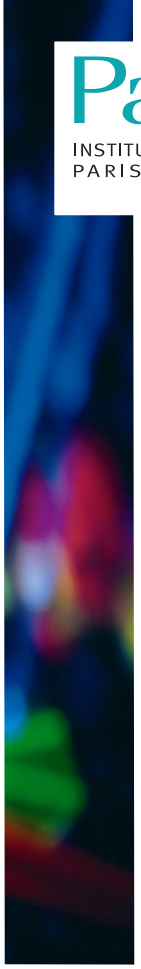
Sécurité pratique de systèmes de cryptographie quantique : étude d'attaques et développement de contre-mesures

Hao Qin



ParisTech
INSTITUT DES SCIENCES ET TECHNOLOGIES
PARIS INSTITUTE OF TECHNOLOGY

TELECOM ParisTech

2015-ENST-0040

EDITE - ED 130

Doctorat ParisTech

T H È S E

pour obtenir le grade de docteur délivré par

TELECOM ParisTech

Spécialité « Informatique et Réseaux »

présentée et soutenue publiquement par

Hao QIN

le 10 juillet 2015

Sécurité pratique de systèmes de cryptographie quantique : Étude d'attaques et développement de contre-mesures

Directeur de thèse : **Romain Alléaume**
Co-encadrement de la thèse : **Pascal Urien**

Jury

M. Vadim Makarov, Professeur, Institute for Quantum Computing, University of Waterloo	Rapporteur
M. Paul Voss, Professeur, School of Electrical and Computer Engineering, Georgia Tech	Rapporteur
M. Thierry Debuisschert, Chercheur (HDR), Thales Research and Technology	Examinateur
M. Yves Jouen, Professeur, Département COMELEC, Télécom ParisTech	Examinateur

TELECOM ParisTech
Ecole de l'Institut Mines-Télécom - Membre de ParisTech

T H È S E

I would like to dedicate this thesis to my family.

Acknowledgements

First of all, I would like to thank my supervisors Romain Alléaume and Pascal Urien for accepting me to pursue this thesis. Foremost I would like to extend my sincere gratitude to Romain Alléaume, for his patient guidance and knowledges supporting my study. I am deeply grateful for his valuable comments, ideas and strict manners to research works. His considerate supervisions help me overcome many difficulties and keep my research progress in right track. My heartfelt thanks also go to Rupesh Kumar who helps me a lot in the lab work and always answers my questions patiently. I also benefit many experimental knowledges and technical skills from him. I appreciate many helpful discussions with Romain Alléaume and Rupesh Kumar that motivate my work.

I would like to extend my special thanks to Vadim Makarov, Paul Voss, Thierry Debuisschert and Yves Jouen, who have agreed to serve as my thesis juries and review this thesis. It is also a great honor to have the most famous quantum hacker, Vadim Makarov, to examine my thesis, as I have admired his work ever since the beginning of this thesis.

It was a great experience to spend my study in the quantum information team of TELECOM ParisTech. I would like to take this opportunity to thank everyone who is now or who stayed in the team: Isabelle Zaquine, Eleni Diamanti, Elham Kashefi, Damian Markham, Tom Lawson, Marc Kaplan, Tanumoy Pramanik, Bill Plick, Anne Marin, Anna Pappa, Zizhu Wang, Adel Sohbi, Leonardo Disilvestro, Adrien Marie, Seiseki Akibue, Niraj Kumar, Paul Jouguet and Sébastien Kunz-Jacques. From quantum lunches, student meetings to Christmas dinners, these activities enrich my academic knowledges and life experiences. I would also like to thank all the members in the Paris Centre for Quantum Computing, I also benefit from various tutorials and seminars organized by this centre in the fields of quantum information and commutation. My thanks also go to all the colleges working in the office at Place d'Italie, it indeed has a nice and relaxing atmosphere which is suitable for research work.

Next, I would like to thank all the people that I have met in the quantum key distribution community, I really appreciate the stimulating discussions with Jingzheng Huang, Zhenyu Li, Yichen Zhang, Fabian Furrer and Frédéric Grosshans. I would also like to extend my thanks to Patrick Trinkler for his full support on my internships in IDQuantique

during 10/2013 and 02/2015. My thanks also go to Mathilde Soucarros, Damien Stucki and Matthieu Legré for their help during my internships.

Finally, I would like to express my sincere gratitude to my parents for their continuous supports and encouragements through my whole life. Without their supports, it would be impossible for me to study in France and not even mentioned to complete this thesis. I would also like to thank all my friends for their accompanies and supports.

Abstract

In this thesis, I study a cryptographic primitive called Quantum Key Distribution (QKD). QKD allows two remote parties, the sender Alice and the receiver Bob to share a secret key, in the presence of an eavesdropper, Eve, whose power is only limited by the laws of quantum physics. In classical cryptography, public key cryptography is widely used to perform secret key agreement. However, the security of public key cryptography is based on some unproven mathematical assumptions while QKD can be proven unconditionally secure, based on the fundamental laws of quantum mechanics. QKD security proofs however only apply to implementations verifying some trust assumptions that may be violated in a practical setup. As a matter of fact, an implementation may leak information through side channels not considered in the security proof, opening security loopholes and the possibility for a potential eavesdropper to launch so-called side channel attacks targeting the implementation. Such attacks have indeed been recently demonstrated both on research and commercial QKD systems. This highlights the importance of implementation security in QKD.

I focus my study on the implementation and the practical security of continuous-variable (CV) QKD protocols and more particularly on the Gaussian-modulated coherent state protocol. More precisely, I have concentrated my work on two important challenges in practical CV QKD:

(1) Side channel attacks on practical CV QKD systems: I have studied different imperfections in an implementation of a CV QKD system and analyzed their impacts on the security and performance. Moreover, for the first time, I have proposed and studied a detector-based side channel attack in CV QKD: saturation attack. This opens a new security loophole that we have characterized experimentally in the lab, on a real CV QKD system.

(2) Integration of a CV QKD system within an optical network: I have studied carefully the different noise impairments that can be encountered when deploying CV QKD in coexistence with intense classical channels in a Dense Wavelength Division Multiplexing (DWDM) network. We have moreover demonstrated experimentally for the first time the feasibility of a CV QKD deployment in a DWDM network.

Keywords: quantum cryptography, quantum key distribution, quantum communication, continuous variable, homodyne detection, practical security, side channel attack, quantum hacking, wavelength division multiplexing

Résumé

Dans cette thèse, j'étudie une primitive cryptographique appelée distribution quantique de clés, (en anglais Quantum Key Distribution ou QKD). La distribution quantique de clés permet à deux parties distantes, l'expéditrice Alice et le récepteur Bob de partager une clé secrète en présence d'une espion, Eve, dont la puissance est seulement limité par les lois de la physique quantique. Contrairement à la cryptographie à clé publique qui est largement utilisée et dont la sécurité est fondée sur des hypothèses non prouvées mathématiques, la sécurité inconditionnelle de la QKD est basée sur les lois fondamentales de la mécanique quantique. Les preuves de sécurité en QKD s'appliquent en revanche uniquement à des dispositifs expérimentaux vérifiant des hypothèses en terme de confiance. Ces hypothèses peuvent être violées dans des configurations pratiques. En effet les dispositifs expérimentaux peuvent présenter des imperfections et rayonner de l'information par des canaux cachés auxiliaires non considérés dans le preuve de sécurité ouvrant la voie à des attaques. Les attaques par canaux auxiliaires qui exploitent les imperfections des appareils ont déjà été démontrés à la fois sur des systèmes QKD de recherche et des systèmes commerciaux. Cela souligne l'importance de la sécurité pratique dans la mise en œuvre des protocoles de QKD. J'ai concentré mon travail de thèse sur la distribution quantique de clés à variables continues (en anglais CV QKD) et en particulier, sur l'étude pratique d'implémentations de protocoles à états cohérents modulés de façon gaussienne. Plus précisément, mes contributions portent sur deux aspects essentiels en CV QKD:

(1) Les attaques par canaux auxiliaires sur des systèmes CV QKD pratiques. J'ai étudié différentes imperfections pouvant intervenir dans la mise en œuvre pratique d'un système de CV QKD et analysé leurs impacts sur la sécurité et leurs effets sur la performance. En particulier, j'ai proposé et étudié théoriquement une attaque par canaux cachés originale, visant les détecteurs en CV QKD: l'attaque par saturation. Nous avons de plus démontré expérimentalement la faisabilité de cette attaque sur un système CV QKD dans notre laboratoire.

(2) L'intégration d'un système de CV QKD au sein des réseaux optiques DWDM. J'ai étudié attentivement les différentes sources de bruit qui peuvent être rencontrées lorsque l'on déploie un système CV QKD en coexistence avec des canaux classiques intense, au

sein d'une architecture optique DWDM. Nous avons en outre démontré expérimentalement pour la première fois la faisabilité du déploiement d'un système CV QKD dans un réseau optique DWDM.

Mots-clés: cryptographie quantique, la distribution quantique de clés, la communication quantique, variables continues, détection homodyne, sécurité pratique, attaque à canal auxiliaire, piratage quantique, multiplexage en longueur d'onde

Table of contents

Résumé en français

Dans cette thèse, j'étudie une primitive cryptographique appelée distribution quantique de clés, (en anglais Quantum Key Distribution ou QKD) et en particulier l'utilisation de variables continues. Plus précisément, j'ai concentré mon travail sur l'étude de sécurité pratique d'implémentations de la distribution quantique de clés à variables continues (en anglais CV-QKD).

Partie I: Introduction

1.1. Cryptographie classique

A l'ère d'Internet, la communication numérique est d'une grande commodité dans la vie des gens. Avec l'augmentation du trafic Internet, la sécurité des communications acquiert une importance croissante, étant donné que tout message non crypté est potentiellement accessible à un espion. Dans une communication sécurisée, un message secret est transmis par une émettrice appelée Alice vers un récepteur appelé Bob, tandis qu'un espion appelé Ève ne devrait accéder en aucune façon au message secret, si la communication est sécurisée. Afin d'assurer la sécurité de la communication, on peut avoir recours à la cryptographie pour effectuer le cryptage, qui joue aujourd'hui un rôle important dans le monde numérique. En cryptographie moderne, il existe principalement deux types de protocoles cryptographiques: *symmetric-key* et *asymmetric-key*.

En cryptographie symétrique, Alice utilise une clé privée pour crypter son message, tandis que Bob utilise la même clé pour décrypter le message envoyé par Alice. Il est donc demandé aux deux parties de partager une clé secrète et d'en préserver le secret pendant le cryptage et le décryptage. En revanche, la cryptographie asymétrique, aussi appelée cryptographie à clé publique, utilise une clé publique pour crypter le message du côté d'Alice, tandis que Bob utilise une clé privée pour décrypter le message. La clé publique est distribuée au public (tout le monde peut y avoir accès), tandis que la clé privée est gardée secrète et qu'elle est connue uniquement de Bob.

Le problème de la distribution des clés et la sécurité informatique Il est prouvé qu'un protocole de cryptage symétrique, appelé masque jetable (en anglais one time pad ou OTP) (appelé également chiffre Vernam [175]), offre une sécurité inconditionnelle [157]. La sécurité inconditionnelle du cryptage implique qu'Ève ne peut rien savoir du message, sans qu'il faille pour autant remettre en doute ses compétences informatiques. Cependant, afin d'assurer la sécurité théorique des informations dans l'implémentation du protocole OTP (masque jetable), il y a plusieurs conditions requises. Notamment, Alice et Bob doivent partager des clés secrètes identiques qui doivent être véritablement aléatoires et dont la longueur doit être au moins égale au message, de plus, la clé ne peut être réutilisée. Ces conditions requises pourraient être difficiles à réaliser. D'abord, les nombres aléatoires vrais ne peuvent apparemment pas être générés au moyen d'un procédé physique classique, en raison de la nature déterministe de la physique classique. Deuxièmement, l'utilisation du protocole OTP implique la distribution d'un nombre important de clés secrètes, si le message à crypter est très long, et une clé secrète ne peut être créée sur un canal dont la sécurité n'est pas assurée. C'est ce que l'on appelle le problème de la distribution des clés. Pour ces raisons, le protocole OTP est utilisé seulement quand un très haut niveau de sécurité est exigé. Par contre, des protocoles de cryptographie symétrique comme Standard de Chiffrement Avancé (en anglais Advanced Encryption Standard ou AES) et Standard de Chiffrement des Données (en anglais Data Encryption Standard ou DES) requièrent seulement un petit nombre de clé secrètes pour chiffrer de grandes quantités de données et sont aujourd'hui largement utilisés pour assurer la sécurité des communications. Cependant, ces techniques ne peuvent toujours pas résoudre totalement le problème de distribution des clés et n'offrent pas une sécurité inconditionnelle.

Étant donné l'augmentation du volume d'informations nécessitant d'être chiffrées, la cryptographie à clé publique est devenue plus populaire et est aujourd'hui largement déployée dans les systèmes de cryptographie. Cela est dû principalement au fait que la cryptographie à clé publique apporte une solution pratique au problème de distribution des clés, comparativement à la cryptographie symétrique. Ainsi, Alice chiffre les données à l'aide d'une clé publique connue de tous et Bob déchiffre les données grâce à une clé privée que lui seul connaît. La sécurité de la cryptographie à clé publique repose sur l'hypothèse mathématique non démontrée qu'il existe des fonctions univoques faciles à calculer mais difficiles à inverser. Par exemple, concernant le protocole RSA largement utilisé [151], sa sécurité repose sur l'hypothèse selon laquelle il est difficile de factoriser de grands entiers. Cependant, cette hypothèse n'a pas encore été prouvée, il est encore possible que quelqu'un trouve des algorithmes hautement efficaces permettant de factoriser de grands nombres et de violer la sécurité de RSA. En fait, dans le domaine du calcul quantique, il a

été démontré que l'algorithme de Shor [160] peut efficacement factoriser un grand nombre. En d'autres termes, si un gros ordinateur quantique venait à être construit, il pourrait être facile de porter atteinte à la sécurité de la plupart des systèmes à clé publique, comme le protocole RSA. Bien que ces grands ordinateurs quantiques soient encore loin d'être une réalité, les éventuels espions peuvent toujours enregistrer la communication aujourd'hui et casser le chiffre plus tard, le jour où un ordinateur quantique sera disponible. En revanche, même avec les technologies actuelles, l'augmentation de la puissance de calcul des super-ordinateurs existant aujourd'hui représente également une menace pour la sécurité de la cryptographie à clé publique. Par exemple, la factorisation d'un module RSA de 768 bits [73] a été réalisée avec succès récemment.

Comme nous l'avons vu, la sécurité de la cryptographie classique repose souvent sur des hypothèses de puissance de calcul non prouvées, ce qui signifie que des avancées matérielles ou des algorithmes seraient susceptibles d'altérer la sécurité. Les hypothèses de calcul peuvent être vues comme une vulnérabilité potentielle pour la cryptographie classique d'aujourd'hui. Lorsque l'on requiert un haut niveau de sécurité de communication, alors il ne faut pas prendre le risque que l'hypothèse soit cassée, ce qui porterait atteinte à la sécurité.

1.2. La distribution quantique de clés

En fait, le problème de distribution des clés peut être potentiellement résolu par l'une des applications les plus prometteuses de la technologie d'information quantique: La distribution quantique de clés (en anglais Quantum Key Distribution ou QKD). Contrairement aux algorithmes de calcul sécurisés, la sécurité de la QKD est établie, indépendamment de la puissance de calcul d'un espion. La sécurité de la QKD repose sur les lois fondamentales de la mécanique quantique, notamment sur la théorie du théorème de non clonage quantique: on ne peut pas copier parfaitement un état quantique inconnu. Le principe d'incertitude d'Heisenberg, étroitement apparenté, lie le phénomène parasitaire des signaux observés chez Alice et Bob aux fuites d'informations potentiellement détournées vers Eve. La perturbation des signaux d'Alice et de Bob augmente au fur et à mesure qu'Eve a accès aux informations. Alice et Bob peuvent choisir une fraction de leurs données au hasard pour évaluer ces perturbations et établir le lien avec l'information accessible à Eve. La fuite d'informations correspondante vers Eve peut alors peut être éliminée dans la clé finale partagée par Alice et Bob, grâce aux méthodes d'amplification de la confidentialité. La clé secrète de QKD générée peut être utilisée pour réaliser un chiffrage OTP, en permettant d'assurer la sécurité inconditionnelle de la communication sur une la liaison (canal authentifié classique et canal quantique public).

Bref aperçu sur le développement de la QKD Le premier protocole de QKD et le plus connu est le BB84 [11]. Il a été introduit par Bennett et Brassard en 1984. Ce protocole repose sur le chiffrage d'informations discrètes (bits) sur la phase ou la polarisation d'états mono photoniques et la valeur de bit est mesurée à la réception par des analyseurs de phase ou de polarisation, puis par des détecteurs mono photoniques. Par conséquent, on parle de protocole QKD à variable discrète (DV). Depuis l'invention du BB84, plusieurs protocoles de QKD ont été proposés [44, 154] et la QKD s'est considérablement développée ces vingt dernières années, à la fois au niveau théorique et expérimental. Sur le plan théorique, un certain nombre de preuves de sécurité ont été rigoureusement établies pour prouver la sécurité théorique des informations de la QKD [154]. Sur le plan expérimental, la distance de distribution de clés de QKD a atteint plus de 300 km sur une liaison à fibres optiques en laboratoire [76] et 144 km d'espace libre [156]. Des taux de génération de clés secrètes supérieurs à 1 Mbits/s ont également été atteints [27]. De plus, les applications de la QKD se sont étendues aux réseaux. Des réseaux de QKD de la taille de grandes villes ont été démontrés dans [131, 153]. Récemment, un réseau de QKD dont il a été fait état dans [177], a non seulement servi à des fins scientifiques mais aussi à des fins de protection des communications réelles des institutions militaires ou financières. Dans cette thèse, plutôt que d'étudier les protocoles de DV QKD comme BB84, je me concentre sur une approche alternative de la QKD, la QKD à variable continue (CV). En CV-QKD, des nombres réels sont encodés dans les quadratures du champ électromagnétique, qui peuvent être mesurés par une détection homodyne au lieu de détecteurs de photons uniques. Le protocole de CV-QKD le plus établi est le GG02 [48], qui a été proposé par Grosshans et Grangier en 2002. Le protocole GG02 requiert seulement des composants télécoms optiques standards pour la préparation et la détection d'états cohérents. Comparativement à la DV QKD, la CV-QKD se trouve à un stage moins avancé aux niveaux théorique et expérimental. Ces dernières années, des résultats remarquables ont cependant été atteints dans ces deux directions. Sur le plan de la théorie, des preuves de sécurité du protocole à modulation gaussienne contre [38, 123] les attaques collectives et arbitraires [92, 147] ont déjà été établies. De récents travaux montrent également que des progrès ont été réalisés en termes de preuves de sécurité de compossibilité [86]. Sur le plan expérimental, plusieurs démonstrations de CV-QKD ont été réalisées avec des systèmes de fibres optiques [25, 34, 64, 68, 103, 137], et il a été récemment prouvé que la CV-QKD peut couvrir 80 km sur une liaison à fibres optiques en laboratoire [68].

Perspectives pour la QKD Grâce aux efforts réalisés par les chercheurs ces vingt dernières années, la QKD a atteint une maturité suffisante pour être mise en œuvre dans le monde réel,

assurant une communication sécurisée. Concernant les approches DV et CV, des produits commerciaux sont sortis sur le marché. Pour la DV QKD, les acteurs principaux sont les sociétés telles qu'ID Quantique [3], MagiQ Technologies Inc., Austrian Institute of Technology [1], Anhui Quantum Communication Technology Co., Ltd.[2], tandis que pour la CV-QKD, on peut citer SeQureNet [5] et Quintessence Labs [4] qui sont allées jusqu'à commercialiser cette technologie. Etant donné le besoin considérable d'un haut niveau de sécurité des communications, la QKD pourrait jouer un rôle important à l'avenir dans une infrastructure de communication sécurisée. Selon les prévisions, le marché mondial de la QKD pourrait représenter plus d'un milliard de dollars US en 2018 [60].

1.3. Motivations sous-tendant notre travail

Comme les QKD sont utilisées pour assurer des communications sûres dans le monde réel, il est crucial de vérifier leur sécurité et performance, surtout pour les mises en service de systèmes commerciaux. Les utilisateurs de QKD sont en fait intéressés par la sécurité et les performances réelles que peuvent offrir les systèmes QKD plutôt que par la sécurité théorique qui est mise en avant. La sécurité pratique des systèmes QKD est un sujet important qui a été activement étudié au cours des dernières années dans la communauté QKD. Deux directions majeures apparaissent dans l'étude pratique des QKD: (1) *le piratage quantique* (ou *les attaques par canaux cachés*) sur les systèmes QKD pratiques; (2) l'intégration des systèmes QKD dans un réseau optique. Dans cette thèse, je me suis plus particulièrement concentré sur ces deux aspects avec les mises en œuvre de protocoles CV-QKD.

Attaques par canaux cachés dans le système CV-QKD Le concept d'attaques par canaux cachés est dérivé de la cryptologie classique, qui définit qu'une une attaque par canaux cachés vise à obtenir des informations grâce à l'installation physique d'un système de cryptologie au lieu d'engager une attaque brutale et violente ou de chercher les faiblesses théoriques dans les algorithmes cryptographiques. Des informations précieuses peuvent fuiter de différents *canaux cachés*, telles que la consommation énergétique, les signaux électromagnétiques ou toute sorte de signaux physiques qui peuvent être émis à partir d'un système de cryptographie. Les attaques par canaux cachés prennent en principe pour cible la manière dont un protocole cryptographique est mis en œuvre, plutôt que le protocole lui-même.

Les systèmes QKD pratiques sont aussi confrontés au défi des attaques par canaux cachés. La sécurité inconditionnelle des QKD repose fortement sur la validité d'hypothèses sur les équipements QKD. Toutefois ces hypothèses ne peuvent pas toujours être vérifiées dans les mises en œuvre réelles, puisque les équipements réels ont toujours quelques im-

perfections qui peuvent les amener à se comporter assez différemment des modèles mathématiques décrits dans la preuve de sécurité. Certaines imperfections peuvent provoquer des failles, permettant à un écouteur clandestin de lancer des attaques pouvant mettre en péril sa sécurité. Il faut noter que l'existence d'attaques par canaux cachés n'est pas en contradiction avec l'existence des preuves de sécurité dans les QKD, puisque les attaques par canaux cachés ne sont pas couvertes par les preuves de sécurité. En fait, les attaques par canaux cachés sur les DV QKD ont été étudiées au cours des années passées et sont devenues un sujet brûlant de la recherche portant sur les QKD. Diverses stratégies de piratage quantique ont été proposées, dans lesquelles les détecteurs de photon unique de Bob sont souvent considérés comme les cibles, par exemple, les attaques par décalage temporel [137, 194], les attaques par aveuglement [42, 116], les attaques "after gate" [185], les attaques sur le temps mort des détecteurs [184], etc. Certaines de ces attaques ont aussi été démontrées expérimentalement [42, 107, 190] y compris une mise en œuvre complète d'un parfait écouteur clandestin [42]. D'autres attaques visant différents équipements ont aussi été proposées pour mettre en péril la sécurité pratique des systèmes DV QKD [43, 93, 168, 190].

Les systèmes CV-QKD ne sont pas non plus à l'abri du problème des attaques par canaux cachés. L'un des problèmes de sécurité essentiels dans la mise en œuvre des CV-QKD concerne une référence de phase classique, l'oscillateur local (OL), qui est généralement transféré par le réseau public sur le canal entre Alice et Bob. Le signal de l'OL ne transporte pas d'informations mais est une référence de phase pour la mesure homodyne et ses caractéristiques ont un lien étroit avec les paramètres dans l'étalonnage d'un système CV-QKD, et particulièrement l'étalonnage du bruit de photon. En effet, en fonction de la manipulation du signal de l'OL, des attaques sur l'étalonnage du bruit de photon ont été proposées pour mettre en péril la sécurité pratique des systèmes CV-QKD [32, 51, 66, 111]. Des mesures possibles pour contrer les attaques visant l'OL ont été proposées ensuite: (1) en contrôlant le signal de l'OL et le bruit de photon en temps réel [66]. (2) en utilisant des techniques d'asservissement de la phase, Alice et Bob peuvent générer localement le signal de l'OL plutôt que de l'envoyer d'un côté vers l'autre au moyen d'un canal ouvert [139, 162].

Afin de réduire l'écart entre la sécurité théorique et la sécurité pratique des DV ou des CV-QKD, en particulier, pour faire face aux menaces d' attaques par canaux cachés sur les QKD, deux approches principales ont été examinées: (1) développer un protocole QKD *device independent* (DI) [6]. (2) examiner autant de canaux cachés possibles dans les mises en œuvre de systèmes QKD, et développer les contremesures correspondantes. Pour ce qui touche à la première approche, la DI QKD permet d'éviter les hypothèses qui doivent s'appliquer aux équipements dans la mise en œuvre de QKD. La DI QKD offre une belle solution en théorie pour contrer les attaques par canaux cachés, toutefois, il ne s'agit pas

d'une solution pratique au regard du niveau de la technologie actuelle. Il apparaît que même pour une efficacité de détection proche de (1), la DI QKD peut seulement générer un taux de clé très bas [23, 45]. Un autre fait qui rend les protocoles DI QKD moins réalistes est qu'ils impliquent un test sans faille des inégalités de Bell qui, jusqu'à présent, n'a pas été démontré expérimentalement. En fait, une approche alternative appelée *measurement device independent* (MDI) QKD [100] a donné quelques résultats utiles ces dernières années. La MDI QKD peut éviter toute attaque par canaux cachés visant une extrémité d'un système QKD, en particulier la partie avec les détecteurs. Les protocoles de MDI QKD ont été mis en œuvre par plusieurs groupes et ont donné des résultats prometteurs en termes de taux de clé et de distance [98, 152, 169, 170]. Tous ces travaux portant la MDI portent sur les protocoles DV QKD. Le développement de protocoles MDI dans le domaine de la CV-QKD est relativement lent. Une raison évidente en est qu'avant cette thèse, aucune faille de sécurité liée aux détecteurs n'avait été rapportée concernant les protocoles CV-QKD. Néanmoins, des protocoles MDI CV-QKD avec des états cohérents [95, 113] et avec des états comprimés [94, 193] ont été proposés ces dernières années. Toutefois, en raison de l'analyse théorique et du niveau de technologie actuel, ils sont encore loin de la mise en œuvre pratique.

L'étude de device independent dépasse le cadre de cette thèse. J'ai choisi une autre approche en étudiant et analysant les différents canaux cachés qui pourrait mettre en péril la sécurité des mises en œuvre pratiques et existantes de CV-QKD. De manière réaliste, il est impossible de découvrir tous les canaux cachés qui pourraient apparaître dans une mise en œuvre pratique. Cependant, je peux toujours étudier ce qui importe le plus pour la sécurité pratique et faire un classement des différents types d'attaques par canaux cachés. En effet, à partir de l'expérience des attaques par canaux cachés connues dans la QKD, une fois qu'une faille spécifique a été trouvée, la protection n'est en général pas trop difficile à mettre en place et, en principe, toutes les attaques par canaux cachés liées à une faille spécifique peuvent être éliminées grâce à une seule contremesure. Par exemple, une fois que le signal de l'OL peut être produit localement chez Alice et Bob [139, 162], les systèmes CV-QKD sont protégés vis-à-vis de toutes les attaques reliées à l'OL. [51, 66, 111]. Par conséquent, l'analyse des canaux cachés améliorerait en fin de compte la sécurité pratique des systèmes CV-QKD et ouvrirait la voie à une certification de sécurité des QKD.

Dans cette thèse, j'ai étudié différentes imperfections dans la mise en œuvre des CV-QKD et analysé leur impact sur la sécurité et la performance. J'ai aussi découvert et étudié une nouvelle faille de sécurité qui peut aboutir à un nouveau type d'attaques par canaux cachés dans un système CV-QKD: l'attaque par saturation.

Intégration de la CV-QKD dans les réseaux optiques Un avantage intéressant de la QKD est qu'elle est compatible avec les réseaux optiques actuels. Un autre sujet de cette thèse est l'étude de l'intégration des systèmes CV-QKD dans les réseaux optiques. Avec le développement des QKD, les QKD peuvent passer d'une application point à point à une configuration de réseau [131, 153]. D'un autre côté, le Multiplexage par répartition en longueur d'onde (en anglais Wavelength-division multiplexing ou WDM) permet d'avoir de multiples canaux optiques, à différentes longueur d'onde, pour partager une seule fibre optique. Il serait intéressant que les QKD soient acheminées par le réseau de fibre optique existant avec des signaux classiques.

La première architecture de coexistence de la technologie WDM avec les QKD a été proposée par [173]. La faisabilité de la coexistence des QKD avec le réseau WDM a été étudiée et démontrée ces dernières années [15, 17, 30, 126, 132]. Ces études ont montré que le bruit induit par les signaux classiques forts pourrait empêcher les communications QKD, parce que la puissance optique des canaux classiques est habituellement plusieurs fois plus élevée que le signal quantique des QKD. Surtout, dans le cas d'une coexistence avec des canaux *de Multiplexage par répartition en longueur d'onde dense* (en anglais Dense Wavelength-division multiplexing ou DWDM), où la différence de longueur d'onde entre le signal quantique et le signal classique est très petite (espacement de canaux de 0,8 nm). Divers bruits additionnels dus à une isolation insuffisante et aux effets optiques non-linéaires des signaux classiques peuvent impacter la communication quantique, ce qui peut finalement aboutir à un taux de clé nulle pour la QKD. La coexistence avec des canaux classiques intenses est en effet un défi pratique pour la QKD.

La plupart des études et démonstrations portent essentiellement les systèmes DV QKD. Par contraste, peu d'études [138] ont été faites sur l'intégration d'un système CV-QKD dans un réseau WDM. Il est probable que la CV-QKD ait un avantage compétitif sur la DV QKD en ce qui concerne l'intégration à un réseau WDM grâce à sa détection cohérente. Une analyse prometteuse a été menée en [138], dans laquelle un système CV-QKD coexiste avec plusieurs canaux classiques dans un réseau WDM, mais il n'y a pas eu de démonstration expérimentale. Ceci conduit à s'interroger sur le fait que la CV-QKD soit plus performante que la DV QKD en termes de taux de clé et de distance, dans le cas d'une coexistence.

Dans cette thèse, nous avons étudié avec soin les différents effets optiques que l'on peut rencontrer dans l'architecture de coexistence de la QKD avec un réseau DWDM. De plus, nous avons démontré expérimentalement, pour la première fois, la faisabilité d'un système CV-QKD dans un réseau DWDM.

Partie II: Une attaque originale par canaux cachés visant les systèmes CV-QKD: attaque par saturation

Dans cette direction, j'ai proposé et étudié théoriquement une attaque par canaux cachés originale, visant les détecteurs en CV-QKD: l'attaque par saturation. Nous avons de plus démontré expérimentalement la faisabilité de cette attaque sur un système CV-QKD dans notre laboratoire.

L'attaque par canaux cachés est un problème vital pour les mises en œuvre pratiques de CV-QKD, car les preuves de sécurité ne prennent pas en compte toutes les imperfections expérimentales possibles. Par exemple, dans la mise en œuvre pratique de CV-QKD [66, 103], l'oscillateur local est transmis sur le réseau public sur la ligne optique reliant Alice et Bob, multiplexée avec le canal quantique. Ainsi, l'oscillateur local est accessible et être ainsi manipulé par un attaquant dans les mises en œuvre pratiques. Il est important de noter que l'oscillateur local peut en principe être généré localement chez Bob, comme cela a été démontré dans de récentes expériences démonstration des principes [139, 162], là où l'oscillateur local est verrouillé en phase avec les signaux quantiques émis par Alice. Toutefois, verrouiller en phase deux lasers distants provoque plus de complexité et de bruit et toutes les démonstrations pratiques complètes sur les CV-QKD ont jusqu'à présent été réalisées sur un oscillateur local "public". Ceci ouvre la porte à différentes stratégies d'attaque basées sur la manipulation d'oscillateur local. Un espion peut, par exemple, modifier plusieurs propriétés de l'impulsion de l'oscillateur local, telles que l'intensité, la longueur d'ondes ou la forme de l'impulsion [51, 56, 57, 66, 111, 112, 114]. L'écouteur clandestin peut, en particulier, fausser l'étalonnage du bruit de photon en manipulant l'intensité de l'oscillateur local ou son chevauchement avec le signal quantique. Nous avons en effet vu que l'excès de bruit est exprimé en unités de bruit de photon. Si le bruit de photon est surévalué alors que toutes les autres mesures demeurent identiques, l'excès de bruit dans l'unité de bruit de photon sera alors sous-évalué. Par conséquent Alice et Bob surévalueront alors leur taux de clé secrète, ce qui aboutira à un problème de sécurité.

Dans cette attaque par saturation, nous présentons une nouvelle faille et démontrons qu'elle peut être utilisée pour attaquer un système pratique CV-QKD mettant en œuvre un protocole d'état cohérent à modulation gaussienne (en anglais Gaussian-modulated coherent state ou GMCS) [50]. Au lieu d'attaquer l'oscillateur local, nous visons la détection homodyne située chez Bob, plus spécifiquement, la partie électronique de la détection homodyne. Dans les points suivants, nous nous attacherons à présenter brièvement l'analyse théorique et la démonstration expérimentale de l'attaque par saturation, ainsi qu'une nouvelle stratégie pour introduire une saturation du détecteur; nous évoquerons aussi les contre-mesures possibles pour répondre à une attaque par saturation.

2.1. La théorie de l'attaque par saturation

Principe de l'attaque par saturation Une hypothèse fondamentale dans les preuves de sécurité des systèmes CV-QKD est que la réponse de la détection homodyne est linéaire en ce qui concerne la quadrature d'entrée. Cette hypothèse est nécessaire car l'évaluation des paramètres suppose implicitement la linéarité de la mesure de quadrature de Bob par rapport à la valeur envoyée par Alice. Toutefois, cette supposition de linéarité ne tient pas si la détection homodyne de Bob est exploitée dans un régime non linéaire. Dans le cas d'un détecteur pratique, la zone de linéarité est limitée. Si la valeur de quadrature d'entrée est trop grande, la linéarité ne peut être vérifiée, ce qui aboutit à un comportement saturé.

D'après le modèle linéaire gaussien, évaluer les paramètres consiste à évaluer la matrice de covariance. La matrice de covariance est invariable quels que soient les changements linéaires. En effet, l'évaluation de la sécurité dans les systèmes CV-QKD repose uniquement sur l'évaluation de moments du second ordre (variance) de la quadrature, alors que les moments du premier ordre (valeur moyenne) ne sont pas contrôlés. Ceci offre à Ève une occasion de manipuler la valeur moyenne des quadratures. En conjuguant cela à l'exploitation de l'existence d'une zone de saturation du détecteur, une stratégie pour Ève pourrait consister à introduire activement un grand déplacement sur la quadrature reçue par Bob pour amener la détection homodyne à fonctionner dans sa région saturée. Comme la valeur moyenne de la sortie de détection homodyne est, par défaut, non contrôlée, Ève peut librement décider de déplacer la valeur moyenne. Ceci peut induire une réponse non linéaire sur le détecteur qu'elle contrôle. Cela permet à Ève d'influencer les résultats de mesures de Bob. L'évaluation des paramètres peut ainsi être faussée et la valeur des paramètres dépendra du déplacement, qui est activement contrôlé par Ève.

En résumé, voici notre idée d'une nouvelle attaque: en introduisant activement un déplacement sur les quadratures mesurées par Bob, Ève peut obliger le détecteur à fonctionner dans la zone saturée ce qui l'aidera à manipuler les résultats des mesures et ainsi l'évaluation des paramètres. Et, plus important encore, contrairement aux attaques dans lesquelles la mesure du bruit de photon est influencée, l'attaque par saturation ne fausse pas l'estimation du bruit de photon mais influence l'évaluation de l'excès de bruit.

Modèle linéaire gaussien et estimation des paramètres dans les CV-QKD Avant d'expliquer en quoi consiste l'attaque par saturation, nous allons tout d'abord brièvement évoquer le mode par canaux et l'évaluation des paramètres dans les CV-QKD, qui sont des éléments cruciaux pour l'étude de la sécurité pratique des systèmes CV-QKD. Dans les systèmes CV-QKD, il a été prouvé que, pour ce qui concerne les attaques individuelles [40, 47] ou collectives [38, 123] un attaquant (Ève) optimisait son attaque en menant une attaque gaussienne.

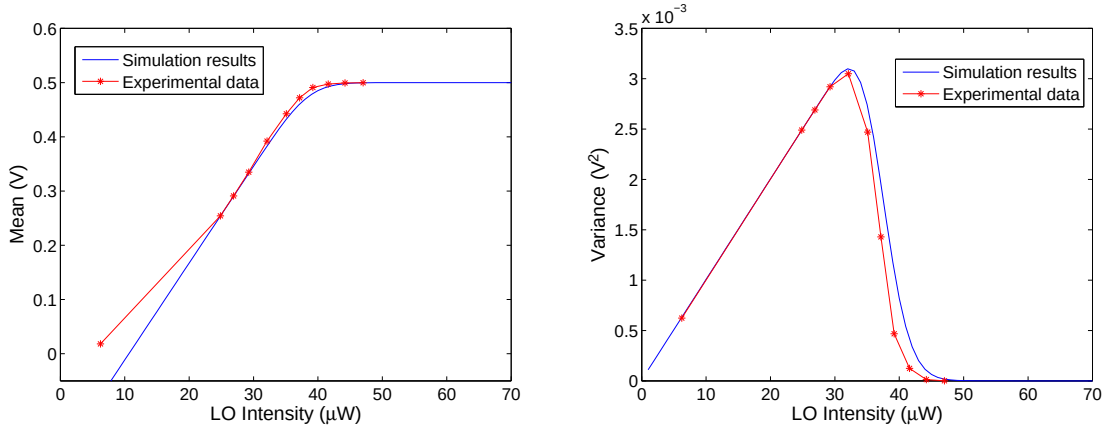
Nous pouvons donc supposer qu'Ève interagit sur un canal gaussien sur lequel Alice et Bob échangent leurs états quantiques. Grâce à l'optimalité de l'attaque gaussienne, le modèle de communication entre Alice et Bob dans les CV-QKD peut donc être caractérisé par le modèle linéaire gaussien et il peut être décrit par un canal à bruit blanc gaussien additif:

$$y = tx + z \tag{1}$$

Où, $t = \sqrt{\eta T}$, T est la transmission par canal et η correspond à l'efficacité de Bob. La modulation d'Alice suit la distribution gaussienne de telle sorte que x est une variable gaussienne aléatoire centrée sur zéro avec une variance donnée. La variable z est le bruit total qui suit une distribution normale centrée avec une variance inconnue. Cette variance comprend le bruit de photon, l'excès de bruit et le bruit électronique de Bob. Le canal linéaire gaussien est caractérisé par deux paramètres: la transmission par canal entre Alice et Bob et un facteur bruit connu comme l'excès de bruit. La transmission par canal a un lien avec la perte de canaux, elle peut être établie directement à partir de la corrélation entre les données d'Alice et de Bob. L'excès de bruit est la variance de bruit au-dessus du bruit de photon qui peut être dû à des imperfections des équipements (à savoir du modulateur, du détecteur, de l'électronique, etc.) ou aux actions d'Ève sur le canal. Des mesures des variances de Bob et d'Alice et de leur covariance sont nécessaires afin d'évaluer ces deux paramètres; une mesure du bruit de photon est aussi nécessaire. Alice et Bob peuvent alors calculer leur matrice de covariance en fonction de l'évaluation des paramètres et ainsi évaluer leurs taux de clé secrètes éventuels.

Saturation de la détection homodyne La mesure de la détection homodyne se fait par la soustraction de deux photocourants suivie par de l'électronique pour l'amplification et l'acquisition. En général, on considère que la portée de la détection linéaire de l'électronique d'acquisition est infinie. Cependant, dans un détecteur homodyne pratique, quelle que soit l'importance de la portée de la détection linéaire, elle ne peut être infinie. Nous proposons donc un modèle de saturation avec des limites supérieures et inférieures prédéfinies de la détection homodyne. Pour les valeurs situées entre ces deux limites, la réponse de la détection homodyne est normale, sinon la réponse est continuelle. Pour simplifier l'analyse, nous avons supposé, dans ce modèle, que la portée de la détection linéaire peut être décrite par un paramètre unique, α, intrinsèque au détecteur:

$$\begin{aligned} y &= \alpha, && tx + z + \Delta \geqslant \alpha \\ y &= tx + z + \Delta, && |\, tx + z + \Delta \,| < \alpha \\ y &= -\alpha, && tx + z + \Delta \leqslant -\alpha \end{aligned} \tag{2}$$



(a) (b)

Fig. 1 Caractérisation expérimentale du comportement à la saturation d'une détection homodyne pratique. (a) Moyenne de la sortie homodyne vs faible intensité. (b) Variance de la sortie homodyne vs faible Intensité.

Δ est défini comme un facteur de déplacement qui peut être introduit et contrôlé par Ève. De plus, nous avons confirmé de façon expérimentale la prédiction de ce modèle de saturation en observant la saturation de notre détection homodyne pour des intensités fortes et faibles. Nous avons mesuré les variances et les moyens de sortie homodyne pour différentes intensités faibles. Quand la détection homodyne n'est pas saturée, les sorties de détections homodyne (valeur moyenne et variance) varient de façon linéaire en ce qui concerne la faible intensité. Cependant, quand l'intensité de l'oscillateur local est relativement élevée, la réponse de la détection homodyne dépassera le seuil de saturation. La réponse de la détection homodyne est alors saturée et la variance mesurée chutera rapidement (Fig.1 (b)). Les résultats de la simulation du modèle de saturation correspondent parfaitement à nos données expérimentales (Fig.1 (a)(b)). Cela démontre que le modèle de saturation que nous avons proposé est réaliste et peut être encore utilisé pour interpréter notre attaque par saturation.

Le stratégie d'attaque par saturation Un projet de la stratégie de l'attaque par saturation est proposé à la Fig.2; il décrit les étapes suivantes:

1. Ève met en œuvre une attaque complète interception-réémission [104] au moyen d'une détection hétérodyne, elle peut obtenir des informations sur les deux quadratures envoyées par Alice, à savoir X et P.

2. Ève renvoie alors un état cohérent dont les quadratures se composent des résultats de ses mesures conjugués à un déplacement approprié des quadratures.

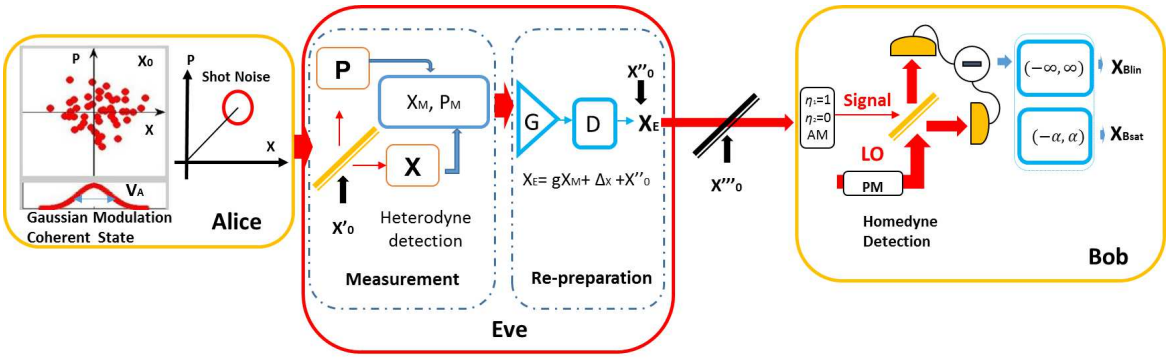
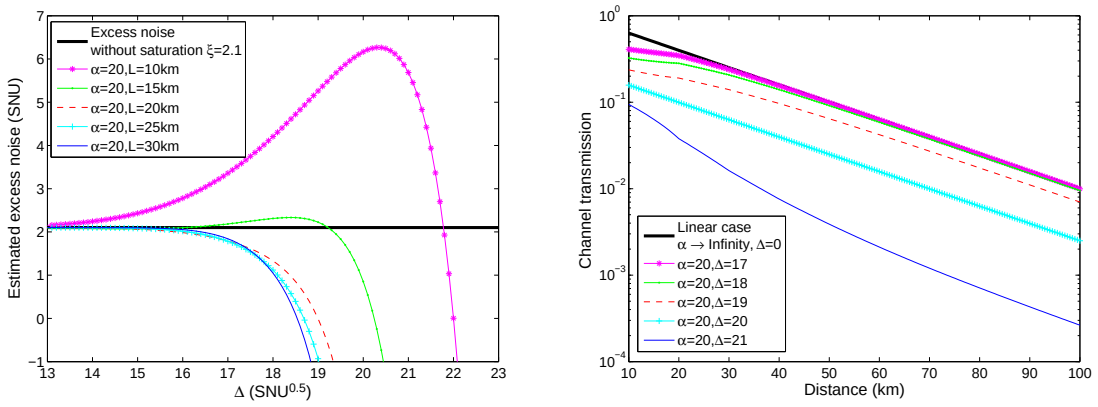


Fig. 2 Description générale des systèmes GMCS CV-QKD soumis à une attaque par saturation. Alice: prépare l'état cohérent avec les quadratures X et P; Ève: phase de mesure et de re-préparation, G: gain, D: déplacement; Bob: réalise la détection homodyne, AM: modulateur d'amplitude, η_1, η_2: coefficients de transmission des signaux, PM: modulateur de phase, $-\alpha, \alpha$: gamme de la linéarité.

3. Alice et Bob évalueront le taux de leur clé avec la détection homodyne saturée, où l'excès de bruit est en fait contrôlé par Ève. Ils sous-évalueront donc l'excès de bruit introduit par l'attaque complète interception-réémission et l'attaque d'Ève pourra rester couvert et lui donner un avantage sur Alice et Bob.

Analyse et résultats de la simulation Une attaque complète d'interception-réémission s'élèvera à deux unités de bruit de photon de l'excès de bruit [104] chez Alice, ce qui révélera la présence d'Ève. Toutefois, Ève peut contrôler la valeur moyenne du déplacement des quadratures qu'elle envoie ensuite à Bob. Elle peut ainsi introduire une saturation de la détection homodyne autant qu'elle le souhaite en changeant la valeur déplacée. Dès lors, Ève peut réduire les deux unités de bruit de photon de l'excès de bruit sur le canal Alice-Bob à une valeur arbitraire basse de l'excès de bruit évaluée par Alice et Bob. Cette attaque peut bien sûr affecter la quantité d'informations entre Alice et Bob et Bob et Ève. Ainsi, cette attaque influencera le taux de clé. Mais les résultats de notre simulation montrent qu'une attaque peut être couronnée de succès sur de très grandes distances. S'ils sont visés par une telle attaque, Alice et Bob peuvent être amenés à croire qu'ils ont des taux de 'clés sécurisées' positifs et accepter des clés qui sont, cependant, totalement non fiables. Cela montre qu'Ève peut voler avec succès des informations sans être détectée. Dans la simulation, comme nous pouvons le constater sur la Fig.3 (a), d'après le modèle linéaire, l'excès de bruit total estimé dans le cas d'une attaque complète interception-renvoi est de 2.1. Avec un tel excès de bruit, Alice et Bob ne peuvent déterminer aucun taux de clé. Toutefois, l'évaluation de l'excès de bruit peut être manipulée en changeant la valeur de déplacement. Sur la Fig.3 (a), pour ce qui concerne les longues distances (à savoir supérieures à 20 km)



(a) (b)

Fig. 3 (a) Excès de bruit $\hat{\xi}_{sat}$ (chez Alice) par rapport au déplacement Δ sur des distances différentes. (b) Transmission par canal quantique par rapport à la distance avec différents Δ. La variance d'Alice $V_A \in \{1,100\}$, l'efficacité de Bob $\eta = 0,55$, l'excès de bruit de l'électronique $v_{\text{ele}} = 0,015$, l'intégralité de l'excès de bruit dans un cas linéaire $\xi = 2,1$, efficacité de réconciliation $\beta = 0,95$, coefficient d'atténuation $a = 0,2dB/km$.

l'excès de bruit sous l'attaque par saturation $\hat{\xi}_{sat}$ diminue toujours alors que Δ augmente. Plus particulièrement, quand Δ est proche de α, $\hat{\xi}_{sat}$ est considérablement réduit. Pour ce qui concerne les distances courtes (à savoir inférieures à 20 km), quand Δ augmente, $\hat{\xi}_{sat}$ augmente d'abord puis diminue, mais $\hat{\xi}_{sat}$ peut toujours devenir arbitrairement petit quand Δ est assez grand. Et, plus important encore, nous pouvons observer à partir de la Fig.3 (a), qu'Ève peut obtenir une valeur arbitraire basse de $\hat{\xi}_{sat}$ en manipulant Δ quelle que soit la distance, ce qui montre qu'en cas d'attaque par saturation, la clé générée d'Alice et Bob a été détériorée.

Un inconvénient de l'attaque par saturation est que la transmission évaluée pour le canal est réduite. Sur la Fig.3 (b) nous déterminons la transmission évaluée pour le canal en échelle logarithmique par rapport à la distance, dans laquelle la courbe noire est la transmission évaluée par rapport à la distance en l'absence d'attaque alors que les autres courbes correspondent à la transmission évaluée dans le cas d'une attaque par saturation. Nous constatons que, la transmission évaluée peut être fortement réduite par rapport à la transmission effective en l'absence d'attaque.

2.2. Démonstration expérimentale de l'attaque par saturation

Nous avons pu démontrer cette attaque lors d'expériences, avec le support des résultats théoriques prometteurs de l'attaque par saturation. Nous avons réalisé une "Ève" fonc-

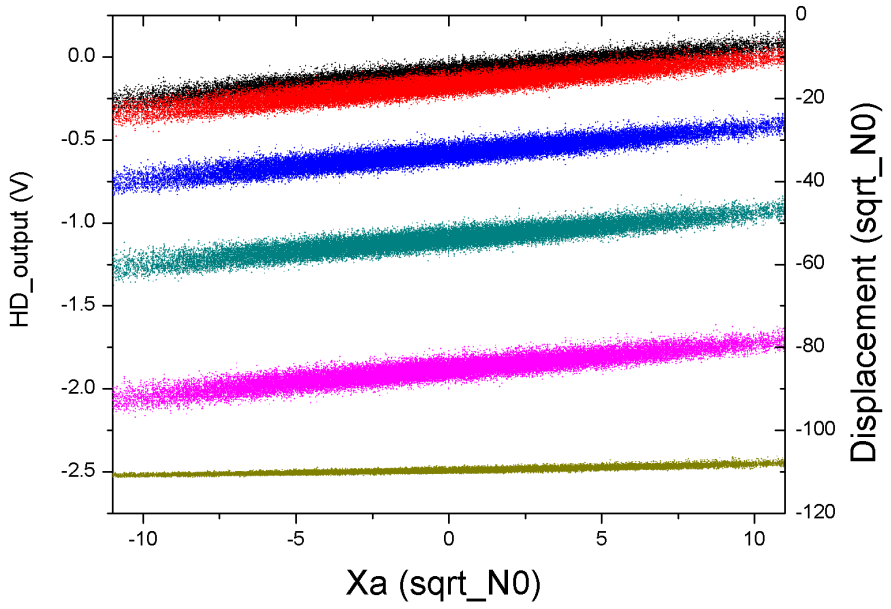


Fig. 4 Résultats expérimentaux: La distribution de X_B par rapport à X_A pour différentes valeurs de déplacement.

tionnelle pour mener l'attaque par saturation de façon expérimentale, dans laquelle l'étape principale consiste à préparer un déplacement précis et important. Plus particulièrement, pour pouvoir provoquer un déplacement contrôlé sur les données renvoyées par Ève, nous avons modifié l' "héritage" du système CV-QKD d'Alice en introduisant une boucle de Sagnac conjugué à un séparateur de faisceaux variable (VBS). Nous examinons la configuration avec un séparateur de faisceaux hautement transmetteur [128] pour provoquer un déplacement.

Avec notre système expérimental, nous effectuons plusieurs tests en changeant les valeurs de déplacement. Pour $V_A = 5$, nous augmentons progressivement la valeur de déplacement et la distribution expérimentale entre X_B et X_A est montrée sur la Fig.8.6. En raison de l'action de déplacement, nous pouvons observer que les distributions sont identiques dans la zone linéaire (0-2V) seules les valeurs moyennes sont différentes les unes des autres. Cependant, en raison de la portée de détection linéaire finie, quand $\Delta < -103,5\sqrt{N_0}$, la distribution se réduit quasiment à une ligne, ce qui révèle l'effet de saturation de notre détection homodyne. De plus, de façon expérimentale, avec une variance de modulation donnée d'Alice $V_A = 5$, nous modifions les valeurs de déplacement et de gain, puis mesurons l'excès de bruit et la transmission par canal par une procédure CV-QKD standard. Les résultats expérimentaux et ceux de la simulation sont montrés sur la Fig.4. Ainsi nous pouvons clairement constater

les évaluations de l'excès de bruit chutent sous les seuils correspondants de taux de clé nulle autour de la limite de saturation, ce qui prouve que notre attaque par saturation peut créer une lacune de sécurité. D'un autre côté, nous pouvons aussi prévoir l'évaluation de l'excès de bruit dans les simulations, et faire une comparaison avec les valeurs expérimentales. Comme l'indique la Fig.5, la prévision correspond au comportement de l'évaluation de l'excès de bruit que nous observons dans les expériences. Cela représente, cependant, un défi par rapport à notre système expérimental, car nous pouvons constater partir de la Fig.5 qu'il est difficile de contrôler avec précision le déplacement de sorte que l'évaluation de l'excès de bruit tombe exactement en-dessous du seuil de clé nulle mais toujours à une valeur positive.

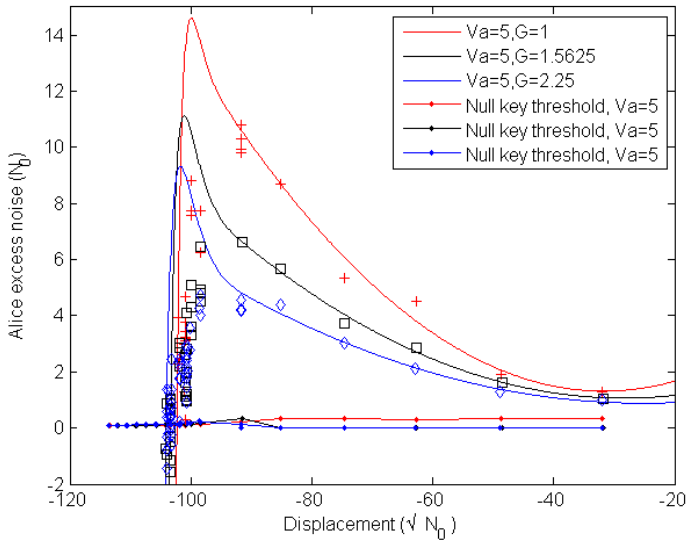


Fig. 5 Excès de bruit d'Alice par rapport au déplacement. Résultats expérimentaux: Symbole plus $G = 1$, carré $G = 1,5625$, diamant $G = 2,25$. Paramètres expérimentaux: variance d'Alice $V_A = 5$, Efficacité de Bob $\eta = 0,55$, excès de bruit de l'électronique $v_{\text{ele}} = 0,015$, limite de détection $\alpha_1 = -103,5$. Résultat de simulation: (1) Lignes continues sur couleur rouge, noire et bleue: évaluations de l'excès de bruit pour des paramètres donnés; (2) Lignes continues avec des pointillés: seuils de clé nulle pour des paramètres donnés; les simulations sont réalisées sur la base de modèle théoriquement, dans lequel les paramètres sont réglés même que paramètres expérimentaux.

Attaque par un laser extérieur Il est difficile de produire expérimentalement un déplacement cohérent directement dans le mode du signal quantique tout en conservant une bonne stabilité. Il est donc intéressant de chercher de nouvelles méthodes pour provoquer la saturation sur la détection homodyne à partir d'une autre approche ayant un système expérimental

plus simple. Pour cette raison, nous avons proposé une nouvelle stratégie d'attaque: nous provoquons un changement important de la mesure homodyne avec une lumière extérieure dans un mode différent du signal QKD.

Lors de cette nouvelle attaque, nous voulons tirer parti d'une autre imperfection de la détection homodyne pratique: La transmission/réflexion du séparateur de faisceaux 50/50 n'est pas exactement identique, ce qui aboutit à une petite fuite de l'oscillateur local sur la sortie de détection homodyne. Une telle fuite provoque un décalage des signaux homodynes et un bruit qui dépend de l'intensité de l'oscillateur local. Le décalage de la détection homodyne joue le rôle du terme de décalage du signal dans Eq.2. La soustraction de l'intensité de l'oscillateur local peut être améliorée en ajustant l'atténuation d'un chemin optique après le séparateur de faisceaux en présence de l'oscillateur local seul. Cependant, si l'on insère une autre impulsion ou une lumière à onde continue avec une intensité relativement forte dans le port signaux, l'équilibre est détruit à nouveau. De plus, la plupart des séparateurs de faisceaux ont des propriétés dépendant des longueurs d'ondes [56, 57, 112], donc la transmission du séparateur de faisceaux peut être faussée de manière significative selon la longueur d'onde de la lumière d'entrée. Dans ce sens, Ève peut contrôler la transmission du séparateur de faisceaux en sélectionnant la longueur d'ondes appropriée.

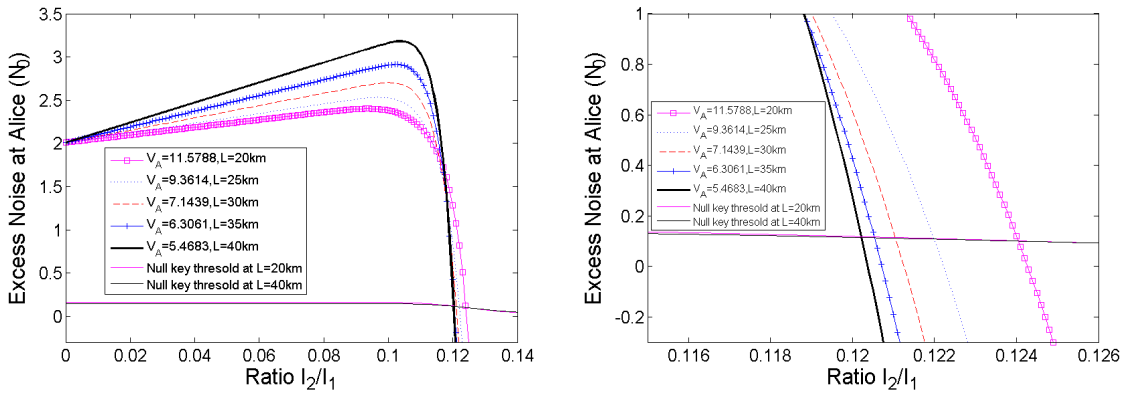
Une nouvelle stratégie d'attaque En prenant en considération les deux imperfections d'une détection homodyne: le déséquilibre d'un séparateur de faisceaux et la portée finie de la détection linéaire), nous pouvons formaliser une nouvelle stratégie d'attaque visant un système pratique CV-QKD:

1. Ève met en œuvre une attaque complète renvoi-attaque [104] (juste après Alice) en faisant une détection hétérodyne.

2. Ève insère un laser extérieur (impulsion ou onde continue) dans le port signaux de Bob, avec une longueur d'ondes différente du signal d'une QKD et une intensité librement choisie. Ainsi, l'intensité du laser extérieur ne peut pas être suffisamment soustraite par la détection homodyne de Bob ce qui provoque un déplacement sur le signal homodyne de Bob. Le laser extérieur provoque deux sortes de bruit: son propre bruit de photon dans un mode différent de faible intensité [112] et le bruit dû à la fluctuation de l'intensité [16].

3. En raison du déplacement à partir du laser extérieur, la détection homodyne de Bob est saturée. Par conséquent, l'évaluation de l'excès de bruit d'Alice et Bob peut être faussée vers une valeur arbitraire faible si Ève règle l'intensité du laser externe de façon appropriée.

Comme nous pouvons le prévoir, avec une détection homodyne linéaire, l'évaluation de l'excès de bruit total d'Alice et Bob se compose du bruit dû à l'attaque d'interception-réémission et au laser extérieur. Cependant, si le déplacement dû au laser extérieur est suffisamment grand, la sortie homodyne peut être saturée comme dans les attaques par saturation [140]. En fait, Ève contrôle activement la valeur de déplacement en sélectionnant les propriétés propres du laser extérieur. Par conséquent, l'action d'Ève peut fausser l'excès de bruit en excès estimé d'une attaque d'interception-réémission et le laser extérieur vers une valeur arbitrairement faible. Comme cela apparaît sur la Fig.6, pour une limite de détection $\alpha_1 = -\alpha_2 = 20$ et la transmission du séparateur de faisceaux $T_{bs} = 0,49$, l'excès de bruit estimé chez Alice varie avec l'intensité du laser extérieur, cela montre l'impact de l'action d' Ève sur l'estimation de l'excès de bruit. Pour une distance donnée, Ève peut choisir une intensité laser appropriée pour fausser l'estimation de l'excès de bruit jusque sous le seuil de clé nulle de sorte qu'Alice et Bob pensent toujours partager une clé sûre selon leurs paramètres d'estimation alors que les clés générées ne sont pas sûres du tout.



(a) (b)

Fig. 6 Estimation de l'excès de bruit à côté d'Alice par rapport au laser externe sur l'oscillateur local (nombre de photons par impulsion I_2/I_1). l'efficacité de Bob η=0,6, l'excès de bruit de l'électronique $V_{\text{ele}} = 0,01$. (a) Valeurs de I_2/I_1: de 0 à 0,14, (b) Valeurs de I_2/I_1: de 0,116 à 0,126.

2.3. Contre-mesure

Pour empêcher une telle attaque basée sur la saturation, de façon intuitive, Bob devrait éviter que la détection homodyne fonctionne dans une zone non linéaire ou saturée lorsqu'il fait des mesures. Bob peut donc tester toutes les données juste après l'acquisition des données et vérifier si les mesures de quadrature ont été acquises dans un régime linéaire. Pour

ce faire, Bob a besoin d'un étalonnage précis de la limite de détection homodyne $[-\alpha, \alpha]$. Le bloc complet qui comprend les données mesurées dans la zone de saturation serait totalement mis au rebut. D'après la post-sélection gaussienne [33], nous pouvons, de plus, traiter les données mesurées dans la zone linéaire et les transformer en entrée gaussienne dans laquelle la preuve de sécurité tient.

La deuxième contre-mesure est proposée par Kunz-Jacques and Jouguet [81]: Alice et Bob testent la linéarité entre le bruit et la mesure du signal en utilisant un procédé d'atténuation active chez Bob, à savoir un modulateur d'amplitude. En principe, la randomisation de l'atténuation des ports signaux peut empêcher Ève de fixer des valeurs propres de déplacement qui amènent la saturation du détecteur. Cependant, dans l'analyse, les auteurs considèrent un cas non réaliste dans lequel il n'y a pas de perte sur le canal entre Alice et Bob $T = 1$. Il n'apparaît pas clairement pourtant qu'un tel test de linéarité puisse aussi fonctionner dans le cas d'un canal ayant des pertes. Nous constatons donc, à partir de l'analyse précédente, que le comportement de l'estimation de l'excès de bruit est, de façon évidente, différente lorsque la distance change. D'un autre côté, un tel test linéaire augmente aussi la complexité de la mise en œuvre là où un modulateur d'amplitude supplémentaire et les paramètres d'estimation sont modifiés.

Comme l'attaque par saturation est une attaque par canaux cachés au moyen d'un détecteur, un "measurement device independent" (MDI) CV-QKD [95, 113] pourrait être une solution potentielle pour contrer de telles attaques. Les protocoles MDI CV QKD ne sont pas éloignés de la mise en œuvre. Très récemment, une preuve de principe de MDI CV-QKD a été réalisée [135].

Partie III: L'intégration d'un système de CV-QKD au sein des réseaux optiques DWDM

Dans cette direction, j'ai étudié attentivement les différentes sources de bruit qui peuvent être rencontrées lorsque l'on déploie un système CV-QKD en coexistence avec des canaux classiques intenses, au sein d'une architecture optique DWDM. Nous avons en outre démontré expérimentalement pour la première fois la faisabilité du déploiement d'un système CV-QKD dans un réseau optique DWDM.

Le multiplexage en longueur d'onde (Wavelength Division Multiplexing ou WDM) permet de partager une seule et même fibre pour transporter de multiples canaux optiques utilisant différentes longueurs d'onde. La compatibilité WDM des communications quantiques et classiques permettrait de déployer la QKD sur des fibres activées. Ceci augmenterait la compatibilité des communications quantiques avec les infrastructures optiques existantes et se traduirait par une amélioration notable en termes de rentabilité et de marchés potentiels pour la QKD.

Comparativement à la DV-QKD, la CV-QKD présente une meilleure tolérance au bruit lorsqu'elle est intégrée à un réseau WDM, grâce à sa détection cohérente. Seuls les photons dans le même mode spatio-temporel et de polarisation que le signal quantique contribueraient à l'excès de bruit, tandis que les photons émettant du bruit dans des modes différents seraient supprimés efficacement. On est parvenu à des résultats prometteurs dans l'analyse de [138], lorsque le bruit de diffusion Raman spontanée et des bruits d'émission spontanée amplifiée d'un amplificateur à fibre dopée à l'erbium (EDFA) sont examinés, dans un régime de coexistence du réseau WDM avec un système CV-QKD. Malheureusement, il n'y a pas de démonstrations expérimentales de ces travaux. Ainsi, il reste à savoir si la CV-QKD fonctionne mieux que la DV-QKD dans une architecture de coexistence avec un réseau WDM.

3.1. Excès de bruit induit sur la CV-QKD dans un réseau DWDM

Nous examinons un environnement de réseau optique relativement générique où le système CV-QKD pourrait être déployé: le système CV-QKD est multiplexé avec propagation avant (d'Alice vers Bob) et arrière (inverse) de canaux DWDM, en utilisant des composants passifs MUX et DEMUX. De plus, un amplificateur erbium est utilisé pour régénérer les canaux classiques vers l'avant. Comme cela a été analysé dans [138], les photons parasites ayant un impact sur le port de signal de la détection homodyne peuvent être ou non dans le même mode spatio-temporel que l'oscillateur local (OL). Comme l'oscillateur local contient 10^8 photons par mode, cela implique que le photocourant associé à un photon dans le mode de l'OL est supérieur de 80dB à un photon dans un autre mode, ce qui illustre la propriété de filtrage « intégré » associée à une détection cohérente. Comme cela a déjà été observé [15, 30, 132], la diffusion Raman spontanée est la source dominante de bruit pour la QKD dans un environnement DWDM, dès que la longueur de la fibre est supérieure à plusieurs kilomètres. Il s'agit d'un processus de diffusion inélastique pendant lequel les photons diffusés sont convertis en photons d'une longueur d'onde plus grande ou plus courte, appelés respectivement diffusion Stokes et Anti-Stokes. La diffusion Anti-Stokes est moins probable que la diffusion Stokes. Par conséquent, afin de minimiser la quantité de bruit due à la diffusion Raman, il est préférable de placer le canal quantique à une longueur d'onde plus courte que pour les canaux classiques. Nous supposerons que cette règle de conception a été suivie et que nous devons seulement nous concentrer sur l'effet des photons de la diffusion Raman Anti Stokes spontanée (SASRS) sur le système CV-QKD.

3.2. Démonstration de la coexistence de la CV-QKD avec des canaux classiques de DWDM intenses (DWDM)

Pour mesurer expérimentalement l'excès de bruit induit par les canaux DWDM multiplexés, nous avons inséré un système CV-QKD dans un banc d'essai DWDM et avons utilisé un système dédié à l'acquisition d'excès de bruit, en minimisant le bruit du système associé aux dérivées temporelles, de façon à ce que le bruit induit par le DWDM puisse se résoudre de façon assez précise. Nous commençons par une description de notre installation CV-QKD puis nous détaillerons le système d'acquisition.

CV-QKD: réalisation expérimentale Notre système CV-QKD met en œuvre le protocole GMCS [48] et utilise un laser DFB avec modulation externe à 1531.12 nm pour générer des impulsions d'une largeur temporelle de 50ns à un taux de répétition de 1MHz. Ces impulsions sont divisées sur un séparateur de faisceaux 90/10 dans l'oscillateur local et les impulsions de signal. Les impulsions de signal sont fortement atténuées (jusqu'à atteindre le niveau de quelques photons par impulsion) et leurs quadratures ont une modulation gaussienne, en utilisant des modulateurs d'amplitude et de phase, avec des variances de quadrature V_A. L'oscillateur local et le signal sont multiplexés dans le temps (retard de 200 ns) et multiplexés par polarisation avant d'être envoyés à Bob par le canal de fibre optique. A la réception, du côté de Bob, le signal et les impulsions de l'oscillateur local sont démultiplexés par polarisation et dans le temps. Une description détaillée de l'installation est donnée dans [64]. L'information de quadrature est récupérée grâce à un détecteur homodyne équilibré de bruit électronique -25dB en dessous du bruit de photon. L'intensité de l'oscillateur local est réglée pour obtenir un nombre moyen de 10^8 photons par impulsion chez Bob. La gamme de tensions d'entrée de la carte d'acquisition de données est réglée de façon suffisamment faible (± 1 Volts) pour obtenir une bonne résolution pour réaliser des mesures à la sortie du détecteur homodyne, ce qui réduit le bruit électronique à 0,3% du bruit de photon. Cependant, ce réglage pourrait permettre des attaques par saturation du système CV-QKD comme proposé récemment [140–142], mais nous n'examinerons pas cette question ici, ou toute autre question liée aux attaques par canaux cachés.

Pour réaliser des mesures du bruit de photon, Alice bloque les impulsions de signal à l'émission avec son modulateur d'amplitude, tandis qu'un deuxième modulateur d'amplitude placé sur le canal classique (en vert sur la Fig.7) est utilisé pour bloquer la sortie optique du canal classique multiplexé. Par ailleurs, lorsqu'à la fois les signaux quantiques et classiques sont multiplexés sur la même fibre, nous disons que la variance du "bruit total" est mesurée. Afin de limiter l'impact de la fluctuation statistique sur les estimations de variance [68], des fenêtres de taille 10^8 impulsion ont été utilisées pour estimer les variances des mesures des

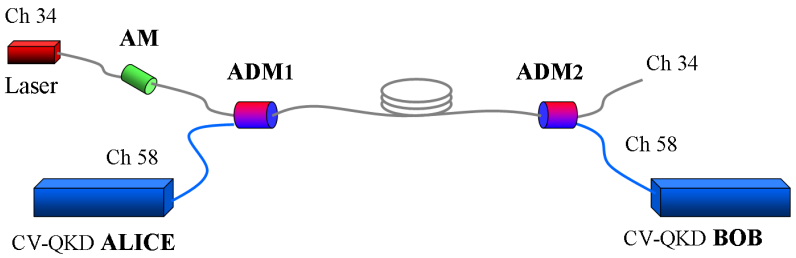


Fig. 7 Installation pour mesures d'excès de bruit pour système CV-QKD fonctionnant en coexistence avec un canal intense DWDM. Des modules d'insertion et d'extraction (ADM 1 et 2) sont utilisés pour insérer et extraire, respectivement, le canal quantique vers et à partir de la fibre optique. Un modulateur d'amplitude (AM) est utilisé pour déconnecter le canal classique, tandis que le signal de sortie d'Alice est bloqué de façon synchrone par le modulateur d'amplitude à l'intérieur du système CV-QKQ d'Alice. La figure représente l'installation avec un canal classique de propagation avant. Quand le canal classique fonctionne en configuration arrière, la sortie de l'AM est connectée à l'entrée d'ADM2 (au lieu de l'entrée d'ADM1).

quadratures à la fois pour le bruit de photon et le bruit total. Nous avons intégré l'installation CV-QKD décrite ci-dessus dans un environnement DWDM et l'installation expérimentale est décrite dans la Fig.7. Nous avons utilisé un laser continu à longueur d'onde accordable (modèle TLS-AG Yenista) pour le canal classique. La longueur d'onde du canal quantique est réglée à 1531.12 nm (canal de l'UIT 58) de façon à ce que le canal quantique soit en configuration Anti-Stockes par rapport à tout canal classique de la bande C [17]. La longueur d'onde du canal classique est réglée à 1550.12 nm (canal de l'UIT 34), en fonction du choix des ADM disponibles dans le laboratoire. Il serait possible de sélectionner une longueur d'onde du canal quantique proche du canal classique, comme illustré dans [30], de façon à minimiser encore le bruit Raman induit. Les deux canaux sont multiplexés et démultiplexés vers et à partir de la bobine de la fibre optique au moyen d'ADM. Un filtre passe-bande supplémentaire (n'apparait pas dans la Fig. 7) avait également été placé (avant l'ADM) sur le canal classique de façon à retirer les bandes latérales (un tel filtrage serait naturellement présent si un multiplexeur (MUX) multi-canaux avait été utilisé, comme cela apparaît sur la Fig.7).

Tests de coexistence expérimentale CV-QKD: résultats et analyse Nous avons fait fonctionner notre banc d'essai expérimental de CV-QKD multiplexé avec un canal classique DWDM à 25km, 50km et 75km à la puissance d'un canal classique après variation de l'ADM de 0mW à 8mW. Pour chaque essai expérimental, la transmission T et l'excès de bruit ξ ont été évalués à partir des données expérimentales. L'excès de bruit mesuré à

la sortie d'Alice comme fonction de la puissance classique apparaît sur la figure8. Nous comparons ces valeurs expérimentales à l'excès de bruit attendu, c'est-à-dire la somme de l'excès de bruit du système (étalonné à $0.03N_0$ dans notre cas, chez Alice) et du bruit associé à l'émission Raman spontanée, qui peut être calculée théoriquement [80, 138]. Nous nous attendons notamment à ce que l'excès de bruit soit une fonction linéaire de la puissance de lancement. Nous positionnons également les seuils de clé nulle sur la Fig.8, c'est-à-dire

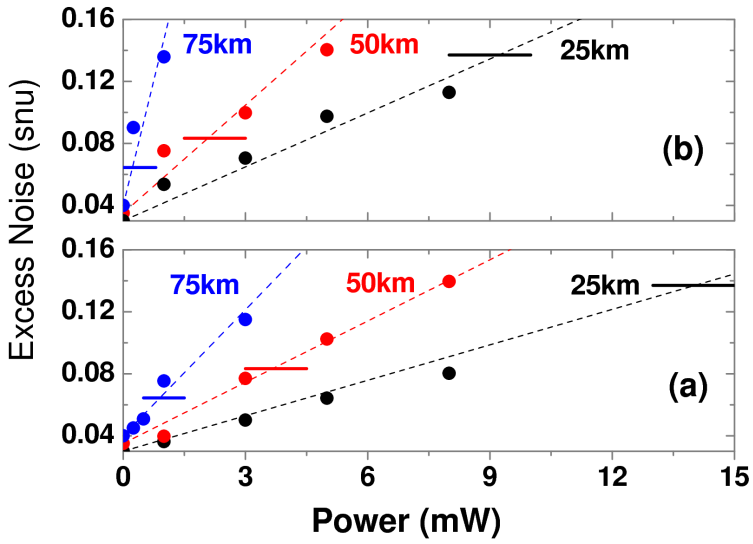


Fig. 8 Mesures de l'excès de bruit en configuration de canal vers l'avant (a) et vers l'arrière (b). Les points de données noirs, rouges et bleus sont l'excès de bruit évalués chez Alice pour une longueur de canal de 25km, 50km et 75km, pour différentes puissances de canal classique. Les lignes en pointillés indiquent la courbe d'excès du bruit attendu et les traits horizontaux pleins sont des seuils de clé nulle pour les distances de canal respectives. Voir texte pour détails.

l'excès de bruit maximum qui peut être toléré, afin de pouvoir obtenir un taux de clé secrète positif. Si l'on considère des attaques collectives et une efficacité de réconciliation de 0.95, le seuil de clé nulle pour 25km est $0{,}137N_0$, $0{,}083N_0$ pour 50km et 0,064 N_0 pour 75km. On observe donc qu'un taux de clé positif peut être obtenu pour une puissance de canal classique allant jusqu'à 14mW à 25km, 3,7mW à 50km et 0,89mW à 75km dans une configuration vers l'avant, tandis que la puissance classique admissible vers l'arrière chute à 9,3mW, 2mW et 0,23mW, respectivement. Le taux de clé de sécurité (en cas d'attaques collectives) a été calculé à partir de l'évaluation de l'excès de bruit ξ et de la transmission T en prenant en compte des effets limités sur la taille du bloc de données de 10^8. Nous nous sommes basés sur les pires estimations de l'excès de bruit (avec une déviation de 3 sigmas), en suivant l'analyse [68]. Avec un seul canal 0dBm à une distance de 25km, le taux de clé

est de 24,11kb/s vers l'avant et de 22,98kb/s vers l'arrière. Sur une longueur de canal de 50km, le taux de clé tombe à 3,16kb/s et à 2,27kb/s, respectivement. Nous avons également obtenu un taux de clé positif de 0,49kb/s à 75km en réduisant la puissance du canal classique (on considère que la sensibilité du récepteur du canal classique est inférieure à -25dBm) à -3dBm vers l'avant et à -9dBm vers l'arrière. Il est important de signaler le rendement (nombre de bits secrets par impulsion de signal QKD) du système CV-QKD dans un environnement WDM. Dans notre expérience avec un canal classique sur une distance de 25km, le rendement est de 485×10^{-4} bits/impulsion, ce qui est deux fois plus élevé que ce qui a été récemment rapporté, 485×10^{-6} bits/impulsion, expérience DV QKD [130]. Par contre, les systèmes DV QKD les plus récents peuvent fonctionner à une fréquence d'horloge de l'ordre du GHz, ce qui n'a toujours pas été démontré avec les systèmes CV-QKD, fonctionnant actuellement à une fréquence d'horloge exprimée en MHz, même si rien n'empêche fondamentalement de l'augmenter à 100 MHz, ou même au Ghz.

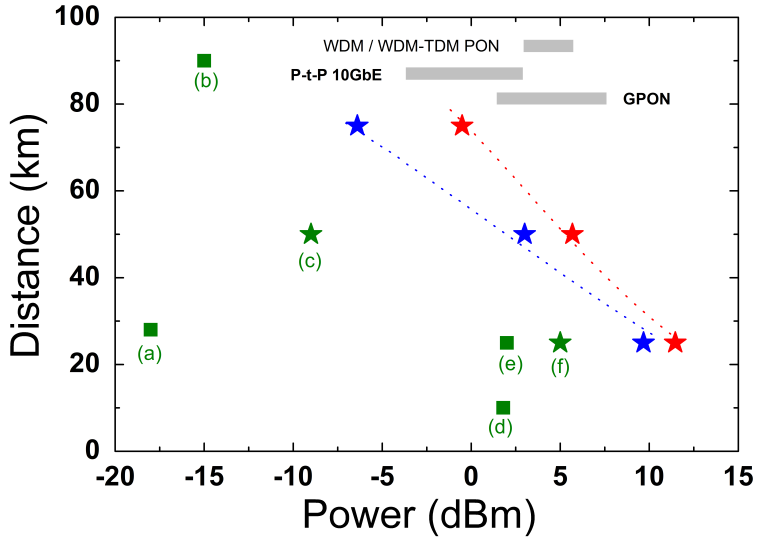


Fig. 9 Puissance de canal classique tolérable par rapport à la distance accessible : Performance de la QKD dans le contexte de coexistence avec des canaux optiques classiques. Les couleurs rouge et bleu représentent nos résultats avec un système CV-QKD, dans une configuration de canal classique vers l'avant et vers l'arrière, tandis que des travaux réalisés auparavant avec les systèmes DV-QKD sont en vert: (a) Townsend [173], (b) Patel et al. [129], (c) Eraerds et al. [30], (d) Choi et al. [17], (e) Chapuran et al. [15], (f) Patel et al. [130]. Étoiles: expériences faites dans la bande C (DWDM). Carrés: expériences faites en CWDM. Les lignes en pointillés rouges et bleus sont la courbe de simulation avant et arrière pour le taux de clé nul dans l'expérience en cours. Les bandes grises montrent la gamme de tensions d'entrée de l'émetteur dans différent réseaux optiques standardisés.

