Security and performance of continuous-variable quantum key distribution systems

Paul Jouguet

▶ To cite this version:

Paul Jouguet. Security and performance of continuous-variable quantum key distribution systems. Cryptography and Security [cs.CR]. Télécom ParisTech, 2013. English. NNT : 2013ENST0048 . tel-01174739

HAL Id: tel-01174739
https://pastel.hal.science/tel-01174739

Submitted on 9 Jul 2015

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

ParisTech
INSTITUT DES SCIENCES ET TECHNOLOGIES
PARIS INSTITUTE OF TECHNOLOGY

TELECOM ParisTech

2013-ENST-0048

EDITE - ED 130

Doctorat ParisTech

THÈSE

pour obtenir le grade de docteur délivré par

TELECOM ParisTech

Spécialité « Informatique et Réseaux »

présentée et soutenue publiquement par

Paul JOUGUET

le 18 septembre 2013

Sécurité et performance de dispositifs de distribution quantique de clés à variables continues

Directeur de thèse : **Eleni DIAMANTI**
Co-encadrement de la thèse : **Romain ALLÉAUME**

Jury
M. Ping Koy LAM, Professeur, Département de physique, Université de Canberra — Rapporteurs
M. Hugo ZBINDEN, Professeur, GAP Optique, Université de Genève
M. Philippe GRANGIER, Directeur de recherche, CNRS, Institut d'Optique — Examinateurs
M. Nicolas TREPS, Professeur, Laboratoire Kastler Brossel, Université Pierre et Marie Curie
M. Nicolas CERF, Professeur, Centre d'Information et Communication Quantique, Université Libre de Bruxelles
M. Sébastien KUNZ-JACQUES, Directeur technique, SeQureNet

THÈSE

TELECOM ParisTech
école de l'Institut Mines-Télécom - membre de ParisTech
46 rue Barrault 75013 Paris - (+33) 1 45 81 77 77 - www.telecom-paristech.fr

Abstract

This thesis focuses on a cryptographic primitive that allows two distant parties, usually called Alice and Bob, to generate an arbitrary amount of secret key even in the presence of an eavesdropper, provided that they share a short initial secret message. This primitive is called quantum key distribution, or in short QKD; and differs from classical key distribution primitives in the sense that no assumption on the capacities of the eavesdropper is required to prove the security of the scheme. While several QKD protocols exist, we focus our study on continuous-variable protocols, which encode the information on the quadratures of the electromagnetic field. Some of these protocols are of particular interest because they can be implemented with standard fiber-based telecommunication components and feature an interferometric detection scheme that exhibits a high resistance to the noise induced by potential adjacent classical channels that propagate on the same optical fiber.

The advantage of QKD over classical primitives relies on fundamental quantum physics principles such as the uncertainty principle: in a carefully designed QKD protocol, an eavesdropper cannot interact with the quantum system without introducing some noise which can be quantified by the parties of the protocol. However, even when there is no active eavesdropper, some errors inevitably occur during the transmission of quantum states between Alice and Bob. Alice and Bob must correct these errors to agree on a common bit string. Since this step is done by revealing some information on a public channel, it results in a limitation of the protocol in terms of tolerance to noise and losses. To overcome this, we develop efficient error-correcting codes that allow to extend the range of a QKD protocol based on a Gaussian modulation of the quadratures of the electromagnetic field.

Security proofs for QKD protocols typically consider an ideal description of the protocol. In practice, however, one has to consider the distance between a practical implementation of a QKD protocol and its theoretical description. We study different aspects of a practical implementation of a Gaussian continuous-variable QKD protocol, such as the imperfect statistical estimation (in the finite-size scenario) of the parameters that are relevant to the security of the protocol and the quality of the practical Gaussian modulation of coherent states. We also consider a calibration attack that can lead to a powerful eavesdropping strategy. We demonstrate experimentally the distribution of secret keys over a 80 km fiber link when taking into account all the known imperfections of our system.

Finally, we make initial deployment tests involving our QKD system and wavelength division multiplexed (WDM) classical channels on the same fiber link. We also demonstrate the long-term stability of our system in combination with high-speed classical encryptors.

Résumé

L'objet de cette thèse est l'étude d'une primitive cryptographique qui permet à deux utilisateurs distants, que l'on appelle Alice et Bob, de générer une quantité arbitraire de clé secrète et cela y compris en présence d'un espion, sous réserve qu'ils partagent un secret initial. Cette primitive est appelée la distribution quantique de clés (Quantum Key Distribution ou QKD en anglais) et diffère des primitives classiques de distribution de clés en ce sens qu'il n'est pas nécessaire de faire des hypothèses sur les capacités de l'espion pour prouver la sécurité du protocole. Bien qu'il existe de nombreux protocoles de QKD, nous restreignons notre étude aux protocoles employant des variables continues et qui encodent l'information sur les quadratures du champ électromagnétique. L'intérêt de ces protocoles tient au fait qu'ils peuvent pour certains être implémentés avec uniquement des composants standards optimisés pour les communications sur fibre optique ainsi qu'à l'usage d'une détection interférométrique particulièrement résistante au bruit induit par des canaux classiques adjacents qui se propagent sur le même lien fibré.

L'avantage de la QKD sur les primitives classiques repose sur des principes fondamentaux de la physique quantique tels que le principe d'incertitude : dans un protocole QKD, un espion ne peut interagir avec le système quantique sans introduire un certain niveau de bruit qui peut être évalué par les protagonistes du protocole.

Même en l'absence d'attaquant, la transmission d'états quantiques entre Alice et Bob ne se fait pas sans erreur en raison des interactions entre les états quantiques et l'environnement. Alice et Bob doivent donc corriger ces erreurs afin de se mettre d'accord sur une chaîne binaire commune. Cette étape de correction d'erreurs s'effectue en révélant de l'information sur un canal public, ce qui limite la tolérance du protocole au bruit et aux pertes. Nous avons mis au point des codes correcteurs d'erreurs efficaces qui permettent d'étendre la portée du protocole QKD basé sur une modulation Gaussienne des quadratures du champ électromagnétique.

Les preuves de sécurité des protocoles QKD considèrent une description idéale du protocole. En pratique, il convient de s'intéresser à la distance entre l'implémentation pratique d'un protocole QKD et sa description théorique. Nous étudions différents aspects de l'implémentation pratique d'un protocole QKD Gaussien à variables continues, tels que l'imparfaite estimation statistique (dans le cas d'un scenario réaliste où Alice et Bob échangent une quantité finie de signaux) des paramètres qui caractérisent la sécurité du protocole et la qualité d'une modulation Gaussienne d'états cohérents de la lumière en pratique. Nous mettons également en évidence une attaque visant la calibration d'un système QKD et pouvant conduire à une stratégie d'espionnage mettant en péril la sécurité du dispositif. Nous démontrons expérimentalement la distribution de clés secrètes sur un lien fibré de 80 km en prenant en compte toutes les imperfections connues de notre système.

Enfin, nous conduisons des tests de déploiement de notre système QKD dans un environnement mettant en scène des canaux classiques multiplexés en longueur d'onde sur le même lien fibré. Nous démontrons également la stabilité sur le long terme de notre système en combinaison avec des chiffreurs classiques haut débit.

Acknowledgements

This thesis was done in an unusual framework since it was done in collaboration between the start-up company SeQureNet, created as a spin-off of the research activities of the Quantum Information research team of Télécom ParisTech, and this research group. I would like to take this opportunity to thank Romain Alléaume and Nicolas Aliacar who founded SeQureNet in 2008 and Gérard Memmi, director of the Computer Science and Networks department of Télécom ParisTech, for having me benefited from ideal material conditions during this research work.

I would like to thank warmly Eleni Diamanti and Sébastien Kunz-Jacques who supervised my research work. Their advice and their friendship were essential during these three years.

Thank to Philippe Grangier who transferred a high-quality research work from the Institut d'Optique to Télécom ParisTech and SeQureNet and thank to Thierry Debuisschert who taught me the bases of the continuous-variable quantum key distribution experiment. I tried to prove myself worthy of their confidence.

Then, I would like to thank all the people from the Quantum Information community I met during my thesis and especially Anthony Leverrier. I had the good luck to meet him at the time he was completing his PhD thesis and both his work commitment and his research skills became a reference for my thesis.

Special thanks to Gérard Mouret and Patrick Busch for their work and availability to help us design and realize the different electronic circuits we used for this work.

I would like to thank Ping Koy Lam and Hugo Zbinden for having accepted to review this manuscript. My thanks also go to Nicolas Cerf and Nicolas Treps who accepted to be members of my jury.

Finally, I would like to thank my family for their constant support throughout my whole life: Anne, Elizabeth, Giselle, Jeanne, Michel, Pierre-Luc and Thiphaine.

Contents

1 From Classical Cryptography to Quantum Cryptography 7

1.1 What is Cryptography? . . . 7

1.2 Modern Cryptography . . . 9

1.2.1 Symmetric and Asymmetric Cryptography . . . 9

1.2.2 Usual Primitives . . . 10

1.2.3 Threats . . . 10

1.3 Quantum Key Distribution . . . 10

1.3.1 Principle . . . 11

1.3.2 Security Characteristics . . . 11

1.3.3 DVQKD vs CVQKD in 2010 . . . 12

1.3.4 Threats . . . 13

1.4 Other Quantum Cryptographic Primitives . . . 13

1.4.1 Coin Flipping . . . 13

1.4.2 Quantum Signatures . . . 14

2 Quantum Information with Gaussian Variables 15

2.1 Quantum mechanics postulates . . . 16

2.1.1 Notations and basic definitions . . . 16

2.1.2 Quantum operators . . . 17

2.1.3 Composite systems . . . 17

2.1.4 Dynamics of a physical system . . . 18

2.2 Classical Information Theory . . . 18

2.2.1 Entropies . . . 18

2.2.2 Channels and Capacities . . . 21

2.2.3 Channel Coding . . . 23

2.3 Single-mode Quantum Optics . . . 24

2.3.1 One-mode Fock States . . . 25

2.3.2 Coherent States . . . 26

2.3.3 Squeezed States . . . 29

2.4 Two-mode Squeezed States . . . 32

2.5 Weyl Operator . . . 33

2.6 Phase-Space Representation . . . 33

2.7 Gaussian States . . . 34

2.7.1 One mode Gaussian states . . . 34

2.7.2 Two mode Gaussian states . . . 35

2.8 Symplectic Analysis for Multimode Gaussian States . . . 36

2.8.1 One-mode normal decomposition . . . 36

2.8.2 Two-mode normal decomposition . . . 36

2.8.3 Three-mode normal decomposition . . . 37

2.9 Entropy of Gaussian States . . . 37

2.9.1 Von Neumann entropy . . . 37

2.9.2 Entropy of Gaussian states . . . 37

2.9.3 Extremality of Gaussian states 38
2.10 Gaussian Operations 38
2.10.1 Gaussian unitary operations 38
2.10.2 Passive transformations 39
2.10.3 Active transformations 39

3 Quantum Key Distribution with Continuous Variables 41
3.1 The Security of a QKD Protocol 42
3.1.1 Key Security Criterion 42
3.1.2 QKD Protocol Steps 43
3.2 A Brief History of QKD Protocols 43
3.3 Security Analysis of the Ideal GG02 Protocol 44
3.3.1 Protocol Description 44
3.3.2 Some Potential Deviations to the Ideal GG02 Protocol 46
3.3.3 Security Proof against Collective Attacks 46
3.3.4 Security proof against General Attacks 49
3.4 Security Analysis of the Imperfect GG02 Protocol 49
3.4.1 Effect of an Imperfect Reconciliation Procedure 50
3.4.2 Effect of an Imperfect Homodyne Detection 51
3.4.3 Security of Gaussian Protocols with an Imperfect Modulation 53
3.4.4 Imperfect Calibration of the Detection Setup 57
3.4.5 Improved Key Rate with Phase Noise Calibration . . . 61
3.5 Conclusion 66

4 Experimental Setup 67
4.1 Optical fibers 67
4.1.1 Waveguides 68
4.1.2 Transmission characteristics 68
4.1.3 Dispersion 69
4.1.4 Connections 70
4.2 Laser Source 70
4.3 Electro-optic Modulators 71
4.4 Light detection 74
4.4.1 Homodyne Detection Principle 74
4.4.2 Impact of the Imperfections on the Homodyne Detection 76
4.4.3 Electronics of the Homodyne Detection 77
4.5 Time and Polarization Multiplexing 77
4.6 Optical Component Characteristics Summary 78
4.7 Acquisition and Control Cards 78
4.8 Random Numbers 80
4.9 Computing Power 84

5 Preventing Calibration Attacks on the Local Oscillator in Continuous-Variable Quantum Key Distribution 85
5.1 Theoretical Security vs Practical Attacks 85
5.2 Security assumptions and calibration techniques 86
5.3 Description of the local oscillator calibration attack 88
5.4 Analysis of the excess noise 90
5.5 A quantitative example 92
5.6 Countermeasure: real-time shot noise measurement techniques 92
5.7 Conclusion 94

6 Increasing the Range of CVQKD 97
6.1 Theory of Reconciliation of Gaussian Variables 98
6.2 Reconciliation of Gaussian Variables: Implementation with LDPC Codes 99
6.2.1 Simulation Results with Rotations 101
6.2.2 Use of rotations in higher dimension spaces 102
6.2.3 Dealing with a continuous range of SNR with puncturing, shortening and repetition 104
6.3 Practical use for a continuous-variable quantum key distribution system 105
6.4 A rate 1/50 multi-edge LDPC code 107
6.5 Puncturing / shortening performance 108
6.6 Conclusion 108

7 Experimental Demonstration of Long-distance CVQKD 111
7.1 Outlook of the Experiment 113
7.2 Experimental Results 114
7.3 Security Conditions 117
7.4 Multidimensional Reconciliation 117
7.5 Local Oscillator Manipulation 117
7.6 Hardware Stability 118
7.7 Post-processing Performance 118
7.8 Conclusion and Perspectives 119

8 Increasing the Speed of CVQKD 121
8.1 Effect of an imperfect error correction step in QKD 121
8.1.1 Secret key rate and error correction 122
8.1.2 Previous work 124
8.2 Polar codes for QKD: efficiency vs. block sizes 124
8.3 Decoding speed: numerical results 126
8.4 Privacy amplification 128
8.5 Network Bandwidth Consumption 129
8.6 Several Bits per Pulse 130

