \propto P_{in} + P_{in}\cos\left(\pi\frac{V_1 - V_2}{V_\pi}\right). \tag{3.5}$$

A typical mode of operation is $V_2 = -V_1$, called push-pull mode. Then, *IQ modulation* is done by introducing a $\pi/2$ phase between the output of two parallel push-pull MZ modulators. To introduce this $\pi/2$ phase, the parallel MZ modulators are nested into another MZ interforemeter, as illustrated in Figure 3.6. Integrated IQ modulators based on LiNbO3 or InP crystals are commercially available. Finally, using two such IQ modulators with orthogonal polarized outputs allows to generate polarization-multiplexed optical signals [72].

Let's note that the transfer function of the MZ modulator, illustrated in Figure 3.5, is not a linear function of the applied voltage. It can be divided into ranges where it is either linear or quadratic, with either 0 or $\pi$ optical phase. Depending on the type of modulation considered (return to zero, non return to zero, binary phase shift keying, etc), the range of values taken by $(V_1 - V_2)$ should be carefully designed. When considering digitally implemented Nyquist pulse shaping, as discussed in subsection 3.5.1, a simple design is to select a range of values where the transfer function is linear. This is the case around the null intensity. It is also possible to digitally compensate for the quadratic shape of the transfer function, to work with a full range of $V_\pi$. Either way, an ambiguity remains on the optical phase, which will have to be removed during digital signal processing.

## 3.3 Description of the coherent optical receiver

### 3.3.1 Fundamental principle of coherent detection

The purpose of a coherent optical receiver is to measure the complex amplitude of an optical signal over time $t$. The main principle is to interfere the received signal with a continuous wave local oscillator (LO) to extract its phase information. Let the complex electric field of the received optical signal be

$$E_s(t) = A_s(t)e^{i(\omega_s t + \phi_{sig}(t))}, \tag{3.6}$$

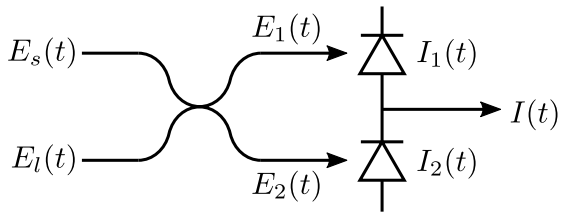



Figure 3.7: Outline of a coherent receiver that measures the phase between the signal and LO field. Balanced detection is used to remove the DC component and increase the sensitivity by 3 dB.

with $A_s(t) \geq 0$ the real amplitude, $\phi_{sig}(t)$ the modulated phase, and $\omega_s = 2\pi c/\lambda$ the angular frequency. Similarly, the complex electric field of the LO is given by

$$E_l(t) = A_l e^{i(\omega_l t + \phi_l(t))}, \tag{3.7}$$

where $A_l$ is constant over time and $\phi_l(t)$ accounts for the random phase noise. Let's detail the configuration of the main building block of a coherent receiver, outlined in Figure 3.7. The following equations are reproduced from [72]. First of all, the signal and LO fields are coupled using a 3 dB optical coupler that adds a 180 ∘ phase shift to the LO field between the outputs. Therefore, the fields at the outputs of this 180° hybrid are

$$E_1(t) = \frac{1}{\sqrt{2}}(E_s(t) + E_l(t)), \tag{3.8}$$

$$E_2(t) = \frac{1}{\sqrt{2}}(E_s(t) - E_l(t)). \tag{3.9}$$

Then, the output photocurrent of the first photodiode is

$$\begin{aligned}
I_1(t) &= R\left|\mathrm{Re}(E_1(t))\right|^2 \\
&= \frac{R}{2}\Big[A_s(t)^2\cos^2(\omega_s t + \phi_{sig}(t)) \\
&\qquad + A_l^2\cos^2(\omega_l t + \phi_l(t)) \\
&\qquad + 2A_s(t)A_l\cos(\omega_s t + \phi_{sig}(t))\cos(\omega_l t + \phi_l(t))\Big] \\
&= \frac{R}{2}\Big[\frac{1}{2}(A_s(t)^2 + A_l^2) \\
&\qquad + \frac{1}{2}\cos(2\omega_s t + 2\phi_{sig}(t)) \\
&\qquad + \frac{1}{2}\cos(2\omega_l t + 2\phi_l(t)) \\
&\qquad + A_s(t)A_l\cos((\omega_s + \omega_l)t + \phi_{sig}(t) + \phi_l(t)) \\
&\qquad + A_s(t)A_l\cos((\omega_s - \omega_l)t + \phi_{sig}(t) - \phi_l(t))\Big]
\end{aligned}$$

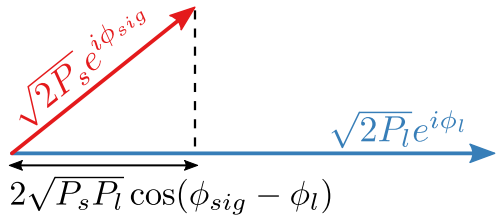



Figure 3.8: Homodyne detection reads the inner product between the phasors of the signal and LO complex fields.

where $R$ denotes the photodiode responsivity. Since $\omega_s$ and $\omega_l$ are angular optical frequencies, in the range of hundreds of THz, they exceed the bandwidth of the photodiode. Therefore,

$$I_1(t) = \frac{R}{2}\left[P_s(t) + P_l + 2\sqrt{P_s(t)P_l}\cos\big((\omega_s - \omega_l)t + \phi_{sig}(t) - \phi_l(t)\big)\right] \tag{3.10}$$

where $P_s(t) = |A_s(t)|^2/2$ and $P_l = |A_l|^2/2$ are respectively the signal power and the LO power. A similar calculation gives, for the second photodiode,

$$I_2(t) = \frac{R}{2}\left[P_s(t) + P_l - 2\sqrt{P_s(t)P_l}\cos\big((\omega_s - \omega_l)t + \phi_{sig}(t) - \phi_l(t)\big)\right]. \tag{3.11}$$

Finally, balanced detection removes the DC component and increases the sensitivity by 3 dB compared to a single photodiode, with

$$\begin{aligned} I(t) &= I_1(t) - I_2(t) \\ &= 2\sqrt{P_s(t)P_l}\cos\big((\omega_s - \omega_l)t + \phi_{sig}(t) - \phi_l(t)\big). \end{aligned} \tag{3.12}$$

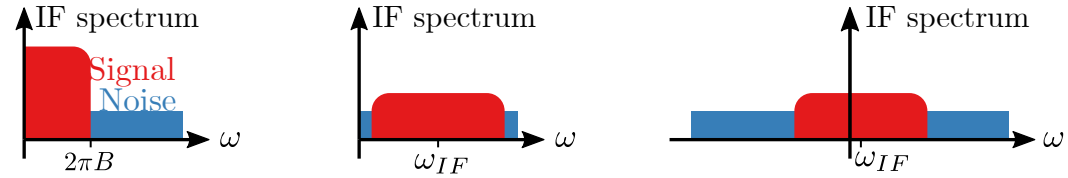
Let's remark that the above lines doesn't include thermal noise or shot noise. To proceed further, a distinction must be made according to the value of the intermediate frequency $\omega_{IF} = |\omega_s - \omega_l|$.

**Homodyne detection** When $\omega_{IF}$ is set to 0, the term *homodyne* detection is used. In that case, the output of the photodetector is

$$I(t) = 2\sqrt{P_s(t)P_l}\cos\big(\phi_{sig}(t) - \phi_l(t)\big) \tag{3.13}$$

$$= 2\sqrt{P_s(t)P_l}\cos\big(\phi_s(t) + \phi_n(t)\big) \tag{3.14}$$

where $\phi_{sig}(t) = \phi_s(t) + \phi_{sn}(t)$ with $\phi_s(t)$ the modulated phase and $\phi_{sn}$ the phase noise of the signal carrier, and $\phi_n(t) = \phi_{sn}(t) - \phi_l(t)$ the total phase noise. Equation (3.13) implies that homodyne detection reads the inner product between the phasors of the complex fields $E_s$ and $E_l$, as illustrated in Figure 3.8. Therefore, only one of the in-phase or quadrature component can be measured by the detector. Moreover, recovering this partial information requires to strictly lock the LO frequency and phase to the frequency and phase noise of the signal. This function can typically be done with an optical phase-locked loop (OPLL). However, the implementation of an OPLL greatly increases the complexity of the system.




(a) Homodyne $\omega_{IF} = 0$ (b) Heterodyne $\omega_{IF} \gg 2\pi B$ (c) Intradyne $\omega_{IF} \approx 0$

Figure 3.9: IF spectrum of several coherent detection schemes: (a) homodyne, (b) heterodyne, described in subsection 3.3.1, and (c) phase-diversity intradyne, described in subsection 3.3.2.

**Heterodyne detection** On the contrary, *heterodyne* detection refers to cases where $\omega_{IF} \gg 2\pi B$ with $B$ the useful bandwidth of the modulated signal, as illustrated in Figure 3.9(b). In such cases, the photocurrent is

$$I(t) = 2\sqrt{P_s(t)P_l}\cos(\omega_{IF}t + \phi_s(t) + \phi_n(t)). \tag{3.15}$$

The advantage of heretodyne detection is that OPPL is no longer required. In fact, the baseband conversion and phase-locked loop (PLL) to compensate for $\phi_n(t)$ and for fluctuations of $\omega_{IF}$ can be performed electronically or digitally. On the downside, it requires at least twice the bandwidth and has a 3 dB worse sensitivity [73].

**Warning note** It should be mentioned that the previously described terms, *homodyne* and *heterodyne*, do not refer to the same process depending on the author's background. The above definitions are commonly used by the research community working on coherent optical communications. However, in the quantum information literature, the term *homodyne detection* refers to the measurement of a single quadrature operator and *heterodyne detection* to the simultaneous measurement of both quadrature operators. In this section, our use of these terms will coincide to the former. In other sections, to the latter, since our practical work is based only on intradyne receivers, to be introduced in the next subsection.

### 3.3.2 Phase-diversity coherent receiver

As illustrated in Figure 3.10, the introduction of a secondary LO with a 90° phase shift allows to read the component orthogonal to the one measured by the homodyne detector of Figure 3.8. This idea leads to the design of a homodyne receiver architecture able to measure both IQ components at the same time. This configuration, outlined in Figure 3.11, includes a 90° hybrid to introduce the phase shift and two homodyne receivers to detect the IQ components. In this receiver, the output fields

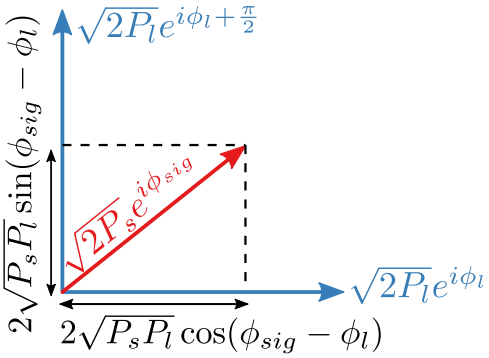



Figure 3.10: Compared to Figure 3.8, the introduction of a secondary LO with a 90° phase shift allows to fully recover the modulated phase of the signal.

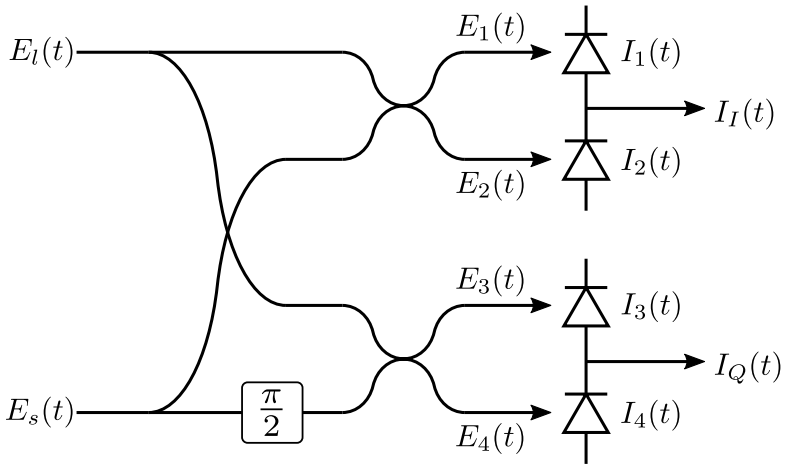



Figure 3.11: Outline of the phase-diversity coherent receiver used to measure simultaneously the in-phase and quadrature components of the signal.

of the optical part are

$$E_1 = \frac{1}{2}(E_s + E_l), \tag{3.16}$$

$$E_2 = \frac{1}{2}(E_s - E_l), \tag{3.17}$$

$$E_3 = \frac{1}{2}(E_s + iE_l), \tag{3.18}$$

$$E_4 = \frac{1}{2}(E_s - iE_l), \tag{3.19}$$

and the output photocurrents of the electric part are

$$I_I(t) = \sqrt{P_s(t)P_l}\cos\big(\phi_s(t) + \phi_n(t)\big), \tag{3.20}$$

$$I_Q(t) = \sqrt{P_s(t)P_l}\sin\big(\phi_s(t) + \phi_n(t)\big). \tag{3.21}$$

Therefore, despite a 3 dB loss in sensitivity compared to the single homodyne receiver, this configuration allows for both IQ components to be measured. It can be referred as the *phase-diversity* homodyne receiver. However, contrary to the single homodyne receiver, the frequency and phase of the LO doesn't need to be strictly locked. In fact, with $\omega_{IF} \approx 0$, we can recover the complex signal with

$$\begin{aligned} I_c(t) &= I_I(t) + iI_Q(t) \\ &= \sqrt{P_s(t)P_l}\; e^{i(\omega_{IF}t + \phi_s(t) + \phi_n(t))}, \end{aligned} \tag{3.22}$$

which contains the whole signal spectrum, represented using negative frequencies as in Figure 3.9(c), and allows for electrical or digital PLL. In contrast, the single homodyne receiver only measures a folded spectrum, as per Figure 3.9(a). This last comment motivates the use of the term *intradyne* detection for phase-diversity receiver, to emphasize the possibility of a free-running LO.

Intradyne detection is the most practical and commonly used scheme in modern coherent communication systems, combined with digital signal processing (DSP) to compensate for $\omega_{IF}$ and $\phi_n(t)$, as well as other physical impairments that will be described in Section 3.4. The most common DSP algorithms for intradyne detection will be described in Section 3.5.

### 3.3.3 Polarization-diversity coherent receiver

The previous calculation did not take into account the polarization of light. In fact, it implicitly assumed that the signal and LO were in the same polarization state. This condition is almost never experimentally verified, because of fiber birefringence. To tackle this issue, a polarization-diversity receiver was introduced. It separates the signal into two signals, $E_s^H(t)$ and $E_s^V(t)$, with arbitrary but orthogonal linear polarization states using a polarization beam splitter (PBS). Then, $E_s^H(t)$ and $E_s^V(t)$ are measured using two phase-diversity homodyne receivers, as illustrated in Figure 3.12. The receiver outputs four photocurrents, one for each IQ component of each orthogonal linear polarization state. Finally, the polarization state of the modulated signal can be retrieved from the two orthogonal linear polarization states

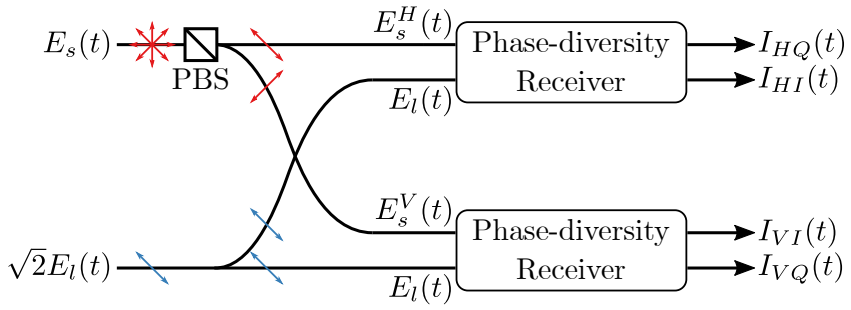



Figure 3.12: Outline of the polarization-diversity coherent receiver, composed of two phase-diversity receivers that measure each orthogonal linear polarization at the output of the PBS.

using DSP, as described in subsection 3.5.2. This receiver and DSP also offer the ability to perform polarization demultiplexing, that is to say to decode two different signals transmitted on the same carrier frequency and modulated onto waves with orthogonal polarization states.

### 3.3.4 Quantum noise of coherent detection

Quantum-mechanical properties of coherent light and coherent detection induces a fundamental noise in the receiver, called shot noise. This noise may be dominant for the receiver's sensitivity when $P_{LO}$ is sufficiently large. Let's review its properties in the case of the coherent optical receiver, following the lines in [72]. This subsection establishes a bridge between the theory of CV-QKD and the effective measurements performed by a coherent receiver.

**Direct detection** Appendix A.3 summarizes the fundamental equations of quantum optics which are necessary for this thesis. It gives that for a coherent state $|\alpha\rangle$, the quadrature operators $\hat{q}$ and $\hat{p}$ are equally noisy and have minimal uncertainty

$$\langle \Delta\hat{q}^2 \rangle = \langle \Delta\hat{p}^2 \rangle = 1. \tag{3.23}$$

The photocurrent associated with direct detection of a coherent state on a photodiode is given by

$$\hat{I} = \frac{e\hat{n}}{T_S} \tag{3.24}$$

where $e$ is the electron charge, $\hat{n}$ the photon number operator and $T_S$ the symbol duration. Therefore, the average photocurrent over time $T_S$ is

$$\langle \hat{I} \rangle = \overline{I} = \frac{e\langle \hat{n} \rangle}{T_S} \tag{3.25}$$

and the variance is

$$\langle \Delta\hat{I}^2 \rangle = \frac{e^2}{T_S^2} \langle \Delta\hat{n}^2 \rangle = \frac{e\overline{I}}{T_S} \tag{3.26}$$

since $\langle \hat{n}^2 \rangle = \langle \hat{n} \rangle = |\alpha|^2$. This leads to the well known equation for the shot noise variance [72],

$$\langle \Delta \hat{I}^2 \rangle = 2e\bar{I}B \tag{3.27}$$

where $B = 1/(2T_S)$ is the minimal bandwidth of a signal with symbol duration $T_S$, as given by the Nyquist sampling theorem.

**Homodyne receiver** The quantum mechanical description of the output current of a balanced photodetector can be described by

$$\begin{aligned} \hat{I} &= \hat{I}_1 - \hat{I}_2 \\ &= \frac{e}{T_S}\Big(\frac{\hat{E}_s^\dagger + \hat{E}_l^\dagger}{\sqrt{2}}\frac{\hat{E}_s + \hat{E}_l}{\sqrt{2}} - \frac{\hat{E}_s^\dagger - \hat{E}_l^\dagger}{\sqrt{2}}\frac{\hat{E}_s - \hat{E}_l}{\sqrt{2}}\Big) \\ &= \frac{e}{T_S}(\hat{E}_s^\dagger \hat{E}_l + \hat{E}_l^\dagger \hat{E}_s) \end{aligned} \tag{3.28}$$

where $\hat{E}_s$, $\hat{E}_s^\dagger$, $\hat{E}_l$ and $\hat{E}_l^\dagger$ are respectively time-dependent annihilation and creation operators associated with the signal and LO field. When the optical power of the LO is high enough, the quantum uncertainty is negligible compared to the constant amplitude $A_l$ of the LO field. Moreover, we can set the phase of the LO as the phase reference and assume that $A_l$ is real. In that case, the time-dependent operators $\hat{E}_l$ and $\hat{E}_l^\dagger$ can be replaced by

$$\hat{E}_l \to A_l \exp(-i\omega_l t) \tag{3.29}$$

$$\hat{E}_l^\dagger \to A_l \exp(i\omega_l t). \tag{3.30}$$

On the other hand, the time-dependent ladder operators of the signal are given by

$$\hat{E}_s = \hat{a}_s \exp(-i\omega_s t) \tag{3.31}$$

$$\hat{E}_s^\dagger = \hat{a}_s^\dagger \exp(i\omega_s t) \tag{3.32}$$

where $\hat{a}_s$ and $\hat{a}_s^\dagger$ are respectively time-independent annihilation and creation operators for the signal. Assuming $\omega_l = \omega_s$, we obtain

$$\hat{I} = \frac{e}{T_S} A_l(\hat{a}_s + \hat{a}_s^\dagger) = \frac{e}{T_S} A_l \hat{q}_s. \tag{3.33}$$

where $\hat{q}_s$ is the in-phase quadrature operator of the signal field. We recognize from equation (3.33) that homodyne detection reads the in-phase component of the signal with respect to the LO phase, as illustrated in Figure 3.8. In this homodyne detection, the quantum noise stems from quantum uncertainty of the signal, amplified by the power of the LO. The variance of $\hat{I}$ is in fact given by

$$\langle \Delta \hat{I}^2 \rangle = \frac{e^2 A_l^2}{T_S^2} \langle \Delta \hat{q}_s^2 \rangle = 2eI_l B \tag{3.34}$$

where $I_l = eA_l^2/T_S$ is the average photocurrent generated by the LO power, and given that $\langle \Delta \hat{q}^2 \rangle = 1$. Equation (3.34) can also be interpreted as the shot noise due to the LO power.

**Heterodyne receiver** In the case of $\omega_{IF} \gg 0$, the beat between the signal and the LO appears around the frequency $\omega_{IF}$, as illustrated in Figure 3.9. Moreover, this frequency also exhibits the beat between the LO and the signal band around $\omega_i$, the symmetrical frequency of $\omega_s$ with respect to $\omega_l$. Even if $\omega_i$ carries no signal, its quantum-mechanical vacuum fluctuation will impact the measurement, leading to a 3 dB increase of the noise power. In that case, the output photocurrent can be described by [72],

$$\hat{I} = \frac{2eA_l}{T_S}(\hat{x}\cos(\omega_{IF}t) + \hat{y}\sin(\omega_{IF}t)) \tag{3.35}$$

where $\hat{x}$ and $\hat{y}$ are noisy versions of the quadratures operators of the signal field,

$$\hat{x} = \hat{q}_s + \delta\hat{q}_s \tag{3.36}$$

$$\hat{y} = \hat{p}_s + \delta\hat{p}_s \tag{3.37}$$

where $\delta\hat{q}_s$ and $\delta\hat{p}_s$ are quantum operators such that $\hat{x}$ and $\hat{y}$ satisfy the commutation relation,

$$[\hat{x}, \hat{y}] = 0. \tag{3.38}$$

Therefore, contrary to homodyne detection, simultaneous measurement of both quadratures is possible. However, this advantage comes with additional noise introducing a 3 dB loss of sensitivity.

**Phase-diversity homodyne receiver** In the case of the phase-diversity homodyne receiver illustrated in Figure 3.11, the signal field is divided in two using a 3 dB coupler. Each output of the coupler is fed to a homodyne receiver performing a noise-free measurement of each quadrature component. However, the signal power was decreased by 3 dB. Therefore, the sensitivity of the phase diversity homodyne receiver is identical to that of the heterodyne receiver. In any case, the measurement of both quadratures comes with a 3 dB cost in sensitivy.

## 3.4 Channel modeling of a single-mode fiber

In 1966, Kao and Hockham first proposed the use of optical fibers for telecommunication applications at optical wavelengths [74]. Since then, optical fibers have been extensively studied and have undergone many developments [75]. They are typically composed of a cylindrical silica core surrounded by a cladding glass layer with lower refractive index and several plastic or polymer coatings to protect the whole, as illustrated in Figure 3.13. Incoming light remains confined to the core of the fiber due to total reflection effects caused by the difference in refractive index between the core and cladding. The light can travel in the fiber by several optical paths which constitute as many spatial propagation modes.

Single-mode fibers (SMF) are the most commonly used fibers in long-distance optical communications. As the name implies, SMF are designed to allow the propagation of a single spatial mode at telecommunication wavelength around 1550 nm. This is made possible by careful adjustment of the core diameter and refractive index difference. Typical diameters are 9 µm for the core and 125 µm for the cladding

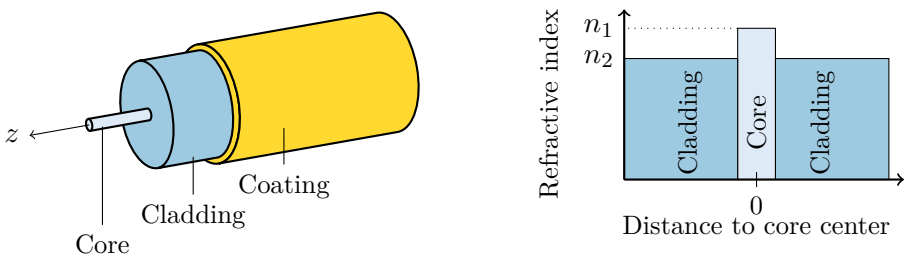



Figure 3.13: Schematic view of a single-mode fiber (SMF) and its refractive index profile.

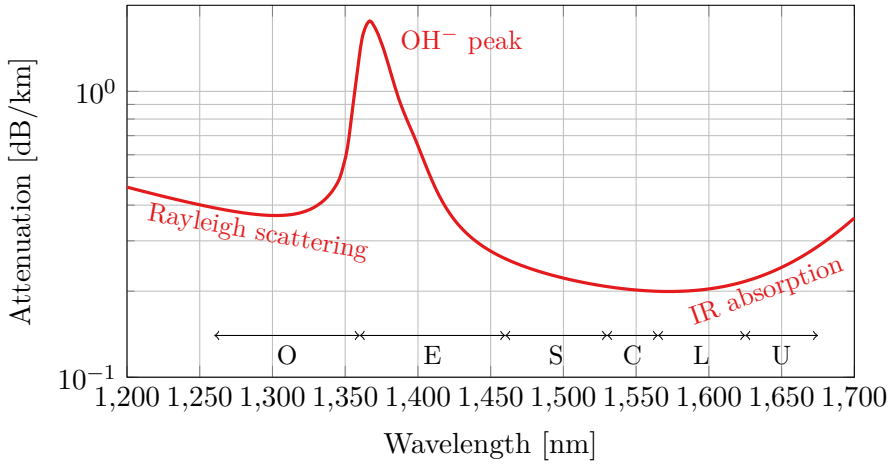



Figure 3.14: Attenuation profile of a standard SMF (analytical fit to experimental data taken from [78]) and ITU-T standard wavelength bands.

layer. Standards for long-haul communications are defined in ITU-T G.652 [76] and ITU-T G.654 [77].

Other types of optical-fibers such as multi-mode fibers (MMF) are also used, mainly for short-reach optical transmissions. In this thesis, we will only study the use of SMF for CV-QKD. This section deals with modeling of impairments in SMF that are relevant to our application.

### 3.4.1 Power attenuation

The main limiting impairment of optical fibers is the power attenuation induced by absorption and scattering loss. In fact, the power $P(z)$ of an optical signal in [W] decreases exponentially with the traveled distance in the fiber $z$ in [m], according to

$$P(z) = P(0)\exp(-\alpha z) \tag{3.39}$$

where $\alpha$ is the attenuation coefficient in $[\mathrm{Np\,m^{-1}}]$, more commonly expressed in $[\mathrm{dB\,km^{-1}}]$ for practical reasons. Figure 3.14 gives the profile of $\alpha$ as a function of the wavelength $\lambda$ for standard SMF fibers. The main effect for low wavelengths is Rayleigh scattering, a scattering of light in all directions caused by the non-

uniformity of the refractive index resulting from manufacturing imperfections. For high wavelengths, losses are mainly due to interactions of photons with the silica, called infrared absorption. Finally, the peak between 1350 and 1400 nm is the consequence of impurities in the fiber, such as $OH^-$ ions.