3.3. Comparaison avec la DV-QKD

Pour illustrer la grande capacité de coexistence DWDM de la CV-QKD, nous avons réalisé une étude comparative par rapport à des expériences précédentes sur la DV-QKD [15, 17, 30, 129, 130, 173], et nous avons montré dans la Fig.9 une comparaison de la distance accessible de la QKD, comme fonction de la puissance multiplexée classique (en CWDM ou DWDM, voir légende). Dans la Fig.9, les points de données pour la CV-QKD indiquent la distance maximum accessible (seuil de taux de clé nulle). Les taux de clé correspondent à des points expérimentaux pris sur notre système CV-QKD et affichés sur la Fig.9 sont: 12b/s pour 25km; 8b/s pour 50km et 9b/s pour 75km. Il faut remarquer que les résultats DV-QKD mentionnés dans la Fig.9 ont aussi été acquis lorsqu'on était tout près du seuil de clé nulle. Il est important de noter que les différents résultats mentionnés dans cette comparaison ne reposent pas tous sur une analyse de sécurité unifiée. Les taux de clé sont liés à des raisons de sécurité contre des attaques collectives dans[17, 30, 130], attaques individuelles dans [173] et des attaques générales dans [129], tandis que parmi ces références, seulement [130] prend en compte des effets limités. Comme cela a été expliqué précédemment, nous avons pris en considération les attaques collectives et les effets de clé de taille finie en compte pour les raisons de sécurité pour les dérivations de clé CV-QKD associées à nos expériences.

On observe que la CV-QKD peut atteindre de plus grandes distances de transmission pour une puissance de lancement d'un canal classique donnée. Par contre, pour une distance de transmission donnée, la CV-QKD peut tolérer du bruit venant de multiples canaux classiques avec une puissance de transmission caractéristique de 0dBm. Ceci est particulièrement vrai pour les distances de transmission de 25 et 50km, comme illustré sur la Fig.9. La CV-QKD peut aussi être déployée en coexistence avec des canaux classiques avec des niveaux de puissance inédits – grâce à la propriété de sélection de mode de sa détection cohérente. Cela facilite l'intégration de la CV-QKD dans différentes architectures de réseaux optiques et, en particulier, dans des réseaux d'accès. Cette intégration requiert, en général, que la QKD soit capable de coexister avec des canaux classiques de plusieurs dBm de puissance. Comme on peut le voir sur la Fig. 9, une bonne co-existence de la CV-QKD permettrait son intégration dans différents réseaux optiques passifs standards comme, par exemple, Gigabit PON, 10G-PON et WDM/TDM PON [7].

Optimisation de l'affectation de canaux classiques A la lumière des résultats expérimentaux et des perspectives prometteuses pour l'intégration de la CV-QKD dans les réseaux optiques, nous avons simulé une intégration réussie de la CV-QKD dans certaines architectures de réseaux optiques passifs WDM (WDM-PON). A cet effet, nous avons appliqué

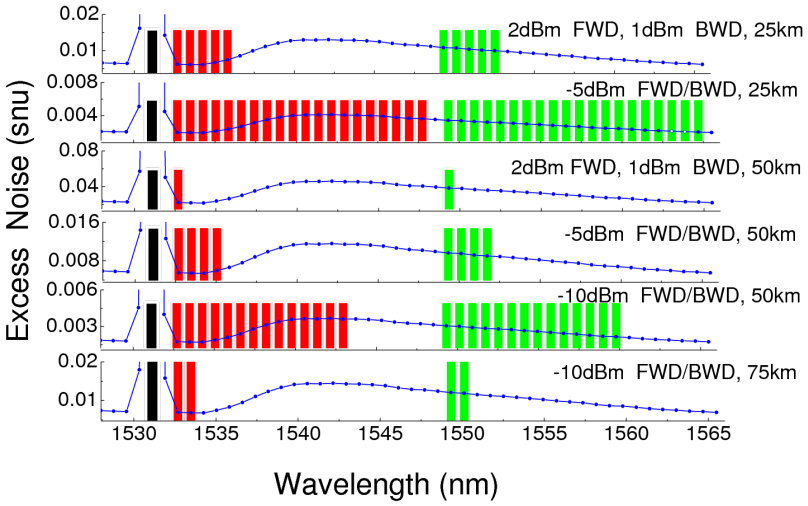


Fig. 10 attribution des canaux classiques optimisée pour la CV-QKD dans le WDM-PON. En noir: le canal 1531.12 nm attribué au canal quantique. Les rayures rouges et vertes représentent les canaux classiques de retour et d'aller, positionnés sur la grille de longueurs d'onde DWDM. Chaque point bleu (relié par la ligne bleue) représente la valeur simulée de l'excès de bruit induit par la diffusion Raman résultant (d'une puissance précisée) d'un canal classique de retour vers le canal quantique. Les données simulées pour l'excès de bruit émanant des canaux d'aller ne figurent pas.

un programme simple d'optimisation pour l'intégration du système CV-QKD dans WDM-PON, ce qui nous a permis de proposer des attributions de canal classique en minimisant l'excès de bruit induit sur la CV-QKD.

Pour une distance de réseau d'accès typique de 25km, nous avons envisagé l'attribution de canaux classiques dans la bande C et il s'est avéré que la CV-QKD pouvait coexister avec 5 paires de canaux classiques (avec une puissance de lancement nominale WDM-PON: 2dBm pour l'aller et 1dBm pour le retour). L'optimisation (à une distance de transmission donnée) se fait en choisissant de façon séquentielle la position du canal classique qui maximise l'excès de bruit supplémentaire sur la QKD, jusqu'à atteindre le nombre maximum de canaux compatibles avec un taux de clé secrète positif.

Si la sensibilité du détecteur sur les canaux classiques le permet, il est même réaliste de penser que l'on peut réduire la puissance du canal classique en dessous des spécifications nominales d'un réseau WDM-PON, tout en continuant de faire fonctionner les canaux classiques. Nous avons étudié l'impact de cette hypothèse dans la Fig.10. Nous pouvons voir, par exemple, que 14 paires de canaux (chacune avec une puissance de lancement de 10dBm) pourraient être multiplexées avec un canal CV-QKD à 50km et tandis que 2 paires de canaux (puissance de lancement également de 10dBm) pourraient coexister avec la CV-

QKD sur 75km. Les résultats de cette simulation indiquent clairement que la grande capacité de coexistence de la CV-QKD avec des canaux classiques multiplexés WDM jouera probablement un rôle important dans l'intégration de la QKD dans les réseaux optiques.

3.4. Conclusion

Le succès des technologies émergentes des réseaux de fibres optiques dépend en grande partie de leur capacité à s'intégrer totalement dans les infrastructures existantes. Nous avons démontré la grande capacité de coexistence de la CV-QKD intense (environ 0 dBm) avec des canaux classiques, dans une configuration DWDM. Nous avons caractérisé et étudié l'influence de la source principale de bruit: la diffusion Raman. Nous avons aussi prouvé par nos expériences que la CV-QKD peut coexister avec une intensité de canaux DWDM atteignant 11,5dBm, tandis qu'un taux de clé positif pourrait aussi être obtenu avec un canal classique multiplexé DWDM de 3dBm avec propagation avant sur une distance de 75 km. Il ressort également que la CV-QKD, qui bénéficie d'un filtrage intégré monomode (associé à la détection cohérente) est moins impactée par le bruit des photons induit par le DWDM que les systèmes DV-QKD testés jusqu'à présent et peut par conséquent atteindre des distances de transmission plus grandes pour une puissance donnée de lancement de canal classique DWDM. Les résultats de ces expériences indiquent que la CV-QKD, et plus généralement les communications cohérentes fonctionnant à la limite du bruit de photon, sont une technologie prometteuse permettant d'utiliser en même temps communications quantiques et classiques sur le même réseau de fibres optiques, et pouvant de ce fait jouer un rôle important pour le développement des communications quantiques sur les réseaux de fibres optiques déjà existants.

Chapter 1

Introduction

1.1 Background

1.1.1 Classical cryptography

The need for encryption

In the age of Internet, digital communication brings great convenience to people's lives. With the increase of Internet traffic, secure communication becomes more and more important, any message without encryption can be potentially accessed by an eavesdropper. In a secure communication, a secret message is transmitted from a sender called Alice to a receiver called Bob, where an eavesdropper called Eve should not have any access to the secret message if the communication is secure. In order to achieve secure communication, cryptography can be used to perform encryption, which now plays an important role in the digital world. In modern cryptography, there are mainly two types of cryptographic protocols: *symmetric-key* cryptography and *asymmetric-key* cryptography.

In symmetric-key cryptography, Alice uses a private key to encrypt her message while Bob uses the same key to decrypt the message sent by Alice. It thus requires two parties to share a secret key and to keep it private between them during the encryption and decryption. By contrast, asymmetric-key cryptography, also known as public-key cryptography, uses a public key to encrypt the message on Alice side, while Bob uses a private key to decrypt the message. The public key is publicly distributed (everyone can access it), while the private key is kept secret and only known to Bob.

It is proven that one particular symmetric-key encryption protocol, called the one-time pad (OTP) protocol (also known as Vernam cipher [175]) is unconditionally secure [157]. The unconditional security of encryption means that Eve cannot learn anything about the

message while no assumption need to be made on her computing capabilities. In the OTP protocol, the message and the key are both in the form of a binary string while the length of the key is equal to the length of the message. For encryption, a bitwise exclusive OR (XOR) is performed on the bits of the message and the key to generate a ciphertext. Decryption is done by performing a bitwise XOR between the bits of the ciphertext and the key.

The key distribution problem

In order to achieve the information-theoretically security in the implementations of OTP protocol, there are several requirements. In particular, Alice and Bob need to share an identical secret keys that must be truly random whose length must be at least the same as the message, moreover key can not be reused. These requirements could be difficult to achieve, first, true random numbers seem to be impossible to generate by means of classical physical process due to the deterministic nature of classical physics. Second, the use of OTP protocol requires large resources of secret key to be distributed if the message to be encrypted is very long and secret key cannot be established over an insecure channel. This is known as the key distribution problem. Traditionally, trusted couriers seem to be the only candidate to solve the key distribution problem, however key are costly and inefficient. For these reasons, OTP is only used when one requires very high level of security. On the other hand, other symmetric-key cryptography protocols such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES) only need small amount of secret keys to encrypt large amount of data, which are now widely used to secure communications. However these techniques still can not fully solve the key distribution problem and do not provide unconditional security.

Computational security

With the increase of information that need to be encrypted, public-key cryptography has become more popular and is widely deployed in cryptographic system nowadays. It is mainly because public-key cryptography provides a practical solution to the key distribution problem compared to symmetric-key cryptography, where Alice encrypts data with a public key that is known by everyone and Bob decrypts data with a private key that is only known by himself. The security of the public-key cryptography relies on the unproven mathematical assumption that there exists one way functions that are easy to compute but difficult to invert. For example, concerning the widely used RSA [151] protocol, its security is based on the assumption that it is difficult to factor large integers. However, such assumption has not been proven yet, it is still possible that one finds high efficient algorithms to factor large

numbers and break the security of RSA. In fact, in the field of the quantum computing, it has been shown that Shor's algorithm [160] can efficiently factor a large number. It means that if a large quantum computer is ever built, most of the classical public-key schemes, such as the RSA protocol, will be broken easily. Although large scale quantum computers are still far away, possible eavesdroppers can still record the communication today and crack the information in the future when quantum computer will be available. On the other hand, even with today's technologies, the increase computational power of current supercomputers is also a threat on the security of public-key cryptography. As an example, factorization of a 768-bit RSA modulus [73] has been successfully demonstrated recently.

As we have seen, the security of classical cryptography often relies on some unproven computational power assumptions, which means that advances in hardware or algorithms could potentially alter the security. Computational assumption can be seen as a potential vulnerability for today's classical cryptography. If one indeed requires high level security of communication, then one may not want to take any risk that the assumption can be broken, leading to a security break.

1.1.2 Quantum key distribution

In fact, the key distribution problem can be potentially solved by one of the most promising applications in quantum information technology: Quantum Key Distribution (QKD). In contrast to computationally secure algorithms, QKD can be proven secure independently of the computational power of an eavesdropper. The security of QKD is based on the fundamental laws of quantum mechanics, in particular the quantum no-cloning theorem: one cannot copy an unknown quantum state perfectly. The closely related Heisenberg's uncertainty principle links the disturbance of Alice's and Bob's observed signals to the information that may have leaked to Eve. The disturbance of Alice and Bob's signal increases with the information that Eve has access to. Alice and Bob can randomly choose a fraction of their data to estimate such disturbance and bound the information accessible to Eve. The corresponding leaked information of Eve can then be eliminated in the final key shared by Alice and Bob through the privacy amplification methods. The generated secret key of QKD can be used to perform OTP encryption, providing method to achieve secure communication over a link (classical authenticated channel and public quantum channel) with unconditional security.

Brief outlook on QKD development

The first and best known QKD protocol is called BB84 [11], which was introduced by Bennett and Brassard in 1984. This protocol relies on encoding discrete information (bits)

onto phase or polarization of single photon states and the bit value is measured at reception with phase or polarization analysers followed by single photon detectors. It is therefore called a discrete-variable (DV) QKD protocol. After BB84 had been invented, several QKD protocols have been proposed [44, 154] and QKD has developed dramatically both at the theoretical and experimental level over the past two decades. On the theoretical side, a number of security proofs have been rigorously established to prove the information theoretic security of QKD [154]. On the experimental side, the key distribution distance of QKD has reached more than 300 km over a optical fiber link in laboratory [76] and 144 km over free space [156]. Secret key generation rates over 1 Mbits/s have also been reached [27]. Moreover, the applications of QKD have been expanded to network. Metropolitan size QKD networks have been demonstrated in [131, 153]. Recently, QKD network which was reported in [177], not only served for scientific purposes but also to protect real communications for military or financial institutions.

In this thesis, rather than studying the DV QKD protocols such as BB84, I focus on an alternative approach of QKD, the so called continuous-variable (CV) QKD. CV QKD encodes real numbers over the continuous variable degree of freedom of the electro-magnetic field, the field quadratures, that can be measured by using a homodyne detection instead of single photon detectors. The most established CV QKD protocol is GG02 [48] which was proposed by Grosshans and Grangier in 2002. GG02 protocol only requires standard optical telecom components for the preparation and detection of coherent states. Compared to DV QKD, CV QKD is still at an earlier stage in both theories and experiments. In recent years, remarkable achievements have however been made in these two directions. In theory, security proof of Gaussian protocols against collective [38, 123] and arbitrary attacks [92, 147] have been already established, recent work also shows progress in composable security proof [86]. On the experimental side, several demonstrations of CV QKD have been performed with fiber systems [25, 34, 64, 68, 103, 137], and it has been demonstrated recently that CV QKD can reach 80 km over a fiber link in laboratory [68].

Prospects for QKD

Thanks to the efforts made by the researchers over the past two decades, QKD is now mature enough to be implemented in real world for secure communication. For both DV and CV approaches, commercial products have been released on the market. For DV QKD, important actors are companies such as ID Quantique [3], MagiQ Technologies Inc., Austrian Institute of Technology [1], Anhui Quantum Communication Technology Co., Ltd.[2] while for CV QKD SeQureNet [5] and Quintessence Labs [4] have pushed the technology up to commercialization. With the great need of high level secure communication, QKD

could potentially play an important role in the future secure communication infrastructure. It is expected that the global market of QKD would reach over 1 billion US dollar in 2018 [60].

1.2 Motivations for our work

As QKD is put in use to ensure secure communication in the real world, it is critical to verify their practical security and performance, especially for commercial system implementations. QKD users are actually interested in the actual security and the performances that QKD systems can provide rather than the theoretical security which has been claimed. Practical security of QKD is an important topic which has been actively studied over the recent years in the QKD community. There are two important directions in the practical study of QKD: (1) *quantum hacking* (or *side channel attacks*) on practical QKD systems; (2)integration of QKD systems within a optical network. In this thesis I focus on these two aspects in particular with the implementations of CV QKD protocols.

1.2.1 Side channel attacks in CV QKD system

The concept of side channel attack comes from classical cryptography, where a side channel attack aims on gaining information from a physical implementation of a crypto-system, instead of performing brute force attack or looking for theoretical weaknesses in the cryptographic algorithms. Valuable information can leak from various *side channels*, such as power consumption, electromagnetic or any kind of physical signals that can be emitted from a crypto-system. Side channel attacks usually target the way a cryptographic protocol is implemented, rather than the protocol itself.

Practical QKD systems also face the challenge of side channel attacks. The unconditional security of QKD strongly relies on the validity of assumptions on the QKD devices. However these assumptions can not be always met in actual implementations, since real devices always have some imperfections that could lead them to behave quite differently from the mathematical models described in the security proof. Certain imperfections may lead to loopholes, enabling an eavesdropper to launch attacks capable of compromising its security. Note that the existence of side channel attacks does not contradict the existence of security proofs in QKD, since side channel attacks are not originally covered by security proofs.

In fact, side channel attacks on DV QKD have been studied through the past years and become a hot topic in QKD research. Various quantum hacking strategies have been proposed, in which, single photon detectors of Bob are often considered as the targets, for

example, time shift attack [137, 194], blinding attack [42, 116], after gate attack [185], detector dead time attack [184] and so on. Some of these attacks have been also demonstrated experimentally [42, 107, 190] including a full field implementation of a perfect eavesdropper [42]. Other attacks aiming on different devices have also been proposed to compromise the practical security of DV QKD systems [43, 93, 168, 190].

CV QKD is also not immune to the problem of side channel attacks. One of the most important security issues in the implementations of CV QKD concerns a classical phase reference, the local oscillator (LO), which is commonly transfered publicly on the channel between Alice and Bob. LO signal does not carry any information but is a phase reference for the homodyne measurement and its characteristics are closely related to the parameters in the calibration of a CV QKD system, and in particular shot noise calibration. Indeed, based on the manipulation of LO signal, shot noise calibration attack have been proposed to compromise the practical security of CV QKD systems [32, 51, 66, 111]. Possible countermeasure against LO related attacks have however been later proposed: (1) Monitoring LO signal and shot noise in real time [66]. (2) By using phase locking technique, Alice and Bob can locally generate LO signal rather than sending it from one side to another through a open channel [139, 162].

In order to close the gap between the theoretical security and the practical security of DV or CV QKD, in particular, to resolve the threats of side channel attacks on QKD, two main approaches are considered: (1) Develop *device independent* (DI) QKD protocol [6]. (2) Address as many as side channels in implementations of QKD systems, and develop corresponding countermeasures. The first approach, DI QKD has a potential to remove the assumptions that needs to be applied to the devices in QKD implementation. DI QKD provides a beautiful solution in theory to counter against side channel attack, however it is not a practical solution regarding to the level of current technology. It turns out that even for near-unity detection efficiency, DI QKD can only generate a very low key rate [23, 45]. Another fact that makes DI QKD protocols less realistic is that they involve a loophole-free Bell test which has not been experimentally demonstrated so far. In fact, an alternative approach called *measurement device independent* (MDI) QKD [100] has reached some fruitful results in recent years. MDI QKD can remove any side channel attacks aiming one side of a QKD system in particular the part with the detectors. MDI QKD protocols have been implemented by several groups and have shown some promising results in terms of key rate and distance [98, 152, 169, 170]. All these works concerning MDI are focused on DV QKD protocols. The development of MDI protocols in CV QKD domain is relatively slow. An noticeable reason is that before this thesis, there had been no security loopholes related to the detector reported for CV QKD protocols. Nevertheless, MDI CV QKD protocols

with coherent states [95, 113] and with squeezed states[94, 193] have been proposed in the recent years. However according to theoretical analysis and present technology level, they are still far from practical implementations. The study of device independent is beyond the reach of this thesis, instead, I have pursued a different approach, studying and analyzing various side channels that could compromise the security of practical and existing CV QKD implementations. Realistically, it is impossible to find all the side channel that would appear in actual implementation. However I can still study what matters most for the practical security and classify different types of side channel attacks. Indeed, from the experience of known side channel attacks in QKD, once a specific loophole is found, the protection is usually not too hard to realize and usually all the side channel attacks related to a specific loophole can be eliminated thanks to a single countermeasure. For example, once LO signal can be locally produced on Alice and Bob side [139, 162], CV QKD system are immune to all the LO based attacks [51, 66, 111]. Therefore side channel analysis would eventually improve the practical security of CV QKD systems and pave the way toward QKD security certification.

In this thesis, I have studied different imperfections in implementations of CV QKD and analyzed their impacts on the security and performance. I have also discovered and studied a new security loophole that can lead to a new type of side channel attack in a CV QKD system: saturation attack.

1.2.2 Integration of CV QKD within optical networks

An appealing advantage of QKD is that it is compatible with current optical network. In this thesis, study of the integration of CV QKD system with optical network is another topic. With the development of QKD, QKD can be extended from a point-to-point application to a network configuration [131, 153]. Meanwhile, Wavelength Division Multiplexing (WDM) allows multiple optical channels, at different wavelengths, to share a single optical fiber. It would be appealing for QKD to be conducted through the existing optical fiber network together with classical signals.

The first coexistence architecture of WDM technology with QKD was proposed by Townsend [173]. In recent years, the feasibility of QKD coexistence with a WDM network has been studied and demonstrated [15, 17, 30, 126, 132]. These studies have shown that the noise induced by strong classical signals could prevent QKD communications, because the optical power of the classical channels is typically many orders of magnitude higher than the quantum signal of QKD. Especially, in case of coexistence with *Dense Wavelength Division Multiplexing* (DWDM) channels, where the wavelength difference between quantum signal and classical signal is very small (0.8 nm channel spacing). Various additional noise

due to insufficient isolation and optical non-linear effects of classical signals can impact on quantum communication which may finally result in a null key rate for QKD. Coexistence with intense classical channels is indeed a practical challenge for QKD.

Most of the studies and demonstrations are limited on DV QKD systems. In contrast, only few studies [138] have been done on the integration of a CV QKD system within a WDM network. CV QKD may have a competitive edge over DV QKD for the integration with WDM network thanks to its coherent detection. A promising analysis has been conducted in [138], where a CV QKD system coexists with several classical channels in a WDM network, however there is no experimental demonstration. This opens the question that whether CV QKD could perform better than DV QKD, in terms of key rate and distance, in a real coexistence implementation.

In thesis, we have studied carefully the different optical effects that can be encountered in the coexistence architecture of CV QKD with a DWDM network. Moreover, we have demonstrated experimentally for the first time the feasibility of a CV QKD system in a DWDM network.

1.3 Outline

- In Chapter 2, the basic elements of continuous variable quantum information theory are presented. These elements are necessary to understand quantum key distribution with continuous variables.

- In Chapter 3, we present general principles and the developments of QKD.

- In Chapter 4, several CV QKD protocols and their implementations are presented. We also briefly present the security proofs of CV QKD.

- In Chapter 5, various imperfections of a practical CV QKD implementation are studied, in which, I mainly focus on studying the imperfections of Bob's device.

- In Chapter 6, we review known side channel attacks in CV QKD system. This chapter is mainly based on [56–58, 66, 72, 111, 112, 165].

- In Chapter 7, we report a newly discovered side channel attack in CV QKD: saturation attack. This attack explores the loophole related to the imperfect linearity of the homodyne detection. We show that for practical realistic parameters, the saturation attack can lead to a full security break.

- In Chapter 8, based on the theoretical study conducted in the previous chapter, we experimentally have demonstrated the saturation attack. We have first prosed a modified strategy which is experimentally realizable. We have analyzed the experimental results and deduced the condition under which a successful attack is possible. We moreover report a new attack strategy to induce detector saturation by inserting an external light and show that it can also lead to a security break.

- In Chapter 9, we study and experimentally demonstrate the coexistence of a CV QKD system with several intense classical channels in a DWDM network.

1.4 Detailed list of contributions

I list my contributions in this thesis below and indicate their corresponding chapters at the end.

1. I have analyzed various imperfections in a practical homodyne detection and included them in an original mathematical model. I have moreover demonstrated a deconvolution method in simulation, that can potentially be useful to improve CV QKD performance when the system is running at a repetition rate higher than the homodyne detection bandwidth.

2. I have experimentally observed the saturation effects on a shot noise limited homodyne detection: the output voltage is not linear with the optical quadrature input. I have moreover identified the sources of saturation and developed several theoretical models to describe our homodyne detection by taking saturation effect into account.

3. By exploiting the saturation effect, I have proposed a new side channel attack in CV QKD: saturation attack [140, 141]. I have studied theoretically this saturation attack and shown that it can lead to a full security break. For the first time, I have demonstrated a detector-based side channel attack in CV QKD, which opens a new type of loopholes in all implementations of CV QKD systems. This new loophole has no connection with the well known vulnerability of LO pulses in the implementation, which thus requires new types of countermeasures.

4. By using a proper detector model that correctly describes the behavior of our homodyne detection, I have optimized Eve's attack parameters under two possible criteria so that a successful saturation attack can be achieved.

5. I have proposed a saturation attack strategy, which is suitable for experimental demonstration. In collaboration with other researchers in our team, we have experimentally realized a functional "Eve", capable of actively performing a controlled displacement of the quadratures in order to induce saturation of the homodyne detection.

6. We have performed an experimental demonstration of saturation attack based on the proposed strategy. We have experimentally studied the relation between Eve parameters and Alice-Bob channel parameter estimation results. Furthermore, I have deduced the condition (Eve's parameter and initial parameter of Alice and Bob) under which a successful saturation attack can be experimentally realized with our experimental setup of Eve.

7. I have proposed a new strategy to induce homodyne detection saturation by inserting an external laser. This new attack can potentially reduce the complexity of the corresponding experimental setup and allows high precision of induced saturation with current technology.

8. I have studied and analyzed theoretically various noise contributions in a co-existence regime of a CV QKD system and a DWDM network.

9. In collaboration with other researchers in our team, we have experimentally demonstrated for the first time that a CV QKD system can co-exist with intense several classical channels in a DWDM network [67, 79, 80].

   The imperfections analysis (contribution 1) is discussed in Chapter 5; theoretical study of the saturation attack (contributions 2, 3, 4) is presented in Chapter 7; experimental demonstration of the saturation attack (contributions 5, 6, 7) is described in Chapter 8 and the co-existence study and demonstration of CV QKD wavelength multiplexed with intense classical signals (contributions 8, 9) is presented in Chapter 9.

1.5 Publications

1. Hao Qin, Rupesh Kumar, and Romain Alléaume. Saturation attack on continuous-variable quantum key distribution system. In *Proc. SPIE 8899, Emerging Technologies in Security and Defence; and Quantum Security II; and Unmanned Sensor Systems X, 88990N*, volume 8899, pages 88990N–88990N–7, 2013. doi: 10.1117/12.2028543. URL http://dx.doi.org/10.1117/12.2028543 [140].

2. Hao Qin, Rupesh Kumar, and Romain Alléaume. Saturation attack on a practical continuous-variable quantum key distribution system, August 2013. URL http://2013.qcrypt.net/program/. Talk at QCrypt 2013 [141].

3. Paul Jouguet, Sébastien Kunz-Jacques, Rupesh Kumar, Hao Qin, and Romain Alléaume. Experimental demonstration of the coexistence of continuous-variable quantum key distribution with an intense DWDM classical channel, August 2013. URL http://2013.qcrypt.net/program/. Talk at QCrypt 2013 [67].

4. Rupesh Kumar, Hao Qin, and Romain Alléaume. Experimental demonstration of the coexistence of continuous-variable quantum key distribution with an intense DWDM classical channel. In *OSA Technical Digest (online)*, pages FM4A.1–, San Jose, California, 2014. Optical Society of America. URL http://www.osapublishing.org/abstract.cfm?URI=CLEO_QELS-2014-FM4A.1[79].

5. Rupesh Kumar, Hao Qin, and Romain Alléaume. Coexistence of continuous variable QKD with intense DWDM classical channels. *New Journal of Physics*, 17(4):043027–, 2015. ISSN 1367-2630. URL http://stacks.iop.org/1367-2630/17/i=4/a=043027 [80].

6. Hao Qin, Rupesh Kumar, and Romain Alleaume. Quantum hacking on a practical continuous-variable quantum cryptosystem by inserting an external light. In *Proc. SPIE 9648, Electro-Optical and Infrared Systems: Technology and Applications XII; and Quantum Information Science and Technology*, volume 9648, pages 9648V–11, 2015. doi: 10.1117/12.2195433. URL http://dx.doi.org/10.1117/12.2195433 [144].

7. Hao Qin, Rupesh Kumar, and Romain Alléaume. Quantum hacking: saturation attack on practical continuous-variable quantum key distribution system. *arXiv preprint arXiv:1511.01007*, 2015 [142].

8. Hao Qin, Rupesh Kumar, and Romain Alléaume. Saturation attack on continuous-variable QKD systems: experimental demonstration, performance analysis and countermeasure. *In preparation*, 2015 [143].

Chapter 2

Quantum information with continuous variables

Quantum information is a young discipline which combines knowledges and techniques from different scientific fields, in particular: quantum mechanics and information theory. Quantum information aims to study the information processing capabilities operated by the manipulation of quantum states. Quantum information also offers new applications such as quantum computation and quantum cryptography, which can not be achieved in the contest of classical information processing.

Quantum information with continuous variable (CV) is interesting to us since we study QKD with continuous variables in this thesis. One motivation to study continuous variable starts from the fact that it captures the behavior of many quantum optical states and measurements that can be realized efficiently in experiments.

In this chapter, we first give a brief presentation of classical information theory, then we present useful tools for studying continuous variables in phase space. The content of this chapter is mainly based on the test books of information theory [21, 115] and quantum optics [84, 155], as well as references [40, 85, 102].

2.1 Classical information theory

In this section, we introduce elements of information theory which will be useful to study QKD. In particular, we will describe the notions of entropy, mutual information and channel capacity which have been introduced by Shannon in 1948 when classical information theory was born. A more detailed presentation can be found in references [21, 115].

2.1.1 Entropy

Entropy, also known as Shannon entropy, is a measure of the uncertainty of a discrete random variable. The entropy $H(X)$ of a random variable X is defined as:

$$H(X) = -\sum_{x\in \mathsf{X}} p(x)\log_2 p(x) \tag{2.1}$$

In which X is a random variable taking values in the alphabet X and $p(x) = Pr\{X = x\}$ is the probability distribution function. The base of the logarithm is 2, thus the entropy is expressed in bits. Note that the entropy can be also expressed in other base of the logarithm. The entropy only depends on the probability distribution of the random variable X, but not on the actual values that are taken by X.

The notion of entropy can be extended to two random variables X and Y with a joint probability distribution function $p(x,y)$, where the *joint entropy* $H(X,Y)$ is defined as:

$$H(X,Y) = -\sum_{x\in \mathsf{X}}\sum_{y\in \mathsf{Y}} p(x,y)\log_2 p(x,y) \tag{2.2}$$

In fact, the joint entropy can be further generalized to n random variables $X_1,\cdots,X_n$, with their joint probability distribution function $p(x_1,\cdots,x_n)$:

$$H(X_1,\cdots,X_n) = -\sum_{x\in \mathsf{X}_1}\cdots\sum_{y\in \mathsf{X}_n} p(x_1,\cdots,x_n)\log_2 p(x_1,\cdots,x_n) \tag{2.3}$$

Based on the definition, several properties of the entropy can be directly deduced:

Theorem 2.1.1.1. *(Properties of the entropy).*

1. $H(X) \geq 0$, $H(X) = 0$ *if* X *is a fixed value.*

2. $H(X_1,\cdots,X_n) \leq H(X_1)+\cdots+H(X_n)$ *with equality only if* $X_1,\cdots,X_n$ *are independent.*

3. *If* X *contains* n *elements and* n *is finite, then* $H(X) \leq log_2 n$ *with equality only if* X *follows uniform distribution on* X.

Conditional entropy is another important notion in the information theory. It quantifies the amount of information that is needed to describe the outcome of a random variable Y while the input of another random variable X is known. The conditional entropy of Y with

given X is defined as:

$$\begin{aligned} H(Y|X) &= \sum_{x\in\mathsf{X}} p(x)H(Y|X=x) \\ &= -\sum_{x\in\mathsf{X}} p(x)\sum_{y\in\mathsf{Y}} p(x|y)\log_2 p(y|x) \\ &= -\sum_{x\in\mathsf{X}}\sum_{y\in\mathsf{Y}} p(x,y)\log_2 p(y|x), \end{aligned} \tag{2.4}$$

In which $p(y|x) = \frac{p(x,y)}{p(x)}$ is the *conditional probability distribution function*. $H(Y|X=x)$ is the entropy of Y conditioned on X with a certain value x. The conditional entropy $H(Y|X)$ can be seen as the result of averaging $H(Y|X=x)$ over all possible values x that X takes.

By comparing to the definition of entropy, we directly have the following property for the conditional entropy :

$$H(X|Y) \leq H(X) \tag{2.5}$$

with equality if X and Y are independent random variables.

The *chain rule* property connects the concepts of entropy, joint entropy and conditional entropy:

$$H(X,Y) = H(Y) + H(X|Y) = H(X) + H(Y|X) \tag{2.6}$$

The chain rule shows that the entropy of two random variables is the entropy of one plus the conditional entropy of the other. From this property we can further deduce that :

$$H(Y|X) = H(X|Y) - H(X) + H(Y), \tag{2.7}$$

which is known as *Bayes' rule*. Besides Shannon entropy, the *Rényi entropy* also describes a family of entropic quantities for a random variable. The Rényi entropy of order α of a random variable X can be defined as:

$$H_\alpha(X) = \frac{1}{1-\alpha}\log_2 \sum_{x\in\mathsf{X}} p(x)^\alpha, \alpha \geq 0, \alpha \neq 1 \tag{2.8}$$

With some particular values of α, one can find several kinds of entropic quantities :

- $\alpha = 0$: *max-entropy* of X, $H_0(X) = \log_2|\mathsf{X}|$. H_0 is the logarithm of the size of the support of X.
- $\alpha \to 1$: Shannon entropy of X, $H_1(X) = H(X)$.
- $\alpha = 2$: *collision-entropy* of X, $H_2(X) = \log_2 \sum_{x\in\mathsf{X}} p(x)^2$.

- $\alpha = \infty$: *min-entropy* of X, $H_\infty(X) = \log_2 \sup_{x \in \mathsf{X}} p(x)^2$. Min-entropy can be understood as the best guessing probability of the random value X.

For a given random variable X, $H_\alpha(X)$ decreases with the value of α, where $H_0(X) \geq H_1(X) \geq H_2(X) \geq H_\infty(X)$. The inequalities becomes saturated when X follows a uniform distribution. For n independent random variables $X_1 \cdots X_n$, their Rényi entropies are additive: $H_\alpha(X_1 \cdots X_n) = H_\alpha(X_1) \cdots H_\alpha(X_n)$.

The Shannon entropy is also related to the optimal compression rate one can achieve for a given random variable, which is given in the *source coding theorem*. A *source code* C of a random variable (or a source) X is a mapping from alphabet X to a set of bit strings with finite-length in the range of X. A source symbol x can be recovered from $C(x)$ with a source code.

Theorem 2.1.1.2. *(Shannon's source coding theorem[158]). N independent and identically distributed (i.i.d.) random variables each with entropy $H(X)$ can be compressed into $NH(X)$ bits or more with negligible risk of information loss, as N tends to infinity; conversely, if they are compressed into fewer than $NH(X)$ bits it is virtually certain that some information will be lost.*

Shannon's source coding theorem shows that one cannot describe a random variable (a source) with a number of bits whose entropy is lower than the one of the source.

2.1.2 Mutual information

We now move to the next important notion: mutual information, which is closely related to entropy. Mutual information quantifies the *degree of dependence* or correlation between two random variables. For two random variables X and Y with a joint probability distribution function $p(x,y)$ and probability distribution functions $p(x)$ and $p(y)$, the mutual information $I(X;Y)$ is the relative entropy between $p(x,y)$ and $p(x)p(y)$:

$$I(X;Y) = -\sum_{x \in \mathsf{X}} \sum_{y \in \mathsf{Y}} p(x,y) \log_2 \frac{p(x,y)}{p(x)p(y)} \tag{2.9}$$

$I(X;Y)$ is a measure of the correlation between X and Y, if X and Y are independent variables, then $I(X;Y) = 0$. Several properties of mutual information can be deduced from its definition and are summarized as follows:

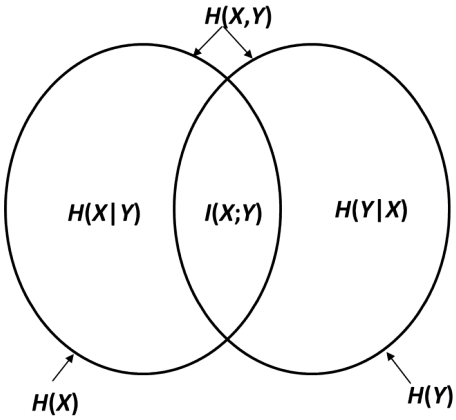


Fig. 2.1 Venn diagram of relationship between entropy and mutual information.

Theorem 2.1.2.1. *(Properties of the mutual information)*

$$I(X;Y) = H(X) - H(X|Y) \tag{2.10}$$
$$I(X;Y) = H(Y) - H(Y|X) \tag{2.11}$$
$$I(X;Y) = H(X) + H(Y) - H(X,Y) \tag{2.12}$$
$$I(X;Y) = I(Y;X) \tag{2.13}$$
$$I(X;X) = H(X) \tag{2.14}$$

Eq.(2.10) illustrates that mutual information $I(X;Y)$ is the reduction in the uncertainty of X given the knowledge of Y. Eq.(2.12) shows the relationship between entropy and mutual information and this relation is shown in Fig.2.1, where $I(X;Y)$ is the intersection of the information in X with the information in Y. Eq.(2.14) proves that the mutual information of a random variable with itself is its entropy. Thus entropy is also refereed to *self-information*.

2.1.3 Channel capacities

Besides entropies and mutual information, *channel capacity* is another important notion which was introduced by Shannon in Shannon's noisy-channel theorem [158]. The channel capacity gives the limit on the rate of communication of information over a *communication channel*. A scheme of communication channel is shown in Fig. 2.2, in which:

- A *transmitter* transforms the message into a signal sent it through the *channel*. In particular, it produces a input variable X within an alphabet X.
- The *channel* is the physical medium which carries the signal while some noise can

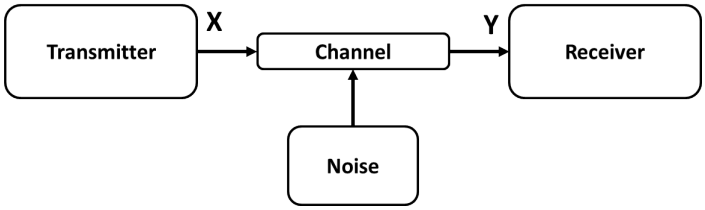


Fig. 2.2 Communication channel scheme.

add to the signal.

- A *Receiver* recovers the message from the received signal. In particular, it produces a output variable Y within an alphabet Y.

The mathematical interpretation of a communication channel is that, the output variable Y of the channel depends probabilistically on the input variable X and a probability transition matrix $p(y|x)$ determines the probability of observing the output y given the input x. If the probability distribution of the output only depends on the input at that time, the channel is considered as *memoryless*. For a memoryless channel with input X and output Y, the capacity C is defined as:

$$C = \max_{p(x)} I(X;Y), \tag{2.15}$$

in which the maximum is taken for all possible distributions $\{p(x)\}$.

One of the most studied channel is the so called *Binary Symmetric Channel* (BSC). One side (transmitter) sends a bit through the BSC. Due to the added noise from the channel, the other side (receiver) receives the correct bit with a probability p or an erroneous bit with a probability $1-p$, while the input X and output alphabet Y are both are $\{0,1\}$. This means that the transition matrix $p(y|x)$ is given by:

$$p(Y=y|X=x) = \begin{cases} 1-p & \text{if} \quad y=x \\ p & \text{if} \quad y\neq x \end{cases} \tag{2.16}$$

A scheme of BSC with the transition probabilities p and $1-p$ is shown in Fig.2.3. The capacity of the BSC is given as:

$$C_{BSC} = 1 - G(p), \tag{2.17}$$

where $G(p) = -p\log_2 p - (1-p)\log_2(1-p)$ is the binary entropy function. One can prove this result by calculating the mutual information of the input variable X and the output

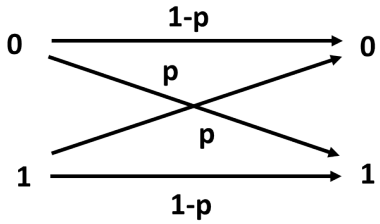


Fig. 2.3 Binary symmetric channel.

variable Y in the BSC:

$$\begin{aligned} I(X;Y) =& H(X) - H(X|Y) && (2.18)\\ =& H(Y) - \sum_{x\in 0,1} p(x) H(Y|X=x) && (2.19)\\ =& H(Y) - \sum_{x\in 0,1} p(x) h(p) && (2.20)\\ =& H(Y) - G(p) && (2.21)\\ \leq& 1 - G(p) && (2.22) \end{aligned}$$

For the last inequality $H(Y) \leq 1$ is because the entropy of a binary random variable is upper bounded by 1. Equality happens when the input distribution of X is uniform. The capacity of BSC is reached when the input distribution is equal to 1 ($p = 1$), and hence X is an uniform binary random variable.

Another important channel is the Additive White Gaussian Noise Channel (AWGNC). which is with great interest for QKD with continuous variables. In the AWGNC, the output Y and the input X are connected by $Y = X + Z$, in which Z is a Gaussian noise centered on zero ($\langle Z \rangle$) and of a variance σ_Z^2. Actually Z is a random variable which follows a normal distribution and is independent of X. A scheme of AWGNC is represented in Fig.2.4.

The capacity of the AWGNC is infinite if there is no restriction on the variance of input variable X. If the variance of X is finite, noted Σ_X^2, then the capacity of the AWGNC is the following:

$$C_{AWGNC} = \frac{1}{2} \log_2 (1 + \mathrm{SNR}), \tag{2.23}$$

in which, SNR is the signal-to-noise ratio which is the ratio of Σ_X^2/σ_Z^2. We compute this capacity in the section 2.1.4 after we generalize the notions of random variable and entropy receptively for infinite dimensional Gaussian variable and for differential entropy.

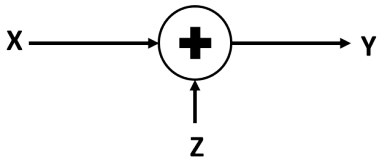


Fig. 2.4 Additive white Gaussian noise channel. It represents the relation: $Y = X + Z$, where X is the input variable, Z is added Gaussian noise variable and Y is the output variable.

2.1.4 Gaussian random variable and its entropy

In the following chapters of this thesis, we will study a specific CV QKD protocol, namely GG02 (Gaussian Modulated Coherent State) protocol [48], that is based on Gaussian random variable encodings and Gaussian channels. Particularly, it is related to the mutual information and entropies of Gaussian variables . In this subsection, we will briefly present important results.

Differential entropy

A Gaussian variable is a *continuous* random variable, where the definition of Shannon entropy is only applied to discrete random variable. A random variable X is said to be continuous, when its cumulative distribution function $F(x) = Pr(X \leq x)$ is continuous. $f(x) = F'(x)$ is the *probability density function* (or probability distribution function) for X and it needs to satisfy $\int_{-\infty}^{\infty} f(x) = 1$.

The notion of Shannon entropy can be extended to continuous random variable by defining the *differential entropy*. The differential entropy of a continuous random variable X with its probability distribution function $f(x)$ is defined as:

$$h(X) = -\int_D f(x)\log_2 f(x)dx, \tag{2.24}$$

where D is the integral domain: the *support set* of the random variable X, where $f(x) > 0$. Unlike entropy of discrete variables, differential entropy can be negative.

The definition of differential entropy of a single random variable can be also extended to a set of random variables $X_1, \cdots, X_n$, where the *joint differential entropy* with their joint probability distribution function $f(x_1, \cdots, x_n)$ is defined as:

$$h(X_1, \cdots, X_n) = -\int f(x_1, \cdots, x_n)\log_2 f(x_1, \cdots, x_n)dx_1 \cdots dx_n \tag{2.25}$$

As in the discrete case, for two random variable X, Y with joint probability distribution

function $f(x,y)$, one can define the *conditional differential entropy* $h(X|Y)$:

$$h(X|Y) = -\int f(x,y)\log_2 f(x|y)dxdy. \tag{2.26}$$

Since $f(x|y) = f(x,y)/f(y)$, we can further deduce that:

$$h(X|Y) = h(X,Y) - h(Y). \tag{2.27}$$

The mutual information between two continuous random variables X and Y with joint distribution function f(x, y) is defined as:

$$I(X;Y) = \int f(x,y)\log_2 \frac{f(x,y)}{f(x)f(y)}dxdy. \tag{2.28}$$

Similarly to the discrete case, we can deduce the properties of mutual information in the continuous case from the definition:

$$\begin{aligned} I(X;Y) =& h(X) - h(X|Y) && (2.29)\\ =& h(X) - h(Y|X) && (2.30)\\ =& h(X) + h(Y) - h(X,Y) && (2.31) \end{aligned}$$

Gaussian random variable

A random variable X is called Gaussian random variable if its probability distribution function follows a normal (Gaussian) distribution:

$$f(X = x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-x_0)^2}{2\sigma^2}}, \tag{2.32}$$

in which x_0 is the mean value or the *expectation* $E(X)$ of the distribution. σ is the *standard deviation* with $V_X = \sigma^2$, the variance of the random variable X. The variance of X is defined as:

$$Var(X) = E[(X - E[X])^2] = E[X^2] - E[X]^2. \tag{2.33}$$

The Gaussian variable X is denoted as $X \sim \mathcal{N}(x_0, \sigma^2)$, which shows that X is determined by the first two moments of its probability distribution function.

An ensemble of Gaussian random variables also follows a Gaussian distribution, and is totally characterized by the first two moments of its probability distribution function. One can describe an ensemble of n Gaussian random variables $\vec{X} = (X_1, \cdots, X_n)$ by its joint

probability distribution function:

$$f(\vec{X}=\vec{x}) = \frac{1}{\sqrt{(2\pi)^n \det(K_{AB})}} e^{-\frac{1}{2}(\vec{X}-\vec{X}_0)K^{-1}(\vec{X}-\vec{X}_0)^T}, \tag{2.34}$$

in which $\vec{X}_0 = (E[X_1], \cdots, E[X_n])$ is a dimension n vector, and $\det(K)$ is the *determinant* of a matrix K. K is called the *covariance matrix*, which is used to generalize the notion of variance to multiple dimensions. The covariance matrix K is defined as

$$K = \begin{bmatrix} Cov(X_1,X_1) & \cdots & Cov(X_1,X_n) \\ Cov(X_2,X_1) & \cdots & Cov(X_2,X_n) \\ \vdots & \ddots & \vdots \\ Cov(X_n,X_1) & \cdots & Cov(X_n,X_n) \end{bmatrix}, \tag{2.35}$$

where each item $Cov(i,j)$ in matrix K is a *covariance* between two variables X_i and X_j with $i = \{1 \cdots n\}$ and $j = \{1 \cdots n\}$:

$$Cov(X_i,X_j) = E[(X_i - E[X_i])(X_j - E[X_j])] = E[X_iX_j] - E[X_i]E[X_j] \tag{2.36}$$

In this thesis, we will focus in particular on the case where two Gaussian random variables X and Y are centered on zero. In such case the covariance matrix of two variables reduces to:

$$K_{AB} = \begin{bmatrix} V_A & \langle XY \rangle \\ \langle XY \rangle & V_B \end{bmatrix}, \tag{2.37}$$

where the variances $V_A = Var(X)$ and $V_B = Var(Y)$. $\langle XY \rangle$ is the covariance between X and Y, because $Cov(X,Y) = E[XY] - E[X]E[Y] = \langle XY \rangle = \int dx \int xyf(x,y)dy$ since $E[X] = 0$. And the joint probability distribution function becomes:

$$f(X=x, Y=y) = \frac{1}{2\pi\sqrt{V_AV_B - \langle XY \rangle^2}} e^{-\frac{x^2V_B - 2xy\langle XY \rangle^2 + y^2V_A}{V_AV_B - \langle XY \rangle^2}}, \tag{2.38}$$

in which the equality $\det(K_{AB}) = V_AV_B - \langle XY \rangle^2$ has been taken into account.

Differential entropy of Gaussian variables

Regarding Gaussian variables, one can calculate analytically the differential entropy of a Gaussian variable X based on the definition (Eq. (2.24)) and the probability distribution

function (Eq. (2.32)) :

$$\begin{aligned} h(X) &= -\int f(x)\log_2(\frac{1}{\sqrt{2\pi\sigma^2}})dx - \int f(x)\log_2(e)\frac{x^2}{2\pi\sigma^2}dx \\ &= \frac{1}{2}\log_2(2\pi\sigma^2) + \frac{1}{2}\log_2(e) \\ &= \frac{1}{2}\log_2(2\pi e\sigma^2) \end{aligned} \tag{2.39}$$

For n Gaussian random variables $X_1, \cdots, X_n$ with their joint probability distribution function defined in Eq. (2.34), the joint differential entropy can be expressed as:

$$h(X_1, \cdots, X_n) = \frac{1}{2}\log_2\left((2\pi e)^n \det(K)\right) \tag{2.40}$$

From this equation, we can further calculate the conditional differential entropy for two Gaussian random variables X and Y (Eq. (2.38)):

$$h(Y|X) = h(Y,X) - h(X) = \frac{1}{2}\log_2\left(2\pi e\frac{\det(K_{AB})}{V_A}\right), \tag{2.41}$$

in which, we define the conditional variance $V_{B|A}$:

$$V_{B|A} = \frac{\det(K_{AB})}{V_A} = V_B - \frac{\langle XY\rangle^2}{V_A} \tag{2.42}$$

Based on the results above, we can further express the mutual information $I(X;Y)$ between two correlated Gaussian random variables X and Y. From Eq. (2.39) and Eq. (2.41), it is clear that:

$$\begin{aligned} I(X;Y) = h(Y) - h(Y|X) =& \frac{1}{2}\log_2(2\pi e V_B) - \frac{1}{2}\log_2(2\pi e V_{B|A}) \\ =& \frac{1}{2}\log_2\left(\frac{V_B}{V_{B|A}}\right) \end{aligned} \tag{2.43}$$

The equivalent expressions of $I(X;Y)$ can be also given as following:

$$I(X;Y) = h(X) - h(X|Y) = \frac{1}{2}\log_2\left(\frac{V_A}{V_{A|B}}\right), \tag{2.44}$$

$$I(X;Y) = h(X) + h(Y) - h(X,Y) = \frac{1}{2}\log_2\left(\frac{V_A V_A}{\det(K_{AB})}\right), \tag{2.45}$$

Capacity of additive white Gaussian noise channel

The previous results can be used to prove the capacity of the additive white Gaussian noise channel which is introduced in the section 2.1.3. The mathematical model of the AWGNC is known as: $Y = X + Z$ (Fig.2.4), in which X is a random variable with variance Σ^2, Z is a Gaussian noise $Z \sim \mathcal{N}(0, \sigma_Z^2)$ and is independent with X, and Y is the output variable. Hence the transition probability of the AWGNC can be given as:

$$f(Y = y|X = x) = \frac{1}{\sqrt{2\pi\sigma_Z^2}} e^{-\frac{(y-x)^2}{2\sigma_Z^2}}, \tag{2.46}$$

To compute the capacity of the AWGNC, we first express the mutual information $I(X;Y)$ between input X and output Y, and use the fact that X and Z are independent:

$$\begin{aligned} I(X;Y) =& h(Y) - h(Y|X) \\ =& h(Y) - h(X+Z|X) \\ =& h(Y) - h(Z|X) \\ =& h(Y) - h(Z), \end{aligned} \tag{2.47}$$

in which, $h(z) = \frac{1}{2}\log_2(2\pi e\sigma_Z^2)$ since $Z \sim \mathcal{N}(0, \sigma_Z^2)$ (Eg.(2.39)). Due to the fact of independence between X and Z, and $E[Z] = 0$, the variance of Y can be given by:

$$Var(Y) = Var(X+Z) = E[(X+Z)^2] - (E[X] + E[Z])^2 \tag{2.48}$$

$$= E[X^2] - E[X]^2 + E[Z^2] \tag{2.49}$$

$$= Var(X) + Var(Z) = \Sigma_X^2 + \sigma_Z^2. \tag{2.50}$$

Moreover, Theorem 8.6.5 in [21] shows that, for a given variance, the normal distribution maximizes the entropy over all distributions, so we can bound $h(Y)$:

$$h(Y) \leq \frac{1}{2}\log_2\left(2\pi e(\Sigma_X^2 + \sigma_Z^2)\right). \tag{2.51}$$

By taking above equation into Eq.(2.47), we find the upper bound of $I(X;Y)$:

$$I(X;Y) = h(Y) - h(X) \leq \frac{1}{2}\log_2\left(1 + \frac{\Sigma_X^2}{\sigma_Z^2}\right), \tag{2.52}$$

where the equality is reached when the input follows a normal distribution. Thus, the capacity of the AWGNC is given by:

$$C_{AWGNC} = \frac{1}{2}\log_2(1+\mathrm{SNR}), \tag{2.53}$$

where $SNR = \Sigma_X^2/\sigma_Z^2$ and the input needs to follow a normal distribution.

2.2 Phase space representation

The goal of this chapter is to present a formalism specifically adapted to study quantum information with the continuous variables in bosonic systems, in particular, the quantized electro-magnetic field. More detailed information of phase space representation can be referred to references [84, 155].

2.2.1 Electromagnetic field and quadrature operators

The electric field $\vec{E}$ and the magnetic field $\vec{H}$ are connected through the Maxwell equations. The electric field follows a wave equation deduced from Maxwell equations in the vacuum:

$$\nabla^2 E - \frac{1}{c^2}\frac{\partial^2 E}{\partial t} = 0, \tag{2.54}$$

in which $c = (\mu_0\varepsilon_0)^{1/2}$ is the speed of light in vacuum and μ_0 and ε_0 are the free space permittivity and permeability. For a given mode m, the solution of the wave function describes the electric field $\vec{E}_n(\vec{r},t)$ in terms of propagating plane waves with the space vector $\vec{r}$ and time t, the multimode electric field $\vec{E}(\vec{r},t)$ can be expressed as:

$$\vec{E}(\vec{r},t) = \sum_m \vec{E}_m(\vec{r},t) \tag{2.55}$$

$$= \sum_m E_{0,n}\vec{e}_m[\alpha_m e^{i(\vec{k}_m\vec{r}-\omega_m t)} + \alpha_m^* e^{i(\vec{k}_m\vec{r}-\omega_m t)}], \tag{2.56}$$

in which ω_m is the angular frequency, $\vec{e}_m$ is the polarization vector, $\vec{k}_m$ is the propagation vector. $\alpha_m = |\alpha_m|e^{i\varphi_m}$ is the complex amplitude where $|\alpha_m|$ is a constant amplitude and φ_m is a constant phase. $E_{0,n}$ contains the prefactors:

$$E_{0,m} = \sqrt{\hbar\omega_m/\varepsilon_0}, \tag{2.57}$$

in which $\hbar$ is the reduced Planck constant. So far, the radiation field is expressed in a classical picture. In quantum optics, by replacing the complex amplitude α_m by the harmonic oscillator *annihilation* operators $\hat{a}_m$ and *creation* operators $\hat{a}_n^\dagger$ of photon, one can quantize the electric field for a given mode m:

$$\vec{E}_m(\vec{r},t) = \sum_m E_{0,m}\vec{e}_m[\hat{a}_m e^{i(\vec{k}_m\vec{r}-\omega_m t)} + \hat{a}_m^\dagger e^{i(\vec{k}_m\vec{r}-\omega_m t)}]. \tag{2.58}$$

$\hat{a}_m$ and $\hat{a}_m^\dagger$ obeys the commutation relation for bosons:

$$[\hat{a}_m,\hat{a}_n] = 0, [\hat{a}_m,\hat{a}_n^\dagger] = \delta_{mn}, [\hat{a}_m^\dagger,\hat{a}_n^\dagger] = 0. \tag{2.59}$$

In which the bracket notation stands for the commutation $[x,y] = xy - yx$ for x and y. As we have seen, the subscript m refers to a particular mode. In the remaining parts, if there is no ambiguity, m will be omitted. With the notion of *quadrature operators* one can rewrite Eq.(2.58) into:

$$\vec{E}(\vec{r},t) = E_0\vec{e}[\hat{X}\cos(\vec{k}\vec{r}-\omega t) + \hat{P}\sin(\vec{k}\vec{r}-\omega t)], \tag{2.60}$$

where $\hat{X}$ and $\hat{P}$ are the quadrature operators of the electric field and their relation with $(\hat{a},\hat{a}^\dagger)$ is given by:

$$\hat{X} = \frac{1}{\sqrt{2}}(\hat{a}^\dagger + \hat{a}), \tag{2.61}$$

$$\hat{P} = \frac{i}{\sqrt{2}}(\hat{a}^\dagger - \hat{a}), \tag{2.62}$$

where the reduced Plank's constant is normalized to 1. It can be done by rescaling the physical units. $\hat{X}$ and $\hat{P}$ are equivalent to the position and momentum of an harmonic oscillator in classical mechanics. In contrast to $(\hat{a},\hat{a}^\dagger)$, $\hat{X}$ and $\hat{P}$ are Hermitian and can thus be measured. The commutation relation of $(\hat{a},\hat{a}^\dagger)$ imposes the commutation rule for $\hat{X}$ and $\hat{P}$:

$$[\hat{X}_m,\hat{P}_n] = i\delta_{mn}, [\hat{P}_m,\hat{P}_n] = 0. \tag{2.63}$$

This rule further leads to the Heisenberg uncertainty relation:

$$\Delta\hat{X}\Delta\hat{P} \geq \frac{1}{2}|\langle[\hat{X},\hat{P}]\rangle| \geq \frac{1}{2}, \tag{2.64}$$

with $\Delta\hat{A} = (\langle A^2\rangle - \langle A\rangle^2)^{1/2}$.

Shot noise unit

We now introduce the notion of *shot noise unit* N_0, which is the basic unit to calibrate the system. If we consider the reduced Planck constant $\hbar$ in the commutation relation and uncertainty relation of the quadrature, Eq.(2.63) and Eq.(2.64) can be given as:

$$[\hat{X},\hat{P}] = i\hbar, \tag{2.65}$$

$$\Delta\hat{X}\Delta\hat{P} \geq \frac{\hbar}{2} \tag{2.66}$$

Naturally, one would use the minimum value of the uncertainty relation as the basic unit of the system, where $N_0 = 1/2\hbar$ such that:

$$[\hat{X},\hat{P}] = 2iN_0, \tag{2.67}$$

$$\Delta\hat{X}\Delta\hat{P} \geq N_0 \tag{2.68}$$

As we shall see, in the following chapters concerning the CV QKD, we will consider $N_0 = 1$ as the shot noise which implies $\hbar = 2$, and it is achievable with rescaling the physical units. In this chapter, we remain use $\hbar = 1$ to present the tools for CV quantum system, which imposes $N_0 = 1/2$.

2.2.2 Continuous-variable quantum system and Fock state representation

A continuous variable (CV) system is a canonical quantum system composes a set of N modes (i.e N modes of the electromagnetic field) of infinite dimension, it can be described in the Hillbert space:

$$\mathscr{H} = \bigotimes_{m=1}^{N} \mathscr{H}_m, \tag{2.69}$$

which is a tensor product of N infinite-dimensional *Fock spaces* $\mathscr{H}_m$. Fock space $\mathscr{H}_m$ is associated with a particular mode, where a mode is characterized by its energy, its polarization and its spatial and temporal mode. $\mathscr{H}_m$ can be described by the *Fock space*: $|0\rangle \cdots |n\rangle \cdots$, in which, $|n\rangle$ is known as the *Fock state* representing the state of n indistinguishable photons present in the specific mode.

The Fock states $\{|n\rangle\}$ are closely connected to the annihilation and creation operators $\hat{a}$ and $\hat{a}^\dagger$. For a single mode of the field with frequency ω, $|n\rangle$ are the eigenstates of the

number operator $\hat{N} = \hat{a}^\dagger \hat{a}$ with eigenvalue n:

$$\hat{a}^\dagger \hat{a}|n\rangle = n|n\rangle. \tag{2.70}$$

This equation can be interpreted as the presence of n quanta in a particular mode. Thus the Fock state $|n\rangle$ is also known as photon number state. A Fock state $|n\rangle$ is an eigenvector of the Hamiltonian:

$$H|n\rangle = \hbar\omega(\hat{a}^\dagger \hat{a} + \frac{1}{2})|n\rangle. \tag{2.71}$$

The state $|0\rangle$ is known as *vacuum state* which implies a state with no photon. In fact, the annihilation and creation operators $\hat{a}$ and $\hat{a}^\dagger$ can be defined with $\{|n\rangle\}$[84, 155]:

$$\hat{a}|n\rangle = \sqrt{n}|n-1\rangle, \tag{2.72}$$

$$\hat{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle \tag{2.73}$$

By adding n photons to a vacuum state $|0\rangle$, one can generate a Fock state:

$$|n\rangle = \frac{1}{\sqrt{n!}}(\hat{a}^\dagger)^n|0\rangle. \tag{2.74}$$

The Fock states $|n\rangle$ are the eigenstates of the number operator $\hat{N}$ and form a basis of orthogonal states with its orthogonality and completeness relation:

$$\langle m|n\rangle = \delta_{mn}, \tag{2.75}$$

$$\sum_{n=0}^{\infty} |n\rangle\langle n| = \mathbb{1}. \tag{2.76}$$

In general, an arbitrary state with one mode can be described by the density matrix operator:

$$\rho = \sum_{m,n=0}^{\infty} \rho_{m,n}|m\rangle\langle n|, \tag{2.77}$$

with $\mathrm{Tr}[\rho] = 1$ and ρ is a Hermitian positive operator which means the eigenvalues are all positive. Such formalism of a single-mode field's basis can be extended to a global Hilbert space $\mathscr{H}$ with N modes, where the basis is defined as:

$$|n_1, \cdots, n_i, \cdots, n_N\rangle = |n_1\rangle \otimes \cdots \otimes |n_m\rangle \otimes \cdots \otimes |n_N\rangle, \tag{2.78}$$

with $n_m \in \mathbb{N}$ photons in the mode $m \in \{1,\ldots,N\}$. The vacuum state of the global Hilbert space $\mathscr{H}$ is denoted as $|0\rangle \equiv |0,\cdots,0,\cdots\rangle$. In order to generate the Fock basis, one can add n_i photons in the mode i to the vacuum state:

$$|n1,\ldots,n_N\rangle = \frac{1}{\sqrt{n_1!\cdots n_N!}}\hat{a}_1^{\dagger n_1}\cdots\hat{a}_N^{\dagger n_N}|0\rangle. \tag{2.79}$$

Accordingly, a density matrix can be expressed as:

$$\rho = \sum_{\vec{m},\vec{n}=0}^{\infty} \rho_{\vec{m},\vec{n}}|m_1,\cdots,m_N\rangle\langle n_1,\cdots,n_N|, \tag{2.80}$$

with $\vec{m} = (m_1,\cdots,m_N)$ and $\vec{n} = (n_1,\cdots,n_N)$. Indeed, it is very useful to study quantum systems with the density matrix when the dimension of the Hilbert space is small. However, for an infinite-dimensional Hilbert space, it might be more convenient to use the quadrature operator than the density matrix to describe the quantum system. In a N mode system, the quadratures can be given in a vector $\hat{u}$:

$$\hat{u} = (\hat{u}_1,\cdot,\hat{u}_{2N})^T = (\hat{X}_1,\hat{P}_1,\cdot,\hat{X}_N,\hat{P}_N)^T \tag{2.81}$$

The commutation relation then turns into:

$$[\hat{u}_k,\hat{u}_l] = i\Omega_{kl} \tag{2.82}$$

in which Ω follows the symplectic form:

$$\Omega = \bigotimes_{m=1}^{N}\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}, \tag{2.83}$$

and an operator S is symplectic if:

$$S\Omega S^T = \Omega, \tag{2.84}$$

which means that it remains invariant under a symplectic transformation.

2.2.3 Quadrature eigenstates and coherent states

In the phase space representation, rather than Fock states, we are concerned with two kinds of states which play important roles: quadrature eigenstates and coherent states.

Quadrature eigenstates

Quadrature eigenstates are eigenstates of the quadrature operators $\hat{X}$ and $\hat{P}$ which obey the following relation:

$$\hat{X}|x\rangle = x|x\rangle, \tag{2.85}$$
$$\hat{P}|p\rangle = p|p\rangle, \tag{2.86}$$

where, $|x\rangle$ is called a position eigenstate and $|p\rangle$ a momentum eigenstate. Since$\hat{X}$ and $\hat{P}$ are Hermitian, they form two orthonormal bases of the Fock space:

$$\langle x|x'\rangle = \delta(x-x'), \tag{2.87}$$
$$\langle p|p'\rangle = \delta(p-p'), \tag{2.88}$$

which further give the resolutions of the identity:

$$\int_{-\infty}^{\infty} |x\rangle\langle x|dx = \mathbb{1}, \tag{2.89}$$
$$\int_{-\infty}^{\infty} |p\rangle\langle p|dp = \mathbb{1}. \tag{2.90}$$

These two bases are connected by Fourier transform:

$$|x\rangle = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-ixp}|p\rangle, \tag{2.91}$$
$$|p\rangle = \frac{1}{\sqrt{2\pi}} \int_{\infty}^{\infty} e^{ixp}|x\rangle. \tag{2.92}$$

For a given quantum state $|\psi\rangle$, its wave function $\psi(x)$and corresponding Fourier transform $\psi(p)$ are linked to the quadrature eigenstates:

$$\psi(x) = \langle x|\psi\rangle, \tag{2.93}$$
$$\psi(p) = \langle p|\psi\rangle \tag{2.94}$$

However, the quadrature eigenstates are not related to physical states since their energy diverges.

Coherent state

The photon number states represent the states with precise number of photons. However, in experiments, such states are difficult to realize for $n > 2$. In contrast, a *coherent state* is

the quantum state output by a laser. This makes coherent state interesting both for theories and experiments. The number of photons in a coherent state is not precisely known. A coherent state $|\alpha\rangle$ is defined as the eigenstate of the annihilation operator:

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle, \tag{2.95}$$

in which α is a complex number. The states $|\alpha\rangle$ are not orthogonal, since $\hat{a}$ is a non-Hermitian operator. On the other hand, a coherent state can be also seen as a *displaced* vacuum state, in order to study it, let us first define unitary displacement operator:

$$\hat{D}(\alpha) = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}, \tag{2.96}$$

which is unitary operator because $i(\alpha\hat{a}^\dagger - \alpha^*\hat{a})$ is Hermitian. As unitary operator, the displacement operator $D(\alpha)$ follows the rules:

$$\hat{D}^{-1}(\alpha) = \hat{D}^\dagger(\alpha) = \hat{D}(-\alpha). \tag{2.97}$$

The Hadamard lemma shows that for two operators $\hat{A}$ and $\hat{B}$:

$$e^{\hat{A}}\hat{B}e^{-\hat{A}} = \hat{B} + [\hat{A}, \hat{B}]. \tag{2.98}$$

If we moreover consider $\hat{A} = \alpha\hat{a}^\dagger - \alpha^*\hat{a}$ and $\hat{B} = \hat{a}$, with the property of the unity operator Eq.(2.97) and the commutation relation of $\hat{a}$ and $\hat{a}^\dagger$ we can further deduce that:

$$\hat{D}^\dagger(\alpha)\hat{a}\hat{D}(\alpha) = \hat{a} + \alpha, \tag{2.99}$$

$$\hat{D}^\dagger(\alpha)\hat{a}^\dagger\hat{D}(\alpha) = \hat{a}^\dagger + \alpha^*. \tag{2.100}$$

which shows that the operation of $D(\alpha)$ displaces the $\hat{a}$ and $\hat{a}^\dagger$ by the amount of α and α^*. If we apply the annihilation operator $\hat{a}$ to a displaced vacuum $\hat{D}(\alpha)|0\rangle$, then we have:

$$\hat{a}\hat{D}(\alpha)|0\rangle = \hat{D}(\alpha)D^\dagger(\alpha)\hat{a}\hat{D}(\alpha) \tag{2.101}$$

$$= \hat{D}(\alpha)(\hat{a} + \alpha)|0\rangle \tag{2.102}$$

$$= \alpha\hat{D}(\alpha)|0\rangle, \tag{2.103}$$

in which, we have considered Eq.(2.97), Eq.(2.99) and $\hat{a}|0\rangle = 0$ to achieve Eq.(2.101). Eq.(2.101) shows that $\hat{D}(\alpha)|0\rangle$ is an eigenstate of the annihilation operator with eigenvalue α, which is just the definition of the coherent state in Eq.(2.95). So that $|\alpha\rangle = \hat{D}(\alpha)|0\rangle$ means that coherent state is a vacuum state with some displacement. With similar tech-

nique, the displacement action on the quadrature operators can be deduced:

$$\hat{D}^{\dagger}(\alpha)\hat{X}\hat{D}(\alpha) = \hat{X} + \sqrt{2}\mathrm{Re}(\alpha), \tag{2.104}$$

$$\hat{D}^{\dagger}(\alpha)\hat{P}\hat{D}(\alpha) = \hat{P} + \sqrt{2}\mathrm{Im}(\alpha). \tag{2.105}$$

In which $\mathrm{Re}(\alpha)$ and $\mathrm{Im}(\alpha)$ are the real and imaginary parts of α. A coherent state $|\alpha\rangle$ can be thus considered as a vacuum state which is displaced by a quantity of $d_x = \mathrm{Re}(\alpha)$ along the quadrature $\hat{X}$ and a quantity of $d_p = \mathrm{Im}(\alpha)$ along the quadrature $\hat{P}$ in the phase space. One can further expand the coherent state $|\alpha\rangle$ in the Fock basis with the help of the Baker-Hausdorff formula:

$$D(\alpha) = e^{-|\alpha|^2/2} e^{\alpha\hat{a}^{\dagger}} e^{-\alpha^*\hat{a}} \tag{2.106}$$

According to the alternative interpretation of coherent state: $\hat{D}(\alpha)|0\rangle$, $|\alpha\rangle$ can be written as:

$$|\alpha\rangle = \hat{D}(\alpha)|0\rangle = e^{-|\alpha|^2/2} e^{\alpha\hat{a}^{\dagger}} e^{-\alpha^*\hat{a}}|0\rangle \tag{2.107}$$

$$= e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n \hat{a}^{\dagger n}}{n!}|0\rangle \tag{2.108}$$

$$= e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}|0\rangle. \tag{2.109}$$

As we can see from Eq.(2.107), the number of photon in a coherent state is not precisely known, but the relative phase can still be well defined. In contrary to Fock states which have totally random phase. One can deduce the probability that n photons can be found in a coherent state $|\alpha\rangle$:

$$P(n) = |\langle n|\alpha\rangle|^2 = e^{-|\alpha|^2} \frac{|\alpha|^{2n}}{n!}, \tag{2.110}$$

which is actually a *Poisson distribution* with mean value and variance equal to $|\alpha|^2$. The set of coherent states does not form an orthonormal basis. By using the Eq.(2.95) and Eq.(2.96), one can deduce the scalar product of two coherent states α and β:

$$\langle\beta|\alpha\rangle = \langle 0|D^{\dagger}(\beta)D^{\dagger}(\alpha)|0\rangle = \langle 0|D(\alpha-\beta)|0\rangle = \langle 0|D(\alpha-\beta)\rangle \tag{2.111}$$

$$= e^{-\frac{1}{2}|\alpha-\beta|^2}, \tag{2.112}$$

which shows that two coherent states are not orthogonal, though they become approximately orthogonal when $|\alpha-\beta| \gg 1$. Note that the completeness relation can be applied to a set

of coherent states:

$$\frac{1}{\pi}\int |\alpha\rangle\langle\alpha| d^2\alpha = \mathbb{1}. \tag{2.113}$$

Finally, let us note that, the Heisenberg uncertainty principle (Eq.(2.64)) is saturated for a coherent state, where the product of uncertainty quantities is minimal. To prove this, we can compute the first and second moment of the quadrature operators for a coherent state $|\alpha\rangle$:

$$\langle\hat{X}\rangle = \langle\alpha|\hat{X}|\alpha\rangle = \frac{1}{\sqrt{2}}\langle\alpha|\hat{a}^\dagger + \hat{a}|\alpha\rangle \tag{2.114}$$

$$= \frac{1}{\sqrt{2}}(\alpha^* + \alpha), \tag{2.115}$$

$$\langle\hat{X}^2\rangle = \langle\alpha|\hat{X}^2|\alpha\rangle = \frac{1}{2}\langle\alpha|\hat{a}^\dagger\hat{a}^\dagger + \hat{a}^\dagger\hat{a} + \hat{a}\hat{a}^\dagger + \hat{a}\hat{a}|\alpha\rangle \tag{2.116}$$

$$= \frac{1}{2}(1 + (\alpha^* + \alpha)^2). \tag{2.117}$$

Similar results can be also found for $\hat{P}$, which gives:

$$\Delta^2\hat{X} = \langle\hat{X}^2\rangle - \langle\hat{X}\rangle^2 = \frac{1}{2}, \tag{2.118}$$

$$\Delta^2\hat{P} = \langle\hat{P}^2\rangle - \langle\hat{P}\rangle^2 = \frac{1}{2}. \tag{2.119}$$

which shows that coherent states have minimal uncertainty on their quadratures.

2.2.4 Wigner function

The *Weyl operator* is a generalization of the displacement operators in the N-mode case:

$$\hat{D}(\vec{\xi}) = e^{-i\vec{\xi}^T\Omega\hat{u}}, \tag{2.120}$$

where $\vec{\xi}$ is a vector in the $2N$-dimensional phase space, $\hat{u}$ and Ω are defined in Eq.(2.81) and Eq.(2.82). The *Wigner characteristic function* is then defined as:

$$\chi_\rho(\vec{\xi}) = \mathrm{Tr}[\rho\hat{D}(\vec{\xi})] \tag{2.121}$$

A state ρ can then be described by the Wigner characteristic function in the phase space instead of using the density matrix:

$$\rho = \frac{1}{(2\pi)^N} \int \chi_\rho(-\vec{\xi}) \hat{D}(\vec{\xi}) d^{2N}\vec{\xi} \tag{2.122}$$

Through the Fourier transform of the characteristic function, the Wigner function of the state can be obtained:

$$W(\vec{\xi}) = \frac{1}{(2\pi)^N} \int e^{-i\vec{\xi}^T \Omega \vec{\zeta}} \chi_\rho d^{2N}\vec{\zeta} \tag{2.123}$$

A N-mode state ρ can be related to its Wigner function parameterized by the quadratures in the N dimensional phase space:

$$\begin{aligned} &W(X_1, P_1, \cdots, X_N, P_N) = \\ &\frac{1}{(2\pi)^N} \int_{\mathbb{R}^N} e^{i(P_1 y 1 + \cdots + P_N y N)} \langle X_1 - y_1, \cdots, X_N - y_N | \rho | X_1 + y_1, \cdots, X_N + y_N \rangle dy_1 \cdots y_N \end{aligned} \tag{2.124}$$

An operational interpretation of Wigner function is that it gives a genuine probability function for a particular quadrature in terms of homodyne measurement results. Specifically, for a N-mode state described by its Wigner function (Eq.(2.124)), the probability distribution of X_N through the homodyne measurement result is given by integrating the Wigner function over the quadratures that are not measured:

$$\Pr(X_N) = \int_{\mathbb{R}^{2N-1}} W(X_1, P_1, \cdots, X_N, P_N) dP_1 \cdots P_N dX_1 \cdots X_{N-1} \tag{2.125}$$

The trace of the state ρ can be achieved by the integration of the Wigner function in the phase space:

$$\mathrm{Tr}[\rho] = \int_{\mathbb{R}^N} W_\rho(\vec{\xi}) d\vec{\xi}. \tag{2.126}$$

Moreover, for an arbitrary operator $\hat{O}$, its expectation can by computed as an average of its Wigner transform in phase space:

$$\langle \hat{O} \rangle = \int_{\mathbb{R}^N} O(\vec{\xi}) W_\rho(\vec{\xi}) d\vec{\xi}. \tag{2.127}$$

More details about Wigner function can be found in [84, 155]. Under the phase space representation, the quantum state is represented by the Wigner function formalism with the

quadrature operators instead of density operator formalism. However, these two formalisms are equivalent. One can choose either of them to study the quantum state, for practical reasons, it is preferred to choose the one with which is easy to perform mathematical manipulation for a specific case.

2.3 Gaussian states

Among various continuous-variable states, Gaussian states are of practical interest as they represent a large clan of the states that can be produced experimentally. A state is said to be Gaussian if its characteristic function and Wigner function are both Gaussian.

For a general state ρ (density operator), the displacement vector $\vec{d} \in \mathbb{R}^{2N}$ is defined as:

$$\vec{d} = \langle \hat{u} \rangle = \mathrm{Tr}[\rho \hat{u}] \tag{2.128}$$

In which $\hat{u} \in \mathbb{R}^{2N}$ is the quadrature operator defined in Eq.(2.81) while the positive semi-definite symmetric $2N \times 2N$ covariance matrix γ is defined by:

$$\gamma_{ij} = \mathrm{Tr}[\rho\{(u_i - d_i)(u_j - d_j) + (u_j - d_j)(u_i - d_i)\}], \tag{2.129}$$

in which u_i and d_i stand for coordinates of the vector $\hat{u}$ and $\vec{d}$. Gaussian states are defined by a Gaussian characteristic function:

$$\chi_\rho(\vec{\xi}) = e^{-\frac{1}{4}\vec{\xi}^T \Gamma \vec{\xi} + iD^T \vec{\xi}}, \tag{2.130}$$

with $D = \Omega\vec{d}$ and covariance matrix $\Gamma = \Omega\gamma\Omega$. The Wigner function of a Gaussian state can be obtained through the Fourier transform of the characteristic function:

$$W(\hat{u}) = \frac{1}{\pi^{2N}\sqrt{\det(\gamma)}} e^{-(\hat{u}-\vec{d})^T \gamma^{-1} (\hat{u}-\vec{d})}. \tag{2.131}$$

Thus Gaussian states are totally described by the first two moments of the Wigner function (Eq.(2.130)), precisely the displacement vector $\vec{d}$ and the covariance matrix γ. Not all real symmetric matrices correspond to physical states, since they do not always satisfy the Heisenberg uncertainty relation. For Gaussian states, a necessary and sufficient condition to be satisfied by the covariance matrix γ is:

$$\gamma + i\Omega \geq 0. \tag{2.132}$$

which generalizes the Heisenberg uncertainty principle.