9 Integration of CVQKD in Optical Networks 131
9.1 QKD and Network Infrastructures 131
9.2 SEQURE demonstration field test 134
9.2.1 Structure of the demonstration 134
9.2.2 The quantum layer 136
9.3 Security considerations 138
9.4 Performance of the quantum layer 139
9.4.1 Events 139
9.4.2 Excess noise 139
9.4.3 Secret key rate 142
9.5 Performance of the encryption layer 142
9.6 SEQURE Demonstration Conclusion and Perspectives 142
9.7 Analysis of the Noise Contributions in a WDM Setup 143
9.7.1 Leakage from Classical Channels 144
9.7.2 Four-wave Mixing 145
9.7.3 Spontaneous Anti-Stokes Raman Scattering 145
9.8 Noise Photons in Local Oscillator Matched Mode 145
9.9 Experimental Results 146
9.10 Concluding Remarks 147

A Matrix Representation of the Octonions 151

B Local Oscillator Power Measurement and Clock Signal Generation 153

C Post-processing Scheduling 155

List of Abbreviations 159

Bibliography 161

List of Figures

1 Cygnus: a quantum key distribution product commercialized by SeQureNet. 5

1.1 Cumulative number of publications concerning QKD systems imperfections and attacks on QKD systems. 13

2.1 Shannon's coding theorem schematics. 21
2.2 Binary symmetric channel transition probabilities. 21
2.3 Additive white Gaussian noise channel schematic. 22

3.1 Discretization grid used to approximate a Gaussian modulation in phase space. 54
3.2 Secret key rate for collective attacks including finite-size effects and calibration imperfections with respect to the distance for different values of the number of samples. 62
3.3 Experimental evaluation of the phase noise. 65
3.4 Secret key rate for collective attacks in the asymptotic regime. 66

4.1 Generic optical fiber design. 68
4.2 Cross section of a Panda type PM fiber. 69
4.3 Schematics of the principle of a LiNBO_3 optical modulator. . 71
4.4 Measured voltage on Alice's photodiode with respect to the voltage applied to the amplitude modulator. 72
4.5 Alice's photodiode answer to a ramp voltage at selected times during a 24 hours period. 73
4.6 Alice's photodiode mean and standard deviation during 20 hours when no feedback control of Alice's amplitude modulator is used. 73
4.7 Alice's photodiode mean and standard deviation during 20 hours when Alice's amplitude modulator feedback is used. . . 74
4.8 Principle of the homodyne detection. 75
4.9 Schematics of the homodyne detection electronics. 77
4.10 Alice's optical device clock signals. 79
4.11 Alice's input and output data. 79
4.12 Bob's device clock signals. 80
4.13 Bob's input and output data. 80
4.14 Bytes statistics with Salsa PRNG for a 1Gb dataset. 83
4.15 Bytes statistics with an aged physical RNG for 1 Gb dataset. 83

5.1 Local oscillator experimental measurement procedure. 87
5.2 Profile of the trigger signal generated at Bob's site depending on the shape of the local oscillator pulse. 88

5.3 Differential signal obtained by the homodyne detector for several modulated quadratures. 89
5.4 Impact of a delayed trigger on the statistics of the homodyne detection. 90
5.5 Real-time shot noise measurement procedures protecting a CVQKD system against a local oscillator calibration attack. 93
5.6 Impact of the real-time shot noise measurement countermeasure on the secret key rate. 95

6.1 Ratios between the capacities of the multidimensional channels ($d = 1, 2, 4, 8$) and the BIAWGNC and between the BI-AWGNC and the AWGNC with respect to the SNR. 102
6.2 Optimal modulation variance with respect to the distance. . . 106
6.3 Secret key rate for collective attacks with respect to the SNR. 106
6.4 Secret key rate for collective attacks with respect to the SNR. 107
6.5 Secret key rate for collective attacks with respect to the distance. 108
6.6 Efficiency of a rate 0.5 LDPC code on the BIAWGNC with respect to noise. 109

7.1 Optical layout of the long-distance CVQKD prototype. 112
7.2 Key rate produced by the system after error correction and privacy amplification during 24 hours. 115
7.3 Experimental excess noise measured during 24 hours with a SNR of 0.17 on Bob's side. 116

8.1 Polar codes efficiency for the BSC for probability errors from 1% to 11% with a 1% step. 126
8.2 Polar codes efficiency for the AWGNC for the SNRs 1.097, 0.161, 0.075, 0.029 from [65]. 127
8.3 Privacy amplification performance on recent CPUs for the implementation of the universal hash family ”multiplication by a random Toeplitz matrix”. 129

9.1 Map of the SEQURE demonstration. 133
9.2 Layer structure of the SEQURE demonstration. 135
9.3 Structure of the SEQURE demonstration. 135
9.4 Optical layout of the CVQKD prototype. 136
9.5 Secret key rate and excess noise during the SEQURE demonstration. 140
9.6 Keys produced during the SEQURE demonstration. 141
9.7 Generic WDM setup. 144
9.8 Theoretical noise induced by a 1 mW classical channel on the homodyne detection. 147
9.9 Operational cost of a QKD deployment over the lifespan of an equipment. 148

B.1 Trigger generation with respect to pulses shapes. 154

C.1 Flow diagram of Alice and Bob post-processing. 157

List of Tables

1.1 Comparison between DVQKD and CVQKD in 2010. 12

4.1 Transmission windows ranges and operating wavelengths of optical fibers with a silica core. 69
4.2 Components used in our experimental setup with their respective insertion losses excluding connection losses at 1550nm. 79
4.3 Amount of randomness per pulse required by Alice and Bob in a usual implementation of a CVQKD protocol. 82

6.1 Multi-edge LDPC codes asymptotic efficiencies. 101
6.2 SNR thresholds on the BIAWGNC for low rate multi-edge LDPC codes (size 2^{20}) using the multidimensional reconciliation scheme ($d = 1, 2, 4, 8$). 101
6.3 Efficiencies (w.r.t. the BIAWGNC capacity) for low rate multi-edge LDPC codes (size 2^{20}) using the multidimensional reconciliation scheme ($d = 1, 2, 4, 8$). 102
6.4 SNR thresholds and channel efficiencies on the BIAWGNC for a rate 1/2 multi-edge LDPC code with respect to the dimension of the multidimensional reconciliation scheme. . . . 104
6.5 SNR thresholds and channel efficiencies on the AWGNC of the multi-edge LDPC codes mentioned in this chapter. 105

8.1 Polar codes decoding speeds on the BSC and the BIAWGNC. 126
8.2 LDPC codes decoding speeds with LDPC codes described in [32] for the BSC and in [113] for the BIAWGNC. 127
8.3 LDPC codes decoding speeds with LDPC codes described in [32] for the BSC and in [113] for the BIAWGNC. 128
8.4 Network traffic for the Gaussian CVQKD protocol used in Cygnus. 130

9.1 SEQURE demonstration link characteristics. 134
9.2 Parameters used for the computation of the secret key rate against collective attacks in the realistic model in a WDM setup. 146
9.3 Experimental parameters of the experimental demonstration of the coexistence between a classical channel and CVQKD on a single optical link. 147
9.4 Experimental excess noise measurements in coexistence with a classical channel. 148
9.5 Evolution of CVQKD performance between 2010 and 2013. . 150

Résumé en français

Cette thèse étudie la sécurité pratique et les performances de la distribution quantique de clés à variables continues. La distribution quantique de clés est une primitive cryptographique qui permet à deux intervenants distants, Alice et Bob, de partager une clé binaire inconnue de tout potentiel attaquant présent lors de l'établissement de la communication. Une fois cette clé obtenue, Alice et Bob peuvent communiquer de façon confidentielle en combinant un bit de clé et un bit de message à transmettre et en ne réutilisant jamais le bit de clé utilisé. Cet algorithme de chiffrement, appelé le *masque jetable* ou *one-time-pad* est prouvé sûr au sens de la théorie de l'information.

Ce schéma semble résoudre le problème de la transmission de messages de façon confidentielle mais présente plusieurs difficultés pratiques qui expliquent son utilisation peu répandue. Premièrement, les meilleurs débits accessible avec les technologies actuelles de distribution quantique de clés sont de l'ordre du megabit par seconde, ce qui reste plusieurs ordres de grandeurs en dessous des débits de communications optiques utilisés dans les infrastructures réseaux actuelles. Ensuite, la sécurité de ce mécanisme repose entièrement sur la sécurité de la clé utilisée. Il est donc nécessaire de pouvoir quantifier de façon précise la sécurité de la clé produite par le dispositif de distribution quantique de clé utilisé. En effet, des démonstrations d'espionnage partiel ou total de clés produites par des équipements de distribution quantique de clés commerciaux ont déjà é té réalisées.

En dehors du débit et de la sécurité pratique des clés produites, la distance maximale de sécurité est le facteur de mérite le plus pertinent pour caractériser un système de distribution quantique de clés. En effet, contrairement aux communications classiques qui ne sont pas limitées en distance en raison de l'utilisation d'amplificateurs erbium par exemple, les états quantiques ne peuvent être régénérés sans détruire l'information portée par ces états et les communications quantiques sont donc fondamentalement limitées en termes de distance. Dans le cas des systèmes de distribution quantique de clés à variables discrètes, les records actuels de distance sont de l'ordre de 250 km en laboratoire et inférieurs à 100 km pour des systèmes commerciaux. La distribution quantique de clés à variables continues n'a jamais été démontrée sur des distances supérieures à 25 km en laboratoire. Cette technologie présente néammoins certaines caractéristiques intéressantes. D'une part, elle peut être implémentée en employant uniquement des composants standards optimisés pour les télécommunications optiques classiques, d'autre part, elle présente un dispositif de détection particulièrement adapté à un fonctionnement en coexistence avec plusieurs canaux optiques sur la même fibre optique.

Dans cette thèse nous levons la limitation de distance de la distribution quantique de clés à variables continues en développant des codes correcteurs

efficaces dans des régimes de bas rapport signal à bruit qui correspondent à de grandes distances de transmission. Nous implémentons un système expérimental stable qui nous permet d'extraire des clés de blocs de grande taille, ce qui est nécessaire pour s'affranchir du bruit statistique qui affecte l'estimation des paramètres du canal quantique, et ce particulièrement pour de grandes distances de transmission. Nous levons également la limitation de débit de cette technologie en implémentant un post-traitement rapide qui tire notamment partie d'architectures matérielles modernes comme les processeurs graphiques. Nous considérons différentes imperfections expérimentales de notre système pouvant donner lieu à des attaques par canaux cachés et proposons différentes approches comme l'implémentation de contre-mesures ou l'intégration de ces imperfections dans les preuves de sécurité. Enfin, nous envisageons différents contextes d'intégration de notre système dans les infrastructures réseaux actuelles. Tout d'abord, nous démontrons la stabilité de notre système sur une période de plusieurs mois sur une fibre de 17.7 km installée sur le terrain, en combinaison avec des chiffreurs symétriques commerciaux de la société Thales. Puis, nous multiplexons en longueur d'onde un canal classique intense sur le même lien fibré que notre canal quantique et obtenons néammoins des taux de clé secrètes pratiques sur une fibre de 25 km.

Chapitre 1 : De la cryptographie classique à la cryptographie quantique

Après un rapide rappel historique de l'évolution des techniques cryptographiques, le premier chapitre de ce manuscrit dresse un panorama des primitives cryptographiques usuelles. Les techniques de cryptographie dites classiques sont regroupées en deux grandes familles, la cryptographie à clé privée ou symétrique et la cryptographie à clé publique ou asymétrique.

Les techniques de cryptographie symétrique sont caractérisées par le partage d'une clé commune entre les deux protagonistes de la communication. Cette clé sert à la fois au chiffrement et au déchiffrement des messages. En cryptographie moderne, la sécurité d'un dispositif de chiffrement ne doit pas reposer sur la confidentialité de l'algorithme de chiffrement mais sur celle de la clé de chiffrement. La clé de chiffrement doit être un élément d'un espace suffisamment grand pour éviter les attaques par force brute qui consistent pour un attaquant en essayer toutes les clés possibles pour déchiffrer un message. Pour cela il est nécessaire d'avoir un critère qui permette de reconnaître un message déchiffré. Puisque la sécurité du chiffrement repose sur la clé de chiffrement, il convient de stocker la clé de façon sécurisée, notamment à l'aide de cartes à puce, et de disposer d'un moyen sûr de partager la clé entre les protagonistes de la communication. Cette dernière tâche est particulièrement délicate et ce d'autant plus que le nombre de clés à partager augmente avec le carré du nombre de protagonistes.

La cryptographie asymétrique appelée également cryptographie à clé publique apporte une réponse satisfaisante à ce dernier point. Chaque participant dispose d'un couple de clés, une clé privée qu'il garde secrète et une clé publique qui est diffusée par exemple sur Internet. La clé publique est utilisée par un protagoniste pour chiffrer les données qu'il souhaite transmettre au détenteur de la clé secrète correspondante. Seul le destinataire légitime pourra déchiffrer ce message au moyen de la clé secrète qu'il est le seul à connaître. Cette famille de primitives cryptographiques permet de résoudre le problème de la distribution de clé secrètes. En revanche, les clés publiques doivent être distribuées de façon authentique. Cela nécessite en général l'intervention d'un tiers de confiance. Les autorités de certification ou infrastructures à clé publiques (PKI pour Public Key Infrastructure) jouent le rôle de ce tiers de confiance. Une autre limitation de la cryptographie à clé publique est que la sécurité des primitives employées repose sur des hypothèses calculatoires. Par exemple, la puissance de calcul à disposition d'un espion est supposée être limitée ou certains problèmes mathématiques sont supposés ne pas pouvoir être résolus en temps polynomial.

En ce qui concerne les menaces concernant la sécurité de ces primitives, certaines tendances semblent se dégager. D'une part, la sécurité des primitives asymétriques repose majoritairement sur un nombre restreint de problèmes mathématiques bien identifiés, comme par exemple la factorisation, d'autre part, les primitives symétriques présentent moins de structure. Les avancées algorithmiques ou mathématiques semblent donc menacer plus directement les primitives asymétriques que les primitives symétriques. Un ordinateur quantique permettrait ainsi par exemple de factoriser les grands nombres en temps polynomial. Une conséquence de cela est qu'une primitive reposant sur la factorisation des grands nombres, comme par exemple RSA, ne présente pas les meilleures garanties de sécurité pour des données qui doivent rester confidentielles à long terme. En effet, un espion pourrait se contenter d'enregistrer toutes les communications aujourd'hui dans l'attente d'avoir à sa disposition un ordinateur quantique et de pouvoir alors déchiffrer une grande quantité de données passées.