Since CV-QKD doesn't permit the use of optical amplifiers, fiber attenuation is critical to performance. Therefore, the most suitable wavelengths for CV-QKD applications are around 1550 nm where the attenuation is minimal. It is also possible to use non-standard SMF fiber with lower attenuation coefficient.

### 3.4.2 Chromatic dispersion

The propagation speed of light is inversely proportional to the dielectric constant of the propagation medium. For optical fibers, the phase velocity $\nu_p$ is given by

$$\nu_p = \frac{c}{n} \tag{3.40}$$

where $c$ is the speed of light in vacuum and $n(\omega)$ the refractive index. Chromatic dispersion is a consequence of the dependence of the refractive index on the wavelength $\lambda$, with $n = n(\lambda)$. It states that spectral components with different wavelengths travel with different velocity through the fiber, leading to pulse broadening and inter-symbol interference. In the absence of fiber nonlinearity, chromatic dispersion can be described by the following partial differential equation on the envelope $A(z,t)$ of the transmitted pulse [79],

$$\frac{\partial A(z,t)}{\partial z} = j\frac{D(\lambda)\lambda^2}{4\pi c}\frac{\partial^2 A(z,t)}{\partial t^2} \tag{3.41}$$

where $z$ is the propagation distance, $t$ the propagation time, and $D(\lambda)$ the dispersion coefficient of the fiber for wavelength $\lambda$, expressed in [ps/(nm km)]. By taking the Fourier transform of equation (3.41), we obtain the frequency domain of the transfer function of chromatic dispersion $G(z,\omega)$,

$$G(z,\omega) = \exp\Big(-j\frac{D(\lambda)\lambda^2}{4\pi c}\omega^2\Big) \tag{3.42}$$

where $\omega$ is the angular frequency. This inverse of the transfer function can be estimated using adaptive equalizers, as described in 3.5.2.

### 3.4.3 Polarization mode dispersion

Any polarized electromagnetic wave may be decomposed as the sum of two waves with orthogonal polarization states. Assuming perfect cylindrical symmetry of the fiber, both polarized modes undergo the same propagation conditions. However, real fibers exhibit asymmetry caused by fiber stress and irregularities during the manufacturing process. It induces a dependence of the refractive index on the polarization state, an effect called birefringence. The consequence is that one orthogonal polarized mode propagates faster than the other one. Therefore, birefringence introduces a difference in propagation time between both modes, called differential group delay (DGD), illustrated in Figure 3.15(a). Moreover, the birefringence changes randomly

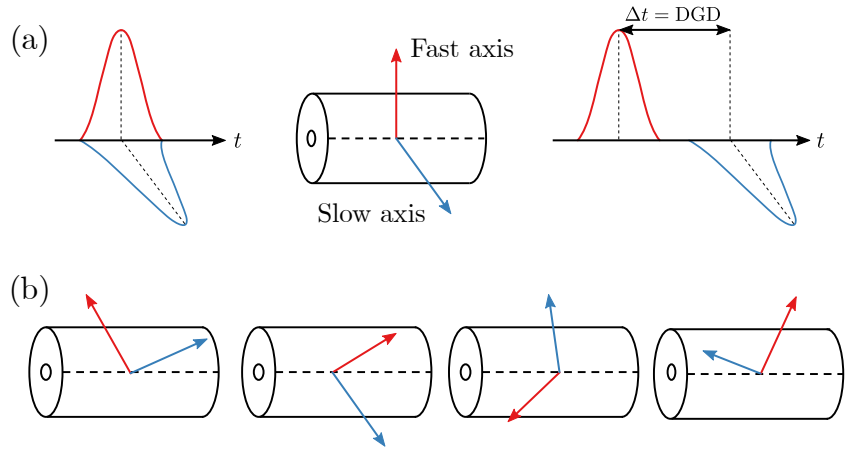



Figure 3.15: (a) Differential group delay (DGD) over a fiber section with constant birefringence, and (b) schematic representation of a real fiber as a concatenation of infinitesimal birefringent sections with random orientation of the fast and slow axis.

along the fiber. This induces a coupling of the transmitted polarization modes, called polarization mode dispersion (PMD). The overall fiber can be modeled by a concatenation of independent randomly oriented birefringent sections, as per Figure 3.15(b), with an overall PMD given by

$$\mathbf{E}_{out} = \prod_i \overline{R}_i \begin{bmatrix} e^{-j(\omega\tau_i+\phi_i)/2} & 0 \\ 0 & e^{j(\omega\tau_i+\phi_i)/2} \end{bmatrix} R_i \, \mathbf{E}_{in} \tag{3.43}$$

where $\phi_i$, $\tau_i$ are respectively the phase shift and DGD between the fast and slow mode of the $i$-th section, and $R_i$ the rotation matrix relative to the mode orientation.

### 3.4.4 Other impairments

In this subsection, we briefly comment on other known impairments of optical communication systems that are not relevant to CV-QKD.

**Polarization dependent loss** In the context of optical communication, light goes through a large number of optical devices such as amplifiers, isolators, re-configurable optical add-drop multiplexers (ROADMs), etc. Asymmetries in the insertion loss or gain of those elements accumulates along the transmission, leading to an effect called polarization dependent loss (PDL). However, PDL can be neglected in the context of a point to point link without any amplifiers, like for CV-QKD.

**Nonlinear Kerr effect** When the amplitude of the electromagnetic field is high, the response of the optical fiber to light becomes nonlinear (NL). Nonlinear impairments have been widely studied in the literature. The first type of nonlinear effect is the Kerr effect. It describes variations in the refractive index of the silica that are proportional to the power of the optical field. A second nonlinear effect is stimulated Raman scattering. It says that a photon of energy $\hbar\omega_p$ scattered by a molecule of

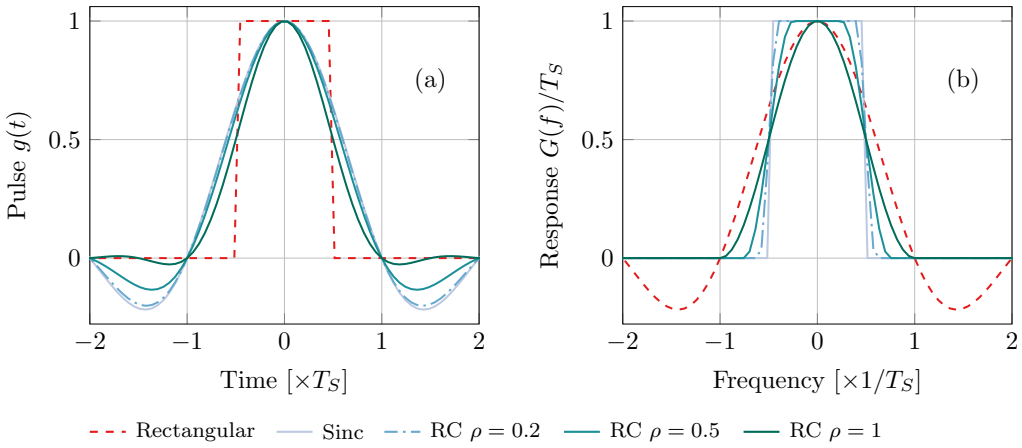



Figure 3.16: (a) Pulse $g(t)$ and (b) frequency response $G(f)$ of different pulse shaping functions. RC stands for raised cosine and $\rho$ is the roll-off factor.

silica moves the molecule to a higher-energy state of vibration, while a new photon is emitted with lower energy $\hbar\omega_s$ ($\omega_s < \omega_p$). Therefore, there is a transfer of energy towards lower frequency components. In CV-QKD, the launch power is typically low enough to neglect those nonlinear effects. Therefore, they will not be studied in this thesis.

## 3.5 Digital signal processing

### 3.5.1 Nyquist pulse shaping

In digital communication systems, the transmitter encodes its message into a series of complex symbols $(s_k)_{k\in\mathbb{N}}$. The symbols are modulated on the amplitude and phase of an electromagnetic wave. Let $f_S = 1/T_S$ be the symbol transmission rate. The complex amplitude of the field $E(t) = E(t, 0)$ is typically

$$E(t) \propto \sum_{k=0}^{+\infty} s_k \, g(t - kT_S) \tag{3.44}$$

where $g(\cdot)$ is called the *pulse shape* of the signal. The most obvious pulse shape is $g(\cdot) = \mathbf{1}_{[-1/T_S, 1/T_S]}$, plotted with a dashed line in Figure 3.16(a). Its inconvenient is that it requires infinite bandwidth, as its frequency response is

$$G(f) = T_S \operatorname{sinc}(f/T_S) \tag{3.45}$$

where $\operatorname{sinc}(x) = \sin(\pi x)/\pi x$, which should not be allowed. Many bandwidth limited pulse shapes can be considered. However, a good pulse shape should be free of inter-symbol interference (ISI), which occurs when at least two symbols interfere at sampling times $(kT_S)_{k\in\mathbb{N}}$. Thankfully, the Nyquist criterion offers a very practical characterization of such $g(t)$.

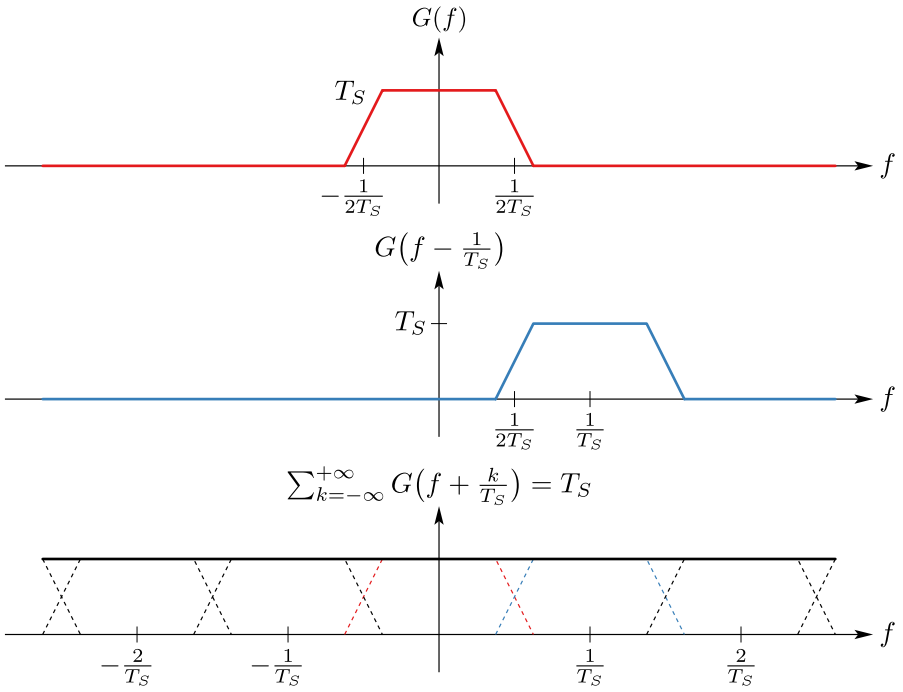



Figure 3.17: A function $g(t)$ satisfying the Nyquist zero ISI criterion (3.47). Figure taken from [66].

**Nyquist criterion** To avoid ISI, $g(t)$ should satisfy the Nyquist criterion for zero ISI [80], which states that

$$g(kT_S) = \begin{cases} 1 & \text{if } k = 0 \\ 0 & \text{if } k \neq 0 \end{cases} \tag{3.46}$$

if and only if its Fourier transform $G(f)$ satisfies

$$\sum_{k=-\infty}^{+\infty} G(f + k/T_S) = T_S. \tag{3.47}$$

Figure 3.17 illustrates this criterion with an example. A consequence of this criterion is that the minimal possible bandwidth of the signal is $W \geq 1/2T_S$. Let's review a few classical examples of pulse shapes, all illustrated in Figure 3.16.

**Sinc pulse** The sinc pulse shape is defined by $g(t) = \text{sinc}(t/T_S)$. Its frequency response is given by $G(f) = T_S$ if $|f| < 1/2T_S$ and 0 otherwise. Therefore, it satisfies the Nyquist criterion with minimal bandwidth $W = 1/2T_S$. The absence of ISI allows recovery of each symbol without any distortion assuming perfect sampling. However, the sinc pulse shape has infinite time duration with slow decay of the amplitude. Thus, imperfect sampling would lead to significant ISI over a large number of symbols.

**Raised cosine pulse** The raised cosine pulse (RC) is commonly used in digital communications. It is a "smooth rectangle" in the frequency domain with an excess bandwidth $\rho/2T_S$ where $\rho \in [0,1]$ is called the *roll-off factor*. Figure 3.16 gives examples with $\rho = 0.2$, 0.5 and 1. Its frequency response is given by

$$G_\rho(f) = \begin{cases} T_S, & \text{if } |f| \leq \dfrac{1-\rho}{2T_S} \\ \dfrac{T_S}{2}\left(1+\cos\left(\dfrac{\pi T_S}{\rho}\left(|f|-\dfrac{1-\rho}{2T_S}\right)\right)\right), & \text{if } \dfrac{1-\rho}{2T_S} < |f| \leq \dfrac{1+\rho}{2T_S} \\ 0, & \text{otherwise} \end{cases} \tag{3.48}$$

and the corresponding pulse shape in the time domain is

$$g_\rho(t) = \begin{cases} \dfrac{\pi}{4}\operatorname{sinc}\left(\dfrac{1}{2\rho}\right), & \text{if } t = \pm\dfrac{T_S}{2\rho} \\ \operatorname{sinc}\left(\dfrac{t}{T_S}\right)\dfrac{\cos(\pi\rho t/T_S)}{1-4\rho^2t^2/T_S^2}, & \text{otherwise.} \end{cases} \tag{3.49}$$

$g_\rho(t)$ satisfies the Nyquist criterion for all value $\rho \in [0,1]$. With a faster decay of the amplitude compared to the sinc pulse, RC pulse is less sensitive to ISI in the case of imperfect sampling. Moreover, the roll-off factor can be tuned to accommodate the system requirements, especially for the bandwidth $W = (1+\rho)/2T_S$.

**Root raised cosine pulse** Last but not least is the root raised cosine (RRC) pulse shape, defined by $g(t) = \sqrt{g_\rho(t)}$. Its interest arises when considering the optimal filter for a channel with additive white Gaussian noise. For a given transmitted pulse shape $g(t)$, the optimal filter is $g^*(-t)$, the complex conjugate with reverse time. This filter is called the *matched filter*. Because of its symmetrical properties, the RRC is its own matched filter. Therefore, when using RRC pulse shape, the overall pulse shape after matched filtering is actually a RC, whose interest was underlined in the previous paragraph.

### 3.5.2 Adaptive equalizer

This subsection introduces an adaptive equalizer commonly used in digital coherent receivers to correct several linear transmission impairments, such as chromatic dispersion or PMD. It is sometimes referred to as polarization demultiplexing equalizer. Let's consider that the launch power is low enough to assume the transmission occurs in the linear regime. Then, the Fourier transform $\mathbf{E}_{out}(\omega) = [E^H_{out}(\omega), E^V_{out}(\omega)]^T$ of the received complex amplitude is

$$\mathbf{E}_{out}(\omega) = \mathbf{H}_o(\omega)\mathbf{E}_{in}(\omega) \tag{3.50}$$

where $\mathbf{E}_{in}(\omega)$ is the Fourier transform of the transmitted complex amplitude. $\mathbf{H}_o(\omega)$ is the transfer function of the link, accounting for linear impairments. Digital coherent receivers implement adaptive equalizer to estimate $\mathbf{H}_o(\omega)^{-1}$, which allows to correct and monitor those linear impairments [81]. This adaptive equalization is performed using finite impulse response (FIR) filters. We will also see that this equalizer is capable of recovering the clock phase between the transmitter and the receiver.

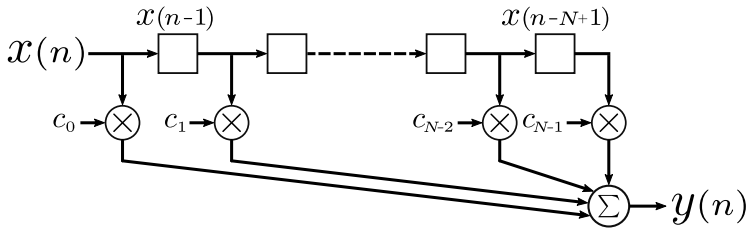



Figure 3.18: Operating scheme of a finite impulse response (FIR) filter.

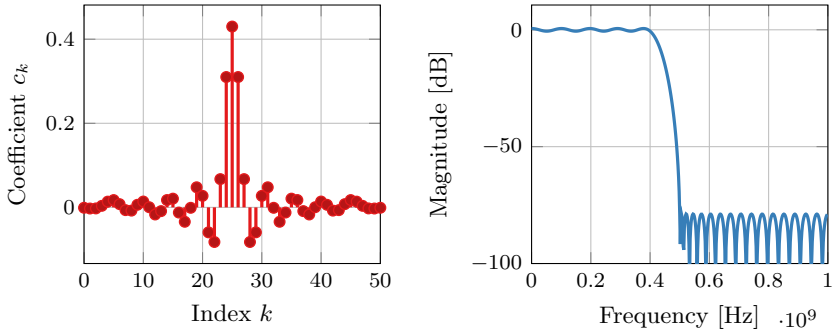



Figure 3.19: Coefficients and magnitude response in dB of a low-pass FIR filter with sample rate 2GHz.

**FIR filters** FIR filters are discrete-time filters with an impulse response of finite duration. Figure 3.18 illustrates the functioning of a FIR filter. At step $n$, the filter's input is $(x(n), x(n-1), ..., x(n-N+1))$, where $N$ is called the depth of the filter. The output is $y(n) = \sum_{k=0}^{N-1} c_k(n)x(n-k)$, where $c_k(n)$ are called the coefficients of the filter. It can be put in vector form as

$$y(n) = \mathbf{c}(n)^T \mathbf{x}(n) \tag{3.51}$$

where $\mathbf{c}(n) = [\, c_1(n) \dots c_{N-1}(n) \,]^T$ and $\mathbf{x}(n) = [\, x(n) \dots x(n-N+1) \,]^T$. For a given FIR filter, the discrete Fourier transform of $\mathbf{c}(n)$ gives the transfer function of the filter. In fact, it is possible to design any transfer function by carefully designing the coefficients and the depth of the FIR filter. As an example, Figure 3.19 shows the coefficients and the magnitude response of a low-pass FIR filter, with sample rate 2GHz.

**Butterfly adaptive equalizer** As already mentioned in the motivation of this subsection, the adaptive equalizer of digital coherent receivers has to estimate

$$\mathbf{H}_o(\omega)^{-1} = \begin{bmatrix} h_{HH}(\omega) & h_{HV}(\omega) \\ h_{VH}(\omega) & h_{VV}(\omega) \end{bmatrix}. \tag{3.52}$$

Each component $h_{..}(\omega)$ of the matrix can be performed by a FIR filter. Equation 3.50 imposes these four FIR filters to be laid out according to a butterfly structure, illustrated in Figure 3.20. The outputs of the filter $\hat{x}_H(n)$ and $\hat{x}_V(n)$, which are

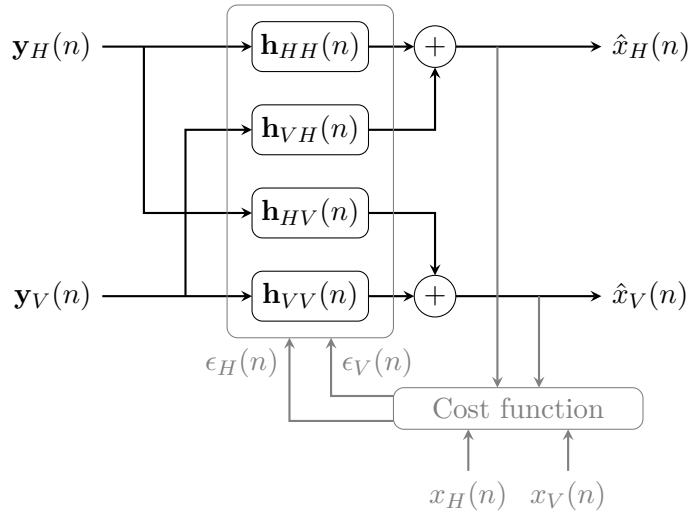



Figure 3.20: Adaptive polarization demultiplexing equalizer with "butterfly" structure.

estimations of the transmitted symbols $x_H(n)$ and $x_V(n)$, are given by

$$\hat{x}_H(n) = \mathbf{h}_{HH}(n)^T \mathbf{y}_H(n) + \mathbf{h}_{HV}(n)^T \mathbf{y}_V(n) \tag{3.53}$$

$$\hat{x}_V(n) = \mathbf{h}_{VH}(n)^T \mathbf{y}_H(n) + \mathbf{h}_{VV}(n)^T \mathbf{y}_V(n) \tag{3.54}$$

where $\mathbf{y}_H(n) = [y_H(n), ..., y_H(n-N+1)]^T$ and $\mathbf{y}_V(n) = [y_V(n), ..., y_V(n-N+1)]^T$ are the received complex amplitudes, $\mathbf{h}_{HH}(n)$, $\mathbf{h}_{HV}(n)$, $\mathbf{h}_{VH}(n)$, $\mathbf{h}_{VV}(n)$ are the coefficient of the four FIR filters corresponding to $h_{HH}(\omega)$, $h_{VH}(\omega)$, $h_{HV}(\omega)$ and $h_{VV}(\omega)$ respectively. Finally, the values of $\hat{x}_H(n)$, $\hat{x}_V(n)$, and eventually $x_H(n)$ and $x_V(n)$, are fed to a cost function which outputs $\epsilon_H(n)$ and $\epsilon_V(n)$. The coefficients are then updated in order to minimize this cost function, following the rule

$$\mathbf{h}_{HH}(n+1) = \mathbf{h}_{HH}(n) + \mu\epsilon_H(n)\hat{x}_H(n)\mathbf{y}_H(n)^* \tag{3.55}$$

$$\mathbf{h}_{HV}(n+1) = \mathbf{h}_{HV}(n) + \mu\epsilon_H(n)\hat{x}_H(n)\mathbf{y}_V(n)^* \tag{3.56}$$

$$\mathbf{h}_{VH}(n+1) = \mathbf{h}_{VH}(n) + \mu\epsilon_V(n)\hat{x}_V(n)\mathbf{y}_H(n)^* \tag{3.57}$$

$$\mathbf{h}_{VV}(n+1) = \mathbf{h}_{VV}(n) + \mu\epsilon_V(n)\hat{x}_V(n)\mathbf{y}_V(n)^* \tag{3.58}$$

where $\mu$ is a step-size parameter [82]. If the sampling rate is $n_{sps}$ samples per symbol, then the coefficients are updated every $n_{sps}$ steps. Depending on the cost function, several type of adaptive equalizers may be considered.

**Direct-detection least-mean-square (DD-LMS)** A simple cost function to minimize is the quadratic distance, which is used for the DD-LMS algorithm [83],

$$\epsilon_H(n) = |x_H(n) - \hat{x}_H(n)|^2 \tag{3.59}$$

$$\epsilon_V(n) = |x_V(n) - \hat{x}_V(n)|^2. \tag{3.60}$$

Of course, it requires the receiver to know the transmitted symbols, which can be done using training sequences. If training sequences are not possible in the system, another algorithm working in blind mode should be introduced.

**Constant modulus algorithm (CMA)** CMA is a blind algorithm which updates the coefficients so that $|\hat{x}_H(n)|^2$ and $|\hat{x}_V(n)|^2$ approach constant unity, using the following cost function [84],

$$\epsilon_H(n) = 1 - |\hat{x}_H(n)|^2 \tag{3.61}$$
$$\epsilon_V(n) = 1 - |\hat{x}_V(n)|^2. \tag{3.62}$$

It typically works well for modulation formats with constant modulus such as QPSK or M-PSK. However, it is also suitable for some higher order QAM constellations [85].

**Pilot aided algorithm** In order to facilitate the convergence of the algorithm, the transmitter can interleave in time a deterministic sequence of symbols, known to the receiver. This additional symbols are called *pilot symbols*, or pilots. To take advantage of this additional knowledge, one can use the error function of DD-LMS when $x(n)$ is a pilot and that of CMA otherwise [86]:

$$\epsilon_H(n) = (1 - p_H(n))(1 - |\hat{x}_H(n)|^2)\hat{x}_H(n) + p_H(n)|x_H(n) - \hat{x}_H(n)|^2, \tag{3.63}$$
$$\epsilon_V(n) = (1 - p_V(n))(1 - |\hat{x}_V(n)|^2)\hat{x}_V(n) + p_V(n)|x_H(n) - \hat{x}_H(n)|^2, \tag{3.64}$$

where $p_{H,V}(n)$ is equal to 1 if the symbol $x_{h,V}(n)$ is a pilot and 0 otherwise.

**Clock phase recovery** As explained earlier, FIR filters can approach any transfer function, so long as the number of coefficients is large enough. When approaching the transfer function $\exp(j\omega\Delta\tau)$, FIR filters operates a time-shift with delay $\Delta\tau$. Therefore, they are able to apply quasi-continuous time delays to an input signal, even with discrete samples.

During adaptive equalization, the four FIR filters delay each I/Q signal such that one out of every $n_{sps}$ samples coincides with the optimal sampling time [72]. Therefore, the adaptive equalizer performs a clock phase recovery function. This phenomenon is illustrated in Figure 3.21 for $n_{sps} = 2$. In (a), the arrows represent the sampled signal with oversampling of 2 samples per symbol. The clock phase has not been optimized. After adaptive equalization in (b), the signal was delayed by a continuous time-shift $\Delta\tau$. Only one out of two samples are kept, at the center of the symbol time interval, where the pulse shape has maximal amplitude. The symbol decision can be performed with these optimal samples.

Let's remark that the FIR filters correct the clock phase of each polarization independently. Moreover, this clock recovery function works even when the clock frequency is not locked between the transmitter and receiver, if enough coefficients are used [87].

### 3.5.3 Carrier estimation

As mentioned in the architecture of an intradyne receiver, the LO angular frequency $\omega_l$ and phase $\phi_l$ don't have to be strictly locked to the frequency $\omega_s$ and phase $\phi_s$ of the signal. However, the intermediate frequency $\omega_{IF}$ and total phase noise $\phi_n$ must

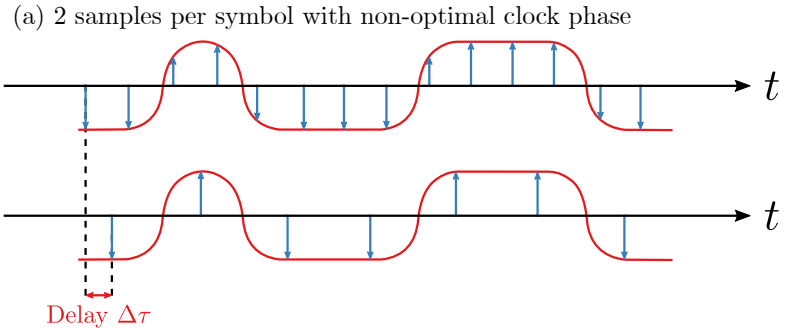



Figure 3.21: Principle of clock-phase recovery with adaptive equalizer. As shown in (a), the sampled signal exhibits a time shift relative to the transmitter clock. After equalization, one out of every two sample points comes to the optimal position of the pulse, in the center where the amplitude is maximal, as shown in (b).

be estimated by the DSP to correctly recover the symbols. This is achieved by a coarse estimation of $\omega_{IF}$, followed by a finer estimation of the slower phase noise $\phi_s$ and the residual frequency offset.