2.3.1 Symplectic Analysis

The covariance matrices of Gaussian states are characterized by the *symplectic invariants*. We now briefly present the symplectic analysis which is useful to study Gaussian states. Williamson theorem shows that for any N covariance matrix γ, there is a non-unique symplectic transformation S such that:

$$S\gamma S^T = \upsilon, \tag{2.133}$$

with υ, a diagonal covariance matrix:

$$\upsilon = \bigotimes_{i=1}^{N} \begin{bmatrix} \upsilon_k & 0 \\ 0 & \upsilon_k \end{bmatrix}, \tag{2.134}$$

where υ_k are known as the *symplectic eigenvalues*, which are the eigenvalues of the matrix $|i\Omega\gamma|$, where $|X|$ means $\sqrt{XX^\dagger}$. Such symplectic diagonalization in the phase space is similar to the density operator diagonalization in the Hilbert space.

With the symplectic eigenvalues υ_k, one can rewrite the uncertainty principle (Eq.(2.132)) into:

$$\upsilon_k \geq 1, \forall k = 1, \cdots, N. \tag{2.135}$$

For *pure* Gaussian states, this bound saturates with $\upsilon_k = \mathbb{1}$. The *purity* μ of a Gaussian state ρ with covariance matrix γ is defined as:

$$\mu = \mathrm{Tr}(\rho^2) = \frac{1}{\sqrt{\det(\gamma)}}. \tag{2.136}$$

One-mode normal decomposition

To decompose a state ρ means to determine the symplectic eigenvector (also known as *symplectic spectrum*) υ for the given covariance matrix γ. If the determinant is applied to Eq.(2.133) one can find:

$$\det(S\gamma S^T) = \det(\gamma) \tag{2.137}$$

$$= \det(\upsilon) = \prod_{k=1}^{N} \upsilon_k^2, \tag{2.138}$$

since the determinant is a symplectic invariant with $S = \mathbb{1}$. For the one-mode case where $N = 1$, one can find the eigenvalue υ_1 as the determinant of the 2×2 covariance matrix γ_1 of the single mode state:

$$\upsilon_1 = \sqrt{\det(\gamma_1)}. \tag{2.139}$$

Two-mode normal decomposition

The two-mode covariance matrix can be expressed as:

$$\gamma_{12} = \begin{bmatrix} \upsilon_1 & C_{12} \\ C_{12}^T & \upsilon_2 \end{bmatrix}, \tag{2.140}$$

with γ_1,γ_2 and C_{12} as 2×2 real matrices. To determine the symplectic eigenvalues υ_1 and υ_2 of υ_{12} of Eq.(2.140), a second symplectic invariant Δ is needed and is given by:

$$\Delta = \upsilon_1^2 + \upsilon_2^2 = \det(\gamma_1) + \det(\gamma_2) + \det(C_{12}) \tag{2.141}$$

With $\det(\gamma_{12}) = \upsilon_1^2\upsilon_2^2$ one can see that the symplectic eigenvalues are solutions of the second order polynomial:

$$A^2 - \Delta A + \det(\gamma_{12}) = 0 \tag{2.142}$$

which give the solution:

$$\upsilon_{1,2}^2 = \frac{1}{2}\left(\Delta \pm \sqrt{\Delta^2 - 4\det(\gamma_{12})}\right) \tag{2.143}$$

2.3.2 One-mode Gaussian state

One-mode Gaussian states are totally described by the displacement operator $d = (d_X, d_P)$ and a covariance matrix γ :

$$\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}. \tag{2.144}$$

Vacuum and coherent state:

The vacuum state is a state with a null mean value that is centered at the origin of phase space ($d = (0,0)$), its covariance matrix is the identity:

$$\gamma = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \mathbb{1}_2, \tag{2.145}$$

Coherent state is a displaced vacuum state characterized by a displacement vector $d = (d_X, d_P)$ $(d_X, d_P \neq 0)$ while its covariance matrix is same as vacuum state (Eq.(2.145)).

Squeezed state:

The *squeezed* coherent state, or *squeezed state* in short is generalized by displacing a squeezed vacuum state. The squeezed vacuum state has null mean value and is achieved by applying a squeezing operator $S(r)$ to the vacuum state $|0\rangle$:

$$S(r)|0\rangle = \frac{1}{\sqrt{\cosh(r)}} \sum_{n=0}^{\infty} \frac{\sqrt{(2n)!}}{2^n n!} \tanh^n(r)|2n\rangle, \tag{2.146}$$

in which r is a squeezing parameter. When $r > 0$, the quadrature $\hat{X}$ is squeezed which means the variance is less than the shot noise and the quadrature $\hat{P}$ is anti-squeezed; for $r < 0$, vise versa. The mean photon number of the squeezed vacuum state is $\sinh^2(r)$ which means the squeezed vacuum states contain photons. The covariance matrix of squeezed vacuum state and squeezed state is both given by:

$$\gamma = \begin{bmatrix} e^{-2r} & 0 \\ 0 & e^{2r} \end{bmatrix}, \tag{2.147}$$

Besides the covariance matrix, squeezed state is characterized by a displacement vector $d = (d_X, d_P)$ $(d_X, d_P \neq 0)$.

Thermal state and noisy coherent state:

The *thermal state* has a null mean $d = (0,0)$ and the covariance matrix is given by:

$$\gamma = \begin{bmatrix} V & 0 \\ 0 & V \end{bmatrix}, \tag{2.148}$$

in which V relates to the the mean number of photons $\bar{n}$ contained in the thermal state $V = 2\bar{n} + 1$. The vacuum can be considered as the case when no photon is contained $\bar{n} = 0$.

With a displacement vector $d = (d_X, d_P)$ $(d_X, d_P \neq 0)$ applied to the thermal state, one can obtain the *noisy coherent state* which is a noisy version of coherent state. At last, we summarize all the states mentioned above in Fig.2.5 represented in phase space.

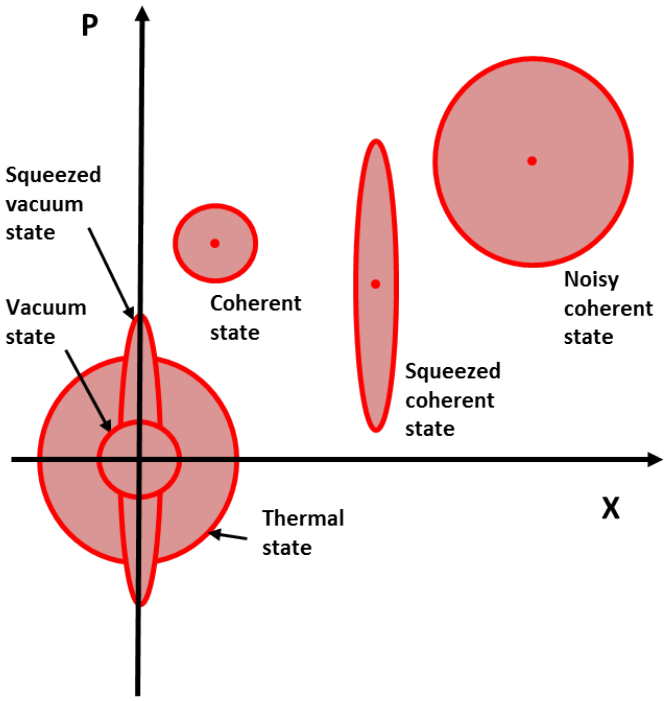


Fig. 2.5 One-mode Gaussian states in phase space, without displacement: vacuum state, squeezed vacuum state, thermal state; with displacement: coherent state, squeezed coherent state, noisy coherent state

2.3.3 Two-mode Gaussian state

A two-mode Gaussian state is characterized by a displacement vector $d = (d_{X_1}, d_{P_1}, d_{X_2}, d_{P_2})$ and a covariance matrix:

$$\gamma_{12} = \begin{bmatrix} \gamma_1 & C_{12} \\ C_{12}^T & \gamma_2 \end{bmatrix}, \tag{2.149}$$

One can trace out the two-mode Gaussian state to get one-mode Gaussian state which is characterized by the covariance matrix γ_1 and displacement $d = (d_{X_1}, d_{P_1})$. If $C_{12} = 0$ which means that there is no correlation between the two modes, then the covariance matrix γ_{12} can be expressed as a tensor products of one mode Gaussian states:

$$\gamma_{12} = \gamma_1 \oplus \gamma_2 \tag{2.150}$$

Two-mode squeezed state:

The two mode squeezed vacuum state plays an important role in CV quantum information processing such as CV QKD and teleportation, it is similar as the Bell state $1/\sqrt{2}(|00\rangle + |11\rangle)$ in qubit quantum information. Such similarity can be observed through the Fock basis

expansion of the two-mode squeezed vacuum state:

$$|\text{TMS}\rangle = \frac{1}{\cosh(r)} \sum_{n=0}^{\infty} \tanh^n(r)|n,n\rangle \tag{2.151}$$

The two-mode squeezed vacuum state has a null mean while the two-mode squeezed state is displaced with the vector $d = (d_{X_1}, d_{P_1}, d_{X_2}, d_{P_2})$. Their covariance matrices are both given by:

$$\gamma_{TMS} = \begin{bmatrix} \cosh(2r)\mathbb{1}_2 & \sinh(2r)\sigma_z \\ \sinh(2r)\sigma_z & \cosh(2r)\mathbb{1}_2 \end{bmatrix}, \tag{2.152}$$

in which the unity $\mathbb{1}_2$ is given in Eq.(2.145) and

$$\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{2.153}$$

Tracing the second mode of a two-mode squeezed vacuum results in a thermal state with its variance $\cosh(2r) = 2\bar{n} + 1$.

2.3.4 Gaussian operations

A Gaussian operation maps every Gaussian input state into a Gaussian output state. The interesting point of Gaussian operations is that it can be performed on Gaussian states through linear optical elements such as phase-shifters, beam-splitters, squeezers and displacements along with homodyne measurement. All these Gaussian operations are achievable with current technology. In chapter 4, we will see that various CV-QKD protocols can be realized through the Gaussian operations on the Gaussian states experimentally.

Any Gaussian unitary transformation corresponds to a symplectic operation $S \in \text{Sp}(2N, \mathbb{R})$ in phase-space. In particular, there is an unitary transformation U related to a real symplectic transformation such that the Weyl operators satisfies the relation:

$$U\hat{D}(\vec{\xi})U^{\dagger} = \hat{D}(S\vec{\xi}), \forall \vec{\xi} \in \mathbb{R}^{2N}. \tag{2.154}$$

In which $\hat{D}$ is the displacement operator which is defined in Eq.(2.96).

Displacement operator:

The displacement operation is a Gaussian operation since it doesn't change the covariance matrix but only changes the mean value of the Gaussian. A displacement operation $\hat{D}(z)$ change the mean values between the output and input state as $d_{out} = d_{in} + z$. Note that

the effect of the displacement operator is not limited to Gaussian states but can be more generally applied to non-Gaussian states.

Let us again focus on the symplectic transformation which corresponds to the unitary transformation U generated from a quadratic Hamiltonian The symplectic transformation implies the mapping between the output and input state:

$$\hat{u}_{out} = S\hat{u}_{in}. \tag{2.155}$$

Through the symplectic operation S, the covariance matrix and the displacement vector between the output and input state can be given by:

$$\gamma_{out} = S\gamma_{in}S^T, \tag{2.156}$$

$$d_{out} = Sd_{in}. \tag{2.157}$$

The symplectic operation S also preserves the canonical commutation relation:

$$S\Omega S^T = \Omega, \tag{2.158}$$

Passive transformations

As an important subset of symplectic transformations, *passive transformation* is formed by orthogonal symplectic transformation: $P(N) = S \in \mathrm{Sp}(2,\mathbb{R}) \bigcap \mathrm{O}(2N)$. These transformations correspond to phase shift and beam splitter operations. Any passive transformation over N modes can be divided into a set of these two operations. Passive transformations preserve the eigenvalues of the covariance matrix which means it keeps the total number of photons unchanged.

Phase Shift:

A phase shift is a single-mode operation which is characterized by a phase θ. It acts a rotation θ on the quadratures in phase space and the symplectic transformation $S_{ps}(\theta) \in \mathrm{Sp}(2,\mathbb{R})$ is given by:

$$S_{ps}(\theta) = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}. \tag{2.159}$$

Beam-splitter:

The beam-splitter operation is characterized by a transmittance T which combines two modes coherently. Its symplectic transformation $S_{bS}(\theta) \in \mathrm{Sp}(4,\mathbb{R})$ is given by:

$$S_{bs}(T) = \begin{bmatrix} \sqrt{T}\mathbb{1}_2 & \sqrt{1-T}\mathbb{1}_2 \\ -\sqrt{1-T}\mathbb{1}_2 & \sqrt{T}\mathbb{1}_2 \end{bmatrix}. \tag{2.160}$$

Active transformations

Unlike the passive transformations, *active transformations*, are another subset of the symplectic transformations that inject photons in the system.

Squeezing:

The symplectic transformation $S_{sq}(r) \in \mathrm{Sp}(2,\mathbb{R})$ of a single mode squeezing operation is given by

$$S_{sq}(r) = \begin{bmatrix} e^{-r} & 0 \\ 0 & e^{r} \end{bmatrix}, \tag{2.161}$$

with r as the squeezing parameter. It can be achieved by pumping a non-linear media with high intensity source using Optical Parametric Amplification (OPA).

For the two-mode squeezing transformation $S_{sq2}(r) \in \mathrm{Sp}(4,\mathbb{R})$, it is described by the squeezing parameter r, the symplectic matrix can be written as:

$$S_{sq2}(r) = \begin{bmatrix} \cosh(r)\mathbb{1}_2 & \sinh(r)\sigma_z \\ \sinh(r)\sigma_z & \cosh(r)\mathbb{1}_2 \end{bmatrix}, \tag{2.162}$$

Euler decomposition

Any Gaussian operation over N modes can be decomposed through Euler decomposition into a first passive transformation over all the N modes, followed by a single-mode squeezing operation for each mode, and a second passive transformation over all N modes. The Euler decomposition of any symplectic transformations $S \in \mathrm{Sp}(2,\mathbb{R})$ can be written as:

$$S = K \bigoplus_{k=1}^{N} \begin{bmatrix} e^{-r_k} & 0 \\ 0 & e^{r_k} \end{bmatrix} L, \tag{2.163}$$

in which $K, L \in P(N)$ are passive transformations. This decomposition provides a way to express any arbitrary symplectic transformations over N modes.

2.3.5 Entropy of Gaussian states

Von Neumann entropy

As we have seen in section 2.1.4, the concept of Shannon entropy is replaced to the one of differential entropy when continuous variables are encountered. A continuous-variable quantum system over N-mode is characterized by the density operator ρ as shown in Eq.(2.80). The Von Neumann entropy can be used on the continuous-variable quantum system, where it is defined as:

$$S(\rho) = -\mathrm{Tr}[\rho \log_2 \rho]. \tag{2.164}$$

$S(\rho)$ is a finite quantity since it is calculated over states with bounded energy. If ρ is diagonal through in the orthogonal basis $|i\rangle$:

$$\rho = \sum_i \lambda_i |i\rangle\langle i|. \tag{2.165}$$

Then the Von Neumann entropy is can be interpreted as the Shannon entropy of the eigenvalues distribution $\{\lambda_i\}$:

$$S(\rho) = H(\lambda). \tag{2.166}$$

Entropy of Gaussian states

At last we would like to determine the entropy of Gaussian states. The entropy is invariant under a displacement operation, so that the entropy of a Gaussian state is not related to its first moment. Thus for a N-mode Gaussian state ρ_g, its entropy is fully determined by its covariance matrix γ_g. Specifically, the Williamson theorem indicates that there exists a symplectic transformation S such that:

$$S\gamma_g S^T = \bigotimes_{k=1}^{N} \begin{bmatrix} \upsilon_k & 0 \\ 1 & \upsilon_k \end{bmatrix}, \tag{2.167}$$

with $\upsilon_k = 1, \cdots, N$ as the symplectic eigenvalues of the state. Based on the Williamson's theorem, the Gaussian state ρ_g can be mapped to a product of N thermal states through a unitary operation with the symplectic eigenvalues $\upsilon_k = 2\bar{n}_k$ where $\bar{n}_k$ is the mean photon

number in the mode k. So that one can have the entropy of a Gaussian state as:

$$S(\rho_g) = \sum_{k=1}^{N} S(\rho_t(\bar{n}_k)), \tag{2.168}$$

where $\rho_t(\bar{n}_k)$ is denoted as a single mode thermal with mean photon number $\bar{n}_k$ for the mode k. So that to generalize the entropy of a Gaussian state, one first needs to compute the Von Neumann entropy of a thermal state. The density matrix of a thermal state is known as:

$$\rho_t = \sum_{n=0}^{\infty} \frac{\bar{n}^n}{(\bar{n}+1)^{n+1}} |n\rangle\langle n|, \tag{2.169}$$

with $\bar{n} = \mathrm{Tr}[\rho n]$ as the mean photon number. The Von Neumann entropy of the state ρ_t can be computed:

$$S(\rho_t) = -\mathrm{Tr}[\rho_t \log_2 \rho_t] = -\frac{1}{\bar{n}+1} \sum_{k=0}^{\infty} \left(\frac{\bar{n}}{\bar{n}+1}\right)^k \log_2 \left[\frac{1}{\bar{n}+1}\left(\frac{\bar{n}}{\bar{n}+1}\right)^k\right] \tag{2.170}$$

$$= -\frac{1}{\bar{n}+1} \sum_{k=0}^{\infty} \left(\frac{\bar{n}}{\bar{n}+1}\right)^k [k\log_2(\bar{n}) - k\log_2(\bar{n}+1) - \log_2(\bar{n}+1)] \tag{2.171}$$

$$= (\bar{n}+1)\log_2(\bar{n}+1) - \bar{n}\log_2\bar{n}. \tag{2.172}$$

in which we have used the relation:

$$\sum_{k=0}^{\infty} kx^k = \frac{x}{(1-x)^2} \tag{2.173}$$

Chapter 3

Practical quantum key distribution

3.1 Quantum key distribution

Quantum Key Distribution (QKD) allows two remote parties, the sender Alice and the receiver Bob, to share a secret key. If an adversary, Eve, eavesdrops on the communication link, her action would unavoidably introduce disturbances, which would be noticed by Alice and Bob. A QKD protocol is designed, so that it aborts if Eve's disturbance is too high, in order to prevent Alice and Bob from accepting compromised keys. An attractive feature of QKD is that generated keys are truly random and can be continuously refreshed. Such properties are well suited to the requirements of OTP encryption protocol, where the keys must be perfect random and can not be reused, in order to achieve information-theoretic secure link encryption [8].

3.1.1 A generic QKD protocol

In order to precisely explain how QKD works, we first present a generic QKD protocol which can be applied for both discrete and continuous variables. A conceptual schematic of QKD is shown in Fig.3.1. There are mainly two stages in a QKD protocol: (1) *quantum communication*; (2) *classical post-processing*, which are carried through two communication channels, respectively: (1) *quantum channel*; (2) *classical channel*. In the following parts, we first present the two stages in QKD, then we describe the two channels that are involved.

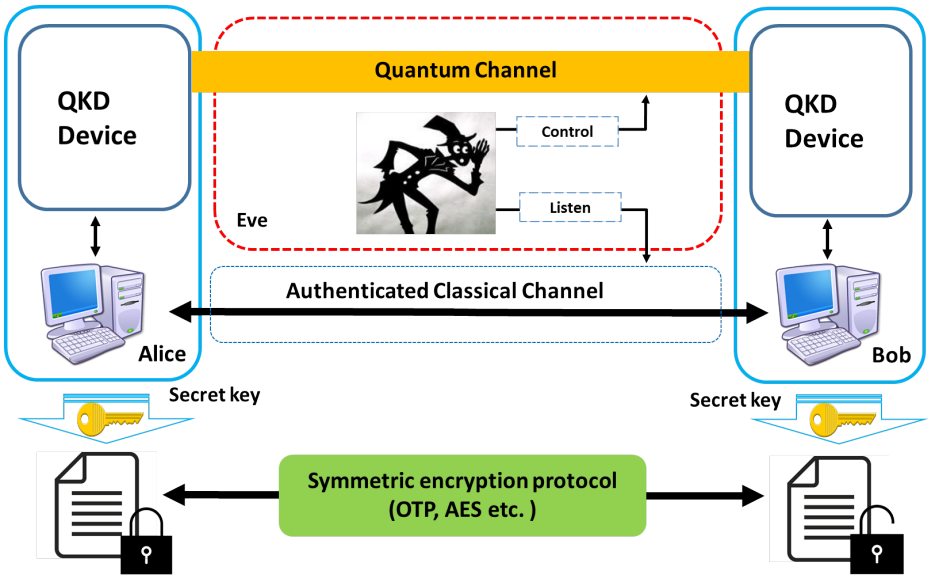


Fig. 3.1 QKD protocol.

Quantum communication

The first stage of a QKD protocol is quantum communication part, which can be described under a *prepared-and-measured* (P&M) scheme or a *entanglement-based* (E-B) scheme:

- P&M scheme: Alice encodes classical information on the quantum states, in particular, she encodes a classical random variable a on non-orthogonal quantum states. Alice then sends these quantum states through a communication channel to Bob, this channel is called quantum channel. At the output of the quantum channel, Bob measures the received quantum states to obtain a classical random variable b which is partially correlated with the random variable a of Alice. By repeating this process, Alice and Bob exchange a significant number of quantum states, and generate two sets of partially correlated data on each side. These two sets of data are called *raw key*.

- E-B scheme: Alice prepares a quantum bipartite states and measures one half of the state which enable her to obtain a classical random variable a. Meanwhile, such measurement projects the quantum bipartite states on a sub-system, on which Alice prepares the corresponding quantum states according to the particular protocol and sends them to Bob. Bob performs the measurements on the quantum states to extract a random variable b. From Bob's point of view, the measurement in EB scheme is same as in the P&M scheme. At the end, Alice and Bob actually share a bipartite

quantum systems described in $\mathscr{H}_A \otimes \mathscr{H}_B$.

In fact, under the P&M scheme Alice and Bob also virtually distribute bipartite quantum states. It has been proven that for any P&M protocol, there is a corresponding EB representation [85]. Such equivalence is often used in proving the security of QKD protocol, where the security proof for the EB protocol can be translated into the corresponding P&M protocol and vice versa.

Classical post-processing

After the quantum communication, Alice and Bob go into the second stage of a QKD protocol: classical post-processing, where they process their raw key by exchanging information over a classical channel. This stage consists of following steps: *sifting*, *parameter estimation*, *error correction* and *privacy amplification*.

1. Sifting: Alice and Bob exchange classical message to indicate which basis or quadrature has been used for the encoding or the measurement in the quantum communication protocol. The two parties then discard the part of the raw key in particular for which encoding and measurement basis are complementary while the key they keep is called the *sifted key*.

2. Parameter estimation: Alice and Bob compare a random subset of their sifted key and estimate their statistics to know different parameters of the quantum channel such as channel transmission and Quantum Bit Error Rate (QBER), QBER refers to the different fractions between Alice's and Bob's bit strings. Based on such parameter estimation , Alice and Bob can estimate the mutual information I_{AB} between their sifted key and compute an upper bound of information that is accessed by Eve for a given attack model. Concerning a particular security proof, if the upper bound of Eve's information is higher than Alice and Bob's mutual information, which means no secret key can be generated, then Alice and Bob abort the following key generation protocol .

3. Error correction (information reconciliation): After the sifting and parameter estimation, the remaining partially correlated key goes into this step. Alice and Bob want to agree on an identical bit string by using classical error correction techniques. Information reconciliation can consist of having Bob sharing a key identical to Alice data (direct reconciliation) or Alice sharing a key identical to Bob data (reverse reconciliation). After error correction, the partially correlated key of Alice and Bob becomes perfectly correlated but some information has leaked to Eve.

4. Privacy amplification: In this step, Alice and Bob process on the correlated key from previous step, in order to eliminate the information that Eve may have. In this step, the choice direct or reverse reconciliation plays an important role. Since the fraction of the key that need to be discard is based on the upper bound information of Eve which is computed in the parameter estimation for direct or reverse reconciliation with a given security proof. After removing the corresponding fraction of the key, Alice and Bob thus transform the correlated key which is partially known by Eve into a secret key which is fully unknown by Eve. Usually, this step is done by using two universal hashing functions.

Two channels

The two stages above of a QKD protocol involve two channels:

- Quantum channel: In the quantum communication part, the quantum channel is the transmission link between Alice and Bob which enables the two parties to exchange a series of quantum states. Eve can perform any actions that are allowed by physics to eavesdrop on the quantum channel, such as measuring or manipulating the states that Alice sends to Bob. In practical implementations, the physical form of the quantum channel can be an optical fiber link or free space.

- Classical channel: Unlike the quantum communication over the quantum channel, the classical post processing over the classical channel must be authenticated which means that Eve is allowed to listen to the classical channel but not allowed to manipulate the messages between Alice and Bob in the classical channel. In order to achieve a secure authentication channel, it requires an initial secret key which is shared by Alice and Bob. The authentication key can be later refreshed from the key generated by QKD after the first round of QKD . In this sense, QKD grows the initial secret keys from short ones into long ones, rather than creating secret keys from nothing. Another important observation of the classical channel is that the different steps of classical post-processing are involved in one-way or two-way classical communication. One-way communication means that one party sends classical information to another one and receive no feedback from the other side. Two-way communication means that two parties both send and receive information bidirectionally. As we mentioned about the step of error correction and privacy amplification that are carried through one way communication from Alice to Bob (forward) or Bob to Alice (backward), which corresponds to direct or reverse reconciliation. The two-way classical communication consists of both backward and forward communication while the steps of

sifting, parameter estimation and post-selection are involved in the two-way classical communication. In practical implementations, the classical channel can be any classical communication links such as Ethernet.

3.1.2 Security of a key in QKD

Intuitively, one would define the security of a key, which is also a measurement of QKD security. Recently, the universal definition of security was given by Renner [148], and it is characterized by the distance between a perfect key and the output key S generated by a realistic protocol. A perfect key means the key shared by Alice and Bob is identical, perfectly random distributed and secure (Eve has no knowledge). According to [148], in a realistic QKD protocol, the joint state of the eavesdropper's quantum system and the key S can be expressed as:

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

In which key S is a random variable with a probability distribution $p_S(s)$ and eavesdropper's state is described by the density matrix ρ_E^s in the Hilbert space $\mathscr{H}_E$ given that $S = s$ (Eve's knowledge on the key S). $|s\rangle$ is an orthonormal basis of the key S in Hilbert space $\mathscr{H}_S$. Then one can define the security of a key : S is ε-secure with respect to $\mathscr{H}_E$ if

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

where ρ_E is any state of Eve and $\rho_s = \sum_{s\in S} \frac{1}{|S|}|s\rangle\langle s|$ is a mixed state in $\mathscr{H}_S$. This illustrates that if a QKD protocol is ε secure, then the keys shared by Alice and Bob are identical, truly random, and independent from the Eve's knowledge except with a small probability ε. A typical value of ε is 10^{-10} which provides sufficient security for the cryptographic purposes [9, 149].

QKD is usually combined with other cryptographic protocols and one would concern the security of the whole cryptographic scheme instead the security of QKD alone. The notion of "composable security" can be then introduced. As shown in [9, 149] QKD can be proven to be composably secure in the security framework defined by Renner [148]. It means in particular if we consider a set of cryptographic protocols (involving QKD), where each of them is ε_i-secure, then as a whole set of protocol is also ε-secure with a security parameter $\sum \varepsilon_i$.

3.1.3 Security model of QKD

Once the security of a key is defined, one can deduce the security proofs of QKD, which give the expression of the secret key rate. In order to prove the security of QKD, one needs to consider certain attack models. In this subsection, we briefly present three types of attacks that are considered in the security proofs of QKD: individual attack, collective attack and coherent attack. Each attack corresponds to a level of Eve's capability. As we shall see security proofs are valid against attacks that are not necessary limited by current technologies but only by quantum physics. On the other hands, the validity of the security proofs also relies on certain assumptions. Thus in the following parts, we will first list the assumptions which are necessary for the security proofs. Then we will classify the different attack models that are considered in QKD security proofs.

Assumptions

Although QKD security can be established independently of computational assumptions, there still are several assumptions need to be satisfied, in order to apply security proofs. We will consider in the following part, only device-dependent QKD that applies to existing practical system.

1. Eve's power is limited by the laws of physics, she can perform any actions on the quantum channel which are allowed by quantum mechanics.

2. The classical channel must be authenticated which means that Eve is allowed to listen to the classical channel but not allowed to modify the messages exchanged between Alice and Bob on the classical channel.

3. Alice's and Bob's devices are considered as safe boxes, where Eve has no access.

4. The hardware of Alice and Bob must function properly and Eve should not have influence on them. (As we will see, this assumption can be hard to be achieved in practice while the violation of this assumption can often lead to a security break.)

5. The random number generators which are used by Alice and Bob need to be truly random which means that the produced random variable can not be predicted.

These requirements are essential for the validity of the security proofs, any violation of any assumptions above could compromise the security of QKD.

Classification of attacks and secret key rates

Based on the operations carried out by Eve, there are three types of attacks that are usually considered in QKD:

- Individual attack: Eve interacts each pulse sent by Alice with an individual ancilla and stores the resulting state of the ancilla in a quantum memory. Eve then measures her ancillas in the appropriate basis after Bob reveals his measurement choice (sifting step). The maximum information that Eve can get on Bob's key is limited by the classical mutual information (Shannon rate in section 2.1.2) I_{BE} (reverse reconciliation) or I_{AB} (direct reconciliation), which is deduced from the Csiszár–Körner bound [22]. After the one way processing, the secret key rate under the individual attack for reverse reconciliation can be expressed as:

$$K_{Individual} = I_{AB} - I_{BE}, \tag{3.3}$$

  in which I_{AB} is the mutual information between Alice's and Bob's ray keys. The secret key rate can be expressed in the analogous way for I_{AE} in the case of direct reconciliation.

- Collective attack: Eve interacts each pulse sent by Alice with an individual ancilla and stores the state of a long block ancilla in a quantum memory until the end of the classical post processing. Then she measures coherently all ancilla with a quantum computer to optimize her information on the block. It is proven by Devetak and Winter [24] that the Eve's information under collective attack (reverse reconciliation) is bounded by Holevo quantity χ_{BE} (Devetak-Winter bound). This Holevo quantity [54] χ_{BE} is given as:

$$\chi_{BE} = S(\rho_E) - \sum_b p(b) S(\rho_{E|b}), \tag{3.4}$$

  in which S is Von Neumann entropy which is defined in section 2.3.5, b is a symbol of Bob's alphabet with $p(b)$ as its probability distribution, $\rho_{E|b}$is the state of Eve's ancilla and $\rho_E = \sum_b p(b)\rho_{E|b}$ is Eve's partial state. Given with Holevo bound [24], we can express the secret key rate under the collective attack for reverse reconciliation with χ_{BE}:

$$K_{Collective} = I_{AB} - \chi_{BE}. \tag{3.5}$$

  And similar for χ_{AE} in the case of direct reconciliation.

- Coherent attack: Eve interacts a pre-entangled multi-pulse ancilla with all pulses exchanged by Alice and Bob. She stores the state of the ancilla in a high-dimensional

quantum memory until the end of the classical post processing. She then measures coherently the ancilla with a quantum computer to optimize her information on the key. Coherent attack is the most powerful attack that is allowed by quantum physics, which is also known as general attack.

3.2 Implementations of QKD: Discrete variable vs continuous variable

There are mainly two approaches to perform QKD in order to generate secret keys: discrete variable QKD (DV-QKD) and continuous variable (CV) QKD, which divides QKD into two families. The important difference between DV and CV QKD lie in the detection part: DV QKD uses single photon detection techniques while CV QKD uses coherent detection techniques.

In this section, we briefly compare DV QKD with CV QKD from the views of implementations. More detailed information on CV QKD can be found in Chapter 4.

Discrete variable

In DV QKD, Alice encodes information with discrete variables such as the phase or the polarization states of single photons. To measure the information, Bob typically uses a single photon detector.

The first and best known DV-QKD protocol is BB84 [11]. In the implementation of the BB84 protocol, it requires perfect single photon sources to meet the assumptions in the security proofs. However in practice, efficient single photon sources are difficult to realize and in most implementations of BB84, weak coherent pulses (WCPs) are used instead, in which the same quantum state may be encoded on more than one photon. The use of WCPs allows Eve to launch the so-called photon number splitting attack (PNS) [59] which imposes to reduce the mean photon number sent by Alice and therefore reduces the distribution length of QKD. Fortunately, the decoy state methods [99, 178] was introduced to beat down the PNS attack, which largely increases the practical performance of DV-QKD in terms of distance and key rate. Regarding to the detection parts, InGaAs avalanche photodiode (APD) are commonly used at telecom wavelengths which are well suit for fiber optics communications. Recently, new technologies, such as self-differencing APD [26], sine-wave gating APD [96, 189] and superconducting nanowire single photon detectors (SNSPDs) [117] have been developed and can improve DV-QKD performance significantly.

Table 3.1 Differences between DV-QKD and CV-QKD.

	DV-QKD	CV-QKD
Source	Single photon source Attenuated coherent laser	Weak modulated coherent laser Squeezed laser
Detector	Single photon detectors	Homodyne detectors
Telecom wavelength	Yes	Yes
Compatibility with WDM	Yes [30, 129, 130]	DWDM friendly [80, 138]
Parameter estimation	QBER	Excess noise and channel loss
Security proof	Arbitrary attack for BB84 [154]	Arbitrary attack for Gaussian protocols [92]
Finite analysis	Yes [172]	Yes [91, 92]

Continuous variable

In CV QKD, information is encoded with continuous variables such as the phase and the amplitude of an electromagnetic field in an infinite dimensional Hilbert space. Alice uses a weak coherent laser for encoding while Bob uses a coherent detection (homodyne or heterodyne detection) to measure the quadratures of the received states. Homodyne detection is a mature technology from optical communications. More information of homodyne detection can be found in section 5.1. In principle, the bandwidth of off-the-shelf homodyne detectors can reach 10 GHz with the electronic noise 10 dB less than the shot noise [28, 61]. The use of homodyne detection can offer another advantage to CV-QKD where the noises in different optical modes can be effectively suppressed. As we will see in Chapter 9, such characteristic will further enable CV-QKD compatibility with dense wavelength division multiplexing (DWDM). In fact, an appealing feature of CV-QKD is that one can implement it fully with off-the-shelf components from telecom industry. A brief history of CV-QKD is presented in the next chapter, which includes presentations of the security proofs and of the implementations.

We have summarized the differences between DV-QKD and CV-QKD in Table.3.1. Interested readers can refer to the technical reviews of QKD in [44, 154] and recent developments of QKD in [101].

Chapter 4

Continuous variable quantum key distribution protocols and security proofs

QKD can be realized with a discrete encoding of classical information onto quantum states of light. The information can for example be encoded in the phase or polarization of single photon states, that can be discriminated with single photon detectors. Continuous-variable (CV) QKD protocols, in which light carries continuous information such as the value of the quadrature of a coherent state or a squeezed state, have been proposed as another option to realize QKD. In this chapter, we present several QKD protocols relying on continuous variable encodings.

We first present a review of the development of CV QKD, presenting both the experimental and theoretical progress in this domain. We then introduce the main protocol investigated in the thesis, the Gaussian Modulated Coherent State (GMCS) protocol [48, 50]. We will also present some other CV QKD protocols such as no-switching protocol [179] and discrete modulation protocol [87, 167, 195]. Finally, we present a brief sketch of the security of CV QKD protocols. For more details on this topic, one can refer to the additional references [44, 154, 182].

4.1 Introduction: An overview of CV QKD

QKD protocols using continuous-variables were first proposed in 1999, based on a discrete modulation of Gaussian states [53, 145, 146]. In 2001, squeezed states protocol based on a continuous (Gaussian) modulation of squeezed states was introduced by Cerf et al. [14]. The idea of Gaussian modulation was soon extended to the coherent states, where Gaussian modulated coherent state (GMCS) protocol [48] was proposed by Grosshans and

Grangier in 2002, thus it is also known as GG02. In the following year, GMCS protocol was implemented with homodyne detection [50]. Instead of using homodyne detection, another coherent state protocol called no-switching protocol was later proposed by Weedbrook et al. [179, 180] and implemented by Lance et al. [82], in which heterodyne detection is used, allowing to operate Bob passively (i.e with no active switching between quadrature measurement). In order to reach longer transmission, reverse reconciliation [50] and post-selection [161] had been introduced to overcome the 3 dB loss limits inherent to coherent state protocols with direct reconciliation. In order to further extend the secure range of CV QKD, multidimensional reconciliation method was proposed by Leverrier et al. [90] and improved by Jouguet et al. [63] for error correction codes with small signal noise ratio (SNR). All these protocols can be considered as Gaussian protocols except post-selection, in which Alice modulates input quadrature with Gaussian modulations, while Bob performs measurement with homodyne or heterodyne detection.

Other than Gaussian modulation protocols, two-way quantum communication protocol [134] and an improved discrete modulation protocol [87] have been later proposed, which have shown the possibility to further improve the transmission range. Weedbrook et al. [181, 183] have also proposed a CV QKD protocol using wavelengths in the microwave regime. Microwave CV QKD would be adapted for exchange secret keys over short distances, although not yet implemented. Recently, the concept of measurement device independent (MDI) [100] has been introduced in CV QKD, where MDI CV QKD protocols with coherent states [95, 113] and with squeezed [94, 193] have been proposed. Such MDI CV QKD protocols are still in an early stage and not yet implemented.

From a practical implementation point of view, GMCS protocol is probably the most mature CV QKD implementation among different CV QKD protocols. GMCS protocol have been realized with stander telecommunication fiber [34, 64, 103, 137] for distances from 5 km to 25 km, including one field test [34] in SECOQC [1] network [8, 131] and another one with classical symmetric encryption system running up to 6 months [64]. Recently, thanks to progress in reconciliation [90] and error correction code [63], GMCS QKD has been demonstrated over 80 km of standard telecom fiber system in lab environment [68].

The activities devoted to study discrete modulation CV QKD protocols are less and the progress have been comparatively slower. Ever since the first discrete modulation CV QKD protocols [53, 145, 146] have been invented, several protocols based on phase encoding have been proposed [52, 119, 122], the main difference of these protocols lie in the number of the prepared coherent states and their positions in the phase space. However, whether the

[1] Secure Communication based on Quantum Cryptography: An European project of Sixth Framework Programme from 1.4.2004 to 10.10.2008 (www.secoqc.net).

optimal attack against such protocols are Gaussian or not is not clear, limiting the generality of the security to be derived [87]. Recently, a generalized protocol has been introduced by Sych and Leuchs [167] which has a general description of different discrete modulation CV QKD protocols. Implementation of discrete modulation CV QKD have been demonstrated also with telecom fibers over a 24 km channel distance [25] and with 10 dB loss of the channel [159].

Regarding to the security proof of CV QKD, Gottesman and Preskill [46] have given the first security proof in CV QKD using squeezed states. For the Gaussian modulation protocols, the security proofs against individual Gaussian attacks were first given by Cerf et al. [14], Grosshans and Grangier [48] for the direct reconciliation and by Grosshans et al. [50] for the reverse reconciliation. Individual Gaussian attacks are further proven as the optimal attack among all collective attacks [47] which covers all the Gaussian and non Gaussian attacks. With the proof that Gaussian attacks are optimal among collective attacks against Gaussian modulation CV QKD, the security proof of CV QKD against collective attacks can be derived [38, 88, 123]. All these collective Gaussian attacks have been fully characterized by Pirandola et al. [133]. Regarding the coherent attack or general attack, by using the exponential de Finetti theorems [147] or the post-selection technique [20], one can reduce a general attack to a collective attack and the security of Gaussian protocol against general attack is proved. It is important to notice that all these security proofs mentioned above are considered in the asymptotic regime, where the finite-size effects and the composable security proof are not included. Finite-size effects have been partially studied in [91], under the assumption of Gaussian attack. Leverrier et al. [92] has then proved the security of CV QKD using coherent states against arbitrary attacks in the finite-size regime. Recently, the composable security proof has been given for a CV QKD protocol with squeezed states [36, 37] and it has been implemented in [41]. More recently, Leverrier [86] has proved the composable security for CV QKD with Gaussian-modulated coherent states.

4.2 Gaussian modulated coherent state protocol

We first start by presenting Gaussian modulated coherent state (GMCS) protocol, which uses the Gaussian modulated quadratures of coherent states to encode information and a homodyne detection to perform the measurement. Then we present an typical implementation of the GMCS protocol as well as the Gaussian linear model that describes the quantum channel in the GMCS protocol. In the end, we briefly present the parameter estimation and related finite size effect.

4.2.1 Protocol

We present here the GMCS protocol without assuming a specific implementation for both direct [48] and reverse protocol[50]. Each step in the generic QKD protocol (section 3.1.1) now becomes more specific. The GMCS protocol consists of two stages: (1) quantum communication with coherent states; (2) classical post-processing with direct or reverse reconciliation. The protocol starts with quantum communication over the quantum channel:

1. Preparation (1): Alice generates $2N$ random numbers $X_{i=1\ldots N}$, $P_{i=1\ldots N}$. Each N random numbers of $X_{i=1\ldots N}$ or $P_{i=1\ldots N}$ are prepared according to a centered normal Gaussian distribution with a variance V_A.

2. Preparation (2): Alice prepares the coherent states $|X+iP\rangle$ with the coordinates of quadratures X and P as $(X_i,P_i)_{i=1\ldots N}$ in the phase space, she then sends these coherent states through the quantum channel.

3. Measurement: Bob generates N random binary numbers $b_{i=1\ldots N}$ and for each pulse $i=1\ldots N$ performs a homodyne detection to measure either X or P quadrature based on the random bit b_i. From the measurements, Bob thus obtains N classical random variables $y_{i=1\ldots N}$.

After the quantum communication, Alice and Bob perform the classical post-processing tasks using the authenticated classical channel:

1. Sifting: Bob reveals Alice the values of random bit $b_{i=1\ldots N}$ about his choice on the quadrature measurement through a public authenticated channel. Alice thus keeps approximately N values of the $2N$ values in $(X_i,P_i)_{i=1\ldots N}$ with respect to Bob's choice of quadrature. These values are known as Alice's data: $x_{i=1\ldots N}$ (different from the quadrature coordinates X_i). So Alice and Bob share a sequence of N correlated classical variables $(x_i,y_i)_{i=1\ldots N}$.

2. Parameter estimation (1): Alice selects randomly a subset of $M<N$ values from the N correlated variables in the previous step. She reveals the M values to Bob as well as their index in the sequence, so that the two parties both select the same random subset data $(x_j,y_j)_{j=1\ldots M}$.

3. Parameter estimation (2): The subset $(x_j,y_j)_{j=1\ldots M}$ will be used to estimate the parameters which characterize the quantum channel: channel transmission T and excess noise ξ. Based on these two values and Alice's variance V_A, Alice and Bob can further estimate the mutual information I_{AB} between them and the upper bound of Eve's

information χ_{AE} for direct reconciliation or χ_{BE} for reverse reconciliation. If I_{AB} is smaller than χ_{AE} or χ_{BE}, it means Eve can have more information than Alice and Bob, and the key generation protocol aborts (no key is output).

4. Error correction (information reconciliation): Based on the estimation of I_{AB}, the two parties choose appropriate binary functions to convert the remaining classical values $(x_k, y_k)_{k=1...N-M}$ into two bits strings on each side. For the reverse reconciliation, Bob sends Alice a syndrome as the reference for Alice to estimate Bob's measurements. By selecting a proper error correction code, Alice can compute a correct value to estimate Bob's measurements thus correct the errors. For the direct reconciliation, the procedure is inversed where Alice sends a syndrome to Bob where Bob performs estimations in order to correct errors.

5. Privacy amplification (1): In case of reverse reconciliation, based on the estimation of Eve's knowledge χ_{BE} in the step 2-3 and the length of the bit strings after the error correction (step 4), Alice can computes the length l of secret key which they can distill from the common bit string shared by the two parties. For the direct reconciliation, Bob compute the length l of secret key based on χ_{AE}.

6. Privacy amplification (2): Alice (reverse reconciliation) or Bob (direct reconciliation) creates a random hashing function to transform the $N-M$ bit string into a l bits string and sends the description of the hashing function through the public authenticated channel to the other party. Alice and Bob both apply this function to their own bit string so that the two parties obtain identical bit strings with a length l, which is known as a secret key.

4.2.2 Implementation

A typical implementation of the GMCS protocol is shown in Fig. 4.1 [68]. On Alice side, she generates 100 ns wide pulses from a continuous-wave distributed feedback laser emitting at 1550 nm with an integrated electro-optics modulator. A repetition rate of 500 kHz is considered in [34, 68, 103]. With the help of a 99/1 beam splitter, these pulses are then split into a strong phase reference pulse (with a typical photon number of 10^8) known as local oscillator (LO), and a weak signal (few photons). With the help of a phase modulator and a amplitude modulator, the signal is continuously modulated to place the coherent states in the complex plane (quadratures X and P) with a two-dimensional Gaussian distribution centered on zero. In order to limit the crosstalk between the LO pulse and the signal pulse, these pulses are multiplexed in time and polarization, where a Faraday mirror delay line

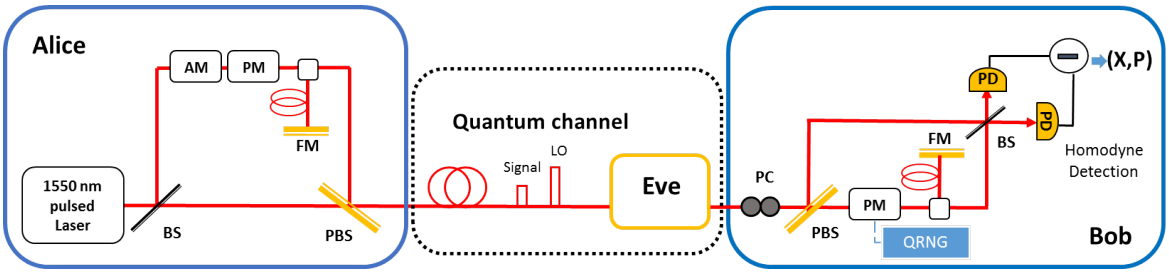


Fig. 4.1 Implementation of GMCS protocol. AM, amplitude modulator; PM, phase modulator; FM, Faraday mirror; PBS, polarization beam splitter; PC, polarization controller; PD, photodetector; and BS beam splitters; QRNG, quantum random number generator.

(typical length: 40 m) is added on the signal path. A Faraday mirror is used at the end of the delay line so that polarization of signal is rotated by 90 degree. Hence the polarizations of signal pulse and the LO pulse on the quantum channel are orthogonal. At the output of Alice, polarization beam splitter (PBS) is used to combine the signal and LO path. Alice sends both the modulated signal pulse and LO pulse through a single fiber to Bob.

At the reception side, a polarization controller is placed at the input of Bob device to adjust the polarizations of received signal and LO pulses. A PBS is followed to separate the signal pulse and LO pulse into signal path and LO path respectively. At the LO path, a phase modulator is added to enable Bob to apply a phase $\varphi = 0$ or $\varphi = \pi/2$ to measure X or P quadrature. In order to measure the quadratures X or P randomly, a quantum random number generator is required to produce truly random bits. A Faraday mirror with 40 m delay is set right after the phase modulator in order to compensate the delay between the signal pulse and LO pulse. The polarization of the LO pulse is rotated by 90 degree to coincide with the polarization of the signal pulse after being reflected on a Faraday mirror. Finally, the signal pulse interferes with the LO pulse on a balanced homodyne detection, since they are in the same spatial-temporal mode. As we shall see in section.5.1, the output of homodyne detection is proportional to the quadrature values.

4.2.3 The Gaussian linear model

In order to further explain the security of the GMCS protocol, we now go into the detail of the quantum communication part over the quantum channel (P&M scheme). As mentioned in section 4.1, the optimal attack for Eve has been proven as Gaussian attack among both individual [40, 47] and collective attacks [38, 123]. Thus we can assume that Eve interacts on a Gaussian channel on which Alice and Bob exchange their quantum states. With the optimality of the Gaussian attack, the communication model between Alice and Bob can therefore be characterized by the Gaussian linear model and can be described by

an AWGNC (see section.2.1.3). The Gaussian linear channel is characterized by two parameters: channel transmission (T) between Alice and Bob and a noise factor known as the excess noise (ξ). The channel transmission is related to the channel loss, it can be derived directly from the correlation between Alice and Bob's data. The excess noise is the noise variance in excess of the shot noise, which can be due to imperfections of devices (i.e modulator, detector, electronics etc.) or Eve's actions on the channel.

In the preparation stage, Alice encodes the continuous variables X_A and P_A (both sampled from a centered Gaussian modulation of variance V_A) onto a coherent state (the results could be described by measuring the optical quadratures with a homodyne detection):

$$\begin{aligned} X &= X_A + X_0 \\ P &= P_A + P_0, \end{aligned} \tag{4.1}$$

where X_0 and P_0 are quadratures of the vacuum state whose variance is one unit of shot noise (N_0). Since the vacuum state is independent of the modulation, the cross term $\langle X_A X_0 \rangle$ is equal to zero. X_A and X_0 are both centered so their mean values are both zero. At the output of Alice, the variance of the quadrature X is [2]:

$$\begin{aligned} V &= \langle X^2 \rangle - \langle X \rangle^2 \\ &= \underbrace{\langle X_A^2 \rangle}_{V_A} + \underbrace{\langle X_A X_0 \rangle}_{\text{null}} + \underbrace{\langle X_0 X_A \rangle}_{\text{null}} + \underbrace{\langle X_0^2 \rangle}_{N_0} - \underbrace{\langle X_A \rangle^2}_{\text{null}} - \underbrace{\langle X_0 \rangle^2}_{\text{null}} \\ &= V_A + N_0 \end{aligned} \tag{4.2}$$

V is the variance of the quadratures of the optical states sent by Alice which includes the modulation variance V_A and the shot noise N_0. Alice sends the coherent states through the quantum channel which is noisy and lossy.

After going through the transmission channel, the excess noise and vacuum noise due to loss will add on the state of Alice at the output of channel: Bob's station. On Bob side, he performs a homodyne detection whose output is proportional to the quadrature value with an efficiency η (see section.5.1). In practice, the homodyne detection also has some electronic noise due to the electronic circuits. The electronic noise is modeled as a thermal state with a variance v_{ele}. The output state of Bob's homodyne measurement for quadrature X on the received state thus reads out:

$$X_B = \sqrt{\eta T}(X_A + X_0 + X_{\text{ex}}) + \sqrt{1 - \eta T} X_0' + X_{\text{ele}}. \tag{4.3}$$

[2] Since the treatment for the quadrature P is totally symmetric with X, we only look at the X quadrature for simplicity.

In which η is the efficiency of the homodyne detection, X_{ele} is the state of electronics noise(variance v_{ele}). η and v_{ele} are two values which are calibrated before the QKD protocols. X_{ex} is the quadrature variable of excess noise (variance ξ). The sources of excess noise can arise from different phenomena: technical noises due to various imperfections of Alice and Bob's devices, Eve's action on the quantum channel. Since the excess noise must be compared to the signal variance at the input of the channel, the excess noise variance (ξ) we consider here is actually brought back to the input of the channel which is on Alice side. In this thesis, if we don't mention specifically otherwise, the expression of the excess noise is always refereed to Alice side. X_0' is a vacuum state associated with the loss of the transmission channel (T) and the detector efficiency (η) with a variance of N_0.

Since the vacuum states X_0 and X_0' are independent from the other states, the variance of Bob can be thus directly deduced from Eq.(4.3):

$$\begin{aligned} Var(X_B) &= \langle (X_B - \langle X_B \rangle)^2 \rangle = \eta T (V_A + N_0 + \xi) + (1 - \eta T) N_0 + v_{\text{ele}} \\ &= \eta T (V_A + N_0 + \underbrace{\frac{1-\eta T}{\eta T} N_0}_{\text{Noise due to the loss}} + \underbrace{\xi + \frac{v_{\text{ele}}}{\eta T}}_{\text{Total excess noise}}) \end{aligned} \tag{4.4}$$

From Eq.(4.4), we can see that there are two parts of noise contribution on the state of Bob: noise due to the loss of the channel and the detector efficiency $\frac{1-\eta T}{\eta T} N_0$; total excess noise including added excess noise ξ and electronic noise $\frac{v_{\text{ele}}}{\eta T}$. All these noises are considered to be brought to Alice side.

As we can see from Eq.(4.4), the noise contribution due to the channel loss and the detector efficiency loss are mixed. In the so called "realistic model" [103], one assumes that Eve can not go inside Bob's device and in particular that Eve can not influence the calibrated value of η and v_{ele}. In this model, one can moreover separate the noise contribution which are added at different stages: (1) the added noise on the open channel; (2) the noise due to the loss of Bob's detector and its electronic noise. The latter part is considered as trusted noises source on which Eve has no access. The application of the realistic model requires to calibrate the values of η and v_{ele} beforehand. More discussion about calibration and its influence on the QKD security can be found in [85].

In fact, Bob's detector can be modeled as a beam splitter with transmission η, due to the loss of the detector, one more vacuum state X_0'' adds on the received state of Bob, which turns Eq.(4.3) into:

$$X_B = \sqrt{\eta T}(X_A + X_0 + X_{\text{ex}}) + (\sqrt{\eta}\sqrt{1-T}X_0' + \sqrt{1-\eta}X_0'') + X_{\text{ele}}. \tag{4.5}$$

From Eq.(4.5), we can further deduce the variance of Bob quadrature measurements:

$$\begin{aligned} Var(X_B) &= \eta T(V_A + N_0 + \xi) + \eta(1-T)N_0 + (1-\eta)N_0 + v_{\text{ele}} \\ &= \eta T(\underbrace{V_A + N_0}_{V} + \underbrace{\frac{1-T}{T}N_0 + \xi}_{\chi_{ch}}) + \eta(\underbrace{\frac{1-\eta}{\eta}N_0 + \frac{v_{\text{ele}}}{\eta}}_{\chi_{hom}}) \\ &= \eta T(V + \chi_{ch}) + \eta\chi_{hom}. \end{aligned} \tag{4.6}$$

The total variance of Bob in Eq.(4.6) is same as in Eq.(4.4), but we can separate the contributions from the channel line χ_{ch} and from Bob's detection χ_{hom}. χ_{ch} consists in the noise due to the loss of the channel $\frac{1-T}{T}N_0$ and the added excess noise ξ which are both brought back to Alice side. χ_{hom} consists in the noise due to the loss of the detector $\frac{1-\eta}{\eta}N_0$ and the electronics noise of detector $\frac{v_{\text{ele}}}{\eta}$, where these two noises are brought to the input of Bob's device. We can now express the total noise on Alice side that adds to the initial state prepared by Alice:

$$\chi_{tot} = \chi_{ch} + \frac{\chi_{hom}}{T}, \tag{4.7}$$

in which the factor $\frac{1}{T}$ indicates that the noise χ_{hom} is brought back to the input of the channel. We can thus express the variance of Bob quadrature measurements as:

$$Var(X_B) = \eta T(V + \chi_{tot}), \tag{4.8}$$

where χ_{tot} is the total added noise. Eq.(4.8) shows that the variance of Bob can be interpreted as the sum of the initial variance of Alice's quadrature and the noise added through a lossy and noisy channel. When we consider that the shot noise unit N_0 as 1, then all the values are normalized in shot units. The covariance matrix of the state shared by Alice and Bob can be thus expressed as:

$$\Gamma_{AB} = \begin{bmatrix} V \cdot \mathbb{1}_2 & \sqrt{\eta T(V^2-1)}\sigma_z \\ \sqrt{\eta T(V^2-1)}\sigma_z & \eta T(V + \chi_{tot}) \cdot \mathbb{1}_2 \end{bmatrix}, \tag{4.9}$$

in which $\mathbb{1}_2$ and σ_z are given in Eq.(2.145) and Eq.(2.153).

4.2.4 Parameter estimation

So far, we have presented the quantum communication part in the GMCS protocol under the assumption of the Gaussian linear model. In the following, we will present the classical post-processing part. First, a subset of the sifted data is used to proceed to parameter estimation. This step is essential for the security of the protocol, since it estimates the chan-

nel transmission and the excess noise which fully characterize the quantum channel in the Gaussian linear model. Based on these estimations, Alice and Bob can further quantify the mutual information between their data, and estimate the upper bound of Eve's information for direct or reverse reconciliation, which can further be used to determine whether a secret key can be generated.

In order to estimate channel transmission T and excess noise ξ from Alice and Bob's correlated variables, we consider the Gaussian linear model between Alice and Bob as we have presented in the previous subsection. This model can be rewritten as followed, where an additive Gaussian noise is added on the initial quadratures prepared by Alice:

$$X_B = tX_A + X_N. \tag{4.10}$$

In Eq.(4.10), $t = \sqrt{\eta T}$, T is the channel transmission and η is the Bob's efficiency. On Alice side, X_A is a Gaussian random variable centered on zero with variance V_A. X_N is the total noise which follows a centered normal distribution with variance $\sigma_N^2 = N_0 + \eta T\xi + v_{\text{ele}}$. This variance includes shot noise N_0, excess noise ξ and electronic noise of Bob v_{ele}.

In order to compute the covariance matrix of the state shared by Alice and Bob, one need to estimate parameters such as the variance of Alice's and Bob's data, $Var(X_A)$ and $Var(X_B)$, and the correlation between Alice and Bob, $Cov(X_A, X_B)$. We obtain the following equations relating measured data to parameter estimation :

$$Var(X_A) = \langle (X_A - \langle X_A \rangle)^2 \rangle = \langle X_A^2 \rangle = V_A, \tag{4.11}$$

$$Var(X_B) = \langle (X_B - \langle X_B \rangle)^2 \rangle = V_B = \underbrace{\eta T}_{t} \underbrace{V_A}_{\langle X_A^2 \rangle} + \underbrace{N_0 + \eta T\xi + v_{\text{ele}}}_{\sigma_N^2}, \tag{4.12}$$

$$Cov(X_A, X_B) = \langle X_A X_B \rangle - \langle X_A \rangle \langle X_B \rangle = \langle X_A X_B \rangle = \sqrt{\eta T} V_A. \tag{4.13}$$

Here in Eq.(4.12), the expression of Bob's variance is equivalent to the one in Eq.(4.4) or Eq.(4.6), σ_N^2 is the total noise variance on Bob's side. It includes the shot noise N_0, the excess noise on Bob side $\eta T\xi$ and the electronic noise of the detector v_{ele}.

Additionally, in order to evaluate the shot noise N_0, Bob needs to perform an additional measurement, he can for example close the signal port so he can measure the variance when the input signal is vacuum. When there is no signal impinging on the homodyne detection, the variance of homodyne detection can be used to calibrate the shot noise value. In this case Eq.(4.10) reduces to $X_{B_0} = X_{N_0}$. Here X_{N_0} follows a centered normal distribution with

variance $\sigma^2_{N_0} = N_0 + v_{\text{ele}}$. Shot noise measurement thus allows to have one more equation:

$$Var(X_{B_0}) = N_0 + v_{\text{ele}}. \tag{4.14}$$

As we have mentioned before, η and v_{ele} are calibrated values, measured before launching the QKD protocol. If we don't consider the finite size effect [91] and assume that all the estimations are in their asymptotic values, the total loss coefficient ηT can be thus estimated by Eq.(4.13):

$$t = \eta T = \frac{\langle X_A X_B \rangle}{Var(X_A)}. \tag{4.15}$$

And the estimation of channel transmission T and excess noise ξ can be deduced from equation Eq.(4.11)-Eq.(4.13):

$$T = \frac{\langle X_A X_B \rangle^2}{\eta Var(X_A)^2}, \tag{4.16}$$

$$\xi = \frac{Var(X_B)}{\eta T} - Var(X_A) - \frac{N_0}{\eta T} - \frac{v_{\text{ele}}}{\eta T}. \tag{4.17}$$

By knowing N_0 (Eq.(4.14)), all variances and correlations can be normalized in shot noise units and can then be used to estimate the mutual information between Alice and Bob, and the upper bound of Eve's information. Thus Alice and Bob can estimate the secret key rate that they can generate.

Finite size effect in parameter estimation

So far we have described the parameter estimation in asymptotic regime, assuming infinite quantity of exchanged data is available. In practice, due to the finite resource for the quantum communication, the parameter estimation is carried out with data of finite block size, where only finite number of data is exchanged. Here we briefly present the finite size effect of parameter estimation in GMCS protocol which has been studied in [65, 91]. The full finite size analysis should also include the secret key rate [91], but here we only focus on the parameter estimation part.

We consider Alice and Bob use a set of correlated variables $(x_j, y_j)_{j=1\ldots M}$ to perform parameter estimation, where x and y are two variables with a finite number quantity M which represent the variables of X_A and X_B in asymptotic limit, x also follows a centered normal distribution with a variance of V_A. The relation between x_j and y_j can be also described by

the Gaussian linear model (Eq.(4.10)):

$$y_j = t x_j + z_j. \tag{4.18}$$

In which $z_{j=1...M}$ is a variable that describes the added noise state X_N (Eq.(4.10)), z follows a centered normal distribution with unknown variance $\sigma_N^2 = N_0 + \eta T \xi + v_{\text{ele}}$. As the analysis in [91] shows, $\hat{t}$ and $\hat{\sigma}^2$ can be estimated through Maximum-Likelihood method [118], for the Gaussian linear model and their estimations are following:

$$\hat{V}_A = \frac{1}{M}\sum_{j=1}^{M} x_j^2, \tag{4.19}$$

$$\hat{t} = \frac{\sum_{j=1}^{M} x_j y_j}{\sum_{j=1}^{M} x_j^2}, \tag{4.20}$$

$$\hat{\sigma}_N^2 = \frac{1}{M}\sum_{j=1}^{M} (y_j - \hat{t} x_j)^2. \tag{4.21}$$

Here the total noise variance $\hat{\sigma}_N^2$ is estimated instead of Bob's variance. It is equivalent to the parameter estimation setup as we show previously (Eq.(4.11)-Eq.(4.13)), since Bob's variance is the summation of the noise variance and Alice's variance. The precisions of each estimation depend on M, that is the number of samples used.

In order to calibrate the shot noise N_0, another set of correlated variables $(x_{0_j}, y_{0_j})_{j=1...M'}$ can be collected when the signal input is vacuum, where $y_{0_j} = z_{0_j}$ and z_0 follows a centered normal distribution with unknown variance $\sigma_0^2 = N_0 + v_{\text{ele}}$. Similar to the previous estimators, $\hat{\sigma}_0^2$ can be estimated by Maximum-Likelihood method:

$$\hat{\sigma}_0^2 = \frac{1}{M'}\sum_{j=1}^{M'} {y_0}_j^2. \tag{4.22}$$

Besides the number of samples, the precision of shot noise N_0 depends also on the estimation of electronic noise Δv_{ele}, which is calibrated before the QKD protocol. The estimators $\hat{V}_A$, $\hat{t}$, $\hat{\sigma}^2$ and ${\hat{\sigma}_0}^2$ are independent with their distributions as:

$$\hat{t} \sim \mathcal{N}\left(t, \frac{\sigma_N^2}{\sum_{j=1}^{M} x_i^2}\right), \tag{4.23}$$

$$\frac{M\hat{V}_A}{V_A}, \frac{M\hat{\sigma}_N^2}{\sigma_N^2} \sim \chi^2(M-1), \tag{4.24}$$

$$\frac{M'{\hat{\sigma}_0}^2}{\sigma_0^2} \sim \chi^2(M'-1). \tag{4.25}$$

In which t, V_A, σ^2 and σ_0^2 are the real values of the parameters (mean values of each distribution). The estimation $\hat{V}_A$, $\hat{t}$, $\hat{\sigma}^2$ and ${\hat{\sigma}_0}^2$ can thus have some deviations to their real values. With large but finite numbers M and M', one can compute the uncertainty part of each parameter estimation:

$$\begin{aligned} &\Delta t = z_{\varepsilon_{PE}/2}\sqrt{\frac{\hat{\sigma}_N^2}{M V_A}}, \Delta\sigma_N^2 = z_{\varepsilon_{PE}/2}\frac{\hat{\sigma}_N^2\sqrt{2}}{\sqrt{M}}, \\ &\Delta\sigma_0^2 = z_{\varepsilon_{PE}/2}\frac{{\hat{\sigma}_0}^2\sqrt{2}}{\sqrt{M'}}, \Delta V_A = z_{\varepsilon_{PE}/2}\frac{\hat{V}_A\sqrt{2}}{\sqrt{M}} \end{aligned} \tag{4.26}$$

By quantifying the uncertainty part of each estimator, Alice and Bob can make sure that the parameter estimation is between its lower and upper bound with a high probability $1-\varepsilon_{PE}/2$. For example, the estimation of loss coefficient is in its confidence interval $[\hat{t}-\Delta t, \hat{t}+\Delta t]$. In Eq. (4.26), $z_{\varepsilon_{PE}/2}$ is the solution of the relation $1-\mathrm{erf}(z_{\varepsilon_{PE}/2}/\sqrt{2})/2 = \varepsilon_{PE}/2$, where $\mathrm{erf}(x) = \frac{2}{\sqrt{\pi}}\int_0^x e^{-t^2}dt$ is the error function and ε_{PE} is the probability that the estimated parameter does not belong to its confidence interval with a typical value $\varepsilon_{PE} = 10^{-10}$.

As we can observe in Eq. (4.26), with the increasing number of the samples used to compute the estimator, the uncertainty of the estimator decrease which will lead to an increase of the estimation's precision. The estimation of channel transmission $\hat{T}$ and excess noise $\hat{\xi}$ can be deduced from Eq.(4.19)-Eq. (4.21)

$$\hat{T} = \frac{\hat{t}^2}{\eta}, \tag{4.27}$$

$$\hat{\xi} = \frac{\hat{\sigma}_N^2 - \hat{\sigma}_0^2}{\hat{t}^2}, \tag{4.28}$$

where the confidence intervals of these two estimations can be referred to the previous estimators. In order to know a tight upper bound of Eve's information (Eve's information is maximum), one expects a worst case estimation of $\hat{T}$ and $\hat{\xi}$, where $\hat{T}$ is at its minimum value while ξ is at its maximum value (section 7.3). It further requires that $\hat{t}$ and $\hat{\sigma}_0^2$ are at their minimum values: $t_{min} = \hat{t} - \Delta t$ and $\sigma_{0_{min}}^2 = \hat{\sigma}_0^2 - \Delta\sigma_0^2$ while $\hat{\sigma}_N^2$ is at its maximum value $\sigma_{N_{max}}^2 = \hat{\sigma}_N^2 + \Delta\sigma_N^2$. The finite size effect of parameter estimation is unavoidable in practice, Alice and Bob should always consider the worst case of estimations to ensure the security of the secret key generation.

4.3 No-switching protocol

In no-switching protocol, Alice also uses the Gaussian modulation of coherent states to encode information [179, 180], where the state preparation stage is equivalent to the one in the GMCS protocol. Compared to the GMCS protocol, the main difference of the no-switching protocol are lying on Bob side and on the classical processing part, which are following:

- In the quantum communication part, the difference lies in the measurement step of Bob: instead of measuring randomly the quadratures X or P, Bob measures the two quadratures simultaneously with a heterodyne detection, where the heterodyne detection consists two homodyne detections. Bob thus doesn't need to generate a random bit in order to randomly switch between the two bases.

- In the classical post-processing part, the sifting step is no longer needed, since the X and P quadratures are simultaneously measured so Alice and Bob don't need to discard the values in wrong bases. Alice and Bob can thus have $2N$ correlated classical variables $(x_i, y_i)_{i=1...2N}$ to further distill secret keys through direct or reverse reconciliation. The available correlated data for the classical post processing is thus 2 times of the one in GMCS protocol which can leads a higher key rate generation. However, 3 dB noise is added on the data when one uses a heterodyne detection, which will lower the secret key rate.

4.3.1 Implementation

In the implementation of no-switching protocol, on Alice side, the setup is same as the one in GMCS protocol. On Bob side, the quantum random number generator and the phase modulator on the LO path are no longer needed compared to the implementation of GMCS protocol. On the other hand, an additional homodyne detection is required to realize a full heterodyne detection. A typical setup of no-switching protocol is shown in Fig.4.2. On the classical post-processing part, except the shifting step is omitted, the remaining steps are same as the step 2-6 in GMCS protocol. Thus error correction code used for GMCS protocol can be also applied on no-switching protocol.

Due to the use of heterodyne detection, no-switching protocol is also known as heterodyne protocol. In fact, the idea of using heterodyne detection can be extended to all the other CV QKD protocols.

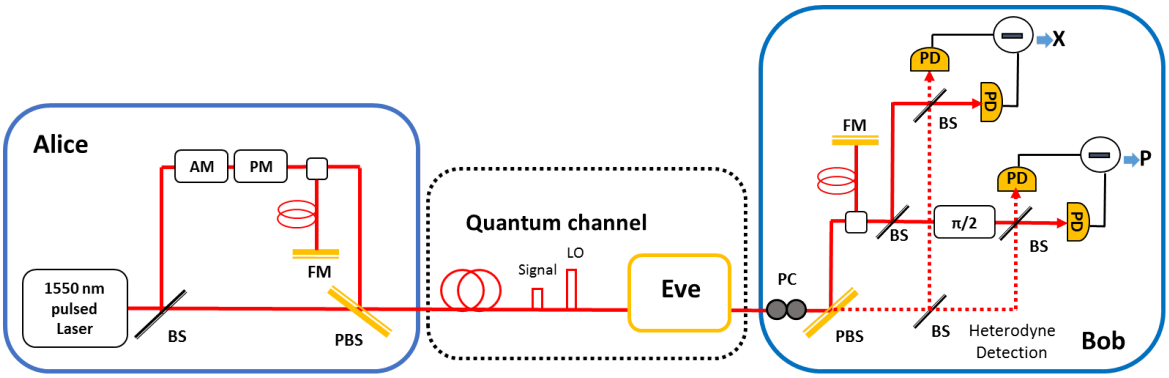


Fig. 4.2 Implementation of no-switching protocol. AM, amplitude modulator; PM, phase modulator; FM, Faraday mirror; PBS, polarization beam splitter; PC, polarization controller; PD, photodetector; and BS beam splitters; $\pi/2$: phase shift; dotted line in Bob: signal path; solid line in Bob: LO path.

4.4 Discrete modulation CV QKD protocol

As we have mentioned in the section 4.1, the first CV QKD protocols were based on the discrete modulation of Gaussian states [53, 145, 146]. In this section, we first present the representative discrete modulation CV QKD protocols: binary modulation [195], four-state [87] and multi-letter protocol [167], where we focus mainly on the quantum communication part. Then we briefly compare the discrete modulation protocols with the Gaussian modulation protocols from the views of implementations and security proofs.

4.4.1 Protocols

Binary modulation protocol

The binary modulation protocol is studied in [195], and its equivalent entanglement-based scheme is BB92 protocol [10]. The protocol starts with quantum communication over the quantum channel:

1. Preparation (1): Alice prepares the states $|\alpha\rangle$ and $|-\alpha\rangle$, which are two coherent states with same amplitude but opposing phase. The reference frame is chosen such that the signal are modulated in X quadratures.

2. Preparation (2): Alice randomly sends $|\alpha\rangle$ or $|-\alpha\rangle$ with equal probability. If $|\alpha\rangle$ is sent, Alice stores a classical variable $x = 1$, while if $|-\alpha\rangle$ is sent, she stores $x = 0$. Alice thus obtains a sequence of classical random variables x.

3. Measurement: Bob generates a random binary number b and performs a homodyne

detection to measure either X or P quadrature based on the random bit b. From the measurements, Bob thus obtains a sequence of classical random variables y.

After the quantum communication, Alice and Bob perform the classical post-processing over the classical channel. Like Gaussian modulation protocols, the shared classical variables (x,y) can be processed through direct or reverse reconciliation to become secret keys. In particular, the classical variables will also go through the sifting, parameter estimation, error correction and privacy amplification. But the main difference is that the data where Bob measures the P quadrature is public announced and is used to estimate Eve's interference. In the sifting step, Alice and Bob dismiss all the data when Bob chooses to measure the P quadrature.

Four state protocol

Now we present for the four-state protocol [87]. The quantum communication of the four-state protocol can be described as:

1. Preparation (1): Alice prepares a series of random number $k = 0,1,2,3$ with equal probability as her classical random variables x.

2. Preparation (2): Alice prepares the corresponding coherent states $|\alpha_k\rangle = ae^{(2k+1)i\pi/4}$ with same amplitudes a and sends them through the quantum channel.

3. Measurement: Bob randomly measure either X or P quadrature by performing a homodyne detection. Through the measurements, Bob wants to reveals the sequence of k, where he obtains a sequence of classical random variables y.

After the quantum communication, Alice and Bob proceed direct or reverse reconciliation to convert the bits strings into secret keys.

Multi-letter protocol

In discrete modulation CV QKD protocol, the preparation states can be actually increasing to an arbitrary number N. The multi-letter protocol [167] can be seen as a general protocol to describe various discrete modulation CV QKD protocols. The quantum communication of the multi-letter protocol can be expressed as:

1. Preparation (1): Alice prepares a series of random number $k = 1 \ldots N$ with equal probability as her classical random variables x.

2. Preparation (2): Alice prepares the corresponding coherent states $|\alpha_k\rangle = ae^{(2k+1)i\pi/N}$ with same amplitudes a and sends them through the quantum channel.

3. Measurement (1): Bob measures X and P quadrature simultaneously by performing a heterodyne detection. The results of the measurements are β_X and β_P which can be considered as a pure coherent state $|\beta\rangle = |\beta_X + i\beta_P\rangle$.

4. Measurement (2): Bob looks for a state α_p which is the closest alphabet's state to the state β where $|\langle\alpha_p|\beta\rangle|^2 = \max_k|\langle\alpha_k|\beta\rangle|^2$. So that he can attributes a classical number p to the measured state β as his variable y.

After the quantum communication, Alice and Bob proceed direct or reverse reconciliation to convert the classical variables x and y into secret keys.

4.4.2 Discrete modulation vs Gaussian modulation CV QKD

In the quantum communication part, discrete modulation protocols are simpler to implement experimentally compared to Gaussian modulation protocols, since they only need phase modulation to encode information, the amplitude modulator on Alice side is not needed. Same as Gaussian protocols, discrete modulation protocols also require homodyne or heterodyne detection on Bob side. In the classical post preprocessing part, the reconciliation problem of discrete modulation protocols can be treated by a model of binary channel with additive noise, for which there exist high efficiency error correction codes such as low-density parity-check codes [150]. Good error correction codes available for discrete modulation protocols also imply that such protocols have potentials to reach long distance for secure key distribution. On the other side, for Gaussian protocols, it has been shown that multidimensional reconciliation methods [90] at low SNR can not reach very high efficiency. Until recently, Jouguet et al. [63] has also developed high efficiency error correction codes at low SNR [63], which enables long distance key distribution for GMCS protocol [68].

For the security proofs, as mentioned in section 4.1, the optimality of Gaussian attacks has not yet been proven valid for discrete modulation CV QKD protocols, where security proofs with optimal Gaussian attacks can not apply to discrete modulation cases [38, 88, 123, 147]. Nevertheless, according to [87], an important observation shows that at low modulation variances of a four-state protocol, the four state modulation has a good approximation to the Gaussian modulation. Consequently, one can prove the security of four-state protocol by using the Gaussian upper bound (less tight) of Eve's information provided in [38]. Moreover, Leverrier and Grangier [89] have proposed a decoy state method

with four state modulation in order to approximate to the Gaussian modulation. Therefore, with such modulation scheme, the authors prove its security against the collective attack, and theoretically such protocol can generate secret keys over 50 km even if the finite size effect is considered.

4.5 Security proof of CV QKD

In this section, we will present the security proof of CV QKD. We focus on the main topic of this thesis: GMCS protocol with reverse reconciliation. Note that we neglect all the finite size effects, which means the numbers of N and M in section 4.2.1 are large enough (but M is a negligible small amount compared to N) so that the secret key rate approaches its asymptotic limit.

We first describe a entanglement based (EB) CV QKD scheme (Fig.4.3) which is a useful tool to study the security proof. Then we will present the secret key rate formulas for individual and collective attacks in the asymptotic limit.

4.5.1 Entanglement based CV QKD scheme

In order to further present secret key rates under different attack models, we first describe a unified EB CV QKD scheme (Fig.4.3), where different Gaussian protocols can be described by it [38–40, 49]. In this EB scheme (Fig.4.3), on Alice side, she first prepares a two-mode squeezed vacuum state (EPR state AB_0) with null mean value $d = (0,0)$ and its covariance matrix is described by:

$$\Gamma_{AB_0} = \begin{bmatrix} V \cdot \mathbb{1}_2 & \sqrt{V^2-1} \cdot \sigma_z \\ \sqrt{V^2-1} \cdot \sigma_z & V \cdot \mathbb{1}_2 \end{bmatrix}. \tag{4.29}$$

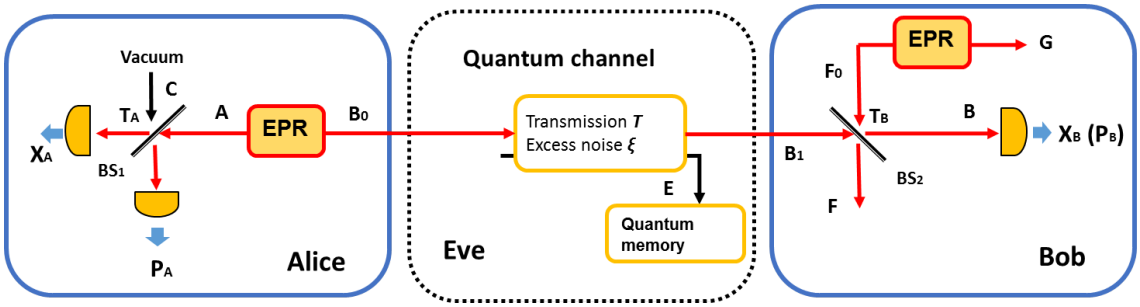


Fig. 4.3 Entanglement-based representation of Gaussian protocols with realistic model of the detector.

In which $V = V_A + 1$ is the variance of a thermal state with shot noise unit N_0 as 1. Alice then measures one half of the state AB_0: mode A, which is mixed with a vacuum mode through a beam splitter (BS_1) with transmission T_A. Alice's measurements output the quadrature (X_A, P_A) and project mode B into a Gaussian state, whose covariance matrix is given by [40]:

$$\Gamma_{B_0}^{X_A,X_B} = \begin{bmatrix} \frac{\mu V+1}{V+\mu} & 0 \\ 0 & \frac{V+\mu}{\mu V+1} \end{bmatrix}. \tag{4.30}$$

in which $\mu = (1-T_A)/T_A$, and its mean value is expressed as:

$$d_{B_0}^{X_A,X_B} = (\frac{\sqrt{T_A(V^2-1)}}{T_A V + (1-T_A)} X_A, \frac{\sqrt{(1-T_A)(V^2-1)}}{(1-T_A)V + T_A} P_A). \tag{4.31}$$

As we can see the projection of mode B is actually a squeezed state who is displaced by a bivariate Gaussian distribution. The value of T_A corresponds to the choice of Alice's detection and the state that mode B projects. If $T_A = 1$, Alice performs a homodyne detection on either X or P of mode A, which projects the mode B_0 onto squeezed states. For example, if Alice measures quadrature X, the connivance matrix and the mean of the projected state are given as:

$$\Gamma_{B_0}^{X_A} = \begin{bmatrix} 1/V & 0 \\ 0 & V \end{bmatrix}, \tag{4.32}$$

$$d_{B_0}^{X_A} = (\sqrt{1-V^2} X_A, 0). \tag{4.33}$$

This Gaussian state is actually a X-squeezed vacuum state displaced along the X quadrature with a amount of $\sqrt{1-V^2}X_A$. Alice can also prepare the corresponding P-squeezed vacuum state by measuring the quadrature P of mode A. Such state preparation exactly agrees with the P&M scheme in the squeezed states protocol [14].