La distribution quantique de clés permet de partager une clé commune aux deux extrémités d'un lien optique sans faire aucune hypothèse sur les moyens à disposition de l'espion avec pour seule exigence que les deux protagonistes de l'échange aient accès à un canal authentique. Des signaux quantiques sont envoyés sur le canal physique qui sépare les deux protagonistes et le principe de non-clonage d'états quantiques empêche tout attaquant de dupliquer l'information envoyée sur ce canal : toute tentative d'un attaquant d'interagir avec les états quantiques pour acquérir de l'information sur ces états introduit du bruit qui est détecté par les protagonistes de la distribution quantique de clés lors d'une étape d'estimation des paramètres du canal. Les statistiques du canal portent la signature de la présence d'un attaquant. Il existe deux familles de protocoles de distribution quantique de clés, les protocoles à variables discrètes et les protocoles à variables continues. Les protocoles à variables discrètes encodent l'information dans des variables discrètes comme la phase ou la polarisation de photons uniques tandis que les protocoles à variables continues encodent l'information dans des variables continues comme les quadratures du champ électromagnétique. Les quantités considérées étant de nature différente, les preuves de sécurité concernant ces deux familles de protocoles font intervenir des outils différents et il en est de même en ce qui concerne les dispositifs pratiques qui permettent de mettre en oeuvre ces protocoles.

Bien qu'il existe des preuves de sécurité prenant en compte les attaques les plus générales autorisées par les lois de la mécanique quantique, la sécurité pratique des dispositifs de distribution quantique de clés pose de nombreux problèmes. En effet, la distance entre la description théorique d'un protocole auquel s'applique la preuve de sécurité, et sa réalisation pratique, peut ouvrir la voie à des attaques non prises en compte dans les preuves de sécurité. Il s'agit des attaques par canaux cachés. Tout comme il existe un domaine de la cryptanalyse classique qui a trait aux défauts d'implémentations pratiques des systèmes de cryptographie classique, et en particulier les attaques par canaux cachés sur les cartes à puce, les imperfections des dispositifs pratiques de distribution quantique de clés ont vu naître un nouveau domaine de recherche très actif depuis le milieu des années 2000, la cryptanalyse quantique (ou quantum hacking). De façon peu surprenante, les menaces sur les systèmes de distribution quantiques de clés sont donc à chercher plutôt du côté des implémentations pratiques que des preuves de sécurité théoriques.

Nous concluons ce chapitre en présentant succinctement les autres primitives cryptographiques pouvant être implémentées avec les dispositifs quantiques actuels. Le tirage à pile ou face quantique permet à deux protagonistes distants et ne se faisant pas confiance de se mettre d'accord sur une valeur binaire. Il est connu que l'une ou l'autre des parties peut biaiser la valeur du tirage à pile ou face avec une grande probabilité sauf moyennant des hypothèses de type calculatoires. L'utilisation d'états quantiques permet de limiter la valeur du biais à une valeur limite de $\frac{1}{\sqrt{2}}$. En pratique, les imperfections des dispositifs quantiques ne permettent pour l'instant pas de démontrer un avantage quantique sur des distances compatibles avec les infrastructures de communication actuelles. La signature quantique permet à l'instar de la signature classique d'empêcher la production d'un certain document par un intervenant non légitime. La signature classique repose sur des hypothèses de difficulté calculatoire, dont certaines sont remises en cause par la mise à disposition d'un ordinateur quantique. La signature quantique permet quant à elle de résister à un attaquant en possession d'un ordinateur quantique. Elle fait appel à des fonctions à sens unique quantiques, qui ne peuvent être inversées, et cela même par un ordinateur quantique. Cependant l'utilisation de ces fonctions introduit des limitations de plusieurs types : le nombre de signatures qui peuvent être produites est limité, ces signatures ne peuvent pas être produites par un autre intervenant, et il est difficile d'assurer que deux intervenants testant la validité d'une signature obtiendront bien le même résultat.

Chapitre 2 : Information quantique avec des variables Gaussiennes

Ce chapitre présente le cadre théorique et les principaux outils mathématiques nécessaires à l'étude de la sécurité de la distribution quantique de clés à variables continues. Nous y introduisons dans un premier temps les postulats fondamentaux de la mécanique quantique.

Puis nous nous intéressons aux outils de base de la théorie de l'information avec des variables classiques. Ce domaine des mathématiques est considéré comme étant né en 1948 avec une publication de Claude Shannon dans laquelle il introduit la notion d'entropie pour quantifier la quantité d'information qui peut être transmise par des variables aléatoires. Le premier théorème de Shannon décrit la quantité d'information minimale qui est nécessaire pour décrire une variable aléatoire. Il s'agit de l'entropie de cette variable aléatoire. La compression d'une sources de données qui peut être décrite par une variable aléatoire dont on peut calculer l'entropie ne peut se faire sans perte de données au delà d'une certaine quantité qui est égale à l'entropie de cette source de données.

Le deuxième théorème de Shannon décrit la quantité maximale d'information par symbole qui peut être transmise sur un certain canal de communication défini par un certain niveau de bruit. Il s'agit de la capacité de ce canal. Pour un canal sans mémoire, c'est à dire pour lequel la variable aléatoire à la sortie du canal à tout instant ne dépend que de la variable aléatoire en entrée de ce canal à ce même instant, la capacité du canal est égale au maximum, pris sur toutes les distributions possibles en entrée du canal, de l'information mutuelle entre les variables aléatoires d'entrée et de sortie. Nous nous intéressons aux capacités de quelques canaux classiques tels que le canal binaire symétrique ou le canal à bruit additif Gaussien.

Une fois introduite la notion de capacité d'un canal bruité, le problème de transmettre des données de façon fiable sur ce canal en présence de bruit reste entier. La réponse à cette question est d'ajouter de la redondance aux données que l'on souhaite transmettre. En effet, lorsque l'on envoie plusieurs fois la même information sur un canal bruité, le bruit qui correspond à une variable aléatoire se manifeste de façon différente lors des différentes transmissions. Il est donc possible de reconstruire le message envoyé à partir de plusieurs observations indépendantes du message reçu. En pratique, il est possible d'envoyer des mots de code au lieu d'envoyer plusieurs fois le même message. On établit pour cela une correspondance entre l'ensemble des messages que l'on souhaite envoyer et un ensemble de mots de code qui sont de longueur plus grande que ces messages. Le ratio entre ces deux quantités définit le taux du code correcteur d'erreur. Le second théorème de Shannon énonce que pour tout taux inférieur à la capacité du canal, il existe une stratégie d'encodage et de décodage qui permet de transmettre de l'information avec une probabilité d'erreur asymptotiquement faible pour des blocs de données de grande taille.

Il n'est pas aisé de construire des codes correcteurs d'erreurs de taux proches de la capacité du canal pour tout type de canal. Les codes LDPC ou les codes polaires permettent d'atteindre la capacité d'un canal pour des blocs de taille arbitrairement grande. En revanche, les stratégies d'encodage et de décodage deviennent algorithmiquement peu efficaces lorsque le taux du code s'approche de la capacité du canal. Dans le chapitre 6, nous construisons des codes LDPC multi-edge avec des taux très proches de la capacité du canal pour des bruits élevés pour le canal à entrée binaire et bruit additif Gaussien. Le chapitre 8 propose une comparaison des performances de codes LDPC multi-edge et de codes polaires pour les canaux utiles pour la distribution quantique de clés. Une implémentation sur processeur graphique est réalisée pour accélérer la vitesse de décodage des codes LDPC multi-edge.

Ensuite, nous présentons différents types d'états quantiques et leurs caractéristiques. Parmi les états monomodes, on distingue les états de Fock, qui sont des états dont le nombre de photons est parfaitement déterminé. Au contraire, les états cohérents n'ont pas un nombre de photons déterminé et n'ont pas une phase totalement aléatoire. Le produit de l'incertitude sur leurs quadratures correspond au minimum autorisé par les lois de la mécanique quantique. Ils sont donc très proches des états classiques. Les états comprimés présentent quant à eux des degrés d'incertitude différents entre leurs quadratures contrairement aux états cohérents. Il est également possible de produire des états comprimés à deux modes qui sont des états pour lesquels la lumière à deux fréquences différentes est corrélée.

Les états Gaussiens sont particulièrement intéressants car ils sont entièrement déterminés par leurs deux premiers moments statistiques. La matrice de covariance des états Gaussiens est donc suffisante pour les décrire. De plus, l'entropie des états Gaussiens peut être calculée grace à sa décomposition sur les états thermiques. Nous donnons les bases d'analyse symplectique qui nous permettront de calculer l'entropie des états qui interviennent lors de la dérivation des preuves de sécurité du protocole Gaussien dans le chapitre 3. Enfin nous décrivons les opérations Gaussiennes, qui sont les opérations qui transforment un état Gaussien en état Gaussien. Ces opérations seront également employées dans le chapitre 3.

Chapitre 3 : La distribution quantique de clés avec des variables continues

Ce chapitre est consacré à l'étude théorique de la sécurité des protocoles de distribution quantique de clés à variables continues. Le but de la distribution quantique de clés est de produire des clés cryptographiques, c'est à dire des chaînes binaires aléatoires secrètes, entre les deux participants du protocole. Ces clés étant destinées à être utilisées dans des applications cryptographiques diverses, telles que le chiffrement ou l'authentification, il est nécessaire de définir un critère de sécurité concernant les clés issues d'un protocole de distribution quantique de clés. Nous donnons la définition universelle de sécurité d'une clé : une clé est dite $\epsilon-sure$ si elle est uniformément distribuée et indépendante de l'espion sauf avec une probabilité ϵ.

Nous rappelons ensuite les principales étapes d'un protocole général de distribution quantique de clés. La première étape est l'échange quantique, étape durant laquelle Alice et Bob échangent des états quantiques à travers le canal quantique (qui n'est autre qu'un medium physique de communication tel qu'une fibre optique ou l'air libre) et réalisent des mesures sur ces états. Suite à cet échange, Alice et Bob communiquent à travers un canal public (mais de façon authentique).

Après un bref rappel de l'évolution historique des protocoles de distribution quantique de clés, nous décrivons en détails le protocole GG02 qui est un protocole de distribution quantique de clés à variables continues dans lequel Alice module des états cohérents dans l'espace des phases avec une distribution Gaussienne bidimensionnelle. Cette thèse s'intéresse particulièrement à la sécurité pratique du protocole GG02. Nous dressons donc une première liste des potentielles imperfections que peut présenter une implémentation pratique du protocole GG02.

La sécurité du protocole GG02 est établie contre les attaques collectives. Cette preuve de sécurité s'étend contre les attaques les plus générales, les attaques cohérentes, dans le cas où l'on considère un nombre infini d'échantillons. Nous rappelons la preuve de sécurité contre les attaques collectives. Dans le cas le plus général, le taux de clé secrète en réconciliation inverse (c'est à dire où les mesures de Bob et non les mesures d'Alice servent de référence pour l'établissement de la clé secrète) entre Alice et Bob est égal à l'information mutuelle classique sur le canal entre Alice et Bob moins l'information de Holevo entre Bob et Eve. Un argument d'optimalité nous permet de nous restreindre à calculer cette information de Holevo pour l'état Gaussien bimode dont la matrice de covariance correspond aux statistiques observées sur le canal. Puis, nous raffinons successivement cette preuve de sécurité pour y intégrer différentes imperfections qui affectent un dispositif expérimental de distribution quantique de clés.

La première de ces imperfections a été bien étudiée pour les protocoles à variables discrètes comme pour les protocoles à variables continues. Il s'agit de l'imperfection de la procédure de correction d'erreurs. En effet, bien qu'il soit en théorie possible d'atteindre la capacité d'un canal, il n'existe pas de codes correcteurs d'erreurs connus qui atteignent cette capacité pour des échantillons de taille finie. Cette imperfection ne menace pas la sécurité du protocole GG02, sous réserve que l'information révélée lors de la procédure de correction d'erreurs soit bien prise en compte lors de l'évaluation du taux de clé secrète. Cela se matérialise par un coefficient β inférieur à 1 qui intervient en facteur de l'information mutuelle entre Alice et Bob. En revanche, plus la distance entre la capacité du canal et la fraction d'information mutuelle réellement extraite par Alice et Bob devient grande, moins le taux de clé secrète est élevé. La limitation en distance des protocoles à variables continues a longtemps été due à la difficulté de mettre en place des procédures de correction d'erreurs efficaces dans des régimes de bas rapport signal à bruit.

Une autre source d'imperfections déjà étudiée correspond aux imperfections liées au dispositif de détection cohérente. Dans notre cas, il s'agit d'une détection homodyne. Un signal intense cohérent avec le signal quantique joue à la fois le rôle d'amplificateur dans le domaine optique et de référence de phase. Un modulateur de phase situé sur la voie de l'oscillateur local permet de choisir librement de mesurer toute quadrature du champ. Dans le cas où aucun signal quantique n'est présent, un tel dispositif permet de mesurer les fluctuations quantiques du vide qui sont alors linéaires en la puissance de l'oscillateur local. En pratique, même en l'absence d'oscillateur local, le signal mesuré par le circuit électronique d'amplification du signal et les cartes d'acquisition subséquentes n'est pas nul : un bruit électronique résiduel est toujours présent. Le dispositif de détection présente également une efficacité quantique limitée. En effet, les pertes du dispositif récepteur se décomposent en plusieurs facteurs : l'efficacité des photodiodes, les pertes optiques en ligne du dispositif récepteur et la visibilité de l'interféromètre. Il est possible de définir un mode dit réaliste dans lequel l'on suppose que l'attaquant ne peut contrôler ni les pertes de Bob ni le bruit électronique ajouté par la détection homodyne. Dans ce cas là, le taux de clé secrète est très peu affecté par ces imperfections du dispositif récepteur.

Nous étudions ensuite l'imperfection liée à la réalisation pratique de la modulation Gaussienne théorique que doit générer Alice. Une telle distribution ne peut être générée parfaitement en raison de la quantité finie d'alea à disposition et de l'amplitude de modulation finie qui est réalisable avec des cartes de contrôle générant des signaux discrets et des modulateurs de dynamique finie. Intuitivement, l'effet discret de la modulation Gaussienne pratique n'est pas gênant en raison de la présence du bruit de photon qui empêche de distinguer parfaitement deux états cohérents. Pour quantifier cette imperfection de manière rigoureuse, nous considérons la distance trace entre le mélange Gaussien idéal (qui correspond à un état thermique) et le mélange discret d'états cohérents réalisé en pratique. Si cette distance est bornée, l'attaquant ne peut distinguer le mélange idéal du mélange pratique qu'avec une probabilité bornée par cette distance trace. Nous avons simulé numériquement les approximations réalistes de la distribution Gaussienne, en coordonnées cartésiennes et en coordonnées polaires, et avons obtenu des bornes de sécurité compatibles avec les niveaux de sécurité attendus en distribution quantique de clés.