If we assume that other impairments have been correctly compensated for, we can model the complex received symbols $(y_k)$ on one polarization by

$$y_k = x_k e^{j(k\theta+\phi_k)} + n_k \tag{3.65}$$

where $(x_k)$ are the complex transmitted symbols, $\theta = \omega_{IF} T_S$ accounts for the impact of $\omega_{IF}$ on discrete symbols sampled at time $kT_S$ with $T_S$ the symbol period, $\phi_k = \phi_n(kT_S)$ is the phase noise and $n_k$ is an additive white Gaussian noise.

**Carrier frequency estimation** First of all, $\phi_k$ is slowly varying compared to $k\theta$. Therefore, we can divide the signal into frames of $N$ symbols where $\phi_k$ can be assumed constant equal to $\phi_0$. Thus, the received symbol along the frame are

$$y_k = x_k e^{j(k\theta+\phi_0)} + n_k. \tag{3.66}$$

When using QAM formats, we can rely on a consequence of the constellation circular symmetry stating that $E(x_k^4) \neq 0$. Let's decompose $y_k^4$ as $E(y_k^4) + e_k$ where $e_k$ is a zero-mean process that can be understood as a disturbance. We have that

$$\begin{aligned} y_k^4 &= (x_k e^{j(k\theta+\phi_0)} + n_k)^4 && (3.67)\\ &= x_k^4 e^{j4(k\theta+\phi_0)} + 4x_k^3 e^{j3(k\theta+\phi_0)} n_k + 6x_k^2 e^{j2(k\theta+\phi_0)} n_k^2 && (3.68)\\ &\quad + 4x_k e^{j(k\theta+\phi_0)} n_k^3 + n_k^4 && (3.69) \end{aligned}$$

Therefore, $(n_k)$ being circularly-symmetric Gaussian noise, we obtain

$$E(y_k^4) = A_0 e^{j4k\theta} \tag{3.70}$$

with $A_0 = E(x_k^4)E(e^{j\phi_0})$ a constant. Then, $y_k^4$ is decomposed as

$$y_k^4 = A_0 E(e^{j\phi_0}) e^{j4k\theta} + e_k. \tag{3.71}$$

Then, we remark that $(y_k)$ is a constant amplitude complex exponential with angular frequency $4\theta$ disturbed by a zero-mean additive noise. As a consequence, the periodogram of $(y_k)^4$ exhibits a peak at angular frequency $4\theta$. Therefore, $\theta$ can be estimated by the argmax of the periodogram [88],

$$\hat{\theta} = \frac{1}{4}\underset{\theta}{\operatorname{argmax}}\left|\frac{1}{N}\sum_{k=0}^{N-1}(y_k)^4 e^{-j\theta k}\right|^2. \tag{3.72}$$

where $N$ is the number of symbols in the frame.

**Carrier phase estimation** After frequency estimation, the received symbols are

$$y_k = x_k e^{j\phi_k} + n_k \tag{3.73}$$

The phase noise $\phi_k$ can be estimated using the blind phase search (BPS) algorithm [89]. The idea is to find an angle $\psi$ that minimizes a cost function, typically the quadratic distance between $y_k e^{-j\psi}$ and the decision symbol $\hat{d}(y_k e^{-j\psi})$, where $\hat{d}(z)$ is the point of the constellation that minimizes the distance to the complex number $z$. The cost function is averaged over $2N+1$ symbols, hence the estimation

$$\hat{\phi}_k = \underset{\psi\in[-\pi,\pi]}{\operatorname{argmin}}\sum_{l=-N}^{N} c(y_{k+l},\psi) \tag{3.74}$$

with the cost function $c(z,\psi)$ being given by

$$c(z,\psi) = \left|ze^{-j\psi} - \hat{d}(ze^{-j\psi})\right|^2 \tag{3.75}$$

Since QAM formats exhibit a rotational symmetry of order 4, $c(z,\psi)$ is $\pi/2$-periodic with $\psi$. Hence, it doesn't have a global minimum on $[-\pi,\pi]$. That's why the minimum will be determined for $\psi \in [0,\pi/2]$. To remove the remaining ambiguity on $\phi_k$, the algorithm uses an unwrap function which removes discontinuities of $\phi_k$, as well as regularly spaced pilot symbols.

Like the adaptive equalizer, this algorithm can be updated to take into account pilot symbols. In that case, the cost function is given by,

$$c(y_k,\psi) = (1-p_k)\left|y_k e^{-j\psi} - \hat{d}(y_k e^{-j\psi})\right|^2 + p_k\left|y_k e^{-j\psi} - x_k\right|^2 \tag{3.76}$$

where $p_k$ is equal to 1 if the symbol $x_k$ is a pilot and 0 otherwise.

### 3.5.4 Final equalizer and parameter estimation

After digital signal processing, the receiver obtains for each quadrature a sequence of real symbols $(y_k)$ expressed in V, that can be modeled by

$$y_k = x_k + w_k \tag{3.77}$$

where $(x_k)$ corresponds to the transmitted symbols after attenuation and $(w_k)$ is additive white Gaussian noise (AWGN). Of course, the $(x_k)$ symbols are unknown

to the receiver. That is why a fraction of $N$ transmitted symbols are revealed for performance analysis. However, the revealed symbols $(\tilde{x}_k)$ are only proportional to the $(x_k)$ by a normalization factor. For the sake of simplicity, let's assume that $(\tilde{x}_k)$ was revealed for $1 \leq k \leq N$. The normalization factor $\rho$ such that $x_k = \rho\tilde{x}_k$ can be estimated by

$$\hat{\rho} = \frac{\sum_{k=1}^{N} \tilde{x}_k y_k}{\sum_{k=1}^{N} \tilde{x}_k^2}. \tag{3.78}$$

Then, the signal to noise ratio is estimated by

$$SNR = \left( \frac{\sum_{k=1}^{N} y_k^2}{\sum_{k=1}^{N} x_k^2} - 1 \right)^{-1}. \tag{3.79}$$

## 3.6 Towards a high-rate CV-QKD system

In this thesis, we aim to exploit the techniques and algorithms presented in this chapter, in order to design a CV-QKD system that can operate at high symbol frequencies. Let us summarize the main features we propose to implement.

- We opt for *PCS-QAM modulation formats*, whose security has been demonstrated in Chapter 2.
- To improve spectral efficiency, the signal is generated digitally with an *RRC pulse shape*, as described in subsection 3.5.1. Therefore, we need some digital to analog converter.
- *Polarization division multiplexing* is carried out. Thus, two CV-QKD protocols occur in parallel on two different channels, corresponding to orthogonal polarization states. Therefore, we need to use dual-polarization optical modulators and receivers.
- We measure both quadrature operators. Therefore, we need to use phase-diversity receivers, as described in subsection 3.3.2.
- We use digital signal processing algorithms presented in Section 3.5, allowing modifications that do not increase the complexity.

The specific constraints of QKD require certain adjustments. The main feature is the low power of the received signal. Indeed, this is imposed by the optimization of the key rate and the impossibility of using optical amplifiers. It is thus necessary to adapt the DSP so that it can function under these extreme conditions, while keeping the excess noise at a minimal level. That's why we add one last feature:

- The PCS-QAM symbols are interleaved in time with QPSK symbols with higher amplitude, called *pilots*. The power and frequency of these pilots must be sufficient for the DSP to work properly.

In the next chapter, we describe the practical realization of such a CV-QKD system and its performance.

# Chapter 4

# Experimental system and results

## 4.1 Experimental system and implementation

### 4.1.1 Experimental hardware

The main idea behind the development of the experimental system was to use off the shelf equipment in order to provide an easily implementable high-rate CV-QKD solution. To achieve the best performance, we selected the latest generation of instruments. The main requirements were high vertical resolution for the analog to digital and digital to analog converters, low level of noise and a bandwidth of at least 1 GHz.

Figure 4.1 depicts the system on Alice's side. A 16 bits and 5 GSamples/s Arbitrary Waveform Generator (AWG) outputs four radio-frequency (RF) signals, each one corresponding to one quadrature of one orthogonal polarization. The signal is modulated onto the electric field of coherent light using a Fujitsu integrated IQ dual polarization modulator which is composed of two dual-nested Mach-Zehnder modulators, as presented in 3.2. The light source is a Pure Photonics telecommunication tunable laser with 10 kHz nominal linewidth. A variable optical attenuator (VOA) followed by an optical powermeter are used to monitor the modulation variance $V_A$.

Bob's system is outlined in Figure 4.2. The received optical signal is converted to the electrical domain using a dual polarization coherent receiver, described in Section 3.3. The receiver is either a 20 GHz integrated coherent receiver, referred to

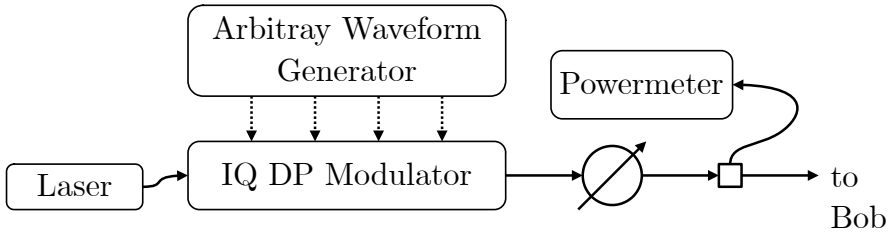



Figure 4.1: Alice's system featuring a 10 kHz linewidth laser source, a standard IQ dual polarization optical modulator, a 5GS/s and 16 bits arbitrary waveform generator, a variable optical attenuator and a powermeter.

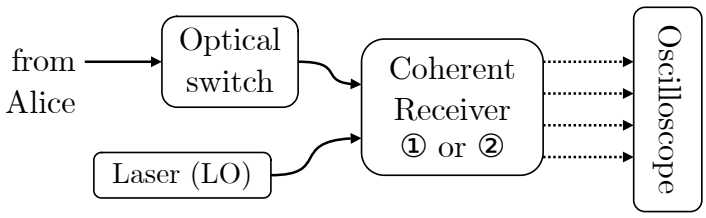



Figure 4.2: Bob's system featuring coherent receiver ① or ②, a 10 kHz linewidth laser as local oscillator, a 1 GHz oscillocope with 5 GS/s sampling rate and 10 bits vertical resolution, and a fast optical switch.

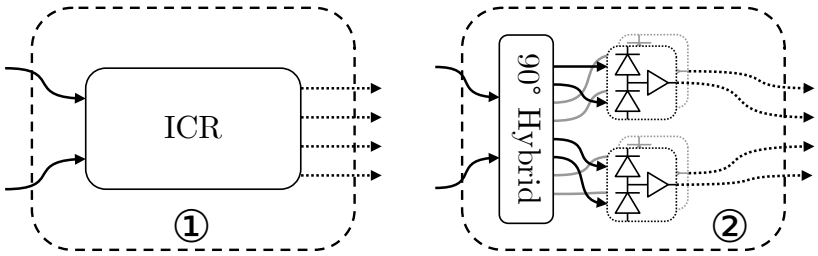



Figure 4.3: Bob's coherent optical receiver is either ① an 20 GHz integrated coherent receiver (ICR) or ② a 90° hybrid combined with four 1.6 GHz amplified balanced photodetectors.

as receiver ①, or an assembly of a 90° hybrid with four 1.6 GHz amplified balanced photodiodes, referred to as receiver ②, as illustrated in Figure 4.3. The local oscillator is identical to Alice's laser. The electrical outputs of the coherent receiver are sampled using a 1 GHz real-time oscilloscope with 5GS/s sampling rate and 10 bits vertical resolution. The sampled waveforms are stored on a hard drive for offline digital signal processing (DSP). Moreover, an optical switch is located before the signal input. It is used to periodically calibrate the shot noise, as will be discussed in subsection 4.1.2.

### 4.1.2 Noise calibration

For each quadrature of each polarization mode, the received symbol variance $V_B$ has to be expressed in shot noise units (SNU). However, Bob effectively measures samples $U$ of an electrical voltage expressed in volts (V). Thus, he obtains a variance $\mathrm{Var}(U)$ in $\mathrm{V}^2$. Hence, he needs to estimate the factor $N_0$ such that $\mathrm{Var}(U) = N_0 \times V_B$. $N_0$ is actually the variance of the shot noise expressed in $\mathrm{V}^2$. A first possible approach would be to give an expression of $N_0$ using a model for the receiver, for example with equations detailed in subsection 3.3.4. A more practical approach would be to experimentally monitor its value. We remind that, for simultaneous detection of both quadratures, Bob's variance is given by

$$V_B = \frac{\eta T}{2} V_A + 1 + V_{el} + \xi_B \tag{4.1}$$

where 1 stands for the shot noise variance, $V_{el}$ the electronic noise variance in SNU and $\xi_B$ the excess noise variance in SNU. When disconnecting the signal input of the

receiver, the output of the receiver is the sum of the shot noise and the electronic noise. Therefore Bob can measure

$$\mathrm{Var}(U) = N_0(1 + V_{el}). \tag{4.2}$$

Then, disconnecting the LO input, Bob measures only the electronic noise,

$$\mathrm{Var}(U') = N_0 V_{el}. \tag{4.3}$$

And finally $N_0 = \mathrm{Var}(U) - \mathrm{Var}(U')$. In our experimental system, this procedure gives four different values $N_0^{(1)}$, $N_0^{(2)}$, $N_0^{(3)}$, and $N_0^{(4)}$, one for each balanced photodetector in the receiver. Unfortunately, the samples measured on a channel are a mix of the quadratures of the coherent states sent by Alice. This comes from several channel impairments such as polarization mode dispersion (PMD) or carrier phase noise. As a consequence, if the $N_0^{(i)}$ are not all equal, they do not correspond to the variances of the shot noise on the quadratures effectively transmitted by Alice. To tackle this issue, we apply to the shot noise samples, recorded during the calibration, the correction of the involved impairments, and estimate the variances afterwards. In other words, the DSP operations (addition, multiplication, ...) applied to the signal samples are simultaneously applied to the noise samples.

To illustrate this, let's detail the case of PMD. When Alice sends coherent states $|\alpha_H\rangle$ and $|\alpha_V\rangle$ on respectively the horizontal and vertical polarization, the polarization state can be represented as a complex column vector $\mathbf{x}$ with size 2×1,

$$\mathbf{x} = \begin{bmatrix} q_H + ip_H \\ q_V + ip_V \end{bmatrix}. \tag{4.4}$$

PMD is modeled by a 2×2 Jones matrix $J$, with $\det(J) = 1$ [90]. The noisy polarization state received by Bob is $\mathbf{y} = J\mathbf{x} + \mathbf{n}$, where

$$\mathbf{n} = \begin{bmatrix} n_1 + in_2 \\ n_3 + in_4 \end{bmatrix}. \tag{4.5}$$

$n_1$, $n_2$, $n_3$, and $n_4$ are additive white Gaussian noise of variance respectively $N_0^{(1)}$, $N_0^{(2)}$, $N_0^{(3)}$, and $N_0^{(4)}$. Assuming perfect DSP, Bob finds $J$ and outputs the corrected noisy polarization state

$$\tilde{\mathbf{y}} = \mathbf{x} + J^{-1}\mathbf{n}. \tag{4.6}$$

Thus, the noise observed by Bob is $J^{-1}\mathbf{n}$. For example with the frequency independent polarization rotation matrix

$$J^{-1} = \frac{1}{2}\begin{bmatrix} 1 & i\sqrt{3} \\ i\sqrt{3} & 1 \end{bmatrix}, \tag{4.7}$$

we obtain

$$J^{-1}\mathbf{n} = \frac{1}{2}\begin{bmatrix} (n_1 + \sqrt{3}n_4) + i(n_2 - \sqrt{3}n_3) \\ (n_3 + \sqrt{3}n_2) + i(n_4 - \sqrt{3}n_1) \end{bmatrix}. \tag{4.8}$$

The variances of the effective shot noise are then

$$N_0^{(IH)} = \frac{N_0^{(1)}}{4} + \frac{3N_0^{(4)}}{4}, \tag{4.9}$$

$$N_0^{(QH)} = \frac{N_0^{(2)}}{4} + \frac{3N_0^{(3)}}{4}, \tag{4.10}$$

$$N_0^{(IV)} = \frac{N_0^{(3)}}{4} + \frac{3N_0^{(2)}}{4}, \tag{4.11}$$

$$N_0^{(QV)} = \frac{N_0^{(4)}}{4} + \frac{3N_0^{(1)}}{4}. \tag{4.12}$$

Therefore, $N_0^{(1)}$, $N_0^{(2)}$, $N_0^{(3)}$ and $N_0^{(4)}$ don't necessary give the variance of the shot-noise effectively applied to the quadratures sent by Alice. This simple example illustrates the necessity of applying DSP corrections to the noise samples and estimating the shot noise variance and electronic noise variance on the output.

Moreover, the shot noise variance may also vary with time. Hence, it is necessary to periodically reiterate the shot noise calibration procedure, as studied in reference [91]. To increase the precision, this calibration should be reiterated as often as possible. As already mentioned in subsection 4.1.1, Bob's setup includes a fast optical switch used to turn on and off the signal light coming from Alice. Using a micro-controller to synchronize the switch to the trigger of the oscilloscope, we are able to consecutively perform noise calibration and signal acquisition with minimal delay. This way, each acquired block of signal comes with its own noise calibration, with the same duration. Let's remark that this method consumes time, and therefore decreases the final key rate. The impact of this calibration procedure on the final key rate will be discussed in Chapter 5.

### 4.1.3 Low frequency noise and single-side band

The first experimental tests of the system showed that the excess noise was too high to enable the distribution of secret keys. A spectral analysis of the excess noise indicated the predominance of low frequency components between DC and a few tens of MHz. To illustrate this phenomenon, Figure 4.4 plots the power spectral density of the experimental excess noise using receiver ①. One identified source of this noise was caused by the electrical driver amplifiers placed between the AWG outputs and the optical modulator. They attenuated low frequencies of the signal, their nominal cutoff frequency being 20 MHz. Removing them from the system reduced the low frequency noise. However, other noise sources around DC remained in the hardware, both at the transmitter and receiver's side. To avoid their negative impact on the performance, we decided to shift the signal spectrum such that it doesn't have any frequency component in the noisy range. The result is that the spectrum of the complex signal has only positive frequency components. Therefore, it is called a single-side band signal. Figure 4.5 illustrates an example of single-side band signal. Let's emphasize that the operation of frequency shift is performed on the digital signal given to the AWG, such that the electrical signals generated by the AWG have no component around DC. Similarly, we can also generate a single-side band signal with only negative frequencies, represented by a dashed line in Figure 4.5. The

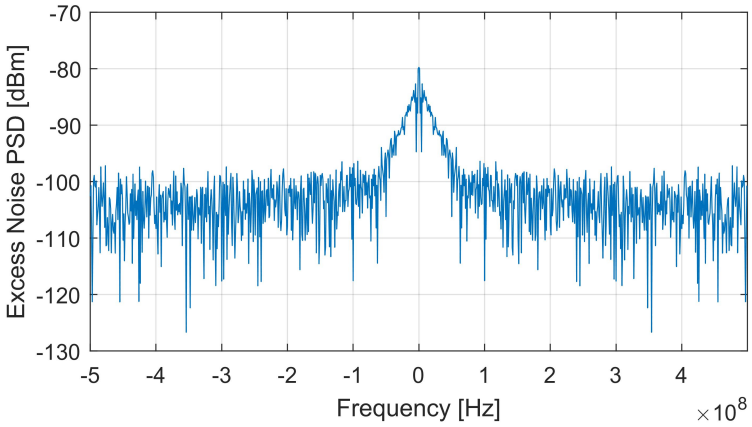



Figure 4.4: Power spectral density of experimental excess noise around DC. We observe the presence of low frequency components with high magnitude.

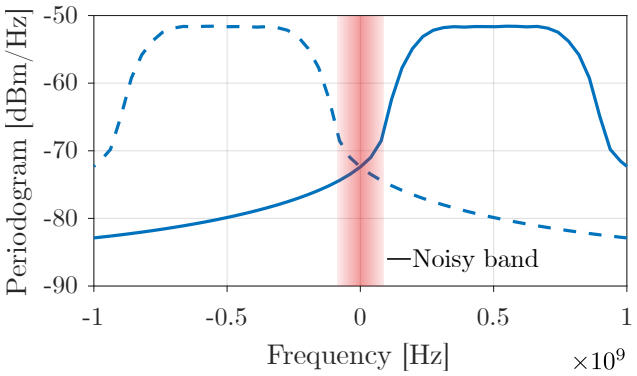



Figure 4.5: Example of a single-side band signal with 600 MBd symbol rate, RRC pulse shape and roll-off factor 0.4. The dashed line represents a signal with symmetric magnitude spectrum, with only negative frequencies. The sum of both gives a digital dual-carrier signal.

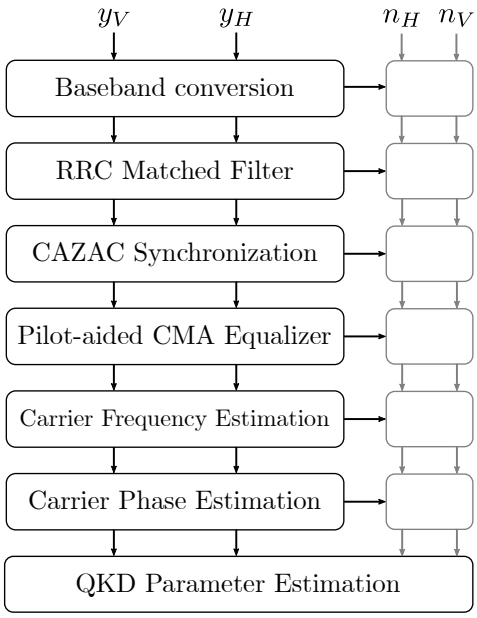



Figure 4.6: Bob's digital signal processing building blocks, detailed in Chapter 3.

sum of both single-side band signals is called digital dual-carrier signal. Modulating such a dual band signal is equivalent to sending two independent QKD signals on two separate subcarriers. However, digital dual carrier signals exhibit crosstalk between the two bands, caused by imperfect modulation, which increases the excess noise in the context of CV-QKD. Hence, digital dual carrier would require additional digital signal processing to correct this impairment. We did not have time to implement this approach in the present thesis, and it remains open for future developments. Therefore, the experiments presented in the following chapter are performed with only single-side band signals.

The use of a single side band signal for CV-QKD comes with potential issues for security. In fact, due to imperfect modulation, a small fraction of the signal may leak to the band symmetrical to the signal bandwidth with respect to the carrier. This leakage creates a side channel that Eve can take advantage of. As studied in [92], this side channel attack can be partially mitigated but results in some reduction of the final length of the secret key. However, we did not have the time to investigate further this topic for our experimental system. Therefore, this side channel attack is neglected in the following experimental results. In a digital dual carrier configuration, the impairment is compensated for by DSP, therefore the side channel is mitigated.

### 4.1.4 Digital Signal Processing

Digital signal processing (DSP) is one the most important practical challenge of this work. The different DSP building blocks are reminded in 4.6. They are based on algorithms used in classical optical transmission [86]. The DSP inputs four sampled waveforms $y_1(k)$, $y_2(k)$, $y_3(k)$, $y_4(k)$ with $n_{sps}$ samples per transmitted symbol. The waveforms are assembled into two complex waveforms $y_H(k) = y_1(k) + jy_2(k)$ and

$y_1(k) + jy_2(k)$. Then, if the signal is single-side band, as described in subsection 4.1.3, it is converted into a baseband signal through a digital frequency shift. Then, a digital filter matching the pulse shape is applied. In our case, we use root-raised cosine (RRC) filters with a given roll-off factor $\rho$ and symbol duration $T_S$, as described in subsection 3.5.1. Then, auto-correlation on the signal is computed in order to retrieve the beginning of the pilot sequence, which was coded with a constant amplitude zero autocorrelation waveform (CAZAC) sequence [93]. Then, linear impairments are compensated for using pilot-aided CMA adaptive equalizer, as described in subsection 3.5.2. Then, carrier frequency and carrier phase estimation algorithms are consecutively applied. Finally, using the noise calibration symbols which underwent the same DSP operations, QKD parameters are estimated to compute an estimate of the achievable secret key rate using the equations detailed in Chapter 2.

These algorithms are obviously unable to perfectly correct channel impairments. These DSP imperfections may be seen as sources of excess noise. Therefore it is crucial to optimize the various DSP parameters to obtain minimal values of excess noise. In this work, the optimization procedure is performed offline on a few acquisitions of the signal, and is described in subsection 4.3.3.

**Pilot amplitude** To correctly retrieve the low SNR QKD symbols, the DSP relies on QPSK pilot symbols with higher power than the QKD symbols. The amplitude of the pilots should also be optimized, using a procedure to be done before signal acquisition. To do so, we acquired QKD signals with various values of pilot over QKD signal power ratio, and applied DSP to estimate the excess noise. Figure 4.7(a) gives boxplots for the experimental excess noise $\xi_B$ for 15 acquisitions of PCS 1024-QAM QKD signal for pilots over QKD symbols power ratio ranging from 12 dB to 17 dB. Using the results of this experiment, we fixed 14 dB of pilots over QKD symbols power ratio for our protocol.

**Pilot rate** The same optimization should also be performed for pilot rate. Contrary to pilot amplitude, the criterion to optimize pilot rate is not the excess noise. In fact, if an increase of the pilot rate decreases the excess noise, it also decreases the rate of QKD symbols. Hence, we need to optimize directly the SKR. Figure 4.7(b) gives boxplots for the experimental achievable secret fraction, for 15 acquisitions of PCS 1024-QAM QKD signal, with receiver ①, for several relevant pilot rates. We fixed our pilot rate to 4 pilots over 8 symbols. Hence, half of the transmitted symbols are actually pilots. Therefore, the final SKR is divided by two.