If $T_A = 1$, Alice performs a homodyne detection which projects the mode B_0 onto squeezed states. If $T_A = 1/2$, Alice performs a heterodyne detection on both X and P of mode A, which projects the mode B_0 onto coherent states. The connivance matrix and the mean of the projected state are given as:

$$\Gamma_{B_0}^{X_A,X_B} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \tag{4.34}$$

$$d_{B_0}^{X_A,X_B} = (\sqrt{2\frac{V-1}{V+1}}X_A, \sqrt{2\frac{V-1}{V+1}}P_A). \tag{4.35}$$

It actually describes a coherent state whose quadrature values of X and P are given by $\sqrt{2(V-1)/(V+1)}X_A$ and $\sqrt{2(V-1)/(V+1)}P_A$ respectively. By using $Var(X_A) = (V+1)/2$, we can calculate the variance of this coherent state:

$$Var(X_{B_0}) = 2\frac{V-1}{V+1}\frac{V+1}{2} = V-1 = V_A. \tag{4.36}$$

This corresponds exactly to the state preparation in the GMCS protocol (P&M scheme) [48] as we have seen in section 4.2.3.

The projected state is then sent to Bob through the quantum channel, where Eve performs eavesdropping, it allows her to have a state E. On Bob side, he performs a homodyne ($T_B = 1$) or a heterodyne ($T_B = 1/2$) detection which corresponds to the transmission of the beam splitter (BS_2), $T_B = 1$ or $T_B = 1/2$. In such case, if the detection is assumed to be perfect which means $\eta = 1$ and $v_{ele} = 0$. Bob thus obtains the quadrature X_B and P_B through his measurements.

In fact, EB scheme can also be used to describe the realistic P&M model, where Bob's detector is modeled by a beam splitter with a transmission ηT_B, where η is the efficiency of the detector. Here we particular focus on the case of homodyne detection where $T_B = 1$. The electronics noise of the detector is modeled by a thermal state F_0 which enter the other input of the beam splitter (BS_2), the variance of F_0 is $V_N = 1 + v_{ele}/(1-\eta)$. In order to simplify the calculation, the state F_0 is considered to be obtained from a two-mode squeezed state F_0G with its variance V_N. After Bob's homodyne projective measurement, it would result the quadrature X_B and the system AFG.

4.5.2 Secret key rate under different attack models

In this subsection, we will present the secret key rate formulas under the individual attack [50] and collective attack [38, 123] for GMCS protocol with reverse reconciliation in the asymptotic limit. For both of the two attacks, we consider the realistic model (Eq.(4.7)) [103] which means Eve has no accessible information on χ_{hom}. Here we take the shot noise N_0 as 1 unit so that all variances are expressed in shot noise units.

Individual attacks

Under individual attacks, the secret key rate can be expressed as:

$$K_{Individual} = \beta I_{AB} - I_{BE}, \tag{4.37}$$

where β is the reconciliation efficiency with a value between 0 and 1 which depends on the error correction code. I_{AB} is the mutual information between Alice and Bob. I_{BE} is the upper bound of the mutual information between Bob and Eve, in the case of reverse reconciliation. For direct reconciliation, the considered quantity is the mutual information between Alice and Eve I_{AE}. I_{AB} and I_{BE} can be both deduced from Shannon formulas which have been introduced in Chapter 2. The communication model between Alice and Bob is based on the AWGNC as shown in section.4.2.3, which allows to compute I_{AB}. Eve performs her measurements between the sifting and the error correction step, where her knowledge is limited to the Shannon information in her ancilla: I_{BE} between her measurement results and Bob's data.

Let us first look at the mutual information I_{AB}, which can be directly deduced from Eq.(2.53). The SNR quantifies the mutual information, in which the "signal" is Alice's modulation variance V_A and the "noise" is the total noise χ_{tot} that is brought back to Alice side.

$$I_{AB} = \frac{1}{2}\log_2(1+\mathrm{SNR}) = \frac{1}{2}\log_2(1+\frac{V_A}{1+\chi_{tot}}) = \frac{1}{2}\log_2\frac{V+\chi_{tot}}{1+\chi_{tot}}. \tag{4.38}$$

In order to calculate I_{BE}, we can use Eq.(2.43):

$$I_{BE} = \frac{1}{2}\log_2\frac{V_B}{V_{B|E}}. \tag{4.39}$$

Thus this problem turns into calculating the conditional variance $V_{B|E}$ while the variance of Bob V_B is known Eq.(4.8) In the realistic model, we consider state B_1 is at the output of the channel where $V_{B|E}$ consists the conditional variance $V_{B_1|E}$ and χ_{hom}:

$$V_{B|E} = \eta V_{B_1|E} + \eta\chi_{hom}. \tag{4.40}$$

The corresponding quadrature X_{B_1} at the output of the channel is actually an estimation of the quadrature X_A sent by Alice with some errors:

$$X_{B_1} = tX_A + X_{NA}. \tag{4.41}$$

In which $V_{B_1|A} = Var(X_{NA})$. One the other hand Eve measures the state B_1 which gives her

quadrature P_E with some errors:

$$P_{B_1} = \lambda P_E + P_{NE}. \tag{4.42}$$

In which $V_{B_1|E} = Var(P_{NA})$. The commutation relation between X_{NA} and P_{NE} can be expressed as:

$$\begin{aligned}
[X_{NA}, P_{NE}] =& [X_{B_1} - tX_A, P_{B_1} - \lambda P_E] && (4.43)\\
=& [X_{B_1}, P_{B_1}] - \lambda [X_{B_1}, P_E] - t[X_A, P_{B_1}] + t\lambda [X_A, P_E] && (4.44)\\
=& [X_{B_1}, P_{B_1}] = 2iN_0, && (4.45)
\end{aligned}$$

in which commutations between two quadratures of different modes are zero. With this commutation relation $[X_{NA}, P_{NE}] = 2iN_0$, one can further express the uncertainty relation:

$$V_{B_1|A} V_{B_1|E} = Var(X_{NA}) Var(P_{NE}) \geq N_0^2. \tag{4.46}$$

In order to calculate $V_{B_1|A}$, one can use the covariance matrix Γ_{AB_1} of the state shared by Alice and the state B_1:

$$\Gamma_{AB_1} = \begin{bmatrix} V \cdot \mathbb{1}_2 & \sqrt{T(V^2-1)} \cdot \sigma_z \\ \sqrt{T(V^2-1)} \cdot \sigma_z & T(V + \chi_{ch}) \cdot \mathbb{1}_2 \end{bmatrix}. \tag{4.47}$$

By using Eq.(2.42), $V_{B_1|A}$ can be expressed as:

$$\begin{aligned}
V_{B_1|A} =& Var(X_{B_1}) - \frac{\langle X_A X_{B_1} \rangle}{\langle X_A^2 \rangle} && (4.48)\\
=& T(V + \chi_{ch}) - \frac{T(V^2-1)}{V} && (4.49)\\
=& T(\frac{1}{V} + \chi_{ch}). && (4.50)
\end{aligned}$$

Now one can inject Eq.(4.50) and Eq.(4.46) into Eq.(4.40) to find the lower bound of $V_{B|E}$:

$$V_{B|E} = \eta V_{B_1|E} + \eta \chi_{hom} \geq \eta \left[\frac{1}{T(\frac{1}{V} + \chi_{ch})} + \chi_{hom} \right]. \tag{4.51}$$

Hence the upper bound of Eve's information can be derived from V_B (Eq.(4.6)) and $V_{B|E}$

(Eq.(4.51)):

$$I_{BE} = \frac{1}{2}\log_2 \frac{T^2(V+\chi_{tot})(\frac{1}{V}+\chi_{ch})}{1+\chi_{hom}T(\frac{1}{V}+\chi_{ch})}. \tag{4.52}$$

Collective attacks

Under collective attacks, the secret key rate can be expressed as:

$$K_{Collective} = \beta I_{AB} - \chi_{BE}, \tag{4.53}$$

in which I_{AB} has been derived for the case of individual attacks (Eq.(4.38)), while the upper bound of Eve's information is given by the Holevo quantity [148]:

$$\chi_{BE} = S(\rho_E) - \int p(X_B) S(\rho_E^{X_B}) dX_B. \tag{4.54}$$

X_B is Bob's measurement output with its probability distribution $p(X_B)$, $\rho_E^{X_B}$ is Eve's state conditional on X_B. $S(\rho)$ stands for the von Neumann entropy of the state ρ [24]. In section.2.3.5, we have given the expression of a n mode Gaussian state's entropy, one can rewrite Eq.(2.168) such that:

$$S(\rho) = \sum_k g\left(\frac{\upsilon_k - 1}{2}\right), \tag{4.55}$$

with υ_k as the symplectic eigenvalues of the covariance matrix which characterizes ρ, and function $g(x)$ is defined as:

$$g(x) = (x+1)\log_2(x+1) - x\log_2 x \tag{4.56}$$

Since Eve's state E is a purifying system of state AB_1 (Fig.4.3), so that $S(\rho_{AB_1}) = S(\rho_E)$. Bob's homodyne measurement outputs X_B and the system $AEFG$ is pure (Fig.4.3), one can deduce that $S(\rho_{AFG}^{X_B}) = S(\rho_E^{X_B})$ and $S(\rho_{AFG}^{X_B})$ is independent of X_B for Gaussian protocols. Then χ_{BE} turns into:

$$\chi_{BE} = S(\rho_{AB_1}) - S(\rho_{AFG}^{x_B}). \tag{4.57}$$

Thus, the calculation of χ_{BE} converts into calculating the symplectic eigenvalues of ρ_{AB_1} and $\rho_{AFG}^{X_B}$. The covariance matrix of ρ_{AB_1} is given by Eq.(4.47). By using Eq.(2.143) of two

mode decomposition (section.2.3.1), one can find the symplectic eigenvalues of Γ_{AB_1}:

$$\upsilon_{1,2}^2 = \frac{1}{2}\left[\Delta_1 \pm \sqrt{\Delta_1^2 - 4D_1}\right], \tag{4.58}$$

In which

$$\Delta_1 = V^2(1-2T) + 2T + T^2(V+\chi_{ch})^2, \tag{4.59}$$

$$D_1 = \det(\Gamma_{AB_1}) = T^2(V\chi_{ch}+1)^2. \tag{4.60}$$

In order to find the covariance matrix of $\rho_{AFG}^{x_B}$, we first describe the matrix of the system AB_1FG (Fig.4.3):

$$\Gamma_{AB_1FG} = \Gamma_{AB} \oplus \Gamma_{F_0G}^{EPR}. \tag{4.61}$$

Based on the equation above, we want to further express the matrix of the system $ABFG$ which requires a model for Bob's detector. A beam splitter transformation $S_{B_1F_0}^{beam}$ can be used to model the efficiency η of Bob's detector and F_0, a thermal state, models the electronic noise of the detector v_ele. By considering such model, the matrix of $ABFG$ is given by:

$$\Gamma_{ABFG} = Y^T[\Gamma_{AB} \oplus \Gamma_{F_0G}^{EPR}]Y \tag{4.62}$$

with $Y = \left(\mathbb{1}_A \oplus S_{B_1F_0}^{beam} \oplus \mathbb{1}_G\right)$. One can then rearrange the lines and columns of the matrix Γ_{ABFG} which gives:

$$\Gamma_{AFGB} = \begin{bmatrix} \Gamma_{AFG} & \sigma_{AFG;B}^T \\ \sigma_{AFG;B} & \Gamma_{B}. \end{bmatrix} \tag{4.63}$$

The state $\rho_{AFG}^{x_B}$ is obtained after Bob's homodyne measurement on the system $AFGB$, such projection gives the covariance matrix of $\rho_{AFG}^{x_B}$:

$$\Gamma_{AFG}^{x_B} = \Gamma_{AFG} - \sigma_{AFG;B}^T(X\Gamma_B X)^{\mathrm{MP}}\sigma_{AFG;B}, \tag{4.64}$$

where $X = diag(1,0,0,0)$ and MP stands for the Moore Penrose inverse of a matrix. One can calculate directly the symplectic eigenvalues of $\Gamma_{AFG}^{x_B}$ which gives

$$\upsilon_{3,4}^2 = \frac{1}{2}(\Delta_2 \pm \sqrt{\Delta_2^2 - 4D_2}). \tag{4.65}$$

in which

$$\Delta_2 = \frac{V\sqrt{D_1} + T(V + \chi_{ch}) + \Delta_1 \chi_{hom}}{T(V + \chi_{tot})}, \tag{4.66}$$

$$D_2 = \sqrt{D_1}\frac{V + \sqrt{D_1}\chi_{hom}}{T(V + \chi_{tot})}. \tag{4.67}$$

And the last symplectic eigenvalue is simply $\upsilon_5 = 1$. Thus the upper bound on Eve's Holevo information bound χ_{BE} is given by:

$$\chi_{BE} = g\left(\frac{\upsilon_1 - 1}{2}\right) + g\left(\frac{\upsilon_2 - 1}{2}\right) - g\left(\frac{\upsilon_3 - 1}{2}\right) - g\left(\frac{\upsilon_4 - 1}{2}\right),$$

where $g(x)$ is defined in Eq.(4.56). Thus the secret key rate formula for Gaussian collective attack is given by:

$$K_{Collective} = \beta I_{AB} - \chi_{BE}. \tag{4.68}$$

In this thesis, we use Eq.(4.68) to calculate secret key rate unless otherwise noted.

Chapter 5

Analysis of imperfections in CV QKD implementations

In section 4.2.2, we have presented a typical implementation of the GMCS protocol. In reality, there exists various imperfections on both sides of the implemented system, such as the laser source and modulators on Alice side, the homodyne detector on Bob side. These device imperfections influence the performance of the CV QKD system, and some of them may lead to security loopholes, thus we need to carefully study and evaluate their impacts.

In this chapter, we analyze several imperfections in a CV QKD system implementing the GMCS protocol. We first analyze imperfections in the homodyne detection on Bob side and their influences on the system performance. Then we show a proof of principle demonstration of a deconvolution method, which can be used to partially solve the pulses overlap problem of the homodyne detector in a CV QKD system, when it is operated at a repetition rate close or above the bandwidth of the homodyne electronics. In the end, we discuses other imperfections such as imperfect Gaussian modulation and phase noise that can be encountered on Alice's side, which have been addressed in [65].

5.1 Imperfections of the homodyne detection

Let us first focus on Bob side in a CV QKD implementation, where Bob performs a homodyne detection to measure the quadratures. The main purpose to study imperfections in a homodyne detection are following: (1) evaluate the impact of imperfections on CV QKD performance; (2) More importantly, evaluate whether there exists vulnerabilities for Eve to launch side channel attacks on the homodyne detection part.

Compared to the photon counting techniques in DV QKD, homodyne detection is a

technology widely used in classical optical telecommunication. Homodyne detection can be realized at low cost, high bandwidth and high efficiency. However due to the requirement of CV QKD, a shot noise limited homodyne detection is needed to be designed specifically, since the performance of CV QKD protocol is sensitive to the detector noise. In order to design a high quality homodyne detection in practice, it is necessary to study possible imperfections that appear in a homodyne detection.

In this section, we explain the principle of homodyne measurement: its output is proportional to the quadrature values. Meanwhile we analyze different imperfections of the homodyne detection which can affect the quadrature measurements and the performance of CV QKD. This is done by developing an original mathematical model of the homodyne detection based on the previous works [35, 102]. In this new model (Fig. 5.1), we consider the following imperfections:

- *Imbalance factor* of the beam splitter (ε): There is a small deviation (less than 10^{-3} in our case) between the transmission ($t_{bs}^2 = 0.5+\varepsilon$) and the reflection ($r_{bs}^2 = 0.5-\varepsilon$) of the 50/50 beam splitter.

- *Efficiencies* of two detectors (η_1, η_2) : In practice, the efficiencies of two photo diodes can not be exactly matched. $\Delta\eta$ is the difference between two efficiency η_1 and η_2, which can be defined as:$\eta_1 = \eta + \Delta\eta/2, \eta_2 = \eta - \Delta\eta/2$, and $\eta = (\eta_1+\eta_2)/2, \Delta\eta = (\eta_1 - \eta_2)$. Such deviation between the two photo detectors can be almost eliminated by adjusting the loss of the two optical paths.

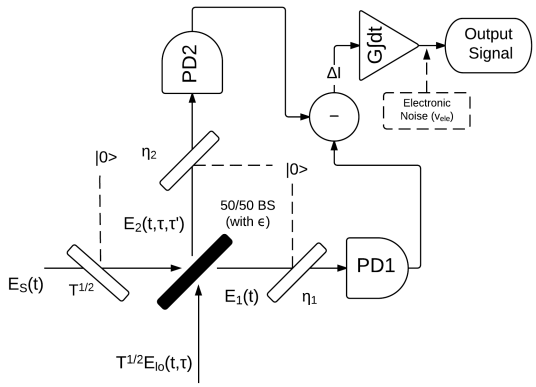


Fig. 5.1 Homodyne detection setup with different imperfections. τ and τ': time delays between optical pulses before and after beam splitter; ε: imbalance of beam splitter; η_1, η_2 efficiencies of two detectors; signal field E_s and LO field E_{LO}; E_1 and E_2: optical fields after beam splitter; T: channel transmission; *PD*: photodiode. $|0\rangle$ is denoted as the added vacuum state due to the loss. G stands for the amplification factor of the homodyne detector's electronics.

- *Chirp* of the laser source : In our system, we use a Alcatel LMI1905 laser as Alice's laser source. According to the experimental test in [35], this laser has a spectral linewidth of $\Delta\lambda = 0.01nm$ (Full width at half maximum, FWHM) with its central wavelength at $1543.2nm$. The corresponding frequency linewidth can be thus given by :

$$\Delta f = \frac{c}{\lambda^2}\Delta\lambda, \tag{5.1}$$

in which c is the speed of the light in vacuum and λ is the central wavelength, which gives $\Delta f = 1.26$ GHz in our case. Moreover, since the laser is externally modulated, the central wavelength of the laser drifts with time during the pulse duration ($100ns$) over a relatively wide range (Chirp effect), this relation can be given by an empirical formula according to the experimental results [35]:

$$\lambda(t) = 1543.2 + 1.08 * 10^{-4}t + 0.02e^{-0.03636(t-8.3)}, \tag{5.2}$$

in which λ is in the unit of *nm* and time t is in *ns*. The frequency of the laser can thus be expressed as:

$$f(t) = \frac{c}{n\lambda(t)}, \tag{5.3}$$

where n is the refractive index of the single mode fiber as $n = 1.5$.

- *Intensity fluctuation*: In practice, the intensity of a laser fluctuates. Such intensity fluctuation can be quantified over a time t_0:

$$f = \sqrt{\langle (I - \langle I \rangle_{t_0})^2 \rangle_{t_0}}/I \tag{5.4}$$

in which I is the laser intensity.

- *Time delay mismatch* between signal and LO pulse before and after beam splitter : Due to the different fiber path lengths, signal and LO pulse will arrive at the beam splitter (τ) and photon detectors (τ') at different time. As we shall see, such imperfection has an impact on the quadrature measurement when the chirp of the laser source is considered.

A figure depicting a practical homodyne detection setup with the imperfections mentioned above is shown in Fig.5.1. In order to analyze the impact of these imperfections, that can possibly influence the quadrature measurements in CV QKD, we need to return to Alice

side where she prepares the quadrature X and P of coherent states. As explained in section 4.2.2, Alice prepares two kinds of pulses: signal pulses and LO pulses. A signal pulse contains only a few photons and is considered as a quantum field. The relations between the signal operators $\hat{a}_s$, $\hat{a}_s^\dagger$ and their quadratures X, P are given by:

$$\hat{a}_s = \frac{X+iP}{2\sqrt{N_0}}, \hat{a}_s^\dagger = \frac{X-iP}{2\sqrt{N_0}}. \tag{5.5}$$

In which N_0 is the shot noise variance. The commutation relation and uncertainty relation of X and P are given by Eq.(2.67) and Eq.(2.68). The LO pulse contains approximately 10^8 photons at reception and is considered as a classical field, its intensity is given by $I_{LO} = a_{LO}a_{LO}^*$, with the classical amplitude a_{LO}. Alice sends signal pulses and LO pulses through a lossy channel with a transmission T. On Bob side, the LO pulse interferes with the signal pulse on a beam splitter of a homodyne detector. Before the beam splitter, the quantum field of the signal pulse ($E_s(t)$) and LO pulse ($E_{LO}(t)$) are give by:

$$\hat{E}_s(t) = \sqrt{T}\hat{a}_s e^{i(2\pi t f(t)+\varphi)} + \sqrt{1-T}\hat{a}_0, \tag{5.6}$$

$$\hat{E}_{LO}(t) = a_{LO}e^{i(2\pi(t+\tau)f(t+\tau))}, \tag{5.7}$$

in which $f(t)$ is the laser's frequency (Eq.(5.3)), t is a time variable and $\hat{a}_0$ is the annihilation operator for a vacuum mode. Due to the different lengths between LO path and signal path, a time delay τ between signal and LO pulse is induced. The phase modulator is placed on the LO path at Bob, which enables him to control the phase φ between LO and signal pulse.

The two fields, $\hat{E}_s(t)$ and $\hat{E}_{LO}(t)$, then interfere on the beam splitter and the two photodiodes (PD) transform the optical fields into photocurrents. In practice, the 50/50 beamsplitter has a small deviation ε with its transmission and the reflection ratio as $t_{bs} = \sqrt{1/2+\varepsilon}$ and $r_{bs} = \sqrt{1/2-\varepsilon}$. After the beam splitter, the loss and the lengths of the two optical paths are not identical but with small deviations. By considering these facts, the output fields of PD 1 and PD 2 are given by:

$$\hat{E}_1(t) = \sqrt{\eta}[\sqrt{T}(r_{bs}\hat{E}_s(t) + t_{bs}E_{LO}(t)) + 1/\sqrt{2}\sqrt{1-T}\hat{a}_0'] + \sqrt{1-\eta}\hat{a}_0^+, \tag{5.8}$$

$$\hat{E}_2(t+\tau') = \sqrt{\eta}[\sqrt{T}(t_{bs}\hat{E}_s(t+\tau') - r_{bs}E_{LO}(t+\tau')) + 1/\sqrt{2}\sqrt{1-T}\hat{a}_0'] + \sqrt{1-\eta}\hat{a}_0^-, \tag{5.9}$$

in which τ' is the time delay between $E_1(t)$ and $E_2(t)$, $\hat{a}_0'$ is associated to the vacuum mode of quadrature operator X_0' introduced on the lossy channel and $a_0^\pm$ is associated to the vacuum mode of quadrature operator X_0'' due to the loss of the detector, with the variance $Var(X_0') = Var(X_0'') = N_0$. Here, we assume $\eta_1 \approx \eta_2 = \eta$ and $\Delta\eta$ is a small value. As we shall see,

$\Delta\eta$ only has an impact in case the strong LO intensity I_{LO}. The photocurrent of homodyne detection is the subtraction between two intensities $I_1 = \hat{E}_1\hat{E}_1^*$ and $I_2 = \hat{E}_2\hat{E}_2^*$:

$$\Delta I(t) = I_1(t) - I_2(t), \tag{5.10}$$

The final output of homodyne detection is actually a voltage signal, which is an integration of photocurrent over the pulse duration ($t_p = 100ns$):

$$\Delta U_{HD} = \frac{1}{t_p}\int_0^{t_p} \Delta I(t)dt. \tag{5.11}$$

Such operation is carried out by a charge amplifier. By taking Eq. (5.5), Eq. (5.8) and Eq. (5.9) into equation above, we can deduce the output of the homodyne detection:

$$\begin{aligned}\Delta U_{HD} = \eta T I_{LO}(\Delta\eta/\eta + 2\varepsilon) + \frac{\sqrt{\eta T I_{LO}}}{\sqrt{N_0}}[\sqrt{\eta T}(X_A\frac{1}{t_p}\int_0^{t_p} A(t)dt + X_0) \\ + \sqrt{\eta T}(P_A\frac{1}{t_p}\int_0^{t_p} B(t)dt + P_0) + \sqrt{\eta}\sqrt{1-T}X_0 + \sqrt{1-\eta}X_0'] + X_{ele},\end{aligned} \tag{5.12}$$

in which X_{ele} is the electronics noise of the detector, Note that the coherent state encoding of Alice "adds" a vacuum mode (X_0, P_0). $A(t)$ and $B(t)$ are given by:

$$A(t) = 0.5(\cos\theta_1(t) + \cos\theta_2(t)), \tag{5.13}$$

$$B(t) = 0.5(\sin\theta_1(t) + \sin\theta_2(t)), \tag{5.14}$$

where $\theta_1(t)$ and $\theta_1(t)$ are both functions of t:

$$\theta_1(t) = [\varphi + 2\pi t f(t) - 2\pi(t+\tau)f(t+\tau)], \tag{5.15}$$

$$\theta_2(t) = [\varphi + 2\pi(t+\tau')f(t+\tau) - 2\pi(t+\tau+\tau')f(t+\tau+\tau')]. \tag{5.16}$$

If we moreover use the relations: $\cos\theta_1 + \cos\theta_2 = 2\cos\frac{\theta_1+\theta_2}{2}\cos\frac{\theta_1-\theta_2}{2}$ and $\sin\theta_1 + \sin\theta_2 = 2\sin\frac{\theta_1+\theta_2}{2}\cos\frac{\theta_1-\theta_2}{2}$ for $A(t)$ and $B(t)$, Eq.(5.12) can be transformed into:

$$\begin{aligned}\Delta U_{HD} &= \frac{1}{t_p}\int_0^{t_p}\Delta I(t)dt \\ &= \eta T I_{LO}(\Delta\eta/\eta + 2\varepsilon) + \frac{\sqrt{\eta T I_{LO}}}{\sqrt{N_0}}[\sqrt{\eta T}(X_\varphi + X_0) + \sqrt{\eta}\sqrt{1-T}X_0' + \sqrt{1-\eta}X_0''] + X_{ele}',\end{aligned} \tag{5.17}$$

in which X_φ is a function of time t, and is the quadrature measurement output of Bob:

$$X_\varphi = \frac{1}{t_p}\int_0^{t_p} \cos[\pi a_2(t,\tau,\tau')]\{(X_A\cos[\varphi+\pi a_1(t,\tau,\tau')]+P_A\sin[\varphi+\pi a_1(t,\tau,\tau')]\}dt, \tag{5.18}$$

whose value is dependent on φ with

$$a_1(t,\tau,\tau') = tf(t)+(\tau'-\tau)f(t+\tau)-(t+\tau+\tau')f(t+\tau+\tau'), \tag{5.19}$$
$$a_2(t,\tau,\tau') = tf(t)-(2t+\tau+\tau')f(t+\tau)+(t+\tau+\tau')f(t+\tau+\tau'). \tag{5.20}$$

From Eq.(5.17), we can observe that, ideally, if there are no imperfections ($\varepsilon = 0, \tau = 0, \tau' = 0$), LO intensity can be subtracted absolutely, and Bob can measure the quadrature X_A or P_A (proportional to LO intensity I_{LO}) by measuring X quadrature with $\varphi = 0$ or P quadrature with $\varphi = \pi/2$. However if we take the imperfections into account, systemic errors will be introduced that will impact the performance of CV QKD: (1) if the imbalance part $\Delta\eta/\eta + 2\varepsilon \neq 0$ then LO intensity won't be eliminated totally, and it will contribute to the excess noise; (2) if the time delays $\tau, \tau' \neq 0$, this will induce excess noise together due to the chirp of Alice's laser source.

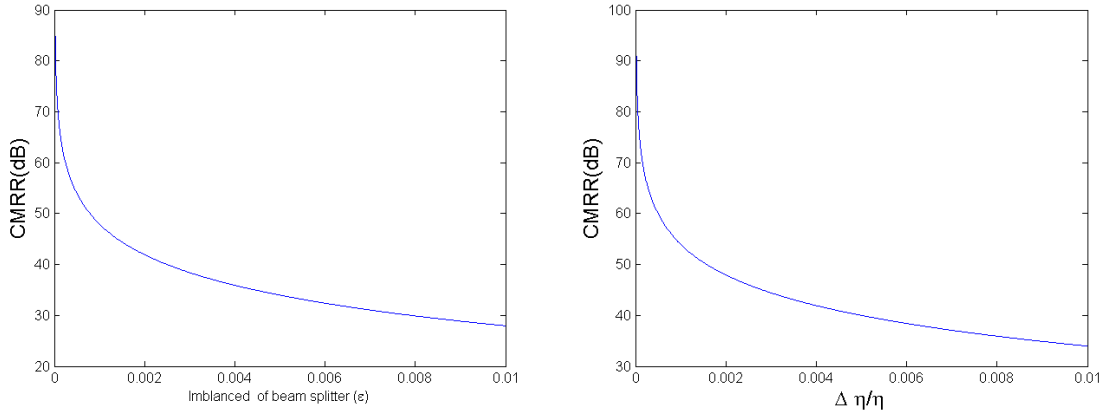
In order to analyze these impacts on the excess noise, we need to study Bob's quadrature output. If we scale the homodyne output by $\sqrt{\eta T I_{LO}/N_0}$, then we can express Bob's measurement result as:

$$X_B = \sqrt{\eta T N_0/I_{LO}}I_{LO}(\Delta\eta/\eta+2\varepsilon)+\sqrt{\eta T}(X_\varphi+X_0)+\sqrt{\eta}\sqrt{1-T}X_0'+\sqrt{1-\eta}X_0''+X_{\text{ele}}, \tag{5.21}$$

where X_B is consistent with Eq.(4.5) but here we have taken the impact of imperfections into account. If we take the shot noise as $N_0 = 1$, Bob's variance is given by:

$$\begin{aligned} Var(X_B) &= \langle (X_B - \langle X_B\rangle)^2\rangle \\ &= \eta T(\Delta\eta/\eta+2\varepsilon)^2 I_{LO}(\langle (I_{LO}-\langle I_{LO}\rangle)^2\rangle/I_{LO}^2)+\eta T[Var(X_\varphi)+1]+\eta(1-T)+(1-\eta)+v_{\text{ele}} \\ &= \eta T(\Delta\eta/\eta+2\varepsilon)^2 I_{LO}(\langle (I_{LO}-\langle I_{LO}\rangle)^2\rangle/I_{LO}^2)+\eta T Var(X_\varphi)+1+v_{\text{ele}}, \end{aligned} \tag{5.22}$$

In which, $f_{LO} = \sqrt{\langle (I_{LO}-\langle I_{LO}\rangle_{t_0})^2\rangle_{t_0}}/I_{LO}$ is known as the LO intensity fluctuation over a time t_0, in this case $t_0 = t_p$. If such fluctuation can be neglected, the imbalance part $\Delta\eta/\eta + 2\varepsilon$ only changes the mean value of X_B. However, if f_{LO} is large, intensity fluctuations will



(a) (b)

Fig. 5.2 (a) CMRR vs imbalance of beam splitter (ε). (b) CMRR vs efficiency deviation ($\Delta\eta/\eta$).

contribute to the excess noise, which is the first term in Eq.(5.22): $I_{LO}(\Delta\eta/\eta + 2\varepsilon)^2 f_{LO}^2$. In order to quantify the leakage of the LO on the homodyne output (or the balance of the homodyne detection), we introduce the common mode rejection ratio (CMRR) which is defined as: $CMRR = -20log_{10}(2\delta)$, where $\delta = \Delta\eta/\eta + 2\varepsilon$. In Fig.5.2, we independently change the values of ε (Fig.5.2(a)) and $\Delta\eta/\eta$ (Fig.5.2(b)) and we can observe that CMRR reduces with the increase of these two values. To achieve a balanced homodyne detection, one needs to adjust both ε and $\Delta\eta/\eta$ to reach a high value of CMRR. In order to evaluate the impact of CMRR and LO intensity fluctuation on the secret key rate, we show the relation between secret key rate and CMRR in Fig.5.3 for two intensity fluctuation ratios: $f_{LO} = 1\%, 5\%$, with the assumption that I_{LO} contains 10^8 photons. From Fig.5.3, we can conclude that if the LO intensity fluctuations are large, then the requirements on the CMMR are more strict. For example, with an intensity fluctuation ratio of 5%, it requires more than 80 dB of CMRR to maintain a positive secret key rate, in contrast, if the intensity fluctuation ratio is 1% then 60 dB CMRR is high enough to achieve such key rate.

We now consider the imperfection related to the imbalance of the optical paths which induces a time delay between signal pulse and LO pulse (τ) and a time delay between two optical pulses after the beam splitter (τ'). As we can see from Eq.(5.18), due to the chirp of the emitting laser $f(t)$ and time delays τ, τ', a phase variation $\pi a_1(t, \tau, \tau')$ is introduced and a factor $\cos[a_2(t, \tau, \tau')]$ is introduced on the quadrature measurement X_φ. It is obvious to see that the factor $\cos[a_2(t, \tau, \tau')]$ reduces the quadrature value of X_φ in Eq.(5.18), which further reduces the correlation between Alice and Bob quadratures. We will consider the case where $a_2(t, \tau, \tau')$ is very small and close to zero such that $\cos[a_2(t, \tau, \tau')] \simeq 1$ and

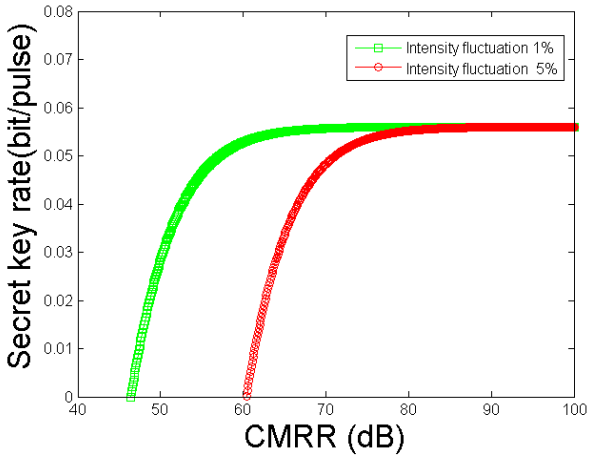


Fig. 5.3 Secret key rate (collective attack) versus CMRR. Alice's variance $V_A = 20$, Bob's efficiency $\eta = 0.55$, excess noise of electronics $v_{\text{ele}} = 0.015$, excess noise from other contributions $\xi = 0.01$, reconciliation efficiency $\beta = 0.9$, channel transmission $T = 0.38$.

make this approximation in the following analysis.

Since the phase variation $\pi a_1(t,\tau,\tau')$ depends on the time t, the homodyne output consists of a time-average of X_φ over the pulse duration. By calculating the integral (Eq.(5.17)) with realistic parameters, the relation between homodyne output ΔU_{HD} and time delays τ is shown in Fig.5.4 (a). As we can see, the deviation of the homodyne output becomes obvious when τ increases. The phase variation even induces oscillation on the output signal when τ is larger than 0.5 ns. Meanwhile, we have also considered taking $\tau' = 1$ ns for each curve in Fig.5.4 (a). However, there are no obvious differences between the curves with τ' and without τ'. Thus we don't show the curves with time delay τ'. And we can conclude that phase variation is more sensitive to the imbalance of optical paths before the beam splitter than to the imbalance of optical paths after the beam splitter. The phase variation $\pi a_1(t,\tau,\tau')$ induces homodyne signal oscillation and the corresponding quadrature measurement X_φ is also influenced. Such phase variation in fact reduces Bob's measured variance. We plot the relation between Bob's variance and time delay τ in Fig.5.4 (b). In order to show the impact of the time delay, we set channel transmission (T) and efficiency of homodyne detection η to 1 and the excess noise as $\xi = 0$. As we can see, even 0.1 ns time delay (2 cm in fiber length) will reduce the measured variance by almost one half. As a consequence, channel transmission estimation is reduced. On the other hand, the phase variation $\pi a_1(t,\tau,\tau')$ also introduces excess noise, which is known as the phase noise. In order to simplify the calculation of phase noise, approximately, we can assume the variation of laser's frequency with time is upper bounded by the change due to the chirp of the laser during the pulse width duration (τ_p =100 ns), where $f(t), f(t+\tau), f(t+\tau+\tau') \sim \Delta f_{ch}$. In our case, considering

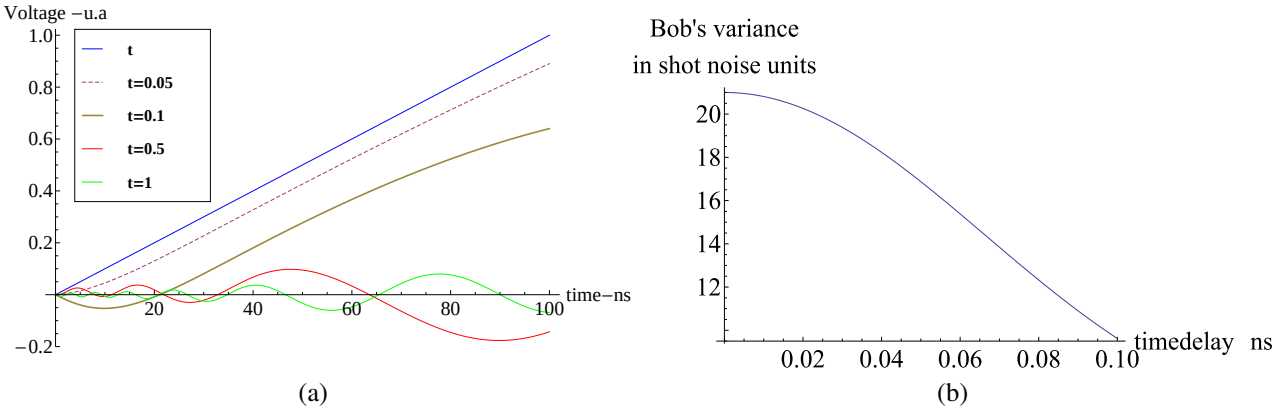


Fig. 5.4 (a) The output signal after charge amplifier of homodyne detection with different time delay (τ =0, 0.05 ns, 0.1 ns, 0.5 ns, 1 ns) between signal and LO pulse before beam splitter. (b) Bob's variance vs time delay between signal pulse and LO pulse before beam splitter. Here we assume Alice's variance $V_A = 20$, electronic noise of homodyne detection $v_{ele} = 0.01$, LO pulse duration is $t_p = 100$ ns, channel transmission $T = 1$ efficiency of homodyne detection $\eta = 1$, excess noise $\xi = 0$.

the time delays are much smaller than the pulse duration where $\tau, \tau' \ll t_p$ and using the wavelength empirical formula (Eq.(5.2)), we can deduce $\Delta f_{ch} = 3.1$ GHz with τ_p =100 ns. Then we can simplify the terms a_1 and a_2 in X_φ (Eq.(5.18)): $a_1 \simeq -2\tau\Delta f_{ch}$ and $a_2 \simeq 0$ which are both independent of time t. Eq.(5.18) can be further simplified to:

$$X_\varphi = X_A \cos(\varphi - 2\pi\tau\Delta f_{ch}) + P_A \sin(\varphi - 2\pi\tau\Delta f_{ch}), \tag{5.23}$$

Thus the phase variation on φ is given by $\Delta\phi = \pi a_1 = -2\pi\tau\Delta f_{ch}$. Provided with Eq.(5.23), we can estimate the excess noise due to the phase variation $\Delta\phi$. If we set $\varphi = 0$ in Eq.(5.23) and assume $\Delta\phi << 1$ (which is a realistic condition), Eq.(5.23) can be approximately turned into :

$$X'_{\varphi=0} = X_A \cos(\Delta\phi) + P_A \sin(\Delta\phi) \simeq X_A + P_A\Delta\phi, \tag{5.24}$$

and the excess noise due to $\Delta\phi$ can be estimated by:

$$\xi_{\Delta\phi} = \langle (X'_{\varphi=0} - X_A)^2 \rangle \simeq \langle (X_A + P_A\Delta\phi - X_A)^2 \rangle = \langle P_A^2 \rangle \Delta\phi^2 = V_A\Delta\phi^2 \tag{5.25}$$

$$\simeq 2\pi\tau\Delta f_{ch} V_A. \tag{5.26}$$

In fact such result also agrees with the analysis in [139], where if we consider a time t for

the phase variation $\Delta\theta(t)$, then the corresponding excess noise can be given by:

$$\xi_{\Delta\theta(t)} = V_A\langle(\Delta\theta(t))^2\rangle, \tag{5.27}$$

in which V_A is Alice' modulation variance, $\Delta\theta(t)$ is the phase variation $\Delta\theta(t)$ respect to a time t. According to [191], $\Delta\theta(t)$ can be approximately treated as a Gaussian variable with a zero mean and its variance can be given by:

$$\langle(\Delta\theta(t))^2\rangle = \frac{2t}{\tau_c}. \tag{5.28}$$

in which t_c is the coherence time of the laser and, in our case, it can be determined by [191]:

$$\tau_c \simeq \frac{1}{\pi\Delta f_{ch}}. \tag{5.29}$$

If we moreover consider the time between $t = 0$ and $t = \tau$, we can deduce the excess noise due to the phase variation:

$$\xi_{\Delta\phi} \simeq 2\pi\tau\Delta f_{ch}V_A. \tag{5.30}$$

For $\Delta f_{ch} = 3.1$ GHz, if we want to limit the phase noise below $0.1N_0$, the time delay τ needs to be lower than 0.002 *ns* for a modulation variance $V_A = 5N_0$. In Fig.5.5, we show such relation between phase noise and time delay τ in our case: $\Delta f_{ch_1} = 3.1$ GHz, and in

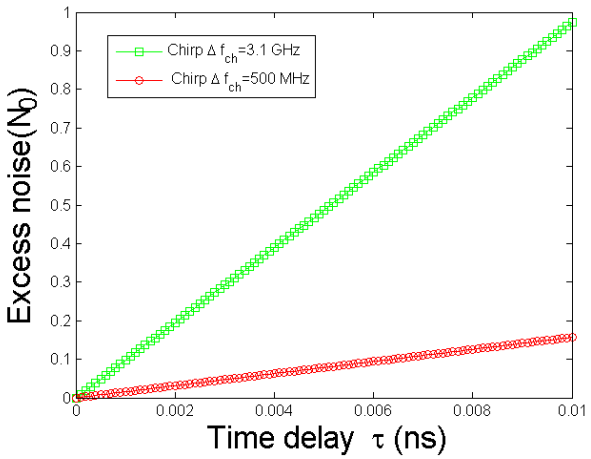


Fig. 5.5 Excess noise due to phase variation $\xi_{\Delta\phi}$ versus time delay τ between signal pulse and LO pulse. Alice's variance $V_A = 5$. Lase linewidth $\Delta f_{ch_1} = 3.1$ GHz,$\Delta f_{ch_2} = 500$ MHz.

comparison to a laser with less chirp effect $\Delta f_{ch_2} = 500$ MHz. We can observe that the excess noise due to the phase variation can be reduced by balancing the optical paths of signal and LO; by reducing the chirp effect of the laser source. Note that such phase noise can be further reduced by using phase compensation techniques which was introduced in [35].

In this section, we have studied two kinds of imperfections: (1) The first kind of imperfections, the imbalance factor $(\varepsilon, \Delta\eta)$ of the homodyne detection results LO intensity leakage on homodyne output signals, which may induce excess noise if the LO intensity fluctuation is large. (2) The second kind of imperfections such as time delays (τ, τ') and chirp of laser source that induce phase variation on Bob's quadrature measurement, which can induce excess noise and reduce the channel transmission estimation. Such observations agree with the analysis in [65], as we shall see in the section 5.3.2 (Eq.(5.39)).

5.2 Deconvolution method: Correct overlapping pulses

5.2.1 Motivation: finite bandwidth of homodyne detection

In order to integrate QKD technology with practical applications, researchers have recently made great efforts to increase the secure distance and the key generation rate. High speed quantum key distribution is becoming a hot topic. In discrete variable QKD, the highest key rate record is 1 Mbit/s over 50 km [27]. CV QKD using homodyne detection is a good candidate to perform high speed QKD. Since, in principle, the homodyne detectors used in CV QKD have no difference from the ones used in classical coherent communication system. However, as we mentioned, GMCS protocol requires a very low electronic noise and shot noise limited homodyne detector to effectively detect Eve's attack. The homodyne detectors used in classical communication system usually cannot meet such requirements, since they usually has high bandwidth but also high electronic noise, which are not suitable for CV QKD. In the design of a shot noise limited homodyne detector, it's challenging to achieve very low electronics noise and large bandwidth at same time. In [103], electronic noise is around 1% of the shot noise with a bandwidth around 2 MHz. Recently, a 300 MHz bandwidth detector was experimentally tested [28] and the level of shot noise is 14 dB higher than the electronic noise.

Intuitively, one can increase the secret key rate of CV QKD by raising the clock repetition rate, since the secret key rate is proportional to its operation rate. However, in practice, due to the finite bandwidth of a practical homodyne detection, when the laser pulse repetition rate becomes close to the bandwidth of the homodyne detection, a non-negligible

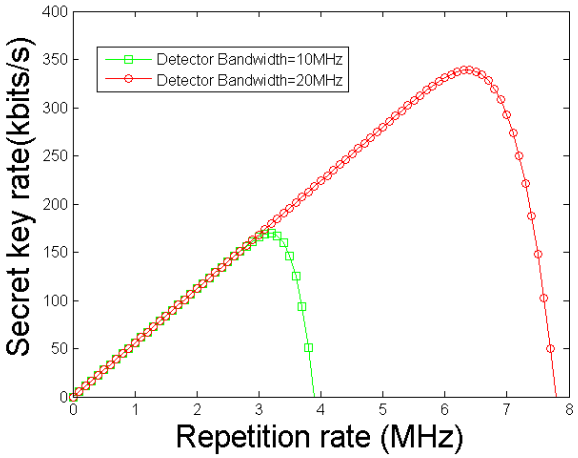


Fig. 5.6 Secret key rate (collective attack) versus repetition rate. Alice's variance $V_A = 20$, Bob's efficiency $\eta = 0.55$, excess noise of electronics $v_{\text{ele}} = 0.015$, excess noise from other contributions $\xi = 0.01$, reconciliation efficiency $\beta = 0.9$, channel transmission $T = 0.38$.

overlap between adjacent electrical pulses at the output of the homodyne detection will be expected. If the electrical pulses have overlap in the time domain, the measured quadrature value contains contributions from adjacent pulses. Such overlap will further contribute to excess noises in GMCS protocol. The estimation of excess noise due to overlapping pulses has been analyzed in [16], where the excess noise contributed by electrical pulses overlap (from the two adjacent pulses) is:

$$\xi_{overlap} = 2(V_A + 1) \times e^{-\frac{B^2}{R^2}}. \tag{5.31}$$

In which R is the laser repetition rate and B is the bandwidth of homodyne detection. The relation between the electrical pulse width τ and bandwidth B is given by $\tau \sim 1/B$. Such relation is verified by the experimental tests [16]. From Eq.(5.31), we can see that the increase of the repetition rate results additional excess noise, which lowers the secret key generation. Our homodyne detector has a bandwidth around few MHz. In order to evaluate the excess noise due to the overlapping effect for a given bandwidth, we assume that two detectors have bandwidths as 10 MHz and 20 MHz respectively. The secret key rate increases proportionally to the repetition rate. However, due to the finite bandwidth of the detector, when the repetition rate reaches a certain value, the overlapping effect becomes important and contributes to excess noise, which will further lower secret key rate. Such behavior can be observed in Fig.5.6, where we can see that secret key rate (under collective attack) significantly increases when the detector bandwidth increases. The simulation parameters are given in the caption and all the units are normalized in shot noise units.

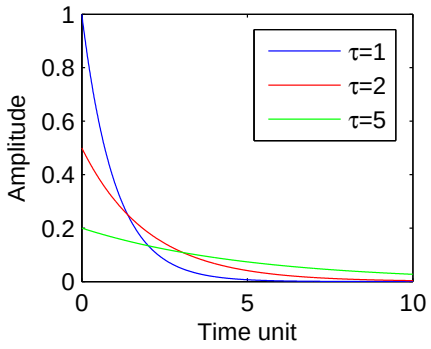


Fig. 5.7 Pulse width with different values of τ.

Fortunately, excess noises dues to the overlapping between adjacent pulses can be further reduced by deconvolution. In the following part, we are going to study such method.

5.2.2 Deconvolution principle

The details of the deconvolution method have been studied in [78] for the homodyne detection. Briefly, in this deconvolution method, one first needs to quantify the overlapping effects that neighboring pulses have on each other. Correlation between two quadrature measurements will describe the influence from the neighboring pulses. The correlations between the i quadrature measurement and $i+j$ th quadrature measurement is defined by:

$$C_j = \langle Q_i Q_{i+j} \rangle \tag{5.32}$$

which is averaged over i. Meanwhile, Q_i is the i th quadrature measurement associated with the ith pulse. Hence for a specific measurement Q_i we can find all the correlations (or influence) from i th to $i+j$ th pulse. Since for a single pulse, the influences come from not only one neighboring pulse but a series of following pulses. Then one can correct the quadrature according to the correlation C_j and the corresponding quadrature measurement:

$$Q_i' = Q_i - \sum_j^{\infty} C_j Q_j, \tag{5.33}$$

in which Q_i' is the quadrature after subtracting the effects from neighboring pulses: the quadrature corrected by the deconvolution. After doing this, one can reduce the influence from overlapping effects. This is so called deconvolution, more details can be found in [78]. The relation between the electrical pulse width τ and the homodyne detection bandwidth B depends on the electrical pulse shape. Here we assume a exponential decay function (Eq.

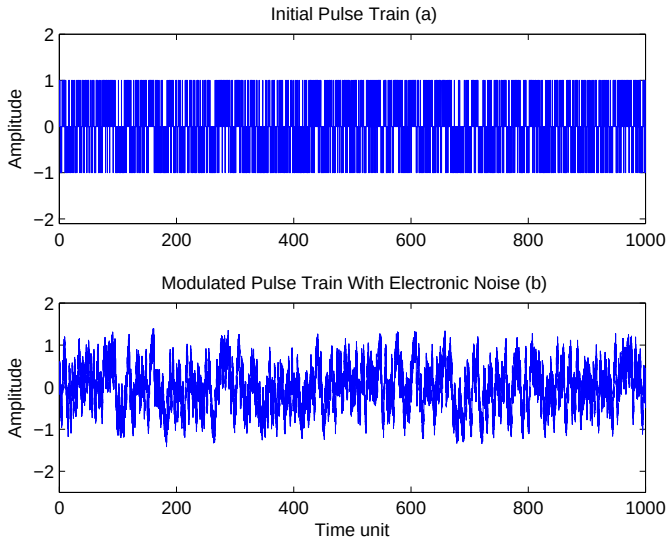


Fig. 5.8 First 1000 pulses vs Time unit. (a) Initial pulses. (b) Modulated pulse with pulse shape and electronic noise.

(5.34)) to describe the electrical pulse shape.

$$S(t) = \frac{1}{\tau} e^{-\frac{t}{\tau}}, \tag{5.34}$$

in which τ value is the discharging time of a peak pulse which relates to the capacitor and resistor in the electronics design. We also vary the pulse width τ, Fig (5.7) shows the shape of the pulse with different values of τ. What matters in this overlapping problem is the ratio between the repetition period and the pulse width τ. If the pulse width is larger than the repetition period T of the pulses train, neighboring pulses will overlap. To study this problem, we set the repetition period of pulse train $T = 1$ time unit, while we set τ to multiple times of the period. In this simulation, we consider $\tau = 2$ which means the pulse width is two times the period, this width is enough to observe overlapping effect.

5.2.3 Proof of principle: deconvolution for homodyne detection in CV QKD

In this section, we present a proof of principle simulation to demonstrate the deconvolution method that can be potentially used in the homodyne detection. We used the Simulink set-up and programs in Matlab to realize the deconvolution demonstration. In the following steps, we first explain how we generate the overlapping pulses, then perform the deconvolution. At last, we evaluate the results.

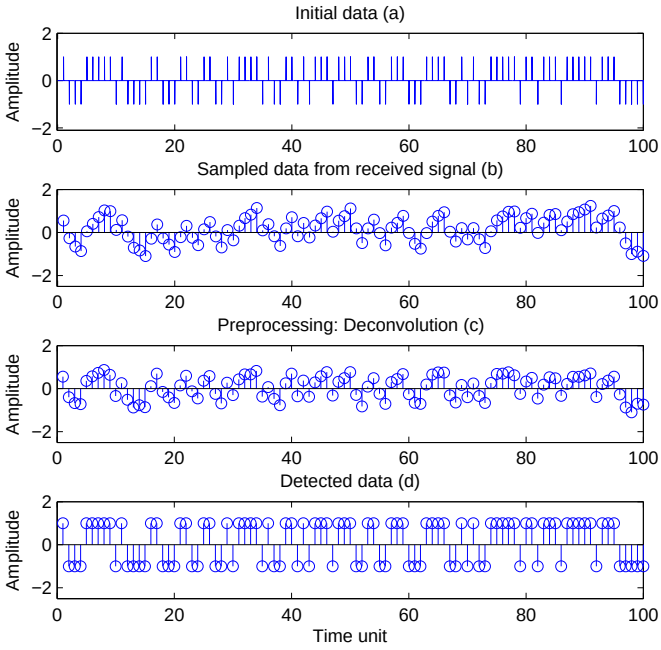


Fig. 5.9 First 100 pulses vs Time unit. (a) Initial pulses. (b) Sampled pulses from Fig.5.(b). (c) Filtered pulses by using deconvolution. (d) Output pulse with gate decision.

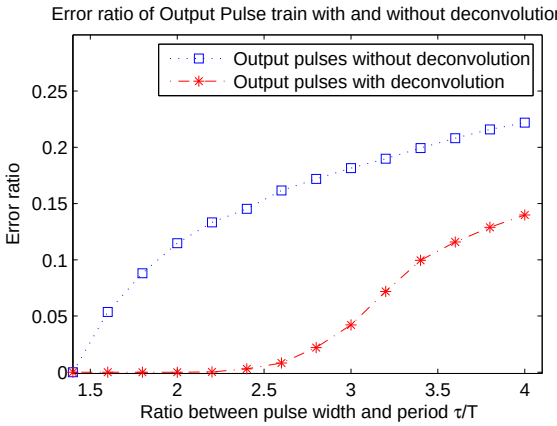


Fig. 5.10 Error ratio of output pulse train with and without deconvolution

First we generate a train of pulses with a binary distribution as initial data, each pulse is a Dirac function with an amplitudes either 1 or -1. Unlike the GMCS protocol using Gaussian modulation, here we only consider a binary modulation as a proof of principle.This corresponds to a binary modulation CV QKD protocol [195], which we have introduced in Chapter 4. Here we use the amplitudes 1 and -1 to designate with the coherent states $|\alpha\rangle$ and $|-\alpha\rangle$, where the sign indicates the phase encoding of the states.

We then apply an exponential decay to each pulse. Two adjacent pulses can have some overlap due to their widths. Additionally, we apply a thermal noise with variance of 0.005 to the curves, in order to simulate the electronic noise of the detector. Such modulated pulses can be seen as the received quadrature signals, here we consider a zero loss channel ($T_{ch} = 1$) and a detector with perfect efficiency ($\eta = 1$). Fig.5.8 shows first 1000 initial pulses and modulated pulses with a shape described by Eq. (5.34).

We sample the modulated pulses at a given frequency and make a gate decision on the sampled data, depending whether its value is below zero (output -1) or above zero (output 1). Due to the overlap, there could be errors at the output compared to the initial data. We then apply the deconvolution method as mentioned before to the sampled pulses.

We illustrate this process in Fig.5.9, where the first 100 initial pulses with binary modulation are shown in Fig.5.9 (a). In Fig.5.9 (b), the 100 sampled pulses are taken from the received signal Fig.5.8(b). Fig.5.9 (c) displaces the filtered pulses with the deconvolution technique. If we compare the individual pulse in Fig.5.9 (b) and Fig.5.9 (c), we can see that the errors introduced by overlapping effect have been reduced thanks to the deconvolution (Fig.5.8 (c)). Fig.5.9 (d) is the final output pulses with a gate decision, they represent the pulses after the deconvolution and will be compared with the initial pulses to evaluate how many errors have been corrected.

The error ratio is computed from 10000 pulses and has been evaluated for different ratios τ/T for pulses that have been processed with or without deconvolution in Fig.5.10. We can see from this figure, after the deconvolution, it is very obvious that the error ratio has been significantly improved, i.e. for a pulse width equal to twice the period $\tau/T = 2$, the error rate is reduced from 11.73% without deconvolution to 0.2 % with deconvolution. It means that only 2 errors appear in the total of 10000 pulse after deconvolution.

In the end we show the improvement of the deconvolution method with difference pulse width-repetition period ratios. As we can see from Fig.5.10, the improvement of error ratio with deconvolution (distance between the blue and the red curve) is significant for $\tau/T < 2.5$, with almost all the errors eliminated. However, the efficiency of such deconvolution technique is limited: when the pulse width is much lager than the repetition period. i.e., $\tau/T = 4$, deconvolution can only partially correct the errors, while it still remains lots of errors due to the overlapping effects.

In this subsection, we have shown the feasibility of the deconvolution method using a simulation. This shows that it is possible to correct the effect of overlap pulses to reduce the error rate and further reduce the excess noise in a discrete modulation CV QKD protocol [195]. Further study need be done to extend this deconvolution method to Gaussian modulation protocols and integrate it into practical set up.

5.3 Other possible imperfections

In the implementation of the GMCS protocol, besides the imperfections of Bob's homodyne detection, there are other imperfections that can influence the security and the performance. In this section, we discuss two device imperfections that can affect Alice based on the analysis of Jouguet et al. [65]. The first one concerns modulation imperfection: in practice, the theoretical Gaussian modulation can be only approximately approached by a discrete modulation. The second one concerns the phase noise that can be introduced in the preparation process of the coherent states.

5.3.1 Imperfect Gaussian modulation

In Gaussian protocols, ideally, for each signal, Alice prepares the quadratures $X, P \sim \mathcal{N}(0, V_A)$ of the coherent state $|X + iP\rangle$ centered on the point (X, P) in phase space. The random variable X or P is supposed to follow a perfect Gaussian distribution, which is continuous and unbounded, and requires an infinite amount of randomness. However, in practice, it is impossible to generate a perfect Gaussian modulation for the quadratures X and P due to the limitations of Alice's hardware and software. First, the analog-to-digital converters, which drive the modulators, generate only discrete voltages with a typical bit depth of 10. Second, amplitude modulator only works over a finite range of values. Third, the speed of the quantum random number generator is limited (for example, 16 Mbit/s for Quantis from ID Quantique). Due to these reasons, the coherent state that Alice actually prepares for the ideal value (X, P) is actually centered on (X', P'), where (X', P') is a point on a finite grid, and it is an approximation value for the ideal value (X, P).

We thus need to compare the quality of the modulation that can be realized in practice with the theoretical perfect Gaussian modulation. This modulation implementation can impact the practical security of a CV QKD setup. In theory, from Eve's view, the state that Alice sends to Bob is a Gaussian mixture of the coherent states (thermal state). Hence if Eve can not tell the difference between a thermal state and the state that is prepared by a discrete modulation in practice, then the security of the practical protocol is not compromised. We can study this problem with ε-secure analysis [148]: considering the usual protocol with perfect Gaussian modulation preparation is ε-secure, and that the trace distance between the ideal state (with perfect Gaussian modulation) and the actual state (with discrete modulation approximation) is bounded by $\varepsilon_{\text{prep}}$, then the practical protocol with approximated modulation is $(\varepsilon + \varepsilon_{\text{prep}})$-secure. To ensure the security of the practical protocol, it is enough to make sure $\varepsilon_{\text{prep}}$ is small enough, where $\varepsilon_{\text{prep}} = 10^{-10}$ can be a realistic value in a practical implementation.

According to the analysis in [65], there are mainly two ways of discretizations for the Gaussian modulation: Cartesian and Polar grid. In order to analyze the quality of the Gaussian modulation realized by these two methods, one can compute the trace distance between the ideal thermal state ρ and the state prepared in practice σ for each case. It is moreover shown that based on the gentle measurement lemma [127, 186], the trace distance $||\rho-\sigma||_1$ can be expressed as:

$$||\rho-\sigma|| \leq R_\rho + \Delta_{\text{diag}} + 2\Delta_{\text{nondiag}} + 2\sqrt{R_\sigma}. \tag{5.35}$$

in which R_ρ,Δ_{diag},Δ_{nondiag} and $\sqrt{R_\sigma}$ are parameters whose values depend on the particular method of preparing Gaussian modulation.

Under the Cartesian grid approximation, the coordinates are discretized uniformly with a square grid $[-N,N]\times[-N,N]$. The discretized values for the vertical and horizontal direction in phase space can be written as: $x_k = p_k = \delta k$, in which $\delta = \frac{A}{N}$ is the predetermined discretization step. Parameter A determines the truncated range of the actual distribution that is prepared in practice. Once A is fixed, N then determines the discretization step. With these parameters fixed, one can express the prepared state σ_c under the Cartesian grid approximation and moreover calculate the trace distance $||\rho-\sigma_c||$.

The authors give an numerical example to show how fine the grid need to be to have a good approximation. The parameters are chosen as: $V_A = 20$, $A = 7\sqrt{V_A}$ and $N = 4A$, in which $A = 7\sqrt{V_A}$ means that the actual Gaussian distribution is cut off at 7 times the standard deviations $\sqrt{V_A}$ with V_A as modulation variance; $N = 4A$ means that the distribution is discretized in steps of $\delta = 1/4$ of shot noise units. For $V_A = 20$, it requires $2\times4\times7\times\sqrt{V_A}+1 = 253$ discretization steps, which is, an 8-bit discretization grid. By taking these values into account, the authors shows that $||\rho-\sigma_c|| \leq 3.31\times10^{-11}$, which means the trace distance is bounded by $\varepsilon_{\text{prep}} = 3.31\times10^{-11}$ and can be considered sufficiently small.

As we have seen in section 4.2.2, in the implementation of the GMCS protocol, the Gaussian modulation is realized using a phase and an amplitude modulator and can naturally be analyzed in polar coordinates. It is also important to study how much discretization is required in polar coordinates to obtain a good approximation of an ideal thermal state ρ. Under the polar grid approximation, the coordinates are discretized uniformly on $[0,R]\times[0,2\pi]$, where the discretized value of the amplitude and phase in polar coordinates can be

written as:

$$r_k = \left(k+\frac{1}{2}\right)\frac{R}{K}, k \in [0, K-1], \tag{5.36}$$

$$\theta_l = \left(l+\frac{1}{2}\right)\frac{2\pi}{L}, l \in [0, L-1]. \tag{5.37}$$

Based on such discretization, one can express the prepared state σ_p and calculate the trace distance $||\rho - \sigma_p||$. An numerical example is also given by the authors, where for $V_A = 20$, $L = 2000$ and $R = 7\sqrt{V_A}$, it requires a 17-bit discretization of the amplitude to achieve $\varepsilon_{\text{prep}} \leq 10^{-10}$. It fuhrer needs 11 bits for the angle and 15.5 bits for the modulus on average to draw values corresponding to this discretization. It shows that in Polar approximation, it requires more discretization steps to achieve the same quality of modulation compared to the Cartesian grid approximation.

5.3.2 Phase noises from the state preparation

Beside the discrete modulation approximation, another kind of imperfection need to be considered on Alice side: some phase noise can be introduced when Alice prepares the quadrature of the coherent state. To be clear, the phase noise means the excess noise due to the phase variation. This kind of noise is unavoidable since it is due to the technical imperfection. A typical value of phase noise variance is around $0.01N_0$ [105]. Since phase noise is introduced on Alice side, such noise will degrade the mutual information between Alice and Bob I_{AB}. However, phase noise won't increase the knowledge of Eve on Bob's measurement in case of reverse reconciliation: the Holevo bound of Eve's information χ_{BE} in the case of collective attack (Eq.(4.53)). χ_{BE} quantifies the information that Eve can obtain on the raw key which does not depended on phase noise. This would however not be true under direct reconciliation where Eve's information depends on Alice's data.

Since phase noise is a local noise on Alice's side, we can consider in a realistic model that the phase noise can be trusted,i.e not given to Eve. This is in contrast to the paranoid model where all noise sources are supposed to be under the control of Eve. As we have seen in Chapter 4, a realistic model can also be applied on the detection stage in CV QKD, where the electronic noise and efficiency of the detector are calibrated before the protocol. If phase noise can be calibrated correctly, it can be subtracted from the excess noise estimation to compute Eve's information, which can lead to a better secret key rates in practice. However, the calibration of the phase noise need to be careful and precise, since if the phase noise is overestimated, then the estimation of excess noise will be underestimated, which could open opportunities to Eve to compromise the security.

To model the phase noise, we refer to the analysis of Jouguet et al. [65] and use the EB CV QKD scheme (section.4.5.1) to apply a phase rotation $U(\theta) = \exp(i\theta a^\dagger a)$ on Alice's state with a random phase θ with its probability distribution $p(\theta)$. Alice then actually prepares a state with a noisy phase: $\rho_\alpha = \int U(\theta)|\alpha\rangle\langle\alpha|U(\theta)^\dagger p(\theta)\mathrm{d}\theta$ instead of preparing the coherent state $|\alpha\rangle$. The coherent state affected by the phase noise is a mixture of states with random phase shifts θ. Alice then sends this state to Bob through the quantum channel. On Bob side, it is assumed that Bob performs a perfect homodyne detection ($\eta = 1$ and $v_{\mathrm{ele}} = 0$) and all the noise contribution are from the phase noise. By considering this things, the covariance matrix shared by Alice and Bob can be given as:

$$\Gamma_{AB} = \begin{bmatrix} V_A \mathbb{1}_2 & \sqrt{\kappa T} V_A \sigma_z \\ \sqrt{\kappa T} V_A \sigma_z & (TV_A + N_0 + T\xi_{ph})\mathbb{1}_2 \end{bmatrix}. \tag{5.38}$$

Where $\sigma_z = \mathrm{diag}(1,-1)$ and $\kappa = (\int p(\theta)\cos\theta \mathrm{d}\theta)^2 = (E[\cos\theta])^2$, is the factor due to the random shifts θ, it corresponds to the square of the expectation value of $\cos\theta$.

For the sake of the security in practical CV QKD system, we need to analyze the impact of the phase noise on parameter estimation. If we take phase noise into account, the channel transmission and the excess noise estimation become:

$$\begin{aligned} \hat{T}_\theta &= T\kappa, \\ \hat{\xi}_\theta &= \xi_{ph} = (1-\kappa)V_A. \end{aligned} \tag{5.39}$$

As we can see from Eq.(5.39), the factor κ will not only introduce extra excess noise, but also reduce the transmission estimation. κ is a value close to 1 with a small deviation due to the phase rotation operation, its impact on the excess noise also depends on the modulation variance V_A. In practice, we moreover need to quantify the value of κ, so that we can bound the phase noise due to the laser source. An example was shown in [65] where the value of $E_1 = E[\sin^2\theta]$ can be experimentally measured, where $E[\sin^2\theta] = 3\times 10^{-}3N_0$ for a modulation variance $V_A = 2.5N_0$. The phase noise is small such that $\sin\theta \simeq \theta$ and $\cos\theta \simeq 1 - 2/\theta^2$. Thus we can further determine:

$$E[\cos\theta] \simeq E[1 - 2/\theta^2] \simeq 1 - E_1/2. \tag{5.40}$$

By taking all these facts into account, the phase noise is $0.0075N_0$ with $V_A = 2.5N_0$. According to [65], such amount of noise can be considered as the trusted noise that is calibrated by Alice and Bob, so that the final secret key rate can be improved in practice. In the next subsection, we will find out the origin of the phase noise and study it from another angle.

Chapter 6

Side channel attacks in practical quantum key distribution systems

In the security proof of QKD, it is assumed that Eve can use every possible measure that is allowed by quantum mechanics to attack the open quantum channel, even if the technologies do not exist today. However, the security proof doesn't take account into all the implementation imperfections, which may open loopholes to Eve to compromise the practical security.

In recent years, quantum hacking or side channel attacks aiming on the QKD implementations has become a hot topic in quantum cryptography field. It is one of the most important challenges that QKD face to move forward to widely practical use. The concept of side channel attack is transverse and also applies to classical cryptography. Thus in this chapter, we start with a brief introduction of side channel attacks in classical cryptography. Then we give a brief overlook on the side channel attacks in discrete variable QKD. At last, we present detailedly and study various side channel attacks in continuous variable QKD; we also discusses possible countermeasures against these attacks.

6.1 Side channel attacks in classical cryptography

In classical cryptography, side channel attacks concerns the attacks on a cryptographic system which can be used to obtain information by exploiting physical properties of the system. Compared to mathematical cryptanalysis which focuses on the algorithm and protocol, side channel attack are usually specific to a given implementation, and for the same reason, are very critical to the practical security of real implementations. Smart cards and field-programmable gate array (FPGA) are often considered in side channel attacks, since

they often constitute the key elements of embedded system.

Here we give a glance on the different methods used in side channel attacks. A more detailed presentations of side channel attacks can be found in [75, 196]. There are several ways to classify the side channel attacks:

1. Considering the interference with the target system operation, side channel attacks can be divided into passive attacks and active attacks. Passive attacks only observe the target system's process, but do not disturb its operation. In contrast, active attacks influence the target system's behavior, such influence would be observed from the outside world, but may not be detected by the system. Usually, the target system works abnormally under active attacks.

2. Depending on the physical contact with the components of the target system, side channel attacks can be sorted as invasive attacks and non-invasive attacks. In invasive attacks, one needs to depackage the target module and access directly its internal components; for example, one can connect a probing needle to the data bus of a cryptographic module to observe the data transfer. On the other hand, non-invasive attacks externally exploit useful information which is not intentionally leaked from the system, the emission can be in the form of running time, power consumption, electromagnetic radiation etc.

3. Depending on the methods used in analyzing the sampled data, side channel attacks can be grouped in simple side channel attack and differential side channel attack. Simple side channel attack can extract the secret key directly from the sampled data of a single trace acquisition from the side channel. This kind of attack is based on a straightforward correlation between the secret information and side channel information. However, in particular, because too much noise appears in the measurements, the connection between leakage and secret keys is usually not obvious. In such case differential side channel attack is required. By using statistical analysis on several side channel acquisition traces, differential side channel attack can be used to guess the secret key even when the correlation between the side-channel leakage and the secret key is weak.

Note that the three axes above are orthogonal. The classification of a given side channel attack depends on the specific methods the attack uses. Some known side channel attack methods have broken the security of the hardware or software implementations in cryptographic systems such as block ciphers (DES, AES, Camellia, etc.), public key ciphers (RSA type ciphers, elliptic curve crypto-system, etc.) and stream cipher. Others have also been

used to break the security of implementations of signature schemes, message authentication code schemes and even networking systems. Examples of typical side channel attacks are listed below:

1. *Timing attacks*: The idea of such attack is to exploit the variance of processing time during a cryptographic operation. The attacker can extract the secret parameters by measuring the running time of each process in a cryptographic system. This attack was first proposed by Kocher [74] against a RSA implementation.

2. *Power analysis attacks*: The power consumption of a cryptographic device can also provide valuable information about the system operation and relevant secret parameters. Among different side channel attacks, power analysis attacks have been proven to be one of the most powerful attacks thanks to its efficiency and simplicity to implement. Various power analysis attacks have been successfully demonstrated against symmetric and public key ciphers. Power analysis attacks can be further divided into simple and differential power analysis, in which the simple ones extract the secret keys directly from the power trace, while the differential ones looks for statistical correlation between the power consumption and secret keys.

3. *Electromagnetic analysis attacks*: Each component of any electrical devices usually emits electromagnetic radiation when the device is under operation. An adversary can observe these emissions and find their relations with the underlying computation or data, and deduce the secret parameters. Electromagnetic side channels can often be used when power side-channels are unavailable. Such attacks can be also performed as simple or differential ones.

4. *Acoustic & visible light attack*: The acoustic emanations is one of the first discovered side channels. One of the primitive acoustic attacks (also as the first official reported side channel attack) was reported by Wright [188]: MI5, the British intelligence agency was trying to listen to the actions of a mechanical cipher machine used by the Egyptian Embassy in London, in order to break the encryption. Recently, it has been showed that the keyboard acoustic emanations can be used to learn English text [197]. The visible lights may also lead to powerful side channels. For example, one can recover the signal of a computer screen by detecting its reflection on a wall [77].

5. *Fault induction attacks*: A cryptographic system is assumed to operate in normal conditions to ensure the security it provides. It has however been shown that hardware faults and errors occurring can indeed lead to security breaks of cryptographic modules. Such kind of attacks is known as fault induction attack. A fault induction

attack usually consists two steps: fault injection and fault exploitation, where the difficulty often lies in the latter step. In the first step, a fault is injected to the target system, where an adversary can induce an inappropriate voltage, radiations and light or change the temperature to disturb the normal operation. Note such fault injection may damage the system which would result in permanent abnormal operation. In the second step, one would try to learn secret parameters from the erroneous behavior with the simple or differential analysis. As a good example, fault induction attack has been demonstrated on digital signature crypto-system using RSA with Chinese Remaindering Theorem (CRT) [70].

In the attack methods listed above, the first four ones are passive and typically non-invasive, since the power consumption, electromagnetic radiations etc. may passively leak information. Meanwhile, fault induction attacks are by essence active but not necessarily invasive. On the other hand, an adversary can combine several side channel analysis and techniques to achieve more powerful attacks.

6.2 Side channel attacks in discrete variable QKD systems

In quantum cryptography, side channel attacks can also aim at the practical implementations of QKD systems. However, the techniques mentioned above have not been exactly implemented in quantum hacking demonstrations. However, the side channel techniques from classical cryptography have inspired researchers in quantum cryptography to discover powerful attack against practical implementation of QKD systems. One of the most powerful attacks in discrete variable QKD system is known as blinding attack, which was first proposed by Makarov [116].

Blinding attack

The blinding attack can be considered as a fault induction attack, it targets the single photon detectors in DV QKD system. The original blinding attack [107, 116] on the avalanche photodiode (APD), consists in two steps: (1) Eve shines a bright light to Bob's APD to force the APD works in the linear mode instead of Geiger mode. Thus the APD is not sensitive to single photon anymore but acts as classical intensity photodiode. (2) Once the APD is set in linear mode, Eve employs the intercept resend attack and resends tailored light pulses to Bob. Such tailored pulses produce a "click" in one of Bob's detectors only if Bob chooses the same basis as Eve's re-prepared signal. As a consequence, Eve can control which detector of Bob generates a "click" each time. This will lead Eve to know the

secret key without disturbing the QKD system, in the sense that QBER has no noticeable change. Blinding attack has been successfully demonstrated on a commercial QKD system [107]. The applicability of the blinding attack is not limit to APD, but can be applied also to superconducting nanowire single-photon detector (SNSPD) [109, 110]. The blinding attack finally leads to a full field implementation of a perfect eavesdropper against a research system [42]. This highlights the importance of the blinding attack in the practical security of QKD. The early proposed countermeasure [192] have been shown that it was not sufficient to defeat the blinding attack [108]. Recently efficient countermeasures against the blinding attack has been proposed, where Bob randomly varies the efficiency of his single photon detector [83, 97]. Following the idea of blinding attack, demonstrations have shown that laser damage on APDs can also give opportunities to Eve for eavesdropping in QKD system [13].

Besides the blinding attack, several other quantum hacking strategies have been also proposed aiming at single photon detectors of DV QKD, such as time shift attack [137, 194], after gate attack [185], detector dead time attack [184] and phase remapping attack [190]. We will not detail the principle of these attack here, one can refer to the corresponding references for more information. Regarding these detector-based attacks, MDI QKD [100] could be a potential solution which removes all side channels threats from the detector part.

Besides single photon detector, other components can also become the target of side channel attacks, such as the laser source [166, 168], beam splitter [93], Faraday mirror [164], modulators [43, 62]. All these attacks essentially exploit the imperfections of QKD implementation, instead of using the sophisticated side channel analysis techniques such as differential power analysis. However, these techniques would be helpful for quantum hackers to discover more powerful attack, which would brings great challenge for the practical security of QKD. In this thesis, I focus on the study of implementation imperfection and related security issues of CV-QKD rather than side channel techniques in classical cryptography. We now move to a detailed presentation of recent reported attacks on CV QKD.

6.3 Side channel attacks in continuous variable QKD systems

In CV QKD, parameter estimation is crucial for Alice and Bob to evaluate the security. Most importantly, excess noise estimation is the reference for Alice and Bob to decide to abort the protocol or proceed to key generation. Any flaw in the excess noise estimation can possibly lead to serious security problem that Eve's action is undiscovered, which can fully

compromise the practical security of CV QKD. As we shall see, in most of the side channel attacks of CV QKD, Eve's action will influence the excess noise estimation in different ways.

In this section, we present and study various side channel attacks in CV QKD. All these attacks explorer the vulnerabilities of CV QKD implementations that allow Eve to break the practical security, some of them can be even achieved with today's technologies. We first start with the intercept-resend attack [104], which is combined with most of the side channel attacks in CV QKD. Then we present the shot noise calibration attacks [66, 111] and wavelength attacks [56, 57, 112] which mainly target Gaussian modulation protocols [48, 179]. We also present the side channel attacks target discrete modulation QKD protocols [195, 195], such as state-discrimination attack [58], single photon detector attack [165] and Trojan horse attack [72].

Besides introducing the original ideas of each attack in Gaussian protocols, we have moreover analyzed the relation between the excess noise estimation and the Eve's action, which clearly illustrate the threat of these attacks. Meanwhile, we also discuses the possible countermeasures against these side channel attacks.

6.3.1 Intercept-resend attack

We first introduce the intercept-resend attack in CV QKD. This attack is achievable with today's technologies and its security analysis has been studied in previous work [104, 121]. Most of the practical attacks have combined the intercept-resend attack or at least used its concept. A proof of principle demonstration has also been shown experimentally by Lodewyck et al. [104].

A full intercept-resend attack breaks any entanglement between Alice and Bob [104, 121]. In such attack, Eve intercepts all the pulses sent by Alice on the quantum channel and measures simultaneously the X and P quadratures, with the help of a heterodyne detection. Eve then prepares a coherent state according to her measurement results and sends it to Bob. Under such attack, the correlation between Eve and Bob data will be stronger than the one between Alice and Bob so that Eve always has an information advantage over Alice and Bob. Due to the heterodyne measurement disturbance and coherent state shot noise, the intercept-resend attack will introduce two shot noise units of excess noise. Moreover, in practice, Eve's device and her action can introduce additional technical excess noise on Bob's measurements. A full intercept-resend attack will therefore introduce in practice at least two shot noise units of excess noise, which will be spotted by Alice and Bob when they estimate the excess noise. In the following part, we will show the impact of the intercept-resend attack on the estimation of channel transmission and excess noise in the GMCS

protocol.

Attack description

A general description of an intercept-resend attack is shown in Fig.6.1, in which there are mainly two parts: the quantum channel between Alice and Bob, and Eve's station. Alice and Bob run the standard GMCS protocol while Eve performs intercept-resend attack. In order to simplify our analysis, we assume that Eve's station is located at Alice's output and that the channel transmission between Alice-Bob and Eve-Bob are equal.