Un autre problème longtemps passé sous silence lors de l'étude de la sécurité de dispositifs de distribution quantique de clés, que ce soit à variables discrètes ou à variables continues, est l'estimation des paramètres entrant en compte dans l'évaluation du taux de clé secrète. De nombreuses preuves de sécurité dites en régime asymptotique considèrent que ces paramètres sont connus avec une précision infinie, en raison du nombre infini d'échantillons qui sont censés être échangés entre Alice et Bob. Un dispositif pratique ne peut bien sûr pas travailler avec des échantillons de taille infinie. Nous étendons une première analyse des effets de taille finie réalisée pour les protocoles de distribution quantique de clés à modulation discrète au cas du protocole à modulation Gaussienne et nous incluons dans l'analyse l'effet d'une imparfaite estimation du bruit électronique et de l'efficacité de la détection homodyne. Il apparaît que l'effet le plus pénalisant est l'incertitude concernant l'excès de bruit introduit par le canal quantique. Afin d'avoir une bonne précision concernant ce paramètre, des blocs de données de taille importante doivent être considérés. En pratique, une telle contrainte peut limiter le taux de clé à quelques dizaines de kilomètres, en raison de la difficulté de conserver des paramètres stables sur des longues périodes de temps. Ce problème peut être résolu en augmentant significativement la fréquence de répétition du dispositif optique mais il convient alors de réaliser des progrès algorithmiques concernant le post-traitement des données qui limite actuellement le débit des dispositifs de distribution quantique de clés à variables continues. Nous verrons dans le chapitre 8 que la vitesse de post-traitement peut ê tre considérablement augmentée en implémentant la correction d'erreurs sur cartes graphiques ou en utilisant d'autres types de codes correcteurs d'erreurs tels que les codes polaires.

Enfin, de la même façon que la calibration du dispositif de détection de Bob permet d'augmenter le taux de clé secrète, nous proposons de prendre en compte le bruit de phase lors de la préparation des états d'Alice dans la preuve de sécurité. Ce bruit de phase peut être modélisé comme une mesure imparfaite côté Alice. Les données classiques mesurées par Alice sont donc bruitées en raison du bruit de phase et cela a pour conséquence de dégrader l'information mutuelle entre Alice et Bob. En revanche, l'attaquant ne peut pas acquérir plus d'information concernant les résultats de mesure de Bob, qui servent de référence pour l'établissement de la clé dans un protocole à réconciliation inverse. Il est donc possible de retrancher la valeur du bruit de phase de la valeur de l'excès de bruit lors du calcul de l'information mutuelle entre Eve et Bob. Dans ce cas, le taux de clé secrète augmente. Pour pouvoir utiliser cette technique, il est impératif de mesurer le bruit de phase d'Alice expérimentalement. Nous proposons une méthode pour mesurer le bruit de phase à l'aide d'une détection homodyne, que ce soit lors d'une phase de calibration préalable au déploiement du système de distribution quantique de clés à variables continues ou bien en cours de fonctionnement. Dans les deux cas, il est nécessaire de supposer que l'attaquant ne peut pas interférer avec le dispositif d'Alice, auquel cas cette estimation du bruit de phase pourrait être faussée et une surestimation de la valeur du bruit de phase conduirait à une surestimation du taux de clé secrète. Nous avons pu mesurer une valeur expérimentale du bruit de phase. Dans des conditions d'excès de bruit relativement pessimistes où l'excès de bruit côté Alice est de l'ordre de 2.5% en unité de bruit de photon, il est ramené à une valeur de 1.75% après soustraction du bruit de phase. Dans le cas d'un espion limité aux attaques collectives et en régime asymptotique, la distance maximale de sécurité est alors augmentée de 40 km.

Chapitre 4 : Réalisation expérimentale

Ce chapitre est consacré à l'étude des caractéristiques des différents éléments qui composent notre système expérimental de distribution quantique de clés à variables continues avec des fibres optiques.

Nous présentons tout d'abord les principales caractéristiques des fibres optiques. Une fibre optique est en général constituée de silice et à symétrie cylindrique. Elle possède en son centre un milieu d'indice optique élevé qui est entouré d'un milieu d'indice optique plus faible. Cette structure a pour conséquence de confiner la lumière entre ses points d'entrée et de sortie. Il existe différents types de fibre. Les fibres multi-modes autorisent plusieurs chemins de propagation tandis que les fibres monomodes ne laissent se propager qu'un seul mode du champ électromagnétique. Quel que soit le type de fibre utilisé, il existe une limite fondamentale de propagation due à la réduction de l'intensité de la lumière au cours de sa propagation en raison notamment d'impuretés dans les fibres optiques. Le maximum d'intensité transmise correspond à une longueur d'onde de 1550 nm, ce qui explique pourquoi cette longueur d'onde est utilisée pour les télécommunications à grande distance. Par ailleurs, les fibres monomodes standards ne conservent pas la polarisation et toute torsion de la fibre peut causer une différence d'index effectif entre les différentes polarisations de la lumière. Nous utilisons pour remédier à cela des fibres à maintien de polarisation pour la plupart des composants de notre système. Un autre critère important dans un montage fibré est la qualité des connexions entre les différents composants. Nous utilisont des connecteurs à ferrules et des fibres polies avec un angle (APC pour Angled Physical Contact) pour empêcher la lumière réfléchie à l'endroit de la connexion de se rétropropager.

En ce qui concerne la source laser, noua avons opté pour une source laser à contre-action répartie (DFB pour Distributed Feedback). Une telle source offre l'avantage d'avoir un spectre relativement étroit, de l'ordre de 1 MHz en régime continu, et d'avoir une longueur d'onde réglable en ajustant la température. Cette propriété est particulièrement intéressante pour pouvoir fonctionner dans un contexte de multiplexage en fréquence avec d'autres canaux classiques (cet aspect est abordé dans le chapitre 9) car les multiplexeurs et démultiplexeurs commerciaux sont alignés sur des grilles de longueurs d'onde standards. En revanche, nous n'utilisons pas cette diode laser en régime continu mais en régime impulsionnel et la largeur spectrale est donc plutôt de l'ordre de 12.5 GHz dans ce régime. Le régime impulsionnel nous permet d'atteindre des extinctions quasi totales et donc une meilleure séparation des impulsions, ce qui est nécessaire car nous utilisons un multiplexage temporel d'un signal intense et d'un signal faible. Ainsi, toute fuite du signal intense sur le signal faible ajoute un bruit important à notre système.

Concernant la modulation du signal quantique, nous utilisons des modulateurs électro-optiques au Niobate de Lithium spécialement optimisés pour les télécommunications à haut débit. Ils permettent d'opérer une modulation à des fréquences de l'ordre de plusieurs dizaines de GHz mais nous ne les utilisons qu'à des fréquences de l'ordre du MHz. Ils peuvent êtres pilotés avec des tensions faibles et la tension de biais qui correspond à la tension à appliquer pour produire une extinction maximale ne dérive pas très vite avec le temps et la température. Nous pouvons donc implémenter un rétrocontrôle qui nous permet de retrouver la valeur de cette tension de biais et de contrôler l'intensité de modulation avec une bonne précision.

Afin de mesurer les quadratures du champ électromagnétique, nous utilisons un dispositif spécifique qui nous permet de mesurer un terme proportionnel à une quadrature et non un terme proportionnel au nombre de photons comme un détecteur de photons ou une photodiode avec son circuit d'amplification. Un tel dispositif est une détection homodyne. Il repose sur un principe d'interférence entre un signal optique intense et un signal optique faible, notre signal quantique, sur une lame séparatrice équilibrée. Le signal intense, appelé oscillateur local, joue à la fois le rôle d'amplificateur dans le domaine optique et de référence de phase. Une modulation de la phase du signal intense nous permet de choisir la quadrature du champ que l'on souhaite mesurer. Après interférence, les intensités optiques des deux voies sont transformées en courants par des photodiodes puis sont directement soustraites par loi des noeuds. Nous présentons les équations de base de la détection homodyne qui montrent que le signal de différence des photocourants est proportionnel à la quadrature du champ signal faible, et ses principales sources d'imperfection. L'équilibrage de la lame séparatrice doit être d'autant plus précis que l'intensité de l'oscillateur local est importante. Les différentes pertes de la détection homodyne, qui sont les pertes optiques, l'efficacité des photodiodes et l'adaptation des modes entre l'oscillateur local et le signal, sont modélisées par l'introduction d'une lame séparatrice qui couple le mode signal avec le mode vide. Dans le cas où aucun champ signal n'est introduit sur la voie signal, les équations de la détection homodyne prédisent une relation linéaire entre la variance des mesures de la détection homodyne et la puissance de l'oscillateur local. En pratique cette relation n'est qu'affine, en raison d'un bruit électronique non nul du circuit pour une puissance d'oscillateur local nulle. Nous présentons notre montage électronique qui utilise notamment un étage d'amplification conçu pour l'amplification bas bruit de faibles courants.

Avant de pouvoir interférer côté Bob, l'oscillateur local et le signal doivent se propager à travers le canal quantique sans interférer. Pour cela, nous utilisons un dispositif de multiplexage à la fois en temps et en polarisation. Côté Alice, les impulsions lumineuses sont séparées en deux voies. La voie signal est retardée et sa polarisation est tournée de $\frac{\pi}{2}$ à l'aide d'un montage constitué d'un séparateur de polarisation, d'une ligne à retard et d'un miroir de Faraday. Elle est alors recombinée avec la voie oscillateur local en sortie d'Alice à l'aide d'un nouveau séparateur de polarisation. Côté Bob, les deux polarisations sont alors séparées par un séparateur de polarisation qui est précédé d'un contrôleur dynamique de polarisation. Les statistiques de la détection homodyne permettent de trouver un état optimal de polarisation. La voie oscillateur local est alors retardée et sa polarisation tournée de $\frac{\pi}{2}$ avec le même dispositif que celui d'Alice. La combinaison de ces deux techniques de multiplexage est particulièrement efficace : le démultiplexage en polarisation est particulièrement facile à implémenter tandis que la séparation temporelle est nécessaire pour éviter des fuites trop importantes de la voie oscillateur local dans la voie signal.

Le contrôle et l'acquisition des signaux de notre système sont réalisés au moyen de cartes National Instruments qui fonctionnent avec un signal d'horloge externe. Côté Alice notre horloge est générée par la carte laser et côté Bob nous la générons en prélevant une partie de l'oscillateur local. Dans les deux cas, l'horloge nous permet à la fois d'acquérir les signaux et de piloter les modulateurs optiques.

Notre système nécessite une quantité importante de nombres aléatoires non prédictibles par un attaquant. Nous rappelons la quantité de nombre aléatoire requise aux différentes étapes du protocole, à la fois pour le pilotage du hardware et pour le post-traitement des données. Nous utilisons des générateurs de nombres aléatoires physiques de la société Intel qui ont le double avantage d'être très rapides et d'inclure un post-traitement des nombres aléatoires issus du processus physique. Cela permet d'éviter d'éventuelles déviations de la source physique sui seraient causées par un vieillissement des composants.

Chapitre 5 : Prévention des attaques de calibration liées à l'oscillateur local pour la distribution quantique de clés à variables continues

Dans ce chapitre, nous étudions une attaque de calibration portant sur l'oscillateur local dans un système pratique de distribution quantique de clés à variables continues.

La preuve de sécurité mentionnée dans le chapitre 3 ne fait pas intervenir l'oscillateur local de manière explicite. En effet, en théorie il n'est pas nécessaire d'envoyer l'oscillateur local sur le canal quantique entre Alice et Bob. Ce dernier pourrait être généré localement par Bob. Cependant, cela est difficile à réaliser expérimentalement car l'oscillateur local doit être cohérent avec le signal afin que les deux signaux puissent interférer. L'oscillateur local est donc envoyé sur le canal quantique, subit les mêmes fluctuations que le signal quantique, et interfère avec le signal côté Bob. Une première possibilité d'attaque consiste pour un attaquant à modifier l'intensité de l'oscillateur local afin de compenser son action sur l'intensité du signal. Une contre-mesure contre une telle attaque est de surveiller l'intensité de l'oscillateur local en temps réel, ce qui est déjà le cas dans notre système.

L'oscillateur local définit également le niveau de référence pour toutes les mesures de bruit. Il s'agit du bruit quantique (ou bruit de photon), qui est mesuré comme la variance des mesures sur la détection homodyne en faisant interférer l'oscillateur local avec le mode vide sur une lame séparatrice équilibrée. La plupart des systèmes de distribution quantique de clés implémentés jusqu'ici calibrent la relation entre le bruit quantique et le niveau de l'oscillateur local en laboratoire et déduisent la valeur du bruit quantique en fonctionnement. Nous proposons une attaque qui vise à fausser la relation calibrée en laboratoire. Il s'agit de modifier la forme de l'impulsion oscillateur local et ainsi décaler le signal d'horloge qui est généré côté Bob à partir de cette impulsion. Les statistiques de la détection homodyne sont affectées par le décalage du trigger et la relation calibrée en laboratoire n' est donc pas utilisable pour établir le niveau de bruit de photon en temps réel.

En pratique, un espion peut exploiter cette faille de calibration pour récupérer la clé échangée par Alice et Bob sans être détecté. Il doit pour cela combiner cette attaque avec une attaque par interception et réémission. Eve intercepte les impulsions envoyées par Alice en mesurant les deux quadratures du signal quantique et envoie ces impulsions à Bob. Une telle attaque effectuée seule introduit un niveau de bruit important. En revanche, lorsqu'elle est combinée avec une modification de la calibration du bruit quantique, le niveau de bruit estimé par Alice et Bob peut devenir nul et l'espionnage reste donc indétecté.

Nous proposons une contre-mesure pour pallier cette attaque. Il s'agit de mesurer le bruit quantique en temps réel. Pour cela, nous proposons deux familles de techniques. La première consiste en l'introduction d'un dispositif d'atténuation sur la voie signal côté Bob. Bob peut ainsi atténuer la voie signal à des moments de son choix imprédictibles par un attaquant. Il peut en déduire une mesure du bruit de photon. En pratique, on utilise un modulateur d'amplitude ou un interrupteur optique, comme implémenté dans le chapitre 9. Une autre famille de techniques est d'utiliser un autre dispositif de détection homodyne côté Bob avec une voie non connectée qui correspond au mode vide et l'autre voie qui correspond à une fraction connue de l'oscillateur local entrant dans le dispositif de Bob. La mesure du bruit quantique peut alors être réalisée directement avec cette détection homodyne.