## 4.2 PCS 1024-QAM with Integrated Coherent Receiver

### 4.2.1 Security of PCS 1024-QAM

The first experiment, presented at the Optical Fiber Conference (OFC) 2021 conference [51], demonstrated the feasibility of using PCS 1024-QAM format to achieve several Mb/s of secret key rate. At the time, no security proof for $M$-QAM formats were available to our knowledge. To derive secret key rates, we tried to quantify

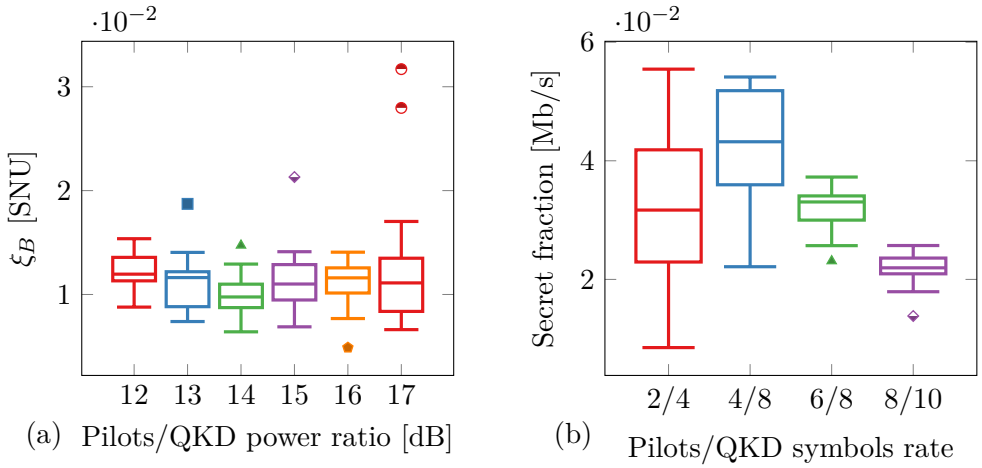



Figure 4.7: Boxplot of the experimental excess noise variance, for (a) several values of the pilot to signal power ratio, and (b) several values of the pilot rate. The boxplot shows the minimal and maximal value, the median, the first and third quartiles, for 15 experimental acquisitions.

how well the PCS 1024-QAM format approximates the Gaussian modulation format. We used the approach described in reference [94], which investigates the impact of quantization on the security of a Gaussian modulation CV-QKD protocol. We compute the trace distance $\epsilon_{prep}$ between the density matrices $\rho$ and $\sigma$ corresponding to statistical mixture of respectively the ideal Gaussian modulation and the PCS QAM format. If the thermal state protocol is $\epsilon$-secure, then the practical protocol is $(\epsilon + \epsilon_{prep})$-secure. In our case with PCS-1024-QAM, the quantum states $\rho$ and $\sigma$ are given by

$$\rho = \sum_n \frac{\langle n \rangle^n}{(1+\langle n \rangle)^{n+1}} |n\rangle\langle n| \tag{4.13}$$

$$\sigma = \sum_{k=1}^{1024} \pi_k |\alpha_k\rangle\langle\alpha_k| \tag{4.14}$$

where $\pi_k$ is the probability of sending state $|\alpha_k\rangle$. For the PCS 1024-QAM, we remind that

$$\pi_k = P(|\alpha_k\rangle) = P(|\frac{q_k + ip_k}{2}\rangle) = \frac{e^{-\nu(q_k^2+q_k^2)}}{\sum_l e^{-\nu(q_l^2+p_l^2)}} \tag{4.15}$$

where $\nu$ is a free parameter. To obtain a modulation variance $V_A = \langle n \rangle/2$, we have to consider the constellation points

$$q_k, p_k \in (q_j, p_j) \in \{\pm\gamma, \pm 3\gamma, ..., \pm 31\gamma\}^2 \tag{4.16}$$

such that

$$\sum_{k=1}^{1024} \pi_k |\alpha_k|^2 = 2V_A. \tag{4.17}$$

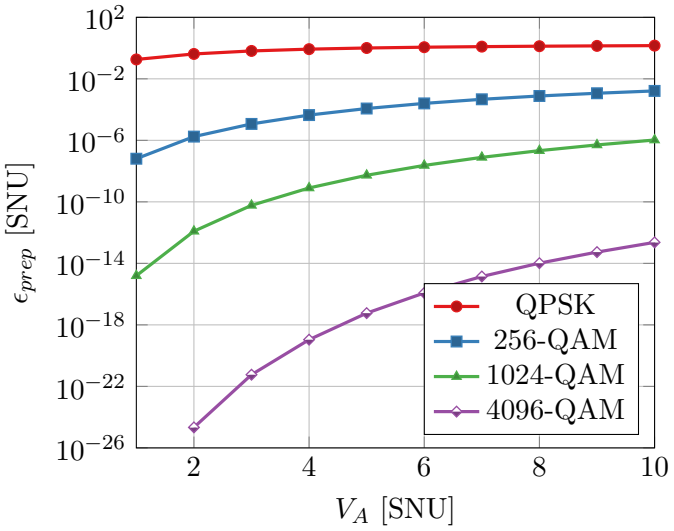



Figure 4.8: Trace distance $\epsilon_{prep}$ to the ideal thermal state, given as a function of Alice variance $V_A$ in SNU, for QPSK, PCS 256-QAM, PCS 1024-QAM, and PCS 4096-QAM formats. For PCS QAM formats, the free parameter $\nu$ in (4.15) was chosen to minimize $\epsilon_{prep}$ for each marker point.

We also remind that the trace distance is given by

$$\epsilon_{prep} = \|\rho - \sigma\| = \mathrm{Tr}\left[\sqrt{(\rho-\sigma)^\dagger(\rho-\sigma)}\right]. \tag{4.18}$$

Numerical evaluations for $V_A$ ranging bewteen 1 SNU and 10 SNU are given in Figure 4.8 with comparison to similar calculation for QPSK, PCS 256-QAM and PCS 4096-QAM. Note that for each marker point, the free parameter $\nu$ of the PCS-QAM format was chosen to minimize the trace distance. We observe that $\epsilon_{prep}$ decreases by several order of magnitude as $V_A$ decreases, and as the cardinality of the QAM increases. For PCS 1024-QAM and $V_A$ ranging from 1 SNU to 10 SNU, $\epsilon_{prep}$ goes from $1.6 \times 10^{-15}$ SNU to $1.1 \times 10^{-6}$ SNU. In [51], we assumed that these values were low enough to provide sufficient security using the Gaussian modulation protocol. With the security proof for an arbitrary discrete modulation protocol, described in Chapter 2, we can analyze whether this assumption was realistic. We compare the asymptotic secret fraction of the Gaussian modulation protocol $r$ to the arbitrary discrete modulation protocol with PCS 1024-QAM format $r'$, and plot in Figure 4.9 the relative error $\Delta r/r = (r-r')/r$ given as a function of the modulation variance $V_A$. The parameters used to compute the secret fractions are close to the experimental parameters of [51]. We observe that, as expected, the relative error decreases with $\epsilon_{prep}$. Moreover, in our range of $V_A$, the relative error is lower than $10^{-3}$. Hence, the approximation of using the Gaussian modulation protocol security proof gives results with a precision of three significant digits. As a conclusion, this analysis validates the approximation used in [51]. It also confirms the intuition in reference [94], that the $(\epsilon + \epsilon_{prep})$-security assumption was too pessimistic. For example, $\epsilon_{prep}$ values of the order $10^{-6}$ are too high to insure security with this assumption. However they

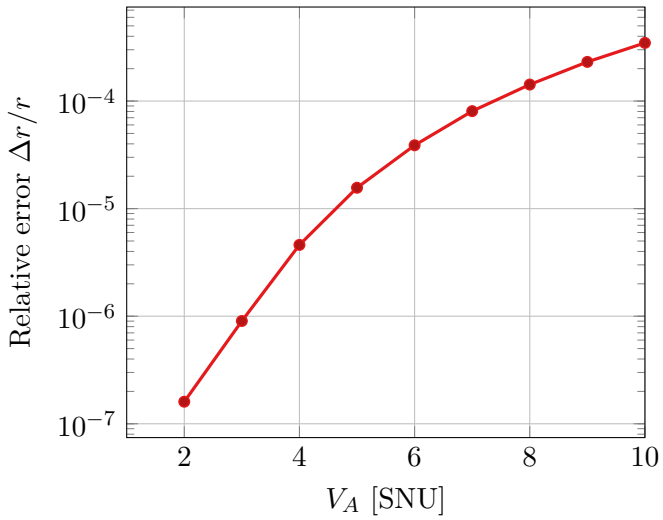



Figure 4.9: Relative error $\Delta r/r = (r - r')/r$ where $r$ and $r'$ are the asymptotic secret fractions in secret bits per transmitted symbols of respectively Gaussian modulation protocol and PCS 1024-QAM protocol with optimized free parameter $\nu$, given as a function of the modulation variance $V_A$ in SNU. The parameters used to derive the secret fractions are transmittance $T = -2.2\,\text{dB}$, quantum efficiency $\eta = 0.65$, excess noise $\xi_B = 0.01\,\text{SNU}$, reconciliation efficiency $\beta = 0.95$, and trusted noise $V_{el} = 0.1\,\text{SNU}$.

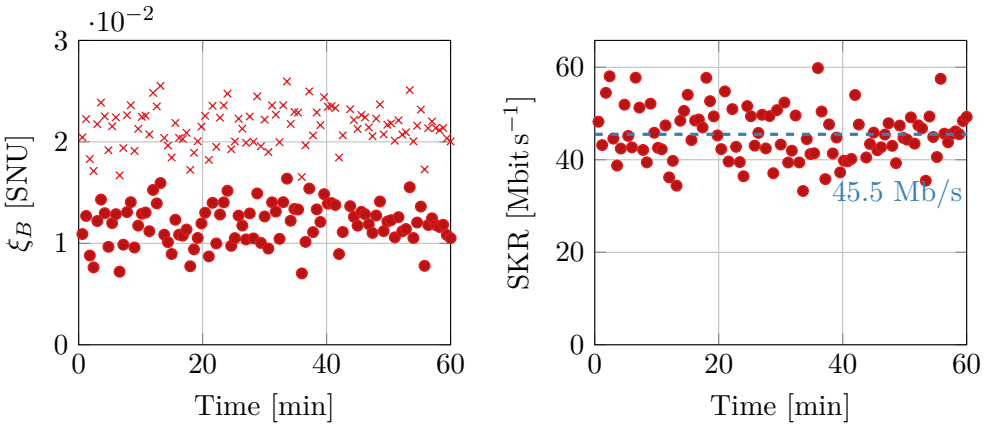
give valid approximations of Gaussian modulation format, like for PCS 1024-QAM with $V_A = 10\,\text{SNU}$.

### 4.2.2 Characterization of receiver ①

To characterize the quantum efficiency of receiver ①, we simply characterize the responsivity at wavelength $\lambda = 1550\,\text{nm}$. Using a monitoring output of the receiver, the electrical currents of each photodiode are measured. The optical power of the signal input takes values ranging between $0\,\text{dBm}$ and $12\,\text{dBm}$. The LO input is turned off, because we are interested in the efficiency of the signal input. The slope of the least squares regression line gives the receiver's responsivity $R_\lambda = 0.8\,\text{A}\,\text{W}^{-1}$, which corresponds for $\lambda = 1550\,\text{nm}$ to quantum efficiency

$$\eta = \frac{R_\lambda}{\lambda} \times \frac{hc}{e} = 0.64 \tag{4.19}$$

We observe that the current is not exactly a linear function of the input optical power. In fact, it scales linearly for optical power values under $12\,\text{dBm}$, then starts to slowly saturate. Hence, the linear regression must be done on a range where the scaling is linear. In our case, we chose $6\,\text{dBm}$ to $12\,\text{dBm}$. The coefficient of determination is estimated to $r^2 = 0.9994$, from which we deduce that the estimation of the responsivity $R$ is correct enough.




(a) Excess noise

(b) Secret key rate

Figure 4.10: (a) Estimated excess noise variance at Bob's site $\xi_B$, worst case estimator (cross marks) and (b) corresponding secret key rate SKR for each block of acquired data during a 1 hour long experiment, plotted as a function of the acquisition time. The experiment is performed with integrated coherent receiver ①, as described in subsection 4.2.3.

### 4.2.3 OFC 2021 results

As mentioned in subsection 4.2.1, the first successful experiment was based on PCS 1024-QAM because its cardinality was high enough to be considered as an approximation of a Gaussian modulation protocol. The free parameter of the PCS 1024-QAM was set to $\nu = 0.0198$, which minimizes the trace distance for the target modulation variance $V_A$. The signal was prepared with symbol rate 400 MBd and RRC pulse shape with roll-off factor 1. Using the experimental system described in Section 4.1.1, with receiver ① characterized in subsection 4.2.2, we performed 100 acquisitions of the signal during 1 hour. The quantum channel was a standard single mode fiber (SMF) link of 9.5 km with 2.2 dB characterized loss. As described in subsection 4.1.2, each signal acquisition was immediately preceded by a calibration of the shot noise. Figure 4.10a shows the measured excess noise variance $\xi_B$ at Bob's side in SNU for each acquisition. The average $\xi_B$ was 0.012 SNU while the maximal value was 0.016 SNU. The excess noise variance was estimated using the standard estimator of the variance for each block of acquisition, with size $N = 1.8 \times 10^6$ symbols. The cross marks in Figure 4.10a shows the worst case excess noise for each acquisition block, with security parameter $\epsilon = 10^{-8}$. We measured an average modulation variance $V_A = 8.22$ SNU. Figure 4.10b shows the SKR for the corresponding excess noise of Figure 4.10a. Unlike published work in [51], we compute here the SKR using the analytic computation for arbitrary discrete modulation described in Chapter 2. The receiver is trusted, with calibrated electronic noise variance $V_{el} = 0.08$. Finite size effects are taken into account using the worst case excess noise. We assume reconciliation efficiency $\beta = 0.95$. We remind that the formula for the secret key rate is

$$SKR = 2R_S \left(1 - R_{pilots}\right) \left(\beta I_{AB} - \chi_{EB}\right) \tag{4.20}$$

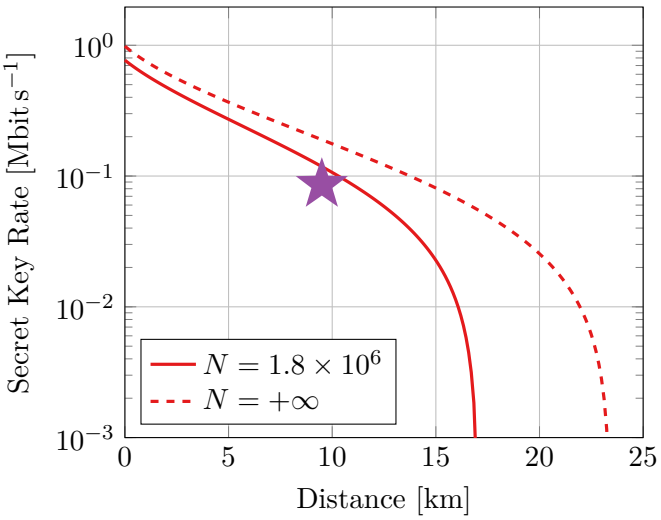



Figure 4.11: Secret fraction vs. distance (assuming SMF with 0.2 dB/km nominal loss), with $\xi_B = 0.016$ SNU and $\beta = 0.95$, plotted for finite size with worst case estimator 0.025 SNU and security parameter $\epsilon = 10^{-8}$, and in the asymptotic case. The star gives the worst experimental secret fraction at 9.5 km of SMF, with 2.2 dB loss.

where 2 comes from the polarization multiplexing, $R_S$ is the symbol rate ($R_S = 400$ MBd), $R_{pilots}$ the pilot rate ($R_{pilots} = 1/2$), $I_{AB}$ the mutual information between Alice and Bob and $\chi_{EB}$ is the Holevo information between Eve and Bob. The averaged achievable secret key rate over 100 acquisitions is 45.5 Mb/s with minimal and maximal values 33.2 and 59.8 Mb/s. Finally, Figure 4.11 shows a theoretical curve for the secret fraction in bits per symbol as a function of the distance, assuming SMF with 0.2 dB loss per km. This secret fraction is given for the maximal experimental excess noise $\xi_B = 0.016$ SNU. The figure compares the secret fraction with finite size effects, using worst case estimator (solid line), and without considering finite size effects (asymptotic rate, dashed line). We can conclude that distances up to 16 km could have been achieved during this experiment, with constant $V_A = 8.22$ SNU and constant excess noise $\xi_B = 0.016$ SNU. A star shows the secret fraction for the experimental distance of 9.5 km with 2.2 dB loss.

### 4.2.4 Observed problems with receiver ①

When calibrating receiver ①, we observe several problems. First of all, we have established in subsection 3.3.4 that the variance of the shot noise $N_0$ should scale linearly with the power of the LO, $P_{LO}$. However, experimental calibration of the shot noise for several values of $P_{LO}$ with receiver ① shows that its behavior is not consistent with this theoretical property. To verify that the problem is to be attributed to receiver ①, and not to the DSP, we directly estimate $N_0$ with the sampled output of the receiver. First of all, samples of the noise are recorded with the signal input turned off and the LO input with optical power $P_{LO}$. Then, the spectral density of the recorded samples is integrated over the signal bandwidth to

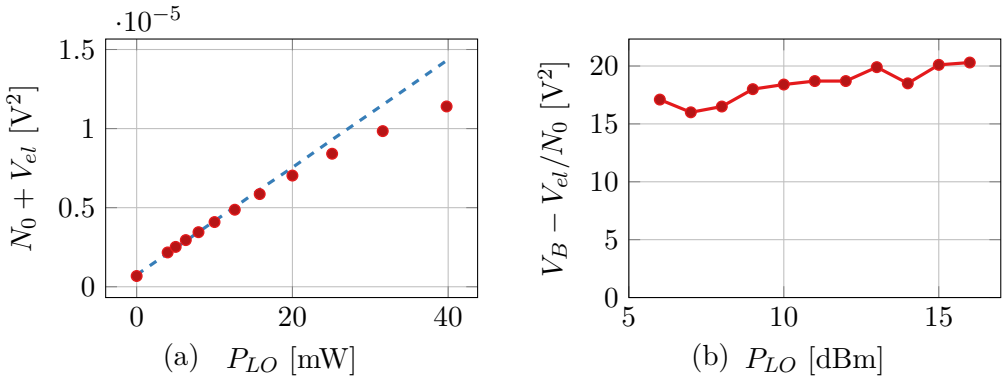



Figure 4.12: (a) Estimation of $N_0 + V_{el}$ [V$^2$] and linear regression (dashed line) vs $P_{LO}$ [mW] and (b) estimation of $V_B - V_{el}/N_0$ as a function of $P_{LO}$, for receiver ①, performed by integrating the periodogram of the signal over the signal band. We observe that it is not constant with $P_{LO}$, not conforming to theory.

obtain an estimate of $N_0 + V_{el}$ in V$^2$, where $V_{el}$ is the electronic noise in V$^2$. Let's note that with $P_{LO} = 0\,\text{mW}$, we actually obtain an estimate of $V_{el}$. Figure 4.12(a) plots the experimental estimation of $N_0 + V_{el}$, with $P_{LO}$ ranging from 0 mW to 40 mW, next to a linear regression computed on the points with $P_{LO} < 12\,\text{mW}$. We observe that the shot noise variance doesn't scale linearly with the optical power. In fact, it starts to slowly saturate for $P_{LO} \geq 12\,\text{mW}$. This effect could be attributed to nonlinear behaviors of the trans-impedance amplifiers, which are integrated in the receiver. This could compromise the validity of estimated key rates, if it causes parameter estimation to be biased.

Another similar issue was observed when calibrating $V_A$ in a back to back configuration, that is to say with Bob's receiver connected right at the output of Alice's lab. In a back to back configuration, the transmittance $T$ is constant and equal to 1. To estimate $N_0 V_B$, we record the output of the receiver with incoming signal from Alice and LO set with optical power $P_{LO}$, then integrate the periodogram over the signal bandwidth. Then we can estimate

$$\frac{\eta}{2} V_A + \xi_B = \frac{(N_0 V_B) - (N_0 + V_{el})}{(N_0 + V_{el}) - V_{el}}. \tag{4.21}$$

This value should theoretically be independent of the optical power $P_{LO}$. However, Figure 4.12 suggests that $\frac{\eta}{2} V_A + \xi_B$ is increasing with $P_{LO}$. This can be explained by an underestimation of $N_0$, which leads to a normalization error, giving a higher value than the actual one.

In conclusion, these observations raise doubts on the calibration of the shot noise of receiver ①, and therefore on the validity of QKD parameter estimation, and estimated secret key rates. As a consequence, for our experiment, we look for a receiver that does not have the same problems. In the following section, we will establish that receiver ② is a good candidate, and analyze its experimental performance.

| | PD 1 | | PD 2 | | PD 3 | | PD 4 | |
|---|---|---|---|---|---|---|---|---|
| | + | − | + | − | + | − | + | − |
| Insertion loss | 0.22 | 0.19 | 0.20 | 0.20 | 0.20 | 0.22 | 0.21 | 0.21 |
| Responsivity [A W$^{-1}$] | 0.93 | 0.98 | 1.08 | 0.98 | 0.92 | 1.00 | 1.07 | 0.86 |

Table 4.1: Characterization at $\lambda = 1550\,\text{nm}$ of the insertion loss between the signal input and each output of the Kylia 90° hybrid and responsivity of each photodiode of the Thorlabs photodetectors. The resulting average quantum efficiency of receiver ② is $\eta = 0.65$.

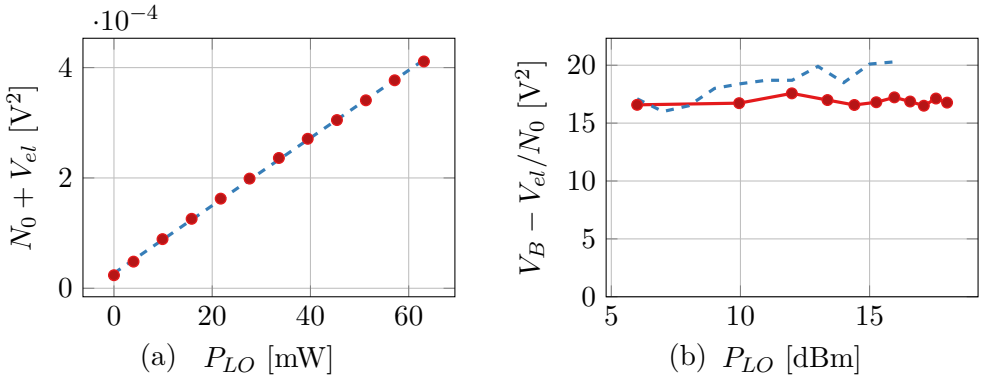



Figure 4.13: (a) Estimation of $N_0 + V_{el}$ [V$^2$] and linear regression (dashed line) vs $P_{LO}$ [mW] and (b) Estimation of $V_B - V_{el}/N_0$ as a function of $P_{LO}$, for receiver ② (solid line) and receiver ① (dashed line), performed by integrating the periodogram of the signal over the signal band. We observe that receiver ② has a behavior corresponding to theory while receiver ① does not.

## 4.3 PCS 64 and 256-QAM with Amplified Balanced Photodetectors

### 4.3.1 Characterization and validation of receiver ②

Receiver ② is built using a Kylia 90° hybrid and four amplified balanced photodetectors from Thorlabs in a polarization and phase diversity configuration, as illustrated in Figure 4.3(b).

**Quantum efficiency** To characterize the quantum efficiency $\eta$, we calibrated separately the insertion losses between the signal input and each output of the 90° hybrid and the responsivity of each photodiode in the photodetectors. The measurements are summarized in Table 4.1 for wavelength $\lambda = 1550\,\text{nm}$. The average power ratio between the input and output of the hybrid for a polarization is 0.83, and the average responsivity is $0.98\,\text{A W}^{-1}$. The resulting average quantum efficiency for $\lambda = 1550\,\text{nm}$ is $\eta = 0.65$.

**Linearity** We want to make sure that this new receiver doesn't exhibit the same problematic behavior as receiver ①. Similarly to subsection 4.2.4, we perform shot

noise calibration and signal acquisition for several values of the LO optical power $P_{LO}$. Without any DSP we can estimate the shot noise variance $N_0$ and Bob's received states variance $V_B$, by integrating the power spectral density over the relevant bandwidth. Figure 4.13 shows the resulting $V_B - V_{el}/N_0$ against $P_{LO}$. We observe that, contrary to receiver ①, $V_B - V_{el}/N_0$ is constant for the whole range of $P_{LO}$. Therefore, until proven otherwise, the parameter estimation with receiver ② can be trusted.

### 4.3.2 ECOC 2021 results, Gaussian attack hypothesis

Using the methods introduced by reference [5] and summarized in Chapter 2, we are able to compute the SKR of PCS-QAM formats with lower cardinality than PCS 1024-QAM. The theoretical study conducted in Chapter 2 shows that the SKR using PCS 256-QAM is nearing the SKR of the Gaussian modulation protocol for optimal values of the modulation variance $V_A$. It also establishes that PCS 64-QAM offers competitive SKR. To verify these claims, we performed experimental acquisitions of CV-QKD signals with PCS 64 and 256-QAM formats.

As discussed in 4.2.4, we used receiver ② to ensure reliable parameter estimation. Moreover, we increased the symbol rate to $R_S = 600\,\text{MBd}$, with pulse shape roll-off factor 0.4, to improve the spectral efficiency and the SKR. Figure 4.14 shows the measured excess noise variance $\xi_B$ at Bob's side in SNU for 200 blocks over a 2 hours long experiment, across 9.5 km SMF, for PCS 64-QAM and PCS 256-QAM. It also shows the worst-case excess noise with cross marks. The excess noise variance is now estimated for acquisition blocks of size $N = 2.8 \times 10^6$ symbols. Figure 4.14 shows the secret key rate for the corresponding excess noise values, computed with calibrated trusted noise $V_{el} = 0.1\,\text{SNU}$, finite size effects using worst-case estimator, and reconciliation efficiency assumption $\beta = 0.95$. We remind that the formula for the final SKR is given in Eq.(4.20). Here, we computed the SKR with the assumption of a Gaussian channel with a given transmittance $T$ and excess noise $\xi$. The validity of this hypothesis will be discussed in subsection 5.2.

Table 4.2 summarizes the average measured values of the modulation variance $V_A$, excess noise $\xi_B$ and SKR. We observe that, given the available commercial components and DSP used during the experiment, the PCS 64-QAM exhibits lower excess noise to the degree that its experimental SKR is slightly better than for PCS 256-QAM. This is true in spite of the fact that PCS 256-QAM has better theoretical performance at constant excess noise. Figure 4.15 shows theoretical secret fraction in secret bits per transmitted symbol, as a function of the distance, for PCS 64 and 256-QAM, compared to Gaussian modulation for the respective experimental values given in Table 4.2. We observe that distances up to 22 km could be achieved with the present state of the system, using PCS 64-QAM format and assuming constant $V_A$ and $\xi_B$. We can also see clearly that PCS 256-QAM is closer to the optimal Gaussian modulation format than PCS 64-QAM. However, its excess noise is poorer, leading to equivalent performance around 10 km, and worse performance for distances higher than 10 km. The maximal achievable distance for PCS 256-QAM, assuming constant $V_A$ and $\xi_B$, is 18 km.

| Modulation | $\nu$ | $V_A$ [SNU] | $\xi_B$ [SNU] | SKR [Mbit s$^{-1}$] |
|---|---|---|---|---|
| PCS 64-QAM | 0.0749 | 4.74 | 6.34E-3 | 67.6 |
| PCS 256-QAM | 0.0294 | 10.1 | 1.10E-2 | 66.8 |

Table 4.2: Average measured modulation variance $V_A$ in SNU, excess noise $\xi_B$ in SNU and SKR in Mbit s$^{-1}$, for PCS 64-QAM with $\nu = 0.0749$ and PCS 256-QAM with $\nu = 0.0294$, using receiver ② during 2 hours of experiment, with 9.5 km of SMF.