In Fig.6.1, the quadrature information (X,P) is encoded and sent by Alice where (X_A,P_A) are centered Gaussian modulated variables of variance V_A; X_0,P_0 designate quadrature of a the vacuum state whose variances is one shot noise unit (N_0). Encoding the information onto a coherent state, we have:

$$\begin{aligned} X &= X_A + X_0, \\ P &= P_A + P_0. \end{aligned} \tag{6.1}$$

Eve in the middle cuts down the quantum channel and intercepts all the pulses sent from Alice. There are mainly two stages of Eve's action: quadrature measurement and quadrature re-preparation.

By using a heterodyne detection, Eve measures Alice's quadrature X_A and P_A simultaneously. Her measurement results (X_M,P_M) can be expressed as:

$$\begin{aligned} X_M &= \frac{1}{\sqrt{2}}(X_A + X_0 + X_0' + X_{N_{A,E}}), \\ P_M &= \frac{1}{\sqrt{2}}(P_A + P_0 + P_0' + P_{N_{A,E}}), \end{aligned} \tag{6.2}$$

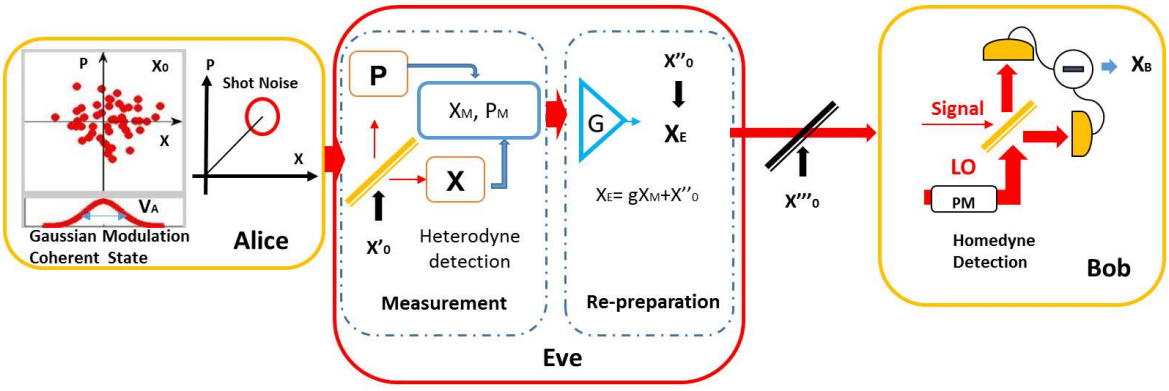


Fig. 6.1 General description of intercept-resend attack. Alice: prepares the coherent state with quadratures X and P; Eve: measurement and re-preparation stage, G:gain, Bob: performs the homodyne detection, AM:amplitude modulator, PM:phase modulator.

in which X_0 is a noise term due to the coherent state encoding of Alice while X_0' is a noise term due to 3 dB loss in the heterodyne detection. $X_{N_{A,E}}$ is a random noise that accounts for the technical noise of Alice's preparation and Eve's measurement process with its variance $\xi_{A,E}$.

In the re-preparation stage, Eve prepares a coherent state with quadratures (X_E, P_E) according to her measurement (X_M, P_M). Eve can also induce an amplification (g) on the data X_M which she will resend to Bob. In our further analysis, we only look at the X quadrature but the treatment for the quadrature P is totally symmetric. The X quadrature of the coherent state resent by Eve can be written as:

$$X_E = gX_M + X_0'' = \frac{g}{\sqrt{2}}(X_A + X_0 + X_0' + X_{N_{A,E}}) + X_0''. \tag{6.3}$$

Where, X_0'' is a noise term due to coherent state encoding of Eve. X_0, X_0' and X_0'' all follow a Gaussian distribution $\mathcal{N}(0, N_0)$ with their variance equal to one unit of shot noise N_0.

On Bob side, Bob performs a homodyne detection on the coherent state sent by Eve. Taken into account the loss and noise introduced by the channel, the measured quadrature X_B can be written as:

$$X_B = t(X_E + X_{N_{E,B}}) + \sqrt{1-t^2}X_0''' + X_{\text{ele}}. \tag{6.4}$$

After the propagation though the lossy channel, technical noise of Eve and Bob $X_{N_{E,B}}$ $(Var(X_{N_{E,B}}) = \xi_{E,B})$, vacuum noise $\sqrt{1-t^2}X_0'''$ $(Var(X_0''') = N_0)$ and electronic noise of Bob X_{ele} $(Var(X_{\text{ele}}) = v_{\text{ele}})$ are added to the quadrature prepared by Eve (X_E). Here $t = \sqrt{\eta T}$, where T is the channel transmission between Eve and Bob, and η is Bob's efficiency. The correlation between Alice and Bob quadratures and the variance of Bob quadrature measurements can be described as:

$$Cov(X_A, X_B) = \langle X_A X_B \rangle - \langle X_A \rangle \langle X_B \rangle = \frac{tg}{\sqrt{2}}\langle X_A^2 \rangle, \tag{6.5}$$

$$\begin{aligned} Var(X_B) = \langle X_B^2 \rangle - \langle X_B \rangle^2 =& \frac{t^2 g^2}{2}[Var(X_A) + 2N_0 + \xi_{sys}] + (1-t^2)N_0 + t^2 N_0 + v_{\text{ele}} \\ =& \eta T \frac{G}{2} Var(X_A) + \eta T \frac{G}{2}(2N_0 + \xi_{sys}) + N_0 + v_{\text{ele}}. \end{aligned} \tag{6.6}$$

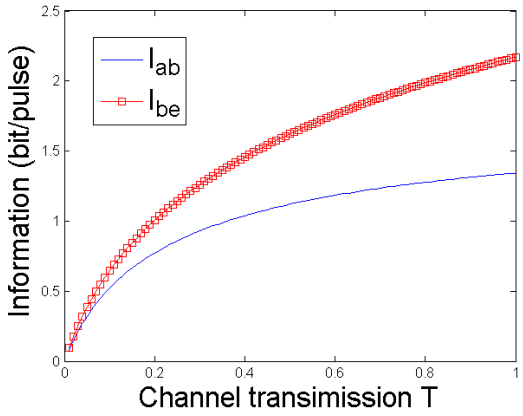


Fig. 6.2 Information evaluation under intercept-resend attack. Alice's variance $V_A = 20N_0$, efficiency of Bob $\eta = 0.6$, excess noise of electronics $v_{\text{ele}} = 0.01N_0$, excess noise due to intercept-resend attack $\xi_{IR} = 2N_0$, excess noise of system $\xi_{sys} = 0.1N_0$.

Information analysis

In Eq. (6.5) and (6.6), we can see that the estimated channel transmission now becomes $\hat{T} = \frac{t^2 g^2}{2} = \frac{TG}{2}$. In order to compensate the loss from the heterodyne detection, we can choose an amplification coefficient $g = \sqrt{2}$, so that the estimated value is not biased ($\hat{T} = T$). Based on Eq.(4.17), the excess noise estimation on Alice side is $\hat{\xi} = 2N_0 + \xi_{sys}$, where $\xi_{sys} = \xi_{A,E} + \frac{2}{G}\xi_{E,B}$. We can introduce a noise variable X_N which contains all the noise added to Bob's measurement, the variance of X_N is $\sigma_N^2 = \eta T \frac{G}{2}(2N_0 + \xi_{sys}) + N_0 + v_{\text{ele}}$.

As we can see, at least two units of excess noise have been added after the intercept-resend action. One can show that such added noise won't allow Alice and Bob to extract any secure keys. In fact, Namiki and Hirano [120] have deduced that, under the intercept-resend attack, a necessary condition to obtain secure key distribution is $\hat{\xi} < 2\hat{T}$. We can moreover observe that under such condition if $\hat{\xi} > 2$, then it implies $T > 1$, which is not a physical channel. It verifies that it's impossible to obtain a secret key under the intercept-resend attack. On the other hand, the intercept-resend attack is not more effective than individual or collective attack, where two units of excess noise is already much higher than the null key thresholds deduced by individual or collective attack for any channel transmission values (section 4.5.2).

In the end, we would like to quantify the information that gained by Eve under the intercept-resend attack. Particularly, we want to evaluate the mutual information between Alice-Bob and Eve-Bob. We have compared these mutual information in Fig.6.2 for different channel transmissions. As shown in 6.2, with reasonable simulation parameters, Eve always has information advantage over Alice and Bob under the intercept-resend attack,

which is another indication that there is no security between Alice and Bob at all under the attack.

6.3.2 Shot noise calibration attack

In CV QKD, shot noise is the variance of the homodyne detection output when local oscillator (LO) interferences with a vacuum mode. Since the estimated excess noise is expressed in shot noise units, if the shot noise is overestimated while all the other measurements remain unchanged, the estimated excess noise in shot noise unit will be underestimated. Alice and Bob will then overestimate their secret key rate which opens chance to Eve to learn a portion of the generated key. In a typical implementation (section.4.2.2), local oscillator is usually transmitted on the open channel between Alice and Bob which can be accessed by Eve. Such configuration leaves an opportunity to Eve to manipulate the LO in different ways.

The concept of calibration attack on CV QKD was first proposed by Ferenczi et al. [32]. The 'calibration' implies the fact that the shot noise level is calibrated while Eve can potentially bias the shot noise measurement by manipulating the LO pulse in different ways, and thus bias the excess noise estimation.

In [32], the authors propose a calibration attack, in which Eve first intercepts the signal and LO pulse as in the intercept attack. In the resending part, Eve changes both the intensity of signal and LO pulse and sends them to Bob. If the intensity of the signal pulse is larger than LO pulse, the analysis shows that Eve can have an information advantage over Alice and Bob. In [51], the authors proposed an equal-amplitude attack on a binary modulation CV QKD protocol, in which, Eve also first intercepts the signal and LO pulse as in intercept attack. According to her measurement results, she reproduces and resends two weak squeezed states with same intensity at the level of the signal pulses. It has been shown that the measured excess noise of Alice and Bob is much lower than the actual shot noise. So the excess noise arising from the attack can appear smaller than the tolerable threshold from the security proofs.

In this section, we focus on presenting and studying two attacks related to the shot noise calibration : Local oscillator intensity attack [111, 114] and calibration attack by changing the shape of LO pulse [66]. These two attacks both target the GMCS protocol and explore the implementation vulnerability related to LO manipulation by Eve. These attacks can break the security under certain assumptions of the shot noise calibration procedure, which will be presented in the following parts.

Traditional shot noise calibration

The exact procedure used to calibrate shot noise calibration depends on the implementation and is not considered in the security proofs of CV QKD. Thus, in practice, there is no standard method to proceed such calibration. However, traditionally, there are mainly two approaches to carry out shot noise calibration in CV QKD experimental implementations:

- *Method A*: Before the CV QKD protocol, Alice and Bob measure the LO power[1]; Bob measures the variance of homodyne detection when the LO pulse interferes with a vacuum mode (no signal). This variance of the homodyne detection output is considered as the calibrated shot noise value. Alice and Bob consider the measured values of intensity and shot noise variance as their references during whole CV QKD protocol. Such calibration procedure was considered in early implementations of CV QKD [50, 51] where the LO intensity was not monitored.

- *Method B*: Before the CV QKD protocol, Alice and Bob establish a linear relationship between the shot noise variance and the LO power. This can be achieved by varying the LO intensity and measuring the corresponding homodyne output variance when the signal input is vacuum. Then during the protocol running, Bob monitors the input power of LO pulse by diverting a small fraction of LO pulses with a beam splitter. By using the previously established linear relationship, Alice and Bob can estimate the shot noise variance level based on the measured LO power during CV QKD. This calibration procedure is usually considered in most of CV QKD implementations. [34, 68, 103].

Local oscillator intensity attack

In the analysis of this attack, we assume that Alice and Bob use the *Method A* (section.6.3.2) to calibrate the shot noise. However, during the key distribution of a GMCS protocol, each LO pulse's intensity can deviate compared to the initial LO intensity which is used for the shot noise calibration. The LO intensity fluctuation is not the quantum fluctuation of each LO pulse itself, but the deviation between the initial pulse for shot noise calibration and the pulse for the key distribution. LO pulse is a strong classical signal and its relative quantum fluctuations are small and can be assumed to be negligible [16]. However, if the LO intensity is not monitored, it gives a chance to Eve to attack the GMCS protocol and affects the parameter estimation of Alice and Bob.

[1] Since intensity is the power transferred per unit area, in practice, we measure the power LO pulse to refer to LO intensity.

LO intensity fluctuations can be quantified by a ratio $\gamma > 0$, where $|\alpha'_{lo}|^2 = \gamma|\alpha_{lo}|^2$, in which α_{lo} is the initial amplitude of LO pulse used for shot noise calibration while α'_{lo} is the actual amplitude of LO pulse. If Bob does not monitor LO intensity, the output of homodyne detection scales with the LO intensity α^2_{lo}. If we neglect the electronic noise, Bob's measured quadrature under LO intensity fluctuation γ can be given by:

$$X_{B,l} = \sqrt{\gamma} X_B \tag{6.7}$$

In [111], the authors have prosed a LO intensity fluctuation attack in which Eve manipulates the LO intensity under a collective attack model. In consequence, Alice and Bob will overestimate the secret key rate that they can generate, which shows that the security can be compromised.

A practical attack with LO intensity fluctuation Here we focus on explaining the idea of LO intensity fluctuation and its impact on practical security with current technology. Importantly, we will study the parameter estimation under the attack. Under the assumption of using *Method. A* (section.6.3.2), we moreover formalize an attack strategy that can break the practical security by taking advantage of LO intensity fluctuation. In this attack, Eve manipulates the LO intensity and combines it with an intercept-resend attack as described in section 6.3.1. In the resending part of the intercept-resend attack, Eve can prepare a LO pulse with an intensity freely chosen by her. Such manipulation of LO intensity can be seen as the LO intensity fluctuation which is considered in [111]. Fig. 6.1 can be used to describe this attack, where in addition Eve also controls LO intensity.

If Eve sends a LO pulse with lower intensity to Bob, the variance measurement of Bob will become smaller due to the reduction of LO intensity. However, if Alice and Bob don't monitor LO intensity they still normalize the variance with the previously measured shot noise. If we moreover consider the combined impact of intercept resend attack and the LO intensity fluctuation ratio γ, the state of Bob can be given as (with $g = 2$ as described in section 6.3.1):

$$X_{B,\gamma} = \sqrt{\gamma}[\sqrt{\eta T}(X_A + X_0 + X'_0 + X''_0 + X_{sys}) + \sqrt{1-\eta T} X'''_0] + X_{\text{ele}}. \tag{6.8}$$

Note that the electronic noise X_{ele} does not scale with LO intensity, since it is independent of LO intensity. We can express the variance of Bob based on $X_{B,l}$ measured data:

$$V_{B,\gamma} = \gamma[\eta T V_A + \eta T(2N_0 + \xi_{sys}) + N_0] + v_{\text{ele}}, \tag{6.9}$$

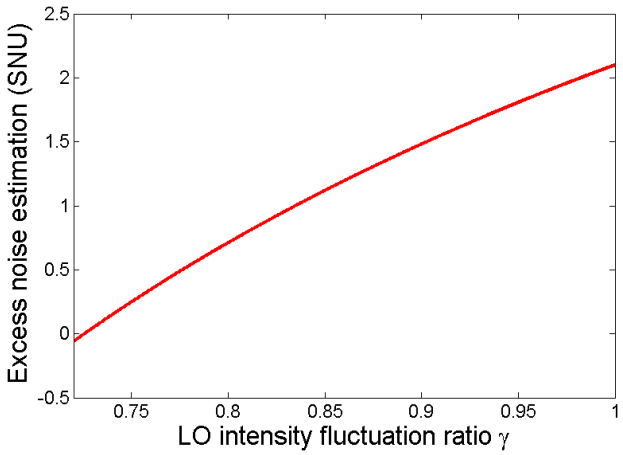


Fig. 6.3 Excess noise estimation versus LO intensity fluctuation ratio under the LO intensity attack. Alice's variance $V_A = 20N_0$, efficiency of Bob $\eta = 0.6$, excess noise of electronics $v_{\text{ele}} = 0.01N_0$, excess noise due to intercept-resend attack $\xi_{IR} = 2N_0$, excess noise of system $\xi_{sys} = 0.1N_0$, channel transmission $T = 0.4$.

N_0 is the calibrated shot noise value. As we can see from Eq.(6.9), the channel transmission estimation under the attack can be also deduced as:

$$\hat{T}_\gamma = \eta\gamma T. \tag{6.10}$$

Based on Eq.(6.9) and (6.10), the excess noise estimation in shot noise units of Alice and Bob can be expressed as:

$$\hat{\xi}_\gamma = \frac{V_{B,l} - N_0 - v_{\text{ele}}}{\eta\hat{T}_\gamma N_0} - \frac{V_A}{N_0} = \frac{\gamma[\eta T V_A + \eta T(2N_0 + \xi_{sys}) + N_0] - N_0}{\eta\gamma T N_0} - \frac{V_A}{N_0}. \tag{6.11}$$

As we can see in Eq.(6.11), $\hat{\xi}_\gamma$ varies with the fluctuation ratio γ, where γ is controlled by Eve. In this sense, Eve can manipulate the excess noise estimation of Alice and Bob by controlling the intensity of LO pulse. We show the relation between $\hat{\xi}_\gamma$ and γ in Fig.6.3, where we can see that, with realistic simulation parameters, $\hat{\xi}_\gamma$ can be set to any small value when γ changes. We have considered here a full intercept-resend attack, which means that no secure key can be generated as shown in section 6.3.1. However, the parameter estimation of Alice and Bob is biased, in particular, the excess noise estimation is manipulated and can reach arbitrary small values, leading to a security break: Alice and Bob will generate keys that are known by Eve.

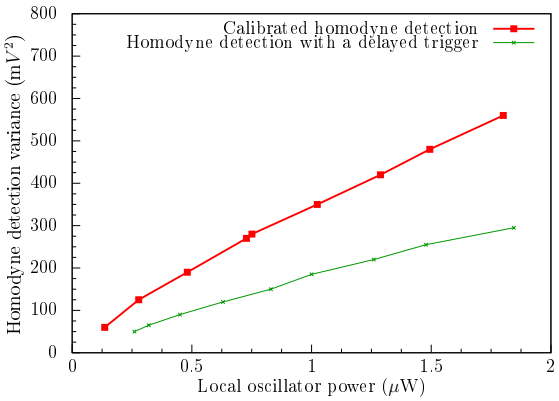


Fig. 6.4 Experimental results in [66]. Red: calibrated linear relationship between the variance of the homodyne detection measurements and the local oscillator power. Green: the linear relationship when delaying the trigger of the homodyne detection by 10 ns

Countermeasure As we can see, the main problem of the LO intensity attack is that Alice and Bob do not monitor the intensity of the LO pulse. However the actual shot noise varies with LO intensity. In [114], the authors have proposed a way to stabilize the LO intensity, Bob monitors the intensity of LO pulses by splitting a small part of LO pulse with a beam splitter and uses an amplifier or attenuator to adjust the LO intensity based on the monitoring value. Hence Alice and Bob can ensure that the received LO intensity pulse is correct. A beam splitter with tunable transmission can also serve this purpose for a simple implementation.

Another solution is considered in [68]: Alice and Bob calibrate the relationship between LO intensity and shot noise variance before the protocol and Bob measures LO intensity during the key distribution protocol and use it to rescale Bob's measurement results. Thus with this method Alice and Bob can ensure the shot noise estimation is correct. However such method can be defeated by the attack we will introduce in the next subsection.

Calibration attack by delaying the LO pulse

Jouguet et al. [66] have proposed a calibration attack in which an eavesdropper changes the shape of the LO pulse to introduce a delay on the clock trigger. As a consequence, the variance of the shot noise measurement can be lowered without changing the LO intensity. The value of the shot noise will be overestimated and consequently the excess noise will be underestimated. In the following, we will briefly explain this calibration attack and its countermeasure[66]. In this attack, it is assumed that Alice and Bob use *Method B* (section.6.3.2) to calibrate the shot noise. In a practical CV QKD system, a trigger signal of

clock is necessary to perform measurements with a pulsed homodyne detection. In particular, the maximum variance of homodyne output is achieved at the end of the optical pulse of duration τ ($\tau = 100$ ns in [66]). As we mentioned, the trigger signal is generated by LO pulse which can be possibly modified by Eve. For example, Eve can attenuate the beginning of the LO pulse, then it will induce a delay on the trigger signal. Once the trigger signal is delayed, the measurement of the homodyne detection output is not at the maximum point. So for a given LO power, the measured shot noise variance is smaller than the prediction arising from the calibrated linear relationship of Method B. In Fig.6.4, Jouguet et al. [66] have measured experimentally the linear relationship between the variance of the homodyne detection measurements and the LO power with and without a delayed trigger, where a delayed trigger of 10 ns results in a decrease of the detection response slope about 60% (the green line in Fig.6.4).

If the trigger signal has been delayed during the QKD protocol, the detection response slope decreases. Thus, if Alice and Bob still use the calibrated relationship then they will overestimate the shot noise variance, and consequently underestimate the excess noise. In this sense, Eve can manipulate the excess noise estimation by controlling the actual relationship between shot noise variance and LO power.

By changing the shape of LO pulse, a calibration attack strategy can be further proposed, which contains mainly two parts:

1. Eve performs a full intercept-resend attack.

2. Eve delays the LO pulses, in order to introduce a delay on the trigger used to perform the homodyne measurement at Bob.

The scheme of the attack is essentially depicted on Fig. 6.1, where in addition Eve resends delayed LO pulses according to the strategy. As we have discussed in Chapter 4, the total noise added on Bob's measurements is $V_N = \eta \hat{T} \hat{\xi} + N_0 + v_{\text{ele}}$, $\hat{T}$ is the channel transmission estimation and $\hat{\xi}$ is the excess noise estimation. If Eve doesn't delay LO pulses, N_0 is the real shot noise that matches with the previously calibrated liner relation.

If Eve can change the slope of the homodyne detection response by delaying the LO pulses and the shot noise can be wrongly estimated from the calibrated relation. The modified shot noise value is denoted as $\hat{N}_0'$. When Eve delays the LO pulse, it does not affect the total noise added on Bob (V_N) expressed in shot noise units, however the excess noise estimation ($\hat{\xi}_{cal}$) will be affected due to the change of shot noise estimation.

Then the excess noise estimations with/without calibration attack can be expressed as follow:

$$\hat{\xi} = \frac{V_N - N_0 - v_{\text{ele}}}{\eta \hat{T}}, \tag{6.12}$$

$$\hat{\xi}_{cal} = \frac{V_N - \hat{N}_0' - v_{\text{ele}}}{\eta \hat{T}}. \tag{6.13}$$

By considering these two equations, the relation between $\hat{\xi_{cal}}$ and $\hat{\xi}$ can be known:

$$\hat{\xi}_{cal} = \hat{\xi} + \frac{\hat{N}_0' - N_0}{\eta \hat{T}}. \tag{6.14}$$

$\hat{\xi}_{cal}$ need to be further transformed into shot noise units, where the shot noise estimation is the modified value ($\hat{N}_0'$):

$$\frac{\hat{\xi}_{cal}}{\hat{N}_0'} = \frac{N_0}{\hat{N}_0'} \left[\frac{\hat{\xi}}{N_0} + \frac{1}{\eta \hat{T}} \left(1 - \frac{\hat{N}_0'}{N_0} \right) \right]. \tag{6.15}$$

Excess noise estimation analysis From Eq. (6.15), we can see that Eve can manipulate the excess noise estimation by controlling the value of $\hat{N}_0'/N_0$, if the value becomes very large, the excess noise estimation under the attack can be arbitrary small. To achieve this, Eve should make Alice and Bob overestimate the shot noise ($\hat{N}_0'/N_0 > 1$), by decreasing the slope of homodyne detection response (Fig.6.4), as mentioned before.

As the second part of the calibration attack, Eve implements a full intercept-resend attack which will introduce at least two units of excess noise (section 6.3.1). In practice, a typical value of excess noise under a full intercept-resend attack is for example 2.1 [104], including 0.1 technical noise in practice. If Eve attacks the shot noise calibration by delaying the LO pulse then the estimated excess noise becomes $\hat{\xi}_{cal}$ (Eq. (6.15)). We show in Fig. 6.5 that Eve can control the excess noise estimation $\hat{\xi}_{cal}$ by changing the ratio $\hat{N}_0'/N_0$.

For different channel transmissions, Eve can choose different $\hat{N}_0'/N_0$ ratios to achieve a relatively low value of excess noise estimation (Fig.6.5). For example, with a transmission $T = 0.3$ or $T = 0.7$, Eve should apply a ratio $\hat{N}_0'/N_0 \approx 1.35$ or $N_0'/N_0 \approx 2$ so that the excess noise estimated by Alice and Bob becomes close to zero, they thus believe that they can still share a secret key, which in fact is not secure at all. The values of $\hat{N}_0'/N_0 \approx 1.35, 2$ are also realistic values as shown in Fig. 6.4.

Countermeasure: Real time shot noise calibration The previously described calibration attack is based on the fact that the shot noise calibration is overestimated using the method B calibration procedure. Alice and Bob can instead measure the shot noise in real time during the quantum communication phase. There are two approaches to realize this idea. The first approach is shown in Fig.6.6 (a), in which an optical switch or an amplitude modulator can

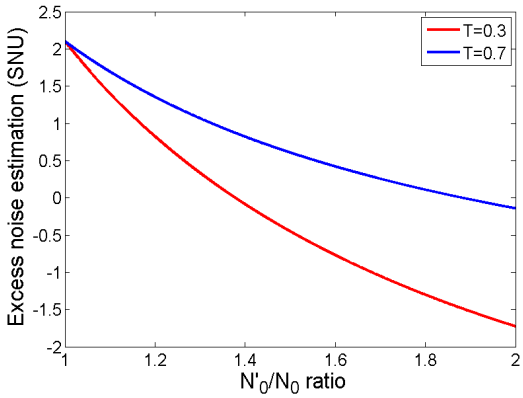


Fig. 6.5 Excess noise estimation versus $\hat{N}_0'/N_0$ ratio under the LO calibration attack. Alice's variance $V_A = 20N_0$, efficiency of Bob $\eta = 0.6$, excess noise of electronics $v_{\text{ele}} = 0.01N_0$, excess noise due to intercept-resend attack $\xi_{IR} = 2N_0$, excess noise of system $\xi_{sys} = 0.1N_0$, channel transmission $T = 0.3, 0.7$.

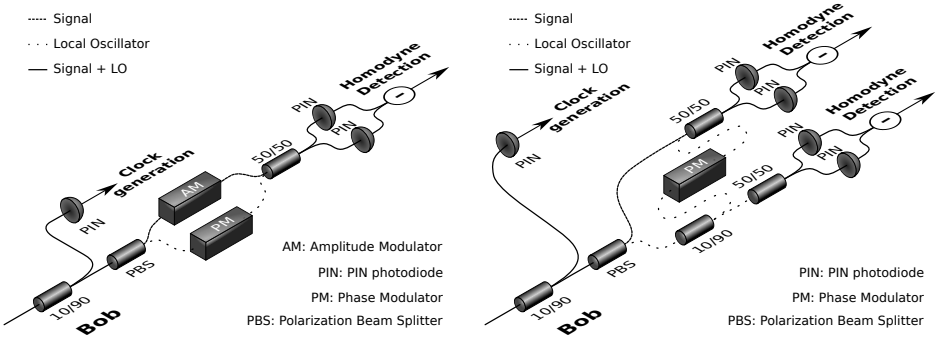


Fig. 6.6 Countermeasure against calibration attack [66]: Real time shot noise calibration. (a) Real-time shot noise measurement using an amplitude modulator on Bob's signal path. (b) Real-time shot noise measurement using a second homodyne detection on Bob's local oscillator path.

be used to randomly apply a strong attenuation (with attenuation ratio $r \approx 0$ and $r \approx 1$) on Bob's signal path. For those signal pulses with $r \approx 0$, Bob receives essentially a vacuum pulse and can measure the shot noise. For those signal pulses with $r \approx 1$, Bob can measure the quadratures.

Another approach is shown in Fig.6.6 (b), where an additional homodyne detector is introduced to measure the shot noise in real time. A 10/90 beam splitter is inserted into LO path to split part of LO intensity so that the additional homodyne detector can measure the variance of this LO part, where the shot noise variance is proportional to this variance with

the ratio of the beam splitter. These two approaches of real time shot noise calibration will be designated as the *Method C* for the shot noise calibration.

However a drawback of such countermeasure is that, since an additional amplitude modulator is introduced, the efficiency of homodyne detection will drop due to extra attenuation. Moreover a portion of the pulses are needed for the shot noise estimation and must be discarded for the secret key generation. These two facts finally result in decreasing the secret key generation rate and reachable distance. It has been shown that after implementing countermeasure, the maximum reachable distance for a positive key rate has dropped from 80 km to 50 km.

6.3.3 Wavelength attack

The wavelength attack has been first proposed on a DV QKD system [93], where Eve can take advantage of the fiber beam splitter whose intensity transmission is wavelength-dependent. By exploiting this property, Huang et al. [56] and Ma et al. [112] have then proposed a wavelength attack on a CV QKD system with no-switching protocol [179]. Huang et al. [57] have moreover extended such wavelength attack to a CV QKD system with GMCS protocol. The wavelength attacks are feasible even under the assumption that Alice and Bob use the real time shot noise calibration (*Method.C* [66]).

Wavelength dependent beam-splitter

Fused bi-conical taper beam splitter are widely used in the fiber QKD systems because of their low cost and low insertion loss. However, intensity transmission of fused bi-conical taper beam splitter is wavelength-dependent. The relationship between wavelength λ and the intensity transmission T_{bs} is given in Ref. [171]:

$$T_{bs}(\lambda) = F^2 \sin^2\left(\frac{C\lambda^{2.5}w}{F}\right). \tag{6.16}$$

where F^2 is the maximal power that is coupled, $C \cdot \lambda^{2.5}$ is the coupling coefficient, and w is the heat source width.

Among different commercial types of fused bi-conical taper beam splitter, the double wavelength type is the most popular one thanks to its stable performance in a wide wavelength range. Huang et al. [57] have experimentally tested the two double wavelength type $10/90$ (reflection/transmittance) and a $50/50$ fused bi-conical taper beam splitter in their laboratory, the results are shown in Table.6.1.

Table 6.1 The transmission T of Thorlabs double wavelength type $10/90$ beam splitter and a $50/50$ beam splitter with different wavelengths λ (nm)[57].

λ(nm)	1270	1290	1310	1330	1350	1370
T_{bs} (10 : 90 BS)	0.9050	0.9066	0.9020	0.8978	0.9014	0.8991
T_{bs} (50 : 50 BS)	0.5327	0.5253	0.5144	0.5052	0.5011	0.4965
λ(nm)	1390	1410	1430	1450	1470	1490
T_{bs} (10 : 90 BS)	0.8985	0.8938	0.8940	0.8985	0.8989	0.8985
T_{bs} (50 : 50 BS)	0.4931	0.4862	0.4902	0.4885	0.4908	0.4873
λ(nm)	1510	1530	1550	1570	1590	1610
T_{bs} (10 : 90 BS)	0.9012	0.8995	0.8956	0.9026	0.9022	0.9060
T_{bs} (50 : 50 BS)	0.4954	0.4960	0.5012	0.5069	0.5155	0.5265

Wavelength attack on GMCS protocol

The transmission of a fused bi-conical taper beam splitter varies with the wavelength due to its wavelength dependent property. Such property can be moreover taken advantage by an Eve to implement a side channel attack. Huang et al. [57] have proposed a wavelength attack on GMCS protocol, in which, there are mainly two parts: Eve implements a full intercept-resend attack; Eve prepares and resends two extra coherent state pulses, so that under certain regimes, she can possibly bias the excess noise estimation of Alice and Bob. The assumptions in this attack are: (1) The beam splitter of Bob's homodyne detection is wavelength dependent and its transmission property is in Table.6.1; (2) Alice and Bob use the improved shot noise calibration procedure that is proposed in section.6.3.2 [66] (*Method.C*): Monitoring LO intensity and measuring shot noise in real time (with attenuation ratio $r_1 \approx 0$ and $r_2 \approx 1$); (3)Alice and Bob use reverse reconciliation to distill the key.

The real time shot noise calibration procedure is considered in this attack, thus the parameter estimation is different from the one mentioned in Chapter 4. Since in practice, the realistic values of the attenuation ratios are considered as $r_1 = 0.001$ for shot noise estimation and $r_2 = 1$ for quadrature measurements [57]. So that the variance measurement of Bob concerning r_1 and r_2 is (i=1,2):

$$V_{B,i} = r_i \eta T (V_A + \xi) N_0 + N_0 + v_{ele} \tag{6.17}$$

The estimation of the excess noise and the shot noise thus become:

$$\begin{aligned} \hat{N}_0 &= \tfrac{r_2 V_{B1} - r_1 V_{B2}}{r_2 - r_1} - v_{ele}, \\ \hat{\xi} &= [\tfrac{V_{B2} - V_{B1}}{(r_2 - r_1)\eta T} - V_A]/\hat{N}_0. \end{aligned} \tag{6.18}$$

The scheme of this wavelength attack can be referred to Fig. 6.1, where Eve's re-preparation pulses are modified and Bob's beam splitter is wavelength dependent. In the first part of the attack, Eve launches a full intercept-resend attack, where she can have the information advantage over Alice and Bob (Full analysis in section 6.3.1). In this part, Eve measures the quadrature X and P of Alice with a heterodyne detection, then prepares the coherent states according to her measurement results, and sends them to Bob. Here the wavelength of the resent pulses is 1550 nm with 0.5 transmission through the beam splitter according to the Table.6.1. Additionally, Eve can change the slope of the homodyne detection response by delaying the trigger time, thus it will reduce the variance measurement, γ is considered as the reduction ratio of variance measurement that is controlled by Eve. In this case the shot noise is calibrated in real time, Alice and Bob can have correct estimation of shot noise with the attenuation ratio r_1 and r_2, instead of overestimating it as mentioned in previous section[66]. In this part, the variance measurement of Bob is :

$$V_{part1,i} = \gamma[r_i \eta T'(V_A + 2N_0 + \xi_{sys}) + N_0] + v_{ele}, \tag{6.19}$$

In which $2N_0$ is due to a full intercept-resend attack, γ and T' are introduced by Eve, where $T = \eta T'$ and T is the normal channel transmission.

In the second part of the attack, Eve prepares and resends two extra sets of fake LO/signal pulses with wavelengths different from the ones that Alice sends to Bob. Precisely, the wavelengths of the fake signal and LO pulses are following:

$$\begin{aligned} \lambda_1^s &= 1410nm, T_{bs1}^s = 0.4862, \\ \lambda_1^{lo} &= 1490nm, T_{bs1}^{lo} = 0.4873; \\ \\ \lambda_2^s &= 1310nm, T_{bs2}^s = 0.5144, \\ \lambda_2^{lo} &= 1590nm, T_{bs2}^{lo} = 0.5155, \end{aligned} \tag{6.20}$$

Since the 50/50 beam splitter is wavelength dependent, for different wavelength pulses, the transmissions through the beam splitter T_i^j $(i = bs1, bs2;\ j = s, lo)$ vary according to the Table.6.1. The notations of s and lo indicate that they will go to the signal path and the LO path, respectively. To achieve this, Eve can prepare the pulses in the same polarization mode as the signal or LO pulse of Alice.

Eve then randomly sends these two sets of fake LO/signal pulses to Bob with same probability, i.e 50% for one set ($\lambda_1^{s,lo}$), 50% for the other set ($\lambda_2^{s,lo}$). Since the fake LO/signal pulses prepared in the second part are in different wavelengths, they won't have any interference on Bob's homodyne detection. However, each pulse, it will generate its own shot noise

and since the transmittances deviate from 0.5, an extra differential current proportional to the light intensity will contribute to the output of homodyne detection. It can be seen as a similar case as the beam splitter is imbalanced, which we have analyzed in the chapter 5. An extra contribution on the first set of LO pulses is $(2T_{b1}^{lo}-1)\eta I_1^{lo} = D_1^{lo}$, which results in a noise variance proportional to the intensity I_1^{lo}. The contributions of all these pulses are following:

$$\begin{aligned} D_1^s &= (1-2T_{b1}^s)\eta I_1^s, \\ D_1^{lo} &= (2T_{b1}^{lo}-1)\eta I_1^{lo}, \\ \\ D_2^s &= (1-2T_{b2}^s)\eta I_2^s, \\ D_2^{lo} &= (2T_{b2}^{lo}-1)\eta I_2^{lo}. \end{aligned} \tag{6.21}$$

The assumption made by the authors is that for each pair of LO/signal: For a signal and a LO pulse, they cancel out their own noise variance contributions with each other, such that $D = D_1^s = -D_1^{lo} = -D_2^s = D_2^{lo}$. Therefore the fake LO/signal pulses only contribute their own shot noises since they don't interfere with each other. By considering such assumption and the procedure that the two sets of LO/signal pulses are randomly chosen to be sent Bob with a probability 50%, the authors have shown that Bob measurement variance in the second part is give by (more details in [57]):

$$V_{part2,i} = (1-r_i)^2 D^2 + (35.81 + 35.47 r_i^2)D. \tag{6.22}$$

On Bob side, Bob measures the quadratures that are prepared by Eve in the first part and also measures the additional pulses in the second part at same time. So the variance of Bob is the total of the ones in the first and the second part of the attack (i=1,2):

$$\begin{aligned} V_{B,i} = V_{part1,i} + V_{part2,i} \quad &= \gamma[r_i \eta T'(V_A + 2N_0 + \xi) + N_0] + v_{ele} \\ &+ (1-r_i)^2 D^2 + (35.81 + 35.47 r_i^2)D. \end{aligned} \tag{6.23}$$

Excess noise estimation analysis By taking $V_{B,1}$ and $V_{B,2}$ into Eq. (6.18), the estimation of shot noise and excess noise under this wavelength attack is:

$$\begin{aligned} \hat{N}_0 \quad &= \gamma N_0 + (1-r_1 r_2)D^2 + (35.81 - 35.47 r_1 r_2)D, \\ \hat{\xi}_{w1} \quad &= [(2N_0 + \xi_{sys}) + V_A - V_A \hat{N}_0 / N_0 \\ &\quad + (r_1 + r_2 - 2)D^2 / \eta\gamma T' + 35.47(r_1 + r_2)D] / \hat{N}_0. \end{aligned} \tag{6.24}$$

Since the noise variance is proportional to the LO intensity, the analysis of the wavelength attack have used the intensity in terms of photon number to represent the noise variance. The

shot noise variance is $N_0 = \eta I_{LO}$, where the intensity of LO is $I_{LO} = 10^8$ in the unit of photon number. In order to launch a successful attack, Eve needs to ensure that the estimation of shot noise is not biased, since the real time shot noise calibration is considered. On the other hand, Eve needs to bias the excess noise estimation.

Here is a numerical example to show the feasibility of this attack. According to Eq. (6.24), it is possible for Eve to make $\hat{N}_0 = N_0$ and $\hat{\xi}$ arbitrarily close to zero by choosing proper intensities of I_i^s, I_i^{lo} and γ. With $\gamma T' = T = 0.5$, $\xi_{sys} = 0.1$, $\eta = 0.5$, $V_A = 10N_0$, $r_1 = 0.001$ and $r_2 = 1$, a simple calculation shows that, by taking the following values into Eq. (6.24): $\gamma = 0.47$, $I_1^s = 3.72 \times 10^5$, $I_1^{lo} = 4.04 \times 10^5$, $I_2^s = 3.56 \times 10^5$ and $I_2^{lo} = 3.31 \times 10^5$, we have $\hat{N}_0 = 1.0002N_0$ and $\hat{\xi_{w1}} = 0.0026N_0$. With such an excess noise estimation, Alice and Bob will conclude that they can still share a secret key, however in the first attack part, Eve has learned all the information by launching a full intercept resend attack, so the practical security has been compromised.

Wavelength attack on no-switching protocol

Huang et al. [56] and Ma et al. [112] have proposed the wavelength attack on a CV QKD system with no-switching protocol [179]. As we have introduce in Chapter 4, the main difference of no-switching protocol's implementation, compared to GMCS protocol with homodyne detection, is that on Bob side, a heterodyne detection is used. The heterodyne detection consists two homodyne detections, which can measure the quadratures X and P simultaneously.

There are two assumptions in this attack: (1) all the beam splitters are wavelength dependent, where their transmissions are according to Eq.(6.16); (2) The efficiencies of the two homodyne detections are both equal to η. (3) Alice and Bob monitor LO intensity while the linear relationship between LO power and shot noise variance has been calibrated (*Method B* in section.6.3.2); (4) Alice and Bob use reverse reconciliation to distill the key.

In this wavelength attack (Fig.6.7), Eve also uses the concept of intercept resend attack as described in 6.3.1, where Eve first cuts down the quantum channel and measures Alice's quadratures X and P by using a heterodyne detection (Eq. (6.2)). On the resending part, instead of preparing the states according to her heterodyne measurement, Eve resends a fake signal pulse and a fake LO pulse with wavelengths λ_s and λ_{lo} and intensities $|a'_s|^2$ and $|a'_{lo}|^2$. Due to the wavelength-dependent property of the beam splitters in different stages, the transmissions of these two pulses are T_1 and T_2. With the help of the wavelength tunable laser diodes and intensity modulators, the wavelength and amplitude of these fake states are carefully chosen to satisfy the following conditions:

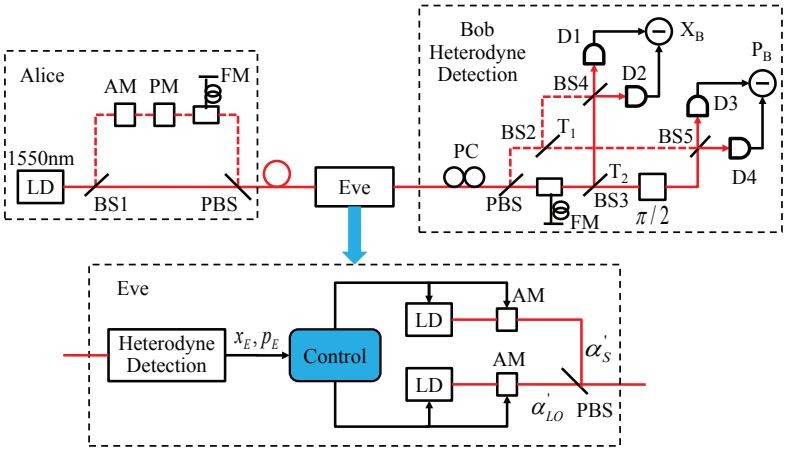


Fig. 6.7 Wavelength attack setup on a practical CVQKD system with heterodyne detection (dashed line: signal path, solid line: LO path) [56, 111]. LD, laser diode; AM, amplitude modulator; PM, phase modulator; FM, Faraday mirror; PBS, polarization beam splitter; PC, polarization controller; D, photodetector; and BS1-5, beam splitters. BS2-5 have the same wavelength-dependent property.

$$\begin{aligned}(1-T_1)(1-2T_1)|a_s'|^2-(1-T_2)(1-2T_2)|a_{lo}'|^2 &= \sqrt{2\eta T}X_M|a_{lo}|,\\ T_1(1-2T_1)|a_s'|^2-T_2(1-2T_2)|a_{lo}'|^2 &= \sqrt{2\eta T}P_M|a_{lo}|.\end{aligned} \tag{6.25}$$

In which $|a_{lo}|^2$ is the LO intensity of Alice, η is the efficiency of homodyne detection, T is the channel transmission between Alice and Bob, (X_M, P_M) is the measured quadrature Eq.(6.2). If Eve chooses the same wavelength and intensity of fake LO pulse as the same as the one sent by Alice, then the transmission of all the beam splitters on the fake LO pulse are equal to 0.5, which turns Eq.(6.25) into:

$$\begin{aligned}(1-T_1)(1-2T_1)|a_s'|^2 &= \sqrt{2\eta T}X_M|a_{lo}|,\\ T_1(1-2T_1)|a_s'|^2 &= \sqrt{2\eta T}P_M|a_{lo}|.\end{aligned} \tag{6.26}$$

Since the fake LO pulse is in same wavelength and amplitude as the one Alice prepares, the shot noise estimation is not biased, it remains equal to N_0 and it won't rise an alarm for Bob when he monitors LO intensity. Eve sends both the fake signal pulse and modified LO pulse to Bob. Bob then measures both quadratures simultaneously with his heterodyne detection. The wavelengths of the fake signal pulse and fake LO pulse are different so that they cannot interfere on the homodyne detection. The outputs of homodyne detection consists of two parts: interferences between fake signal pulse and vacuum state; between fake LO pulse and

vacuum state. The measurements of Bob will thus become:

$$\begin{aligned} X_{B,wave} &= \sqrt{\frac{\eta T}{2}}(X_A + X_0 + X_0' + X_{sys}) + X_{NW}, \\ P_{B,wave} &= \sqrt{\frac{\eta T}{2}}(P_A + P_0 + P_0' + P_{sys}) + P_{NW}. \end{aligned} \tag{6.27}$$

$X_{B,wave}$ or $P_{B,wave}$ describes the output state of the homodyne detection that Bob initially measures X quadrature (with phase choice $\varphi = 0$) or P quadrature (with phase choice $\varphi = \pi/2$), where the fake signal pulse goes through BS2/BS4 and the fake LO pulse go through BS3/BS4. X_{NW} or P_{NW} is the deviation of $X_{B,wave}$ or $P_{B,wave}$ from X_M or P_M. X_{sys} or P_{sys} is the excess noise due to the device's imperfections and the factor $\sqrt{1/2}$ is due to the heterodyne detection. The variance of X_{NW} and P_{NW} can be approximated by (more details in [111]):

$$V_{NW} \approx 2\eta T_2(1-T_2)(1-2T_2)^2 N_0 + 8\eta T_2(1-T_2)^2 N_0 \tag{6.28}$$

In fact V_{NW} is the sum of the fake signal pulse's and the LO pulse's shot noises after they go through the beam splitters in the heterodyne detention part, since they both contribute their own shot noise, instead of interfering on the homodyne detection. We can then further express the variance of Bob under this wavelength attack as:

$$V_B = \frac{\eta T}{2}(V_A + 2N_0 + \xi_{sys}) + 2\eta T_2(1-T_2)(1-2T_2)^2 N_0 + 8\eta T_2(1-T_2)^2 N_0 \tag{6.29}$$

Excess noise estimation analysis By using Eq.(6.29) for excess noise estimation (Eq.(4.17)), one can deduce that:

$$\hat{\xi}_{w2} = 2N_0 + \xi_{sys} - \frac{2N_0}{\eta T} + \frac{2V_{NW}}{\eta T}, \tag{6.30}$$

where $\hat{\xi}_{w2}$ is a function of the transmission T_2 (since V_{NW} depends on T_2) and Eve can control T_2 by changing the wavelength of the resent signal pulse. As mentioned before, the excess noise estimation is further normalized in shot noise units. In Fig.6.8, we show the excess noise estimation of Alice and Bob versus transmission T_2, where Eve is able to induce a small value of excess noise by selecting proper wavelength of the fake signal and thus controlling the beam splitter's transmission (T_2). In the security analysis of [56] and [112], the authors have analyzed the conditional variance $V_{B|A}^{wave}$ under the individual attacks. To show the feasibility of the attack, if the conditional variance $V_{B|A}^{wave}$ under the attack is smaller than $V_{B|A}$, then it means that Alice and Bob underestimate $V_{B|A}^{wave}$, so that an attack is possible. Such analysis is actually equivalent to the excess noise analysis, since

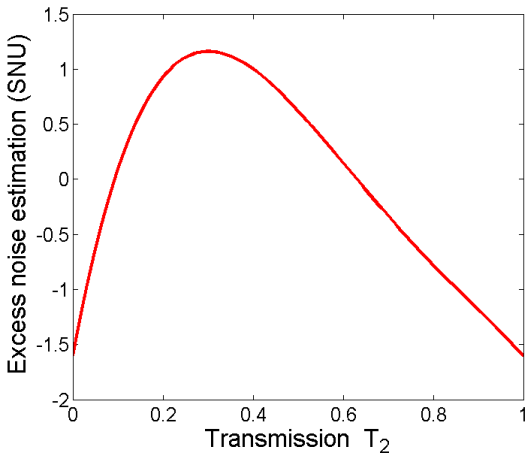


Fig. 6.8 Excess noise estimation of Alice and Bob vs beam splitter transmission T_2 (fake sigal) under wavelength attack. Alice's variance $V_A = 20$, efficiency of Bob $\eta = 0.6$, channel transmission $T = 0.9$, excess noise due to intercept-resend attack $\xi_{IR} = 2$, excess noise of system $\xi_{sys} = 0.1$.

the conditional variance $V_{B|A}$ quantifies the total noise that add to the final measurement, where $V_{B|A} = \eta T\xi/2 + N_0$, ξ is the excess noise that secret key is possible. Thus if $V_{B|A}^{wave} < \eta T/2\xi + N_0$, the wavelength attack reduces the estimated excess noise, and the practical security is compromised.

Countermeasure on wavelength attack Unlike the calibration attack focusing on manipulating the shape of LO pulses, the wavelength attack aims at wavelength-dependent beam splitters: instead of modifying LO pulses, Eve re-prepares extra signal and LO pulses with different wavelengths and intensities to influence the excess noise estimation. A possible countermeasure consists in adding wavelength filters before the detection (to ensure that the wavelengths used for the attacks are close to the system wavelength, which would force the attacker to use high-power signals to launch the attack), and a monitoring of the local oscillator intensity (to detect these high-power signals). An improved shot noise real time calibration is also proposed as a countermeasure: with one more attenuation ratio ($r_3 = 0.5$) to test the linearity of the excess noise estimation, the attack can be prevented [81].

6.3.4 State-discrimination attack

All of the attacks that we have studied so far, are aiming on the CV QKD protocols with Gaussian modulations. Other than Gaussian modulation protocols, discrete modulation CV QKD protocols (section 4.4) have been proposed as another approaches [87, 119, 122, 195],

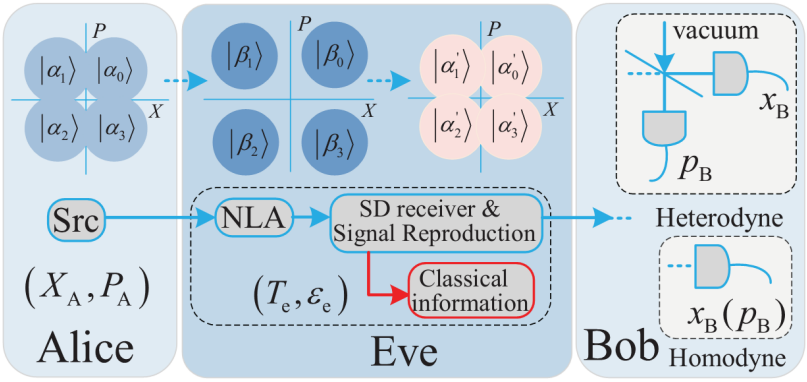


Fig. 6.9 The state-discrimination attack on a four-state protocol [58].

which may potentially improve the secure distances, since the exist error correction codes are at high efficiency for long distance. In discrete modulation protocols, Alice encodes the information on the phase of some nonorthogonal coherent states, and Bob performs homodyne detection to obtain the quadratures to extract the discrete key information. As mentioned in Chapter 4, there are several discrete modulation protocols based on the ways that Alice prepares the coherent states, such as binary modulation [195], four state [87], six state [122] and multi-letter protocol [167].

It has been shown in theory and experiments that a state-discrimination receiver can discriminate the nonorthogonal coherent states with error rates below the standard quantum limit which referred to the limit of a perfect homodyne detection [29, 174]. It implies that, with a proper eavesdropping strategy, Eve may detect the phase information of signal states without introducing too much disturbance on the quantum channel by using a state-discrimination receiver [29, 174].

In such state-discrimination attack [58], the authors have proposed an eavesdropping strategy, which can be seen as an alternative intercept-resend attack (section 6.3.1) where Eve uses a state-discrimination receiver to performer the measurements instead of using the heterodyne detection. In the next part, we explain the details of this state-discrimination attack targeting on the four state protocol [87].

Attack description In the four state protocol [87], Alice randomly sends one of the four coherent states with same probability $\frac{1}{4}$: $|\alpha_k\rangle = |\alpha e^{i(2k+1)\pi/4}\rangle$ with $k \in \{0,1,2,3\}$, where α is the amplitude and is related to the modulation variance $V_A = 2\alpha^2$. On Bob side, Bob randomly measures one or both of the two quadratures X and P by performing homodyne detection or heterodyne detection. After reconciliation and privacy amplification, Alice and Bob can share a secret key.

The assumptions in the state-discrimination attack: (1) Alice and Bob use reverse reconciliation to distill the key, (2) Bob performs a perfect homodyne detection where the efficiency $\eta = 1$ and electronic noise $v_{\text{ele}} = 0$, (3) Alice and Bob use a perfect channel to connect with each other, where the channel transmission $T = 1$.

In this attack (Fig.6.9), Eve in the middle cuts down the quantum channel and intercepts all the coherent states sent by Alice. She then amplifies the received states with a heralded noiseless linear amplifier [12]. The purpose of such noiseless linear amplifier is in principle to decrease the error rate for the discrimination of the four nonorthogonal states. A probabilistic noiseless linear amplifier can amplify the amplitude of a coherent state without introducing extra noise. So that the use of noiseless linear amplifier can decrease the error probability of the state-discrimination receiver at the expense of a rate decrease. After amplifying the states with a probabilistic noiseless linear amplifier, Eve prepares the coherent states $|\beta_k\rangle\langle\beta_k| = |g\alpha_k\rangle\langle g\alpha_k|$ with a success probability P_s that depends on the gain of amplifier $g \geqslant 1$. When Eve fails to amplify the states (i.e. with probability $1 - P_s$), a vacuum state $|0\rangle\langle 0|$ is generated. The amplification of the noiseless linear amplifier can be described as a trace-preserving operation:

$$\mathscr{T}[|\alpha_k\rangle\langle\alpha_k|] = P_s|g\alpha_k\rangle\langle g\alpha_k| + (1 - P_s)|0\rangle\langle 0| \tag{6.31}$$

The success probability of the noiseless linear amplifier depends on several experimental factors. Based on the general principles in [12], its upper bound can be expressed as:

$$P_s \leqslant \frac{1 - e^{-|\alpha|^2}}{1 - e^{-|g\alpha|^2}} \tag{6.32}$$

Eve then measures the amplified coherent states $|\beta_k\rangle\langle\beta_k|$, $k \in \{0,1,2,3\}$ with her state-discrimination receiver to capture the encoded classical information of $|\alpha_k\rangle\langle\alpha_k|$: the phases of the states. Then she re-encodes on the coherent states according to her state-discrimination measurements. Since her state-discrimination receiver is not perfect, there can be a certain probability that Eve can not discriminate the coherent states. According to [29, 174], the error probabilities to discriminate the four amplified nonorthogonal coherent states in a quadrature phase-shift keying (QPSK) is:

$$P_e = 1 - [1 - \frac{1}{2}\text{erfc}(\sqrt{|g\alpha|^2/2})]^2, \tag{6.33}$$

in which $\text{erfc}(x) = \frac{2}{\sqrt{\pi}} \int_{-} \infty^{\infty} e^{-t^2} dt$. When Eve fails to discriminate the state $|\alpha_k\rangle$, she thus produces a state $|\alpha'_k\rangle \neq |\alpha_k\rangle$ with a failure probability P_e. The reproduced states of Eve thus

contain three parts: The coherent states $|\alpha_k\rangle$ with a successful discrimination probability $1-P_e$; The coherent states $|\alpha'_k\rangle$ with a error discrimination probability P_e; The vacuum state that have been introduced with the noiseless linear amplifier. It is moreover assumed that Eve uses a lossless and noiseless channel to connect Bob, Bob performs a perfect homodyne detection ($\eta = 1$,$v_{\text{ele}} = 0$), and Eve's failure discriminations will introduce error bits. By performing a homodyne detection, Bob measures the states that are sent by Eve, the state of Bob under these assumptions can be expressed as:

$$\rho_B = P_s(1-P_e)|\alpha_k\rangle\langle\alpha_k| + P_sP_e|\alpha'_k\rangle\langle\alpha'_k| + (1-P_s)|0\rangle\langle 0| \tag{6.34}$$

For the security analysis, it is necessary to evaluate the parameter estimation under such attack: channel transmission and excess noise. From Eq.(6.34), the channel transmission becomes:

$$\hat{T}_{SD} = P_s(1-P_e) \tag{6.35}$$

And Bob' variance measurement becomes:

$$V_B = P_sV_A + N_0 \tag{6.36}$$

Thus we can further express the excess noise estimation by taking Eq.(6.35) and Eq.(6.36) into Eq.(4.17):

$$\hat{\xi}_{SD} = \frac{V_AP_e}{1-P_e} \tag{6.37}$$

Where the contributions of excess noise are from the vacuum state $|0\rangle$ and the error state $|\alpha'_k\rangle$. From Eq.(6.37), we can see the excess noise is mainly due to the error probability that Eve discriminates the coherent states. Based on $\hat{T}_{SD}$ and $\hat{\xi}_{SD}$, Alice and Bob can moreover evaluate the Holevo bound under collective attack to estimate the information that can be accessed by Eve. Meanwhile, the real mutual information between Bob and Eve, I_{BE}, can be seen as classical information that Eve sends to Bob, and can be derived from Bob's measured variance Eq.(6.36), and the conditional variance $V_{B|E} = P_s(1-P_e) + P_sP_e + 1 - P_s = 1$ as:

$$I_{BE} = \frac{1}{2}\log_2(P_sV_A + N_0) \tag{6.38}$$

To analyze whether Eve can steal information without being noticed by Alice and Bob, one need further compare the mutual information I_{AB} between Alice and Bob, the Holevo information χ_{BE} that is estimated by Alice and Bob, and the real mutual information I_{BE} between Eve and Bob. For a successful attack Eve must verify: $I_{AB} > \chi_{BE}$ so that Alice and Bob believe that they can extract a secret key (with perfect reconciliation efficiency, $\beta = 1$)

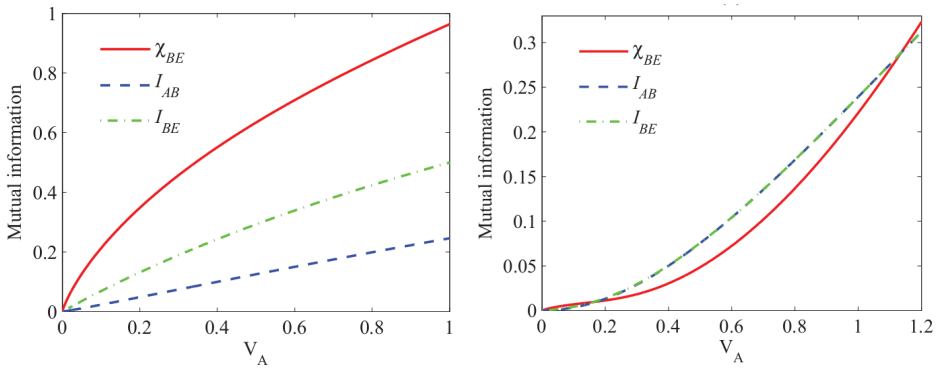


Fig. 6.10 The mutual information I_{AB}, χ_{BE} and I_{BE} as a function of modulation variance V_A of the four-state protocol under the state-discrimination attack for (a) Gain value g = 1 (b) Gain value g = 6 [58].

and $I_{BE} > \chi_{BE}$ so that Eve can have more information than the upper Holevo bound that Alice and Bob estimate for Eve, thus Alice and Bob underestimate Eve's information and still believe there is a secret key, so the security is compromised.

In Fig. 6.10, the authors compare the three values I_{AB}, χ_{BE} and I_{BE} for different gain value g. In which Fig.6.10 (a) shows that with $g = 1$ (the amplifier doesn't work), with relatively small amplitudes of the states, Eve will have relatively high error probability to discriminate the coherent states that she intercepts. If the error probability is high, then the excess noise estimation becomes large Eq.(6.37) and Alice and Bob will conclude $\chi_{BE} > I_{AB}$, and abort the protocol. However, when Eve uses the noiseless linear amplifier, for example, with a gain value $g = 6$ (Fig.6.10 (b)), the error discrimination probability can be dramatically decreased so that excess noise becomes relatively small, thus according to Alice and Bob's estimation, $I_{AB} > \chi_{BE}$. However the real information that Eve can get is more than the Holevo information estimated by Alice and Bob $I_{BE} > \chi_{BE}$. Hence Eve can have information advantage over Alice and Bob, and the security of discrete modulation CV QKD has been compromised.

In [58], the authors have moreover studied a lower error discrimination bound for P_e, that is allowed in quantum mechanics, known as Helstrom bound. Such Helstrom bound can help Eve to optimize her strategy to achieve a better performance. We can consider the error discrimination bound P_e is between the bound that is deduced in Eq.(6.33) and the Helstrom bound. Thus Eve's state-discrimination attack can at least achieve the performance that is shown in Fig.6.10 (b) with a gain value $g = 6$.

Countermeasure: Decoy state method Such attack can be prevented by the decoy state method which is introduced in [87] for the four-state protocol. In this improved four-state protocol, Alice randomly prepares and sends the state for the key generation σ_{key} and the decoy state σ_{decoy} with probability p and $1-p$, such that the mixed state that Bob will measure is a Gaussian state σ_G.

$$p\sigma_{key} + (1-p)\sigma_{decoy} = \sigma_G \tag{6.39}$$

Alice can randomly use the Gaussian state σ_G to perform parameter estimation or use σ_{key} for key distribution. When Alice and Bob introduce decoy states, Eve cannot distinguish whether the state is σ_{key}, σ_{decoy} or σ_G. According to [87], with the decoy state method, the four state protocol can thus be treated as a Gaussian modulation CV QKD protocol. The discrimination receiver is noneffective for Gaussian states, since the key information is encoded in both the amplitudes and the phases of the signal states, which are not QPSK signals. In this case, the state-discrimination attack will be not more effective than the general collective attacks.

Single photon detector attack

Other than using a state discriminator to discriminate the coherent states, a single photon detector also can be used for this purpose. In [165], the authors have proposed a single photon detector (SPD) attack on a binary modulation CV QKD protocol [195], in which, Eve launches a modified intercept resend attack where she uses a single photon detector instead of heterodyne detection to measure the two states $|\alpha\rangle$ and $|-\alpha\rangle$ of Alice. The single photon detector can be seen as an alternative state discriminator that introduces enough low error probability to discriminate the two states of Alice. The excess noise due to such error can be low enough to allow Alice and Bob to extract a secret key under certain conditions (See the analysis in Sec.6.3.4). The security analysis in [165] has shown that the error rate that the single photon detector introduces can be even smaller than the error rate due to the channel loss under certain parameter regions, so that Eve can learn information without being noticed. The main specificity of single photon detector attack, compared to the state-discrimination attack is that Eve uses a single photon detector as the state discriminator and the target protocol is a binary coherent state modulation protocol.

Similarly to the state-discriminate attack, such attack does not apply to the Gaussian modulation protocol, hence the decoy state method mentioned before can be also a countermeasure. Another possible countermeasure, for Alice and Bob, would be to reconstruct the probability density distribution of each state measured by Bob, since Eve's attack will affect

the probability density distribution of Bob's measurement.

6.3.5 Trojan horse attacks on CV QKD

Trojan-horse attack was first proposed against some DV QKD systems [43]. In Trojan horse attack, Eve shines a bright light towards Alice or Bob's device and probes its reflected light to read out the phase or amplitude information of different modulators. Trojan-horse attack can be achieved by different techniques such as, Optical Frequency Domain Reflectometry (OFDR), Optical Time Domain Reflectometry (OTDR) or even homodyne detection.

Recently, a Trojan-horse attack has been proposed by Khan et al. [72] on practical CV QKD systems, in particular, on the binary modulation protocol [71, 195] where Alice encodes the information on the phase of two coherent states ($|\alpha\rangle$ and $|-\alpha\rangle$). Unlike the other attacks we have introduced so far, this proposed attack has been demonstrated in experiment as a proof of principle. In the demonstration, the authors only consider Alice's device, since the goal for Eve is to read out the phase encoded information of Alice's phase modulator.

In this attack Fig.6.11, Eve prepares a strong signal as Trojan-horse pulse (contains up to 10^9 photon) and a LO pulse. Eve uses a 50/50 fiber coupler to connect her device with Alice's and sends the Trojan-horse pulse into Alice's device. After traveling through the components in Alice, the strong Trojan-horse pulse will attenuate to a very weak signal due to the loss of components. This weak back reflected signal pulse carries the phase information of the phase modulator which can be recovered by interfering with the LO pulse on the two homodyne detections of Eve. These two homodyne detections can be seen as a heterodyne detection which can measure both X and P quadratures. By performing such Trojan-horse attack, Eve can try to discriminate between the two phase modulated coherent

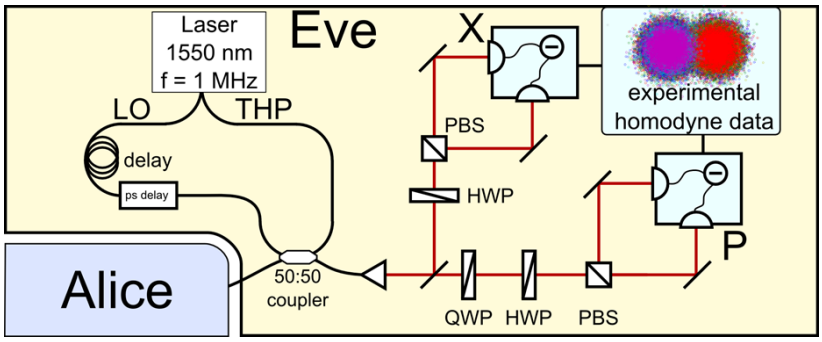


Fig. 6.11 The Trojan-horse attack, Eve's setup. LO: local oscillator; THP: Trojan-horse pulse; PC: polarization controller;HWP/QWP: half quarter wave plate; PBS: polarizing beam splitter [72].

states at the output of Alice.

The principle of this Trojan-horse attack is simple, however technical issues can make the attack difficult to realize in practice. The first challenge is the delay of the LO pulse with respect to the back reflected pulse: the delay of LO pulse needs to be carefully controlled so that it is as same as the delay of the Trojan-horse pulse which travels inside Alice's device. A fiber patch cord and a motorized picosecond delay stage can be used to control the delay of the LO pulse so that when the back reflected signal pulse returns to Eve's device, it overlaps with the prepared LO pulse. Another challenge is the visibility of Eve's detection. In order to increase the visibility, the transmission of the Trojan-horse pulse inside Alice need to be optimized. To achieve this, polarization controllers are used in Eve's setup and the variable attenuator of Alice is set to 0 dB. Moreover, homodyne detection data is further processed with calibration pulse [71] to eliminate the error due to the phase drifts of the two coherent states prepared by Alice. After considering all these issues, Khan et al. [72] have achieved a success rate of 98.73 % to read out the phase modulation information of Alice to discriminate the two coherent states.

To study the security impact of Trojan-horse attack, it is essential to analyze the parameter estimation, especially the estimated excess noise as the previous attacks show. As matter of a fact, the Trojan horse attack could possibly introduce additional excess noise. Such analysis thus requires a full implementation of CV QKD protocol. Moreover, it is also important to quantify the information that is gained by Eve. Since the Trojan-horse pulse may pass once or twice through Alice's modulator, the phase-space distribution of states received by Eve may not coincide with the distribution set by Alice. So the mutual information between Alice-Bob, and Bob-Eve still remains as a question according to the analysis in [72]. This question further determines whether Eve can steal information without being noticed. For the Gaussian modulation protocols [68], since Alice uses both phase and amplitude modulators to achieve a Gaussian modulation and it is also a continuous modulation, it will be much more difficult for Eve to read out the amplitude and phase information at same time. Further study still need to be done to show the feasibility of the Trojan-horse attack on Gaussian modulation CV QKD protocols [72].

A possible countermeasure against this Trojan-horse attack could be to employ a watchdog detector to monitor the incoming light into Alice or to use an optical isolator at the entrance of Alice's device to prevent incoming Trojan-horse pulses.

6.3.6 Conclusions

In this section, we have presented the main side channel attacks against CV QKD. For the attacks against Gaussian protocols, we have evaluated the impact of Eve's action on

the excess noise estimation. The bias of the excess noise estimation leads Alice and Bob to underestimate Eve's accessed information, which brings chance for Eve to fully compromise the security without being discovered.

Regarding to the vulnerability in the practical implementation of CV QKD system, manipulating the LO is an important issue that Eve can possibly take advantage of. LO manipulation problem concerns all the CV QKD protocol, where LO pulse is sent in a open channel. It concerns not only Gaussian protocols, but also discrete modulation protocols. The main approach to comprise the practical security in CV QKD is to manipulate LO in different ways so that Eve can bias the estimation of shot noise and thus the excess noise. The threat of such attacks can be removed if Alice and Bob monitor LO in a proper way or measure the shot noise in real time.

In order to compromise the security of discrete modulation CV QKD protocols, an option for Eve is to discriminate the coherent states of Alice without introducing too much noise. To achieve this, Eve can use a state discriminator or single photon detector to perform measurements. Another possible approach for Eve is to use a Trojan horse pulse to probe the encoded information of the phase modulator that Alice uses. However, all of these attacks aiming on the discrete modulation protocols cannot be easily applied against Gaussian modulation protocols.

Finally, almost all the successful side channel attacks in CV QKD combine the intercept-resend attack with their own strategies or at least use the concept of intercept-resend. The intercept resend attack can be achieved with simple implementation from today's technologies. By launching such attack, Eve learns all the encode information of Alice with the cost of introducing two shot noise units of excess noise on Bob's measurement. In order to perform an efficient side channel attack, Eve must combine the intercept-resend attack with a particular strategy to bias the excess noise estimation of Alice and Bob. As we have seen, there are several possibilities for Eve to achieve this by taking advantage of vulnerability in CV QKD implementations. In the end, we summarize all these side channel attacks in CV QKD in Table.6.2.

Table 6.2 Summary of various side channel attacks in CV QKD.

Attack CV QKD	**Protocol**	**IR**	**Target**	**Countermeasure**
Equal-amplitude [51]	Binary modulation	•	State of LO, signal	LO intensity monitor
Calibration [32]	GMCS	•	Intensity of LO, signal	LO intensity monitor
Calibration [111, 114]	GMCS	•	LO intensity fluctuation	LO intensity monitor
Calibration [66]	GMCS	•	LO pulse shape	Real time shot noise measurement
Wavelength [57]	GMCS	•	Beam splitter; Wavelength of LO, signal	Wavelength filter
Wavelength [56, 112]	No-switching	•	Beam splitter; Wavelength of LO, signal	Wavelength filter; Check the linearity of excess noise
State-discrimination [58]	Four state	○	Signal state discrimination	Decoy state method
Single photon detector [165]	Binary modulation	○	Signal state discrimination by SPD	Decoy state method; Probability distribution reconstruction
Trojan horse [72]	Binary modulation	∗	Alice's modulators	Watch dog detector; Isolator

•: Attack uses an intercept-resend attack (Heterodyne detection) [104];
○: Attack is of the intercept-resend type, but the intercept does not use the heterodyne detection;
∗: Attack has no relation with intercept-resend attack.

Chapter 7

A new side channel attack on CV QKD system: Saturation attack

As we have seen from the previous chapter, side channels are crucial problem for practical implementations of CV QKD, since security proofs do not take into account all possible experimental imperfections. In this chapter, we present a new loophole and show that it can be used to attack a practical CV QKD system implementing Gaussian-modulated coherent state (GMCS) protocol [50]. Instead of attacking local oscillator, we aim at the homodyne detection located on Bob side, specifically, the electronics of the homodyne detection. We propose an attack that we name saturation attack, consisting in a full intercept-resend attack [104] combined with the exploitation of the induced nonlinear response of homodyne detection. Under this saturation attack, we can show that Eve can manipulate the measurement results on Bob's side and get information without being discovered. Importantly, our attack is practical that can be realistically launched against existing implementations.

This chapter is organized as follows. We first present the idea of the saturation attack in section 7.1. Then in section 7.2, we show the influences of saturation effect on a practical homodyne detector in experiments. In section 7.3, we propose a practical attack using the saturation of the homodyne detection electronics. In section 7.4, we use numerical simulations to analysis the estimation of channel transmission, excess noise and secret key rate under the saturation attack. In the end, we give the counter measures and conclusions in section 7.5 and 7.6.

7.1 Principle of the saturation attack

Unlike the attacks aiming at the local oscillator, we introduce a new attack which explores the non linearity of the homodyne detection response. A fundamental assumption in the security proofs of CV QKD is that the response of homodyne detection is linear with respect to input quadrature. This assumption is necessary because parameter estimation implicitly assumes the linearity of Bob quadrature measurement with respect to the value sent by Alice. However, this linearity assumption does not hold if Bob's homodyne detection is operated in a non linear regime. For a practical detector, the linearity region is limited. If the value of input quadrature is too large, linearity may not be verified, leading to a saturated behavior.

From section 4.2.4, we can observe that, based on the Gaussian linear model (Eq.(4.10)), the parameter estimation consists in the evaluation of the covariance matrix. The covariance matrix is invariant under any linear shifts. Indeed the security evaluation in CV QKD relies solely on the evaluation of second order moments of the quadrature, while the first order moments (mean value) are not monitored. This leaves Eve a chance to manipulate the mean value of quadratures. Combining this with exploiting the existence of a detector's saturation region, a strategy for Eve is to actively introduce a large displacement on the quadrature received by Bob to force the homodyne detection to operate in its saturated region. Since mean value of the homodyne detection output is by default not monitored, Eve can freely decide to displace the mean value. This can induce a non linear response on the detector which is under her control. This enables Eve to influence Bob's measurement results. Parameter estimation can thus be biased and the value of the parameters will depend on the displacement, which is actively controlled by Eve.

In brief, here is our idea for a new attack: by actively introducing a displacement on the quadratures measured by Bob, Eve can force the detector to work in the saturated region which will help her to manipulate the measurement results and thus the parameter estimation. Importantly, unlike the attacks in which the shot noise measurement is influenced, saturation attack does not bias the shot noise estimation but influences the excess noise estimation.

7.2 Saturation of homodyne detection

Saturation typically occurs when the input field quadrature overpasses a threshold. This threshold depends on parameters of homodyne detector's electronics, such as the amplifiers linearity domain or the data acquisition card (DAQ) range (Fig.7.1). If Bob measures

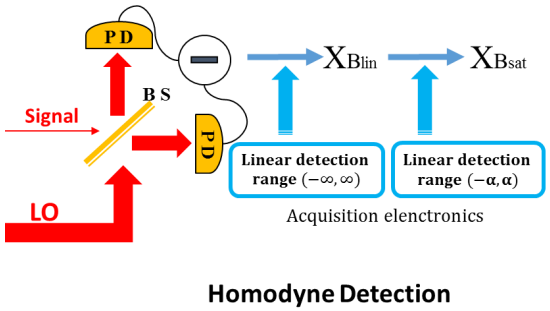


Fig. 7.1 A practical homodyne detection with different linear detection range. PD: photodiode, BS: Beam splitter, LO: Local oscillator

quadrature signals falling outside of the detector's linearity range, the variance is modified by a factor that depends on the detector linearity range and on the data range. However, it will typically lead to a wrong variance estimation. The linear model (Eq.(4.10)) in particular does not hold under saturation of the homodyne detection.

7.2.1 Saturation model

The quadrature measurement at Bob side is carried out by a homodyne detection. This measurement is performed via the subtraction of two photo-currents followed by an electronics for amplification and acquisition. Usually we consider that the linear detection range of the acquisition electronics is infinite which was the case considered in the previous section. We then denote the measured quadrature as $X_{B_{lin}}$ (X_B in section II). However, in a practical homodyne detector, no matter how large the linear detection range is, it can not be infinite. We propose a saturation model (Eq.(7.1)) with predefined upper and lower bounds of the homodyne detection response. For values between these two bounds, the response of homodyne detection behaves normally, otherwise the response is constant. To simplify the analysis, we have assumed in this model that the linear detection range can be described by one single parameter, α, intrinsic to the detector. Under this saturation model with the linear detection limit $[-\alpha, \alpha]$, the measured quadrature is called $X_{B_{sat}}$. The relation between $X_{B_{sat}}$ and $X_{B_{lin}}$ is the following:

$$\begin{array}{lll} & X_{B_{lin}} \geqslant \alpha, & X_{B_{sat}} = \alpha \\ if & |X_{B_{lin}}| < \alpha, \quad then & X_{B_{sat}} = X_{B_{lin}} (\alpha >> 1) \\ & X_{B_{lin}} \leqslant -\alpha, & X_{B_{sat}} = -\alpha \end{array} \tag{7.1}$$

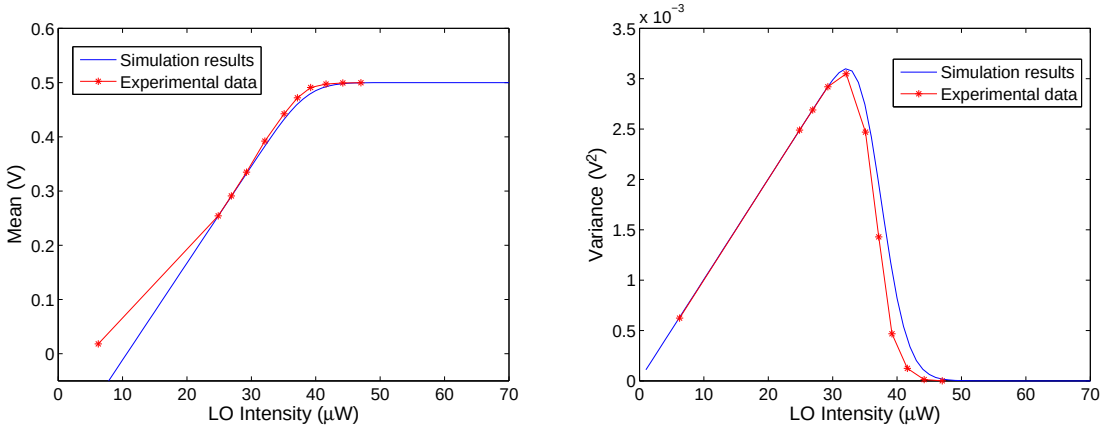
As expected, if $\alpha \to \infty$, the saturation model returns to the linear model. In a typical (non saturated) CV QKD implementation, the value of α is large enough to ensure that field quadratures almost never overpass the limit of homodyne detection response. Alice and Bob can make sure of this by choosing a relativity high value of α^2 for Bob's detector compared to number of photons impinging on the detector. Since the limit α is fixed only by the acquisition electronics linearity, a practical way to guarantee with high probability that $\alpha >> X_{B_{lin}}$ is to lower the LO intensity so that the shot noise value $N_0 << \alpha^2$. In general, input quadrature modulation variance are calibrated in shot noise units which depends on LO intensity and Alice can choose a Gaussian modulation with $\langle X_{B_{lin}} \rangle = 0$ and $Var(X_{B_{lin}}) << \alpha^2$ so that the detector does not saturate. However, as mentioned earlier this procedure cannot cope with situation where $X_{B_{lin}}$ is strongly displaced between emission and reception after propagation through a open channel, as it will be the case in saturation attack.