Nous étudions l'effet de la première famille de contre-mesures en calculant le taux de clé secrète contre les attaques collectives en régime asymptotique dans le mode réaliste où les pertes de Bob ne sont pas accessibles à l'attaquant. Dans ce cas là, l'efficacité de Bob est diminuée d'une quantité correspondant aux pertes du dispositif d'atténuation introduit dans le dispositif et la fraction des données utilisées pour évaluer le bruit quantique n'est plus utilisée pour extraire de la clé secrète. Pour des paramètres expérimentaux réalistes, la distance de sécurité maximale est alors réduite de 10 km.

Chapitre 6 : Amélioration de la distance de sécurité de la distribution quantique de clés à variables continues avec une modulation Gaussienne

Dans le chapitre 3, l'effet d'une procédure de correction d'erreurs imparfaite a été abordé. Dans le cas des protocoles de distribution quantique de clés à variables continues, cet effet a longtemps limité la distance maximale de sécurité. La raison en est l'absence de procédures de correction d'erreurs efficaces pour une modulation Gaussienne et un canal à bruit Gaussien pour des régimes de faible rapport signal à bruit, qui correspondent à de grandes distances de transmission entre Alice et Bob.

Une première solution à ce problème a été apportée en 2008 par Anthony Leverrier. Pour de faibles rapports signal à bruit, la capacité du canal à modulation Gaussienne et à bruit Gaussien devient très proche de la capacité du canal à modulation binaire et à bruit Gaussien. Or, il existe des codes correcteurs d'erreur efficaces pour ce dernier canal : les codes LDPC (Low Density Parity Check) multi-edge. Une procédure de virtualisation de canal peut alors être utilisée. Il s'agit d'utiliser d copies du canal à modulation Gaussienne et à bruit Gaussien pour construire d copies d'un nouveau canal virtuel à modulation binaire et à bruit Gaussien. L'efficacité de la correction d'erreurs sur le canal originel dépend alors de deux facteurs :

- l'efficacité des codes correcteurs sur le canal cible (ici le canal à modulation binaire et à bruit Gaussien)
- la qualité de l'approximation entre le canal virtuel et le canal cible (qui augmente avec la dimension d)

Il est donc possible d'améliorer l'efficacité de la réconciliation avec des variables Gaussiennes en concevant des codes avec de meilleures efficacités sur le canal à modulation binaire et à bruit Gaussien ou en augmentant la dimension de la virtualisation de canal.

Il apparaît que la virtualisation de canal ne peut pas être opérée en dimension supérieure à 8 en raison de l'absence d'une division pour les dimensions supérieures à 8. Il existe néammoins des méthodes probabilistes qui fonctionnent en dimension supérieure mais présentent plusieurs inconvénients : leur complexité calculatoire est importante, elles consomment des nombres aléatoires en quantité importante et nécessitent plus de communications réseaux.

Nous avons conçu des codes LDPC multi-edge pour le canal à modulation binaire et à bruit Gaussien avec des efficacités élevées pour de bas rapports signal à bruit. Les codes LDPC sont très utilisés dans les télécommunications classiques car ils ont des efficacités très proches de la capacité de Shannon et peuvent être décodés avec un algorithme itératif rapide appelé Belief Propagation. Pour un certain rapport signal à bruit, on peut calculer la capacité du canal et l'efficacité du code (comprise entre 0 et 1) est définie par le rapport entre le taux du code et la capacité du canal. Plus le niveau de bruit est élevé (ce qui correspond à de grandes distances de transmission), plus la capacité du canal est faible et donc plus il est nécessaire de concevoir des codes LDPC de taux faibles.

Un outil standard permet de concevoir des codes LDPC de taux donné : il s'agit de l'algorithme génétique *Differential Evolution*. Il permet de faire évoluer les distributions de probabilité des degrés des noeuds pour améliorer la performance des codes LDPC de taux correspondant à ces noeuds et ces degrés et leur probabilité d'occurrence. Le niveau de bruit maximum qui peut être corrigé par un code est appelé le *seuil* de ce code et l'algorithme *Density Evolution* est utilisé pour calculer ce seuil.

Nous avons pu concevoir des codes LDPC multi-edge de taux 0.5, 0.1, 0.05 et 0.02, qui nous permettent d'atteindre des rapports signal à bruit compris entre 1.1 et 0.03 avec des efficacités comprises entre 93.6% et 96.9% sur le canal Gaussien. A titre de comparaison les techniques de correction d'erreurs précédentes permettaient au mieux des efficacités de l'ordre de 90% pour des rapports signal à bruit de 0.5 et pour des valeurs supérieures.

Afin de pouvoir travailler sur des intervalles de rapports signal à bruit plus grands et non à des valeurs fixes, nous proposons plusieurs techniques. Les codes à répétition concaténés aux codes LDPC multi-edge permettent d'atteindre des rapports signal à bruit arbitrairement bas sans perte notable d'efficacité car les codes à répétition sont pratiquement optimaux pour des bruits très élevés. Il est possible de modifier le taux d'un code LDPC à l'aide de techniques de *puncturing* et de *shortening* dans une certaine mesure tout en maintenant une efficacité élevée. Enfin, la présence d'un modulateur d'amplitude chez Alice permet d'ajuster la variance de modulation afin de maintenir un rapport signal à bruit optimal en ce qui concerne le taux de clé secrète chez Bob.

Chapitre 7 : Démonstration expérimentale de distribution quantique de clés à variables continues à longue distance

Nous présentons dans ce chapitre les performances obtenues à longue distance avec notre dispositif expérimental. La distance maximale obtenue à longtemps été limitée à environ 25 km en raison de l'absence de procédures de correction d'erreurs efficaces pour des rapports signal à bruit faibles, c'est à dire pour de longues distances. Nous avons développé dans le chapitre 6 des codes correcteurs d'erreurs efficaces qui nous permettent en théorie de générer des clés secrètes à des distances supérieures à 100 km. Ici, nous démontrons expérimentalement la distribution quantique de clés à variables continues à une distance de 80 km (16.1 dB de pertes).

Nous implémentons le protocole à modulation Gaussienne d'états cohérents présentés dans le chapitre 3. Alice utilise une diode laser télécom en régime impulsionnel à une fréquence de 1 MHz pour des impulsions d'une durée de 100 ns. Les impulsions sont séparées en deux à l'aide d'un coupleur déséquilibré de rapport 99/1. La voie la moins atténuée correspond à l'impulsion oscillateur local. Sur la voie la plus atténuée, un modulateur d'amplitude et un modulateur de phase sont utilisée pour générer la modulation Gaussienne bidimensionnelle du protocole GG02. Le niveau de variance du signal est ajusté à l'aide d'un réglage grossier avec des atténuateurs variables mécaniques et d'un réglage fin en utilisant le modulateur d'amplitude. L'impulsion signal est retardée d'environ 200 ns à l'aide d'une ligne à retard de 20 m et d'un miroir de Faraday. La polarisation de l'impulsion signal est ainsi également tournée d'un angle de $\frac{\pi}{2}$ par rapport à l'impulsion oscillateur local et le multiplexage en polarisation est réalisé au moyen d'un combineur de polarisation. Sur la voie signal, une partie du signal est prélevée au moyen d'un coupleur puis injectée dans une photodiode et son circuit d'amplification. Ce système permet de surveiller le niveau du signal en cours de fonctionnement et ainsi d'ajuster le niveau de modulation d'Alice. Ce rétrocontrôle permet d'une part de compenser les dérives de la tension de biais du modulateur d'amplitude et d'autre part de choisir le niveau de signal en sortie d'Alice pour obtenir un rapport signal à bruit optimal chez Bob. Après s'être propagées à traver le canal quantique, les impulsions signal et oscillateur local sont séparées chez Bob à l'aide d'un séparateur de polarisation et d'un contôleur de polarisation dynamique. Avant cela, une fraction fixe de ces signaux est prélevée afin de générer un signal d'horloge qui permet de réaliser les mesures sur la détection homodyne. Une deuxième ligne à retard côté Bob permet de superposer temporellement les impulsions signal et oscillateur local. Un modulateur de phase situé sur la voie oscillateur local permet de sélectionner aléatoirement une quadrature du signal. Le canal quantique est constitué de plusieurs rouleaux de fibre optique et la distance maximale de production de clés de notre système est de 80 km.

Conformément à l'analyse de sécurité présentée dans le chapitre 3, l'état quantique à deux modes partagé entre Alice et Bob est entièrement caractérisé par la variance de modulation d'Alice, la transmission et l'excés de bruit du canal quantique. La variance de modulation d'Alice et l'excés de bruit devant être exprimés en unités de bruit de photon, nous estimons également le bruit de photon. Tous ces paramètres sont estimés en temps réel en révélant aléatoirement une fraction des signaux échangés entre Alice et Bob.

Dans le mode réaliste, deux autres paramètres, qui sont l'efficacité et le bruit électronique de la détection homodyne, doivent être estimés. Ces paramètres sont estimés en laboratoire avant l'execution de la distribution quantique de clés et nous devons donc supposer qu'un attaquant potentiel ne peut pas altérer leur valeur. La variance de modulation d'Alice est ajustée en temps réel afin de maintenir un rapport signal à bruit chez Bob qui est proche du seuil de décodage d'un des codes correcteurs d'erreurs disponibles.

La procédure de correction d'erreurs s'effectue en deux parties. Les valeurs mesurées par Bob sont tout d'abord regroupées huit par huit et Bob tire des valeurs binaires aléatoires de taille huit qui vont servir de référence pour la clé. Bob transmet alors à Alice des vecteurs de taille huit qui décrivent la rotation entre le vecteur reçu par Bob et le vecteur tiré aléatoirement. On peut montrer que cette information transmise de Bob à Alice ne révèle rien à propos de la clé. En utilisant cette rotation, Alice peut alors calculer un vecteur qui correspond au vecteur de référence tiré chez Bob plus un bruit proche du bruit Gaussien introduit par le canal. Il est alors possible de regrouper 2^{17} vecteurs de taille huit chez Alice et chez Bob afin de former des vecteurs de taille 2^{20} sur lesquels une procédure de correction d'erreurs standards est appliquée. Bob calcule le syndrome associé à son vecteur de r 'e férence en le multipliant par la matrice de parité du code LDPC multi-edge choisi pour le rapport signal à bruit constaté entre Alice et Bob. Alice reçoit ce syndrome et applique un décodage itératif pour corriger les erreurs. Nous utilisons un processeur graphique pour décoder plusieurs vecteurs à la fois et ainsi obtenir des vitesses de correction d'erreurs compatibles avec un post-traitement des données en temps réel. Des vitesses de plusieurs megabits par seconde sont obtenues sur des processeurs graphiques AMD Tahiti comme présenté dans le chapitre 8.

L'amplification de confidentialité est réalisée en accumulant plusieurs vecteurs après correction d'erreurs et en les multipliant par des matrices de Toeplitz aléatoires. Cette étape peut s'implémenter efficacement sur des processeurs récents y compris pour des tailles d'entrée importantes. Pour des tailles d'entrée de 10^9 et de sorties de l'ordre de 10^6, nous obtenons des vitesses de l'ordre de 40 megabits par seconde sur un coeur de processeur i7-920.

Afin de pouvoir obtenir des taux de clé positifs à longue distance en prenant en compte les effets de taille finie, il est nécessaire d'estimer les paramètres utilisés pour calculer le taux de clé secrète sur des blocs de grande taille. En effet, l'information mutuelle entre Bob et Eve dans le cas des tailles finies est calculée comme le maximum de cette information mutuelle sur les intervalles de confiance obtenus lors de l'estimation des paramètres sur des blocs de données de taille finie. Le principal effet de l'analyse en taille finie correspond à l'incertitude sur l'excés de bruit du canal quantique. L'incertitude sur l'estimateur de l'excés de bruit augmente avec la distance de transmission et il faut donc considérer des blocs de taille de plus en plus grande pour réduire cette incertitude pour de grandes distances de transmission. En pratique, à 80 km nous devons estimer nos paramètres sur des blocs de taille 10^9 pour obtenir un taux de clé positif. Cela n'est possible que si le système est stable sur des durées permettant d'acquérir des blocs de taille 10^9 c'est à dire quelques minutes pour un taux de répétition optique de l'ordre du MHz.

Chapitre 8 : Amélioration du débit de la distribution quantique de clés à variables continues

Ce chapitre est consacré à l'amélioration du débit de la distribution quantique de clés à variables continues. Le débit des précédentes démonstrations, et notamment le débit du système combiné à un système de chiffrement symétrique dans le chapitre 9, était limité par la vitesse de post-traitement des données issues du système. Au sein du tuyau de post-traitement, la correction d'erreurs était l'étape limitante en raison de l'utilisation d'algorithmes itératifs tels que Belief Propagation dont la vitesse de convergence est lente pour des niveaux de bruit proches du seuil du code correcteur d'erreurs utilisé. De plus, travailler loin des seuils des codes correcteurs pour améliorer la vitesse de décodage n'aurait pas permis de maintenir des taux de clé positifs pour des distances acceptables.

Nous avons implémenté l'étape de décodage des codes LDPC sur un processeur graphique à l'aide du langage de programmation OpenGL. L'important parallélisme offert par ces processeurs permet d'atteindre des vitesses allant jusqu'à 10 Mb/s tout en conservant les efficacités élevées obtenues avec les codes correcteurs d'erreurs conçus dans le chapitre 6. Nous comparons ces vitesses avec celles obtenues sur des unités centrales de traitement modernes. Le gain est d'environ un ordre de grandeur et va en augmentant car la pente de l'évolution de la vitesse des processeurs graphiques est plus importante que celle des unités centrales de traitement.