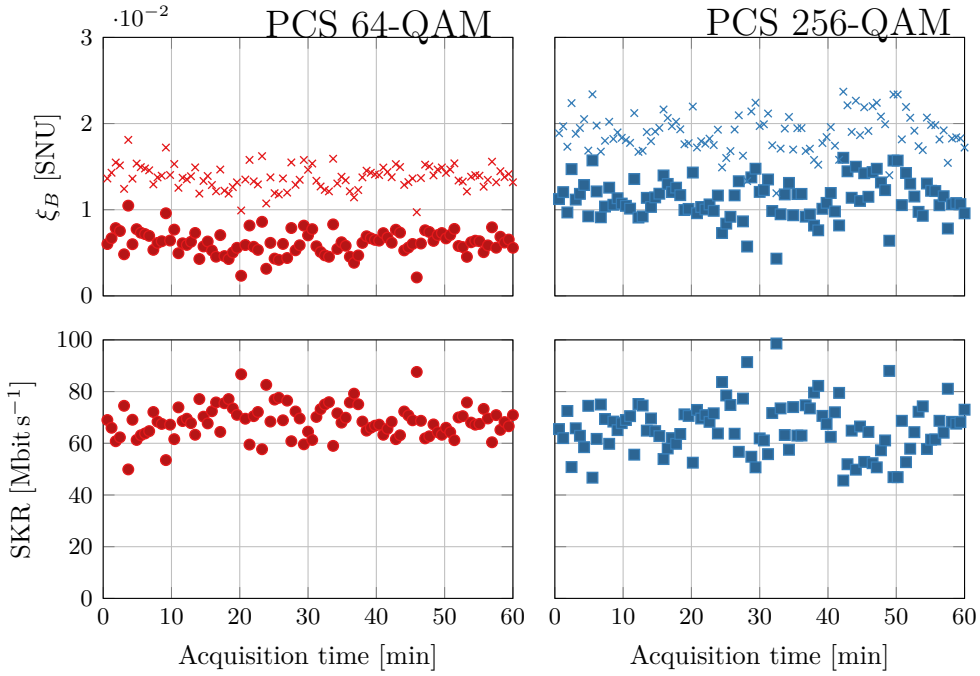



Figure 4.14: Estimated excess noise variance at Bob's site $\xi_B$, worst case estimator (cross marks) and corresponding secret key rate SKR for each block of acquired data during a 2 hours long experiment, plotted as a function of the acquisition time, for PCS 64 and 256-QAM. The experiment is conducted with coherent receiver ② and a 9.5 km SMF link (with 2.2 dB loss). The signal is 600 MBd with pulse shape roll-off factor 0.4. The estimation of $\xi_B$ is performed with $N = 2.8 \times 10^6$ symbols for each data block. The SKR is derived using the security proof for arbitrary discrete modulation, with reconciliation efficiency assumption $\beta = 0.95$, trusted receiver noise $V_{el} = 0.1$ SNU, and worst case estimator to account for finite size effects.

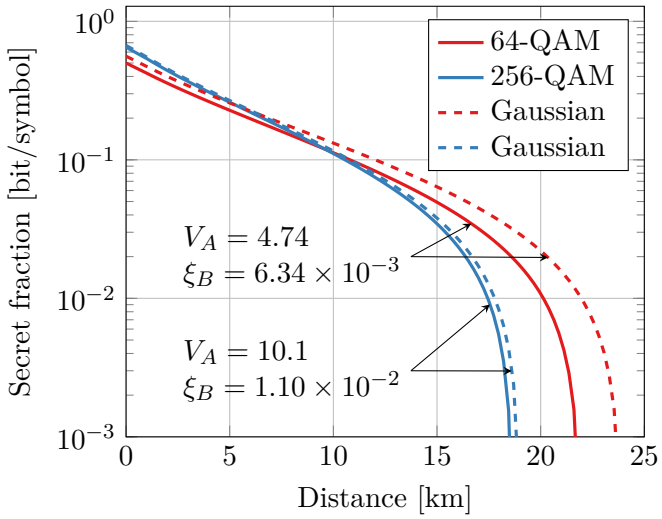



Figure 4.15: Secret fraction vs. distance (assuming SMF with 0.2 dB/km nominal loss), with reconciliation efficiency $\beta = 0.95$, worst case estimator for $N = 2.8 \times 10^6$ symbols and security parameter $\epsilon = 10^{-8}$, for PCS 64 and 256-QAM, compared to Gaussian modulation, with experimental parameters given in Table 4.2.

### 4.3.3 DSP parameters optimization

For each experiment, we want to find the DSP parameters that minimize the excess noise. Since the DSP is performed offline, we can do a brute force optimization for the most relevant parameters, on a few acquisitions. To start with, we jointly optimize two parameters of the adaptive equalizer for polarization demultiplexing: $n_{coef}$, number of coefficients, and $\mu$, the step size. For details on the adaptive equalizer, refer to Section 3.5. For each couple $(n_{coef}, \mu)$ under test, the DSP is applied to twelve different acquisitions. The other DSP parameters are fixed. Figure 4.16 shows the average excess noise for all the tested parameter couples $(n_{coef}, \mu)$, on experimental PCS 256-QAM data with similar conditions as in subsection 4.3.2. We observe that the lowest values of excess noise are achieved with 97 coefficients and step size $\mu$ $1 \times 10^{-6}$.

### 4.3.4 Improved results, Gaussian attack hypothesis

We perform the same experiment as in subsection 4.3.2, with 9.5 km of SMF and 25 km of EX3000 fiber. The 25 km fiber link has a total channel loss of 4.3 dB. Similarly to subsection 4.3.3, we optimize the most critical DSP parameters to minimize the excess noise. For this experiment, we also want to increase the number $N$ of QKD symbols per acquisition. Until now, we performed both noise calibration and signal acquisition for each use of the oscilloscope. In this way, the two steps were done consecutively without any delay. Unfortunately, this method reduces the oscilloscope memory dedicated to the signal acquisition by two. In this new experiment, we perform each step separately, and the noise calibration is performed every five signal acquisitions. The new acquisition length is 20 ms, and the number of QKD symbols

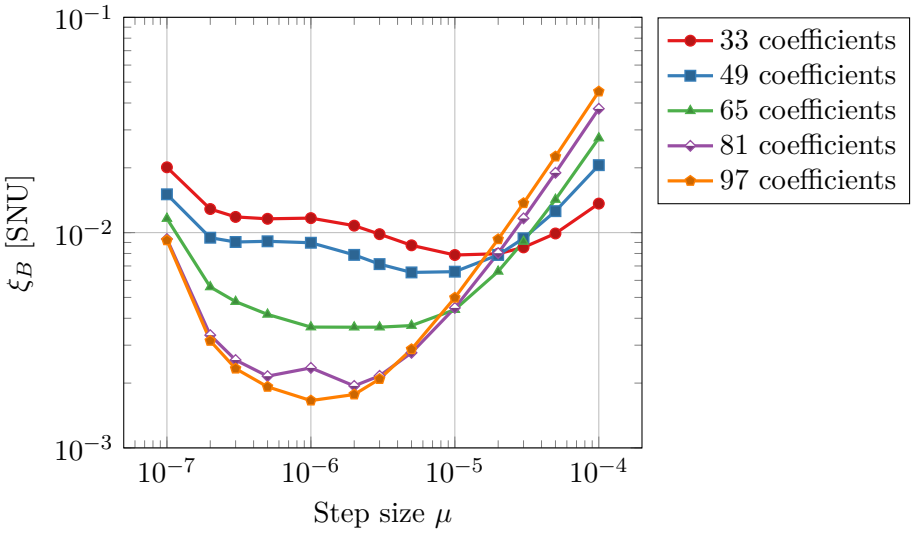



Figure 4.16: Excess noise $\xi_B$ vs step size $\mu$ and number of coefficients of adaptive equalizer described in subsection 3.5.2, averaged over 12 acquisitions of PCS 256-QAM signal with receiver ② and 25 km of EX3000 fiber.

for parameter estimation is $N = 5 \times 10^6$.

The offline DSP optimization process described in subsection 4.3.3 is performed on a subset of 12 acquisitions. In fact, Figure 4.16 was obtained with acquisition from this last experiment. Then, the DSP is performed with the optimized DSP parameters given in 4.3.3.

Figure 4.17 give the estimated and worst-case excess noise of this new experiment, for the 9.5 km SMF and the 25 km EX3000 fiber, for PCS 64 and 256-QAM, as well as the associated SKR, estimated using the security proof for arbitrary modulation protocol, with assumption $\beta = 0.95$, and worst case estimator with $N = 5 \times 10^6$ and security parameter $\epsilon = 10^{-8}$. Again, we computed the SKR with the assumption of a Gaussian channel, a hypothesis which will be discussed in subsection 5.2. Let's remark that some excess noise values are actually negative. This is due to statistical fluctuations of the estimations of $V_B$ and $N_0 + V_{el}$, and the fact that the average excess noise is very low. However, the worst-case excess noise values used to actually compute the SKR are all positive values. Table 4.3 summarizes the results with average values for the modulation variance $V_A$, excess noise $\xi_B$ (both in SNU) and SKR in Mb/s.

To conclude, we report block average achievable SKR of 127.8 Mb/s over 9.5 km and 38.7 Mb/s over 25 km, using PCS 256-QAM format, averaged over 100 transmission blocks of $N = 5 \times 10^6$ QKD symbols. PCS 64-QAM exhibits averaged achievable SKR of 115.0 Mb/s and 35.6 Mb/s over respectively 9.5 km and 25 km. Let's remark that contrary to the previous experiment, PCS 256-QAM achieves the best performance, with excess noise values equivalent to that of PCS 64-QAM. We can attribute this gain to a better optimization of the DSP parameters.

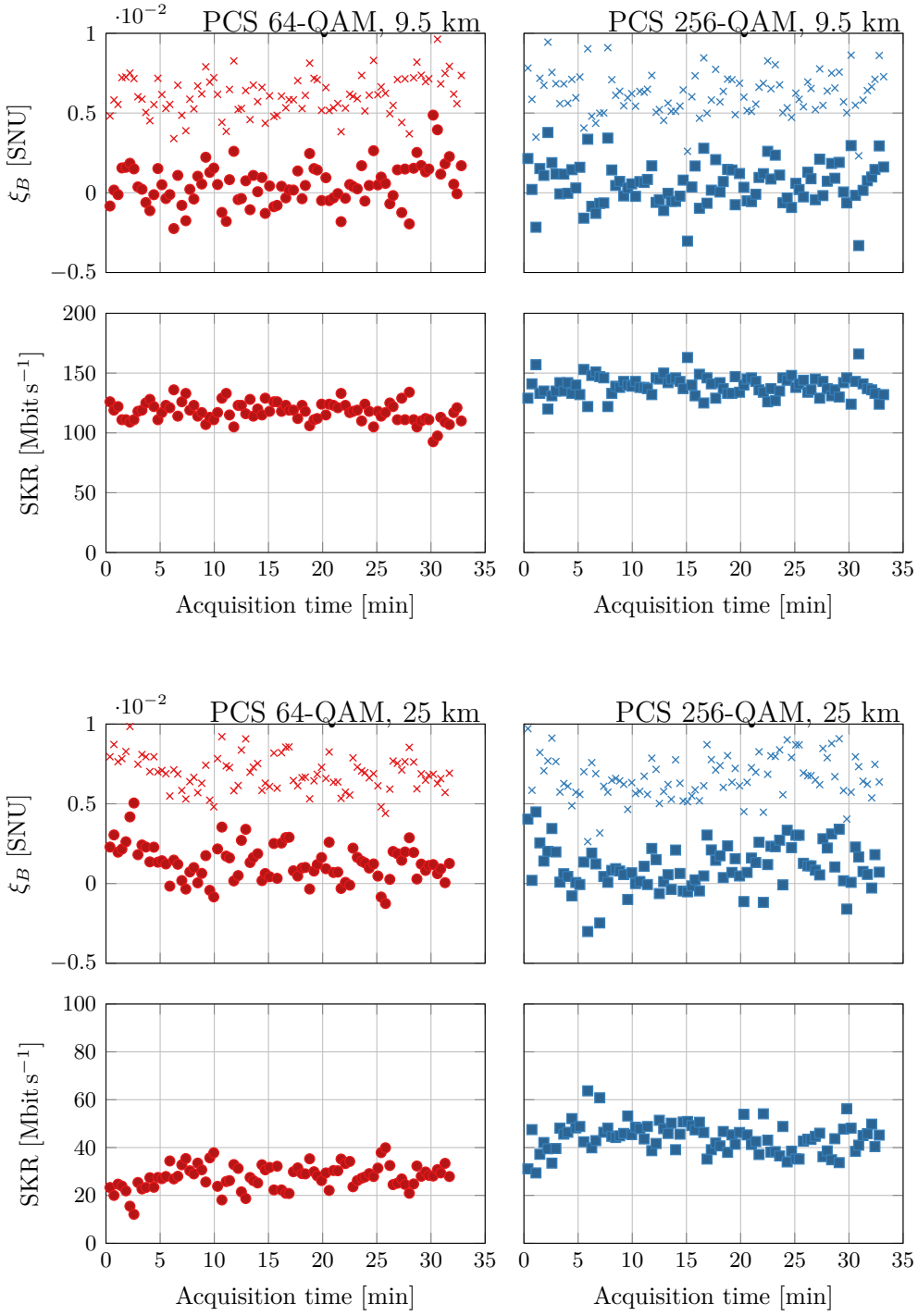



Figure 4.17: Estimated excess noise variance at Bob's site $\xi_B$, worst case estimator (cross marks) and corresponding secret key rate SKR for each block of acquired data, plotted as a function of the acquisition time, for PCS 64 and 256-QAM, for the experiment described in subsection 4.3.5 with 9.5 km of SMF or 25 km EX3000 fiber link.

| Modulation | Distance [km] | $\nu$ | $V_A$ [SNU] | $\xi_B$ [SNU] | SKR [Mbit s$^{-1}$] |
|---|---|---|---|---|---|
| PCS 64-QAM | 9.5 | 0.0688 | 5.32 | 1.97E-4 | 117.7 |
| PCS 64-QAM | 25 | 0.0460 | 4.20 | 1.17E-3 | 35.6 |
| PCS 256-QAM | 9.5 | 0.0362 | 7.11 | 1.32E-4 | 138.8 |
| PCS 256-QAM | 25 | 0.0380 | 6.53 | 9.00E-4 | 44.0 |

Table 4.3: Average measured modulation variance $V_A$ in SNU, excess noise $\xi_B$ in SNU and SKR in Mbit s$^{-1}$, for PCS 64-QAM and PCS 256-QAM, using receiver ② during 1 hour of experiment, with 9.5 km of SMF and 25 km of EX3000 fiber.

### 4.3.5 Improved results, general attack

In the previous subsection, the key rates were calculated under the assumption of a Gaussian channel. In this paradigm, we estimate the transmittance $T$ and the excess noise variance $\xi_B$ and the SKR is given by a function $g(T, \xi)$. Unfortunately, Gaussian attacks are not the most efficient attacks for Eve when Alice uses discrete modulation. That is why a better approach would be to directly estimate the parameters $c_1$, $c_2$ and $n_B$, and compute the SKR with another function $f(c_1, c_2, n_B)$. These functions are described in Section 2.4.

Under experimental conditions, we found the effective channel to be very well described by a Gaussian model. In particular, the direct estimation of $c_1$, $c_2$ and $n_B$ gives very close values to the formulas for a Gaussian channel with the estimates of $T$ and $\xi_B$. Therefore, we observe $f(\hat{c}_1, \hat{c}_2, \hat{n}_B) \simeq g(\hat{T}, \hat{\xi}_B)$. However, the direct evaluation of these formulas with the estimates doesn't take into account finite size effects. To avoid too optimistic values of the SKR, we evaluate the formulas with worst case estimators. For example, in the previous subsection, we evaluated $g(\hat{T}^{\min}, \hat{\xi}_B^{\max})$. Without the assumption of Gaussian attacks, we rather compute $f(\hat{c}_1^{\min}, \hat{c}_2^{\min}, \hat{n}_B^{\max})$. The worst-case estimators $\hat{c}_1^{\min}$, $\hat{c}_2^{\min}$, and $\hat{n}_B^{\max}$ are evaluated using the method described in subsection 2.7.3, which consists in approximating by normal distributions. The calculation of the expected values and variances of the estimators are detailed in Appendix B. Let's note that we use the second estimator presented for $\hat{c}_1$ in this Appendix, and that we obtain approximation of its variance using Monte-Carlo simulations.

Figure 4.18 gives the SKR evaluated in this way for PCS 64-QAM with 9.5 km SMF and PCS 256-QAM with 9.5km SMF and 25 km EX3000 fiber, with $N = 5\times10^6$ QKD symbols, security parameter $\epsilon = 10^{-10}$, and reconciliation efficiency $\beta = 0.95$. We see that the key rates are more pessimistic than those presented before. In particular, we do not have positive SKR for PCS 64-QAM with 25 km of EX3000 fiber. The explanation lies in the worst-case estimators $\hat{c}_1^{\min}$, $\hat{c}_2^{\min}$ and $\hat{n}_B^{\max}$ which are less favorable than when evaluated for $\hat{T}^{\min}$ and $\hat{\xi}_B^{\max}$ and a Gaussian channel. Specifically, we have that

$$n_B(\hat{T}^{\min}, \hat{\xi}_B^{\max}) = \hat{T}^{\min}\frac{V_A}{2} + \hat{\xi}_B^{\max} \tag{4.22}$$

is much more favorable than $\hat{n}_B^{\max}$ because the term $\hat{T}^{\min}\frac{V_A}{2}$ tends to give lower values. Although pessimistic, we will retain these last results, summarized in Table

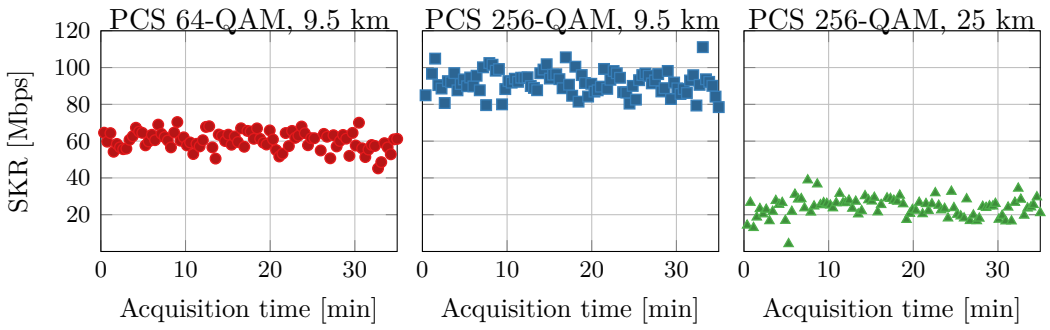



Figure 4.18: Secret key rate for general attacks, computed with worst case estimators for $c_1$, $c_2$ and $n_B$, for each block of acquired data, plotted as a function of the acquisition time, for PCS 64 and 256-QAM, for the experiment described in subsection 4.3.5 with 9.5 km SMF and 25 km EX3000 fiber link.

| Modulation | Distance [km] | $\nu$ | $V_A$ [SNU] | $\xi_B$ [SNU] | SKR [Mbit s$^{-1}$] |
|---|---|---|---|---|---|
| PCS 64-QAM | 9.5 | 0.0688 | 5.3 | 2.0E-4 | 60.2 |
| PCS 64-QAM | 25 | 0.0460 | 4.2 | 1.2E-3 | 0.0 |
| PCS 256-QAM | 9.5 | 0.0362 | 7.1 | 1.3E-4 | 91.9 |
| PCS 256-QAM | 25 | 0.0380 | 6.5 | 9.0E-4 | 24.0 |

Table 4.4: Average measured modulation variance $V_A$ in SNU, excess noise $\xi_B$ in SNU and SKR in Mbit s$^{-1}$, for PCS 64-QAM and PCS 256-QAM, using receiver ② during 1 hour of experiment, with 9.5 km of SMF and 25 km of EX3000 fiber.

4.4. Indeed, they correspond to a more rigorous implementation of the protocol with the proof of security for a discrete modulation.

Figure 4.19 compares these final results, given by red stars, to state of the art experimental results published in the last years. The results taking into account finite-size effects are given by blue circles, while asymptotic results are given by light blue circles. A theoretical curve shows the performance of a Gaussian modulation format with excess noise $\xi_B = 0.0005$, and optimal modulation variance $V_A$, for a channel with 0.172 dB loss per km, corresponding to the EX3000 fiber we used in our experiment.

### 4.3.6 Statistical study

To justify the use of the worst-case estimator for the excess noise, we must ensure that the fluctuations observed on the excess noise are indeed of a statistical nature. To do so, we compare the population variance on the experimental estimators $\hat{\xi}_B$ of all acquisitions to the theoretical variance of the excess noise variance estimator. This variance should scale with $1/N$ where $N$ is the number of symbols used to calculate the estimator. Figure 4.20 shows this comparison for each experiment of subsection 4.3.5. We observe that the experimental population variance does not fit perfectly the theoretical estimator variance. This could be caused by the size of the population of estimators being too small. It could also be caused by

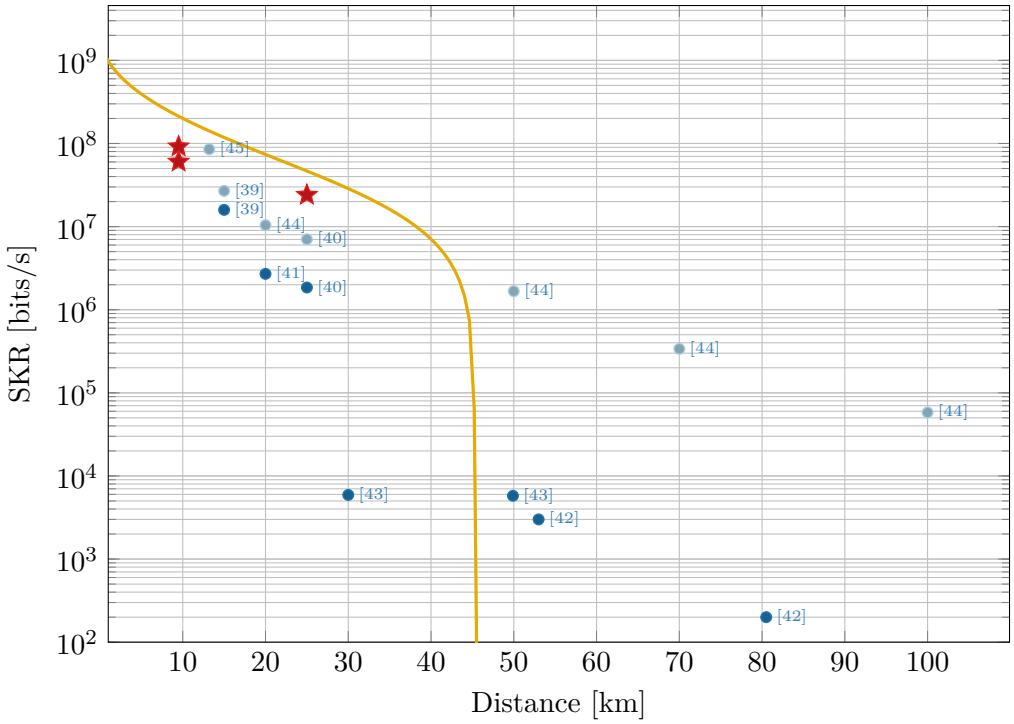



Figure 4.19: Comparison of the final experimental result of this thesis, given by red stars, to state of the art publications. Blue circles denotes finite-size results, while light blue results denotes asymptotic results. The yellow curve is a theoretical curve for a Gaussian modulation with excess noise $\xi_B = 0.0005$, optimal modulation variance $V_A$, for a channel with 0.172 dB loss per km.

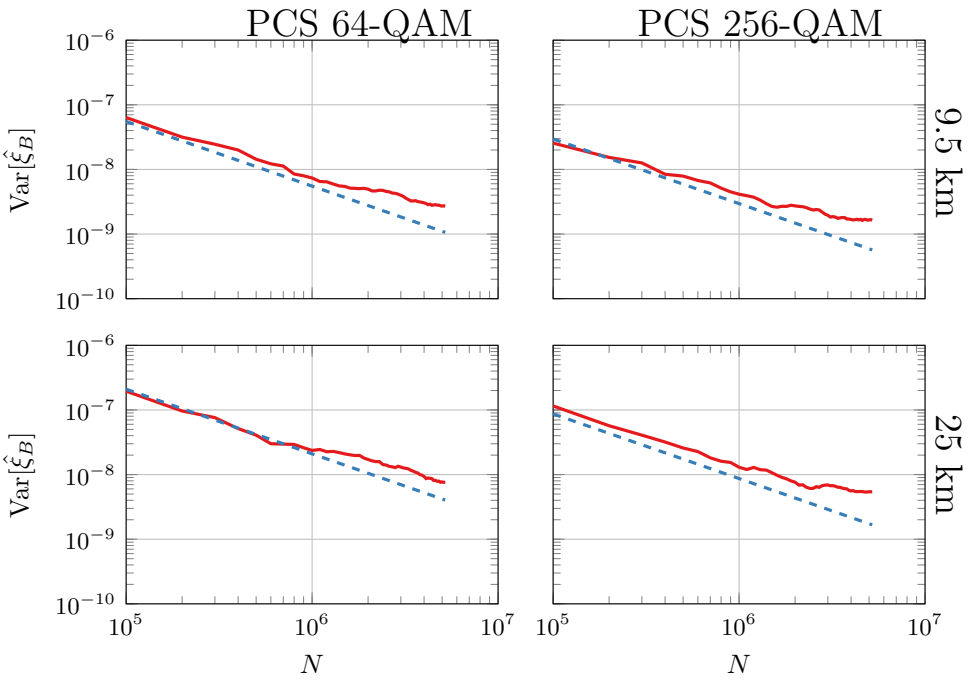



Figure 4.20: Experimental population variance of excess noise estimator $\hat{\xi}_B$ over 90 acquisitions (solid line) vs number of symbols $N$ used in the calculation of $\hat{\xi}_B$, compared to the theoretical value for the variance of the estimator (dashed line). The comparison is done for each experiment of subsection 4.3.5.

the experimental estimators being non identically distributed, for example if the excess noise is slowly varying during the whole experiment. Overall, the population variance can be considered sufficiently close to the theoretical variance to assume that fluctuations on the excess noise measured are essentially of statistical nature. Therefore, the use of the worst-case estimator for the excess noise is an acceptable way to take into account finite size effects on the security of the protocol.

## 4.4 Feasibility of wavelength division multiplexing of QKD channels

Our last experiment is a feasibility study of wavelength division multiplexing (WDM) of QKD channels. The idea is that Alice and Bob perform several QKD protocols simultaneously. The coherent states of each protocol are sent through different WDM channels.

The experimental system of Alice, outlined in Figure 4.21, is very similar to the one described in Section 4.1.1. The main difference is that the optical input of the modulator is now a frequency comb made with four external cavity laser sources with 30 kHz nominal linewidth. Their frequencies are respectively tuned to 193 396 GHz, 193 400 GHz, 193 404 GHz, and 193 408 GHz. The output is a super channel with 4 WDM carriers. To measure each channel, Bob can use four receivers with four

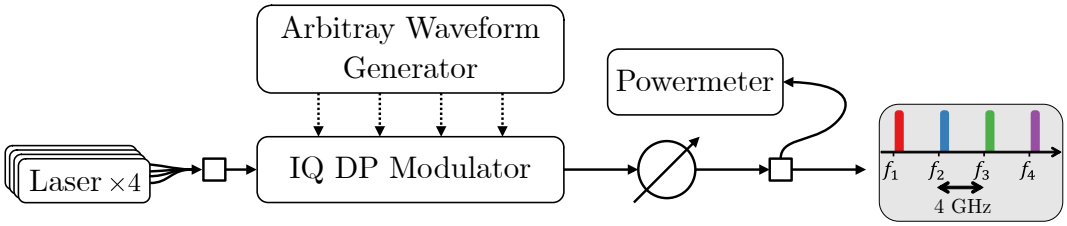



Figure 4.21: Experimental system of Alice for WDM-like CV-QKD. It features four 30 kHz linewidth lasers sources tuned at 193 396 GHz, 193 400 GHz, 193 404 GHz, and 193 408 GHz, a conventional IQ dual polarization (DP) optical modulator, and a 5GS/s 16 bits arbitrary waveform generator (AWG).