7.2.2 Experimental observation of saturation

In a practical balanced homodyne detector, the common mode rejection ration (CMRR) is not infinite and the mean value of the homodyne detection in absence of input signal is affected by the imbalance, leading to: $\langle X_{B_{0,lin}} \rangle = \varepsilon I_{LO}$, where I_{LO} is the LO intensity, and ε is the imbalance factor which is dependent on experimental imperfections such as photodiode quantum efficiency mismatch or beam-splitter imbalance.

Accounting for these imperfections (but in absence of saturation), the relation between measured noise variance (in volts squared) and LO intensity (in watt) usually can be written as: $Var(X_{B_{0,lin}}) = AI_{LO} + B$ (We neglect the quadratic part since in our case the LO power is relatively low) [16]. I_{LO} is the LO intensity, A is linear with I_{LO} and is related to shot noise while B is independent of I_{LO} and is related to electronic noise. The value of A and B can be determined experimentally.

Due to the limit linearity range of acquisition electronics in our homodyne detector, our experimental shot noise measurement tests have revealed that the measured shot noise variance can drop non-linearly when the LO intensity is above a certain value. We have analyzed this behavior with the saturation model presented in the previous subsection and compared its prediction to experimental measurements of Fig.7.2. We display the measured variance and mean of the homodyne detection output with vacuum input signal for different LO intensities. When the homodyne detection is not saturated, the shot noise variance is linear with respect to LO intensity. Due to imperfect balancing of homodyne detection, measured mean value $\langle X_{B_{0,lin}} \rangle$ also increases linearly with LO intensity. In Fig.7.2, such linear behavior can be observed when LO intensity is below 35 μW in our setup. Due to the imbalance of homodyne detection (ε), mean value of homodyne detection output



(a) (b)

Fig. 7.2 Shot noise measurements of homodyne detection (a) Mean value $\langle X_{B_{0,sat}} \rangle$vs LO Intensity. (b) Shot noise variance $Var(X_{B_{0,sat}})$ vs LO Intensity.

can become very high when LO intensity is relatively strong. If those values overpass the threshold of DAQ card (in the present case 0.5 V), the detection response is saturated and its output becomes constant (Fig.7.2 (a)). As a consequence, measured shot noise variance strongly decreases (Fig.7.2 (b)) when such saturation happens.

In order to check the validity of the saturation model introduced in Eq.(7.1), we have simulated the expected homodyne detection response with our saturation model and compared it with experimental measurement. We first determine the parameter ε, A and B from linear fit on $\langle X_{B_{0,lin}} \rangle$ and $Var(X_{B_{0,lin}})$ versus LO intensity, in the linearity domain ($I_{LO} < 35\mu w$). The saturation parameter α is here fixed by our DAQ range: $\alpha = 0.5V$. We then apply the saturation model Eq.(7.1) to the variable $X_{B_{0,lin}}$ to obtain $X_{B_{0,sat}}$. We compute the mean $\langle X_{B_{0,sat}} \rangle$ and the variance $Var(X_{B_{0,sat}})$, which result in the behavior shown in Fig.7.2. For the measured shot noise under saturation, the simulation results match very well with our experimental data. It indicates that our proposed saturation model is realistic and can be further used to interpret our saturation attack.

7.3 Attack strategy

7.3.1 Intercept-resend attack

Before we explain our attack strategy, we first remind the intercept-resend attack which is an important part of the saturation attack (section 6.3.1). The intercept-resend attack in CV QKD is achievable with today's technologies and its security analysis has been studied

in previous work [104]. A full intercept-resend attack breaks any entanglement between Alice and Bob. In such attack, Eve intercepts all the pulses sent by Alice on the quantum channel and measures simultaneously the X and P quadratures, with the help of a heterodyne detection. Eve then prepares a coherent state according to her measurement results and sends it to Bob. Under such attack, the correlation between Eve and Bob data will be stronger than the one between Alice and Bob so that Eve always has an information advantage over Alice and Bob. However due to the heterodyne measurement disturbance and coherent state shot noise, the intercept-resend attack will introduce two shot noise units of excess noise. Moreover, in practice, Eve's device and her action can introduce additional excess noise on Bob's measurements. So a full intercept-resend attack in practice will introduce at least two shot noise units of excess noise, which will be spotted by Alice and Bob when they estimate the excess noise and secret key rate. This assumes that the estimation procedure is not biased, we will see that a saturation attack can, on the contrary, bias the estimation and lead to an attack.

7.3.2 Saturation attack strategy

In our saturation attack, the goal of Eve is to combine a full intercept-resend attack with an induced saturation of Bob detector, so that Bob's measurements and Alice-Bob parameter estimation are biased and lead to accept key material that is totally insecure (potentially fully known by Eve). In order to learn the information on data encoded by Alice, Eve can simply launch a full intercept-resend attack [104]. By inducing saturation, Eve can bias the estimated excess noise below the null key threshold (calculated under collective attack in asymptotic limit[38, 123]), so that according to their estimation, Alice and Bob will assume they can obtain a positive key rate while no secure key can be obtained from the actual correlation.

We propose a general description of our saturation attack in Fig.7.3, in which there are mainly two parts: Alice-Bob channel, and Eve's station. Alice and Bob run the standard GMCS protocol while Eve performs saturation attack. In order to simplify our analysis, we assume that Eve's station is located at Alice's output and that the channel transmission between Alice-Bob and Eve-Bob are equal. Moreover, we assume that Alice and Bob measure their shot noise and monitor the LO intensity in real time [66], with two transmission coefficients of signal randomly decided at Bob side ($\eta_1 = 1, \eta_2 = 0$).

In Fig.7.3, Eve in the middle cuts down the quantum channel and intercepts the signal sent from Alice. There are mainly two stages of Eve's action: quadrature measurement and quadrature re-preparation. By using a heterodyne detection, Eve measures Alice's quadra-

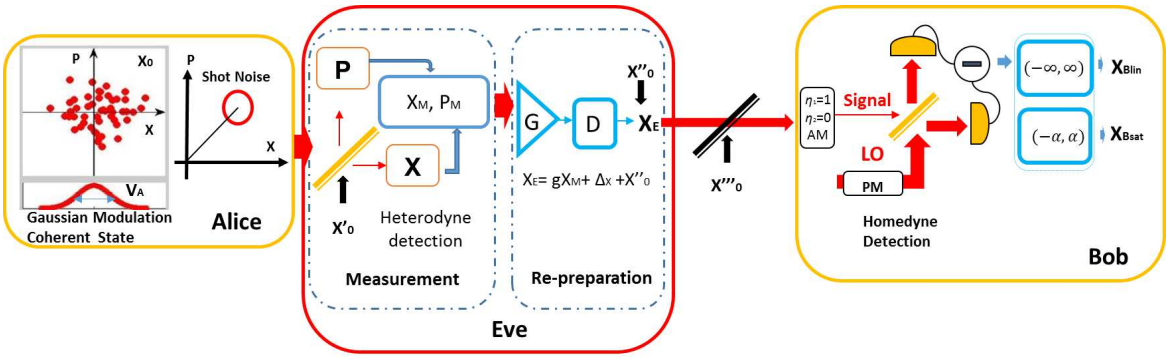


Fig. 7.3 General description of GMCS CV QKD under the saturation attack. Alice: prepares the coherent state with quadratures X and P; Eve: measurement and re-preparation stage, G:gain, D:displacement; Bob: performs the homodyne detection, AM:amplitude modulator, η_1, η_2: signal transmission coefficients, PM:phase modulator, $-\alpha, \alpha$: linear working range.

ture X_A and P_A simultaneously. Her measurement results (X_M, P_M) are expressed as:

$$X_M = \frac{1}{\sqrt{2}}(X_A + X_0 + X_0' + X_{N_{A,E}}) \tag{7.2}$$

$$P_M = \frac{1}{\sqrt{2}}(P_A + P_0 + P_0' + P_{N_{A,E}}) \tag{7.3}$$

Where X_0 is a noise term due to the coherent state encoding of Alice while X_0' is a noise term due to 3 dB loss in the heterodyne detection. $X_{N_{A,E}}$ is a random noise that accounts for the technical noise of Alice's preparation and Eve's measurement process with its variance $\xi_{A,E}$.

In the re-preparation stage, Eve prepares a coherent state with quadratures (X_E, P_E) according to her measurement (X_M, P_M). Eve can also induce a displacement (Δ_X, Δ_P) and an amplification (g) on the data X_M before optical encoding. In our further analysis, we only look at the X quadrature but the treatment for the quadrature P is totally symmetric. The resend quadrature of Eve can be written as:

$$X_E = gX_M + \Delta_X + X_0'' = \frac{g}{\sqrt{2}}(X_A + X_0 + X_0' + X_{N_{A,E}}) + \Delta_X + X_0'' \tag{7.4}$$

Where, X_0'' is a noise term due to coherent state encoding of Eve. X_0, X_0' and X_0'' all follow $\mathcal{N}(0, N_0)$ with their variance equal to one unit of shot noise (N_0).

Introducing displacement on coherent states is experimentally achievable [187] and since Eve prepares the new states, the displacement parameter (Δ_X, Δ_P) can be freely chosen by her. In order to compensate the loss from the heterodyne detection, we can choose an amplification coefficient $g = \sqrt{2}$.

Linear detection On Bob side, Bob measures the quadrature sent by Eve by performing a homodyne detection. We first consider Bob uses a homodyne detection whose linear detection range is infinite (Fig.1). The measured quadrature ($X_{B_{lin}}$) can be written as

$$X_{B_{lin}} = t(X_E + X_{N_{E,B}}) + \sqrt{1-t^2}X_0''' + X_{ele} \tag{7.5}$$

After the propagation though the lossy channel, technical noise of Eve and Bob $X_{N_{E,B}}$ ($Var(X_{N_{E,B}}) = \xi_{E,B}$), vacuum noise $\sqrt{1-t^2}X_0'''$ ($Var(X_0''') = N_0$) and electronic noise of Bob X_{ele} ($Var(X_{ele}) = v_{\text{ele}}$) are added to the quadrature prepared by Eve (X_E). Here $t = \sqrt{\eta T}$, where T is the channel transmission between Eve and Bob, and η is Bob's efficiency. The correlation between Alice and Bob and the variance of Bob can be described as:

$$Cov(X_A, X_{B_{lin}}) = \langle X_A X_{B_{lin}} \rangle = \frac{tg}{\sqrt{2}}\langle X_A X_A \rangle + t\Delta_X \langle X_A \rangle = \frac{tg}{\sqrt{2}}Var(X_A), \tag{7.6}$$

$$\begin{aligned} Var(X_{B_{lin}}) = \langle X_{B_{lin}}^2 \rangle - \langle X_{B_{lin}} \rangle^2 =& \frac{t^2 g^2}{2}[Var(X_A) + 2N_0 + \xi_{sys}] + (1-t^2)N_0 + t^2 N_0 + v_{\text{ele}} \\ &+ t^2\Delta_X^2 - t^2\Delta_X^2 = \eta T\frac{G}{2}Var(X_A) + \eta T\frac{G}{2}(2N_0 + \xi_{sys}) + N_0 + v_{\text{ele}} \end{aligned} \tag{7.7}$$

In Eq. (7.6) and (7.7), we can see that with an ideal linear detection range, the induced displacement Δ_x has no influence on the measurement results, since the terms of Δ_x has been removed in both correlation and variance measurements.

Under linear detection and intercept-resend attack with the gain $G = g^2 = 2$, the correlation (Eq.(7.6)) is not modified by Eve's action, so that the estimated channel transmission is not biased ($\hat{T}_{lin} = T$). Based on Eq.(7), the excess noise estimation on Alice side is $\hat{\xi}_{lin} = 2N_0 + \xi_{sys}$, where $\xi_{sys} = \xi_{A,E} + \frac{2}{G}\xi_{B,E}$. Similarly in section 4.2.4, we introduce the noise variable X_N which contains all the noise added to Bob's measurement, the variance of X_N is $\sigma_N^2 = \eta T\frac{G}{2}(2N_0 + \xi_{sys}) + N_0 + v_{\text{ele}}$.

Saturation detection As we have seen the linearity of the homodyne detection cannot be guaranteed by arbitrary large detection range, a more realistic model is taking saturation into account, with a linear detection region limited between α and $-\alpha$ (Eq.(7.1)). Under this modified model, we denote $X_{B_{sat}}$ as the quadrature measured by Bob. $X_{B_{sat}} = X_{B_{lin}}$ only if $X_{B_{lin}}$ does not overpass the linear detection limit $[\alpha, -\alpha]$. Otherwise the measurement

results are constant, equal to the value of detection limit.

$$\begin{aligned} & X_{B_{lin}} \geqslant \alpha, && X_{B_{sat}} = \alpha, \\ if\ & |\, X_{B_{lin}} \,| < \alpha, then && X_{B_{sat}} = t(X_E + X_{N_{E,B}}) + \sqrt{1-t^2}X_0''' + X_{ele}, \\ & X_{B_{lin}} \leqslant -\alpha, && X_{B_{sat}} = -\alpha \end{aligned} \tag{7.8}$$

Since Eve actively induces the displacement (Δ_X, Δ_P), she can freely set the displacement value so that $X_{B_{lin}}$ can partially overpass the limit $[-\alpha, \alpha]$. In further analysis, we consider $\Delta = t\Delta_X$ as the displacement value of Eve. In order to realize a fixed value of Δ, Eve can choose a proper Δ_X once she knows t, that typically depends on the distance between Eve and Bob. The measured quadrature $X_{B_{sat}}$ will be influenced by the saturation due to the induced displacement. The correlation $\langle X_A X_{B_{sat}} \rangle$ and Bob's variance $Var(X_{B_{sat}})$ will both decrease due to saturation. As we shall see, parameter estimation affected by saturation can lead to excess noise below the null key threshold.

In the next section, we will show that under certain conditions of our attack strategy, Eve can manipulate the channel transmission and the excess noise estimated by Alice and Bob, so that her intercept resend action can remain under cover while fully compromising the practical security of the CV QKD protocol.

7.4 Security Analysis

7.4.1 Parameter estimation under the saturation attack

The channel transmission and excess noise estimation fully characterize the quantum channel of CV QKD, we thus only need to analyze the impact of saturation on these two estimated parameters. It is in particular critical to evaluate whether an induced saturation can reduce the excess noise estimation as thus opens the door to severe attacks.

Channel transmission estimation

Under the saturation attack, Alice encodes X_A and Bob measures $X_{B_{sat}}$ (Eq.(7.8)) and they evaluate the correlation coefficient: $Cov(X_A, X_{B_{sat}})$ (calculation details can be found in Appendix A.1.). From this correlation coefficient (Eq.(A.3)), the estimation of the channel transmission under saturation attack, $\hat{T}_{sat}$, can be expressed as:

$$\hat{T}_{sat} = T\frac{G}{8}[1 + \mathrm{erf}(\frac{\alpha - \Delta}{\sqrt{2Var(X_{B_{lin}})}})]^2 \quad (\Delta > 0) \tag{7.9}$$

In which, erf is the error function defined as $\text{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt$ and $Var(X_{B_{lin}})$ is the variance of Bob's measurement under linear detection. As we have discussed in section III, a reasonable assumption for the detector linearity limit α is that $\alpha^2 >> Var(X_{B_{lin}})$ and $\alpha^2 >> N_0$, so that the measurement results of Bob (without displacement) and thus the parameter estimation cannot be affected by saturation. This agrees with the prediction of Eq.(7.9): if $\alpha - \Delta$ is much larger than $\sqrt{2Var(X_{B_{lin}})}$, then $\hat{T}_{sat} \cong T\frac{G}{2}$ which is the estimated value under the linear model. However when Δ is close to α, the impact of saturation becomes important, and $\hat{T}_{sat}$ becomes smaller. An extreme case is when Δ is much larger than α, the error function becomes -1 and $\hat{T}_{sat} = 0$.

Excess noise estimation

Eq.(4.17) shows that the estimated excess noise depends on the variance of Bob's measurement and on the channel transmission between Alice and Bob. Under the saturation attack, these two values will both decrease. We need to evaluate these two values to see whether the induced saturation will result in reducing the estimated excess noise. We have already analyzed $\hat{T}_{sat}$ in the previous subsection (Eq.(7.9)). With Eq.(7.8), we can calculate $Var(X_{B_{sat}})$ (Eq.(A.17)) under saturation attack (calculation details can be found in Appendix A.2.). Based on $\hat{T}_{sat}$ and $Var(X_{B_{sat}})$, we are able to express the estimated excess noise in shot noise units under the saturation attack:

$$\frac{\hat{\xi}_{sat}}{N_0} = \frac{2Var(X_{B_{lin}})(1+A-\frac{B^2}{\pi}) - 2\sqrt{\frac{2Var(X_{B_{lin}})}{\pi}}(\alpha-\Delta)A*B + (\alpha-\Delta)^2(1-A^2) - 4N_0 - 4v_{\text{ele}}}{\eta\frac{G}{2}(1+A)^2 N_0} - \frac{V_A}{N_0} \tag{7.10}$$

in which

$$A = \text{erf}\left(\frac{\alpha-\Delta}{\sqrt{2Var(X_{B_{lin}})}}\right), \tag{7.11}$$

$$B = e^{-\frac{(\alpha-\Delta)^2}{2Var(X_{B_{lin}})}} \tag{7.12}$$

From Eq.(7.10), we can find that when the value of $\alpha - \Delta$ is much larger than $\sqrt{2Var(X_{B_{lin}})}$, then $A \to 1$ and $B \to 0$, so that $\hat{\xi}_{sat} = \frac{Var(X_B)}{\eta T} - Var(X_A) - \frac{N_0}{\eta T} - \frac{v_{\text{ele}}}{\eta T} = \hat{\xi}_{lin}$ (Eq.(4.17)). It can be considered that no saturation is induced and the excess noise estimation is not affected.

A necessary condition for reducing estimated excess noise A necessary condition to have a successful attack is to reduce the excess noise estimation $\hat{\xi}_{sat} < \hat{\xi}_{lin}$. We can then study under which condition the excess noise estimation is reduced by the saturation attack. We have seen that to have obvious saturation effect, Δ needs to be close to α. By considering $\varepsilon = \alpha - \Delta$, when Δ is close to α, ε can be considered as a small value and particularly, $\varepsilon << \sqrt{2Var(X_{B_{lin}})}$. So we can make the following approximation: $A \approx \frac{\varepsilon}{\sqrt{2Var(X_{B_{lin}})}}$, $B \approx 1 - \frac{\varepsilon^2}{2Var(X_{B_{lin}})}$ with higher order terms in ε that can be neglected. By solving the inequality $\hat{\xi}_{sat} < \hat{\xi}_{lin}$ for small ε and considering the gain value $G = 2$, we can obtain the condition:

$$(1 - \frac{2}{\pi})\sigma_B^4 + \sqrt{2}\varepsilon\sigma_B^3 - 3(N_0 + v_{\text{ele}})\sigma_B^2 - 2\sqrt{2}\varepsilon(N_0 + v_{\text{ele}})\sigma_B < 0 \tag{7.13}$$

where $\sigma_B^2 = Var(X_{B_{lin}})$. Since $\varepsilon << \sigma_B$, the terms of second or higher in ε have been neglected. Inequality Eq.(7.13) will be always satisfied (for small ε) if $Var(X_{B_{lin}}) < \frac{3(N_0+v_{\text{ele}})}{1-\frac{2}{\pi}}$. Such necessary condition turns into a condition on the channel transmission and on Alice's input modulation. Eve can not choose Alice's input modulation and the necessary condition reduces to a condition on the channel transmission: $T < \frac{2\pi+2}{\pi-2}\frac{N_0+v_{\text{ele}}}{V_A+\xi}$. This maximal channel transmission is related to the minimal distance that enables Eve to reduce the excess noise estimation by launching a saturation attack.

Estimated excess noise can be made arbitrary small According to the intermediate value theorem, we can prove that $\hat{\xi}_{sat}$ can be manipulated to be arbitrary close to zero when the value of Δ is chosen probably between 0 and 2α. $\hat{\xi}_{sat}$ is a function of Δ, and when $\Delta = 0$, $\hat{\xi}_{sat}(0) = \hat{\xi}_{lin} = \xi$, where $\xi = 2N_0 + \xi_{sys}$ under intercept-resend attack. When $\Delta = 2\alpha$, since we assume that $\alpha^2 >> Var(X_{B_{lin}})$ then we have $A = -\text{erf}(\frac{\alpha}{\sqrt{2Var(X_{B_{lin}})}}) = -1$, and $\hat{\xi}_{sat}(2\alpha) \to -\infty$. Moreover, $\hat{\xi}_{sat}$ is a continuous function of Δ over the interval $[0, 2\alpha)$. Then according to the intermediate value theorem, for any target excess noise that Eve wants to achieve ξ_T in $(-\infty, \xi]$, there always exists a $\Delta \in [0, 2\alpha)$ so that $\hat{\xi}_{sat} = \xi_T$. In a practical attack, Eve wants to manipulate the estimated excess noise to be as small as possible but positive. Eve is always able to find a particular Δ_T that enables $\hat{\xi}_{sat}(\Delta_T) = \xi_T$ for any $0 < \xi_T << N_0$.

7.4.2 Defining criteria of success for the saturation attack

Alice and Bob estimate the key rate based on their estimation of excess noise and channel transmission. If the excess noise is too large, it won't allow Alice and Bob to distill any secret key. A full security break consists in an attack where Eve has full knowledge on the

generated key while Alice and Bob still accept this compromised key material. An intercept-resend attack is an attack strategy that leads, in general, to a denial of service but not to a full security break on CV QKD. By performing saturation attack, we can however obtain a full security break under certain conditions. It is important to clarify what one means by an attack in this context. For this reason, we define a level I criteria for a successful attack:

Level I criteria for a successful attack:

- The attacker Eve performs the saturation attack (Intercept-resend attack on each pulse combined with displacement of each resent pulse).
- Alice and Bob obtain a positive key rate from their estimated parameters $\hat{T}_{sat}$ and $\hat{\xi}_{sat}$.

This condition corresponds to a full security break because Alice and Bob will obtain a positive key rate under the attack and thus accept key material, while this key is insecure as it can be fully obtained by Eve.

While level I criteria defines conditions for a successful attack, the induced saturation can in practice strongly decrease the estimated channel transmission (Eq.(7.9)). This can be a problem in practice since Alice and Bob usually have a good *a-priori* estimate of the channel transmission based on the distance and the attenuation coefficient. If the measured channel transmission is much lower than the expected value for the given link distance, it is reasonable for Alice and Bob to be suspicious and they may reject the key. Moreover, secret key rate drops when channel transmission becomes smaller. Such facts weaken the attacking power of Eve. By choosing different values of Δ and g, the attacker Eve can however mitigate these effects and seek to achieve a stronger criteria for a successful attack:

Level II criteria for a successful attack:

- The attacker Eve performs the saturation attack (Intercept-resend attack on each pulse combined with displacement of each resent pulse).
- Maintain the channel transmission estimation unaffected ($\hat{T}_{sat} = T$).
- Alice and Bob obtain a positive key rate from their estimated parameters $\hat{T}_{sat}$ and $\hat{\xi}_{sat}$.

7.4.3 Analysis and simulation results

We formalize two strategies in order to meet the two criteria for the success of the saturation attack, respectively. We use Eq.(7.9) and Eq.(7.10) to perform numerical evaluation of T_{sat} and ξ_{sat}, in order to study the impact of the saturation attack.

Numerical simulations

We have performed numerical simulations of the estimated excess noise $\hat{\xi}_{sat}$, the estimated channel transmission $\hat{T}_{sat}$, and the secret key rate under collective attack. We have used the simulation parameters which are referred to realistic values given in [68]: Bob's efficiency $\eta = 0.55$, electronic noise $v_{\text{ele}} = 0.015$, fiber attenuation coefficient $a = 0.2dB/km$. We consider the total excess noise (in the absence of saturation) as the sum of the system excess noise $\xi_{sys} = 0.1$ and of the excess noise $\xi_{IR} = 2$ due to intercept-resend attack [104]. The value of system excess noise $\xi_{sys} = 0.1$ is relatively high compared to the other experiment results in CV QKD [68] but it has been encountered in the experimental study[104]. It can moreover be considered as a pessimistic value from Eve's preceptive that therefore will not weaken our predictions concerning the power of the saturation attack on practical systems.

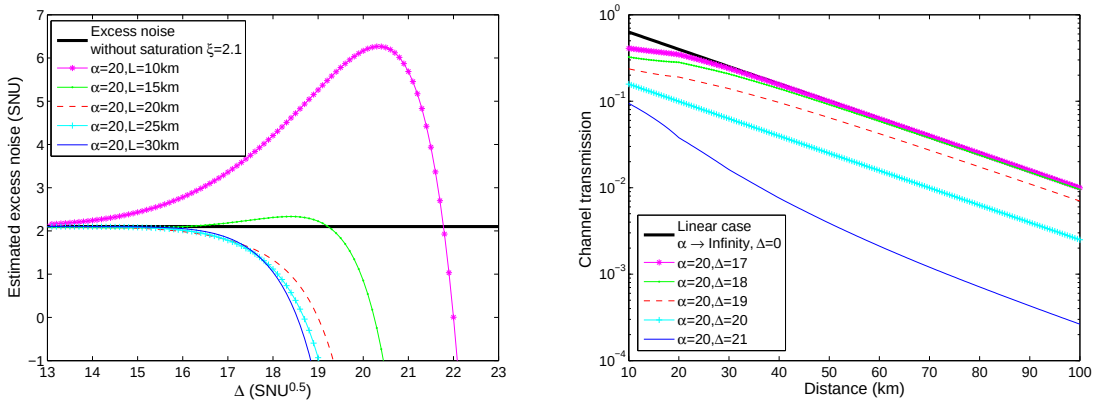
We have followed the procedure described in [63] to set Alice's variance with respect to distance: to achieve a high reconciliation efficiency in practical CV QKD ($\beta = 0.95$), optimized error correction codes need to work with a fixed signal to noise ratio (SNR); then Alice thus needs to optimize her modulation variance with respect to the distance in order to work at a given SNR.

Meeting level I criteria: reduce the excess noise below the null key threshold

To meet this criteria, we formalize strategy I:

- Eve implements the saturation attack as described in the section VI.B.
- Eve chooses the gain value $G = g^2 = 2$ in order to compensate the loss due to heterodyne detection.
- By choosing the value of Δ, Eve bias the excess noise estimation of Alice and Bob below the null key threshold, so that Alice and Bob can obtain a positive key rate.

The key idea of this strategy is that, for a given distance with the knowledge of $Var(X_{B_{lin}})$, Eve can manipulate $\hat{\xi}_{sat}$ by changing Δ. More importantly, Eve needs to manipulate $\hat{\xi}_{sat}$ below the null key threshold to meet the level I criteria of our saturation attack. $\hat{\xi}_{sat}$ is a function of Δ (Eq.(7.9)), the behavior of $\hat{\xi}_{sat}$ versus Δ is shown in Fig.7.4 (a). Under the linear

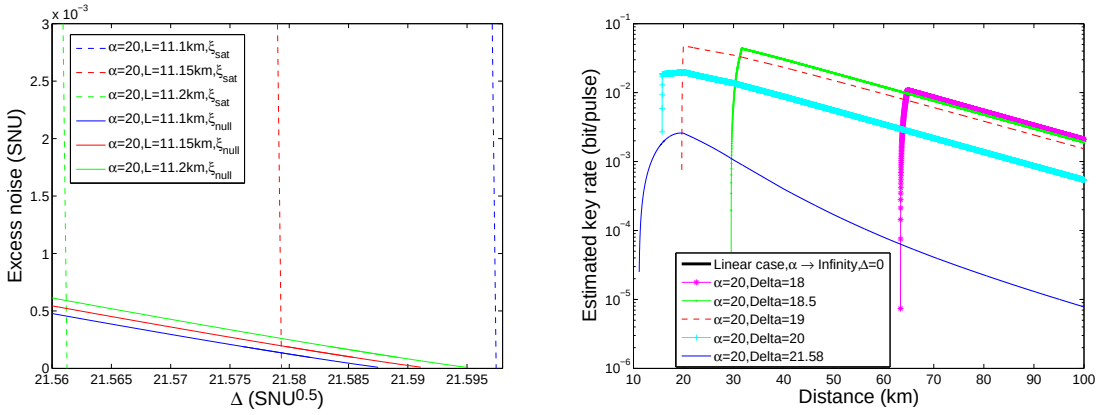


(a) (b)

Fig. 7.4 Strategy I (a) Excess noise (Alice side) versus Δ with different distance. (b) Quantum channel transmission versus distance with different Δ. Alice's variance $V_A \in \{1, 100\}$, Bob's efficiency $\eta = 0.55$, excess noise of electronics $v_{\text{ele}} = 0.015$, total excess noise in linear case $\xi = 2.1$, reconciliation efficiency $\beta = 0.95$, attenuation coefficient $a = 0.2dB/km$.

model, the total estimated excess noise under a full intercept-resend attack is $\hat{\xi}_{lin} = \xi = 2.1$, including 0.1 technical noise (black curves in Fig.7.4 (a)). With such an excess noise, no key rate can be established by Alice and Bob. However, $\hat{\xi}_{sat}$ can be manipulated by changing the value of Δ. In Fig.7.4 (a), for long distance (i.e. above 20 km) $\hat{\xi}_{sat}$ always decreases when Δ increases. Especially when Δ is close to α, $\hat{\xi}_{sat}$ is significantly reduced, which agrees with the analysis in subsection 7.4.1 For short distance (i.e. below 20 km), when Δ increases, $\hat{\xi}_{sat}$ first increases then decreases, but $\hat{\xi}_{sat}$ can still become arbitrary small when Δ is large enough. Importantly, from Fig.7.4 (a), we can see that Eve can obtain an arbitrary small value of $\hat{\xi}_{sat}$ by manipulating Δ at any distance, which agrees with the analysis in subsection 7.4.1.

As already mentioned in subsection 7.4.1, a drawback of the saturation attack is that the estimated channel transmission is reduced $\hat{T}_{sat} < T$ (Eq.(7.9)). In Fig.7.4 (b) we plot the estimated channel transmission in log scale versus distance, in which the black curve is the estimated channel transmission (T) versus distance in absence of attack while the other curves are estimated channel transmission ($\hat{T}_{sat}$) under the saturation attack. We can see that, the estimated channel transmission can be strongly reduced in comparison to the actual transmission in absence of attack. This is especially true at short distance, where Δ needs to be large enough to effectively reduce the excess noise estimation: larger Δ means more loss is induced on channel transmission. However with a lower channel transmission estimation, the corresponding null key threshold (i.e. the maximum tolerable estimated excess noise



(a) (b)

Fig. 7.5 Strategy I. (a) Null key threshold and estimated excess noise versus Δ. Solid line: null key threshold under saturation attack. Dash line: estimated excess noise under saturation attack. (b) Key rate versus distance. Alice's variance $V_A \in \{1, 100\}$, Bob's efficiency $\eta = 0.55$, excess noise of electronics $v_{\text{ele}} = 0.015$, total excess noise in linear case $\xi = 2.1$, reconciliation efficiency $\beta = 0.95$, attenuation coefficient $a = 0.2dB/km$.

allows a positive key rate) becomes smaller. In our case we consider a choice of Alice's modulation variance optimizing the key rate based on realistic key rate. At short distance the chosen variance can be relatively large (around 30 SNU) while at long distance it is relatively small (below 5 SNU).

Although Eve can bias ξ_{sat} to an arbitrary small value at any distance, it is still not enough to guarantee that Alice and Bob can obtain a positive key rate for any distance. The null key threshold (ξ_{null}) is computed from channel transmission estimation $\hat{T}_{sat}$ (Fig.7.4(a)) and can be possibly smaller than $\hat{\xi}_{sat}$, especially at shorter distances. We need to study further the condition under which Alice and Bob can obtain a positive key rate. Under saturation attack, ξ_{null} varies with $\hat{T}_{sat}$ and thus with Δ. By varying Δ, we can compare ξ_{null} and $\hat{\xi}_{sat}$ to study the condition of $\hat{\xi}_{sat} < \xi_{null}$ so that Alice and Bob can obtain a positive key rate under saturation attack. In Fig.7.5(a) we plot ξ_{null} and $\hat{\xi}_{sat}$ versus Δ, where the solid line is ξ_{null} and dash line is $\hat{\xi}_{sat}$ with different colors for different link distances. We can see that for link distance 11 km, no matter how small $\hat{\xi}_{sat}$ is, there is no intersection between ξ_{null} and $\hat{\xi}_{sat}$, so that there exists no value of Δ that can meet the condition $\hat{\xi}_{sat} < \xi_{null}$. When the distance increases to 11.15 km, there is an intersection around $\Delta = 21.58$. At 11.15 km, as long as Eve chooses a value of Δ slightly larger than 21.58, she can make sure that $\hat{\xi}_{sat} < \xi_{null}$ so that the level I criteria of our saturation attack is achieved. At large distance, there always exists intersections between ξ_{null} and $\hat{\xi}_{sat}$, so that it is always possible for Eve to achieve $\hat{\xi}_{sat} < \xi_{null}$ by manipulating Δ. In our case, 11.15 km is the shortest distance for

which level I criteria can be satisfied.

For $\Delta = 21.58$ and other values of Δ close to α, we evaluate the estimated secret key rate versus distance in Fig.7.5 (b). For a fixed Δ, the impact of saturation attack varies with the distance. For example when $\Delta = 21.58$, $\hat{\xi}_{sat}$ is just below null key threshold at 11.15 km, however with same $\Delta = 21.58$ at 12 km, $\hat{\xi}_{sat}$ becomes negative. In our simulation, we assume that if $\hat{\xi}_{sat} < 0$, Eve can always add an extra noise to guarantee $\hat{\xi}_{sat} = 0.0001$, which is smaller than the null key threshold at the minimal attack distance. Under this assumption, we show the variation of estimated secret key rate with respect to distance for different fixed values of Δ. For $\Delta < 21.58$, the shortest distance under which a positive key rate can be obtained becomes larger than 12 km. The key rate also decreases when Δ increases illustrating the increasing impact of the saturation attack and $\hat{T}_{sat}$ decreasing in comparison to T.

Meeting level II criteria: reduce the excess noise below the null key rate threshold and maintain the channel transmission unaffected

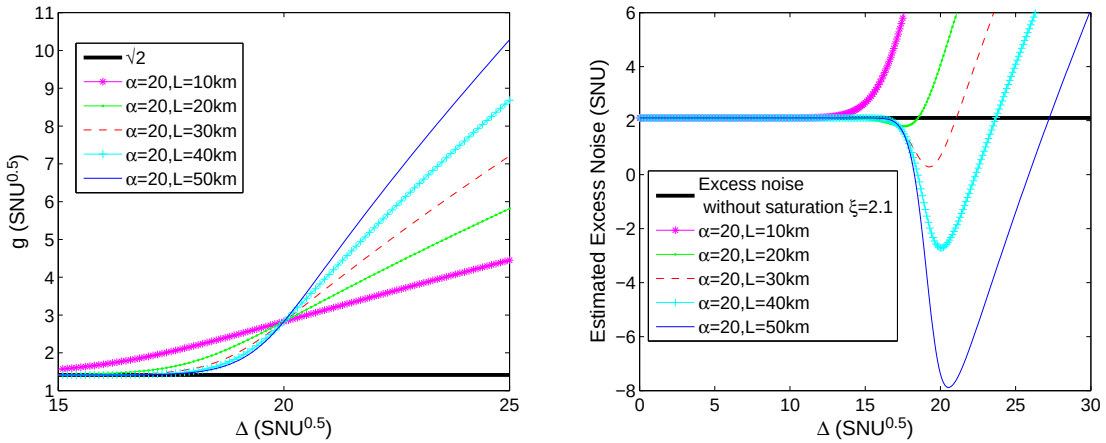
The saturation of the homodyne detection can lower the correlation between Alice and Bob's data, which will result in the decrease of the estimated channel transmission $\hat{T}_{sat}$ (Fig.7.4(b)). However, in the context of the intercept-resend attack, there is no restriction on the gain (g) for Eve: Eve can choose a proper value of g to compensate the loss due to the saturation attack so that the measured channel transmission appear unaffected. To meet criteria II of our saturation attack, we formalize the strategy II. Strategy II is similar to strategy I except for the second step where the choice of the gain is decided as followed.

Eve estimates how much loss the saturation attack will induce to the channel transmission estimation (Eq.(7.9)), and determines a value of g in order to compensate the loss due to the saturation. If g satisfies the condition:

$$\frac{2\sqrt{2}}{g} - 1 = \mathrm{erf}\left(\frac{\alpha - \Delta}{\sqrt{2[\eta T \frac{g^2}{2} Var(X_A) + \eta T \frac{g^2}{2}(2N_0 + \xi_{sys}) + N_0 + v_{\mathrm{ele}}]}}\right) \tag{7.14}$$

As a matter of fact, if Eq.(7.14) is accepted, then $\langle X_A X_{B_{sat}} \rangle = \frac{1}{2}\langle X_A^2 \rangle t$ and channel transmission estimation becomes $\hat{T}_{sat} = T$, which meets our requirement that the channel transmission estimation for Alice and Bob is not biased.

The gain g can be described as a function of Δ, we can find the numerical solutions of Eq.(7.14) to determine the value of g, this corresponds to the curves displayed in Fig.7.6 (a). Furthermore, in order to see whether we can have a full security break with this new choice of g under the saturation attack, we still need to analyze the estimation of excess noise and

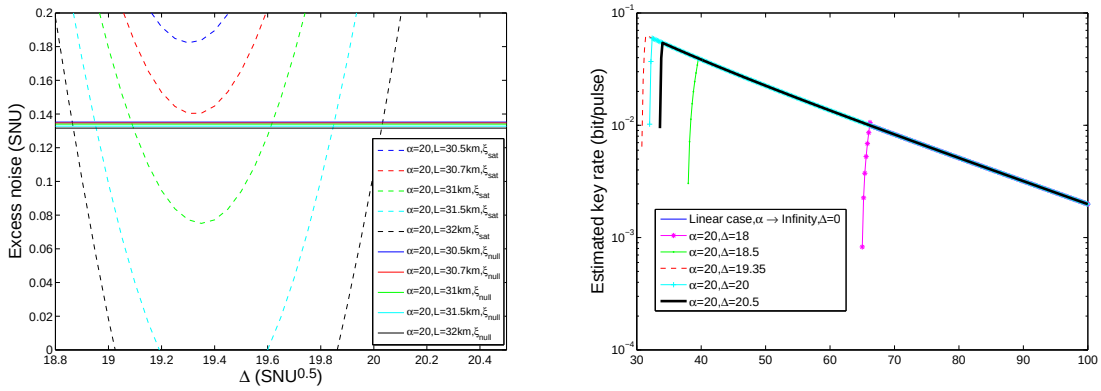


(a) (b)

Fig. 7.6 Strategy II. (a) Decision of g. (b) Excess noise (Alice side) versus Δ with different distance. Alice's variance $V_A \in \{1, 100\}$, Bob's efficiency $\eta = 0.55$, excess noise of electronics $v_{\text{ele}} = 0.015$, total excess noise in linear case $\xi = 2.1$, reconciliation efficiency $\beta = 0.95$, attenuation coefficient $a = 0.2dB/km$.

secret key rate for Alice and Bob. By taking the g solutions of Eq.(7.14) into account, the behavior of $\hat{\xi}_{sat}$ versus Δ is shown in Fig.7.6 (b). As we can see, for long distance (above 30 km), it is still possible to reduce $\hat{\xi}_{sat}$ close to zero by choosing a value of Δ close to α. Thus the power of our attack under this strategy is also limited by the distance according to Fig.7.6 (b). We also need to study the condition for $\hat{\xi}_{sat} < \xi_{null}$ as we previously did in level I criteria. However the analysis is simpler, because the estimated channel transmission is not biased, so that the null key threshold does not depend on the attack parameter Δ. Under strategy II, the null key threshold only varies with distance. In Fig.7.7 (a) we enlarge the scale of Fig.7.6 (b) and compare the estimated excess noise to the null key threshold for different distances. As we can see, when the distance reaches 31 km, the condition $\hat{\xi}_{sat} < \xi_{null}$ can be satisfied with a choice of Δ around 19.5. For larger distance, it is always possible to meet the level II criteria conditions under strategy II by manipulating Δ and g.

We also estimate the secret key rate of Alice and Bob versus distance (Fig.7.7 (b)) with the assumption that if $\hat{\xi}_{sat} < 0$, $\hat{\xi}_{sat}$ is set to 0.005, i.e. a value is much smaller than the null key threshold at the shortest attacking distance. The shortest reachable distance where Alice and Bob can obtain a positive key rate varies with different values of Δ. As excepted from Fig.7.7 (a), $\Delta = 19.35$ corresponds to the optimal attack parameter, for which an attack is possible for all distances above 31 km, and this is confirmed in Fig.7.7 (b). Moreover, an advantage of strategy II is that for the achievable distance in Fig.7.7 (b), the key rate is always higher with strategy II than with strategy I (Fig.7.5 (b)) for the same distance. Strat-



(a) (b)

Fig. 7.7 Strategy II (a) Null key threshold and estimated excess noise versus Δ. Solid line: Null key threshold under saturation attack with strategy II. Dash line: Estimated excess noise under saturation attack. (b) Key rate versus distance. Alice's variance $V_A \in \{1, 100\}$, Bob's efficiency $\eta = 0.55$, excess noise of electronics $v_{\text{ele}} = 0.015$, total excess noise in linear case $\xi = 2.1$, reconciliation efficiency $\beta = 0.95$, attenuation coefficient $a = 0.2dB/km$.

egy II optimizes the choice of g to maintain the channel transmission estimation unaffected and leads to a more powerful attack, that can however not be valid for all experimental parameters. Reaching level II criteria makes our attack more efficient and convincing.

7.5 Countermeasure

After figuring out a loophole that leads to the above described attack, now we are trying to propose possible countermeasures. To prevent such saturation attack, intuitively, Bob should avoid the homodyne detection working in a nonlinear or saturated region when he makes measurements. Therefore Bob can test all the data just after data acquisition and check whether quadrature measurements have been acquired in a linear regime. In order to do this, Bob thus needs a precise calibration of the homodyne detection limit $[-\alpha, \alpha]$. The whole block which contains the data measured in saturation region would be totally discarded. Based on Gaussian post-selection [33], we can moreover process on the data that are measured in the linear region and transform them into a Gaussian input where security proof holds.

The second countermeasure is proposed by Kunz-Jacques and Jouguet [81]: Alice and Bob test the linearity between the noise and signal measurement by using an active attenuation device on Bob's side, i.e. an amplitude modulator. In principle, the randomization of signal port's attenuation can prevent Eve to set proper values of displacement that in-

duce detector saturation. However, in the analysis, the authors consider a unrealistic case where there is no loss on the channel between Alice and Bob $T = 1$. It is not clear yet that such linearity test can also works when a lossy channel is considered. As we can see from previous analysis, the behavior of excess noise estimation obviously is very different when distance changes. On the other hand, such linear test also increases the complexity of the implementation, where an additional amplitude modulator and the parameter estimation is modified.

Since the saturation attack is a detector-based side channel attack, measurement device independent (MDI) CV QKD [95, 113] could be a potential solution to defeat such kind of attack. MDI CV QKD protocols are not far away from implementations, very recently, a proof-of-principle demonstration of MDI CV QKD has been already performed in experiment [135].

7.6 Conclusions

We have proposed the saturation attack combined with a full intercept-resend attack. In simulations, we have shown the feasibility of our attack under realistic experimental conditions. Unlike other attacks manipulating LO in CV QKD, our attack has no influence on the LO but on the displacement value of quadratures, so that even if Alice and Bob monitor the LO intensity in real time, our saturation attack can still work. Our attack is achievable with current technology and impacts the security of a practical CV QKD system. It highlights the importance of exploring the assumptions in security proofs when implementing QKD protocol on practical setups. Suitable counter measures are necessary for practical CV QKD to fix the loopholes that attackers can exploit.

Chapter 8

Experimental study of saturation attack on a CV QKD system

In this chapter, we present the experimental demonstrations of the saturation attack studied in chapter 7. We have realized a functional "Eve" to perform the saturation attack experimentally, in which, the key step is to prepare a precise and strong displacement. However, this step is a technical challenge. Producing a coherent displacement directly in the mode of the quantum signal is difficult to achieve with good stability. It is therefore interesting to seek new methods to induce saturation on homodyne detection from another approach with simpler experimental setup. For this reason, we have proposed a new attack strategy: we induce strong shift in the homodyne measurement with an external light in a different mode from the QKD signal. In this chapter, we will tackle these issues one by one and show that our results are important steps towards a fully experimental saturation attack.

8.1 Saturation attack with two stations for Eve

8.1.1 Attack strategy

In the saturation attack strategy from section.7.3.2, we assume that Eve has a single station which is close to Alice. In this station, Eve launches the saturation attack with two actions: quadrature measurement and quadrature re-preparation. However, Eve can optimize further her strategy: she can perform her two actions in two remote stations which are respectively close to Alice and to Bob. Under this assumption, we propose a modified saturation attack strategy: Eve in the middle cuts down the quantum channel and places a station A close to Alice in order to perform quadrature measurements. She then sends her measurement information classically to another station close to Bob (station B), based

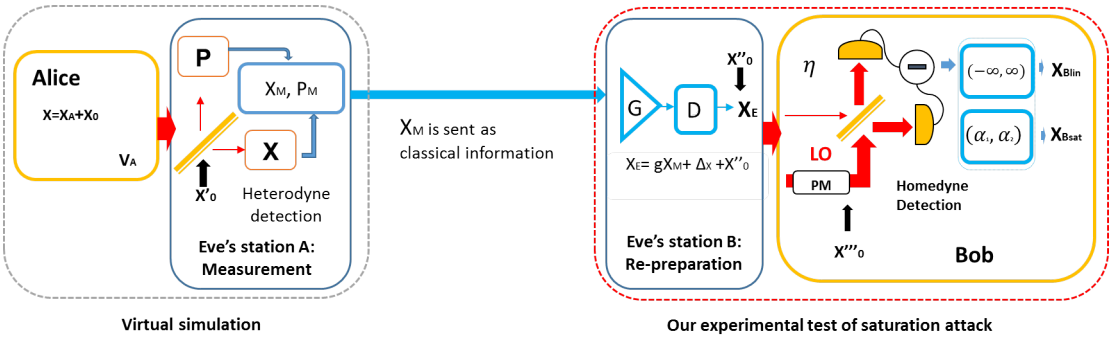


Fig. 8.1 Experimental implementation of the saturation attack with two stations for Eve. The part on the left is simulated.

on the classical measurement information Eve re-prepares the corresponding coherent state, that she displaces before sending it to Bob. Bob then performs an homodyne detection, with a detector which is assumed to be perfectly linear over a region $[-\alpha,\alpha]$, and saturated beyond. This attack scheme is represented in Fig.8.1. In order to avoid confusion with the attack strategy proposed in section.7.3.2, let us briefly go through this new strategy and clarify notations for each step of Eve's action and Alice-Bob protocol:

1. Alice's quadrature preparation: Alice prepares the Gaussian modulation coherent states [50] (variance V_A) with its quadrature X and P[1]:

$$X = X_A + X_0, \tag{8.1}$$

in which X_0 is a noise term due to the coherent state encoding of Alice.

2. Eve's quadrature measurement in station A: Eve performs a full heterodyne detection on the state of Alice, which gives her the measurement of quadrature X (and P):

$$X_M = \frac{1}{\sqrt{2}}(X_A + X_0 + X_0' + X_{N_{A,E}}), \tag{8.2}$$

In which X_0' is a noise term due to 3 dB loss of heterodyne detection. $X_{N_{A,E}}$ is a noise variable with its variance $\xi_{N_{A,E}}$:

$$X_{N_{A,E}} = X_{N_A} + \sqrt{2}X_{N_{E_m}}, \tag{8.3}$$

in which X_{N_A} is the technical noise of Alice's preparation, while $X_{N_{E_m}}$ is the technical noise due to Eve's measurement. Eve then sends her (classical) measurement

[1] Similar as in previous chapter, we neglect the analysis of quadrature P by symmetry.

information X_M to Eve's station B which is close to Bob.

3. Eve's quadrature re-preparation and resending in station B: Eve receives the classical information X_M from station A, she prepares a corresponding coherent state X_E according to X_M with a gain g:

$$X_E = gX_M + \Delta_X + X_0'' = \frac{g}{\sqrt{2}}(X_A + X_0 + X_0' + X_{N_{A,E}}) + \Delta_X + X_0'' \tag{8.4}$$

Eve induces a displacement (Δ_X, Δ_P) and applies an amplification (g) on the data X_M before optical encoding. X_0'' is a noise term due to coherent state encoding of Eve. Eve then sends the new state X_E to Bob who is next to her station B.

4. Bob's quadrature measurement: Bob performs a homodyne detection on the received state X_E. If the linear detection range is infinite $(-\infty, \infty)$, we would have:

$$X_{B_{lin}} = \sqrt{\eta}(X_E + X_{N_E}) + \sqrt{1-\eta}X_0''' + X_{ele}, \tag{8.5}$$

in which X_{N_E} is a noise variable with its variance ξ_{N_E}, which is due to the technical noise of Eve's preparation. Since Eve's station B is close to Bob, then there is no loss induced on X_E. Based on Eq.(8.5), we could further compute Bob's variance:

$$\begin{aligned} Var(X_{B_{lin}}) =& \langle X_{B_{lin}}^2 \rangle - \langle X_{B_{lin}} \rangle^2 \\ =& \eta \frac{G}{2} V_A + \eta \frac{G}{2}(2N_0 + \xi_{sys}) + N_0 + v_{\text{ele}} \end{aligned} \tag{8.6}$$

in which $\xi_{sys} = \xi_{A,E} + \frac{2}{G}\xi_E$, is the total technical excess noise variance due to Alice, Eve and Bob's action, $2N_0$ is due to the full heterodyne detection in step 2, $G = g^2$ is the amplification applied by Eve. Considering a realistic homodyne detection whose linear detection range is limited by $[\alpha_1, \alpha_2]$, then Bob's measurement on X_E yields:

$$X_{B_{sat}} = \begin{cases} \alpha_1, \text{if } X_{B_{lin}} \leqslant \alpha_1 < 0 \\ \sqrt{\eta}(X_E + X_{N_E}) + \sqrt{1-\eta}X_0''' + X_{ele}, \text{if } \alpha_1 < X_{B_{lin}} < \alpha_2 \\ \alpha_2, \text{if } X_{B_{lin}} \geqslant \alpha_2 > 0 \end{cases}, \tag{8.7}$$

in which η is the efficiency of Bob and we consider a more realistic case where the lower bound α_1 and upper bound α_2 are not symmetric $\alpha_2 \neq -\alpha_1$.

In this new strategy, Eve circumvents the whole quantum channel and transmits the classical information between Eve's station A and B without any loss. This is also the main difference

between the saturation attack with one station (chapter 7) and two stations. In order to evaluate Alice and Bob's estimations of channel transmission and excess noise under this new strategy with two stations, we can refer to the analysis of chapter 7 and simply set the real channel transmissions $T = 1$, such that Eq.(7.9) and Eq.(7.10) can be applied to this new case. The necessary condition to reduce excess noise estimation when $\Delta \approx \alpha$ (Eq.(7.13)) still holds, where $Var(X_{B_{lin}})$ now refers to Eq.(8.6). In fact, all the conclusions drawn from chapter 7 can be extended to this new strategy with the change of $T = 1$ and with $Var(X_{B_{lin}})$ given by Eq.(8.6).

8.1.2 Experimental demonstration model

Our goal is to experimentally demonstrate the saturation attack and show that it leads to a full security break. In particular, we need to evaluate whether the estimated excess noise is below the null key threshold and whether or not the estimated channel transmission is biased, which are the two criteria in section.7.4.2. Note that as an important part of the saturation attack, the intercept-resend attack has already been realized experimentally by Lodewyck et al. [104]. Indeed, the consequence of a full heterodyne detection in step (2) is 2 shot noise units of excess noise induced on Alice and Bob's parameter estimation. Such amount of noise can be simulated by adding Gaussian noise. In order to study experimentally the impact of the saturation effect, we decide to experimentally realize the step (3) (4) of the saturation attack with two stations (section. 8.1.1) while virtually simulating the step (1) (2), as shown in Fig.8.1. Specifically, in Eve's station B, we act as a modified 'Eve' and generate two independent Gaussian variables X_A and $X_{N_{IR}}$, X_A represents Alice's variable with a variance $Var(X_A) = V_A$, while $X_{N_{IR}}$ is a independent variable with variance $Var(X_{N_{IR}}) = 2N_0$. In this sense, we prepare numerically the received classical measurement information $X_M = X_A + X_{N_{IR}}$, which has been simulated at the step (1) (2). On the other hand, Eve has the ability to freely control the displacement value Δ_X and the amplification g as shown in Eq.(8.4) of step (3). In experiment, we have the control over 4 factors: X_A, $X_{N_{IR}}$, g and Δ_x. This can be summarized in the following equation:

$$X_E = gX_M + \Delta_X + X_0'' \tag{8.8}$$

$$= \underbrace{g}_{\text{Controlled by Eve}} \Big(\underbrace{X_A}_{\text{Simulation of Alice}} + \underbrace{X_0 + X_0'}_{\text{Simulated by } X_{N_{IR}}} + X_{N_E} \Big) + \underbrace{\Delta_x}_{\text{Controlled by Eve}} + \underbrace{X_0''}_{\text{Encoding}} \tag{8.9}$$

Compared to Eq.(8.4), we remove the factor $1/\sqrt{2}$, since the heterodyne detection is simulated and we can directly compensate this factor by increasing g. X_{N_E} corresponds to the

experimental technical noise due to Eve. We need to calibrate its variance $Var(X_{N_E}) = \xi_E$ in experiment. In step (4), Bob performs a homodyne detection on the received state X_E. The linear detection range of the homodyne detection $[\alpha_1, \alpha_2]$ also needs to be calibrated in experiment. Bob's measurement output $X_{B_{sat}}$ is given by Eq.(8.7), in which X_E is given by Eq.(8.8). Bob's variance under linear detection is given by:

$$Var(X_{B_{lin}}) = \eta G V_A + \eta G(2N_0 + \xi_E) + N_0 + v_{\text{ele}}. \tag{8.10}$$

Let us now consider the parameter estimation between Alice and Bob. The channel transmission and excess noise can be thus estimated through standard procedure described in section.4.2.4: By taking $Var(X_A)$, $Var(X_{B_{sat}})$ and $Cov(X_A, X_{B_{sat}})$ into Eq.(4.16) and Eq.(4.17), we can deduce $\hat{T}_{sat}$ and $\hat{\xi}_{sat}$ under our saturation attack. These two values can be measured from experimental data.

We can also predict parameter estimations under our attack by using a saturation model and conducting through an analysis similar to the one in chapter 7. The channel transmission estimation is given by:

$$\hat{T}_{sat} = \frac{G}{4}[1 + \text{erf}(\frac{\Delta - \alpha_1}{\sqrt{2Var(X_{B_{lin}})}})]^2, \quad (|\Delta - \alpha_1| << |\Delta - \alpha_2|, \Delta < 0, \alpha_1 < \Delta < 0). \tag{8.11}$$

And the excess noise estimation in shot noise units is given by:

$$\begin{aligned}\frac{\hat{\xi}_{sat}}{N_0} =& \frac{2Var(X_{B_{lin}})(1 + A - \frac{B^2}{\pi}) - 2\sqrt{\frac{2Var(X_{B_{lin}})}{\pi}}(\Delta - \alpha_1)A * B + (\Delta - \alpha_1)^2(1 - A^2) - 4N_0 - 4v_{\text{ele}}}{\eta G(1 + A)^2 N_0} \\ & - \frac{V_A}{N_0}, \quad (|\Delta - \alpha_1| << |\Delta - \alpha_2|, \Delta < 0, \alpha_1 < 0),\end{aligned} \tag{8.12}$$

in which

$$A = \text{erf}(\frac{\Delta - \alpha_1}{\sqrt{2Var(X_{B_{lin}})}}), \tag{8.13}$$

$$B = e^{-\frac{(\Delta - \alpha_1)^2}{2Var(X_{B_{lin}})}}. \tag{8.14}$$

$Var(X_{B_{lin}})$ is given by Eq.(8.10) and $\Delta = \sqrt{\eta}\Delta_X$. The condition $|\Delta - \alpha_1| << |\Delta - \alpha_2|$ means that the Δ is closer to the lower limit α_1 than the upper limit α_2. In experiment, we intend to prepare displacement Δ that is close to α_1. Eq.(8.11) and Eq.(8.12) provide theoretical predictions of parameter estimation under our proposed attack strategy. They are also our ref-

erences to set the experimental values of Δ and G to achieve the two criteria of a successful attack (section.7.4.2). Note that under our strategy, although there is no loss between Eve's station B (Alice) and Bob, the estimated channel transmission $\hat{T}_{sat}$ could be smaller than 1 when the saturation effect appears according to Eq.(8.11), i.e $\hat{T}_{sat} \simeq G/4$ when $\Delta \sim \alpha_1$. These values of Δ and G are under the control of Eve while the other parameters in Eq.(8.11) and Eq.(8.12) need to be experimentally calibrated. Besides the standard calibrations in a normal CV QKD protocol, such as Bob's efficiency η, detector electronics noise v_{ele} and shot noise N_0, we also need to calibrate the values of lower linear detection limit α_1 and technical noise due to the displacement preparation ξ_E. We emphasize that in this attack, we don't influence shot noise calibration, but only focus on studying the consequence of homodyne detection saturation. Given these calibrated values, we can evaluate the impact of detector saturation on parameter estimation and further compare them with experimental data.

8.2 Experimental demonstration of saturation attack

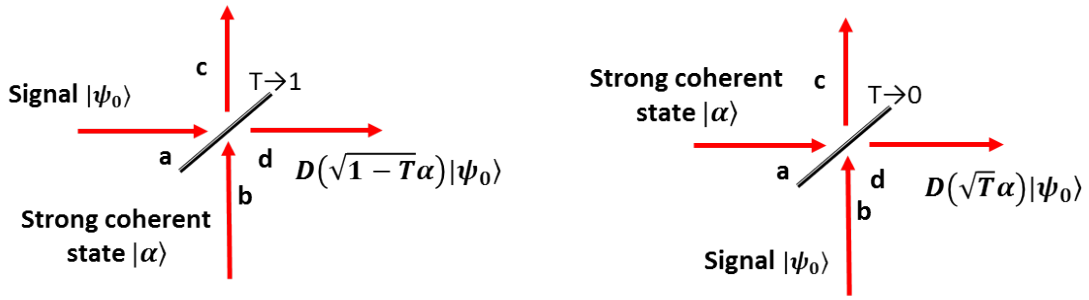
Based on the experimental proposal in the previous section, we have realized each step in experiment to perform the demonstration of saturation attack. According to the analysis in the previous parts, the key step to launch saturation attack is to prepare a strong and precise displaced coherent state signal. In this section, we focus on explaining our implementation of displacement in the attack and analyzing the experimental results.

8.2.1 Implementation of displacement

The implementation of displacing an arbitrary state was first proposed by Paris [128]. Briefly, phase space displacement of a arbitrary state can be realized by interfering the arbitrary state with an intense coherent state on a very asymmetric beam splitter, where the transmittance $T \to 1$ (or $T \to 0$). Such method has been used to experimentally displace a Fock state [106], a squeezed state [124] and a coherent state [187]. The specific implementation details of displacement in each of these experiments are different, but they can be mainly summarized as the following two cases: (a) In Fig.8.2(a), an arbitrary quantum state $|\psi_0\rangle$ (port b) is fed by a strong coherent state $|\alpha\rangle$ (port b) over a highly transmitting beam splitter (the transmittance $T \to 1$), the output (port d) state $|\psi\rangle$ is a displaced state of $|\psi_0\rangle$ with a displacement $\sqrt{1-T}\alpha$. Experimentally, the strong coherent state is realized by an intense laser of amplitude α. Such configuration is considered in [187]. (b) In Fig.8.2(b), an arbitrary quantum state $|\psi_0\rangle$ (port a) interferes a strong coherent state $|\alpha\rangle$

(port b) on a highly reflecting beam splitter (the transmittance $T \to 0$), $|\psi_0\rangle$ is displaced at the output (port d) of beam splitter with a displacement $\sqrt{T}\alpha$. Such configuration is used by Lvovsky and Babichev [106] and Neergaard-Nielsen et al. [124] with some modifications. In Lvovsky and Babichev [106], the beam splitter is replaced by a dielectric mirror with the reflectivity of 99.99 %; in [124], the authors have used the half-wave plates (HWP) and a polarizing beam splitter (PBS) to independently tune the splitting ratios of the two input beams (port a and b). Note that one can lock the phase of displacement by monitoring the other output port (port c) with a standard photo diode [124].

The results of these two configurations are equivalent: a displacement is induced on an arbitrary state. According to the experimental requirements, one can choose either of them to realize displacement of a quantum state.



(a) (b)

Fig. 8.2 Experimental implementation of displacement with (a) a highly transmitting beam splitter $T \to 1$; (b) a highly reflecting beam splitter $T \to 0$.

8.2.2 Experimental setup

According to the experimental demonstration proposal in section.8.1.2, we have realized experimentally the step (3) and step (4) of the saturation attack with two stations. Particularly, in order to be able to induce a controlled displacement on Eve resent data (step(3)), we have modified the "heritage" CV QKD Alice system by introducing a Sagnac loop combined with variable beam splitter (VBS). We consider the configuration with a highly transmitting beam splitter to induce the displacement (Fig.8.2(a)), the experimental setup is shown in Fig.8.3. Displacing the signal is achieved as follows. The VBS, with splitting ratio T=99.9% (the transmittance), splits the pulse from the circulator into two. The signal pulse, which is the less intense pulse along the clockwise direction, goes under Gaussian modulation by amplitude modulator (AM1) and phase modulator (PM1) and further heavily attenuated by

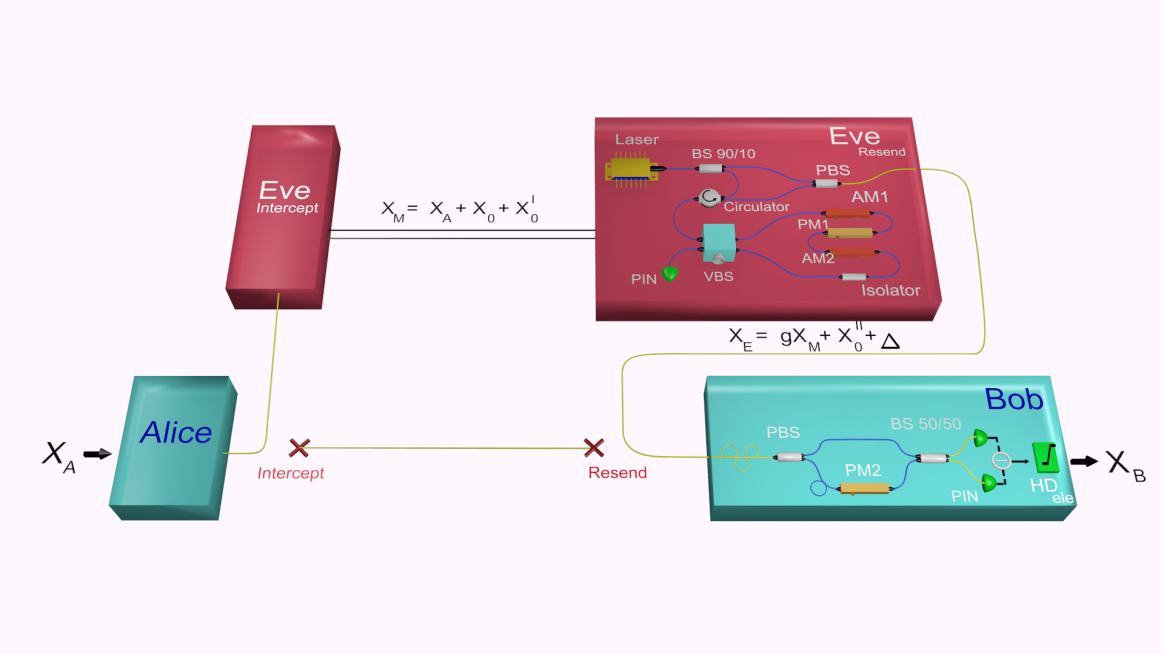


Fig. 8.3 Experimental setup: saturation attack by coherent displacement on a CV QKD system.

isolator (connected in reverse to achieve an attenuation higher than 30dB). High intense pulse travels along anti-clockwise directions, named as pump pulse, meets the signal pulse at VBS. The interference on this strongly unbalanced beam splitter effectively displaces the signal pulse. The amplitude modulator AM2 controls the intensity of the pump and thence the amount of displacement. A PIN diode attached to the VBS helps to monitor the stability in displacement. Finally, the circulator directs the displaced signal towards the polarization beam splitter (PBS) that polarization multiplex the local oscillator and displaced signal to the output fiber channel.

At Bob station (step(4)), displaced signal and local oscillators are de-multiplexed and send to homodyne detector. A phase modulator PM2 applies either 0 or 90 degree of phase on local oscillator for measuring either of the quadratures. This phase modulator is also used for stabilizing relative phase drift between signal and local oscillator.

8.2.3 Parameter calibration

As mentioned in section.8.1.2, we need to calibrate several experimental parameters, such as Bob's efficiency $\eta = 0.54$, electronic noise $v_{ele} = 0.01N_0$ and shot noise N_0, these calibrations are performed as in the normal CV QKD protocol. To launch the saturation attack, we (Eve) need to calibrate two extra parameters: technical noise due to the displace-

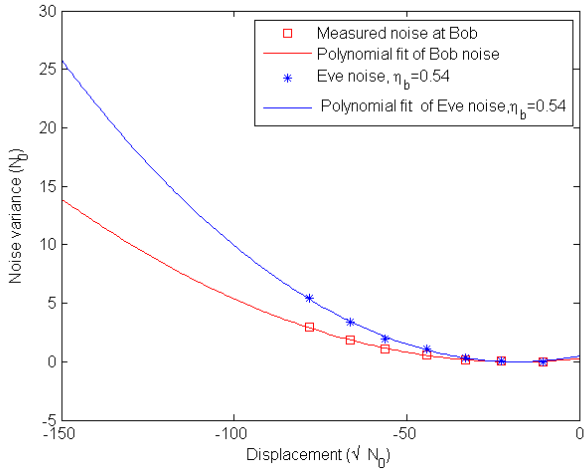


Fig. 8.4 Excess noise due to displacement preparation vs Displacement.

ment preparation ξ_E and lower linear detection limit α_1. Such calibration can be realized by strongly displacing the vacuum state with our experimental setup mentioned in previous section. When there is no signal input but with a strong displacement, the output of homodyne detection is given by:

$$X_{B_{lin,0}} = \Delta + X_0 + X_{ele}, \tag{8.15}$$

From $X_{B_{lin,0}}$, we can deduce its mean and variance :

$$\langle X_{B_{lin,0}} \rangle = \Delta, \tag{8.16}$$

$$Var(X_{B_{lin,0}}) = \eta \xi_E + N_0 + v_{ele}. \tag{8.17}$$

Thus in the linear region $\alpha_1 < X_{B_{lin}} < \alpha_2$, we can experimentally measure the excess noises ξ_E due to the displacement added on final measurements, provided we have calibrated the efficiency η and shot noise N_0. Note that, on the other hand, in the saturation region of homodyne detection, we are unable to correctly measure such noise in experiments due to the saturation effect as we have seen in chapter 7. In order to calibrate the technical noises at high values of displacement under our experimental setup, we use the polynomial fitting of order 2 on the measured values in linear region and it gives:

$$\xi_E(\Delta) = 1.484 \times 10^{-3}\Delta^2 + 5.538 \times 10^{-2}\Delta + 0.4753. \tag{8.18}$$

From the equation above, we find the relation between the induced technical noise from displacement preparation in Eve's station B and the value of displacement. All these results

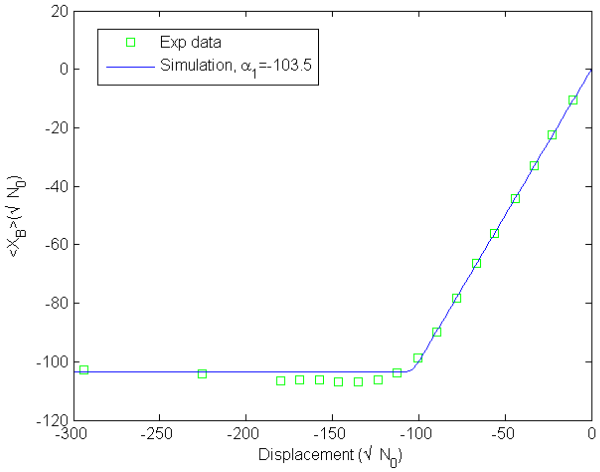


Fig. 8.5 Experimental measurements and predictions of relation Mean vs Displacement.

can be summarized in the Fig.8.4. Meanwhile, with highly displaced vacuum signal, we can also predict the lower saturation limit α_1 when the displacement is high enough. The mean value for $X_{B_{sat,0}} \leqslant \alpha_1 < 0$ in the saturation region directly reveals α_1:

$$\langle X_{B_{sat,0}} \rangle = \alpha_1. \tag{8.19}$$

As shown in Fig.8.5, the experimental data (green square) in the linear region can be described by Eq.(8.16), and the data in the saturation region can be described by Eq.(8.19) which gives the value of α_1. We also use the saturation model Eq.(8.7) to predict the behavior as shown in Fig.8.5(blue curve) where the noise of displacement ξ_E has been calibrated by Eq.(8.18). Another observation from the experimental data and simulation is that the turning point between linear and saturation region is not exactly sharp but somehow smooth, and it is due to the added noise ξ_E. From Fig.8.5, we calibrate the lower bound of detection limit as $\alpha_1 = -103.5\sqrt{N_0}$. It corresponds to a voltage value of -2.5 V for our homodyne detector. Note that in our setup of homodyne detection, the range of DAQ is set to [-10V, 10V] instead of [-0.5V, 0.5V] in section.7.2, thus the saturation effect is due to the electronics and amplifiers of the homodyne detection and not due the DAQ range setup.

8.2.4 Analysis of experimental results

With our experimental setup, we perform several tests by changing the values of displacement Δ and gain G. For $V_A = 5$, we gradually increase the displacement value Δ and the experimental distribution between X_B and X_A is shown in Fig.8.6. Due to the displacement action, we can observe that the distributions are same in the linear region (0-2V) except

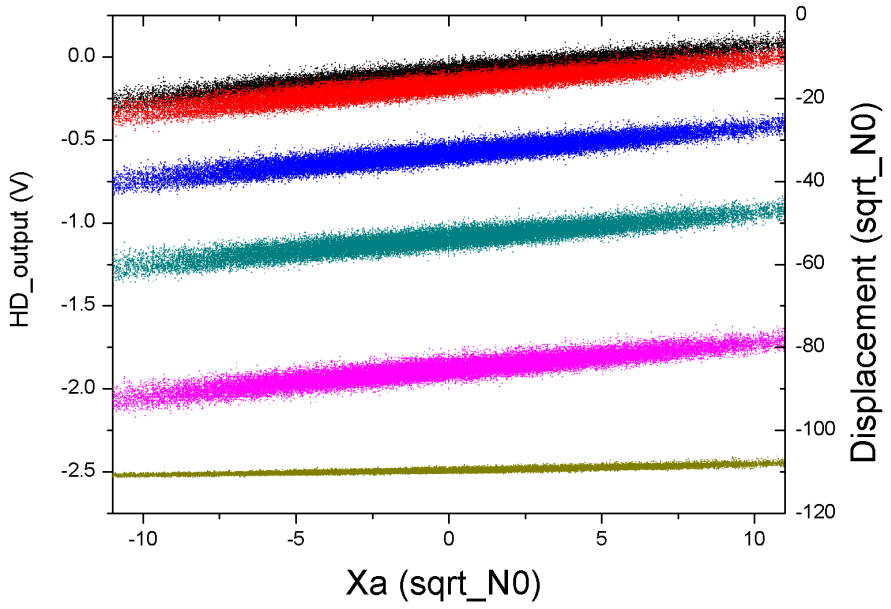


Fig. 8.6 Experimental distribution X_B vs X_A for different values of displacement.

the mean values are different from one to another. However, due to the finite linear detection range, when $\Delta < -103.5\sqrt{N_0}$, the distribution shrinks to almost a line which reveals the saturation effect of our homodyne detection. In our experiments, for each set value of Δ and G, the corresponding parameter estimation yields excess noise $\hat{\xi}_{sat}$ and channel transmission $\hat{T}_{sat}$. Experimentally, with a given modulation variance of Alice $V_A = 5$, we vary the values of Δ, G and measure $\hat{\xi}_{sat}$, $\hat{T}_{sat}$ through a standard CV QKD procedure as mentioned in section.8.1.2. As we can see in Fig. 8.7, for Alice modulation variance $V_A = 5$, it is clear that the excess noise estimation $\hat{\xi}_{sat}$ drops below the null key threshold around the saturation limit α_1, and the null key threshold ξ_{null} is deduced based on the corresponding $\hat{T}_{sat}$ and $V_A = 5$. On the other hand, given by the calibrated values $\alpha_1 = -103.5$ and ξ_E (Eq.8.18), we can also predict the excess noise estimation $\hat{\xi}_{sat}$ with Eq.(8.11) in simulations, and compare them with experimental values. As shown in Fig. 8.7, the prediction from Eq.(8.11) matches the behavior of excess noise estimation that we observe in experiments.

An important observation of Fig. 8.7 is that the excess noise estimation $\hat{\xi}_{sat}$ falls sharply around the detection limit, where for a small range of Δ values, ξ_{sat} varies from a large positive value quickly to a negative value. The large variations of $\hat{\xi}_{sat}$ respect to small values of Δ is mainly due to the saturation effect itself as we can see from the simulation curves in Fig. 8.7 and also by the analysis in chapter 7. The variation of $\hat{\xi}_{sat}$ can be moreover quantified by its variance. In the case of $G = 2.25$ shown in Fig. 8.7, for 25 measured values

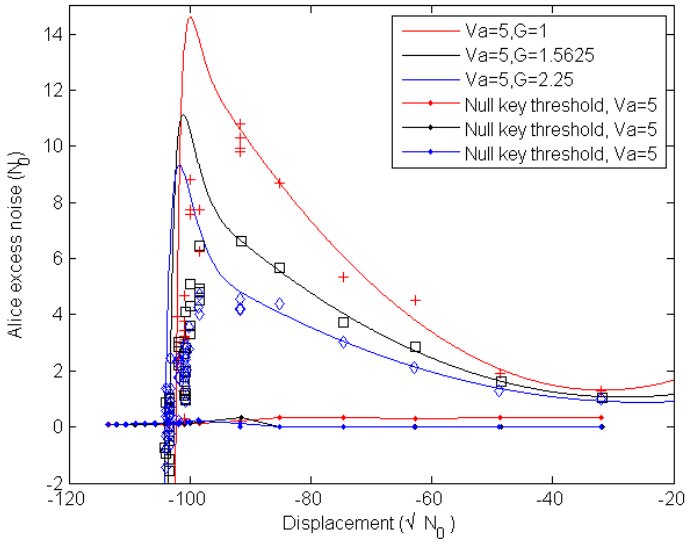


Fig. 8.7 Alice Excess noise vs displacement. Experimental results: Symbol plus $G = 1$, square $G = 1.5625$, diamond $G = 2.25$. Experimental parameters: Alice's variance $V_A = 5$, Bob's efficiency $\eta = 0.55$, excess noise of electronics $v_{\text{ele}} = 0.015$, detection limit $\alpha_1 = -103.5$. Simulation results: (1) Solid lines on color red, black and blue: excess noise estimations for given parameters; (2) Solid lines with dots: null key thresholds for given parameters; simulations are performed based on Eq.(8.11) and Eq.(8.12), in which parameters are set same as experimental parameters and the noise due to displacement is referred to Eq.(8.18).

of $\hat{\xi}_{sat}$ around saturation limit $-103.986 < \Delta < -103.184$, we can calculate its variance $Var(\xi_{sat}) = 1.1942$, which can not archive the requirement for a successful attack. In fact, in order to achieve a successful saturation attack, we need to bias $\hat{\xi}_{sat}$ into the region $0 < \hat{\xi}_{sat} < \xi_{null}$ and further reduce $Var(\hat{\xi}_{sat}) < 10^{-2}N_0$ for our saturation model. Approximately, it implies a precision about $10^{-3}\sqrt{N_0}$ on Δ. It however represents a challenge with our experimental system, as we can see from Fig. 8.7, it is difficult to precisely control $\Delta \sim \alpha_1$ such that the excess noise estimation falls exactly into the region $0 < \hat{\xi}_{sat} < \xi_{null}$.

In order to achieve a successful attack so that a positive key rate must be obtained. We need to further determine the choice of Δ and G on our experimental setup. In order to achieve this, for $V_A = 5$ with given calibrated values $\alpha_1 = -103.5$ and ξ_E (Eq.(8.18)), we continuously change the values of Δ and G in Eq.(8.11) and Eq.(8.12) to predict $\hat{\xi}_{sat}$ and $\hat{T}_{sat}$. For each set of (Δ, G), we further calculate the secret key rate K_{sat} based on corresponding $\hat{\xi}_{sat}$, $\hat{T}_{sat}$ with the assumption that if $\hat{\xi}_{sat} < 0$, K_{sat} is set to zero. By repeatedly calculating K_{sat}, we find the values of G and Δ compatible with a positive key rate: $K_{sat} > 0$. This result is shown in Fig.8.8. In this figure, we construct a 3D key rate curve from which we can

predict the optimal choice of Δ and G where the key rate is maximum.

Moreover, from Fig.8.8 we can study when the second criteria of a successful attack (section.7.4.2) is met: when the channel transmission between Alice and Bob is not biased while they are still able to generate a positive key rate. We consider a procedure that Alice's modulation variance is optimized depending on the distance [63]. In our case, optimal modulation variance $V_A = 5$ corresponds to a loss $T = 0.05$. Based on Eq.(8.11), we also calculate $\hat{T}_{sat}$ from the values of Δ and G. A given estimated loss, i.e, $\hat{T}_{sat} = 0.05$, corresponds to a pair value of Δ and G as shown in Fig.8.8 (Red dash line). The intersection points between this red dash line ($\hat{T}_{sat} = 0.05$) and the positive key rate projection line (2D blue line) thus give the choice of Δ and G that meet the second criteria $\hat{T}_{sat} = T$. There can be sometimes no intersection points between yellow/green dash lines ($\hat{T}_{sat} = 0.11, 0.2$) and the blue line. Indeed for distances below 44 km, we can not meet the second criteria $\hat{T}_{sat} = T$ for $V_A = 5$. Fig.8.8 can be used as a reference for Eve to choose the values of Δ and G so that the first or the second criteria (section.7.4.2) of a successful attack can be met.