Nous avons également généré un autre type de codes, des codes polaires, à la fois pour le canal binaire symétrique qui est le canal de référence pour la distribution quantique de clés à variables discrètes, et pour le canal à entrée binaire et bruit Gaussien pour la distribution quantique de clés à variables continues. Les codes polaires ont été découverts en 2008 et ont la particularité d'atteindre la capacité de Shannon en limite asymptotique pour tous les canaux binaires symétriques sans mémoire. Ils s'accompagnent de plus de techniques d'encodage et de décodage efficaces. Pour les codes polaires, différentes copies du canal sont combinées récursivement pour former un nouvel ensemble de canaux de façon à ce qu'en limite asymptotique les canaux soient ou bien sans bruit ou bien totalement bruités, avec une fraction de canaux sans bruit égale à la capacité du canal. Ce phénomène est appelé la polarisation de canal. En limite asymptotique, les bits d'information peuvent être envoyés sur les canaux sans bruit pour atteindre la capacité du canal mais en pratique, l'on peut uniquement atteindre une fraction de cette capacité avec une probabilité d'erreur proche de zéro pour des tailles de blocs finies. La vitesse de convergence des canaux en canaux sans bruit ou en canaux bruités est appelée la vitesse de polarisation.

Nous avons utilisé *Density Evolution* pour calculer les capacités des différents canaux pour des codes polaires de différentes tailles. Les bits correspondant aux canaux de faible capacités sont simplement révélés et constituent les bits gelés du code. La méthode de construction utilisée nous permet de calculer une borne sur la probabilité d'erreur de décodage des codes construits. Nos résultats de simulation montrent que la vitesse de polarisation des codes polaires dépend fortement du canal. Pour le canal binaire symétrique, nous avons obtenu des codes d'efficacité supérieure à 95% pour tout l'invervalle utile de probabilité d'erreur $[0; 0.11]$ avec des codes de taille supérieure à 2^{24}. Pour le canal à entrée binaire et bruit Gaussien, nous n'avons pu atteindre que des capacités de l'ordre de 90% avec des codes polaires de taille 2^{27}. En ce qui concerne la vitesse de décodage, la structure récursive régulière des codes polaires nous a permis d'implémenter un décodeur récursif qui atteint des vitesses de l'ordre de 10 Mb/s sur des processeurs récents.

En ce qui concerne l'amplification de confidentialité, nous donnons nos vitesses de hachage sur des processeurs récents pour la famille "multiplication par une matrice de Toeplitz aléatoire". Les vitesses obtenues sont un à deux ordres de grandeur supérieures aux vitesses obtenues pour la correction d'erreur. Cette étape n'est donc toujours pas limitante en vue d'une augmentation de la fréquence de notre système. Nous rappelons enfin le débit de communication réseaux pour les différentes étapes de notre système. Ce débit est bien inférieur aux débits réseaux actuellement accessibles.

Chapitre 9 : Intégration de la distribution quantique de clés à variables continues dans les réseaux optiques

Le dernier chapitre est consacré à l'intégration de la distribution quantique de clés à variables continues dans les réseaux optiques. Nous présentons dans un premier temps une démonstration de la stabilité long-terme (sur une période de six mois) d'une implémentation du protocole GG02 sur un lien optique fibré déployé sur le terrain et non en laboratoire. Dans le cadre de cette démonstration, le dispositif de CVQKD est couplé à des chiffreurs symétriques commerciaux qui implémentent un chiffrement AES. Le système CVQKD est utilisé pour renouveler les clés de ces chiffreurs. La deuxième partie de ce chapitre vise à démontrer la compatibilité de la CVQKD avec des signaux classiques multiplexés sur la même fibre optique. Après avoir rappelé l'analyse théorique des bruits ajoutés sur un canal quantique par des canaux classiques à d'autres longueurs d'onde, nous présentons les résultats expérimentaux obtenus sur une fibre de 25 km avec notre système de CVQKD et un canal classique intense.

Puisque le taux de clé secrète que l'on peut obtenir avec tout système QKD décroît avec l'augmentation des pertes et donc avec la distance de transmission, l'utilisation du chiffrement à masque jetable qui consiste en la combinaison d'un bit de clé secrète pour un bit de message à transmettre n'est pas adaptée aux communications à haut débit. En effet, les communications numériques actuelles atteignent des débits de plusieurs dizaines de gigabits par seconde sur des distances arbitraires (en utilisant un nombre potentiellement grand d'amplificateurs optiques) tandis que les meilleurs taux de clé secrètes obtenus avec des dispositifs QKD en laboratoires sont de l'ordre du megabit par seconde et même du kilobit par seconde pour les systèmes commerciaux. A l'opposé, des systèmes de chiffrement classiques basés sur des primitives avec des implémentations rapides, comme l'AES, permettent d'atteindre des débits de plusieurs dizaines de gigabits par seconde. La mise à la clé de ces systèmes peut se faire de plusieurs façons. La première consiste en un prépartage des clés entre équipements lors de leur sortie d'usine. Un défaut de cette approche est que le vol d'un équipement ou bien l'accès à un équipement à un certain moment compromet la sécurité de toutes les communications postérieures. Une autre possibilité est d'utiliser des primitives asymétriques, comme le protocole Diffie Hellman. Un tel protocole permet de renouveler la clé un nombre quelconque de fois, et force donc un espion à récupérer la nouvelle clé après chaque renouvellement afin de pouvoir déchiffrer l'intégralité des communications. Le défaut de cette approche est que la sécurité de cette primitive repose sur des hypothèses de nature algorithmiques. Il est également possible d'utiliser un messager de confiance, en d'autres termes un convoi sécurisé, pour partager les clés entre Alice et Bob mais cette approche est peu pratique car non automatisable et très coûteuse. Une dernière possibilité est donc d'utiliser la distribution quantique de clés, qui présente l'avantage de ne reposer sur aucune hypothèse algorithmique et de permettre un renouvellement de clés fréquent et automatique.

Cette démonstration du renouvellement de clés symétriques de chiffreurs AES par la QKD et de chiffrement à 1 Gb/s s'est effectuée sur un lien fibré de 17.7 km présentant 5.6 dB de pertes entre Massy et Palaiseau en région Parisienne. La couche physique du dispositif QKD a été réalisée avec un dispositif similaire à celui décrit dans le chapitre 7 fonctionnant à une fréquence de 500 kHz et à une longueur d'onde de 1550 nm. Le post-traitement des données générées par les boîtiers optiques est fait par des unités centrales indépendantes qui implémentent les étapes d'estimation des paramètres physiques du canal quantique, de correction d'erreur, d'amplification de confidentialité et de vérification de la clé. L'authentification et la gestion des clés est réalisée sur ces mêmes ordinateurs à l'aide de la couche logicielle réalisée dans le cadre du projet Européen SECOQC par l'Austrian Institute of Technology. Les clés sont injectées dans les chiffreurs Mistral par les dispositifs QKD à une fréquence de 10 secondes qui est paramétrable à travers la console de gestion des chiffreurs. Enfin, des unités centrales supplémentaires sont utilisées pour générer du trafic à 1 Gb/s qui est chiffré par les Mistral.

Le système a fonctionné pendant six mois et était surveillé à travers une connexion sécurisée à distance. Des prises commandables grâce à un accès réseau permettaient également d'éteindre et de rallumer les systèmes en cas de problème. Une panne matérielle a interrompu le fonctionnement du système pendant une semaine puis des fluctuations de température importantes ont altéré son fonctionnement. Un taux de clé secrète de l'ordre de 600 bits par seconde contre les attaques collectives a été obtenu lors de la première partie de la démonstration puis de l'ordre de 400 bits par seconde contre les attaques individuelles après la panne matérielle et dans des conditions de fonctionnement dégradées.

Nous nous intéressons ensuite aux différents bruits ajoutés dans le cadre du fonctionnement d'un système de CVQKD avec d'autres canaux classiques situés à d'autres longueurs d'onde sur la même fibre optique. La première source de bruit est la fuite des canaux classiques dans le canal quantique en raison de la largeur spectrale des sources laser utilisées. Cette fuite devient très faible en pratique en utilisant des multiplexeurs et démultiplexeurs avec des isolations importantes entre canaux. La deuxième source de bruit est le Four Wave Mixing (FWM) qui correspond à l'interaction entre au moins deux canaux classiques et la non linéarité des fibres optiques. Dans le cas du FWM, trois signaux optiques de fréquences différentes interagissent pour créer un quatrième signal à une fréquence qui est une combinaison linéaire des fréquences précédentes. Le FWM peut être une source majeure de bruit à courte distance mais il est largement dominé par l'effet Raman sur des distances métropolitaines de l'ordre de 25 km. De plus son effet peut être diminué par exemple en augmentant l'espacement entre canaux classiques ou en omettant un canal entre le canal quantique et le canal classique suivant.

Pour ces raisons, nous négligeons l'effet du FWM dans notre étude. Enfin, lorsque le canal quantique est placé à une longueur d'onde inférieure aux canaux classiques, l'effet Raman spontané de type anti-Stokes est l'effet dominant. Il s'agit de l'émission spontanée de photons à d'autres longueurs d'onde que la longueur d'onde de ce champ avec un nombre de photons proportionnel à la puissance du canal classique qui les créent ainsi qu'à la longueur d'onde de ce champ.

L'effet Raman s'avère désastreux pour la DVQKD mais beaucoup moins pour la CVQKD. En effet, l'oscillateur local qui interfère avec le signal quantique joue le rôle de filtre pour les photons générés par effet Raman car seuls les photons qui sont dans le même mode spatiotemporel et de polarisation que l'oscillateur local vont interférer avec lui. Une partie importante du bruit va donc être filtrée par la détection interférométrique. Nous simulons l'excés de bruit ajouté sur notre système CVQKD par un canal classique et nous calculons le taux de clé secrète que nous pouvons espérer atteindre pour le système du chapitre 7 en coexistence avec un canal classique. Puis nous réalisons la démonstration expérimentale. Dans un système où d'autres canaux classiques peuvent générer un bruit de photon sur la détection homodyne, l'utilisation d'une relation calibrée pour dé terminer le bruit de photon ne peut pas être utilisée. Nous avons donc choisi d'implémenter l'une des contre-mesures proposées dans le chapitre 5. Nous avons introduit un interrupteur optique sur la voie signal du dispositif Bob. Cela nous permet de fermer cette voie à des instants aléatoires et de mesurer le bruit de photon en temps réel. L'implémentation de cette méthode ajoute un bruit intrinsèque à notre système et nous ne sommes pas en mesure d'obtenir les mêmes niveaux de bruit que dans le chapitre 7. Notre démonstration de la coexistence entre un canal classique non atténué et notre système CVQKD est donc ici limitée à un lien de 25 km.

Introduction

This manuscript deals with the security and performance of a continuous-variable quantum key distribution system that employs coherent states of light. *Quantum Key Distribution* (QKD) is, together with *Quantum Random Number Generators* (QRNG), one of the first applications of *quantum information*, a modern research field situated at the intersection between *quantum mechanics* and *information theory*.

Contrary to classical key distribution methods, QKD allows us to transmit a secret message through a *public* communication channel without making any assumption regarding the power of an eavesdropper attempting to learn this secret. The security of this technique relies on the laws of quantum physics and is said to be *unconditional*, while the security of classical key distribution methods relies on some computational hardness assumptions and can only be proven against some restricted classes of attackers. The protocol using coherent states of light offers the advantage of using only standard components, optimized for high-speed optical telecommunications. In this thesis, we started from coherent state prototypes designed at Thales Research & Technology and the Institut d'Optique Graduate School in the context of the *Secure Communication based on Quantum Cryptography* (SECOQC) European project. We then designed a commercial product called Cygnus which has an improved performance in terms of operating distance, speed, security and integration in current network infrastructures.

Scientific context at the beginning of the thesis

The first quantum key distribution protocols used discrete variables, i.e. they encoded the information in discrete states of the light such as the polarization of single photons [120]. Only twenty years after the seminal paper of Bennett and Brassard [9] that introduced this idea, on the one hand, some start-up companies, like MagiQ Technologies [3] and IdQuantique [2], designed fiber optics based commercial systems using discrete variables protocols. A few years later, the Austrian Institute of Technology developed another QKD system built around a source of entangled photons. On the other hand, the first protocols employing continuous variables were introduced a few years later. Experimental continuous variables protocols were demonstrated over both free space and fiber links. Contrary to *Discrete Variables Quantum Key Distribution* protocols which require specific components such as actively cooled single photon detectors, *Continuous Variables Quantum Key Distribution* (CVQKD) protocols using coherent states employ only standard telecommunication components. However, CVQKD performance was not suitable for long distance communications and no secret key could be distributed over distances larger than 25 km [83]. In contrast, DVQKD was performed over 200 km of optical fibre thanks to cutting-edge superconducting single photon detectors [137].

In parallel to the development of QKD commercial systems, a new research field emerged: *quantum hacking*. Indeed, while *in theory* QKD offers an unprecedented level of security, *in practice* this security can be threatened because of implementation problems [121]. This is because the security proof of a QKD protocol does not take into account *real* and therefore imperfect devices but *ideal* versions of these devices. Consequently, a malicious eavesdropper can exploit such deviations from the theoretical description of the protocol in order to perform powerful attacks that cannot be detected [91, 155, 86, 58]. Hence, the existing security proofs were modified in order to include effects not taken into account into the previous security proofs, including the issue of *finite-size effects* [122, 77].

Finally, from an industrial point of view, performance and security are not the only relevant criteria concerning QKD adoption in security infrastructures. Actually, QKD *integration* in current network infrastructures might even be the main driver to a broader market. This is why several field demonstrations of QKD were performed and not only laboratory experiments. In [104, 119], QKD was demonstrated over real metropolitan networks, while in [37], the authors demonstrate the coexistence of QKD and classical encryption over a single point-to-point fiber link. However, this latter demonstration suffers from DVQKD lack of tolerance to the noise introduced by classical channels on the quantum channel. In fact, the feasibility of quantum key distribution through a *Dense Wavelength Division Multiplexing* (DWDM) network is an important topic addressed in [106]: in this theoretical analysis CVQKD compared favorably to DVQKD as regards deployments in a DWDM network.

Content of the manuscript

Chapter 1 of this manuscript introduces the basis concepts of cryptography and presents briefly the new tools brought by quantum cryptography to the field. Chapter 2 describes the building blocks of quantum information with Gaussian variables that are necessary for the theoretical analysis of the quantum key distribution protocols with continuous variables that are studied in chapter 3. In chapter 4, we detail the experimental setup we used for the implementation of the coherent states CVQKD protocol. In chapter 5, we describe a potential attack on a CVQKD system and provide possible countermeasures. In chapter 6, we explain how to increase the range of CVQKD thank to a set of error-correcting codes we developed. These error-correcting codes, together with the improved stability of our hardware setup, allow for an experimental demonstration of long-distance in chapter 7. Chapter 8 provides high-speed error-correction software tools that enable an increase of the speed of our system. Chapter 9 is dedicated to CVQKD integration in optical networks: it describes a field demonstration of a CVQKD prototype combined with classical encryptors and gives preliminary results concerning the compatibility of our CVQKD setup with a DWDM environment.