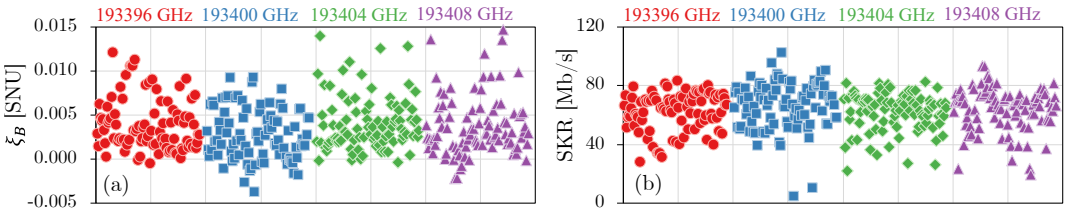



Figure 4.22: (a) Estimated excess noise $\xi_B$ for each acquisition of each subcarrier and (b) corresponding SKR with reconciliation efficiency assumption $\beta = 0.95$ and worst-case estimator of the excess noise.

different LO tuned to frequencies 193 396 GHz, 193 400 GHz, 193 404 GHz, and 193 408 GHz. In practice during our experiment, we use only one receiver and measure the channel consecutively and not simultaneously. Our goal is only to estimate the parameters and give an achievable SKR for each channel. The experiment was done with receiver ②, with a 13.5 km link of SMF.

For each of the four WDM channels, we perform 100 acquisitions of 20 ms over 1 hour, with PCS 256-QAM format. For each acquisition, we apply the DSP and estimate the QKD parameters, including modulation variance $V_A$ and excess noise $\xi_B$. Figure 4.22(a) gives the estimated excess noise for each acquisition. The estimation is done with $N = 5 \times 10^6$ QKD symbols. Figure 4.22(b) gives the corresponding SKR for each acquisition, computed using the proof for arbitrary modulation protocol, with trusted electronic noise and worst-case estimator for the excess noise with security parameter $\epsilon = 10^{-8}$ and $N = 5 \times 10^6$ symbols. We assumed reconciliation efficiency $\beta = 0.95$. The averaged estimated values for each channel are summarized in Table 4.5. The average excess noise over the different WDM channels is $\xi_B = 3.7 \times 10^{-3}$ SNU . The sum of the achievable SKR of the 4 WDM channels is 254.6 Mb/s, with average 63.7 Mb/s SKR on each WDM channel.

We remind that the baseband signal at the output of the AWG has been upshifted by 500 MHz, to avoid low frequency noise sources. Therefore, only positive frequencies are modulated on the optical carriers, as illustrated in the insert of Figure 4.21. Similarly, it is possible to create an only negative frequencies signal, that can be digitally multiplexed. This digital dual-carrier method should help us increase the SKR by a factor up to two.

We also note that the experiment uses only one modulator. Therefore, the four

| | 193 396 GHz | 193 400 GHz | 193 404 GHz | 193 408 GHz |
|---|---|---|---|---|
| $V_A$ [SNU] | 7.61 | 7.11 | 7.07 | 7.44 |
| $\xi_B$ [SNU] | 3.93E-3 | 3.12E-3 | 4.01E-3 | 3.74E-3 |
| SKR [Mb/s] | 62.5 | 66.5 | 62.1 | 63.5 |

Table 4.5: Experimental values of modulation variance $V_A$ in SNU, average excess noise $\xi_B$ in SNU, and average secret key rate in Mb/s, for each WDM subcarrier.

WDM channel carry the same signal. This could potentially offer more favorable conditions than real WDM and challenge the conclusions of the experiment. However, our system works at low launch power (lower than -40 dBm) and short distance. In these conditions, nonlinear impairments can be considered as negligible. This fact corroborates the conclusion of our experiment: the implementation of WDM techniques with PCS 256-QAM CV-QKD protocol is possible with high performance. However, new experiments with real WDM channels should be conducted to confirm the results.

# Chapter 5

# Discussion on the experiment and possible improvements

## 5.1 About the experimental processing time

The experimental system currently suffers from some inefficiencies that slow down its operational functioning. To begin with, the acquisition of the signal is performed by an oscilloscope which stores the sampled waveform in its local memory. The processing and writing time is particularly long, taking about 20 seconds for 20 ms of actual data. Therefore, the actual key rate with the current system should be divided by 1000. In addition, the digital signal processing is carried out in a delayed manner using the Matlab calculation software. The time required to process blocks of 20 ms of data, with a sampling rate of 8 sps, is about 30 minutes on the machine currently used. This penalizes even more the potential effective key rate, knowing that on top of that the reconciliation time is not taken into account. In fact, this test system has been designed to validate the feasibility of PCS-QAM modulations, without taking into account the constraints that a commercial system would have. Let us therefore mention the main constraints of such a system, and verify their practicality.

The signal is 600 MBaud with 8 sample per symbol rate. The sample rate is therefore 4.8 Gsample per second. The digital signal processing used is very similar to that of conventional coherent optical transceivers. The latest generation of such transceivers is capable of real-time processing of several tens of GBaud signals. This is for example the case of Nokia's PSE-V technology, which has been tested in the field [95]. Therefore, we have good reason to believe that it is possible to implement our system in real time.

Let us also mention that the symbols used for parameter estimation should be discarded, and not counted in the key rate. And yet, in our experimental tests, we used 100% of the symbols in each block to perform this step. This is due to the limitations imposed by the oscilloscope and the low speed of the signal processing. One should consider our experimental acquisitions as monitoring steps for a QKD system. For example, if we monitor during 20 ms every second, 2% of the symbols are used for the estimation. In that case, we would have to multiply our rates by 98% to obtain the actual SKR of the system. In practice, a commercial system would

have to make a compromise between the number of symbols revealed for estimation, and the frequency at which the estimation is done to follow the evolution of the parameters with enough precision.

To conclude this paragraph, let us state that our experiment allowed us to evaluate the capacity of the hardware and DSP to transmit secret keys, using PCS-QAM modulation. However, to allow the effective distribution of these keys, it would be necessary to upgrade the system to operate in real time, including DSP and post-processing (reconciliation and privacy amplification), while optimizing the duration of parameter estimation.

## 5.2 About the assumption of Gaussian channel

In Section 4.3 except subsection 4.3.5, the key rates were calculated assuming that the channel was Gaussian. That is, instead of directly estimating the quantities $c_1$, $c_2$ and $n_B$ as defined in Section 2.4, we estimated the transmittance $T$ and the excess noise $\xi_B$. Then, we used the formulas given in subsection 2.4.4 which we recall below,

$$c_1 = \sqrt{T}\,\mathrm{Tr}(\bar{\tau}^{\frac{1}{2}}\hat{a}\bar{\tau}^{\frac{1}{2}}\hat{a}^\dagger), \tag{5.1}$$

$$c_2 = \sqrt{T}\frac{V_A}{2}, \tag{5.2}$$

$$n_B = T\frac{V_A}{2} + T\frac{\xi}{2}, \tag{5.3}$$

where $\tau$ is the density matrix corresponding to the statistical mixture of Alice's coherent states, and $\hat{a}^\dagger$ and $\hat{a}$ the creation and annihilation operators on Alice's mode respectively.

Therefore, the actual estimated quantities of the channel were the transmittance $T$ and the excess noise variance $\xi_B$. This very conventional approach has a certain flaw in our case, already mentioned in subsection 4.3.5. The issue is that Gaussian attacks are not optimal in the case of non-Gaussian modulation formats. This is why Denys et al. developed the calculation summarized in Chapter 2 [5], whose practical realization involves the estimation of the parameters $c_1$, $c_2$ and $n_B$, as explained in subsection 2.4.3.

By directly measuring the quantities $c_1$, $c_2$ and $n_B$ from the experimental data, we observe that they are well approximated by the above formulas, evaluated with the experimental estimations of $T$ and $\xi_B$. To illustrate this, Table 5.1 compares $c_1$, $c_2$, $n_B$ with direct estimation and Gaussian channel formulas, for 6 different experimental PCS 256-QAM data blocks. We also give the asymptotic SKR computed with each method. We observe that both methods give very similar results.

As already observed with the results of subsection 4.3.5, the difference arises when considering worst case estimators. We then obtain SKR values around 20 Mbps, when the worst-case estimators for $T$ and $\xi_B$ give SKR around 40 Mbps. We deduce that the estimators of $c_1$, $c_2$ and $n_B$ are less statistically stable than the estimators of $T$ and $\xi_B$, and make the SKR more sensitive to statistical fluctuations.

To conclude, we can say that the assumption of a Gaussian channel only partially invalidates the results presented under this assumption, at least in terms of asymp-

| | $c_1$ | | $c_2$ | | $n_B$ | | SKR [Mb/s] | |
|---|---|---|---|---|---|---|---|---|
| | Estimated | Gaussian | Estimated | Gaussian | Estimated | Gaussian | Estimated | Gaussian |
| 1 | 2.366134 | 2.366122 | 2.080334 | 2.080333 | 1.278215 | 1.278043 | 57.18 | 57.53 |
| 2 | 2.354593 | 2.354580 | 2.070185 | 2.070186 | 1.259258 | 1.259101 | 78.14 | 78.65 |
| 3 | 2.370297 | 2.370278 | 2.083988 | 2.083988 | 1.283041 | 1.282878 | 55.61 | 55.95 |
| 4 | 2.332108 | 2.332097 | 2.050420 | 2.050418 | 1.237734 | 1.237570 | 63.92 | 64.30 |
| 5 | 2.365543 | 2.365526 | 2.079809 | 2.079809 | 1.274735 | 1.274555 | 71.80 | 72.26 |
| 6 | 2.351207 | 2.351199 | 2.067213 | 2.067213 | 1.258396 | 1.258231 | 66.48 | 66.88 |

Table 5.1: Comparison of experimental estimations of quantities $c_1$, $c_2$, $n_B$ with their values for a Gaussian channel evaluated with experimental values of $V_A$, $T$ and $\xi$, and corresponding evaluation of the secret key rate in Mb/s. The results are given for 6 data blocks from the experiment described in subsection 4.3.5, with 25 km and PCS 256-QAM.

totic security. However, in the absence of better finite size analysis, it is preferable to retain only the SKR of subsection 4.3.5, calculated without this assumption. We also note two possible directions for improvement. The first one consists in increasing the number of symbols used for the estimation of the parameters. The second is to find better estimators for $c_1$, $c_2$ and $n_B$ or to propose a proof using other quantities that are easier to estimate from a statistical point of view.

## 5.3 Parameter estimation: divergence between theory and experiment

To establish the security of the protocol, we must assume that the quantum channel is under the control of Eve. In particular, for a Gaussian channel, we assume that Eve controls the transmittance $T$ and the excess noise $\xi$. It is therefore crucial to estimate correctly these two quantities, and to follow their possible variations in time. The modulation variance $V_A$ is also an important parameter for calculating the key rate. Its knowledge is in particular required to estimate $T$ and $\xi$, as detailed in subsection 2.7.1.

In practice, there is no eavesdropper in the lab. The transmittance $T$ is only due to dispersion in the optical fiber, as discussed in subsection 3.4.1. Therefore, it is constant over time and very easy to measure using a laser source and an optical power-meter. However, the estimation of $V_A$ is somewhat challenging. In theory, its value should be directly related to the optical power $P_{sig}$ coming out of Alice's lab, measured with a power meter. For a dual polarization signal, we should have,

$$\begin{aligned} V_A = 2\langle n \rangle &= 2 \times \frac{1}{2} \times R_{pil} \times \frac{1}{E_\lambda} \times P_{LO} \\ &= R_{pil} \frac{\lambda}{hc} P_{LO} \end{aligned} \tag{5.4}$$

where $R_{pil}$ is the QKD symbols over pilots power ratio and $E_\lambda = hc/\lambda$ is the energy of a photon with wavelength $\lambda$. In practice, we observe that estimating $T$ from the formulas in subsection 3.4.1 evaluated with $V_A$ measured this way yields values inconsistent with the measured attenuation of the fiber.

To circumvent this problem in the experiment, we start by using a fixed value for $T$, corresponding to the measured value. Thus, instead of estimating $T$, Bob estimates the value of $V_A$ as follows. Alice reveals a fraction of the transmitted symbols ($\tilde{x}_k$), with an arbitrary modulation variance. Then Bob wants to know the normalization factor $\hat{\rho}$, such that his received symbols are $y_k = \hat{\rho}\tilde{x}_k + w_k$ where $w_k$ is an additive white Gaussian noise. The normalization factor is given by

$$\hat{\rho} = \frac{\sum_{k=1}^{N} \tilde{x}_k y_k}{\sum_{k=1}^{N} \tilde{x}_k^2}. \tag{5.5}$$

Then, the modulation variance $V_A$ is estimated as

$$V_A = \frac{1}{\hat{N}_0} \frac{2}{\eta T} \hat{\rho}^2 \operatorname{Var}(x_k), \tag{5.6}$$

where $\hat{N}_0$ is the estimation of the shot noise unit.

The theory requires a fixed value for $V_A$,. That's why we estimate its value for all acquisitions, then fix its value to the average $V_A$. Then Bob can obtain the symbols ($x_k$) with modulation variance $V_A$ and proceed to he estimation of $T$ and $\xi$ as described in subsection 2.7.1.

## 5.4 About single side band signals

As explained in subsection 4.1.3, the QKD signal is single side band. This means that the complex digital signal has only positive frequency components. On the optical modulated signal, this is manifested by the spectrum of the signal entirely to the right of the carrier. However, imperfections in the optical modulator cause part of the signal to leak into the symmetrical band, to the left of the carrier. This introduces a side channel that Eve can take advantage of, without Alice and Bob noticing. The impact of this side channel on the key rate has been studied in reference [92], but was neglected in our work. To consolidate the results obtained, it would therefore be necessary to repeat the calculations of this reference.

Another possibility is to introduce a second digital signal, whose spectrum is shifted in the negative frequencies, on the symmetrical band of the first signal. We thus obtain a digital dual carrier signal. From a theoretical point of view, we can consider the two signals as two orthogonal QKD channels multiplexed in frequency, i.e. as two QKD protocols taking place simultaneously on the physical channel. This method makes it possible to double the key rate without increasing the bandwidth of the equipment. Moreover, the negative band is now monitored by Alice and Bob and is no longer to be considered as a side channel.

The consequences of the modulation imperfections are then a crosstalk between the channels. This crosstalk, if not corrected, introduces additional noise which is attributed to Eve. Therefore, it may be necessary to add a new step to the DSP. This could be done by a new adaptive filter similar to the one described in subsection 3.5.2, but taking as inputs and outputs the 8 real quadratures (two for each polarization of each channel).

# Conclusion

In conclusion of this thesis, we highlight the main contributions of our three years of research work, as well as the conclusions that can be drawn.

First, we have developed an experimental high-rate CV-QKD system. It was built from commercially available equipment, which is commonly used in optical digital transmissions. To make it functional, conventional digital signal processing algorithms were used and adapted to the specificities of our application, in particular by using temporal pilots. Moreover, we have developed a method for precise calibration of the shot noise allowing accurate parameter estimation. In addition, it should be noted that the system allows for polarization and wavelength division multiplexing.

The main originality of our approach compared to the state of the art is to use discrete modulations known as PCS QAM. These are actually discretized Gaussian modulations, coming from classical digital communications. The security proof of Denys et al. validates the theoretical possibility to use such modulations [5]. Our experimental work is the first to our knowledge to implement the details in this proof. In addition, to allow its practical use, we have adapted the secret key rate calculations to the trusted receiver model, and we have taken into account statistical finite size effects by computing the relevant worst case estimators.

We have demonstrated the experimental feasibility of key rates of several tens of Mbps, using PCS 64-QAM and PCS 256-QAM modulations, across a few tens of km of optical fiber. Specifically, for PCS 64-QAM, we estimated the possibility of obtaining 60 Mbps with 9.5 km of single-mode fiber. For PCS 256-QAM, we estimated 92 Mbps and 24 Mbps with respectively 9.5 km of single mode fiber and 25 km of EX3000 fiber (whose attenuation is 0.17 dB/km). In addition, we note that the security proof of Denys et al. requires the estimation of three quantities that are different from the usual quantities of other security proofs. We have observed that the estimators of these quantities make the secret key rate more sensitive to finite size statistical effects.

We believe that our approach offers many advantages for the practical implementation of CV-QKD technologies. In particular, we expect the use of discrete modulations to offer an effective answer to the practical impossibility of true Gaussian modulation. In addition, the use of equipment and techniques derived from optical digital transmissions allows us to expect the rapid resolution of technological obstacles to the commercialization of CV-QKD technologies.

The accomplished work opens the way to possible improvements and new experiments. In particular, one challenge is to make the receiver operate in real time and

to implement the classical post-processing steps, thus allowing the effective generation of keys. It is also possible to go further in the study of frequency multiplexing, in particular the coexistence with classical telecommunication channels. Finally, let's mention the possibility of DSP improvements, for example to allow digital dual carrier signals.

# Appendix A

# Quantum information fundamentals

## A.1 Postulates of quantum mechanics

### A.1.1 Quantum states

The term quantum system refers to any physical system that can be described by the laws of quantum mechanics. The *state* of a quantum system determines the probability distribution of any measurement of the system. The first mathematical postulate of quantum mechanic describes the mathematical structure of quantum states.

**Postulate 1** *The state of an isolated quantum system is represented, at a fixed time $t$, by a unit vector $|\psi\rangle$ belonging to a complex separable Hilbert space $\mathcal{H}$, called the state space.*

Let's remind that a Hilbert space is an inner vector space which is also complete with respect to the metric induced by the inner product. Moreover, a topological space is said separable if it contains a countable and dense subset. A separable Hilbert space has the remarkable property of having a countable orthonormal basis, which will come in handy.

**Bra-ket notation** The bra-ket notation, or Dirac notation, is a convention used to denote quantum states. A *ket* is of the form $|\psi\rangle$ and represents the state of a quantum system, i.e. a unit vector in a Hilbert space $\mathcal{H}$. A *bra* is of the form $\langle\varphi|$. It denotes a linear map from $\mathcal{H}$ to $\mathbb{C}$, defined by

$$\langle\varphi| : |\psi\rangle \mapsto \langle\varphi|\psi\rangle \tag{A.1}$$

where $\langle\varphi|\psi\rangle$ is the inner product between vectors $|\varphi\rangle$ and $|\psi\rangle$. Let's remind that the inner product of a complex Hilbert space is anti-linear with the first variable, and linear with the second variable.

**Remark** In fact, a quantum state should be identified to an equivalence class of the relation $\sim$ on non-zero vectors of $\mathcal{H}$ defined by

$$|\psi\rangle \sim |\phi\rangle \iff \exists \lambda \in \mathbb{C} \setminus \{0\},\ |\psi\rangle = \lambda |\varphi\rangle. \tag{A.2}$$

Such equivalence classes are called *rays* and the set of all rays is called a projective Hilbert space. The vector $|\psi\rangle$ in the first postulate is actually a representative vector chosen with unit norm. As a consequence of this formalism, the unitary vectors $|\psi\rangle$ and $e^{j\theta}|\psi\rangle$ represent the same quantum state. We note that the representative vector of a ray is not unique.

### A.1.2 Observable and measurement

An observable is a physical quantity that can be measured, such as the position and momentum of a particle. This second postulate sheds light on the mathematics behind physical measurements on a quantum system.

**Postulate 2** *Any observable is described by a Hermitian operator $\hat{A}$ on the state space $\mathcal{H}$. When measuring an observable $\hat{A}$ on a state $|\psi\rangle \in \mathcal{H}$, the possible outputs are the eigenvalues of $\hat{A}$, which are real values. The probability of obtaining eigenvalue $a \in \mathbb{R}$ is $p_a = \langle\psi|\pi_a|\psi\rangle$ where $\pi_a$ is the projection operator on the eigenspace associated with $a$. The state of the system after this measurement is $\frac{\pi_a|\psi\rangle}{\sqrt{p_a}}$.*

Let's remind that an operator $\hat{A}$ is called Hermitian if it's equal to its Hermitian adjoint $\hat{A}^*$. In that case, the eigenvalues of $\hat{A}$ are real values. Moreover, there exists an orthonormal basis of eigenvectors of $\hat{A}$. Conversely, any orthonormal basis can be associated with an observable of which it is a basis of eigenvectors.

**First example** Let $\mathcal{H}$ be a complex Hilbert space of dimension 2, and $(|0\rangle, |1\rangle)$ an orthonormal basis of $\mathcal{H}$. A physical system described by $\mathcal{H}$ is called a *qubit*. Its quantum states are of the form $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ where $\alpha$ and $\beta$ are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$. The vector representation of ket $|\psi\rangle$ in the basis $(|0\rangle, |1\rangle)$ is

$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}. \tag{A.3}$$

Let's consider the operator $\sigma_z$, whose representation in the basis $(|0\rangle, |1\rangle)$ is

$$\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{A.4}$$

It is a Hermitian operator on $\mathcal{H}$, thus an observable of the qubit. Its eigenvalues are 1 and $-1$, of respective eigenvectors $|0\rangle$ and $|1\rangle$. A measurement of the observable $\sigma_z$ on state $|\psi\rangle$ outputs 1 with probability $|\alpha|^2$ and $-1$ with probability $|\beta|^2$. If $\alpha \neq 0$ or $\beta \neq 0$, $|\psi\rangle$ is called a superposition state.

### A.1.3 Composite system and entanglement

Let's introduce the fundamental concept of entanglement. It derives from the mathematical description of composite systems, i.e. physical systems composed of several isolated quantum systems, given by the following postulate.

**Postulate 3** *The state of a composite quantum system is described by a unit vector* $|\psi\rangle$ *in the tensor product* $\bigotimes_{i=1}^{n} \mathcal{H}_i$ *of the state spaces of the quantum subsystems,* $\mathcal{H}_i$*,* $i \in \{1, \ldots, n\}$*. Moreover, if each subsystem is in a state* $|\psi_i\rangle \in \mathcal{H}_i$*,* $i \in \{1, \ldots, n\}$*, then the composite system is in the state* $\bigotimes_{i=1}^{n} |\psi_i\rangle$*.*

The states $|\psi\rangle \in \bigotimes_{i=1}^{n} \mathcal{H}_i$ that can be decomposed as $|\psi\rangle = \bigotimes_{i=1}^{n} |\psi_i\rangle$ where $|\psi_i\rangle \in \mathcal{H}_i$, $i \in \{1, \ldots, n\}$ are called *separable* states. Entanglement comes from the fact that not all vectors in a tensor product are separable. Non-separable states are called *entangled* states. When a composite system is in an entangled state, the state of a subsystem cannot be described by a unit vector in the corresponding state space.

**Density operator** A subsystem of an entangled state is in fact a statistical mixture of states $|\psi_i\rangle \in \mathcal{H}$. This concept is described by the more general notion of *density operators*, or density matrices. When the system is described by a state $|\psi\rangle \in \mathcal{H}$, the associated density operator is the projection operator $\rho = |\psi\rangle\langle\psi|$. In that case, $\rho$ is called a *pure* state. A general density operator $\rho$ is a positive semi-definite operator with trace $\mathrm{Tr}(\rho) = 1$. When $\rho$ is not pure, it is called a *mixed* state. In that case, $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ for some orthonormal states $|\psi_i\rangle$ and positive numbers $p_i$ with $\sum_i p_i = 1$. Let's mention that the mean value of an operator $\hat{A}$ is given by $\langle\hat{A}\rangle = \mathrm{Tr}(\rho\hat{A})$.

**Density matrix of a subsystem** Let $\hat{\rho}$ be the density matrix of a bipartite system $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ with subsystems $A$ and $B$. The density matrix of subsystem $A$, denoted by $\hat{\rho}_A$, is uniquely defined by

$$\langle\psi_i|\hat{\rho}_A|\psi_{i'}\rangle = \sum_j \langle\psi_i, \varphi_j|\hat{\rho}|\psi_{i'}, \varphi_j\rangle \tag{A.5}$$

where $(|\psi_i\rangle)_i$ and $(|\varphi_j\rangle)_j$ are orthonormal basis of respectively $\mathcal{H}_A$ and $\mathcal{H}_B$. $\hat{\rho}_A$ is called the reduced density operator of subsystem $A$. It is in fact the partial trace of $\rho$ over $B$, denoted by

$$\rho_A = \mathrm{Tr}_B(\rho) \tag{A.6}$$

Similarly, we can define $\rho_B = \mathrm{Tr}_A(\rho)$. Let's note that the state of a composite system is entangled if and only if the reduced density operators of its subsystems are mixed states.

**State purification** When considering a potentially mixed state $\rho_A$ of a Hilbert space $\mathcal{H}_A$, it is possible to construct a second Hilbert space $\mathcal{H}_B$ and a pure state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ such that $\rho_A$ is the partial trace of $|\psi\rangle\langle\psi|$ over $B$,

$$\rho_A = \mathrm{Tr}_B(|\psi\rangle\langle\psi|). \tag{A.7}$$

We say that $|\psi\rangle$ is a *purification* of $\rho_A$, or that it purifies $\rho_A$.

### A.1.4 Evolution of a quantum system

The following postulate provides a mathematical description of the temporal evolution of a quantum state.

**Postulate 4** *The evolution of an isolated quantum system over time $\Delta t$ can be described by a unitary operator $\hat{U}$. The state $|\psi_1\rangle$ of the system at time $t_1 = t + \Delta t$ is related to the state $|\psi\rangle$ of the system at time $t$ by the relationship:*

$$|\psi_1\rangle = \hat{U}|\psi\rangle. \tag{A.8}$$

We remind that an operator $\hat{U}$ is called *unitary* when it satisfies $\hat{U}^*\hat{U} = \hat{U}\hat{U}^* = \mathrm{Id}_{\mathcal{H}}$ where $U^*$ is the adjoint operator of $U$ and $\mathrm{Id}_{\mathcal{H}}$ the identity operator on $\mathcal{H}$. An alternative to Postulate 4 is that the evolution of the system is described by the Schrödinger equation,

$$j\hbar\frac{d}{dt}|\psi(t)\rangle = \hat{H}(t)|\psi(t)\rangle, \tag{A.9}$$

where $\hat{H}$ is the Hamiltonian operator of the system, i.e. the observable associated with the total energy of the system.