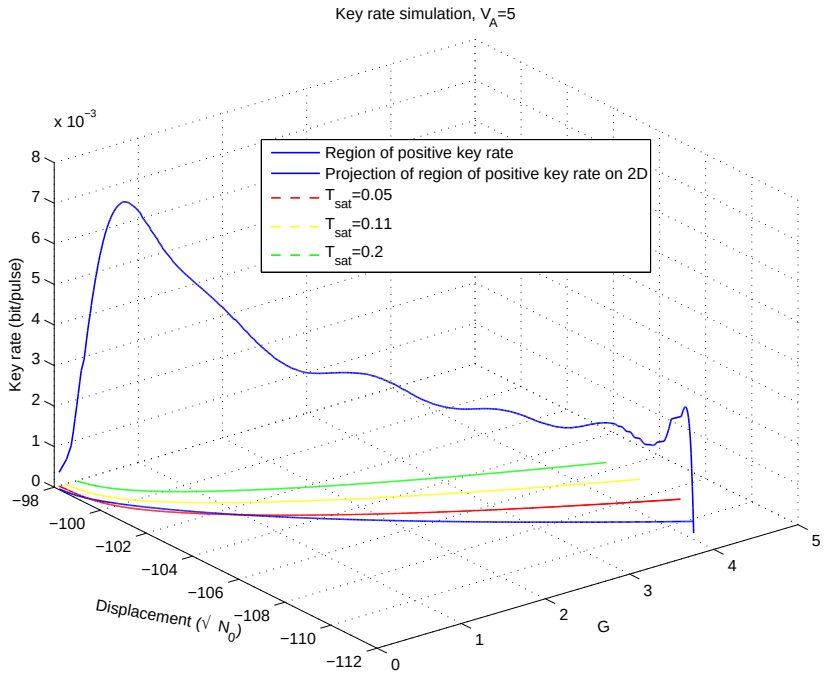


Fig. 8.8 3D Key rate vs displacement & Gain.

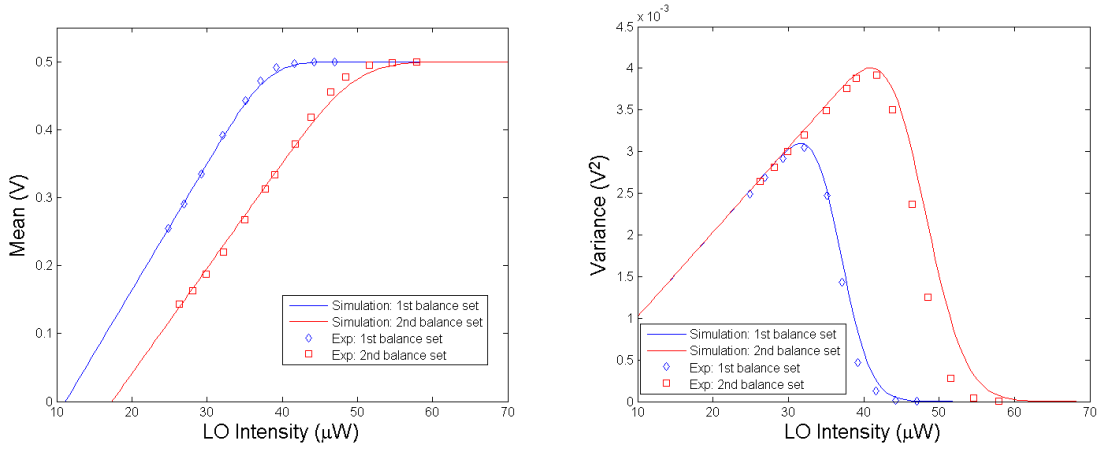
8.3 A side channel attack on CV QKD by inserting an external laser

In the previous section, we have described an experimental demonstration of the saturation attack, however, the stability and precision experimentally achievable for displacement preparation are not good enough to allow Eve to launch the attack efficiently. For this reason, we propose a new attack strategy to induce saturation on homodyne detection: instead of a strong displaced signal, we propose to insert an external light into Bob's signal port. This new strategy is simple to implement experimentally and allows a high precision control of induced saturation.

8.3.1 Imperfections of a balanced homodyne detection

In this attack with an external laser, we want to take advantage of imperfection in a practical homodyne detection: The transmission and reflection of a 50/50 beam splitter are not exactly equal. In CV QKD, this imperfection results in a small LO intensity leakage on the homodyne detection output. Such leakage contributes to a DC component in the measured quadrature signal and a noise variance which depends on the laser intensity. The DC component induces a offset on homodyne output signal, which actually plays a role as signal displacement (Δ) in saturation attack (Eq.(8.4)). The noise variance consists of two parts: the shot noise of LO pulse and a noise term depends on the LO intensity fluctuation (Eq.(5.22)), which have been addressed in section.5.1. In order to balance a homodyne detection (reduce LO intensity leakage), in practice one can adjust the attenuation of one of the optical paths after the beam splitter.

However, such balancing is only valid for the LO pulse going into the LO port. On the other hand, for the light going the signal port is not balanced. If one sends an intense laser on the signal port, then a large DC component due to this laser will be induced on the homodyne output signal. Moreover, most of the beam splitters have wavelength dependent properties [56, 57, 112], thus the transmission of the beam splitter can be biased significantly depending on the wavelength of the input light. In this sense, Eve has the possibility to 'control' the transmission of Bob's beam splitter by selecting proper wavelength of an external light. In order to study how these two imperfections (saturation and imbalance) impact on the homodyne output signal, we perform a simple experiment test. This test is actually a shot noise measurement (input signal as vacuum) as we have performed in section.7.2.2, but we intentionally imbalance the homodyne detector with two setups: 1st and 2nd, by adjusting the optical loss before two photo diodes. The homodyne detection bal-



(a) (b)

Fig. 8.9 Shot noise measurements of homodyne detection with two balance sets (a) Mean value vs LO Intensity. (b) Shot noise variance vs LO Intensity.

ance of 1st setup is worse than the 2nd balance set. It means that imbalance factor for the 1st setup $\varepsilon_1 = 1-2T_1$ is larger than the imbalance factor for the 2nd setup $\varepsilon_2 = 1-2T_2$. $T_{i=1,2}$ is an equivalent transmission of the beam splitter which has taken the optical losses before two photo diodes into account. For the 1st or 2nd setup, the outputs of homodyne detection are given by:

$$X_{B,0_{1,2}} = \sqrt{\eta}(1-2T_{1,2})I + X_0 + X_{ele}, \tag{8.20}$$

in which I is photon number per pulse. We adjust the DAQ detection range to $[-0.5V, 0.5V]$ which are the linear detection limits. Any homodyne signals out of this range will be saturated to $-0.5V$ or $0.5V$. By increasing the LO intensity, the mean value and noise variance for the 1st and 2nd sets both increase proportionally with the LO intensity in the linear region as discussed in section.7.2.2. However when LO intensity is relatively high, the response of homodyne detection overpasses the saturation threshold and the detection is saturated so that the mean value is constant (Fig.8.9(a)) and the measured variance drops quickly (Fig.8.9(b)). By using the saturation model (Eq.(8.7)) we can account such results.

Another observation from this test is that, for a same LO intensity ($30\mu W$), saturation happens in the 1st setup (Blue curve in Fig.8.9(b)) but not 2nd setup. The reason for this behavior is the following: when we vary the LO intensity, for each measurement, the homodyne output signal always includes a DC component whose value is proportional to the balance factors ε_1 or ε_2. With our setup the 1st balance is worse than the 2nd where $\varepsilon_1 > \varepsilon_2$, consequently the homodyne signal of 1st setup reaches the detection limit at a smaller value

of LO intensity compared to the 2nd setup. The impact of ε_1 and ε_2 can also be observed on the mean value measurements as shown in Fig.8.9(b). The mean value is proportional to the balance factors as predicted by Eq.(8.20).

These experimental tests comfort use to propose us to formalize a new attack, where Eve inserts an external laser into the signal port, such that the balance of the homodyne detection is biased.

8.3.2 Attack strategy

By considering the two imperfections (saturation and imbalance) of a homodyne detection mentioned above, we formalize a new hacking strategy targeting on a CV QKD system. In this attack, an external light is inserted into the signal port of Bob's homodyne detection, in order to function as the displacement in the saturation attack. We have two assumptions in this attack: (1) The balance of Bob's homodyne detection for LO port is perfect, which means the transmission of the beam splitter for LO pulse is $T_{lo} = 0.5$. (2) We implement the real time shot calibration (*Method. C* in section. 6.3.2), thus the shot noise measurement is not influenced. Let us now go into details of this new attack and analyze the impact of the external laser. This attack is mainly divided into two parts:

1. Eve implements a full intercept-resend attack [104] by performing a heterodyne detection, which gives her full information of both quadratures X and P sent by Alice. In order to simplify the analysis, we consider the case where Eve performs measurements and resending with single station right after Alice as in Chapter 7. We can thus deduce Bob's variance from this step under a linear detection:

$$V_{B1} = \eta T \frac{G}{2} V_A + \eta T \frac{G}{2} (\xi_{IR} + \xi_{sys}) + 1 + v_{\text{ele}}, \tag{8.21}$$

   in which $\xi_{IR} = 2$ is the excess noise due to IR attack, ξ_{sys} is system excess noise, T is channel transmission and $G = g^2$ is a gain factor introduced by Eve. All the units are normalized in shot noise units ($N_0 = 1$).

2. Eve inserts an external laser (pulsed or CW) into the signal port of Bob's homodyne detection in general is not coherent with the CV QKD signal. In practice, Eve can set the polarization of the second laser as the one of the CV QKD signal, if the polarization multiplexing technique is used (section.4.2.2). Since this external light is incoherent with LO, there is no interference between the external light and LO, we can thus independently analyze the impact of this external light on the homodyne output. According to the analysis mentioned before, the imbalance of the signal where

the external laser is sent, leads to a DC component on the output signal:

$$X_{B,2} = \sqrt{\eta}(1-2T_{bs})I_2 + X_0 + X_{ele}, \tag{8.22}$$

in which T_{bs} is the transmission of homodyne detector's beam splitter for the external light, it includes the optical loss before two photo-diodes, in this attack we consider $T_{bs} = 0.49$. Note that the value of T_{bs} is assumed to be known by Eve as in the wavelength attack [56, 57, 112]. I_2 is the number of photons per pulse of the external laser impinging on Bob's signal port. The impact of the DC component on homodyne output plays the same role as the displacement Δ in the saturation attack: bias the mean value of the measured quadrature signal. Under this external laser attack, the equivalent displacement of Bob homodyne measurement can be given by:

$$\Delta = \sqrt{\eta/I_1}(1-2T_{bs})I_2 = r\sqrt{\eta I_1}(1-2T_{bs}), \tag{8.23}$$

in which I_1 is the photon number of one LO pulse, $r = I_2/I_1$ is the photon number ratio between one LO pulse and the external light with I_2 as the photon number of the second laser. Δ is normalized in the square root of shot noise units. On the other hand, the external laser includes two kinds of noise: its own shot noise in a different mode of LO and the noise due to its intensity fluctuation [16]. The shot noise can be deduced from an unbalanced two port homodyne detection model [112]:

$$N_{0,2} = 4T_{bs}(1-T_{bs})I_2. \tag{8.24}$$

The noise due to intensity fluctuation has been analyzed in [16] and also in section.5.1. If the the intensity fluctuation ratio of the second laser is given by $f_2 = \sqrt{\langle I_2^2\rangle - \langle I_2\rangle^2}/I_2$, then the corresponding noise variance is given by:

$$V_{f,2} = \eta f_2^2(1-2T_{bs})^2 I_2^2. \tag{8.25}$$

In our analysis, we consider $f_2 = 0.1\%$. Given with $N_{0,2}$ and $V_{f,2}$, the total noise variance induced by the external laser in shot noise units is given by:

$$V_{B2} = N_{0,2} + V_{f,2} = 4T_{bs}(1-T_{bs})r + \eta r^2 f_2^2(1-2T_{bs})^2 I_1. \tag{8.26}$$

In order to achieve a security break, Eve needs to properly set the intensity of the second laser I_2 to effectively bias the noise due to the intercept-resend attack and the second laser. We will analyze this issue in the following subsection.

8.3.3 Security analysis and simulations

The second laser is incoherent with LO pulses, thus, under the linear detection region, Bob's measurement variance is the summation of the variances in step 1 and 2 of the attack:

$$Var(X_{B_{lin}}) = V_{B1} + V_{B2} \tag{8.27}$$

$$= \eta T \frac{G}{2} V_A + \eta T \frac{G}{2}(\xi_{IR} + \xi_{sys}) + 1 + 4T_{bs}(1 - T_{bs})r + \eta r^2 f_2^2 (1 - 2T_{bs})^2 I_1 + v_{\text{ele}} \tag{8.28}$$

If we further choose $G = 2$, by taking Eq.(8.27) ($Var(X_{B_{lin}})$) into Eq.(4.17), we can deduce the excess noise estimation of Alice and Bob with a linear detection:

$$\hat{\xi}_{lin} = \xi_{IR} + \xi_{sys} + V_{B2}/(\eta \hat{T}_{lin}). \tag{8.29}$$

And the channel transmission estimation:

$$\hat{T}_{lin} = T. \tag{8.30}$$

However, if the equivalent displacement (Δ in Eq.(8.23)) due to the external light is large enough, homodyne detection output can be saturated as in saturation attack [140]. In fact, Eve actively controls the value of Δ by selecting proper properties of the external light, in particular the value of I_2. In consequence, Eve's action can bias the estimated excess noise of intercept-resend attack and the external light to an arbitrary small value.

Similar as in the previous analysis, we perform the parameter estimation of Alice and Bob under the attack, since they determine whether Eve can have a security break. In order to analyze the estimations of channel transmission $\hat{T}_{sat}$ and excess noise $\hat{\xi}_{sat}$ under this attack, we refer to the results of saturation attack with one Eve's station (Chapter 7). We can simply use the expressions of Δ (Eq.(8.23)) and $Var(X_{B_{lin}})$ (Eq.(8.27)) into the saturation model (Eq.(7.8)). Moreover, by taking Eq.(8.23) and Eq.(8.27)into Eq.(7.9) and Eq.(7.10), we can deduce $\hat{T}_{sat}$ and $\hat{\xi}_{sat}$ under this attack with an external laser. With such modifications, we can perform simulations to predict $\hat{T}_{sat}$ and $\hat{\xi}_{sat}$ with respect to Eve's action (choice of I_2) in simulations. The simulation parameters are considered as follows: gain factor of Eve $G = 2$, beam splitter ratio for second laser $T_{bs} = 0.49$, intensity fluctuation of the second laser $f_2 = 0.1\%$, beam splitter ratio for LO pulse $T_{lo} = 0.5$, photon number per one LO pulse $I_1 = 10^8$, detection limit $\alpha_1 = -\alpha_2 = 20$, detector efficiency $\eta = 0.6$, detector electronic noise $v_{\text{ele}} = 0.01$, V_A is optimized with distance according to the procedure in [63].

In order to calculate $\hat{\xi}_{sat}$ and ξ_{null}, we continuously change the value of I_2 and thus the

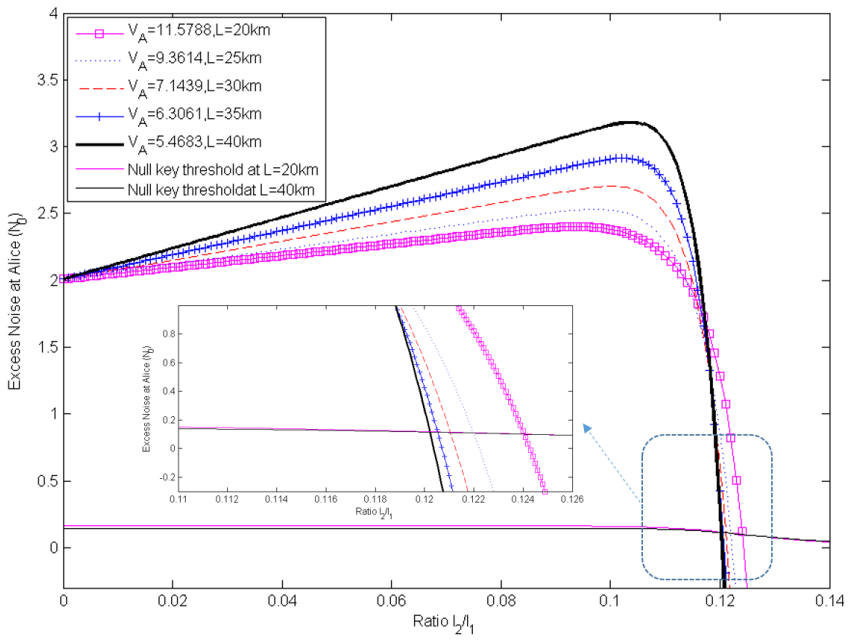


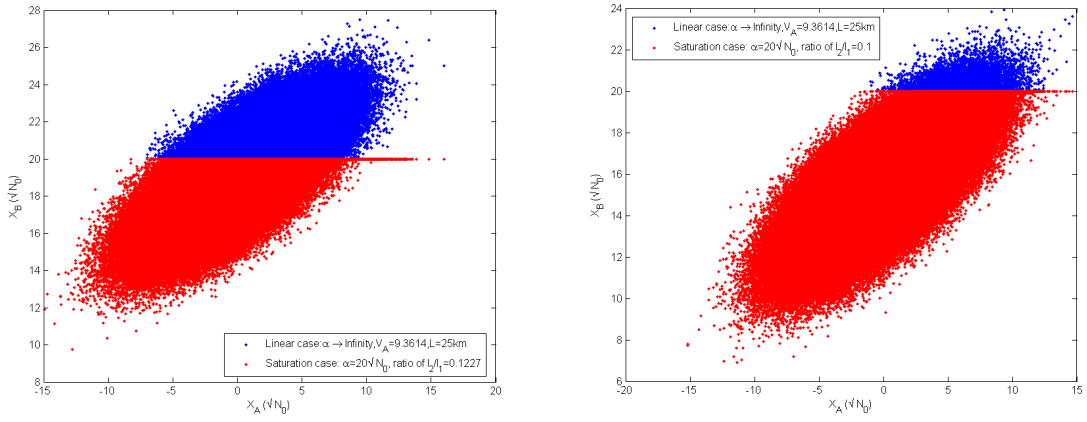
Fig. 8.10 Estimation of Alice excess noise vs photon number per pulse ratio r. $\eta = 0.6$, $T_{bs} = 0.49$, $v_{\text{ele}} = 0.01$

ratio r, each value of r corresponds to a set of $\hat{T}_{sat}$ and $\hat{\xi}_{sat}$ as the parameter estimation of Alice and Bob. For a given variance V_A and $\hat{T}_{sat}$, we can further deduce the corresponding null key threshold ξ_{null}. These results are shown in Fig.8.10 with several distances (20, 25, 30, 35, 40km), the estimated excess noise at Alice side varies with the ratio r, it shows the impact of Eve's action on parameter estimation. Similarly as in the saturation attack, the behavior of $\hat{\xi}_{sat}$ is 'sharp' around detection limit, which meets our expectations. Since the saturation effect is the detector's own property, in this attack, we just use a new method to induce saturation. Although the curves are sharp around $r = 0.12$ in Fig.8.10, if we enlarge the scale of r, each value of $\hat{\xi}_{sat}$ does correspond to an unique value of r. It means once Eve has enough precision on the intensity of the second laser, she can accurately manipulate the excess noise estimation.

A drawback of this attack is that if Eve wants to induce enough saturation, the corresponding noises becomes large since it increase with the ratio r, as shown in Fig.8.10. On the other hand, for a same ratio r, the excess noise estimation in the linear region at short distance, i.e 25km, is larger than the one at long distance, i.e.40 km, which is due to the factor $1/(\eta \hat{T}_{lin})$ in Eq. (8.29). For a given distance, Eve can choose a proper ratio r to bias the estimated excess noise $\hat{\xi}_{sat}$ below the null key threshold $\hat{\xi}_{null}$ such that Alice and Bob still believe they share a secure key according to their parameter estimation, however

the generated keys are not secure at all. Thus the first criteria defined in section.7.4.2 is achieved. Moreover, we can also achieve the second criteria : $\hat{T}_{sat} = T$ and $\hat{\xi}_{sat} < \xi_{null}$. It requires Eve to set the value of g according to Eq.(7.14), where Δ and $Var(X_{B_{lin}})$ are referred to Eq.(8.23) and Eq.(8.27).

In order to clearly demonstrate influences of saturation effect on the parameter estimations, in Fig.8.11 we plot the distribution between Alice and Bob's data for a saturation (red dots) and non saturation case (blue dots), with (a) $r = 0.1227$ and (b) $r = 0.1$ at 25 km. The first observation from Fig.8.11 is that if the linear detection is arbitrary large, the distribution of $X_{B_{lin}}$ vs X_A is not biased but with a displacement (blue dots). However, if we consider a realistic detector, the distribution of $X_{B_{sat}}$ vs X_A has been significantly altered (red dots) due to detector saturation, which result in wrong parameter estimation. The second observation is that Eve needs to increase the ratio r to a enough high value such that $\hat{\xi}_{sat}$ is biased below ξ_{null}. In Fig.8.11(a), the choice of $r = 0.1227$ corresponds to a security break which means $\hat{\xi}_{sat} < \xi_{null}$ while the choice of $r = 0.1$ in Fig.8.11(b) can not lead to a security break. It means that Eve needs to insert a light with sufficient high intensity to bias Bob's distribution in order to achieve a security break, otherwise, Alice and Bob can still detect the noise due to intercept-resend attack through their parameter estimation even if saturation is induced. Fig.8.10 is the reference that Eve can set the value of r.



(a) (b)

Fig. 8.11 Bob vs Alice's data distribution. Red: $X_{B_{sat}}$, blue: $X_{B_{lin}}$ (1) $r = 0.1227$, security break; (2) $r = 0.1$, no security break.

Furthermore, we can also extend this attack to the case where Eve has two stations as discussed in section.8.1. It is also possible to further propose a corresponding experimental plan as in section.8.1.2 where the setup consists of a intercept-resend attack with two Eve's

stations and a second laser inserted into signal port of Bob's homodyne detection. In order to analyze the security, we can just apply a few modifications on the previous analysis, to deduce the estimations of excess noise and channel transmission: (1) Take Eq.(8.27) with $T = 1$ into Eq.(8.11) and Eq.(8.12); (2) Replace Δ in Eq.(8.11) and Eq.(8.12) with Eq.(8.23) for $T_{bs} > 0.5$. With such modifications, we can moreover deduce the conditions that can satisfy the first and second criteria of a successful attack as mentioned in section.7.4.2.

Compared to saturation attack relying on coherent displacement, this new attack is much easier to realize experimentally, since Eve doesn't need to prepare a strong displacement signal with very high precision, which is experimentally challenging as shown in the previous section. Moreover, this attack only requires the precision of the laser intensity. According to the simulations before, a successful attack is possible with the choice of $I_2 = rI_1 = 0.1227 \times 10^8 = 1227 \times 10^4$, which shows that Eve needs a precision of 10^4 photons on the second laser to accurately bias the excess noise estimation. Such precision is realistic and achievable with current technology. On the other hand, this attack also explores the imperfection of detector saturation, thus the countermeasures available for saturation attack can be also applied to this attack.

8.4 Conclusion

In this chapter, we have performed the first experimental demonstration of the saturation attack in experiment. This demonstration is based on a modified saturation attack strategy where Eve has two stations, which is slightly different from the case analyzed in Chapter 7. Importantly, we have experimentally realized a functional "Eve" to perform a coherent displacement operation which is a core part of our saturation attack. We have experimentally studied the relation between Eve parameters (gain and displacement) and Alice-Bob parameter estimation. Based on our experimental parameters, we have moreover deduced the choices of Eve's parameters (gain and displacement) that two possible criteria for a successful attack (section.7.4.2) can be achieved. However, the precision and stability of the coherent displacement operation can not meet the strict requirements in saturation attack. In fact, implementation of strong and precise displacement is experimental challenging, where we still need more efforts to improve it. For this reason, we have proposed a new attack strategy to induce detector saturation. By exploring the imperfection of the beam splitter used in homodyne detection, we use an external light to function like the strong displacement as in saturation attack. According to our analysis, this new attack can also lead to a security break of a CV QKD system, we have also deduced Eve's parameter choice that a successful attack is possible. Moreover, this new attack is more experimentally friendly compared to satura-

tion attack, since it only requires accurate control of laser intensity instead of complicated implementation of displacement.

Chapter 9

Compatibility of CV QKD system with WDM network

In this chapter we move to another topic in this thesis: study the compatibility of CV QKD system with Wavelength Division Multiplexing (WDM) network. Such study is an important step towards integration of CV QKD systems into real optical network.

This chapter is mainly divided in two parts: (1) In the preliminary work, I have analyzed different noise contributions in a coexistence regime of Dense Wavelength Division Multiplexing (DWDM) classical channels with CV QKD system and their impacts on the system performance. It is done through theoretical analysis and simulations with realistic experimental parameters, along with few simple experimental tests. (2) In the main work, we perform a full demonstration of coexistence of CV QKD with intense DWDM classical channels [80], where a CV QKD system is inserted into a DWDM test-bed. This part of work has been done through the collaboration with several researchers in our team and in particular, Dr.Rupesh Kumar.

9.1 Introduction

Wavelength Division Multiplexing (WDM) allows to share a single optical fiber to transport multiple optical channels using different wavelengths. WDM compatibility of quantum and classical communications would allow to deploy QKD on lit fiber. This would boost the compatibility of quantum communications with existing optical infrastructures and lead to a significant improvement in terms of cost-effectiveness and addressable market for QKD.

However, coexistence with intense classical channels raises new challenges for QKD. The optical power used on optical classical channels is orders of magnitude higher than for

quantum communication. Multiplexing classical and quantum signals on a single fiber can result in very important additional noise for the quantum communication, due to insufficient isolation or to optical non-linear effects [18]. Coping with such noise is in general a major problem for QKD systems and filtering techniques are needed to improve the ratio between quantum signal and WDM-induced noise. The implementation of this filtering can result in additional losses and severely impact the performance of QKD. This is in particular the case for systems that rely on spectrally wide-band single photon detectors[163].

Pioneering work on QKD and wavelength division multiplexing has been performed at the very early days of QKD research by Paul Townsend and coworkers [173], with one classical channel at 1550nm multiplexed with a quantum channel at 1300nm. This corresponds to a Coarse Wavelength Division Multiplexing (CWDM) configuration, that has been studied in several other works [15, 17]. The large spectral separation the quantum and the classical channels presents the advantage of reducing the amount of noise due to Raman scattering (that is approximately 200nm wide) onto the quantum channel. CWDM-QKD integration configuration has however several limitations: it can only accommodate shorter distance (due to the higher attenuation for QKD at 1300nm) and the coexistence is limited to a small number (below 8) of classical channels due to the large inter-channel spacing in CWDM. One could thus use this configuration in priority in the context of access networks, where it seems best suited [7].

On the other hand, if QKD is to be transported over long-distance links (beyond 50km) and in coexistence with a large number of classical channels, which is the case in core or wide-area optical networks, then Dense Division Wavelength Multiplexing (DWDM) is required. DWDM compatibility, i.e. the capacity to coexist with standard optical channels, all multiplexed in the C band (wavelength range 1530–1565nm), with relatively narrow channel spacing (from 1.6nm to 0.2nm), is the focus of the present article. DWDM compatibility of QKD has initially been studied by Peters et al. [132], where Raman noise was identified as the main impairment for links longer than a few km. A coexistence test of QKD with two forward-propagating classical channel and a total input power of 0.3 mW has been performed. Despite this input power below typical optical network specifications and the use of some filtering, QKD could not be operated beyond 25 km. More recently, several new DWDM compatibility experiments have been performed, with discrete variable QKD (DV-QKD) systems and more efficient filtering techniques. In [30], 4 classical channels where multiplexed with a DV-QKD system and 50km operation was demonstrated. However, the input power of the classical channels was attenuated below -15dBm, to the smallest possible power compatible with the sensitivity limit of the optical receiver (-26dBm). This technique was also used in [129] with an input power limited down to -18.5dBm and in addition the

use of a temporal filtering technique developed in [17] to obtain a range of 90km.

The extended working range for DV-QKD coexistence with DWDM channels demonstrated in [30, 129] is of practical interest. However, these demonstrations have been performed with strongly attenuated classical channels, more that 15dB below the standard level of optical input power commonly used in existing optical network. This indicates the difficulty of integrating DV-QKD in optical networks in coexistence with standard optical power (around 0dBm). Coexistence of DV-QKD with 0dBm channels has however recently been demonstrated over 25 km [130], but it requires additional use of fine-tuned time and spectral filtering.

In fact compared to DV-QKD, CV QKD has a better noise tolerance in the integration with WDM network thanks to its coherent detection. Only photons in the same spatio-temporal and polarization mode as the quantum signal would contribute as excess noise while noise photons in different modes would be suppressed effectively. Promising results have been shown in the analysis of [138], where spontaneous Raman scattering noise and amplified spontaneous emission noises of an erbium-doped fiber amplifier (EDFA) are considered in a coexistence regime of WDM network with CV QKD system. Unfortunately, there are no experimental demonstrations of this work, which leave a question that whether CV QKD can performer better than DV-QKD in such coexistence architecture with WDM network.

In the first part of this chapter, we extend the analysis of Qi et al. [138] and study different source of excess noise from the classical channels. In the second part of this chapter, we show that the use of CV QKD could be advantageous in order to deploy QKD in DWDM coexistence with standard optical channels: we have shown that CV QKD can coexist with classical channels whose cumulated power could be as high as 11.5 dBm at 25 km. We have also demonstrated CV QKD operation (with a key rate of 0.49kbit/s) at 75 km in coexistence with a -3 dBm channel. This stronger coexistence capability can be obtained without any additional filtering and could be of significant advantage in many practical situations related to QKD integration in standard optical networks.

9.2 Preliminary: analysis of noise contributions and simulations

In a coexistence regime of WDM classical channels with CV QKD system, there are different noise contributions on the CV QKD signal, such as noises due to classical channels leakage, spontaneous anti-Stokes Raman scattering (SASRS), cross phase modulation

(XPM) and four-wave mixing (FWM). If the wavelength of the noise photons coincides with that of the quantum signal, they cannot be filtered out at Bob's side and will contribute to excess noise and lower the performance of CV QKD system. However, compared to DV-QKD in WDM network, the homodyne detection in CV QKD acts as a mode selector so that the noise photons in modes orthogonal to the LO mode are suppressed efficiently. Only photons in the same spatiotemporal and polarization mode as LO will contribute to excess noise [138]. As mentioned in chapter 4, excess noise is the key factor which need to be evaluated in CV QKD protocol, we would like to evaluate excess noise variances due to various nonlinear optical effects in a coexistence regime.

In order to evaluate these noises, we consider a coexistence model of CV QKD signal and classical signals as shown in Fig.9.1: the CV QKD system is multiplexed with forward (from Alice to Bob) and backward (reverse) propagating DWDM channels, by using multiplexer (MUX) and de-multiplexer (DEMUX) passive components. The wavelengths of quantum channel signal and classical channel signal are considered as λ_q and λ_c. The efficiencies of MUX and DEMUX are denoted as η_M and η_D.

9.2.1 Excess noise due to spontaneous Raman scattering effect

As already notice in [15, 30, 132], Spontaneous Raman Scattering (SRS) is the dominant source of noise for QKD in a DWDM environment, as long as the fiber length is beyond a few km. It is an inelastic scattering process during which scattered photons get converted into photons of either longer or shorter wavelength, respectively called Stokes and Anti-Stokes scattering. Anti-Stokes scattering is less probable than Stokes. Therefore, in order to minimize the amount of noise due to Raman scattering, it is preferable to place the quantum channel at a wavelength lower than the ones of the classical channels ($\lambda_c < \lambda_q$). We will assume here that this design rule has been followed so that we only need to focus on the effect of Spontaneous Anti-Stokes Raman Scattering (SASRS) photons on CV QKD system.

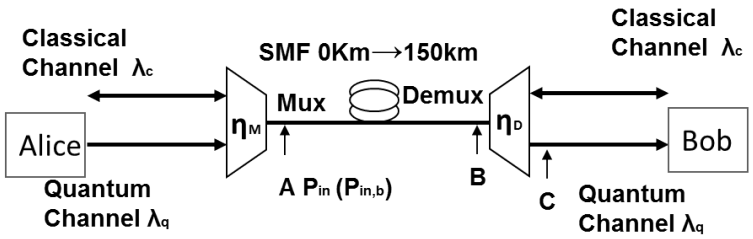


Fig. 9.1 Coexistence model of CV QKD signal and classical signals. P_{in}:Input power at point A, SMF:Single mode fiber. MUX: multiplexer, DEMUX: demultiplexer, η_M: Efficiency of MUX, η_D: Efficiency of DEMUX, η_{Bob}: Efficiency of Bob.

Since the SASRS noise varies with distance, it is interesting to evaluate its value at the output of DEMUX (C point in Fig.9.1) or the excess noise at Bob side.

Based on the analysis in [138], let us evaluate the excess noise due to SASRS photons. If the total input power at point A in Fig.9.1 is P_{in}, then the forward SASRS noise power within a bandwidth of $\Delta\lambda_q$ (measured at point B) is given by [15, 30]:

$$P_{SASRS} = P_{in}\beta_r L e^{-\alpha L}\Delta\lambda_q, \tag{9.1}$$

in which β_r is the spontaneous Raman scattering coefficient, P_{in} (measured at point A in Fig.9.1) is the input power of the classical signal, L is the fiber length and α is the fiber attenuation coefficient (dB/km).

As we mentioned, only the SASRS photons in the spatiotemporal mode as LO would contribute in band excess noise. Thus we need to estimate the SASRS noise photon number per spatiotemporal mode. In order to estimate this number, we first evaluate the total mode number N_{mode} and total number of SASRS photons N_{tot} for a given bandwidth $\Delta\lambda_q$ of the quantum channel. In experiments, if we measure the SASRS power P_{SASRS} by using an optical power meter at point B in Fig.9.1, the readout of optical power meter is the total energy received in one second:

$$P_{SASRS} = N_{tot}h\nu, \tag{9.2}$$

in which $h\nu$ is the energy of one photon with h as Planck constant and ν is the frequency of the quantum signal. N_{tot} is the total number of SASRS photons within a bandwidth of $\Delta\lambda_q$ and a time window of $\Delta t = 1s$ at point B. Corresponding to $\Delta\lambda_q$ and $\Delta t = 1s$, N_{mode} is given by:

$$N_{mode} = |\Delta\nu\Delta t| = \frac{c}{\lambda_q^2}\Delta\lambda_q, \tag{9.3}$$

In which λ_q is the central wavelength of the quantum signal laser, c is the speed of light in vacuum. With the efficiency of DEMUX as η_D, the SASRS photon number in one mode at the output of DEMUX is given by:

$$\langle N_{SASRS}\rangle = \frac{N_{tot}\eta_D}{N_{mode}} = \frac{P_{SASRS}}{h\nu N_{mode}}\eta_D = \frac{\lambda_q^3}{hc^2}P_{in}\beta_r L e^{-\alpha L}\eta_D, \tag{9.4}$$

in which λ_q is the LO wavelength, h is plank constant, c is the speed of light in vacuum.

Since LO defines a single spatiotemporal mode, the number of noise photons in matched mode with LO at Bob (point C in Fig.9.1) can be deduced from Eq.(9.4) and given by:

$$\langle N_{GMCS}^{in}\rangle = \frac{1}{2}m\langle N_{SASRS}\rangle = \frac{1}{2}mP_{in}\beta_r L e^{-\alpha L}\eta_D\frac{\lambda_q^3}{hc^2}, \tag{9.5}$$

in which the factor 1/2 is due to the polarization selection of the LO, m is the number of classical channels. According to [138], SASRS is modeled as output of a chaotic source with Bose–Einstein photon statistics, thus the excess noise due to SASRS in matched modes is given by:

$$\xi_{SASRS} = 2\eta_{Bob}\langle N^{in}_{GMCS}\rangle N_0 = \eta_{Bob} m P_{in} \beta_r L e^{-\alpha L} \eta_D \frac{\lambda_q^3}{hc^2} N_0, \tag{9.6}$$

where η_{Bob} is efficiency of Bob, and N_0 is shot noise. With the similar approach, we can also derive the excess noise due to the backward SASRS. With the backward SASRS power $P_{in,b}$ (measured at point A), we can know this power within a bandwidth of $\Delta\lambda$:

$$P_{SASRS,b} = P_{in,b}\beta_r \frac{1-e^{-2\alpha L}}{2\alpha}\Delta\lambda_q. \tag{9.7}$$

Thus the excess noise contributed by backward SASRS noise photons in matched mode with quantum signal is given by:

$$\xi_{SASRS,b} = \eta_{Bob} m P_{in,b} \beta_r L \frac{1-e^{-2\alpha L}}{2\alpha} \eta_D \frac{\lambda_q^3}{hc^2} N_0. \tag{9.8}$$

In order to characterize the excess noise due to SASRS, we perform simulations with realistic experimental parameters (Table.9.1). According to Eq.(9.6), we plot the excess noise (on Bob side) due to forward SASRS versus distance for different input powers of one classical channel. It simulates the situation that several classical channels (with input

Table 9.1 Simulation Parameters

Parameter	Value
α (Fiber attenuation coefficient)	0.21dB/km
β_r (Spontaneous Raman scattering coefficient)	$2\times10^{-9}/(km\cdot nm)$
λ_c (Wavelength of classical channel)	1559.75 nm
λ_q (Wavelength of quantum channel)	1554.94 nm
$\Delta\lambda$ (3 dB linewidth of LO)	0.02 nm
Δt_q (Duration of LO pulse)	100 ns
$\Delta\lambda_{filter}$ (1dB passband of WDM filter)	0.46 nm
η_D (Efficiency of DEMUX filter)	0.64 (or -1.9 dB)
η_{Bob} (Efficiency of homodyne detection)	0.6
P_{in} (Input power of one classical channel)	1mw $\longrightarrow$ 20mw
L (Length of fiber)	0km $\longrightarrow$ 100km

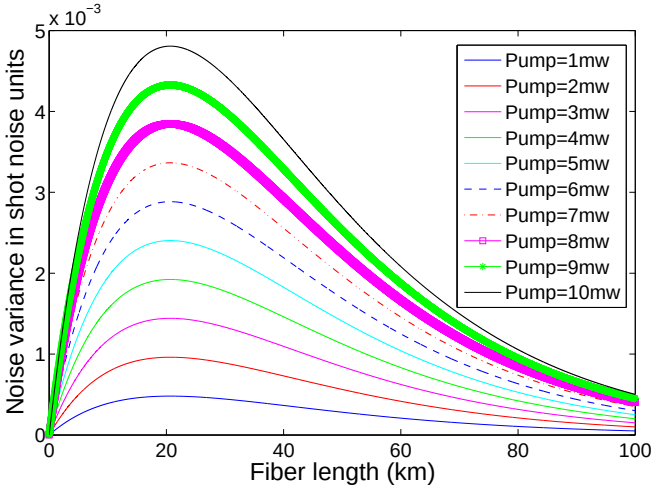


Fig. 9.2 Simulation of excess noise (on Bob side) due to spontaneous anti-Stokes Raman scattering (forward) with different input powers of one classical channel, simulation parameters are in Table.9.1.

power per channel as 0 dBm) are inserted into the DWDM system, since the excess noise (Eq.(9.6)) is proportional to both the input power (P_{in}) and the number of channels (m). As shown in Fig.9.2, the maximum noise variance is found at about 21 km, then the excess noise decreases with distance. And SASRS excess noise is three orders of magnitude lower than the shot noise. It thus requires high precision of CV QKD system to observe SASRS excess noise in experiments.

CV QKD performance with SASRS noises

In order to show the CV QKD performance in a DWDM integration environment. It is interesting to evaluate the secret key rate of CV QKD when there are several DWDM classical channels. We have simulated the secret key rate for GMCS protocol with reverse reconciliation for collective attack (section.4.5.2). The simulation parameters are given in Fig.9.3 which are realistic values for a practical CV QKD system. We have assumed input power of each classical channel is 0 dBm. As shown in Fig.9.3, one classical channel will shorten the secure distance about from 50 km to 45 km. But when there are 10 classical channels, CV QKD can still operate with a distance of more than 25 km. We can see that it is possible to multiplex CV QKD with several 0 dBm classical channels without significantly reducing its performance.

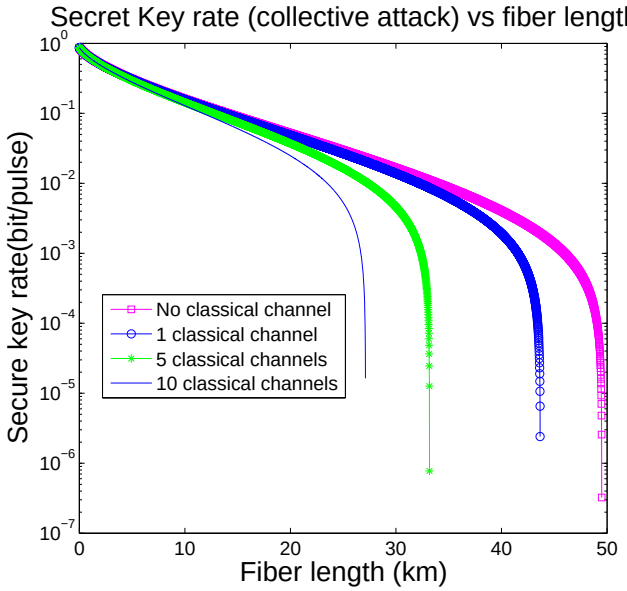
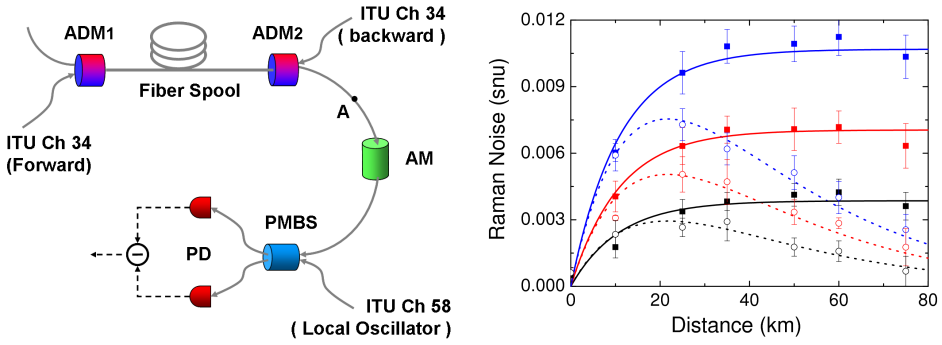


Fig. 9.3 Secure key rate with collective attack. Secure key rates are calculated under different conditions: no classical channel and different number of classical channels; Simulation parameter: Alice's variance $V_A = 10$, efficiency of Bob $\eta_{Bob} = 0.6$, efficiency of DEMUX filter $\eta_D = 0.64$, excess noise of electronics $v_{\text{ele}} = 0.01$, excess noise of system $\xi_{sys} = 0.01$, reconciliation efficiency $\beta = 0.9$, attenuation coefficient $\alpha = 0.21 dB/km$.

Experimental characterization of Spontaneous Raman Scattering in DWDM environment

In order to validate the prominence of Raman Scattering as source of noise, we have conducted experiments to estimate the value of the Raman scattering coefficient, β_r, and to validate experimentally the validity of Eq.(9.6) in order to predict the amount of excess noise induced by Spontaneous Raman Scattering on homodyne detector.

The experimental setup is shown in Fig.9.4(a). Classical channel at 1550.12nm (ITU channel 34) is multiplexed either in forward of backward direction into the fiber through Add and Drop Modules (ADM1/ADM2) and we perform noise measurement with a homodyne detector. Add and Drop Modules are DWDM elements that allow to multiplex/demultiplex (add/drop) a particular wavelength to/from an optical fiber channel on which it is placed. ADMs exhibits comparatively less insertion loss ($\approx$ 0.5dB) than WDM modules ($\approx$ 2dB). Moreover, we have obtained cross channels isolation of -46dB between adjacent channels and -96dB between non-adjacent channels. The wavelength of the classical channel is scanned over the entire C band (1530nm - 1565nm) with 5mW input power. Raman scattered photons at the wavelength 1531.12nm (ITU channel 58) of the quantum channel are collected through the Add/Drop port of ADM2.



(a) (b)

Fig. 9.4 Characterization of Raman noise.(a): Experimental setup. ADM- Add/Drop module, AM- Amplitude modulator, PMBS- Polarization Maintaining 50/50 Beam Splitter, PD- Photo diodes. (b): Noise (in excess of shot noise) induced by a classical channel of various power on a homodyne detection. Circles and squares are experimental data obtained for the classical channel in forward and backward directions, respectively. Blue, red and black colors indicate classical channel power of 8mW, 5mW and 3mW, respectively. Experimental data is fitted using Eq.(9.6) and Eq.(9.8) in forward (dotted) and backward (solid) directions.

We have characterized the Raman scattering coefficient, β_r, by measuring the intensity of backscattered photons, from a fiber spool of 25 km, using a power meter (model NOVA II, OPHIR optronics) at the point A in Fig. 9.4 (a) and an ADM of bandwidth 0.8 nm. We can use Eq.(9.6) to relate the power of Raman backscattering to the value of the coefficient β_r, whose measurement (that depends on the wavelength of the classical channel) varies from 1.5×10^{-9}/km.nm. to 3.1×10^{-9}/km.nm and agrees with that given in [30].

For the characterization of the excess noise induced by Raman scattered photons on the homodyne measurement we have used a specific technique to evaluate both total noise and shot noise variance. An amplitude modulator (AM) is used to close the signal port of homodyne detector during the shot noise measurement and is kept open for total noise measurement. In order to minimize the effect of homodyne output drift, shot noise and total noise measurements are taken in every alternative intervals. Forward and backward Raman noise variance are measured for different fiber channel lengths with various classical channel launch power. Results are as shown in Fig.9.4 (b). As we can see, in the forward scattering direction Raman noise reaches a maximum at $1/\alpha \sim 21$km, where $\alpha = 0.046$ is the fiber attenuation per km, and then decreases along with classical channel power. In the backward direction, noise reaches a saturation level as the distance increases. The experimental data is fitted using respective parts of Eq.(9.6) and Eq.(9.8) and found in good agreement with

the theory.

9.2.2 Excess noise due to classical channel leakage

We now move forward to another noise source in the coexistence regime of CV QKD with DWDM: leakage from classical channels. Compared to quantum signal, the power of classical channel is several orders of magnitude higher. Despite the wavelength of quantum signal is different from classical channel, a small fraction of the classical signal can leak into the quantum channel due to the finite isolation of the DEMUX (a typical value for non-adjacent channel is -80 dB while adjacent channel is -40 dB). However this kind of noise is so called out-band noise which can be effectively filtered out by the homodyne detection, according to the analysis in [138], such contribution on excess noise is negligible. Here we focus on studying the in-band noise due to side band photons of the classical channel. A classical channel laser has a broadband noise background which generates the sideband photons. The sideband photons at same wavelength as quantum channel can not be filtered out by the homodyne detection and they contribute excess noise in matched mode with quantum signal. For typical semiconductor distributed feedback (DFB) laser, the power of sideband photons is typically -60dB below the main mode (central wavelength). However, if the power of classical channel is large, the excess noise due to sideband photons is not negligible, since it contributes in-band noise. Similar as the study of SASRS noise, in order to evaluate the excess noise due to side band photons, we need to deduce the total number of noise photons $N_{tot,sb}$ and total modes number N_{mode} corresponding to the bandwidth $\Delta\lambda_q$ and a time window $\Delta t = 1s$, where the N_{mode} is given by Eq.(9.3). With a input power of classical channel at point A in Fig.9.1 as P_{in}, the total number of sideband photons is given by:

$$N_{tot,sb} = \frac{r_{sb} P_{in} e^{-\alpha L}}{h\nu}, \tag{9.9}$$

Here r_{sb} is side band ratio for the classical channel laser, a typical value is around -60 dB. Thus the number of sideband photons per mode is given by:

$$\langle N_{SB} \rangle = \frac{N_{tot,sb}}{N_{mode}} = \frac{\lambda_q^3}{hc^2 \Delta\lambda_q} P_{in} e^{-\alpha L} r_{sb} \eta_D. \tag{9.10}$$

According to Eq.(9.5) and Eq.(9.6), the excess noise due to sideband photons is given by:

$$\xi_{sb} = m\eta_{Bob} \langle N_{SB} \rangle N_0. \tag{9.11}$$

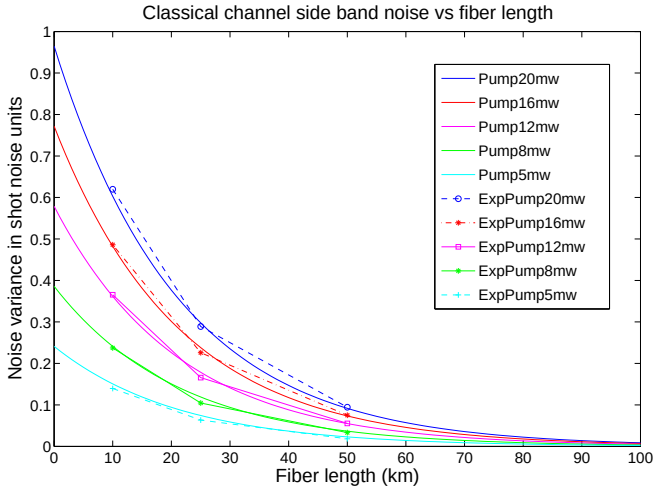


Fig. 9.5 Excess noise due to sideband photons versus fiber length, $\lambda_c = 1559.75$ nm, $\lambda_q = 1554.94$ nm, $r_{sb} = -61.62$ dB, $\eta_D = -1.9$ dB, $m = 1$.

In order to observe the excess noise due to sideband photons, we remove the MUX and increase the power of the classical channel, the experimental scheme can be refereed to Fig. 9.4 without using ADM1. The wavelength of classical channel is set to $\lambda_c = 1559.75nm$, while the quantum channel is $\lambda_q = 1554.94nm$. We vary the input power of classical channel (pump) from 20 mw to 5 mw for three fiber pool lengths: 10km, 25km and 50km. As shown in Fig.9.5, we observe that the sideband noises are much higher than SASRS noises. It is mainly due to the following reasons: (1) Sideband photons contribute in-band noise; (2) The input power is up to 20 mw which is relative high; (3) We remove the MUX in the experiment, thus there is no bandpass filtering on the sideband photons. In fact, as we shall see, if the MUX is added, the sideband noises can be reduced to a great extent thanks to the bandpass filtering property (or isolation) of the MUX. The theoretical predictions from Eq.(9.11) in Fig.9.5 also match well with the experimental data. If we moreover add the MUX, Eq.(9.11) can be re-written as:

$$\xi_{sb} = m r_{bp} \eta_{Bob} \langle N_{SB} \rangle N_0, \tag{9.12}$$

in which r_{bp} is the channel isolation of the MUX, a typical value for adjacent channel is about -30 dB. We can thus predict the expected excess noise due to sideband photons if MUX is used. For example, sideband photons from a 0 dBm channel adjacent to quantum channel would lead to an amount of excess noise about $1.6 * 10^{-4} N_0$ at 25 km. We can conclude that the excess noise due to the classical channel leakage is negligible in a coexistence regime of CV QKD and DWDM system.

9.2.3 Excess noise due to cross phase modulation

Cross phase modulation (XPM) is another nonlinear effect. The presence of a classical channel will change the nonlinear part of silica's refractive index sensed by the quantum channel. Due to this nonlinear refractive index of silica, a phase shift of the quantum channel that depends on the classical channel power will be introduced after propagating on a distance of fiber [18]. This nonlinear phenomenon is called XPM. In brief, XPM effect in WDM systems converts power fluctuations in a particular channel to phase fluctuations in the other channels. We can quantify these phase fluctuations. The refractive index has the form:

$$n = n_0 + n_2 \frac{P_{in}}{A_{eff}}, \tag{9.13}$$

in which n_0 is the ordinary refractive index of the optical fiber, n_2 is the intensity-dependent refractive index ($3 \times 10^{-23} m^2/mw$), A_{eff} is effective core area of fiber, P_{in} is the optical power in mw launched into the fiber at point A (Fig.9.1) and L_e is effective length defined by

$$L_e = \frac{1 - e^{-\alpha L}}{\alpha} \tag{9.14}$$

Here α is the fiber attenuation coefficient and L is the real fiber length. The optical power fluctuations change the refractive index (Eq.(9.13)) and the refractive index fluctuation changes the phase after propagation of the optical fiber. This part of phase variation is

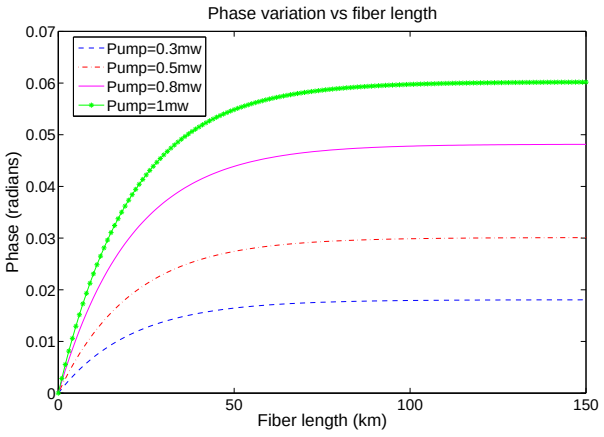


Fig. 9.6 Phase variation of XPM with different input power P_{in}, fiber attenuation coefficient α=0.21 dB/km, intensity-dependent refractive index, $n_2 = 3 \times 10^{-23} m^2/mw$, wavelength of pump λ_c=1559.75 nm, wavelength of LO λ_q=1554.94 nm, effective area of fiber A_{eff}=83μm^2, efficiency of DEMUX filter ξ=0.64.

given by [18], [19]:

$$\phi_0 = \frac{4\pi n_2 L_e P_{in}}{\lambda_c A_{eff}}, \tag{9.15}$$

in which, ϕ_0 is the phase variation in radians (in case P_{in} is constant) and λ_c is the wavelength of classical channel. In Fig.9.6, we can see that the phase variation will become higher when fiber length goes longer. But when the distance goes over 50 km, attenuation of the classical channels makes the phase drift variation saturate with distance. Clearly, any fluctuations in the optical power of the classical channel will produce corresponding phase changes in the quantum channel and can potentially impact the CV QKD system. The signal pulse and LO pulse propagate with classical channel through a same fiber. Due to optical power fluctuations and modulation of classical channel, XPM can induce phase variation both on the quantum signal and on the local oscillator. These variations can be different since LO and signal pulses are time-multiplexed, the phase between signal pulse and LO pulse can drift. The homodyne detection at Bob side in GMCS CV QKD protocol is very sensitive to such phase drift. The relation between phase drift and excess noise variance have been already estimated in [137]. Approximately, a phase drift ($\Delta\phi$) between LO and signal will introduce an amount of $V_A\Delta\phi^2$ excess noise, where V_A is Alice modulation variance. Considering pessimistic value (i.e.high) for the power fluctuations in classical channel (1% to 5% of input power) and since the phase variation is linear with input power (Eq. (9.15)), the statistical law followed by the power fluctuation will give us the phase noise variance. If we assume that the power fluctuations follow a centered Gaussian distribution of 0.05 mw power fluctuation (5% of 0 dBm classical channel power), XPM will introduce a maximum phase fluctuations variance of about $9 * 10^{-6}$ in squared radians. The phase noise variance on the relative phase between signal and LO will be in same order of magnitude as the phase fluctuations. If we moreover assume that Alice modulation variance is 20 shot noise units (SNU), a pessimistic estimate for the introduced excess noise ($V_A\Delta\phi^2$) will be around $1.8 * 10^{-4}$ in SNU. For one 0 dBm classical channel, a rough upper bound on the XPM excess noise will be lower than the noise introduced by Raman scattering.

9.3 Demonstration of coexistence of CV QKD with intense DWDM classical channels

9.3.1 Excess noise on CV QKD operated in DWDM coexistence regime: experimental set-up

To experimentally measure the excess noise induced by multiplexed DWDM channels, we have inserted a CV QKD system in a DWDM test-bed, and have used a dedicated scheme for excess noise acquisition, minimizing system noise associated to temporal drifts, so that DWDM-induced noise could be resolved with enough precision. We start by a description of our CV QKD set-up and then detail our acquisition scheme.

CV QKD experimental set-up

Our CV QKD system implements the GMCS Protocol [48] and uses a externally modulated DFB laser at 1531.12 nm to general pulses of temporal width 50ns at a repetition rate of 1MHz. These pulses are split on a 90/10 beam splitter into local oscillator and signal pulses. Signal pulses are strongly attenuated (to the level of a few photons per pulse) and their quadratures are Gaussian modulated using amplitude and phase modulators, with quadrature variance V_A. Local oscillator and signal are time multiplexed (200ns delay) and polarization multiplexed, before being sent to Bob through the fiber channel. At reception, on Bob side, signal and local oscillator pulses are polarization and time de-multiplexed. Detailed description of the setup is given in [64]. The quadrature information is retrieved by using a balanced homodyne detector of electronic noise -25dB below the shot noise. The intensity of the local oscillator is set in order to have a mean number of 10^8 photons per pulse at Bob. The input voltage range of the data acquisition card is set sufficiently low (± 1 Volts) to obtain a good resolution for the homodyne output measurement, which reduces the electronic noise down to 0.3% of shot noise. Such setting however could open a door for recently proposed saturation attack on CV QKD system (chapter 7) [140], but we will not be considering this issue, or other issue related to side-channel attacks here.

To perform shot noise measurement (Eq.(4.14)) Alice blocks the signal pulses at emission with her amplitude modulator while a second amplitude modulator, placed on the classical channel (in green on Fig.9.7) is used to block the optical input of the multiplexed classical channel. On the other hand, when both quantum and classical signals are multiplexed on the same fiber, we say that the "total noise" variance (Eq.(4.14)) is being measured. In order to limit the impact of statistical fluctuation in variance estimation [68], windows of size 10^8 pulses were used to estimate the quadrature measurement variances both for shot

noise and for total noise.

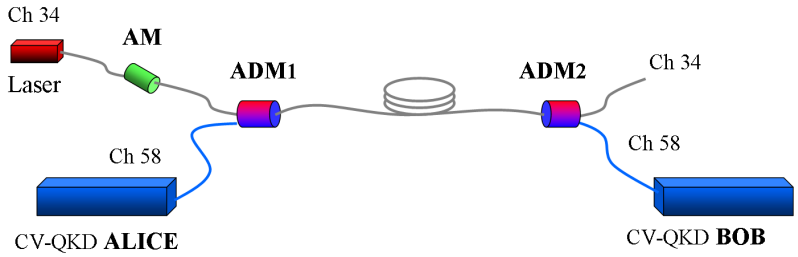
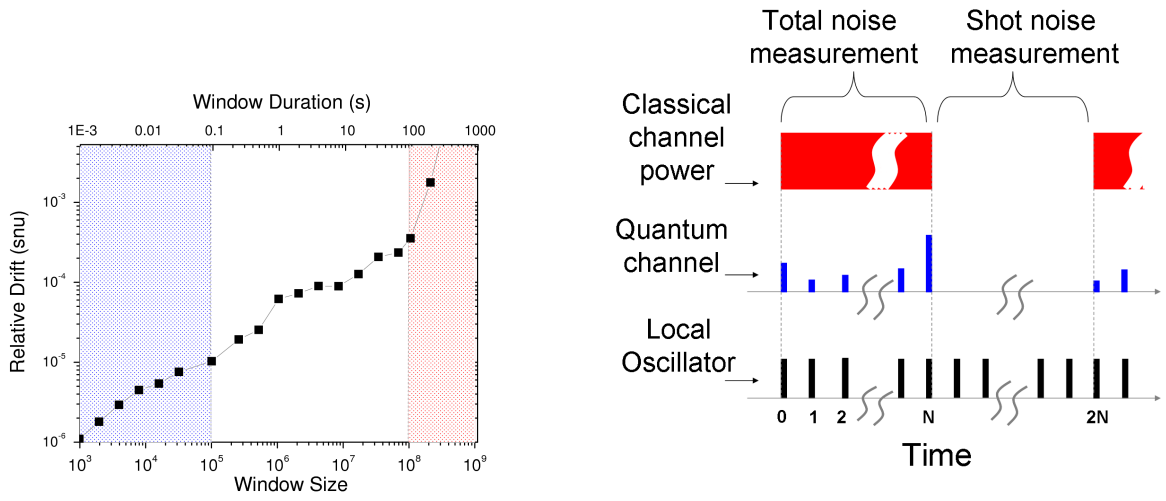


Fig. 9.7 Setup for excess noise measurement for CV QKD system operated in coexistence with one DWDM intense channel. Add-Drop Modules (ADM 1 and 2) are used to add and drop, respectively, the quantum channel to and from the optical fiber. Amplitude modulator (AM) is used to switch off the classical channel, while Alice output signal is synchronously blocked by the AM inside Alice CV-QKQ system. The figure represents the set-up with a forward propagating classical channel. When the classical channel is operated in backward configuration, the output of the AM is connected to the input of ADM2 (instead of the input of ADM1).

We have integrated the above described CV QKD setup into a DWDM environment and the experimental setup is depicted in Fig. 9.7. We have used a wavelength tunable continuous laser (model TLS-AG from Yenista) for the classical channel. The wavelength of the quantum channel is set at 1531.12 nm (ITU channel 58) so that the quantum channel would be in the Anti-Stockes configuration with respect to any classical channel in the C band [17]. The wavelength of the classical channel is set at 1550.12 nm (ITU channel 34) based on the choice of available ADMs in the laboratory. It would be possible to select a quantum channel wavelength close to the classical channel, as illustrated in [30], in order to further minimize the Raman induced noise. Both channels are multiplexed and de-multiplexed to and from the optical fiber spool by means of ADMs. An additional bandpass filter (not shown in Fig. 9.7) had also placed (before the ADM) on the classical channel in order to remove sidebands (such filtering would naturally be present if a multi-channel MUX had been used, as shown in Fig.9.1).

In our derivation of the secret key rate, we have opted for a conservative approach and have considered that the losses associated to the ADMs are part of the fiber channel and not of the QKD system. This approach is conservative because it does not require to assume that the ADMs insertion loss are calibrated (and this calibration trusted). Moreover, this approach allows to directly take into account possible variations of the insertion loss of the ADMs, due to wavelength drift of the CV QKD laser around the transmission window of the ADMs, in the estimation of channel transmittance T (Eq.(4.13)).



(a) (b)

Fig. 9.8 **(a)**: Drift of homodyne output. Relative drift between shot noise variance measurements in consecutive blocks, as a function of data window size. Data window size ranging from 1ms to 200s have been used (corresponding to window size ranging from 10^3 to 2×10^8 homodyne measurements). At short time scales (below 10^5 measurements) the relative drift is negligible (region shaded in blue), while it becomes comparable to the system noise ($10^{-3}N_0$ for time scales of several seconds (regions shaded in red). **(b)**: Timing diagram. Data acquisition is divided in relatively short periods (N =10^5 pulses, corresponding to 100 ms). Shot noise and total noise measurements are performed alternatively on each consecutive period, in order to limit the relative drift.

Excess noise measurement and drift compensation

To evaluate the excess noise with a good statistical precision large data blocks should be used. This is indeed an important issue when one wants to deal properly with finite-size issues [68]. In our case, we should typically compute estimators on data blocks of size 10^8 in order to have a statistical fluctuations around $10^{-4}N_0$ and thus below system excess noise. However, the value of homodyne output can drift with time (essentially due to temperature fluctuations that modify the balancing conditions of the homodyne detection). This temporal drift results in an additional noise that depends on data block size, as one estimates shot noise and total noise on two consecutive data blocks, as we can see from Fig.9.8(a). If large window size (200s) were used to measure consecutively total noise and shot noise, then the drift could generate an additional noise of the order of $1.5 \times 10^{-3}N_0$ and thus strongly affect the precision of our DWDM-induced noise measurements.

One way to mitigate this effect is on the other hand to use smaller data blocks so that the

noise induced by the relative drift becomes negligible at this timescale. Using this principle, we have used data blocks of size 10^5 pulses (100ms) alternatively for the acquisition shot noise and total signal measurements. Excess noise estimation on data blocks of 10^8 acquisition is then obtained by concatenating 10^3 data blocks obtained at the 100 ms timescale, reducing the relative statistical uncertainty.

To perform shot noise measurement in our set-up, the emission of Alice and the emission of the laser source on the classical channel were shut down simultaneously during 100ms with respective amplitude modulators, as depicted on Fig. 9.8(b). The relative drift at the 100ms timescale is around $10^{-5}N_0$ (measured at Bob), can be neglected since it is significantly smaller than the CV QKD system excess noise ($10^{-3}N_0$ in our case, at Bob).

As proposed in [66], it is possible to use another scheme in order to perform time-resolved shot noise measurements: it consists in using an amplitude modulator located at the entrance of Bob to modulate η_B, and to use Eq.(4.12) (for different value of η_B) to evaluate both shot noise and excess noise variance. This approach is feasible but would interfere with some routines already implemented in our CV QKD implementation, related to Alice-Bob data synchronization and phase tracking. We have therefore not opted for this design in our DWDM test-bed but plan to do so it in future field trials.

9.3.2 CV QKD experimental coexistence tests: results and analysis

We have operated our experimental test-bed of CV QKD multiplexed with one DWDM classical channel (described in the previous section), at 25km, 50km and 75km with a classical channel power after the ADM varied from 0mW to 8mW. For each experimental run, transmission T and excess noise ξ were evaluated from the experimental data, using the Eq.(4.11,4.12,4.13,4.14).

The measured excess noise at the output of Alice as a function of classical power are displayed in Fig.9.9. We compare these experimental values to the expected excess noise, i.e. the sum of the system excess noise (that is calibrated to be $0.03N_0$ in our case, at Alice) with the noise associated to spontaneous Raman emission, that can be computed from Eq.(9.6) and Eq.(9.8). We in particular expect the excess noise to be a linear function of the launch power.

We also position the null key thresholds on Fig.9.9, i.e. the maximum excess noise that can be tolerated in order to be able to obtain a positive secret key rate. Assuming collective attacks and 0.95 reconciliation efficiency, the null key threshold for 25km is $0.137N_0$, $0.083N_0$ for 50km and $0.064N_0$ for 75km.

It can thus be seen that a positive key rate can be obtained for classical channel power up to 14mW at 25km, 3.7mW at 50km and 0.89mW at 75km in forward configuration whereas

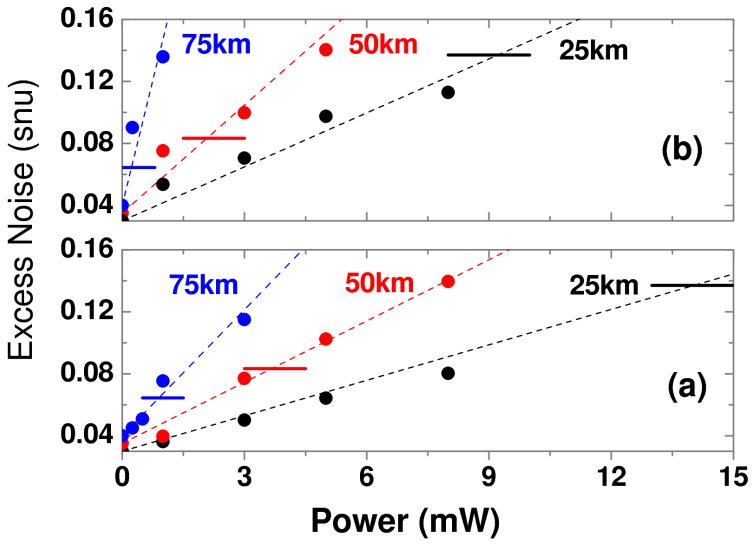


Fig. 9.9 Excess noise measurements in forward (a) and backward (b) channel configuration. Black, red and blue data points are the excess noise evaluated at Alice for channel length of 25km, 50km and 75km, for different classical channel power. Dashed lines indicate the expected excess noise curve and solid horizontal lines are null key threshold for respective channel distance. See text for details.

in backward direction admissible classical power drops to 9.3mW, 2mW and 0.23mW, respectively. The secure key rate (under collective attacks) has been calculated from the evaluated excess noise ξ and transmission T taking into account finite-size effects with our data block size of 10^8. Worst-case estimators for the excess noise (with 3 sigma of deviation) have be used, following the analysis [68]. With single 0dBm channel at distance 25km, the key rate is 24.11kb/s in forward and 22.98kb/s in backward direction. In 50km channel length the key rate drops to 3.16kb/s and 2.27kb/s, respectively. We have also obtained a positive key rate of 0.49kb/s at 75km by reducing the classical channel power (while considering classical channel receiver sensitivity below -25dBm) to -3dBm in forward and -9dBm in backward direction. One important thing to point at here is the yield (secure key bit per QKD signal pulse) of CV QKD system in WDM environment. In our experiment with 0dBm classical channel over 25km the yield is of 485×10^{-4} bits/pulse which is two order of magnitude higher than the recently reported, 485×10^{-6} bits/pulse, DV-QKD experiment [130]. On the other hand, the latest DV-QKD system can be operated at GHz-clock rate, which has still not yet been demonstrated with CV QKD systems, currently operated at MHz clock rate, even though no fundamental barrier prevents to upgrade it to 100 MHz if not GHz clock rate.

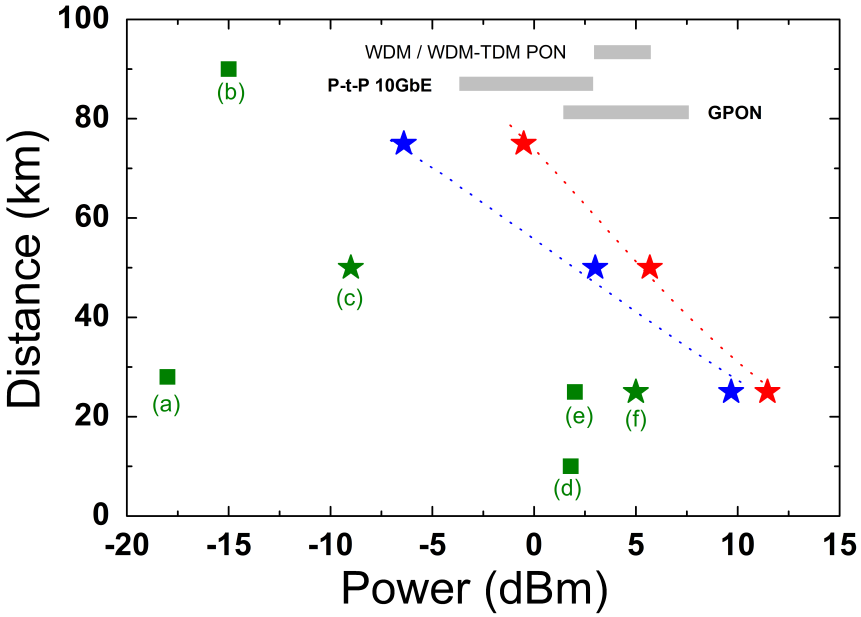


Fig. 9.10 Tolerable classical channel power vs Reachable distance: Performance of QKD in the context of coexistence with classical optical channels. Red and blue colors represents our results with a CV QKD system, in forward and backward classical channel configuration, while previous works with DV-QKD systems are in Green: (a) Townsend [173], (b) Patel et al. [129], (c) Eraerds et al. [30], (d) Choi et al. [17], (e) Chapuran et al. [15], (f) Patel et al. [130]. Stars: experiments conducted in the C-band (DWDM). Squares: experiments conducted in CWDM. The doted red and blue lines are the forward and backward simulation curve for the null key rate in the current experiment. Gray bands show transmitter input power range in different standardized optical networks.

Comparison with DV QKD

To illustrate the strong DWDM coexistence capacity of CV QKD, we have made a comparative study with previously reported DV-QKD experiments [15, 17, 30, 129, 130, 173], and displayed in Fig.9.10 a comparison of the reachable distance of QKD, as a function of the classical multiplexed power (in CWDM or DWDM, see caption). In Fig.9.10, the data points for CV QKD indicate the maximum reachable distance (null key threshold). The key rates corresponding to experimental points taken with our CV QKD system and displayed on Fig.9.10 are: 12b/s for 25km; 8b/s for 50km and 9b/s for 75km. Note that DV QKD performances mentioned in Fig.9.10 have also been acquired very close to the null key threshold. One important thing to note that the different results mentioned in this comparison do not all rely on a unified security analysis. Key rates are derived for security proofs valid against collective attacks in [17, 30, 130], individual attacks in [173] and general attacks in[129], while among these references, only [130] takes finite-size effects into account. As previ-

ously explained, we have considered collective attacks and have taken finite-key effects into account for the CV QKD secure key derivations associated to our experiments.

It can be seen that CV QKD can reach longer transmission distances for a given classical channel launch power. Conversely, for a given transmission distance, CV QKD can tolerate noise from multiple classical channels with typical transmission power of 0dBm. This is particularly true for 25km and 50km transmission distance as shown in Fig.9.10. CV QKD can also be deployed in coexistence with classical channels of unprecedent power levels-thanks to the mode selection property of its coherent detection. This gives CV QKD an advantage for the integration into different optical network architectures and in particular into access networks. Such integration requires, in general, capacity for QKD to co-exist with classical channels of several dBm of power. As it can be seen in Fig. 9.10, strong co-existence of CV QKD would allow its integration into different standard passive optical networks such as, for example, Gigabit PON, 10G-PON and WDM/TDM PON [7].

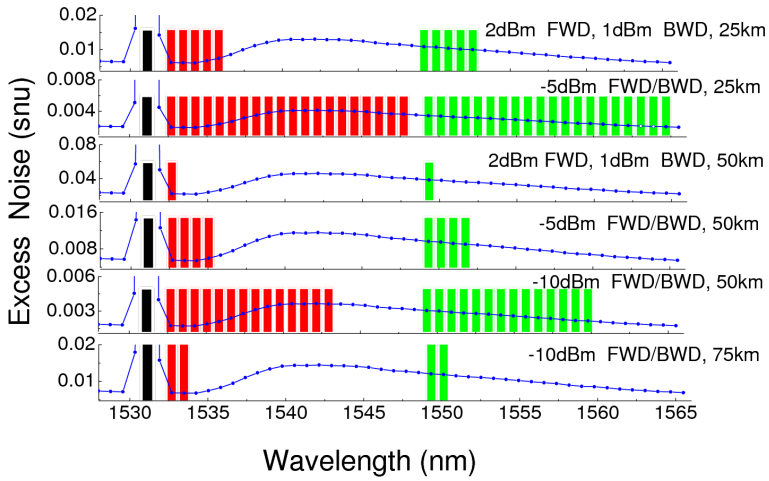


Fig. 9.11 Optimized classical channel allocation for CV QKD in WDM-PON network. In Black: the 1531.12 nm channel allocated for the quantum channel. Red and Green bars represents the backward and forward classical channels, positioned on the DWDM wavelength grid. Each blue dot (connected by the blue line) represents the simulated value of the Raman-induced excess noise arising from one backward (of specified power) classical channel onto the quantum channel. Simulated data for excess noise from forward channels is not shown.

Optimization of classical channel allocation

In the light of the experimental results and the promising perspective defined for CV QKD integration in optical networks, we have simulated how we could effectively integrate CV QKD in some WDM Passive Optical Network architectures (WDM-PON). To this effect, we have applied a simple optimization routine to the integration of CV QKD system into WDM-PON, that allowed us to propose classical channel allocations by minimizing the excess noise induced on CV QKD.

For a typical access network distance of 25km, we have considered classical channel allocation in the C band and found that CV QKD could coexist with 5 pairs of classical channels (with nominal WDM-PON channel launch power: 2dBm in forward and 1dBm backward). Optimization(at a give transmission distance) is performed by choosing sequentially the position of the classical channel that maximize the additional excess noise on QKD, up to the maximum number of channels compatible with a positive secret key rate.

If the detector sensitivity on the classical channels allows, it might even be realistic to reduce the classical channel power below the nominal specifications of a WDM-PON network, while still being able to operate the classical channels. We have studied the impact of this hypothesis in Fig.9.11. We can see for example that 14 pairs of channels (each with -10dBm launch power) could be multiplexed with one CV QKD channel at 50km and while 2 pairs of channels (also with -10dBm launch power) could coexist with CV QKD at 75km. These simulation results clearly indicate that the strong coexistence capacity of CV QKD with WDM multiplexed classical channels is likely to play an important role in the integration of QKD into optical networks.

9.3.3 Conclusion

The success of emerging optical network technologies relies for a large part on their ability to be seamlessly integrated into existing infrastructures. We have demonstrated the successful co-existence capability of CV QKD intense (around 0 dBm) classical channels, in a DWDM configuration. We have characterized and studied the influence of the main source of noise: Raman scattering and have demonstrated experimentally that CV QKD can coexist with a DWDM channel intensity as high as 11.5dBm, while positive key rate could also be obtained with a -3dBm forward DWDM multiplexed classical channel at 75km.

It can be also seen that CV QKD, benefiting from a built-in single mode filtering (associated with the coherent detection) is less affected by DWDM-induced noise photons that the DV QKD systems tested so far in this regime, and can therefore reach longer transmission distances for a given DWDM classical channel launch power.

These experimental results indicate that CV QKD, and more generally coherent communications operated at the shot noise limit are a promising technology in order to jointly operated quantum and classical communications on the same optical fiber network, and can therefore play an important role for the development of quantum communications over existing optical networks.

Chapter 10

Conclusion and Perspectives

In this thesis, I have mainly studied the practical security of continuous variable quantum key distribution system from both theoretical and experimental sides. At the beginning and during the time of this thesis, there are some important achievements that have been made in CV QKD: on the theoretical side, security proofs against general attack in asymptomatic region [147] and finite size region [92] have been gradually established. Composable security for CV QKD with Gaussian-modulated coherent states [86] has been also analyzed. On the experimental side, CV QKD in standard telecom fiber systems over 80 km [68] and secret key rate over 1 Mbps [55] have been demonstrated in lab environment. All these results have reduced the gap between the discrete variable and continuous variable QKD protocols. These achievements also indicate that CV QKD is forwarding towards the next stage: practical use in real world and commercial products [5], which rise the importance of practical study in CV QKD. In this thesis, I have concentrated my work on two important challenges in practical study of CV QKD: side channel attacks on practical CV QKD systems and the integration of a CV QKD system within an optical network.

10.1 Side channel attacks in CV QKD

In the study of side channel attack, for the first time I have proposed and studied a detector-based side channel attack in CV QKD: saturation attack, which opens a new type of loophole in all implementations of CV QKD systems using homodyne detection. This new loophole has no connection with the well known vulnerability of local oscillator pulses in the implementation of CV QKD, which thus requires new types of countermeasures. We have moreover performed an experimental demonstration of saturation attack, in which we have experimentally studied the condition under which a successful saturation attack can be realized with our experimental setup of Eve.

Saturation attack highlights the importance of exploring the assumptions in security proofs when implementing CV QKD protocol on practical setups. The discover of the saturation attack has changed the stereotype that the detection part in CV QKD is robust against side channel attacks, and our attack would be a great motivation for developing practical Measurement-Device-Independent (MDI) CV QKD [94, 95, 113, 135, 193]. In DV QKD, many quantum hacking strategies targeting on single photon detectors have been already demonstrated experimentally on research and commercial systems [42, 42, 107, 116, 137, 190, 194], which is one of the most important reasons for the birth of MDI QKD.

Beside its network configuration, the main advantage of MDI QKD is to defeat detector based side channel attack, thus our saturation attack, a detector-based side channel attack, for sure will push forward the study of MDI CV QKD. Indeed, MDI CV QKD protocols [94, 95, 113, 193] have been proposed not very late after the saturation attack and recently proof of principle demonstration has also been performed [135]. However, MDI CV QKD protocols still face challenges or even limitations from the points of the views of theories and practical implementations [31]. For examples, the performance of MDI CV QKD largely depends on the efficiency of homodyne detector, it requires almost one unity efficiency (98% in the analysis of [135], however this value is unrealistic) to achieve a significant key rate when loss is encountered. The implementation of local oscillator in MDI CV QKD also faces the challenge that an eavesdropper can manipulate the local oscillator in a untrusted relay. Possible solutions have been proposed by [136], however most of technical issues of these solutions have not yet been solved (and will not be solved very soon), which means it still needs much more efforts to implement a practical MDI CV QKD.