Academic publications and conferences

The results of this thesis have been published in several peer-reviewed journals. Here is the list in chronological order:

- P. Jouguet, S. Kunz-Jacques, and A. Leverrier, “Long Distance Continuous-Variable Quantum Key Distribution with a Gaussian Modulation”, *Phys. Rev. A* **84**, 062317 (2011).
- P. Jouguet, S. Kunz-Jacques, T. Debuisschert, S. Fossier, E. Diamanti, R. Alléaume, R. Tualle-Brouri, P. Grangier, A. Leverrier, P. Pache, and P. Painchault, “Field Test of Classical Symmetric Encryption with Continuous Variable Quantum Key Distribution”, *Opt. Express* **20**, 14030 (2012).
- P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, “Analysis of Imperfections in Practical Continuous-Variable Quantum Key Distribution”, *Phys. Rev. A*, **86**, 032309 (2012).
- P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, “Experimental demonstration of long-distance continuous-variable quantum key distribution”, *Nat. Phot.*, **7**, 378 (2013).
- P. Jouguet, S. Kunz-Jacques, and E. Diamanti, “Preventing Calibration Attacks on the Local Oscillator in Continuous-Variable Quantum Key Distribution”, *Phys. Rev. A*, **87**, 062313 (2013).
- P. Jouguet, and S. Kunz-Jacques, “High Performance Error Correction for Quantum Key Distribution using Polar Codes”, *Quant. Inf. Comp.*, Vol. **14**, No. 3&4 (2013).
- S. Kunz-Jacques, and P. Jouguet, “Using Hash-Based Signatures to Bootstrap Quantum Key Distribution”, submitted to *IEEE Trans. Inf. Forens. Sec.* (2013).
- A. Pappa, P. Jouguet, T. Lawson, A. Chailloux, M. Legré, P. Trinkler, I. Kerenidis, and E. Diamanti, “Experimental plug & play quantum coin flipping”, submitted to *Nat. Comm.*, (2013).

The results of this thesis have also been presented in posters and presentations at the following conferences in chronological order:

- P. Jouguet, “Long-distance CVQKD with a Gaussian modulation”, Continuous Variable Quantum Information Processing 2011 (CVQIP 2011), Paris, France, September 2011 (presentation).
- P. Jouguet, “Towards High-performance CVQKD”, FREQUENCY project meeting, Waterloo, Canada, November 2011 (presentation).
- P. Jouguet, S. Kunz-Jacques, A. Leverrier, E. Diamanti, “High Performance Continuous-Variable Quantum Key Distribution”, First GDR - IQFA workshop, Paris, France, November 2011 (poster).
- P. Jouguet, “Performance and security of CVQKD”, Continuous Variable Quantum Information Processing 2012 (CVQIP 2012), Federiksdal, Denmark, April 2012 (presentation).
- P. Jouguet, S. Kunz-Jacques, A. Leverrier, E. Diamanti, “Improving the Performance of Continuous-Variable Quantum Key Distribution: Study of Practical Imperfections and High-Performance Reconciliation”, QCRYPT 2012, Singapore, September 2012 (poster).
- P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, E. Diamanti “Experimental demonstration of CVQKD over 80 km of standard telecoms fiber”, QCRYPT 2012, Singapore, September 2012 (presentation).
- P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, E. Diamanti,

"Experimental Demonstration of Long-Distance Continuous-Variable Quantum Key Distribution", Second GDR - IQFA workshop, Grenoble, France, November 2012 (presentation).

- P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, E. Diamanti, "Experimental Demonstration of Long-Distance Continuous-Variable Quantum Key Distribution", Topical Research Meetings on Physics: Quantum technologies: taking concepts through to implementations, London, United Kingdom, December 2012 (presentation).
- P. Jouguet, "Integration of CVQKD in Future Optical Networks", Continuous Variable Quantum Information Processing 2013 (CVQIP 2013), Paris, France, January 2013 (presentation).
- P. Jouguet, "SeQureNet Coherent-State CVQKD Implementation", National Institute of Communications and Technology (NICT) seminar, Tokyo, Japan, March 2013 (presentation).
- P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, E. Diamanti, "Experimental demonstration of continuous-variable quantum key distribution over 80 km of standard telecoms fiber", Conference on Lasers and Electro-Optics - International Quantum Electronics Conference 2013 (CLEO - IQEC 2013), Munich, Germany, May 2013 (presentation).
- P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, E. Diamanti, "Experimental demonstration of continuous-variable quantum key distribution over 80 km of standard telecoms fiber", Conference on Lasers and Electro-Optics:Quantum Electronics and Laser Science - Fundamental Science 2013 (CLEO:QELS - Fundamental Science 2013), San Jose, USA, June 2013 (presentation).
- P. Jouguet, S. Kunz-Jacques, R. Kumar, H. Qin, R. Gabet, E. Diamanti, R. Alléaume, "Experimental demonstration of the coexistence of continuous-variable quantum key distribution with an intense DWDM classical channel", QCRYPT 2013, Waterloo, Canada, August 2013 (presentation).
- P. Jouguet, S. Kunz-Jacques, E. Diamanti, "Preventing calibration attacks in continuous variables quantum key distribution", QCRYPT 2013, Waterloo, Canada, August 2013 (poster).

At QCRYPT 2012 conference, the work entitled "Experimental demonstration of continuous-variable quantum key distribution over 80 km of standard telecoms fiber" received the Best Student Paper Award by the conference program committee.

Scientific collaborations

This work greatly benefited from several scientific collaborations. This research was supported by the the ANRT (Agence Nationale de la Recherche et de la Technologie), the French National Research Agency, through the FREQUENCY (ANR-09-BLAN-0410) and HIPERCOM (2011-CHRI-006) projects, by the European Union through the projects Q-CERT (FP7-PEOPLE-2009-IAPP) and by the DIRECCTE Ile-de-France through the QVPN (FEDER-41402) project.

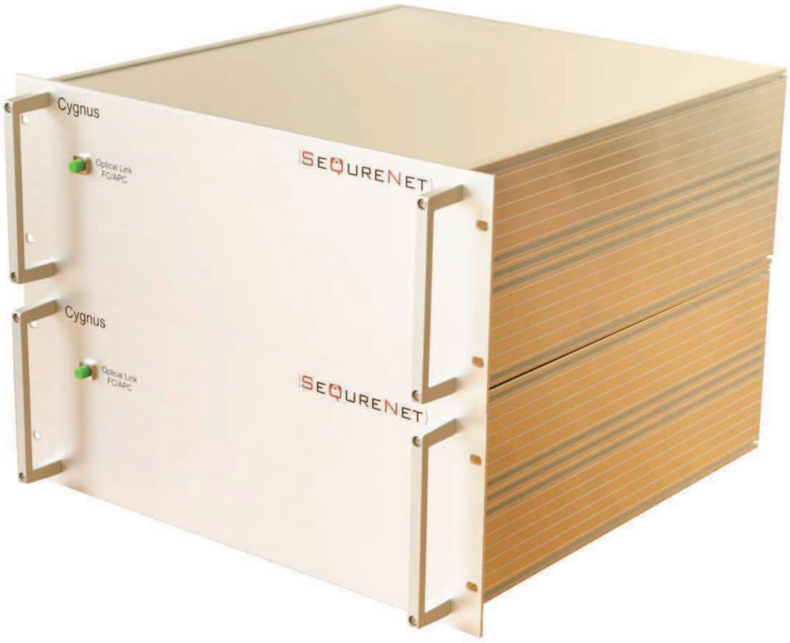


Figure 1: Cygnus: a quantum key distribution product commercialized by SeQureNet. The optical part is composed of two standard 19 inches rackable boxes of 4U, one for Alice and the other for Bob. They are driven by two computers that also perform the different post-processing steps.

Industrial and commercial impact

The first Continuous-Variables Quantum Key Distribution product, called Cygnus (see Figure 1), has been released and sold by SeQureNet during this thesis. A patent application focused on real time shot noise measurement techniques for continuous variables quantum communication systems has been filed. Some of these techniques are described in chapter 5.

Chapter 1

From Classical Cryptography to Quantum Cryptography

Contents

1.1 What is Cryptography? 7
1.2 Modern Cryptography 9
1.2.1 Symmetric and Asymmetric Cryptography 9
1.2.2 Usual Primitives 10
1.2.3 Threats 10
1.3 Quantum Key Distribution 10
1.3.1 Principle 11
1.3.2 Security Characteristics 11
1.3.3 DVQKD vs CVQKD in 2010 12
1.3.4 Threats 13
1.4 Other Quantum Cryptographic Primitives . . . 13
1.4.1 Coin Flipping 13
1.4.2 Quantum Signatures 14

1.1 What is Cryptography?

The word *cryptography* stems from Greek $\kappa\rho\upsilon\pi\tau\omega$ that means *hidden* or *secret*. It refers to a set of techniques allowing for secure communications in the presence of third parties, also called adversaries, attackers or eavesdroppers. Historically, the only purpose of cryptography was data confidentiality, which consists in preventing any non-legitimate party to access a message some legitimate parties want to share. Secrecy of communications is for example of utmost importance as regards military operations or diplomacy. Message confidentiality can be achieved using *encryption*, which is the process of converting an ordinary message (called plaintext) into apparent nonsense (called ciphertext). *Decryption* is the reverse operation that recovers the plaintext from the ciphertext. Encryption and decryption are performed using a pair of algorithms, also called a *cipher*. A cipher can be instantiated by a *key*, i.e. a secret chosen in a large set, which is used both to encrypt and decrypt the messages. If the key that indexes the cipher is not chosen in a large enough set, the security of the cipher relies on the secrecy of the cipher. This is because the knowledge of the cipher is sufficient to perform encryption and decryption which allows for a straightforward strategy for an attacker, the *exhaustive search*. He can try to decrypt the message successively with all the possible keys until he finds an intelligible message, which can be done in finite time for a finite set of keys.

Let us consider a famous example, Caesar cipher, or the shift cipher, named after Julius Caesar who used it to communicate with his generals. It simply consists in substituting each letter in the plaintext by a letter shifted by some fixed number of positions in the alphabet. For instance, with a right shift of 3, A is replaced by D, B by E, and so on. The plaintext HELLO is encrypted in the ciphertext KHOOR. One can easily see that the number of possible keys for the cipher is equal to the number of letters in the alphabet, i.e. 26. Thus, an attacker aware of the shift cipher can try successively to shift the letters of the ciphertext KHOOR by a number of positions between 1 and 26 until he recovers the plaintext. This is a *brute force* attack where the attacker tries all the possible keys until he encounters the plaintext (this requires to define a criteria to recognize a plaintext that does not give too many false positives) without using more sophisticated approaches. Another possible attempt to break such a cipher consists in analysing the frequency of occurrence of the letters in the ciphertext. Since a shift cipher also shifts the frequency of occurrence of the letters of the plaintext, an attacker can recover the key from the ciphertext analysis. In the English language, E is the most frequent letter, thus encrypting a long enough plaintext (for example a book) with the shift cipher and the key 3 is likely to produce a ciphertext whose most frequent letter if H. If the message is long enough, an eavesdropper can deduce that the key is 3 from this simple observation. More generally, *cryptanalysis* regroups all the techniques that can be used to recover some information on plaintexts from ciphertexts without knowledge of the encryption key. In practice, we say that a cipher is good if there is no procedure allowing to recover the plaintext faster than brute force. In this case, the security of the cipher is equivalent to the secrecy of the key.

In the modern era, cryptography and cryptanalysis have developed quickly, in particular because they are eased by the use of computers. On the cryptanalytic side, the development of computers allows us to carry out repetitive and difficult tasks, which led for example to the decryption of ciphers generated by the German Army's Lorenz SZ40/42 machine (a mechanical cipher machine) during the World War II. Computers also enabled the development of much more complex ciphers. One important feature of modern cryptography is the manipulation of binary sequences by computers while mechanical machines were limited to letters and digits: this enables the encryption of any kind of data that can be represented in binary format, such as images, audio files or video files for example.

The use of cryptography has expanded especially with the development of digital communication infrastructures, such as network infrastructures. This is a direct consequence of the increase of the volume of digital communications over the world. In addition to national security usage, data protection now also concerns companies, private individuals and even machines, which represent an increasing portion of the global volume of communications with the expansion of *Internet Protocol* (IP) networks that made machine-to-machine communication easier. The physical media of communication are also diverse, ranging from fiber optics to free space that include short distance transmission protocols (like the famous Wi-Fi protocol) but also long distance satellite communications. Finally, a great diversity of techniques are currently used in addition to data confidentiality: data *integrity*, user identity *authentication* and *digital signatures* are among the most famous ones.

The multi-level complexification of data communication infrastructures which are composed of a large diversity of both hardware and software building blocks faces an increasing number of security threats which led people to consider a broader field of research, *Information Security*, which is beyond the scope of this manuscript. In the next sections, we focus on some modern cryptography techniques which are relevant to understand which services can or cannot be improved with the help of quantum cryptography.

1.2 Modern Cryptography

1.2.1 Symmetric and Asymmetric Cryptography

Symmetric cryptography, or *secret key cryptography*, gathers together all the encryption and authentication methods where the different parties share the same key. This key is used for both encryption and decryption of a message. Even if the cipher is good, it is still very important to define a secure procedure allowing to share the key since any leak (even partial) of the key considerably weakens the security of the symmetric scheme. A confidential meeting between the parties can play this role, or the *encryptors* used to perform the encryption and the decryption are simply made with a common secret. Another possibility is to send a trusted *secret courrier*, i.e. a secure means of transport, for example some militaries holding secret keys stored on a protected storage medium such as *smart cards*. The major drawback of these procedures is that the number of secret keys that need to be exchanged, and also the deployment cost, scales quadratically with the number of parties. For a large scale infrastructure, like electronic commerce, such methods are not satisfactory. Another drawback is that if a key leaks at some point, the procedure must be done again.

Asymmetric cryptography, or *public key cryptography*, aims at solving these difficulties. It employs two different keys for encryption and decryption: the encryption key is public while the decryption key remains secret. With such a scheme, it is not required any more to share a common secret before transmitting confidential data. However, the two keys are related and the security of the scheme relies on some assumptions, for example the computational power of the eavesdropper is assumed to be bounded or some mathematical problems (e.g. factorizing large numbers) are assumed to have a non-polynomial complexity.