## A.2 Continuous variables

### A.2.1 Multimode bosonic system

In this thesis, we are interested in continuous variable quantum systems i.e. infinite dimensional Hilbert spaces described by observables with continuous spectra of eigenvalues. The archetype of such spaces are multimode bosonic spaces $\mathcal{H} = \bigotimes_{k=1}^{N} \mathcal{H}_k$ where each $\mathcal{H}_k$ is a Fock space representing a mode. A Fock space $\mathcal{H}_k$ is spanned by its Fock basis, i.e. a basis of the form $\{|0\rangle_k, |1\rangle, \dots, |n\rangle_k, \dots\}$ where the states $|n\rangle_k$ are called Fock states. The corresponding pairs of bosonic operators $(a_k, a_k^\dagger)$, called annihilation and creation operators respectively, are defined by their action on Fock states,

$$\hat{a}_k^\dagger|n\rangle_k = \sqrt{n+1}|n+1\rangle_k \tag{A.10}$$

$$\hat{a}_k|n\rangle_k = \sqrt{n}|n-1\rangle_k. \tag{A.11}$$

They can be assembled as a vectorial operator $\hat{b}$,

$$\hat{b} = (\hat{b}_1, \dots, \hat{b}_{2N})^T = (\hat{a}_1, \hat{a}_1^\dagger, \dots, \hat{a}_N, \hat{a}_N^\dagger)^T \tag{A.12}$$

which satisfies the commutation relation,

$$[\hat{b}_k, \hat{b}_l] = \Omega_{k,l}, \tag{A.13}$$

where $\Omega$ is the symplectic bilinear form, with $2N \times 2N$ matrix defined by

$$\Omega = \bigoplus_{k=1}^{N} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \tag{A.14}$$

Let's note that the commutation relation implies that $\hat{n}_k|n\rangle_k = n|n\rangle_k$ where $\hat{n}_k$ is the number operator $\hat{n}_k = \hat{a}_k^\dagger \hat{a}_k$. Then, the Fock states $|n\rangle_k$ are eigenvectors of the number operators $\hat{n}_k$. The bosonic system may also be described using the quadratures operators arranged in a array $\hat{x}$,

$$\hat{x} = (\hat{x}_1, \ldots, \hat{x}_{2N})^T = (\hat{q}_1, \hat{p}_1, \ldots, \hat{q}_N, \hat{p}_N)^T. \tag{A.15}$$

They are defined by

$$\hat{q}_k = \hat{a}_k + \hat{a}_k^\dagger \tag{A.16}$$

$$\hat{p}_k = j(\hat{a}_k^\dagger - \hat{a}_k) \tag{A.17}$$

and satisfy the commutation relation

$$[\hat{x}_k, \hat{x}_l] = 2j\Omega_{k,l}. \tag{A.18}$$

The quadrature operators are observables with continuous spectra of real eigenvalues, with eigenstates $|q\rangle_k$ and $|p\rangle$ such that

$$\hat{q}_k|q\rangle_k = q|q\rangle_k, \tag{A.19}$$

$$\hat{p}_k|p\rangle_k = p|p\rangle_k, \tag{A.20}$$

for any real values $q$ and $p$. Both sets of eigenstates $|q\rangle_k$ and $|p\rangle_k$ are Hilbert basis of the $k$th mode, linked to each other by a Fourier transform,

$$|q\rangle_k = \frac{1}{2\sqrt{\pi}} \int e^{-jqp/2}|p\rangle_k dp \tag{A.21}$$

$$|p\rangle_k = \frac{1}{2\sqrt{\pi}} \int e^{jqp/2}|q\rangle_k dq \tag{A.22}$$

In the $N$-mode bosonic space, we can write

$$\hat{x}^T|x\rangle = x^T|x\rangle \tag{A.23}$$

where $x \in \mathbb{R}^{2N}$ and $|x\rangle = (|x_1\rangle, \ldots, |x_{2N}\rangle)^T$. The quadrature eigenvalues $x$ can be used to described the state of the system using the phase space representation.

The Fock basis of the multimode space $\mathcal{H}$ can also obtained with the tensor product of the elements of each Fock basis,

$$\{|n_1 \ldots n_N\rangle | (n_1, ..., n_N) \in \mathbb{N}^N\} \tag{A.24}$$

A quantum state in $\mathcal{H}$ can be described by a density operator $\rho$, which is defined by its action on the elements of the Fock basis, and can be represented as a "matrix" with infinite countable dimension. However this formalism is highly unpractical in the case of infinite dimensions. A more practical point of view is the phase space formalism.

### A.2.2 Phase space representation

Any density operator $\rho$ can equivalently be represented by a quasi-probability distribution over a real symplectic space. To do so, we introduce the Weyl operator,

$$\hat{D}(\xi) = \exp(j\hat{x}^T \Omega \xi), \tag{A.25}$$

where $\xi \in \mathbb{R}^{2N}$. Then a density operator $\rho$ is equivalent to a Wigner characteristic function

$$\chi_\rho(\xi) = \mathrm{Tr}(\rho \hat{D}(\xi)) \tag{A.26}$$

and also equivalent to the Wigner function, defined by a Fourier transform,

$$W_\rho(x) = \frac{1}{(2\pi)^{2N}} \int_{\mathbb{R}^{2N}} \chi_\rho(\xi) \exp(-jx^T \Omega \xi) d\xi. \tag{A.27}$$

The Wigner function is normalized to 1, but can take negative values. It is in fact a quasi-probability distribution. The vector $x \in \mathbb{R}^{2N}$ is a vector of continuous variable which are eigenvalues of the quadrature operators $\hat{x}$. They span a real symplectic space $\mathcal{K} = (\mathbb{R}^{2N}, \Omega)$, called the *phase space*.

When considering a quantum state represented by a Wigner function over a symplectic space, we are interest in its statistical moments. The first moment, called *displacement vector* or mean value, is defined by

$$\bar{x} = \langle \hat{x} \rangle = \mathrm{Tr}(\hat{x}\rho) \tag{A.28}$$

and the second moment is the *covariance matrix* $\Gamma$ whose elements are defined by

$$\Gamma_{k,l} = \frac{1}{2}\{\hat{x}_i - \langle \hat{x}_i \rangle; \hat{x}_j - \langle \hat{x}_j \rangle\}, \tag{A.29}$$

where $\{\cdot;\cdot\}$ is the anti-commutator of the operators. This covariance matrix is symmetric of size $2N \times 2N$ and satisfies the uncertainty principle,

$$\Gamma + j\Omega \geq 0 \tag{A.30}$$

which is a consequence of the commutation relations in Equation (A.18).

### A.2.3 Gaussian states

The Gaussian states are a particular class of states that is perfectly characterized by its first two moments, i.e. by its displacement vector and its covariance matrix. They are defined as bosonic states with Gaussian characteristic and Wigner functions,

$$\chi_\rho(\xi) = \exp\Big(\frac{1}{2}\xi^T(\Omega\Gamma\Omega^T)\xi - j(\Omega\bar{x})^T\xi\Big), \tag{A.31}$$

$$W_\rho(x) = \frac{1}{(2\pi)^N \sqrt{\det \Gamma}} \exp\Big(-\frac{1}{2}(x-\bar{x})^T\Gamma^{-1}(x-\bar{x})\Big) \tag{A.32}$$

### A.2.4 Symplectic analysis for Gaussian multimode states

Williamson's theorem asserts that any positive-definite real matrix with even dimension can be put in a diagonal form through a symplectic transformation [96]. In particular, for a covariance matrix $\Gamma$, there exists a symplectic matrix $S$ such that,

$$S^T \Gamma S = \Gamma' \tag{A.33}$$

where $\Gamma'$ is a diagonal matrix of the form

$$\Gamma' = \bigoplus_{k=1}^{N} \begin{bmatrix} \nu_k & 0 \\ 0 & \nu_k \end{bmatrix} \tag{A.34}$$

for a given array of positive values $(\nu_1, \ldots, \nu_N)$, called the *symplectic eigenvalues*. $\Gamma'$ is called the Williamson's form of $\Gamma$. As a reminder, a matrix $S$ is said to be symplectic if $S\Omega S^T = \Omega$. The symplectic eigenvalues of a covariance matrix $\Gamma$ can be computed using the standard eigenvalues of matrix $|j\Omega\Gamma|$, where $|M| = \sqrt{M^\dagger M}$, which is a diagonalizable matrix. The modulus of its $2N$ eigenvalues gives the $N$ symplectic eigenvalues of $\Gamma$.

**One-mode state** The symplectic eigenvalue of a $2\times2$ covariance matrix $\Gamma_1$ is given by its determinant. In fact, since $\det(S) = 1$, we have that $\det(\Gamma_1') = \det(S^T \Gamma_1 S) = \det(\Gamma_1)$, therefore,

$$\nu_1 = \sqrt{\det(\Gamma_1)}. \tag{A.35}$$

**Two-mode state** We want to compute the two symplectic eigenvalues $\nu_1$ and $\nu_2$ of the two-mode $4 \times 4$ covariance matrix $\Gamma_{12}$ given by,

$$\Gamma_{12} = \begin{bmatrix} \Gamma_1 & \sigma_{12} \\ \sigma_{12}^T & \Gamma_2 \end{bmatrix}. \tag{A.36}$$

We introduce the quantity $\Delta$, which is left invariant by symplectic transformation like the determinant,

$$\Delta = \det(\Gamma_1) + \det(\Gamma_2) + 2\det(\sigma_{12}). \tag{A.37}$$

We have that $\det(\Gamma_{12}) = \nu_1^2 \nu_2^2$ and $\Delta = \nu_1^2 + \nu_2^2$. Therefore, $\nu_1^2$ and $\nu_2^2$ are roots of the polynomial equation,

$$r^2 - \Delta \times r + \det(\Gamma_{12}) = 0, \tag{A.38}$$

which are given by

$$\nu_{1,2}^2 = \frac{\Delta \pm \sqrt{\Delta^2 - 4\det(\Gamma_{12})}}{2}. \tag{A.39}$$

**Three-mode state** Let's generalize to the a $N$-mode covariance matrix $\Gamma$ of size $2N \times 2N$. It can be written as a block matrix with $2 \times 2$ block,

$$\Gamma = \begin{bmatrix} \sigma_{11} & \sigma_{12} & \dots & \sigma_{1N} \\ \sigma_{12}^T & \sigma_{22} & \dots & \sigma_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_{1N}^T & \sigma_{2N}^T & \dots & \sigma_{NN} \end{bmatrix}. \tag{A.40}$$

We can construct $N$ symplectic invariant quantities $\Delta_1^N, \dots, \Delta_N^N$ where $\Delta_k^N$ is given by

$$\Delta_k^N = \sum_{1 \le l_1 < \dots < l_k \le N} \det \Gamma_{l_1,\dots,l_k} \tag{A.41}$$

where $\Gamma_{l_1,\dots,l_k}$ is extracted from $\Gamma$ by removing the block rows and block columns of index $l_1, \dots, l_k$.

## A.3 Quantum optics

**Ladder operators** The annihilation and creation operators are uniquely defined by their actions on Fock states,

$$\hat{a}^\dagger |n\rangle = \sqrt{n+1}|n+1\rangle \tag{A.42}$$
$$\hat{a}|n\rangle = \sqrt{n}|n-1\rangle. \tag{A.43}$$

The operator $\hat{n} = \hat{a}^\dagger \hat{a}$ is called boson-number operator. Equations (A.42) and (A.43) implies that

$$\hat{n}|n\rangle = \hat{a}^\dagger \hat{a}|n\rangle = n|n\rangle. \tag{A.44}$$

Thus, any Fock state $|n\rangle$ is eigenvector of the number operator, associated with eigenvalue $n$.

**Coherent states** Coherent states $|\alpha\rangle$ are defined as eigenstates of the annihilation operator, associated with the eigenvalue $\alpha = \frac{q+jp}{2}$,

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle. \tag{A.45}$$

The first two moments of the photon number of a coherent state $|\alpha\rangle$ are given by

$$\langle \hat{n} \rangle = \langle \alpha | \hat{n} | \alpha \rangle = \langle \alpha | \hat{a}^\dagger \hat{a} | \alpha \rangle = \alpha^* \alpha \langle \alpha | \alpha \rangle = |\alpha|^2, \tag{A.46}$$

and

$$\langle \hat{n}^2 \rangle = \langle \alpha | \hat{a}^\dagger \hat{a} \hat{a}^\dagger \hat{a} | \alpha \rangle = \langle \alpha | \hat{a}^\dagger (\hat{a}^\dagger \hat{a} + \mathbf{1}) \hat{a} | \alpha \rangle = |\alpha|^4 + |\alpha|^2. \tag{A.47}$$

Therefore, the variance of the photon number is given by

$$\langle \Delta \hat{n}^2 \rangle = \langle \hat{n}^2 \rangle - \langle \hat{n} \rangle^2 = |\alpha|^2. \tag{A.48}$$

**Quadrature operators** The real and imaginary parts of $\alpha = \frac{q+ip}{2}$ can be seen as the values of the quadrature operators $\hat{q}$ and $\hat{p}$. The quadrature operators are defined by

$$\hat{q} = \hat{a} + \hat{a}^\dagger \tag{A.49}$$

$$\hat{p} = -j(\hat{a} - \hat{a}^\dagger) \tag{A.50}$$

They fulfill the commutation relation

$$\begin{aligned}[\hat{q}, \hat{p}] &= -j[\hat{a} + \hat{a}^\dagger, \hat{a} - \hat{a}^\dagger] && \text{(A.51)}\\ &= -j([\hat{a}, \hat{a}] - [\hat{a}, \hat{a}^\dagger] + [\hat{a}^\dagger, \hat{a}] - [\hat{a}^\dagger, \hat{a}^\dagger]) && \text{(A.52)}\\ &= 2j. && \text{(A.53)}\end{aligned}$$

The fact that $[\hat{q}, \hat{p}] \neq 0$ implies that one cannot perform simultaneous measurements of both quadratures. In fact, using Robertson's inequality, we obtain the inequality

$$\langle \Delta\hat{q}^2 \rangle \langle \Delta\hat{p}^2 \rangle \geq \left| \frac{1}{2}[\hat{q}, \hat{p}] \right|^2 = 1. \tag{A.54}$$

**Quadratures of a coherent state** We will see that the quadratures a coherent state are equally noisy and have the minimum uncertainty allowed by equation (A.54). The first moments of $\hat{q}$ and $\hat{p}$ of a coherent state $|\alpha\rangle$ are given by

$$\begin{aligned}\langle \hat{q} \rangle &= \langle \alpha | \hat{q} | \alpha \rangle = \langle \alpha | \hat{a} + \hat{a}^\dagger | \alpha \rangle = \langle \alpha | \hat{a} | \alpha \rangle + \langle \alpha | \hat{a}^\dagger | \alpha \rangle \\ &= \alpha + \alpha^* = 2\,\mathrm{Re}(\alpha) = q, && \text{(A.55)}\\ \langle \hat{p} \rangle &= \langle \alpha | \hat{p} | \alpha \rangle = -j\langle \alpha | \hat{a} - \hat{a}^\dagger | \alpha \rangle = -j\langle \alpha | \hat{a} | \alpha \rangle + j\langle \alpha | \hat{a}^\dagger | \alpha \rangle \\ &= -j\alpha + j\alpha^* = 2\,\mathrm{Im}(\alpha) = p, && \text{(A.56)}\end{aligned}$$

and the second moments are

$$\begin{aligned}\langle \hat{q}^2 \rangle &= \langle \alpha | \hat{q}^2 | \alpha \rangle = \langle \alpha | (\hat{a} + \hat{a}^\dagger)^2 | \alpha \rangle \\ &= \langle \alpha | \hat{a}^2 | \alpha \rangle + \langle \alpha | \hat{a}\hat{a}^\dagger | \alpha \rangle + \langle \alpha | \hat{a}^\dagger \hat{a} | \alpha \rangle + \langle \alpha | (\hat{a}^\dagger)^2 | \alpha \rangle \\ &= \langle \alpha | \hat{a}^2 | \alpha \rangle + \langle \alpha | \hat{n} + \mathbf{1} | \alpha \rangle + \langle \alpha | \hat{n} | \alpha \rangle + \langle \alpha | (\hat{a}^\dagger)^2 | \alpha \rangle \\ &= \alpha^2 + 2\alpha^*\alpha + 1 + (\alpha^*)^2 \\ &= \frac{q^2}{4} - \frac{p^2}{4} + j\frac{qp}{2} + \frac{q^2}{2} + \frac{p^2}{2} + 1 + \frac{q^2}{4} - \frac{p^2}{4} - j\frac{qp}{2} \\ &= q^2 + 1, && \text{(A.57)}\\ \langle \hat{p}^2 \rangle &= \langle \alpha | \hat{p}^2 | \alpha \rangle = -\langle \alpha | (\hat{a} - \hat{a}^\dagger)^2 | \alpha \rangle \\ &= -\langle \alpha | \hat{a}^2 | \alpha \rangle + \langle \alpha | \hat{a}\hat{a}^\dagger | \alpha \rangle + \langle \alpha | \hat{a}^\dagger \hat{a} | \alpha \rangle - \langle \alpha | (\hat{a}^\dagger)^2 | \alpha \rangle \\ &= -\langle \alpha | \hat{a}^2 | \alpha \rangle + \langle \alpha | \hat{n} + \mathbf{1} | \alpha \rangle + \langle \alpha | \hat{n} | \alpha \rangle - \langle \alpha | (\hat{a}^\dagger)^2 | \alpha \rangle \\ &= -\alpha^2 + 2\alpha^*\alpha + 1 - (\alpha^*)^2 \\ &= -\frac{q^2}{4} + \frac{p^2}{4} - j\frac{qp}{2} + \frac{q^2}{2} + \frac{p^2}{2} + 1 - \frac{q^2}{4} + \frac{p^2}{4} + j\frac{qp}{2} \\ &= p^2 + 1. && \text{(A.58)}\end{aligned}$$

Therefore, the variances of $\hat{q}$ and $\hat{p}$ are

$$\langle \Delta \hat{q}^2 \rangle = \langle \hat{q}^2 \rangle - \langle \hat{q} \rangle^2 = 1, \tag{A.59}$$

$$\langle \Delta \hat{p}^2 \rangle = \langle \hat{p}^2 \rangle - \langle \hat{p} \rangle^2 = 1. \tag{A.60}$$

# Appendix B

# Statistical estimators

In the following, we consider that Alice reveals that she transmitted the coherent states $|\alpha_k\rangle$ with $\alpha_k = (q_k + jp_j)/2$. For these revealed states, Bob has the quadratures measured after quantum heterodyne detection

$$s_k = N_0\left(\sqrt{\frac{T}{2}}q_k + w_k^{(1)}\right)$$
$$r_k = N_0\left(\sqrt{\frac{T}{2}}p_k + w_k^{(2)}\right)$$

where $w_k^{(1)}$ and $w_k^{(2)}$ are additive white Gaussian noise with variance $(1 + T\xi_A/2)$, and $N_0$ is the shot noise variance. We estimate the quantum symbol before the beam-splitter of the heterodyne detection as

$$\hat{\beta}_k = \frac{1}{\sqrt{2\hat{N}_0}}(s_k + jr_k), \tag{B.1}$$

where $\hat{N}_0$ is an estimator for the shot-noise variance $N_0$.

## B.1 Shot-noise estimator

Bob can estimate the shot noise variance using the calibrated noise symbols $n_k$, real-valued additive white Gaussian noise with variance $N_0$. The estimator is

$$\hat{N}_0 = \frac{1}{N}\sum_{k=1}^{N} n_k^2. \tag{B.2}$$

In fact, the random variable $(N\hat{N}_0/N_0)$ follows a chi-squared distribution. During parameter estimation, we normalize Bob's measured quadratures to the shot noise unit by dividing by $\hat{N}_0^{\frac{1}{2}}$. That's why we will require the moments of the random variable $(N_0/\hat{N}_0)^{\frac{1}{2}}$. First of all, by Monte-Carlo estimation, we obtain heuristically that

$$E\left[\sqrt{\frac{N_0}{\hat{N}_0}}\right] \approx 1 + \frac{3}{4N} \tag{B.3}$$

Then, the first two moments of the inverse chi-squared ($N_0/(N\hat{N}_0)$) are known and give that

$$E\Big[\frac{N_0}{\hat{N}_0}\Big] = \frac{N}{N-2} \approx 1 + \frac{2}{N} \tag{B.4}$$

$$E\Big[\Big(\frac{N_0}{\hat{N}_0}\Big)^2\Big] = \frac{N^2}{(N-2)(N-4)} \approx 1 + \frac{6}{N} \tag{B.5}$$

## B.2 $\hat{c}_2$ estimator

An estimator for the quantity $c_2$ is given by

$$\begin{aligned}\hat{c}_2 &= \mathrm{Re}\Big(\frac{1}{K}\sum_{k=1}^{K}\overline{\alpha_k}\hat{\beta}_k\Big) \\ &= \frac{1}{\sqrt{\hat{N}_0}}\frac{\sqrt{2}}{4K}\sum_{k=1}^{K} q_k s_k + p_k r_k.\end{aligned}$$

If the real and imaginary part of the modulation are independent and identically distributed, we can reduce to the case of real symbols

$$\hat{c}_2 = \frac{1}{\sqrt{\hat{N}_0}}\frac{\sqrt{2}}{2N}\sum_{k=1}^{N} x_k y_k \tag{B.6}$$

with $N = 2K$, $x_{2k-1} = s_k$, $x_{2k} = r_k$, and $y_k = N_0(\sqrt{\frac{T}{2}}x_k + w_k)$ with $w_k$ AWGN of variance $(1 + T\xi_A/2)$. Finally, we obtain

$$\hat{c}_2 = \sqrt{\frac{N_0}{\hat{N}_0}}\Big(\frac{\sqrt{T}}{2N}\sum_{k=1}^{N} x_k^2 + \frac{\sqrt{2}}{2N}\sum_{k=1}^{N} x_k w_k\Big). \tag{B.7}$$

**Expected value**

$$\begin{aligned}E[\hat{c}_2] &= E\Big[\sqrt{\frac{N_0}{\hat{N}_0}}\Big]\Big(\frac{\sqrt{T}}{2}E[x_k^2] + \frac{\sqrt{2}}{2}E[x_k]E[w_k]\Big) \\ &= E\Big[\sqrt{\frac{N_0}{\hat{N}_0}}\Big]\sqrt{T}\langle n\rangle \\ &\approx c_2 + \frac{3}{4N}c_2.\end{aligned} \tag{B.8}$$

**Second moment**

$$\hat{c}_2^2 = \frac{N_0}{\hat{N}_0}\Big(\frac{T}{4N^2}\sum_{k} x_k^2 x_l^2 + \frac{\sqrt{2T}}{2N^2}\sum_{k,l} x_k^2 x_l w_l + \frac{1}{2N^2}\sum_{k,l} x_k w_k x_l w_l\Big) \tag{B.9}$$

$$
\begin{aligned}
E[\hat{c}_2^2] &= E\left[\frac{N_0}{\hat{N}_0}\right]\left(\frac{T}{4N^2}(NE[x_1^4] + N(N-1)E[x_1^2]^2) + \frac{1}{2N^2}NE[x_1^2]E[w_1^2]\right) \\
&= \frac{N}{N-2}\left(\frac{T}{4N}E[x_1^4] + \frac{N-1}{N}c_2^2 + \frac{1}{N}\langle n\rangle(1+\xi_B)\right) \\
&= c_2^2 + \frac{1}{N-2}\left(\frac{T}{4}E[x_1^4] + c_2^2 + \langle n\rangle(1+\xi_B)\right) \qquad \text{(B.10)}
\end{aligned}
$$

**Variance**

$$
\begin{aligned}
\mathrm{Var}(\hat{c}_2) &= E[\hat{c}_2^2] - E[\hat{c}_2]^2 \\
&\approx \frac{1}{2K}\left(\frac{T}{4}E[x_1^4] + \langle n\rangle(1+\xi_B) - \frac{1}{2}c_2^2\right) \qquad \text{(B.11)}
\end{aligned}
$$

## B.3 $\hat{c}_1$ estimator

An estimator for the quantity $c_1$ is given by

$$
\begin{aligned}
\hat{c}_1 &= \mathrm{Re}\left(\frac{1}{K}\sum_{k=1}^{K}\overline{\gamma_k}\hat{\beta}_k\right) \\
&= \frac{1}{\sqrt{\hat{N}_0}}\frac{\sqrt{2}}{2K}\sum_{k=1}^{K}\mathrm{Re}(\gamma_k)s_k + \mathrm{Im}(\gamma_k)r_k.
\end{aligned}
$$

In the case of 1024-QAM, $\mathrm{Re}(\gamma_k)$ and $\mathrm{Im}(\gamma_k)$ are independent and identically distributed. Therefore we can reduce to the case of real symbols with $a_{2k-1} = \mathrm{Re}(\gamma_k)$ and $a_{2k} = \mathrm{Im}(\gamma_k)$,

$$
\begin{aligned}
\hat{c}_1 &= \frac{1}{\sqrt{\hat{N}_0}}\frac{\sqrt{2}}{N}\sum_{k=1}^{N}a_k y_k \qquad \text{(B.12)} \\
&= \sqrt{\frac{N_0}{\hat{N}_0}}\left(\frac{\sqrt{T}}{N}\sum_{k=1}^{N}a_k x_k + \frac{\sqrt{2}}{N}\sum_{k=1}^{N}a_k w_k\right). \qquad \text{(B.13)}
\end{aligned}
$$

**Expected value**

$$
\begin{aligned}
E[\hat{c}_1] &= E\left[\sqrt{\frac{N_0}{\hat{N}_0}}\right]\sqrt{T}E[a_1 x_1] \qquad \text{(B.14)} \\
&= c_1 + \frac{3}{4N}c_1 \qquad \text{(B.15)}
\end{aligned}
$$

**Second moment**

$$
(\hat{c}_1)^2 = \frac{1}{N^2}\frac{N_0}{\hat{N}_0}\left(T\sum_{k,l}a_k a_l x_k x_l + 2\sqrt{2T}\sum_{k,l}a_k x_k a_l w_l + 2\sum_{k,l}a_k w_k a_l w_l\right) \qquad \text{(B.16)}
$$

$$
\begin{aligned}
E[(\hat{c}_1)^2] &= \frac{1}{N^2} E\left[\frac{N_0}{\hat{N}_0}\right] \Big( T(NE[a_1^2 x_1^2] + N(N-1)E[a_1 x_1]^2) + 2NE[a_1^2](1+\xi_B) \Big) \\
&= \frac{1}{N} \frac{N}{N-2} \Big( T(E[a_1^2 x_1^2] - E[a_1 x_1]^2) + NTE[a_1 x_1]^2 + 2E[a_1^2](1+\xi_B) \Big) \\
&= \frac{1}{N-2} \Big( T \operatorname{Var}(a_1 x_1) + N c_1^2 + 2E[a_1^2](1+\xi_B) \Big) \\
&\approx c_1^2 + \frac{1}{N} \Big( T \operatorname{Var}(a_1 x_1) + 2c_1^2 + 2E[a_1^2](1+\xi_B) \Big)
\end{aligned} \tag{B.17}
$$

**Variance**

$$
\begin{aligned}
\operatorname{Var}(\hat{c}_1) &= E[\hat{c}_1^2] - E[\hat{c}_1]^2 \\
&\approx \frac{1}{2K} \Big( \frac{c_1^2}{2} + T \operatorname{Var}(a_1 x_1) + E[a_1^2](1+\xi_B) 2 \Big)
\end{aligned} \tag{B.18}
$$

We note that $\operatorname{Var}(a_1 x_1)$ and $E[a_1^2]$ can be computed numerically and only depend on the modulation and $V_A$.