On the other hand, in order to defeat side channel attacks in CV QKD and improve the participial security of CV QKD, other than developing device independent QKD, we can pursue another approach: address as many as vulnerabilities in implementations of CV QKD systems, and develop corresponding countermeasures. As we have presented in chapter 6, we have reviewed side channel attacks in CV QKD which are recently reported. Along with our saturation attack, the main targets of side channel attack in CV QKD can be summarized as: local oscillator, homodyne detection and source preparation, in which the first two targets seem to have important impacts on the practical security of CV QKD, where suitable countermeasures are needed. However these known side channel attacks are not end of story, since current security proofs have not include the side channel attacks, any implementation flaws can still open new security loopholes in CV QKD. By discovering more loopholes in the implementations of CV QKD and performing systematic tests of different side channel attacks, we can eventually move towards the certification of CV QKD. Such action is actually undergoing in DV QKD [176], while CV QKD still has a long way

to go.

10.2 Integration of CV QKD within optical networks

In the study of integration of a CV QKD system within an optical network, we have demonstrated the successful co-existence capability of CV QKD intense (around 0 dBm) classical channels, in a DWDM configuration. We have characterized and studied the influence of the main source of noise: Raman scattering and have demonstrated experimentally that CV QKD can coexist with a DWDM channel with high intensity. It can be also seen that CV QKD, benefiting from a built-in single mode filtering (associated with the coherent detection) is less affected by DWDM-induced noise photons that the DV QKD systems tested so far in this regime, and can therefore reach longer transmission distances for a given DWDM classical channel launch power. These experimental results indicate that CV QKD, and more generally coherent communications operated at the shot noise limit are a promising technology in order to jointly operated quantum and classical communications on the same optical fiber network, and can therefore play an important role for the development of quantum communications over existing optical networks.

Our work is the first experimental confirmation that CV QKD has good compatibility with intense classical signal under a DWDM environment, however our demonstration was performed under a lab environment, where there is no real traffic on classical channels. Thus it will be interesting to insert a CV QKD system into a real optical network to test the performance of CV QKD where real modulated classical signals co-exist with quantum signals. At the end of the chapter 9, we have proposed the optimization of classical channel allocation for a real optical network specification. Under a real field test of CV QKD system co-existing with real classical signals in a optical network, CV QKD system could suffer much more critical conditions compared to the test in a lab environment, not only the classical signal, but also the environment such as temperature, humidity, physical variation could also impact the performance and stability of the CV QKD system. It is very important to verify that CV QKD can be performed under all these realistic conditions, while in DV QKD, several field tests have been already performed [153, 177].

If we would like to further improve the compatibility of CV QKD with classical channels in terms of key distribution distance and key rate, we need eventually to improve the performance of CV QKD. There are still large spaces to improve CV QKD performance from both quantum communication and post processing parts. In the quantum communication parts, high clock rate and high bandwidth homodyne detection can largely improve the secret key rate. Recent demonstration has shown that CV QKD system can generate 1

Mbps secret key rate [55]. Although homodyne detection is a mature technology in classical optical communication, it is still challenge to achieve the features of homodyne detection that are favorable to CV QKD, such as high bandwidth, high efficiency and low electronic noise. In the post processing part, error correction code with small signal noise ratio [63] has been already been proposed for long distance key distribution [68]. Recently high speed reconciliation algorithm has been proposed [69] to allow extract more than 1 bit of secret key per channel use. CV QKD with high key rate output could be a future direction, since CV QKD usually outperforms DV QKD in secret key rate at short distance, however the performance of CV QKD is sensitive to transmission loss.

Appendix A

Calculation details in saturation attack

A.1 Calculation of the correlation under the saturation attack

In order to clearly show the calculation, we consider y_{sat}, y, x and z as the notations of $X_{B_{sat}}$, $X_{B_{lin}}$, X_A and X_N respectively. We use $X_{B_{sat}}$ (Eq.(7.8)) to calculate the correlation $Cov(X_A, X_{B_{sat}})$ under the saturation attack. We assume here $\alpha >> 1$ and consider $\Delta \geq 0$, while the analysis of $\Delta \leq 0$ is similar. The saturation model can be considered as:

$$\begin{aligned} y_{sat} &= \alpha, && t\frac{g}{\sqrt{2}}x+z+\Delta \geqslant \alpha \\ y_{sat} &= t\frac{g}{\sqrt{2}}x+z+\Delta, && |\, t\frac{g}{\sqrt{2}}x+z+\Delta \,| < \alpha (\alpha >> 1, \Delta \geq 0) \\ y_{sat} &= -\alpha, && t\frac{g}{\sqrt{2}}x+z+\Delta \leqslant -\alpha \end{aligned} \tag{A.1}$$

$x \sim \mathcal{N}(0, \sigma_x^2)$ and $z \sim \mathcal{N}(0, \sigma_z^2)$ are both centered Gaussian variables with probability density function $p_X(x)$ and $p_Z(z)$, respectively:

$$p_X(x) = \frac{e^{-\frac{x^2}{2\sigma_x^2}}}{\sqrt{2\pi}\sigma_x}, \qquad p_Z(z) = \frac{e^{-\frac{z^2}{2\sigma_z^2}}}{\sqrt{2\pi}\sigma_z}. \tag{A.2}$$

In which $\sigma_x^2 = Var(X_A)$ and $\sigma_z^2 = N_0 + \eta T \xi + v_{\text{ele}}$. By knowing $p_X(x)$ and $p_Z(z)$, we can calculate $Cov(x, y_{sat})$ with double integral of x and z in the domain D_{xz}. D_{xz} is defined in Eq.(A.1): $-\alpha < \frac{tg}{\sqrt{2}}x+z+\Delta < \alpha$, $\frac{tg}{\sqrt{2}}x+z+\Delta \leq -\alpha$ and $\frac{tg}{\sqrt{2}}x+z+\Delta \geq \alpha$. A long but

straight forward calculation of $Cov(x, y_{sat})$ is presented as follows:

$$
\begin{aligned}
Cov(X_A, X_{B_{sat}}) &= \langle xy_{sat}\rangle - \langle x\rangle\langle y_{sat}\rangle = \langle xy_{sat}\rangle \\
&= \iint\limits_{D_{xz}} xyp_X(x)p_Z(z)dxdz = \iint\limits_{-\alpha<\frac{tg}{\sqrt{2}}x+z+\Delta<\alpha} (\frac{tg}{\sqrt{2}}x^2 + x\Delta + xz)p_X(x)p_Z(z)dxdz + \\
&\iint\limits_{\frac{tg}{\sqrt{2}}x+z+\Delta\leq-\alpha} -\alpha x p_X(x)p_Z(z)dxdz + \iint\limits_{\frac{tg}{\sqrt{2}}x+z+\Delta\geq\alpha} \alpha x p_X(x)p_Z(z)dxdz \\
&= \frac{1}{2\pi\sigma_x\sigma_z}\int\limits_{-\infty}^{\infty}(\frac{tg}{\sqrt{2}}x^2 + x\Delta)e^{-\frac{x^2}{\sigma_x^2}}dx \int\limits_{-\alpha-\Delta-\frac{tg}{\sqrt{2}}x}^{\alpha-\Delta-\frac{tg}{\sqrt{2}}x} e^{-\frac{z^2}{2\sigma_z^2}}dz \\
&= \frac{1}{2\pi\sigma_x\sigma_z}\int\limits_{-\infty}^{\infty}(\frac{tg}{\sqrt{2}}x^2 + x\Delta)e^{-\frac{x^2}{\sigma_x^2}}\sqrt{\frac{\pi}{2}}\sigma_z[\mathrm{erf}(\frac{\alpha+\Delta+\frac{tg}{\sqrt{2}}x}{\sqrt{2}\sigma_z}) + \mathrm{erf}(\frac{\alpha-\Delta-\frac{tg}{\sqrt{2}}x}{\sqrt{2}\sigma_z})]dx \\
&= \frac{1}{2\pi\sigma_x}\sqrt{\frac{\pi}{2}}[\frac{tg}{\sqrt{2}}\int\limits_{-\infty}^{\infty}x^2e^{-\frac{x^2}{2\sigma_x^2}}dx + \Delta\int\limits_{-\infty}^{\infty}\mathrm{erf}(\frac{\alpha-\Delta-\frac{tg}{\sqrt{2}}x}{\sqrt{2}\sigma_z})xe^{-\frac{x^2}{2\sigma_x}}dx] \\
&= \frac{tg}{2\sqrt{2}\pi\sigma_x}\sqrt{\frac{\pi}{2}}\sqrt{2\pi}\sigma_x^3 + \frac{tg}{2\sqrt{2}\pi\sigma_x}\sqrt{\frac{\pi}{2}}\sqrt{2\pi}\sigma_x^3\mathrm{erf}(\frac{\alpha-\Delta}{\sqrt{2(\sigma_z^2+\frac{t^2g^2}{2}\sigma_x^2)}}) \\
&= \frac{tg}{2\sqrt{2}}\sigma_x^2[1+\mathrm{erf}(\frac{\alpha-\Delta}{\sqrt{2(\sigma_z^2+\frac{t^2g^2}{2}\sigma_x^2)}})] = \frac{tg}{2\sqrt{2}}\langle X_A^2\rangle[1+\mathrm{erf}(\frac{\alpha-\Delta}{\sqrt{2Var(X_{B_{lin}})}})].
\end{aligned}
\tag{A.3}
$$

In which, the error function $\mathrm{erf}(x)$ is defined as:

$$
\mathrm{erf}(x) = \frac{2}{\sqrt{\pi}}\int_0^x e^{-t^2}dt. \tag{A.4}
$$

And we have used the integral formulas of $\mathrm{erf}(x)$ provided in [125]. In Eq.(A.3), $Var(X_{B_{lin}}) = \sigma_z^2 + \frac{t^2g^2}{2}\sigma_x^2$ is variance of Bob with no saturation. In this calculation, the integrals of the odd functions with symmetric bounds $(-\infty, \infty)$ are equal to zero.

A.2 Calculation of the variance of Bob under the saturation attack

In order to calculate the variance of Bob under the saturation attack, we use the step function $\theta(x)$ which is defined as:

$$\theta(x) = \begin{cases} 1, x \in [0, \infty) \\ 0, x \in (-\infty, 0] \end{cases} \tag{A.5}$$

With Eq.(A.5) we can transform Eq.(A.1) into:

$$\begin{aligned} y_{sat} &= y\theta(y+\Delta+\alpha)\theta(-y-\Delta+\alpha) + \alpha[1-\theta(y+\Delta+\alpha)\theta(-y-\Delta+\alpha)] \\ &\approx \alpha + (y+\Delta-\alpha)\theta(-y-\Delta+\alpha) = \alpha + (y-\varepsilon)\theta(-y+\varepsilon). \end{aligned} \tag{A.6}$$

in which:

$$\varepsilon = \alpha - \Delta(\alpha > 0, \Delta \geq 0), \tag{A.7}$$

$$y = t\frac{g}{\sqrt{2}}x + z. \tag{A.8}$$

Since x and z are both Gaussian variables, y is also a Gaussian variable ($y \sim \mathcal{N}(0, \sigma_y^2)$), with its probability function $p_Y(y) = \frac{e^{-\frac{y^2}{2\sigma_y^2}}}{\sqrt{2\pi}\sigma_y}$ and $\sigma_y^2 = Var(X_{B_{lin}})$ is the variance of Bob under linear detection. In order to estimate $Var(X_{B_{sat}}) = Var(y_{sat}) = \langle y_{sat}^2 \rangle - \langle y_{sat} \rangle^2$, we need to calculate $\langle y_{sat} \rangle$ and $\langle y_{sat}^2 \rangle$, respectively:

$$\langle y_{sat} \rangle = \alpha + \langle (y-\varepsilon)\theta(-y+\varepsilon) \rangle = \alpha + C, \tag{A.9}$$

$$\langle y_{sat}^2 \rangle = \langle \alpha^2 + 2\alpha(y-\varepsilon)\theta(-y+\varepsilon) + (y-\varepsilon)^2\theta(-y+\varepsilon) \rangle \tag{A.10}$$

$$= \alpha^2 + 2\alpha C + D. \tag{A.11}$$

In which C and D are equal to $\langle (y-\varepsilon)\theta(-y+\varepsilon) \rangle$ and $\langle (y-\varepsilon)^2\theta(-y+\varepsilon) \rangle$, and can be

calculated as follows:

$$C = \int_{-\infty}^{\infty} p_Y(y)(y-\varepsilon)\theta(-y+\varepsilon)dy = \int_{-\infty}^{\infty} p_Y(y'+\varepsilon)y'\theta(-y')dy' = \int_{-\infty}^{0} p_Y(y'+\varepsilon)y'dy' \tag{A.12}$$

$$= -[\frac{\sigma_y}{\sqrt{2\pi}}e^{-\frac{\varepsilon^2}{2\sigma_y^2}} + \frac{\varepsilon}{2} + \frac{\varepsilon}{2}\text{erf}(\frac{\varepsilon}{\sqrt{2}\sigma_y})], \tag{A.13}$$

$$D = \langle (y-\varepsilon)^2\theta(-y+\varepsilon)\rangle = \int_{-\infty}^{\infty} p_Y(y)(y-\varepsilon)^2\theta(-y+\varepsilon)dy \tag{A.14}$$

$$= \int_{-\infty}^{\infty} p_Y(y'+\varepsilon)y'^2\theta(-y')dy' = \int_{-\infty}^{0} p_Y(y'+\varepsilon)y'^2dy' \tag{A.15}$$

$$= \frac{\varepsilon\sigma_y}{\sqrt{2\pi}}e^{-\frac{\varepsilon^2}{2\sigma_y^2}} + \frac{\varepsilon^2+\sigma_y^2}{2}[1+\text{erf}(\frac{\varepsilon}{\sqrt{2}\sigma_y})]. \tag{A.16}$$

We have used $y' = y - \varepsilon$ in the calculations of C and D. Provided with C and D, we can calculate $Var(y_{sat})$:

$$\begin{aligned} Var(y_{sat}) &= \langle y_{sat}^2\rangle - \langle y_{sat}\rangle^2 = \alpha^2 + 2\alpha C + D - (\alpha+C)^2 = D - C^2 \\ &= \sigma_y^2[\frac{1+\text{erf}(\frac{\varepsilon}{\sqrt{2}\sigma_y})}{2} - \frac{e^{-\frac{\varepsilon^2}{\sigma_y^2}}}{2\pi}] - \frac{\varepsilon\sigma_y}{\sqrt{2\pi}}\text{erf}(\frac{\varepsilon}{\sqrt{2}\sigma_y})e^{-\frac{\varepsilon^2}{2\sigma_y^2}} + \frac{\varepsilon^2}{4}[1-\text{erf}^2(\frac{\varepsilon}{\sqrt{2}\sigma_y})] \\ &= Var(X_{B_{lin}})(\frac{1+A}{2} - \frac{B^2}{2\pi}) - (\alpha-\Delta)\sqrt{\frac{Var(X_{B_{lin}})}{2\pi}}A*B + \frac{(\alpha-\Delta)^2}{4}(1-A^2) \end{aligned} \tag{A.17}$$

in which:

$$A = \text{erf}(\frac{\alpha-\Delta}{\sqrt{2Var(X_{B_{lin}})}}), B = e^{-\frac{(\alpha-\Delta)^2}{2Var(X_{B_{lin}})}} \tag{A.18}$$

References

[1] Austrian Institute of Technology. https://sqt.ait.ac.at/software/. URL https://sqt.ait.ac.at/software/.

[2] Anhui Quantum Communication Technology Co., Ltd. http://www.quantum-info.com/en.php. URL http://www.quantum-info.com/en.php.

[3] ID Quantique. http://www.idquantique.com. URL http://www.idquantique.com.

[4] Quintessence Labs. http://www.quintessencelabs.com/. URL http://www.quintessencelabs.com/.

[5] SeQureNet. http://www.sequrenet.com/. URL http://www.sequrenet.com/.

[6] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.*, 98:230501, Jun 2007. doi: 10.1103/PhysRevLett.98.230501. URL http://link.aps.org/doi/10.1103/PhysRevLett.98.230501.

[7] S. Aleksic, D. Winkler, G. Franzl, A. Poppe, B. Schrenk, and F. Hipp. Quantum key distribution over optical access networks. In *Network and Optical Communications (NOC), 2013 18th European Conference on and Optical Cabling and Infrastructure (OC&i), 2013 8th Conference on*, pages 11–18, 2013.

[8] R. Alléaume, C. Branciard, J. Bouda, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, N. Lütkenhaus, C. Monyk, P. Painchault, M. Peev, A. Poppe, T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfurter, and A. Zeilinger. Using quantum key distribution for cryptographic purposes: A survey. *Theoretical Computer Science*, 560, Part 1(0): 62 – 81, 2014. ISSN 0304-3975. doi: http://dx.doi.org/10.1016/j.tcs.2014.09.018. URL http://www.sciencedirect.com/science/article/pii/S0304397514006963. Theoretical Aspects of Quantum Cryptography - celebrating 30 years of BB84.

[9] Michael Ben-Or, Michał Horodecki, DebbieW. Leung, Dominic Mayers, and Jonathan Oppenheim. The universal composable security of quantum key distribution. In Joe Kilian, editor, *Lecture Notes in Computer Science*, volume 3378, pages 386–406–. Springer Berlin Heidelberg, 2005. URL http://dx.doi.org/10.1007/978-3-540-30576-7_21.

[10] Charles Bennett, Gilles Brassard, and N. Mermin. Quantum cryptography without bell's theorem. *Phys. Rev. Lett.*, 68:557–559, Feb 1992. doi: 10.1103/PhysRevLett.68.557. URL http://link.aps.org/doi/10.1103/PhysRevLett.68.557.

[11] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings IEEE International Conference on Computers, Systems and Signal Proceedings*, number 0, pages 175–179, 1984.

[12] Rémi Blandino, Anthony Leverrier, Marco Barbieri, Jean Etesse, Philippe Grangier, and Rosa Tualle-Brouri. Improving the maximum transmission distance of continuous-variable quantum key distribution using a noiseless amplifier. *Phys. Rev. A*, 86:012327, Jul 2012. doi: 10.1103/PhysRevA.86.012327. URL http://link.aps.org/doi/10.1103/PhysRevA.86.012327.

[13] Audun Nystad Bugge, Sebastien Sauge, Aina Mardhiyah M. Ghazali, Johannes Skaar, Lars Lydersen, and Vadim Makarov. Laser damage helps the eavesdropper in quantum cryptography. *Phys. Rev. Lett.*, 112:070503, Feb 2014. doi: 10.1103/PhysRevLett.112.070503. URL http://link.aps.org/doi/10.1103/PhysRevLett.112.070503.

[14] N. J. Cerf, M. Lévy, and G. Van Assche. Quantum distribution of gaussian keys using squeezed states. *Phys. Rev. A*, 63:052311, Apr 2001. doi: 10.1103/PhysRevA.63.052311. URL http://link.aps.org/doi/10.1103/PhysRevA.63.052311.

[15] T E Chapuran, P Toliver, N A Peters, J Jackel, M S Goodman, R J Runser, S R McNown, N Dallmann, R J Hughes, K P McCabe, J E Nordholt, C G Peterson, K T Tyagi, L Mercer, and H Dardy. Optical networking for quantum key distribution and quantum communications. *New Journal of Physics*, 11(10):105001–, 2009. ISSN 1367-2630. URL http://stacks.iop.org/1367-2630/11/i=10/a=105001.

[16] Yue-Meng Chi, Bing Qi, Wen Zhu, Li Qian, Hoi-Kwong Lo, Sun-Hyun Youn, A I Lvovsky, and Liang Tian. A balanced homodyne detector for high-rate gaussian-modulated coherent-state quantum key distribution. *New Journal of Physics*, 13(1):013003, 2011. ISSN 1367-2630. URL http://stacks.iop.org/1367-2630/13/i=1/a=013003.

[17] Iris Choi, Robert J Young, and Paul D Townsend. Quantum information to the home. *New Journal of Physics*, 13(6):063039–, 2011. ISSN 1367-2630. URL http://stacks.iop.org/1367-2630/13/i=6/a=063039.

[18] Andrew R. Chraplyvy. Limitations on lightwave communications imposed by optical-fiber nonlinearities. *Lightwave Technology, Journal of*, 8(10):1548–1557, 1990. ISSN 0733-8724.

[19] Stone J. Chraplyvy, A.R. Measurement of crossphase modulation in coherent wavelength-division multiplexing using injection lasers. *Electronics Letters*, 20 (24):996–997, 1984. URL http://digital-library.theiet.org/content/journals/10.1049/el_19840678.

[20] Matthias Christandl, Robert König, and Renato Renner. Postselection technique for quantum channels with applications to quantum cryptography. *Phys. Rev. Lett.*, 102:020504, Jan 2009. doi: 10.1103/PhysRevLett.102.020504. URL http://link.aps.org/doi/10.1103/PhysRevLett.102.020504.

[21] Thomas M. Cover and Joy A. Thomas. *Elements of information theory*. Wiley-Interscience, 1991.

[22] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *Information Theory, IEEE Transactions on*, 24(3):339–348, 1978. ISSN 0018-9448.

[23] Marcos Curty and Tobias Moroder. Heralded-qubit amplifiers for practical device-independent quantum key distribution. *Phys. Rev. A*, 84:010304, Jul 2011. doi: 10.1103/PhysRevA.84.010304. URL http://link.aps.org/doi/10.1103/PhysRevA.84.010304.

[24] Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 461(2053):207–235, January 2005. URL http://rspa.royalsocietypublishing.org/content/461/2053/207.abstract.

[25] Quyen Dinh Xuan, Zheshen Zhang, and Paul L. Voss. A 24 km fiber-based discretely signaled continuous variable quantum key distribution system. *Opt. Express*, 17(26):24244–24249, 2009. URL http://www.opticsexpress.org/abstract.cfm?URI=oe-17-26-24244.

[26] A. R. Dixon, Z. L. Yuan Dynes, J. F. and, A. W. Sharpe, A. J. Bennett, and A. J. Shields. Ultrashort dead time of photon-counting ingaas avalanche photodiodes. *Applied Physics Letters*, 94(23):231113, 2009. doi: http://dx.doi.org/10.1063/1.3151864. URL http://scitation.aip.org/content/aip/journal/apl/94/23/10.1063/1.3151864.

[27] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields. Continuous operation of high bit rate quantum key distribution. *Applied Physics Letters*, 96 (16):–, 2010. doi: http://dx.doi.org/10.1063/1.3385293. URL http://scitation.aip.org/content/aip/journal/apl/96/16/10.1063/1.3385293.

[28] Huang Duan, Fang Jian, Wang Chao, Huang Peng, and Zeng Gui-Hua. A 300-mhz bandwidth balanced homodyne detector for continuous variable quantum key distribution. *Chinese Physics Letters*, 30(11):114209, 2013. ISSN 0256-307X. URL http://stacks.iop.org/0256-307X/30/i=11/a=114209.

[29] BecerraF. E., FanJ., BaumgartnerG., GoldharJ., KosloskiJ. T., and MigdallA. Experimental demonstration of a receiver beating the standard quantum limit for multiple nonorthogonal state discrimination. *Nat Photon*, 7(2):147–152, February 2013. ISSN 1749-4885. URL http://dx.doi.org/10.1038/nphoton.2012.316.

[30] P Eraerds, N Walenta, M Legré, N Gisin, and H Zbinden. Quantum key distribution and 1gbps data encryption over a single fibre. *New Journal of Physics*, 12(6):063027–, 2010. ISSN 1367-2630. URL http://stacks.iop.org/1367-2630/12/i=6/a=063027.

[31] Xu Feihu, Curty Marcos, Qi Bing, Qian Li, and Lo Hoi-Kwong. Discrete-variable measurement-device-independent quantum key distribution suitable for metropolitan networks. *arXiv preprint arXiv:1506.04819*, 2015.

[32] A Ferenczi, P. Grangier, and F. Grosshans. Calibration attack and defense in continuous variable quantum key distribution. In *Lasers and Electro-Optics, 2007 and the International Quantum Electronics Conference. CLEOE-IQEC 2007. European Conference on*, pages 1–1, 2007. doi: 10.1109/CLEOE-IQEC.2007.4386772. URL http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4386772.

[33] Jaromír Fiurášek and Nicolas J. Cerf. Gaussian postselection and virtual noiseless amplification in continuous-variable quantum key distribution. *Phys. Rev. A*, 86: 060302, Dec 2012. doi: 10.1103/PhysRevA.86.060302. URL http://link.aps.org/doi/10.1103/PhysRevA.86.060302.

[34] S Fossier, E Diamanti, T Debuisschert, A Villing, R Tualle-Brouri, and P Grangier. Field test of a continuous-variable quantum key distribution prototype. *New Journal of Physics*, 11(4):045023, 2009. ISSN 1367-2630. URL http://stacks.iop.org/1367-2630/11/i=4/a=045023.

[35] Simon Fossier. *Mise en oeuvre et évaluation de dispositifs de cryptographie quantique à longueur d'onde télécom*. PhD thesis, 2009.

[36] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner. Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks. *Phys. Rev. Lett.*, 109:100502, Sep 2012. doi: 10.1103/PhysRevLett.109.100502. URL http://link.aps.org/doi/10.1103/PhysRevLett.109.100502.

[37] Fabian Furrer. Reverse reconciliation continuous variable quantum key distribution based on the uncertainty principle. *arXiv preprint arXiv:1405.5965*, pages –, 2014.

[38] Raúl García-Patrón and Nicolas J. Cerf. Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.*, 97:190503, Nov 2006. doi: 10.1103/PhysRevLett.97.190503. URL http://link.aps.org/doi/10.1103/PhysRevLett.97.190503.

[39] Raúl García-Patrón and Nicolas J. Cerf. Continuous-variable quantum key distribution protocols over noisy channels. *Phys. Rev. Lett.*, 102:130501, Mar 2009. doi: 10.1103/PhysRevLett.102.130501. URL http://link.aps.org/doi/10.1103/PhysRevLett.102.130501.

[40] Raúl García-Patrón Sánchez. *Quantum Information with Optical Continuous Variables: from Bell Tests to Key Distribution/Information Quantique avec Variables Continues Optiques: des Tests de Bell à la Distribution de Clé*. PhD thesis, 2007.

[41] Tobias Gehring, Vitus Händchen, Jörg Duhme, Fabian Furrer, Torsten Franz, Christoph Pacher, Reinhard F Werner, and Roman Schnabel. Arbitrary-attack-proof quantum key distribution without single photons. *arXiv preprint arXiv:1406.6174*, pages –, 2014.

[42] Ilja Gerhardt, Qin Liu, Antia Lamas-Linares, Johannes Skaar, Christian Kurtsiefer, and Vadim Makarov. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nat Commun*, 2:349–, June 2011. URL http://dx.doi.org/10.1038/ncomms1348.

[43] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy. Trojan-horse attacks on quantum-key-distribution systems. *Phys. Rev. A*, 73:022320, Feb 2006. doi: 10.1103/PhysRevA.73.022320. URL http://link.aps.org/doi/10.1103/PhysRevA.73.022320.

[44] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74:145–195, Mar 2002. doi: 10.1103/RevModPhys.74.145. URL http://link.aps.org/doi/10.1103/RevModPhys.74.145.

[45] Nicolas Gisin, Stefano Pironio, and Nicolas Sangouard. Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier. *Phys. Rev. Lett.*, 105:070501, Aug 2010. doi: 10.1103/PhysRevLett.105.070501. URL http://link.aps.org/doi/10.1103/PhysRevLett.105.070501.

[46] Daniel Gottesman and John Preskill. Secure quantum key distribution using squeezed states. *Phys. Rev. A*, 63:022309, Jan 2001. doi: 10.1103/PhysRevA.63.022309. URL http://link.aps.org/doi/10.1103/PhysRevA.63.022309.

[47] Frédéric Grosshans and Nicolas J. Cerf. Continuous-variable quantum cryptography is secure against non-gaussian attacks. *Phys. Rev. Lett.*, 92:047905, Jan 2004. doi: 10.1103/PhysRevLett.92.047905. URL http://link.aps.org/doi/10.1103/PhysRevLett.92.047905.

[48] Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.*, 88:057902, Jan 2002. doi: 10.1103/PhysRevLett.88.057902. URL http://link.aps.org/doi/10.1103/PhysRevLett.88.057902.

[49] Frédéric Grosshans, Nicolas J. Cerf, Jérôme Wenger, Rosa Tualle-Brouri, and Philippe Grangier. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. *Quantum Info. Comput.*, 3(7):535–552, October 2003. ISSN 1533-7146. URL http://dl.acm.org/citation.cfm?id=2011564.2011570.

[50] Frederic Grosshans, Gilles Van Assche, Jerome Wenger, Rosa Brouri, Nicolas J. Cerf, and Philippe Grangier. Quantum key distribution using gaussian-modulated coherent states. *Nature*, 421(6920):238–241, January 2003. ISSN 0028-0836. URL http://dx.doi.org/10.1038/nature01289.

[51] Hauke Häseler, Tobias Moroder, and Norbert Lütkenhaus. Testing quantum devices: Practical entanglement verification in bipartite optical systems. *Phys. Rev. A*, 77:032303, Mar 2008. doi: 10.1103/PhysRevA.77.032303. URL http://link.aps.org/doi/10.1103/PhysRevA.77.032303.

[52] Matthias Heid and Norbert Lütkenhaus. Efficiency of coherent-state quantum cryptography in the presence of loss: Influence of realistic error correction. *Phys. Rev. A*, 73:052316, May 2006. doi: 10.1103/PhysRevA.73.052316. URL http://link.aps.org/doi/10.1103/PhysRevA.73.052316.

[53] Mark Hillery. Quantum cryptography with squeezed states. *Phys. Rev. A*, 61:022309, Jan 2000. doi: 10.1103/PhysRevA.61.022309. URL http://link.aps.org/doi/10.1103/PhysRevA.61.022309.

[54] Alexander Semenovich Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii*, 9(3):3–11, 1973.

[55] Duan Huang, Dakai Lin, Chao Wang, Weiqi Liu, Shuanghong Fang, Jinye Peng, Peng Huang, and Guihua Zeng. Continuous-variable quantum key distribution with 1 mbps secure key rate. *Opt. Express*, 23(13):17511–17519, 2015. URL http://www.opticsexpress.org/abstract.cfm?URI=oe-23-13-17511.

[56] Jing-Zheng Huang, Christian Weedbrook, Zhen-Qiang Yin, Shuang Wang, Hong-Wei Li, Wei Chen, Guang-Can Guo, and Zheng-Fu Han. Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack. *Phys. Rev. A*, 87:062329, Jun 2013. doi: 10.1103/PhysRevA.87.062329. URL http://link.aps.org/doi/10.1103/PhysRevA.87.062329.

[57] Jing-Zheng Huang, Sébastien Kunz-Jacques, Paul Jouguet, Christian Weedbrook, Zhen-Qiang Yin, Shuang Wang, Wei Chen, Guang-Can Guo, and Zheng-Fu Han. Quantum hacking on quantum key distribution using homodyne detection. *Phys. Rev. A*, 89:032304, Mar 2014. doi: 10.1103/PhysRevA.89.032304. URL http://link.aps.org/doi/10.1103/PhysRevA.89.032304.

[58] Peng Huang, Jian Fang, and Guihua Zeng. State-discrimination attack on discretely modulated continuous-variable quantum key distribution. *Phys. Rev. A*, 89:042330, Apr 2014. doi: 10.1103/PhysRevA.89.042330. URL http://link.aps.org/doi/10.1103/PhysRevA.89.042330.

[59] B. Huttner, N. Imoto, N. Gisin, and T. Mor. Quantum cryptography with coherent states. *Phys. Rev. A*, 51:1863–1869, Mar 1995. doi: 10.1103/PhysRevA.51.1863. URL http://link.aps.org/doi/10.1103/PhysRevA.51.1863.

[60] Icon Group International. *The 2013-2018 World Outlook for Quantum Cryptography*. ICON Group International, Inc., 7 2013. URL http://amazon.com/o/ASIN/B00E8X4WIG/.

[61] Ezra Ip, Alan Pak Tao Lau, Daniel J. F. Barros, and Joseph M. Kahn. Coherent detection in optical fiber systems. *Opt. Express*, 16(2):753–791, 2008. URL http://www.opticsexpress.org/abstract.cfm?URI=oe-16-2-753.

[62] N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs. Risk analysis of trojan-horse attacks on practical quantum key distribution systems. *Selected Topics in Quantum Electronics, IEEE Journal of*, 21(3):1–10, 2015. ISSN 1077-260X.

[63] Paul Jouguet, Sébastien Kunz-Jacques, and Anthony Leverrier. Long-distance continuous-variable quantum key distribution with a gaussian modulation. *Phys. Rev. A*, 84:062317, Dec 2011. doi: 10.1103/PhysRevA.84.062317. URL http://link.aps.org/doi/10.1103/PhysRevA.84.062317.

[64] Paul Jouguet, Sébastien Kunz-Jacques, Thierry Debuisschert, Simon Fossier, Eleni Diamanti, Romain Alléaume, Rosa Tualle-Brouri, Philippe Grangier, Anthony Leverrier, Philippe Pache, and Philippe Painchault. Field test of classical symmetric encryption with continuous variables quantum key distribution. *Opt. Express*,

20(13):14030–14041, 2012. URL http://www.opticsexpress.org/abstract.cfm?URI=oe-20-13-14030.

[65] Paul Jouguet, Sébastien Kunz-Jacques, Eleni Diamanti, and Anthony Leverrier. Analysis of imperfections in practical continuous-variable quantum key distribution. *Phys. Rev. A*, 86:032309, Sep 2012. doi: 10.1103/PhysRevA.86.032309. URL http://link.aps.org/doi/10.1103/PhysRevA.86.032309.

[66] Paul Jouguet, Sébastien Kunz-Jacques, and Eleni Diamanti. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. *Phys. Rev. A*, 87:062313, Jun 2013. doi: 10.1103/PhysRevA.87.062313. URL http://link.aps.org/doi/10.1103/PhysRevA.87.062313.

[67] Paul Jouguet, Sébastien Kunz-Jacques, Rupesh Kumar, Hao Qin, and Romain Alléaume. Experimental demonstration of the coexistence of continuous-variable quantum key distribution with an intense DWDM classical channel, August 2013. URL http://2013.qcrypt.net/program/. Talk at QCrypt 2013.

[68] Paul Jouguet, Sebastien Kunz-Jacques, Anthony Leverrier, Philippe Grangier, and Eleni Diamanti. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat Photon*, 7(5):378–381, May 2013. ISSN 1749-4885. URL http://dx.doi.org/10.1038/nphoton.2013.63.

[69] Paul Jouguet, David Elkouss, and Sébastien Kunz-Jacques. High-bit-rate continuous-variable quantum key distribution. *Phys. Rev. A*, 90:042329, Oct 2014. doi: 10.1103/PhysRevA.90.042329. URL http://link.aps.org/doi/10.1103/PhysRevA.90.042329.

[70] Marc Joye, Arjen K. Lenstra, and Jean jacques Quisquater. Chinese remaindering based cryptosystems in the presence of faults. *Journal of Cryptology*, 12:241–245, 1999.

[71] Imran Khan, Christoffer Wittmann, Nitin Jain, Nathan Killoran, Norbert Lütkenhaus, Christoph Marquardt, and Gerd Leuchs. Optimal working points for continuous-variable quantum channels. *Phys. Rev. A*, 88:010302, Jul 2013. doi: 10.1103/PhysRevA.88.010302. URL http://link.aps.org/doi/10.1103/PhysRevA.88.010302.

[72] Imran Khan, Nitin Jain, Stiller Brigit, Paul Jouguet, Sébastien Kunz-Jacques, Eleni Diamanti, Christoph Marquardt, and Gerd Leuchs. Trojan-horse attacks on practical continuous-variable quantum key distribution systems. In *QCrypt 2014, 4th international conference on quantum cryptography*, 2014.

[73] Thorsten Kleinjung, Kazumaro Aoki, Jens Franke, ArjenK. Lenstra, Emmanuel Thomé, JoppeW. Bos, Pierrick Gaudry, Alexander Kruppa, PeterL. Montgomery, DagArne Osvik, Herman te Riele, Andrey Timofeev, and Paul Zimmermann. Factorization of a 768-bit rsa modulus. In Tal Rabin, editor, *Lecture Notes in Computer Science*, volume 6223, pages 333–350–. Springer Berlin Heidelberg, 2010. URL http://dx.doi.org/10.1007/978-3-642-14623-7_18.

[74] PaulC. Kocher. Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. In Neal Koblitz, editor, *Lecture Notes in Computer Science*, volume 1109, pages 104–113–. Springer Berlin Heidelberg, 1996. URL http://dx.doi.org/10.1007/3-540-68697-5_9.

[75] François Koeune and François-Xavier Standaert. Foundations of security analysis and design iii. chapter A Tutorial on Physical Security and Side-channel Attacks, pages 78–108. Springer-Verlag, Berlin, Heidelberg, 2005. ISBN 3-540-28955-0, 978-3-540-28955-5. URL http://dl.acm.org/citation.cfm?id=2137760.2137764.

[76] Boris Korzh, Charles Ci Wen Lim, Raphael Houlmann, Nicolas Gisin, Ming Jun Li, Daniel Nolan, Bruno Sanguinetti, Rob Thew, and Hugo Zbinden. Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nat Photon*, advance online publication:–, February 2015. ISSN 1749-4893. URL http://dx.doi.org/10.1038/nphoton.2014.327.

[77] M.G. Kuhn. Compromising emanations of lcd tv sets. *Electromagnetic Compatibility, IEEE Transactions on*, 55(3):564–570, 2013. ISSN 0018-9375.

[78] R. Kumar, E. Barrios, A. MacRae, E. Cairns, E.H. Huntington, and A.I. Lvovsky. Versatile wideband balanced detector for quantum optical homodyne tomography. *Optics Communications*, 285(24):5259–5267, November 2012. ISSN 0030-4018. URL http://www.sciencedirect.com/science/article/pii/S0030401812008255.

[79] Rupesh Kumar, Hao Qin, and Romain Alléaume. Experimental demonstration of the coexistence of continuous-variable quantum key distribution with an intense DWDM classical channel. In *OSA Technical Digest (online)*, pages FM4A.1–, San Jose, California, 2014. Optical Society of America. URL http://www.osapublishing.org/abstract.cfm?URI=CLEO_QELS-2014-FM4A.1.

[80] Rupesh Kumar, Hao Qin, and Romain Alléaume. Coexistence of continuous variable QKD with intense DWDM classical channels. *New Journal of Physics*, 17(4):043027–, 2015. ISSN 1367-2630. URL http://stacks.iop.org/1367-2630/17/i=4/a=043027.

[81] Sébastien Kunz-Jacques and Paul Jouguet. Robust shot-noise measurement for continuous-variable quantum key distribution. *Phys. Rev. A*, 91:022307, Feb 2015. doi: 10.1103/PhysRevA.91.022307. URL http://link.aps.org/doi/10.1103/PhysRevA.91.022307.

[82] Andrew M. Lance, Thomas Symul, Vikram Sharma, Christian Weedbrook, Timothy C. Ralph, and Ping Koy Lam. No-switching quantum key distribution using broadband modulated coherent light. *Phys. Rev. Lett.*, 95:180503, Oct 2005. doi: 10.1103/PhysRevLett.95.180503. URL http://link.aps.org/doi/10.1103/PhysRevLett.95.180503.

[83] M. Legre and G. RIBORDY. Apparatus and method for the detection of attacks taking control of the single photon detectors of a quantum cryptography apparatus by randomly changing their efficiency, 2012. URL http://google.com/patents/WO2012046135A3?cl=ja.

[84] Ulf Leonhardt. *Measuring the Quantum State of Light (Cambridge Studies in Modern Optics)*. Cambridge University Press, 11 2005. ISBN 9780521023528. URL http://amazon.com/o/ASIN/0521023521/.

[85] Anthony Leverrier. *Theoretical study of continuous-variable quantum key distribution*. Theses, Télécom ParisTech, November 2009. URL https://tel.archives-ouvertes.fr/tel-00451021.

[86] Anthony Leverrier. Composable security proof for continuous-variable quantum key distribution with coherent states. *Phys. Rev. Lett.*, 114:070501, Feb 2015. doi: 10.1103/PhysRevLett.114.070501. URL http://link.aps.org/doi/10.1103/PhysRevLett.114.070501.

[87] Anthony Leverrier and Philippe Grangier. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Phys. Rev. Lett.*, 102:180504, May 2009. doi: 10.1103/PhysRevLett.102.180504. URL http://link.aps.org/doi/10.1103/PhysRevLett.102.180504.

[88] Anthony Leverrier and Philippe Grangier. Simple proof that gaussian attacks are optimal among collective attacks against continuous-variable quantum key distribution with a gaussian modulation. *Phys. Rev. A*, 81:062314, Jun 2010. doi: 10.1103/PhysRevA.81.062314. URL http://link.aps.org/doi/10.1103/PhysRevA.81.062314.

[89] Anthony Leverrier and Philippe Grangier. Continuous-variable quantum-key-distribution protocols with a non-gaussian modulation. *Phys. Rev. A*, 83:042312, Apr 2011. doi: 10.1103/PhysRevA.83.042312. URL http://link.aps.org/doi/10.1103/PhysRevA.83.042312.

[90] Anthony Leverrier, Romain Alléaume, Joseph Boutros, Gilles Zémor, and Philippe Grangier. Multidimensional reconciliation for a continuous-variable quantum key distribution. *Phys. Rev. A*, 77:042325, Apr 2008. doi: 10.1103/PhysRevA.77.042325. URL http://link.aps.org/doi/10.1103/PhysRevA.77.042325.

[91] Anthony Leverrier, Frédéric Grosshans, and Philippe Grangier. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A*, 81:062343, Jun 2010. doi: 10.1103/PhysRevA.81.062343. URL http://link.aps.org/doi/10.1103/PhysRevA.81.062343.

[92] Anthony Leverrier, Raúl García-Patrón, Renato Renner, and Nicolas J. Cerf. Security of continuous-variable quantum key distribution against general attacks. *Phys. Rev. Lett.*, 110:030502, Jan 2013. doi: 10.1103/PhysRevLett.110.030502. URL http://link.aps.org/doi/10.1103/PhysRevLett.110.030502.

[93] Hong-Wei Li, Shuang Wang, Jing-Zheng Huang, Wei Chen, Zhen-Qiang Yin, Fang-Yi Li, Zheng Zhou, Dong Liu, Yang Zhang, Guang-Can Guo, Wan-Su Bao, and Zheng-Fu Han. Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources. *Phys. Rev. A*, 84:062308, Dec 2011. doi: 10.1103/PhysRevA.84.062308. URL http://link.aps.org/doi/10.1103/PhysRevA.84.062308.

[94] Zhengyu Li, Xiang Peng, and Hong Guo. Continuous-variable measurement-device-independent quantum key distribution with imperfect detectors. In *OSA Technical Digest (online)*, pages FM4A.2–, San Jose, California, 2014. Optical Society of America. URL http://www.opticsinfobase.org/abstract.cfm?URI=CLEO_QELS-2014-FM4A.2.

[95] Zhengyu Li, Yi-Chen Zhang, Feihu Xu, Xiang Peng, and Hong Guo. Continuous-variable measurement-device-independent quantum key distribution. *Phys. Rev. A*, 89:052301, May 2014. doi: 10.1103/PhysRevA.89.052301. URL http://link.aps.org/doi/10.1103/PhysRevA.89.052301.

[96] Xiao-Lei Liang, Jian-Hong Liu, Quan Wang, De-Bing Du, Jian Ma, Ge Jin, Zeng-Bing Chen, Jun Zhang, and Jian-Wei Pan. Fully integrated ingaas/inp single-photon detector module with gigahertz sine wave gating. *Review of Scientific Instruments*, 83(8):083111, 2012. doi: http://dx.doi.org/10.1063/1.4746291. URL http://scitation.aip.org/content/aip/journal/rsi/83/8/10.1063/1.4746291.

[97] C.C.W. Lim, N. Walenta, M. Legre, N. Gisin, and H. Zbinden. Random variation of detector efficiency: A countermeasure against detector blinding attacks for quantum key distribution. *Selected Topics in Quantum Electronics, IEEE Journal of*, 21(3): 1–5, 2015. ISSN 1077-260X.

[98] Yang Liu, Teng-Yun Chen, Liu-Jun Wang, Hao Liang, Guo-Liang Shentu, Jian Wang, Ke Cui, Hua-Lei Yin, Nai-Le Liu, Li Li, Xiongfeng Ma, Jason S. Pelc, M. M. Fejer, Cheng-Zhi Peng, Qiang Zhang, and Jian-Wei Pan. Experimental measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 111:130502, Sep 2013. doi: 10.1103/PhysRevLett.111.130502. URL http://link.aps.org/doi/10.1103/PhysRevLett.111.130502.

[99] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94:230504, Jun 2005. doi: 10.1103/PhysRevLett.94.230504. URL http://link.aps.org/doi/10.1103/PhysRevLett.94.230504.

[100] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 108:130503, Mar 2012. doi: 10.1103/PhysRevLett.108.130503. URL http://link.aps.org/doi/10.1103/PhysRevLett.108.130503.

[101] Hoi-Kwong Lo, Marcos Curty, and Kiyoshi Tamaki. Secure quantum key distribution. *Nat Photon*, 8(8):595–604, August 2014. ISSN 1749-4885. URL http://dx.doi.org/10.1038/nphoton.2014.149.

[102] Jérôme Lodewyck. *Dispositif de distribution quantique de clé avec des états cohérents à longueur d'onde télécom*. PhD thesis, 2006.

[103] Jérôme Lodewyck, Matthieu Bloch, Raúl García-Patrón, Simon Fossier, Evgueni Karpov, Eleni Diamanti, Thierry Debuisschert, Nicolas J. Cerf, Rosa Tualle-Brouri, Steven W. McLaughlin, and Philippe Grangier. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A*, 76:042305, Oct 2007. doi: 10.1103/PhysRevA.76.042305. URL http://link.aps.org/doi/10.1103/PhysRevA.76.042305.

[104] Jérôme Lodewyck, Thierry Debuisschert, Raúl García-Patrón, Rosa Tualle-Brouri, Nicolas J. Cerf, and Philippe Grangier. Experimental implementation of non-gaussian attacks on a continuous-variable quantum-key-distribution system. *Phys. Rev. Lett.*, 98:030503, Jan 2007. doi: 10.1103/PhysRevLett.98.030503. URL http://link.aps.org/doi/10.1103/PhysRevLett.98.030503.

[105] Jérôme Lodewyck, Thierry Debuisschert, Rosa Tualle-Brouri, and Philippe Grangier. Controlling excess noise in fiber-optics continuous-variable quantum key distribution. *Phys. Rev. A*, 72(5):050303–, November 2005. URL http://link.aps.org/doi/10.1103/PhysRevA.72.050303.

[106] A. I. Lvovsky and S. A. Babichev. Synthesis and tomographic characterization of the displaced fock state of light. *Phys. Rev. A*, 66:011801, Jul 2002. doi: 10.1103/PhysRevA.66.011801. URL http://link.aps.org/doi/10.1103/PhysRevA.66.011801.

[107] Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat Photon*, 4(10):686–689, October 2010. ISSN 1749-4885. URL http://dx.doi.org/10.1038/nphoton.2010.214.

[108] Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov. Avoiding the blinding attack in qkd. *Nat Photon*, 4 (12):801–801, December 2010. ISSN 1749-4885. URL http://dx.doi.org/10.1038/nphoton.2010.278.

[109] Lars Lydersen, Mohsen K Akhlaghi, A Hamed Majedi, Johannes Skaar, and Vadim Makarov. Controlling a superconducting nanowire single-photon detector using tailored bright illumination. *New Journal of Physics*, 13(11):113042–, 2011. ISSN 1367-2630. URL http://stacks.iop.org/1367-2630/13/i=11/a=113042.

[110] Lars Lydersen, Nitin Jain, Christoffer Wittmann, Øystein Marøy, Johannes Skaar, Christoph Marquardt, Vadim Makarov, and Gerd Leuchs. Superlinear threshold detectors in quantum cryptography. *Phys. Rev. A*, 84:032320, Sep 2011. doi: 10.1103/PhysRevA.84.032320. URL http://link.aps.org/doi/10.1103/PhysRevA.84.032320.

[111] Xiang-Chun Ma, Shi-Hai Sun, Mu-Sheng Jiang, and Lin-Mei Liang. Local oscillator fluctuation opens a loophole for eve in practical continuous-variable quantum-key-distribution systems. *Phys. Rev. A*, 88:022339, Aug 2013. doi: 10.1103/PhysRevA.88.022339. URL http://link.aps.org/doi/10.1103/PhysRevA.88.022339.

[112] Xiang-Chun Ma, Shi-Hai Sun, Mu-Sheng Jiang, and Lin-Mei Liang. Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol. *Phys. Rev. A*, 87:052309, May 2013. doi: 10.1103/PhysRevA.87.052309. URL http://link.aps.org/doi/10.1103/PhysRevA.87.052309.

[113] Xiang-Chun Ma, Shi-Hai Sun, Mu-Sheng Jiang, Ming Gui, and Lin-Mei Liang. Gaussian-modulated coherent-state measurement-device-independent quantum key distribution. *Phys. Rev. A*, 89:042335, Apr 2014. doi: 10.1103/PhysRevA.89.042335. URL http://link.aps.org/doi/10.1103/PhysRevA.89.042335.

[114] Xiang-Chun Ma, Shi-Hai Sun, Mu-Sheng Jiang, Ming Gui, Yan-Li Zhou, and Lin-Mei Liang. Enhancement of the security of a practical continuous-variable quantum-key-distribution system by manipulating the intensity of the local oscillator. *Phys. Rev. A*, 89:032310, Mar 2014. doi: 10.1103/PhysRevA.89.032310. URL http://link.aps.org/doi/10.1103/PhysRevA.89.032310.

[115] David J. C. MacKay. *Information Theory, Inference & Learning Algorithms*. Cambridge University Press, 2002.

[116] Vadim Makarov. Controlling passively quenched single photon detectors by bright light. *New Journal of Physics*, 11(6):065003–, 2009. ISSN 1367-2630. URL http://stacks.iop.org/1367-2630/11/i=6/a=065003.

[117] F Marsili, VB Verma, JA Stern, S Harrington, AE Lita, T Gerrits, I Vayshenker, B Baek, MD Shaw, and RP Mirin. Detecting single infrared photons with 93 *Nature Photonics*, 7:210–214, 2013. URL http://dx.doi.org/10.1038/nphoton.2013.13.

[118] Alain Monfort. *Cours de statistique mathématique*. Economica, 1997. ISBN 2717832173. URL http://www.amazon.com/Cours-statistique-math%C3%A9matique-Alain-Monfort/dp/2717832173%3FSubscriptionId%3D0JYN1NVW651KCA56C102%26tag%3Dtechkie-20%26linkCode%3Dxm2%26camp%3D2025%26creative%3D165953%26creativeASIN%3D2717832173.

[119] Ryo Namiki and Takuya Hirano. Security of quantum cryptography using balanced homodyne detection. *Phys. Rev. A*, 67:022308, Feb 2003. doi: 10.1103/PhysRevA.67.022308. URL http://link.aps.org/doi/10.1103/PhysRevA.67.022308.

[120] Ryo Namiki and Takuya Hirano. Practical limitation for continuous-variable quantum cryptography using coherent states. *Phys. Rev. Lett.*, 92:117901, Mar 2004. doi: 10.1103/PhysRevLett.92.117901. URL http://link.aps.org/doi/10.1103/PhysRevLett.92.117901.

[121] Ryo Namiki and Takuya Hirano. Security of continuous-variable quantum cryptography using coherent states: Decline of postselection advantage. *Phys. Rev. A*, 72:024301, Aug 2005. doi: 10.1103/PhysRevA.72.024301. URL http://link.aps.org/doi/10.1103/PhysRevA.72.024301.

[122] Ryo Namiki and Takuya Hirano. Efficient-phase-encoding protocols for continuous-variable quantum key distribution using coherent states and postselection. *Phys. Rev. A*, 74:032302, Sep 2006. doi: 10.1103/PhysRevA.74.032302. URL http://link.aps.org/doi/10.1103/PhysRevA.74.032302.

[123] Miguel Navascués, Frédéric Grosshans, and Antonio Acín. Optimality of gaussian attacks in continuous-variable quantum cryptography. *Phys. Rev. Lett.*, 97:190502, Nov 2006. doi: 10.1103/PhysRevLett.97.190502. URL http://link.aps.org/doi/10.1103/PhysRevLett.97.190502.

[124] Jonas S. Neergaard-Nielsen, Makoto Takeuchi, Kentaro Wakui, Hiroki Takahashi, Kazuhiro Hayasaka, Masahiro Takeoka, and Masahide Sasaki. Optical continuous-variable qubit. *Phys. Rev. Lett.*, 105:053602, Jul 2010. doi: 10.1103/PhysRevLett.105.053602. URL http://link.aps.org/doi/10.1103/PhysRevLett.105.053602.

[125] Edward W Ng and Murray Geller. A table of integrals of the error functions. *Journal of Research of the National Bureau of Standards B*, 73:1–20, 1969.

[126] N. I. Nweke, P. Toliver, R. J. Runser, S. R. McNown, J. B. Khurgin, T. E. Chapuran, M. S. Goodman, R. J. Hughes, C. G. Peterson, K. McCabe, J. E. Nordholt, K. Tyagi, P. Hiskett, and N. Dallmann. Experimental characterization of the separation between wavelength-multiplexed quantum and classical communication channels. *Applied Physics Letters*, 87(17):–, 2005. doi: http://dx.doi.org/10.1063/1.2117616. URL http://scitation.aip.org/content/aip/journal/apl/87/17/10.1063/1.2117616.

[127] T. Ogawa and H. Nagaoka. A new proof of the channel coding theorem via hypothesis testing in quantum information theory. In *Information Theory, 2002. Proceedings. 2002 IEEE International Symposium on*, pages 73–, 2002. doi: 10.1109/ISIT.2002.1023345. URL http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=1023345.

[128] Matteo G.A. Paris. Displacement operator by beam splitter. *Physics Letters A*, 217(2–3):78–80, July 1996. ISSN 0375-9601. URL http://www.sciencedirect.com/science/article/pii/0375960196003398.

[129] K. A. Patel, J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields. Coexistence of high-bit-rate quantum key distribution and data on optical fiber. *Phys. Rev. X*, 2:041010, Nov 2012. doi: 10.1103/PhysRevX.2.041010. URL http://link.aps.org/doi/10.1103/PhysRevX.2.041010.

[130] K. A. Patel, J. F. Dynes, M. Lucamarini, I. Choi, A. W. Sharpe, Z. L. Yuan, R. V. Penty, and A. J. Shields. Quantum key distribution for 10 gb/s dense wavelength division multiplexing networks. *Applied Physics Letters*, 104(5):051123, 2014. doi: http://dx.doi.org/10.1063/1.4864398. URL http://scitation.aip.org/content/aip/journal/apl/104/5/10.1063/1.4864398.

[131] M Peev, C Pacher, R Alléaume, C Barreiro, J Bouda, W Boxleitner, T Debuisschert, E Diamanti, M Dianati, J F Dynes, S Fasel, S Fossier, M Fürst, J-D Gautier, O Gay, N Gisin, P Grangier, A Happe, Y Hasani, M Hentschel, H Hübel, G Humer, T Länger, M Legré, R Lieger, J Lodewyck, T Lorünser, N Lütkenhaus, A Marhold, T Matyus, O Maurhart, L Monat, S Nauerth, J-B Page, A Poppe, E Querasser, G Ribordy, S Robyr, L Salvail, A W Sharpe, A J Shields, D Stucki, M Suda, C Tamas, T Themel, R T Thew, Y Thoma, A Treiber, P Trinkler, R Tualle-Brouri, F Vannel, N Walenta, H Weier, H Weinfurter, I Wimberger, Z L Yuan, H Zbinden, and A Zeilinger. The secoqc quantum key distribution network in vienna. *New Journal of Physics*, 11(7):075001–, 2009. ISSN 1367-2630. URL http://stacks.iop.org/1367-2630/11/i=7/a=075001.

[132] N A Peters, P Toliver, T E Chapuran, R J Runser, S R McNown, C G Peterson, D Rosenberg, N Dallmann, R J Hughes, K P McCabe, J E Nordholt, and K T Tyagi. Dense wavelength multiplexing of 1550nm qkd with strong classical channels in reconfigurable networking environments. *New Journal of Physics*, 11(4):045012–, 2009. ISSN 1367-2630. URL http://stacks.iop.org/1367-2630/11/i=4/a=045012.

[133] Stefano Pirandola, Samuel L. Braunstein, and Seth Lloyd. Characterization of collective gaussian attacks and security of coherent-state quantum cryptography. *Phys. Rev. Lett.*, 101:200504, Nov 2008. doi: 10.1103/PhysRevLett.101.200504. URL http://link.aps.org/doi/10.1103/PhysRevLett.101.200504.

[134] Stefano Pirandola, Stefano Mancini, Seth Lloyd, and Samuel L. Braunstein. Continuous-variable quantum cryptography using two-way quantum communication. *Nat Phys*, 4(9):726–730, September 2008. ISSN 1745-2473. URL http://dx.doi.org/10.1038/nphys1018.

[135] Stefano Pirandola, Carlo Ottaviani, Gaetana Spedalieri, Christian Weedbrook, Samuel L. Braunstein, Seth Lloyd, Tobias Gehring, Christian S. Jacobsen, and Ulrik L. Andersen. High-rate measurement-device-independent quantum cryptography. *Nat Photon*, 9(6):397–402, June 2015. ISSN 1749-4885. URL http://dx.doi.org/10.1038/nphoton.2015.83.

[136] Stefano Pirandola, Carlo Ottaviani, Gaetana Spedalieri, Christian Weedbrook, Samuel L. Braunstein, Seth Lloyd, Tobias Gehring, Christian S. Jacobsen, and Ulrik L. Andersen. Mdi-qkd: Continuous- versus discrete-variables at metropolitan distances. *arXiv preprint arXiv:1506.06748*, 2015.

[137] Bing Qi, Lei-Lei Huang, Li Qian, and Hoi-Kwong Lo. Experimental study on the gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers. *Phys. Rev. A*, 76:052323, Nov 2007. doi: 10.1103/PhysRevA.76.052323. URL http://link.aps.org/doi/10.1103/PhysRevA.76.052323.

[138] Bing Qi, Wen Zhu, Li Qian, and Hoi-Kwong Lo. Feasibility of quantum key distribution through a dense wavelength division multiplexing network. *New Journal of Physics*, 12(10):103042–, 2010. ISSN 1367-2630. URL http://stacks.iop.org/1367-2630/12/i=10/a=103042.

[139] Bing Qi, Pavel Lougovski, Raphael Pooser, Warren Grice, and Miljko Bobrek. Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection. *Phys. Rev. X*, 5:041009, Oct 2015. doi: 10.1103/PhysRevX.5.041009. URL http://link.aps.org/doi/10.1103/PhysRevX.5.041009.

[140] Hao Qin, Rupesh Kumar, and Romain Alléaume. Saturation attack on continuous-variable quantum key distribution system. In *Proc. SPIE 8899, Emerging Technologies in Security and Defence; and Quantum Security II; and Unmanned Sensor Systems X, 88990N*, volume 8899, pages 88990N–88990N–7, 2013. doi: 10.1117/12.2028543. URL http://dx.doi.org/10.1117/12.2028543.

[141] Hao Qin, Rupesh Kumar, and Romain Alléaume. Saturation attack on a practical continuous-variable quantum key distribution system, August 2013. URL http://2013.qcrypt.net/program/. Talk at QCrypt 2013.

[142] Hao Qin, Rupesh Kumar, and Romain Alléaume. Quantum hacking: saturation attack on practical continuous-variable quantum key distribution system. *arXiv preprint arXiv:1511.01007*, 2015.

[143] Hao Qin, Rupesh Kumar, and Romain Alléaume. Saturation attack on continuous-variable QKD systems: experimental demonstration, performance analysis and countermeasure. *In preparation*, 2015.

[144] Hao Qin, Rupesh Kumar, and Romain Alleaume. Quantum hacking on a practical continuous-variable quantum cryptosystem by inserting an external light. In *Proc. SPIE 9648, Electro-Optical and Infrared Systems: Technology and Applications XII; and Quantum Information Science and Technology*, volume 9648, pages 9648V–11, 2015. doi: 10.1117/12.2195433. URL http://dx.doi.org/10.1117/12.2195433.

[145] T. C. Ralph. Continuous variable quantum cryptography. *Phys. Rev. A*, 61:010303, Dec 1999. doi: 10.1103/PhysRevA.61.010303. URL http://link.aps.org/doi/10.1103/PhysRevA.61.010303.

[146] M. D. Reid. Quantum cryptography with a predetermined key, using continuous-variable einstein-podolsky-rosen correlations. *Phys. Rev. A*, 62:062308, Nov 2000. doi: 10.1103/PhysRevA.62.062308. URL http://link.aps.org/doi/10.1103/PhysRevA.62.062308.

[147] R. Renner and J. I. Cirac. de finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. *Phys. Rev. Lett.*, 102: 110504, Mar 2009. doi: 10.1103/PhysRevLett.102.110504. URL http://link.aps.org/doi/10.1103/PhysRevLett.102.110504.

[148] Renato Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 6(01):1–127, 2008. ISSN 0219-7499.

[149] Renato Renner and Robert König. Universally composable privacy amplification against quantum adversaries. In Joe Kilian, editor, *Lecture Notes in Computer Science*, volume 3378, pages 407–425–. Springer Berlin Heidelberg, 2005. URL http://dx.doi.org/10.1007/978-3-540-30576-7_22.

[150] T.J. Richardson, M.A. Shokrollahi, and R.L. Urbanke. Design of capacity-approaching irregular low-density parity-check codes. *Information Theory, IEEE Transactions on*, 47(2):619–637, 2001. ISSN 0018-9448.

[151] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, 1978. doi: 10.1145/359340.359342.

[152] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel. Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks. *Phys. Rev. Lett.*, 111:130501, Sep 2013. doi: 10.1103/PhysRevLett.111.130501. URL http://link.aps.org/doi/10.1103/PhysRevLett.111.130501.

[153] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger. Field test of quantum key distribution in the tokyo qkd network. *Opt. Express*, 19(11):10387–10409, 2011. URL http://www.opticsexpress.org/abstract.cfm?URI=oe-19-11-10387.

[154] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81:1301–1350, Sep 2009. doi: 10.1103/RevModPhys.81.1301. URL http://link.aps.org/doi/10.1103/RevModPhys.81.1301.

[155] Wolfgang P. Schleich. *Quantum Optics in Phase Space*. Wiley-VCH, 1 edition, 2 2001. ISBN 9783527294350. URL http://amazon.com/o/ASIN/352729435X/.

[156] Tobias Schmitt-Manderbach, Henning Weier, Martin Fürst, Rupert Ursin, Felix Tiefenbacher, Thomas Scheidl, Josep Perdigues, Zoran Sodnik, Christian Kurtsiefer, John G. Rarity, Anton Zeilinger, and Harald Weinfurter. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Phys. Rev. Lett.*, 98:010504, Jan 2007. doi: 10.1103/PhysRevLett.98.010504. URL http://link.aps.org/doi/10.1103/PhysRevLett.98.010504.

[157] C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715, 1949. ISSN 1538-7305. URL http://dx.doi.org/10.1002/j.1538-7305.1949.tb00928.x.

[158] Claude Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 623–656, 1948.

[159] Yong Shen, Hongxin Zou, Liang Tian, Pingxing Chen, and Jianmin Yuan. Experimental study on discretely modulated continuous-variable quantum key distribution. *Phys. Rev. A*, 82:022317, Aug 2010. doi: 10.1103/PhysRevA.82.022317. URL http://link.aps.org/doi/10.1103/PhysRevA.82.022317.

[160] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997. doi: 10.1137/S0097539795293172.

[161] Ch. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs. Continuous variable quantum cryptography: Beating the 3 db loss limit. *Phys. Rev. Lett.*, 89:167901, Sep 2002. doi: 10.1103/PhysRevLett.89.167901. URL http://link.aps.org/doi/10.1103/PhysRevLett.89.167901.

[162] Daniel B. S. Soh, Constantin Brif, Patrick J. Coles, Norbert Lütkenhaus, Ryan M. Camacho, Junji Urayama, and Mohan Sarovar. Self-referenced continuous-variable quantum key distribution protocol. *Phys. Rev. X*, 5:041010, Oct 2015. doi: 10.1103/PhysRevX.5.041010. URL http://link.aps.org/doi/10.1103/PhysRevX.5.041010.

[163] Darius Subacius, Anton Zavriyev, and Alexei Trifonov. Backscattering limitation for fiber-optic quantum key distribution systems. *Applied Physics Letters*, 86(1):011103, 2005. doi: http://dx.doi.org/10.1063/1.1842862. URL http://scitation.aip.org/content/aip/journal/apl/86/1/10.1063/1.1842862.

[164] Shi-Hai Sun, Mu-Sheng Jiang, and Lin-Mei Liang. Passive faraday-mirror attack in a practical two-way quantum-key-distribution system. *Phys. Rev. A*, 83:062331, Jun 2011. doi: 10.1103/PhysRevA.83.062331. URL http://link.aps.org/doi/10.1103/PhysRevA.83.062331.

[165] Shi-Hai Sun, Mu-Sheng Jiang, and Lin-Mei Liang. Single-photon-detection attack on the phase-coding continuous-variable quantum cryptography. *Phys. Rev. A*, 86: 012305, Jul 2012. doi: 10.1103/PhysRevA.86.012305. URL http://link.aps.org/doi/10.1103/PhysRevA.86.012305.

[166] Shi-Hai Sun, Mu-Sheng Jiang, Xiang-Chun Ma, Chun-Yan Li, and Lin-Mei Liang. Hacking on decoy-state quantum key distribution system with partial phase randomization. *Sci. Rep.*, 4:–, April 2014. URL http://dx.doi.org/10.1038/srep04759.

[167] Denis Sych and Gerd Leuchs. Coherent state quantum key distribution with multi letter phase-shift keying. *New Journal of Physics*, 12(5):053019–, 2010. ISSN 1367-2630. URL http://stacks.iop.org/1367-2630/12/i=5/a=053019.

[168] Yan-Lin Tang, Hua-Lei Yin, Xiongfeng Ma, Chi-Hang Fred Fung, Yang Liu, Hai-Lin Yong, Teng-Yun Chen, Cheng-Zhi Peng, Zeng-Bing Chen, and Jian-Wei Pan. Source attack of decoy-state quantum key distribution using phase information. *Phys. Rev. A*, 88:022308, Aug 2013. doi: 10.1103/PhysRevA.88.022308. URL http://link.aps.org/doi/10.1103/PhysRevA.88.022308.

[169] Yan-Lin Tang, Hua-Lei Yin, Si-Jing Chen, Yang Liu, Wei-Jun Zhang, Xiao Jiang, Lu Zhang, Jian Wang, Li-Xing You, Jian-Yu Guan, Dong-Xu Yang, Zhen Wang, Hao Liang, Zhen Zhang, Nan Zhou, Xiongfeng Ma, Teng-Yun Chen, Qiang Zhang, and Jian-Wei Pan. Measurement-device-independent quantum key distribution over 200 km. *Phys. Rev. Lett.*, 113:190501, Nov 2014. doi: 10.1103/PhysRevLett.113.190501. URL http://link.aps.org/doi/10.1103/PhysRevLett.113.190501.

[170] Zhiyuan Tang, Zhongfa Liao, Feihu Xu, Bing Qi, Li Qian, and Hoi-Kwong Lo. Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 112:190503, May 2014. doi: 10.1103/PhysRevLett.112.190503. URL http://link.aps.org/doi/10.1103/PhysRevLett.112.190503.

[171] V. J. Tekippe. Passive fiber optic components made by the fused biconical taper process. volume 1085, pages 88–115, 1990. doi: 10.1117/12.952938. URL http://dx.doi.org/10.1117/12.952938.

[172] Marco Tomamichel, Charles Ci Wen Lim, Nicolas Gisin, and Renato Renner. Tight finite-key analysis for quantum cryptography. *Nat Commun*, 3:634–, January 2012. URL http://dx.doi.org/10.1038/ncomms1631.

[173] P.D. Townsend. Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing. *Electronics Letters*, 33(3):188–190, 1997. ISSN 0013-5194.

[174] Kenji Tsujino, Daiji Fukuda, Go Fujii, Shuichiro Inoue, Mikio Fujiwara, Masahiro Takeoka, and Masahide Sasaki. Quantum receiver beyond the standard quantum limit of coherent optical communication. *Phys. Rev. Lett.*, 106:250503, Jun 2011. doi: 10.1103/PhysRevLett.106.250503. URL http://link.aps.org/doi/10.1103/PhysRevLett.106.250503.

[175] G.S. Vernam. Secret signaling system, 1919. URL http://www.google.com/patents/US1310719.

[176] Nino Walenta, Mathilde Soucarros, Damien Stucki, Dario Caselunghe, Mathias Domergue, Michael Hagerman, Randall Hart, Don Hayford, Rapha´el Houlmann, Matthieu Legré, M, Todd McCandlish, Jean-Benoît Page, Maurice Tourville, and Richard Wolterman. Practical aspects of security certification for commercial quantum technologies. volume 9648, pages 96480U–96480U–11, 2015. doi: 10.1117/12.2193776. URL http://dx.doi.org/10.1117/12.2193776.

[177] Shuang Wang, Wei Chen, Zhen-Qiang Yin, Hong-Wei Li, De-Yong He, Yu-Hu Li, Zheng Zhou, Xiao-Tian Song, Fang-Yi Li, Dong Wang, Hua Chen, Yun-Guang Han, Jing-Zheng Huang, Jun-Fu Guo, Peng-Lei Hao, Mo Li, Chun-Mei Zhang, Dong Liu, Wen-Ye Liang, Chun-Hua Miao, Ping Wu, Guang-Can Guo, and Zheng-Fu Han. Field and long-term demonstration of a wide area quantum key distribution network. *Opt. Express*, 22(18):21739–21756, 2014. URL http://www.opticsexpress.org/abstract.cfm?URI=oe-22-18-21739.

[178] Xiang-Bin Wang. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.*, 94:230503, Jun 2005. doi: 10.1103/PhysRevLett.94.230503. URL http://link.aps.org/doi/10.1103/PhysRevLett.94.230503.

[179] Christian Weedbrook, Andrew M. Lance, Warwick P. Bowen, Thomas Symul, Timothy C. Ralph, and Ping Koy Lam. Quantum cryptography without switching. *Phys. Rev. Lett.*, 93:170504, Oct 2004. doi: 10.1103/PhysRevLett.93.170504. URL http://link.aps.org/doi/10.1103/PhysRevLett.93.170504.

[180] Christian Weedbrook, Andrew M. Lance, Warwick P. Bowen, Thomas Symul, Timothy C. Ralph, and Ping Koy Lam. Coherent-state quantum key distribution without random basis switching. *Phys. Rev. A*, 73:022316, Feb 2006. doi: 10.1103/PhysRevA.73.022316. URL http://link.aps.org/doi/10.1103/PhysRevA.73.022316.

[181] Christian Weedbrook, Stefano Pirandola, Seth Lloyd, and Timothy C. Ralph. Quantum cryptography approaching the classical limit. *Phys. Rev. Lett.*, 105:110501, Sep 2010. doi: 10.1103/PhysRevLett.105.110501. URL http://link.aps.org/doi/10.1103/PhysRevLett.105.110501.

[182] Christian Weedbrook, Stefano Pirandola, Raúl García-Patrón, Nicolas J. Cerf, Timothy C. Ralph, Jeffrey H. Shapiro, and Seth Lloyd. Gaussian quantum information. *Rev. Mod. Phys.*, 84:621–669, May 2012. doi: 10.1103/RevModPhys.84.621. URL http://link.aps.org/doi/10.1103/RevModPhys.84.621.

[183] Christian Weedbrook, Stefano Pirandola, and Timothy C. Ralph. Continuous-variable quantum key distribution using thermal states. *Phys. Rev. A*, 86:022318, Aug 2012. doi: 10.1103/PhysRevA.86.022318. URL http://link.aps.org/doi/10.1103/PhysRevA.86.022318.

[184] Henning Weier, Harald Krauss, Markus Rau, Martin Fürst, Sebastian Nauerth, and Harald Weinfurter. Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors. *New Journal of Physics*, 13(7):073024–, 2011. ISSN 1367-2630. URL http://stacks.iop.org/1367-2630/13/i=7/a=073024.

[185] C Wiechers, L Lydersen, C Wittmann, D Elser, J Skaar, Ch Marquardt, V Makarov, and G Leuchs. After-gate attack on a quantum cryptosystem. *New Journal of Physics*, 13(1):013043–, 2011. ISSN 1367-2630. URL http://stacks.iop.org/1367-2630/13/i=1/a=013043.

[186] A. Winter. Coding theorem and strong converse for quantum channels. *Information Theory, IEEE Transactions on*, 45(7):2481–2485, 1999. ISSN 0018-9448. doi: 10.1109/18.796385. URL http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=796385.

[187] Christoffer Wittmann, Masahiro Takeoka, Katiúscia N. Cassemiro, Masahide Sasaki, Gerd Leuchs, and Ulrik L. Andersen. Demonstration of near-optimal discrimination of optical coherent states. *Phys. Rev. Lett.*, 101:210501, Nov 2008. doi: 10.1103/PhysRevLett.101.210501. URL http://link.aps.org/doi/10.1103/PhysRevLett.101.210501.

[188] Peter Wright. *SpyCatcher: The Candid Autobiography of a Senior Intelligence Officer*. Dell, 1st edition, 7 1988. ISBN 9780440201328. URL http://amazon.com/o/ASIN/0440201322/.

[189] Qing-Lin Wu, Naoto Namekata, and Shuichiro Inoue. Sinusoidally gated ingaas avalanche photodiode with direct hold-off function for efficient and low-noise single-photon detection. *Applied Physics Express*, 6(6):062202–, 2013. ISSN 1882-0786. URL http://stacks.iop.org/1882-0786/6/i=6/a=062202.

[190] Feihu Xu, Bing Qi, and Hoi-Kwong Lo. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New Journal of Physics*, 12(11):113026–, 2010. ISSN 1367-2630. URL http://stacks.iop.org/1367-2630/12/i=11/a=113026.

[191] Amnon Yariv and Pochi Yeh. *Photonics: Optical Electronics in Modern Communications (The Oxford Series in Electrical and Computer Engineering)*. Oxford University Press, 2006. ISBN 0195179463. URL http://www.amazon.com/Photonics-Electronics-Communications-Electrical-Engineering/dp/0195179463%3FSubscriptionId%3D0JYN1NVW651KCA56C102%26tag%3Dtechkie-20%26linkCode%3Dxm2%26camp%3D2025%26creative%3D165953%26creativeASIN%3D0195179463.

[192] Z. L. Yuan, J. F. Dynes, and A. J. Shields. Avoiding the blinding attack in qkd. *Nat Photon*, 4(12):800–801, December 2010. ISSN 1749-4885. URL http://dx.doi.org/10.1038/nphoton.2010.269.

[193] Yi-Chen Zhang, Song Yu, and Wanyi Gu. Squeezed-state measurement-device-independent quantum key distribution. In *OSA Technical Digest (online)*, pages FM4A.4–, San Jose, California, 2014. Optical Society of America. URL http://www.opticsinfobase.org/abstract.cfm?URI=CLEO_QELS-2014-FM4A.4.

[194] Yi Zhao, Chi-Hang Fred Fung, Bing Qi, Christine Chen, and Hoi-Kwong Lo. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A*, 78:042333, Oct 2008. doi: 10.1103/PhysRevA.78.042333. URL http://link.aps.org/doi/10.1103/PhysRevA.78.042333.

[195] Yi-Bo Zhao, Matthias Heid, Johannes Rigas, and Norbert Lütkenhaus. Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks. *Phys. Rev. A*, 79:012307, Jan 2009. doi: 10.1103/PhysRevA.79.012307. URL http://link.aps.org/doi/10.1103/PhysRevA.79.012307.

[196] Yongbin Zhou and DengGuo Feng. Side-channel attacks: Ten years after its publication and the impacts on cryptographic module security testing, 2005.

[197] Li Zhuang, Feng Zhou, and J. D. Tygar. Keyboard acoustic emanations revisited. *ACM Trans. Inf. Syst. Secur.*, 13(1):3:1–3:26, November 2009. ISSN 1094-9224. doi: 10.1145/1609956.1609959. URL http://doi.acm.org/10.1145/1609956.1609959.

Sécurité pratique de systèmes de cryptographie quantique : Étude d'attaques et développement de contre-mesures

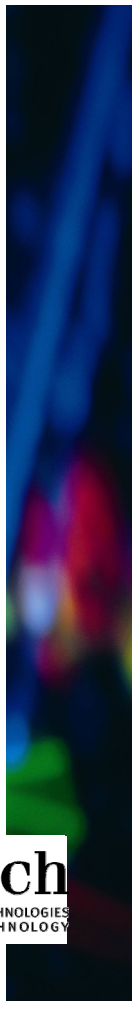
Hao QIN

RESUME : Dans cette thèse, j'étudie une primitive cryptographique appelée distribution quantique de clés. La distribution quantique de clés permet à deux parties distantes de partager une clé secrète en présence d'une espion, dont la puissance est seulement limité par les lois de la physique quantique. J'ai concentré mon travail de thèse sur la distribution quantique de clés à variables continues et en particulier, sur l'étude pratique d'implémentations. J'ai proposé et étudié théoriquement une attaque par canaux cachés originale, visant les détecteurs : l'attaque par saturation. Nous avons de plus démontré expérimentalement la faisabilité de cette attaque sur un système de la distribution quantique de clés à variables continues dans notre laboratoire. Enfin, nous avons en outre démontré expérimentalement pour la première fois la faisabilité du déploiement d'un système de la distribution quantique de clés à variables continues dans un réseau optique du multiplexage en longueur d'onde dense.

MOTS-CLEFS : cryptographie quantique, la distribution quantique de clés, la communication quantique, variables continues, détection homodyne, sécurité pratique, attaque à canal auxiliaire, piratage quantique, multiplexage en longueur d'onde

ABSTRACT : In this thesis, I study a cryptographic primitive called quantum key distribution which allows two remote parties to share a secret key, in the presence of an eavesdropper, whose power is only limited by the laws of quantum physics. I focus my study on the implementation and the practical security of continuous-variable protocols. For the first time, I have proposed and studied a detector-based side channel attack on a continuous-variable system : saturation attack. This attack opens a new security loophole that we have characterized experimentally in our laboratory, on a real continuous-variable system. Finally, we have demonstrated experimentally for the first time the feasibility of a continuous-variable system deployment in a Dense Wavelength Division Multiplexing network, where quantum signals coexist with intense classical signals in a same fiber.

KEY-WORDS : quantum cryptography, quantum key distribution, quantum communication, continuous variable, homodyne detection, practical security, side channels, quantum hacking, wavelength division multiplexing



TELECOM ParisTech

EDiTE

ParisTech
INSTITUT DES SCIENCES ET TECHNOLOGIES
PARIS INSTITUTE OF TECHNOLOGY