## B.4 $\hat{n}_B$ estimator

An estimator for the quantity $n_B$ is given by

$$
\begin{aligned}
\hat{n}_B + 1 &= \frac{1}{K} \sum_k |\beta_k|^2 \\
&= \frac{1}{\hat{N}_0} \frac{1}{2K} \sum_k s_k^2 + r_k^2 \\
&= \frac{N_0}{\hat{N}_0} \Big( \frac{T}{2N} \sum_k x_k^2 + \frac{\sqrt{2T}}{N} \sum_k x_k w_k + \frac{1}{N} \sum_k w_k^2 \Big)
\end{aligned} \tag{B.19}
$$

**Expected value**

$$
\begin{aligned}
E[\hat{n}_B + 1] &= E\left[\frac{N_0}{\hat{N}_0}\right] \big( \frac{T}{2} E[x_1^2] + E[w_1^2] \big) \\
&= \frac{N}{N-2} (T\langle n \rangle + 1 + \xi_B) \\
&= \frac{N}{N-2} (n_B + 1)
\end{aligned} \tag{B.20}
$$

**Second moment**

$$
\begin{aligned}
(\hat{n}_B + 1)^2 = \frac{N_0^2}{N^2 \hat{N}_0^2} \Big( & \frac{T^2}{4} \sum_{k,l} x_k^2 x_l^2 + 2T \sum_{k,l} x_k w_k x_l w_l + \sum_{k,l} w_k^2 w_l^2 \\
& + T\sqrt{2T} \sum_{k,l} x_k^2 x_l w_l + T \sum_{k,l} x_k^2 w_l^2 + 2\sqrt{2T} \sum_{k,l} x_k w_k w_l^2 \Big)
\end{aligned} \tag{B.21}
$$

$$
\begin{aligned}
E[(\hat{n}_B+1)^2] &= \frac{1}{N^2}E\left[\frac{N_0^2}{\hat{N}_0^2}\right]\Big\{\frac{T^2}{4}\big(NE[x_1^4]+N(N-1)E[x_1^2]^2\big)+2TNE[x_1^2]E[w_1^2] \\
&\qquad + NE[w_1^4]+N(N-1)E[w_1^2]^2+TN^2E[x_1^2]E[w_1^2]\Big\} \\
&\approx \frac{1}{N}\Big(1+\frac{6}{N}\Big)\Big\{\frac{T^2}{4}\big(E[x_1^4]+(N-1)V_A^2\big)+2TV_A(1+\xi_B) \\
&\qquad + 3(1+\xi_B)^2+(N-1)(1+\xi_B)^2+TNV_A(1+\xi_B)\Big\} \\
&\approx \frac{1}{N}\Big(1+\frac{6}{N}\Big)\Big\{\frac{T^2}{4}\big(E[x_1^4]-V_A^2\big)+2TV_A(1+\xi_B)+2(1+\xi_B)^2 \\
&\qquad + N\Big((1+\xi_B)^2+TV_A(1+\xi_B)+\frac{T^2}{4}V_A^2\Big)\Big\} \\
&\approx \frac{1}{N}\Big(1+\frac{6}{N}\Big)\Big\{\frac{T^2}{4}\big(E[x_1^4]-3V_A^2\big)+2(n_B+1)^2+N(n_B+1)^2\Big\} \\
&\approx (1+n_B)^2+\frac{1}{N}\Big(\frac{T^2}{4}\big(E[x_1^4]-3V_A^2\big)+8(n_B+1)^2\Big)
\end{aligned}
\tag{B.22}
$$

**Variance**

$$
\begin{aligned}
\mathrm{Var}(\hat{n}_B) &= E[\hat{n}_B^2]-E[\hat{n}_B]^2 \\
&= \frac{1}{2K}\Big(\frac{T^2}{4}\big(E[x_1^4]-3V_A^2\big)+4(n_B+1)^2\Big)
\end{aligned}
\tag{B.23}
$$

## B.5 Alternative $\hat{c}_1$ estimator

To estimate the quantity $c_1$, we rather use the estimator given in [5], which is more robust to statistical fluctuations. For each possible $\alpha_{(i)}$ in the constellation, with $i \in \{1,\dots,M\}$, we derive the average $\beta_{(i)}$ received by Bob when Alice transmitted $|\alpha_{(i)}\rangle$. Thus,

$$
\beta_{(i)} = \frac{1}{N_i}\sum_{k=1}^{K}\delta_{k,i}\beta_k \tag{B.24}
$$

where $\delta_{k,i}=1$ if $\alpha_k=\alpha_{(i)}$, and $\delta_{k,i}=0$ otherwise, and $N_i=\sum_{k=1}^{K}\delta_{k,i}$. If $N_i=0$, we use the convention $\beta_{(i)}=0$. In fact, the random variable $\delta_{k,i}$ follows a Bernoulli distribution with parameter $p_i$, the probability of the symbol $\alpha_{(i)}$ in the modulation, and $N_i$ follows a binomial distribution with parameters $(K,p_i)$. Finally, an estimator

for the quantity $c_1$ is given by

$$\begin{aligned}\hat{c}_1 &= \mathrm{Re}\Big(\sum_{i=1}^{M} p_i \overline{\gamma_{(i)}}\beta_{(i)}\Big),\\ &= \mathrm{Re}\Big(\sum_{i=1}^{M} p_i \overline{\gamma_{(i)}}\frac{1}{N_i}\sum_{k=1}^{K}\delta_{k,i}\beta_k\Big),\\ &= \sum_{i=1}^{M}\sum_{k=1}^{K} p_i \frac{\delta_{k,i}}{N_i}\,\mathrm{Re}(\overline{\gamma_{(i)}}\beta_k),\end{aligned} \tag{B.25}$$

where $\gamma_{(i)} = \langle\alpha_{(i)}|a_\tau|\alpha_{(i)}\rangle$. We compute the expected value of $\frac{\delta_{1,i}}{N_i}$,

$$\begin{aligned}E\Big[\frac{\delta_{1,i}}{N_i}\Big] &= p_i E\Big[\frac{\delta_{k,i}}{\sum_k \delta_{1,i}}\Big|\delta_{1,i}=1\Big]\\ &= p_i E\Big[\frac{1}{1+N_i'}\Big]\end{aligned}$$

where $N_i'$ follows a binomial distribution with parameters $(K-1, p_i)$. Then,

$$\begin{aligned}E\Big[\frac{\delta_{1,i}}{N_i}\Big] &= p_i\sum_{k=0}^{K-1}\frac{1}{1+k}\binom{K-1}{k}p_i^k(1-p_i)^{K-1-k}\\ &= \sum_{k=0}^{K-1}\frac{1}{K}\binom{K}{k+1}p_i^{k+1}(1-p_i)^{K-(k+1)}\\ &= \frac{1}{K}\sum_{k=1}^{K}\binom{K}{k}p_i^k(1-p_i)^{K-k}\\ E\Big[\frac{\delta_{1,i}}{N_i}\Big] &= \frac{1}{K}(1-(1-p_i)^K)\end{aligned} \tag{B.26}$$

Then, we come back to the calculation of $\hat{c}_1$,

$$\begin{aligned}\hat{c}_1 &= \sum_{i=1}^{M}\sum_{k=1}^{K} p_i\frac{\delta_{k,i}}{N_i}Re(\overline{\gamma_{(i)}}\beta_k)\\ &= \sqrt{\frac{N_0}{\hat{N}_0}}\sum_{i=1}^{M}\sum_{k=1}^{K} p_i\frac{\delta_{k,i}}{N_i}Re(\overline{\gamma_{(i)}}(\sqrt{T}\alpha_k + w_k))\\ &= \sqrt{\frac{N_0}{\hat{N}_0}}\Big(\sqrt{T}\sum_{i=1}^{M}\sum_{k=1}^{K} p_i\frac{\delta_{k,i}}{N_i}Re(\overline{\gamma_{(i)}}\alpha_k) + \sum_{i=1}^{M}\sum_{k=1}^{K} p_i\frac{\delta_{k,i}}{N_i}Re(\overline{\gamma_{(i)}}w_k)\Big).\end{aligned}$$

We deduce that

$$\begin{aligned}E[\hat{c}_1] &= E\Big[\sqrt{\frac{N_0}{\hat{N}_0}}\Big]\sqrt{T}\sum_{i=1}^{M}\sum_{k=1}^{K} p_i E\Big[\frac{\delta_{1,i}}{N_i}\Big]Re(\overline{\gamma_{(i)}}\alpha_{(i)})\\ &= \Big(1+\frac{3}{4K}\Big)\sqrt{T}\sum_{i=1}^{M} p_i(1-(1-p_i)^K)Re(\overline{\gamma_{(i)}}\alpha_{(i)})\\ &= \Big(1+\frac{3}{4K}\Big)\Big(c_1 - \sqrt{T}\sum_{i=1}^{M} p_i(1-p_i)^K Re(\overline{\gamma_{(i)}}\alpha_{(i)})\Big).\end{aligned} \tag{B.27}$$

**Variance** The calculation of the second moment is more complicated because of the non independence of the random variables $N_i$. Therefore, we rather estimate the variance using Monte-Carlo estimations, for each values of the parameters ($V_A$, $\xi_B$, $T$, etc).

# List of Acronyms

| | |
|---|---|
| AWG | arbitrary waveform generator |
| AWGN | additive white Gaussian noise |
| BPS | blind phase search |
| CAZAC | constant amplitude zero autocorrelation waveform |
| CMA | constant modulus algorithm |
| CV-QKD | continous-variable quantum-key-distribution |
| DC | direct current |
| DD-LMS | direct-detection least-mean-square |
| DGD | differential group delay |
| DSP | digital signal processing |
| DV-QKD | discrete-variable quantum-key-distribution |
| EB | entanglement-based |
| EPR | Einstein–Podolsky–Rosen |
| FIR | finite impulse response |
| IF | intermediate frequency |
| IQ | in-phase and quadrature |
| ISI | inter-symbol interference |
| LO | local oscillator |
| MZ | Mach-Zehnder |
| QKD | quantum-key-distribution |
| OPLL | optical phase-locked loop |
| PBS | polarization beam splitter |
| PCS | probabilistic constellation shaping |
| PLL | phase locked-loop |
| PM | prepare-and-measure |
| PMD | polarization mode dispersion |
| PSK | phase shift keying |
| QAM | quadrature amplitude modulation |
| QPSK | quadrature phase shift keying |
| RC | raised cosine |
| RF | radio-fréquence |
| RRC | root raised cosine |

| | |
|---|---|
| SKR | secret key rate |
| SNR | signal to noise ratio |
| SNU | shot noise unit |
| SMF | single mode fiber |
| VOA | variable optical attenuator |
| WDM | wavelength division multiplexing |

# List of Figures

# Bibliography


[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 7–11, Dec. 2014.

[2] F. Grosshans and P. Grangier, "Continuous Variable Quantum Cryptography Using Coherent States," *Physical Review Letters*, vol. 88, p. 057902, Jan. 2002.

[3] S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, "Asymptotic Security of Continuous-Variable Quantum Key Distribution with a Discrete Modulation," *Physical Review X*, vol. 9, p. 021059, June 2019.

[4] J. Lin, T. Upadhyaya, and N. Lütkenhaus, "Asymptotic Security Analysis of Discrete-Modulated Continuous-Variable Quantum Key Distribution," *Physical Review X*, vol. 9, p. 041064, Dec. 2019.

[5] A. Denys, P. Brown, and A. Leverrier, "Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation," *Quantum*, vol. 5, p. 540, Sept. 2021.

[6] S. M. Bellovin, "Frank Miller: Inventor of the One-Time Pad," *Cryptologia*, vol. 35, pp. 203–222, July 2011.

[7] "Secret signaling system," July 1919.

[8] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, pp. 656–715, Oct. 1949.

[9] N. I. o. S. and Technology, "Data Encryption Standard (DES)," Tech. Rep. Federal Information Processing Standard (FIPS) 46 (Withdrawn), U.S. Department of Commerce, Jan. 1977.

[10] B. Schneier, "Description of a new variable-length key, 64-bit block cipher (Blowfish)," in *Fast Software Encryption* (R. Anderson, ed.), Lecture Notes in Computer Science, (Berlin, Heidelberg), pp. 191–204, Springer, 1994.

[11] N. I. o. S. and Technology, "Advanced Encryption Standard (AES)," Tech. Rep. Federal Information Processing Standard (FIPS) 197, U.S. Department of Commerce, Nov. 2001.

[12] W. Diffie and M. E. Hellman, "Multiuser cryptographic techniques," in *Proceedings of the June 7-10, 1976, National Computer Conference and Exposition*, AFIPS '76, (New York, NY, USA), pp. 109–112, Association for Computing Machinery, June 1976.

[13] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120–126, Feb. 1978.

[14] N. I. o. S. and Technology, "Digital Signature Standard (DSS)," Tech. Rep. Federal Information Processing Standard (FIPS) 186-4, U.S. Department of Commerce, July 2013.

[15] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Journal on Computing*, vol. 26, pp. 1484–1509, Oct. 1997.

[16] J. L. Park, "The concept of transition in quantum mechanics," *Foundations of Physics*, vol. 1, pp. 23–33, Mar. 1970.

[17] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, pp. 802–803, Oct. 1982.

[18] D. Dieks, "Communication by EPR devices," *Physics Letters A*, vol. 92, pp. 271–272, Nov. 1982.

[19] N. Herbert, "FLASH—A superluminal communicator based upon a new kind of quantum measurement," *Foundations of Physics*, vol. 12, pp. 1171–1179, Dec. 1982.

[20] G. Ghirardi, *Entanglement, Nonlocality, Superluminal Signaling and Cloning*. IntechOpen, Apr. 2013.

[21] S. Wiesner, "Conjugate coding," *ACM SIGACT News*, vol. 15, pp. 78–88, Jan. 1983.

[22] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nature Communications*, vol. 8, p. 15043, Apr. 2017.

[23] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Physical Review Letters*, vol. 67, pp. 661–663, Aug. 1991.

[24] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Physical Review Letters*, vol. 68, pp. 557–559, Feb. 1992.

[25] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics," *Reviews of Modern Physics*, vol. 83, pp. 33–80, Mar. 2011.

[26] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, pp. 400–403, May 2018.

[27] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, "Experimental quantum key distribution beyond the repeaterless secret key capacity," *Nature Photonics*, vol. 13, pp. 334–338, May 2019.

[28] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu, F. Zhou, H.-F. Jiang, T.-Y. Chen, H. Li, L.-X. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, "Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas," *Nature Photonics*, vol. 15, pp. 570–575, Aug. 2021.

[29] D. Mayers and A. Yao, "Quantum Cryptography with Imperfect Apparatus," *arXiv:quant-ph/9809039*, Sept. 1998.

[30] R. Colbeck, "Quantum And Relativistic Protocols For Secure Multi-Party Computation," *arXiv:0911.3814 [quant-ph]*, Feb. 2011.

[31] P. T. Fraser and B. C. Sanders, "Loophole-Free Bell Tests and the Falsification of Local Realism," *Journal of Student Science and Technology*, vol. 10, Aug. 2017.

[32] H.-K. Lo, M. Curty, and B. Qi, "Measurement-Device-Independent Quantum Key Distribution," *Physical Review Letters*, vol. 108, p. 130503, Mar. 2012.

[33] F. Xu, M. Curty, B. Qi, and H.-K. Lo, "Practical aspects of measurement-device-independent quantum key distribution," *New Journal of Physics*, vol. 15, p. 113007, Nov. 2013.

[34] M. Hillery, "Quantum cryptography with squeezed states," *Physical Review A*, vol. 61, p. 022309, Jan. 2000.

[35] T. C. Ralph, "Continuous variable quantum cryptography," *Physical Review A*, vol. 61, p. 010303, Dec. 1999.

[36] M. D. Reid, "Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations," *Physical Review A*, vol. 62, p. 062308, Nov. 2000.

[37] N. J. Cerf, M. Lévy, and G. V. Assche, "Quantum distribution of Gaussian keys using squeezed states," *Physical Review A*, vol. 63, p. 052311, Apr. 2001.

[38] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using gaussian-modulated coherent states," *Nature*, vol. 421, pp. 238–241, Jan. 2003.

[39] S. Ren, S. Yang, A. Wonfor, I. White, and R. Penty, "Demonstration of high-speed and low-complexity continuous variable quantum key distribution system with local local oscillator," *Scientific Reports*, vol. 11, p. 9454, May 2021.

[40] H. Wang, Y. Pi, W. Huang, Y. Li, Y. Shao, J. Yang, J. Liu, C. Zhang, Y. Zhang, and B. Xu, "High-speed Gaussian-modulated continuous-variable quantum key distribution with a local local oscillator based on pilot-tone-assisted phase compensation," *Optics Express*, vol. 28, pp. 32882–32893, Oct. 2020.

[41] N. Jain, H.-M. Chin, H. Mani, C. Lupo, D. S. Nikolic, A. Kordts, S. Pirandola, T. B. Pedersen, M. Kolb, B. Ömer, C. Pacher, T. Gehring, and U. L. Andersen, "Practical continuous-variable quantum key distribution with composable security," *arXiv:2110.09262 [quant-ph]*, Oct. 2021.

[42] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," *Nature Photonics*, vol. 7, pp. 378–381, May 2013.

[43] Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, X. Wang, Y. Huang, C. Xu, X. Zhang, Z. Wang, M. Li, X. Zhang, Z. Zheng, B. Chu, X. Gao, N. Meng, W. Cai, Z. Wang, G. Wang, S. Yu, and H. Guo, "Continuous-variable QKD over 50 km commercial fiber," *Quantum Science and Technology*, vol. 4, p. 035006, May 2019.

[44] T. Wang, P. Huang, L. Li, Y. Zhou, and G. Zeng, "Boosting higher secret key rate in quantum key distribution over mature telecom components," Jan. 2022.

[45] D. Milovančev, N. Vokić, F. Laudenbach, C. Pacher, H. Hübel, and B. Schrenk, "High Rate CV-QKD Secured Mobile WDM Fronthaul for Dense 5G Radio Networks," *Journal of Lightwave Technology*, vol. 39, pp. 3445–3457, June 2021.

[46] H. Wang, Y. Li, Y. Pi, Y. Pan, Y. Shao, L. Ma, J. Yang, Y. Zhang, W. Huang, and B. Xu, "Sub-Gbps key rate four-state continuous-variable quantum key distribution within metropolitan area," *arXiv:2111.09540 [quant-ph]*, Nov. 2021.

[47] T. Hirano, T. Ichikawa, T. Matsubara, M. Ono, Y. Oguri, R. Namiki, K. Kasai, R. Matsumoto, and T. Tsurumaru, "Implementation of continuous-variable quantum key distribution with discrete modulation," *Quantum Science and Technology*, vol. 2, p. 024010, June 2017.

[48] A. Leverrier, "Security of Continuous-Variable Quantum Key Distribution via a Gaussian de Finetti Reduction," *Physical Review Letters*, vol. 118, p. 200501, May 2017.

[49] T. A. Eriksson, T. A. Eriksson, R. S. Luís, K. Gümüş, G. Rademacher, B. J. Puttnam, H. Furukawa, N. Wada, Y. Awaji, A. Alvarado, M. Sasaki, and M. Takeoka, "Digital Self-Coherent Continuous Variable Quantum Key Distribution System," in *Optical Fiber Communication Conference (OFC) 2020 (2020), Paper T3D.5*, p. T3D.5, Optical Society of America, Mar. 2020.

[50] M. Rückmann, S. Kleis, and C. G. Schaeffer, "17 GBd Sub-Photon Level Heterodyne Detection for CV-QKD Enabled by Machine Learning," in *Optical Fiber Communication Conference (OFC) 2020 (2020), Paper Th2A.54*, p. Th2A.54, Optical Society of America, Mar. 2020.

[51] F. Roumestan, A. Ghazisaeidi, J. Renaudier, P. Brindel, E. Diamanti, and P. Grangier, "Demonstration of Probabilistic Constellation Shaping for Continuous Variable Quantum Key Distribution," in *2021 Optical Fiber Communications Conference and Exhibition (OFC)*, pp. 1–3, June 2021.

[52] F. Roumestan, A. Ghazisaeidi, J. Renaudier, L. T. Vidarte, E. Diamanti, and P. Grangier, "High-Rate Continuous Variable Quantum Key Distribution Based on Probabilistically Shaped 64 and 256-QAM," in *2021 European Conference on Optical Communication (ECOC)*, (Bordeaux, France), pp. 1–4, IEEE, Sept. 2021.

[53] G. van Assche, *Quantum Cryptography and Secret-Key Distillation*. Cambridge: Cambridge University Press, 1st edition ed., Oct. 2012.

[54] P. Jouguet, D. Elkouss, and S. Kunz-Jacques, "High-bit-rate continuous-variable quantum key distribution," *Physical Review A*, vol. 90, p. 042329, Oct. 2014.

[55] A. Leverrier, "Composable Security Proof for Continuous-Variable Quantum Key Distribution with Coherent States," *Physical Review Letters*, vol. 114, p. 070501, Feb. 2015.

[56] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Reviews of Modern Physics*, vol. 81, pp. 1301–1350, Sept. 2009.

[57] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, "Continuous-Variable Quantum Key Distribution with Gaussian Modulation – The Theory of Practical Implementations," *Advanced Quantum Technologies*, vol. 1, p. 1800011, Aug. 2018.

[58] T. Upadhyaya, T. van Himbeeck, J. Lin, and N. Lütkenhaus, "Dimension Reduction in Quantum Key Distribution for Continuous- and Discrete-Variable Protocols," *PRX Quantum*, vol. 2, p. 020325, May 2021.

[59] P. Papanastasiou and S. Pirandola, "Continuous-variable quantum cryptography with discrete alphabets: Composable security under collective Gaussian attacks," *Physical Review Research*, vol. 3, p. 013047, Jan. 2021.

[60] I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states," *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, Jan. 2005.

[61] R. Renner and J. I. Cirac, "De Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography," *Physical Review Letters*, vol. 102, p. 110504, Mar. 2009.

[62] R. Renner, "Symmetry of large physical systems implies independence of subsystems," *Nature Physics*, vol. 3, pp. 645–649, Sept. 2007.

[63] R. García-Patrón and N. J. Cerf, "Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution," *Physical Review Letters*, vol. 97, p. 190503, Nov. 2006.

[64] M. Navascués, F. Grosshans, and A. Acín, "Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography," *Physical Review Letters*, vol. 97, p. 190502, Nov. 2006.

[65] 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*, vol. 3, pp. 535–552, Oct. 2003.

[66] A. Lapidoth, *A Foundation in Digital Communication*. Cambridge: Cambridge University Press, second edition ed., Feb. 2017.

[67] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, pp. 379–423, July 1948.

[68] G. Frank, "Pulse code communication," Mar. 1953.

[69] G. Böcherer, P. Schulte, and F. Steiner, "Probabilistic Shaping and Forward Error Correction for Fiber-Optic Communication Systems," *Journal of Lightwave Technology*, vol. 37, pp. 230–244, Jan. 2019.

[70] L. Zehnder, "Ein neuer Interferenzrefraktor," *Zeitschr. für Instrumentenkunde*, vol. 11, pp. 275–285, 1891.

[71] E. Mach, "über einen Interferenzrefraktor," *Zeitschr. für Instrumentenkunde*, vol. 12, pp. 89–93, 1892.

[72] K. Kikuchi, "Fundamentals of Coherent Optical Fiber Communications," *Journal of Lightwave Technology*, vol. 34, pp. 157–179, Jan. 2016.

[73] S. Schaefer, M. Gregory, and W. Rosenkranz, "Coherent receiver design based on digital signal processing in optical high-speed intersatellite links with M-phase-shift keying," *Optical Engineering*, vol. 55, p. 111614, Oct. 2016.

[74] K. C. Kao and G. A. Hockham, "Dielectric-fibre surface waveguides for optical frequencies," *Proceedings of the Institution of Electrical Engineers*, vol. 113, pp. 1151–1158, July 1966.

[75] P. J. Winzer, D. T. Neilson, and A. R. Chraplyvy, "Fiber-optic transmission and networking: The previous 20 and the next 20 years [Invited]," *Optics Express*, vol. 26, pp. 24190–24239, Sept. 2018.

[76] ITU-T, "G.652 : Characteristics of a single-mode optical fibre and cable," Nov. 2016.

[77] ITU-T, "G.654 : Characteristics of a cut-off shifted single-mode optical fibre and cable." https://www.itu.int/rec/T-REC-G.654-202003-I/, Mar. 2020.

[78] M. C. Fugihara and A. N. Pinto, "Attenuation fitting functions," *Microwave and Optical Technology Letters*, vol. 51, no. 10, pp. 2294–2296, 2009.

[79] G. Agrawal, *Nonlinear Fiber Optics*. Academic Press, 2001.

[80] J. Proakis and M. Salehi, *Digital Communications*. Boston: McGraw-Hill Higher Education, 5e édition ed., Nov. 2007.

[81] M. S. Faruk, Y. Mori, C. Zhang, K. Igarashi, and K. Kikuchi, "Multi-impairment monitoring from adaptive finite-impulse-response filters in a digital coherent receiver," *Optics Express*, vol. 18, pp. 26929–26936, Dec. 2010.

[82] S. J. Savory, "Digital filters for coherent optical receivers," *Optics Express*, vol. 16, pp. 804–817, Jan. 2008.

[83] S. Qureshi, "Adaptive equalization," *Proceedings of the IEEE*, vol. 73, pp. 1349–1387, Sept. 1985.

[84] D. Godard, "Self-Recovering Equalization and Carrier Tracking in Two-Dimensional Data Communication Systems," *IEEE Transactions on Communications*, vol. 28, pp. 1867–1875, Nov. 1980.

[85] R. Johnson, P. Schniter, T. Endres, J. Behm, D. Brown, and R. Casas, "Blind equalization using the constant modulus criterion: A review," *Proceedings of the IEEE*, vol. 86, pp. 1927–1950, Oct. 1998.

[86] A. Ghazisaeidi, I. Fernandez de Jauregui Ruiz, R. Rios-Müller, L. Schmalen, P. Tran, P. Brindel, A. Carbo Meseguer, Q. Hu, F. Buchali, G. Charlet, and J. Renaudier, "Advanced C+L-Band Transoceanic Transmission Systems Based on Probabilistically Shaped PDM-64QAM," *Journal of Lightwave Technology*, vol. 35, pp. 1291–1299, Apr. 2017.

[87] K. Kikuchi, "Clock recovering characteristics of adaptive finite-impulse-response filters in digital coherent optical receivers," *Optics Express*, vol. 19, pp. 5611–5619, Mar. 2011.

[88] M. Selmi, C. Gosset, M. Noelle, P. Ciblat, and Y. Jaouen, "Block-Wise Digital Signal Processing for PolMux QAM/PSK Optical Coherent Systems," *Journal of Lightwave Technology*, vol. 29, pp. 3070–3082, Oct. 2011.

[89] T. Pfau, S. Hoffmann, and R. Noe, "Hardware-Efficient Coherent Digital Receiver Concept With Feedforward Carrier Recovery for M-QAM Constellations," *Journal of Lightwave Technology*, vol. 27, pp. 989–999, Apr. 2009.

[90] J. P. Gordon and H. Kogelnik, "PMD fundamentals: Polarization mode dispersion in optical fibers," *Proceedings of the National Academy of Sciences*, vol. 97, pp. 4541–4550, Apr. 2000.

[91] H. H. Brunner, S. Bettelli, L. C. Comandar, D. Hillerkuss, C.-H. F. Fung, D. Wang, S. Mikroulis, A. Poppe, and M. Peev, "Precise Noise Calibration for CV-QKD," in *Optical Fiber Communication Conference (OFC) 2019 (2019), Paper Th1J.2*, p. Th1J.2, Optical Society of America, Mar. 2019.

[92] N. Jain, I. Derkach, H.-M. Chin, R. Filip, U. L. Andersen, V. C. Usenko, and T. Gehring, "Modulation leakage vulnerability in continuous-variable quantum key distribution," *Quantum Science and Technology*, vol. 6, p. 045001, Oct. 2021.

[93] A. Milewski, "Periodic Sequences with Optimal Properties for Channel Estimation and Fast Start-Up Equalization," *IBM Journal of Research and Development*, vol. 27, pp. 426–431, Sept. 1983.

[94] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, "Analysis of Imperfections in Practical Continuous-Variable Quantum Key Distribution," *Physical Review A*, vol. 86, p. 032309, Sept. 2012.

[95] A. Arnould, H. Mardoyan, F. Pulka, A. Ghazisaeidi, V. Aref, B. Bordez, P. Tondo, L. D. Cort, E. Pincemin, N. Brochier, F. Chatter, V. Guillot-Common, O. Bertran-Pardo, M. Frascolla, L. Luchesini, and J. Renaudier, "Field Trial Demonstration over Live Traffic Network of 400 Gb/s Ultra-Long Haul and 600 Gb/s Regional Transmission," in *2020 European Conference on Optical Communications (ECOC)*, pp. 1–4, Dec. 2020.

[96] J. Williamson, "On the Algebraic Problem Concerning the Normal Forms of Linear Dynamical Systems," *American Journal of Mathematics*, vol. 58, no. 1, pp. 141–163, 1936.