Another asymmetric cryptographic primitive of particular interest is *digital signature*. With a pair composed of one private key and one public key, a user can sign a message with his secret key and output a signature. Then, any other user can check the authenticity of the signature with the public key and the signer cannot pretend he did not produce the signature since he is supposed to be the unique owner of his secret key. Symmetric primitives do not permit to produce *non-repudiable* signatures. This is because the same key is used both for the signature and the signature checking. This prevents any user from making the difference between signatures produced by the legitimate signatory and signatures produced by any other user.

Though asymmetric cryptography does not require to share secret keys, it requires to share *authentic* keys. Indeed, if one encrypts a message with the public key of a non-legitimate recipient, this non-legitimate recipient can decrypt the message. The usual solution used to ensure the authenticity of the public keys is called a *Public Key Infrastructure* (PKI). This consists in defining some *certification authorities*, which are in charge of verifying the matches between public keys and user identities. They provide certificates that describe a user identity and the associated public key. Digital signatures allow us to check the validity of these certificates.

1.2.2 Usual Primitives

The most famous symmetric encryption primitive is the *Advanced Encryption Standard* (AES)[41]. It is a block cipher, which means that the message is divided into blocks of size 128 bits and each block is encrypted using the algorithm and the secret key (usual key sizes are 128, 192 or 256 bits).

1.2.3 Threats

The security of asymmetric cryptography mostly relies on a small family of well-identified hypotheses of hardness of simple mathematical problems. For instance, the *Rivest Shamir Adleman* (RSA) hypothesis - related to, and not stronger than factoring - for RSA [116], the discrete logarithm in finite fields or elliptic curves for DSA/ECDSA [40, 59] and Schnorr Signatures [124], or related problems like the Computational Diffie-Hellman problem, etc. Thus, a sudden breakthrough either in mathematics or in algorithmics can impact abruptly the security of asymmetric schemes. Furthermore, for example, on a quantum computer Shor algorithm [129] allows to factorize large numbers in polynomial time. Even if a quantum computer able to manipulate thousands of quantum bits (or qubits) should remain out of reach for a while, RSA is definitely not a primitive that will likely provide long-term security guarantees. Indeed, an attacker can still record all the communications until such a device is available.

The situation is rather different for symmetric ciphers. They exhibit a lack of structure which has two consequences: there is no provable security reduction between symmetric algorithms, but conversely their security is not likely to collapse because of some sudden theoretical advance. In fact, the last 30 years of cryptanalytic progress showed that the security of symmetric primitives of early designs like DES [42] or hashing functions like SHA1 tend to erode slowly rather than abruptly, and that more mature designs (the AES competition contenders, the SHA2 family and now the SHA3 family) exhibit a very good resistance to cryptanalysis.

1.3 Quantum Key Distribution

Quantum Key Distribution is a technique allowing to create shared and secret random values at both ends of a communication link, with a security guaranteed without computational hardness assumptions [120]. It requires however a classical authenticated channel, together with an untrusted *quantum* channel, i.e. a physical channel that is used to send quantum states.

In practice, light is a medium of choice to prepare and exchange quantum states. Indeed, one can easily encode information in *discrete variables* such as the phase or the polarization of *single photons*, or in *continuous variables*, such as the phase of the amplitude of the electromagnetic field. The first family of techniques is denoted as DVQKD and the second as CVQKD. For both families the communication medium can be either an optical fiber or a free space optical link.

A lot of QKD demonstrations have been done during the past twenty years and some discrete variables commercial products have been developed [2, 3]. The work of this thesis led to the first commercial product based on continuous variables [5]. The main interest of this technology is that it is implemented with only off-the-shelf components optimized for the telecommunications industry.

1.3.1 Principle

QKD security relies on the fundamental no-cloning theorem which states that one cannot duplicate quantum states without introducing some noise. Consequently, the two participants of a QKD protocol can prepare random states, send them on a quantum channel and reveal at random a fraction of the states they prepared in order to estimate the amount of noise induced by the quantum channel. Any eavesdropper who wants to learn information from the quantum states will interact with them and introduce some noise since he cannot copy them. When the noise level is above a certain limit, the two parts simply abort the protocol and no secret key is obtained.

Even when no eavesdropper tries to measure the quantum states, these states are altered because of their interaction with the environment. The amount of secret key Alice and Bob can extract from a quantum exchange is a function of the noise introduced by the quantum channel. This leads to several practical limitations:

- There must not be any amplifier on the quantum channel: such an equipment actually makes copies of the input signals and therefore introduces a level of noise that is not compatible with the extraction of secret keys.
- Any other signal on the physical channel can disturb the quantum states and therefore prevents the participants from extracting any secret key: in chapter 9, we study the impact of the coexistence of a classical channel with a CVQKD on the same optical fiber.
- The maximum secure distance depends on the losses of both the physical channel and the detection apparatus: commercial systems can deal with about 100 km of optical fiber today while some laboratory experiments were demonstrated over about 250 km.

QKD is currently suited for metropolitan applications. It is worth noting than the use of passive optical switches (that do not amplify the optical signal) can allow to mitigate the number of links that are required to cover a metropolitan network. Dealing with long distances is still possible but requires to use trusted nodes to propagate the keys generated by two consecutive QKD links.

1.3.2 Security Characteristics

The main security property as regards QKD is the *forward secrecy* property. This means that any key produced by a QKD session is totally independent (when the protocol is correctly designed) from the initial key. Thus, the leakage of any past key does not compromise the security of future keys. This property is of utmost practical importance. First, it mitigates the impact of any key leakage due to organizational flaws. Second, it enables the

	Discrete	Continuous (2010)
carrier	photon phase/polarisation	field amplitude-phase
detection	photon counters	coherent
range	100 km	25 km
rate	1Mb/s	10kb/s
components	active cooling	standard
WDM integration	-	+
limitation	detectors	data processing
stability	+	-
side channels	+	-

Table 1.1: This table summarizes the main characteristics of DVQKD and CVQKD and their respective performance and security status in 2010.

production of several independent keys that can be used to encrypt several communications on the same link.

This forward secrecy property cannot be achieved with classical cryptography, except with additional assumptions that do not provide any long-term security guarantees. Furthermore, it contradicts the following common criticism against QKD: since QKD speed does not allow to produce enough keys to encrypt communications using one-time-pad but requires an initial secret key and given the respective price of QKD systems and hard disk storage, why could not one just preshare a high volume of keys instead of constantly generating them with a QKD system? While a one time compromise of the key storage compromises the whole encrypted traffic, only an attacker both compromising the initial key and performing an attack at this very moment would compromise the security of the whole traffic if QKD is employed.

1.3.3 DVQKD vs CVQKD in 2010

Table 1.1 summarizes DVQKD and CVQKD in terms of their characteristics and performance at the beginning of this thesis. The achievable distance of CVQKD was limited to 25 km in 2010 because of the lack of efficient error-correction procedures. This complex data processing also prevented CVQKD from achieving secret key rates higher than 10 kb/s. Concerning DVQKD, it is the dark count rate of the single photon detectors that restricts the range. DVQKD maximum achievable distance is about 100 km with IdQuantique [2] commercial products while some laboratory experiments demonstrated the extraction of secret keys for distances higher than 200 km [137] using superconducting single photon detectors. As regards stability, DVQKD features commercial products that can operate during several years while CVQKD experiments were only reported to work during a few days [44]. Practical demonstrations of side channel attacks against DVQKD have been conducted while the practical security of CVQKD had not been studied yet. A key point related to the integration of QKD in networks is its compatibility with intense classical channels that are wavelength multiplexed on the same optical fiber than the one used for quantum key distribution. The coherent detection used in CVQKD features an intrinsic tolerance to the noise induced by non linear effects in optical fibers [106] while DVQKD requires active filtering to deal with this noise.

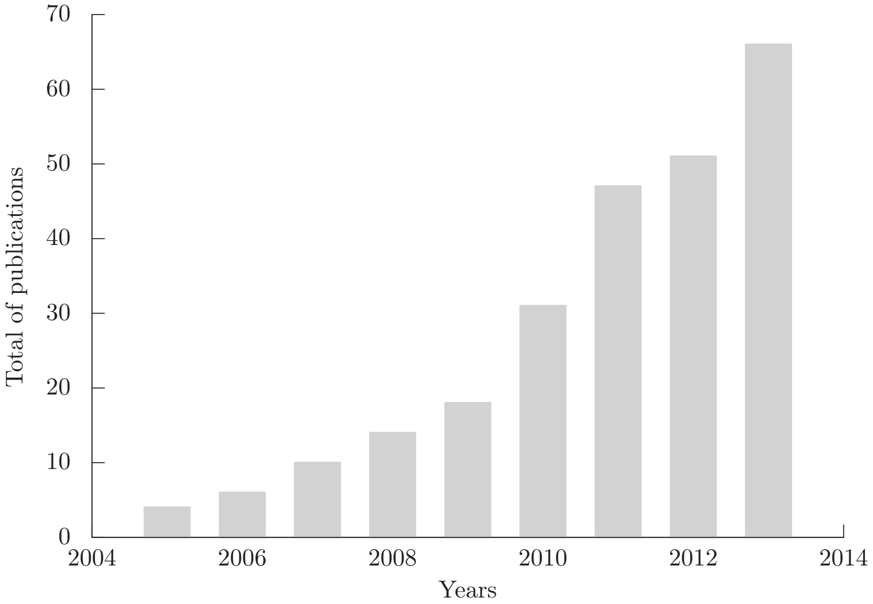


Figure 1.1: Number of publications concerning QKD system imperfections and attacks on QKD systems per year.

1.3.4 Threats

Although QKD protocols provide *theoretical* security proofs that aim at taking into account all the possible attacks accessible to an eavesdropper limited by the quantum mechanics laws, the *practical* security of QKD has been a growing research field over the past ten years as shown in figure 1.1. Indeed, the deviations between theoretical protocols and their practical implementations can open security loopholes also called *side channels*. In chapter 3, we study several practical imperfections of a CVQKD protocol while in chapter 5, we propose a practical attack against a CVQKD protocol and a family of countermeasures to defeat this attack.

Side-channel attacks have been studied for a long time in classical cryptography, mainly in the smart cards community, and had naturally been expected to develop for QKD systems as well. The development of side-channels attacks against equipments that claim unconditional security might seem to sound the death knell of QKD technology but the situation is actually more complicated. Quantum cryptographers developed new theoretical tools allowing us to design device-independent QKD protocols, i.e. protocols whose security do not depend on the details of their implementation. Finally, from a practical security point of view, performing side-channel attacks is a rather difficult task since it must be done during a QKD run and should remain undetected (at least partially).

1.4 Other Quantum Cryptographic Primitives

1.4.1 Coin Flipping

Coin Flipping is a cryptographic protocol which allows two distant distrustful parties to agree on a bit [15]. Unless computational assumptions are made, it is known that any malicious party can bias the coin, even if some quantum communication is allowed between the two parties [81, 96].

However, quantum mechanics allow in theory [131, 6, 19] to limit the bias to an ultimate asymptotic bound of $1/\sqrt{2}$.

In practice, demonstrations must consider all imperfections such that losses in the quantum channel and measurement apparatus or multi-photon pulses generated by standard telecom coherent light sources. In [11], the authors implement a loss-tolerant protocol proposed in [10], but do not demonstrate a quantum advantage for distances longer than a few meters. By means of additional assumptions, such as restricting the security against adversaries limited to imperfect quantum memories, experimental demonstrations of closely related protocols like quantum bit commitment can be realized [156]. In [102], we implemented a coin flipping protocol using a commercial QKD system commercialized by IdQuantique [2]. It demonstrates a quantum advantage over classical protocols for practical distances up to 20 km.

1.4.2 Quantum Signatures

Quantum signatures are the quantum equivalent to classical digital signatures, i.e. they allow a user to protect a document against forgery by another party. However, as previously explained, the security of classical signatures relies on the difficulty of solving some mathematical problems, which may become feasible with a quantum computer. Quantum digital signatures are designed to provide security even against attackers who possess a quantum computer.

For classical signatures, the public key is computed from the private key using a *classical one-way function*, that is a function designed such that computing the output from the input is easy but computing the input given the output is difficult. Quantum signatures follow the same principle but use a *quantum one-way function*. Such a function relies on the *uncertainty principle*, therefore it cannot be inverted even with a quantum computer. In practice, one uses the input private key to prepare a quantum state in such a way that this quantum state leaks a bounded amount of information about the private key to any party that measures the state. Thus, there is an upper bound on the number of quantum public keys that can be created with such a scheme. This is a fundamental difference with the classical case where the number of public keys is not restricted. Furthermore, since it is impossible to copy a quantum state without knowing the state, public keys can be emitted only by the owner of the private key. Another difficulty that occurs when implementing quantum digital signature schemes is designing a procedure allowing to check that different recipients get the same answer when testing the validity of a signed message. While comparing two bit strings is easy, comparing quantum systems is a difficult task. This can be done for example using a *swap test* [48], but this requires a quantum computer, which is hard to implement. Another possibility is quantum comparison of coherent states. This technique was used for the first experimental demonstration of quantum digital signatures in [24].

Chapter 2

Quantum Information with Gaussian Variables

Contents

2.1 Quantum mechanics postulates 16
2.1.1 Notations and basic definitions 16
2.1.2 Quantum operators 17
2.1.3 Composite systems 17
2.1.4 Dynamics of a physical system 18
2.2 Classical Information Theory 18
2.2.1 Entropies 18
2.2.2 Channels and Capacities 21
2.2.3 Channel Coding 23
2.3 Single-mode Quantum Optics 24
2.3.1 One-mode Fock States 25
2.3.2 Coherent States 26
2.3.3 Squeezed States 29
2.4 Two-mode Squeezed States 32
2.5 Weyl Operator 33
2.6 Phase-Space Representation 33
2.7 Gaussian States 34
2.7.1 One mode Gaussian states 34
2.7.2 Two mode Gaussian states 35
2.8 Symplectic Analysis for Multimode Gaussian States 36
2.8.1 One-mode normal decomposition 36
2.8.2 Two-mode normal decomposition 36
2.8.3 Three-mode normal decomposition 37
2.9 Entropy of Gaussian States 37
2.9.1 Von Neumann entropy 37
2.9.2 Entropy of Gaussian states 37
2.9.3 Extremality of Gaussian states 38
2.10 Gaussian Operations 38
2.10.1 Gaussian unitary operations 38
2.10.2 Passive transformations 39
2.10.3 Active transformations 39

In this chapter, we present the theoretical tools that are useful for the understanding of this manuscript. We start by describing the postulates of quantum mechanics. Then, we introduce the basics of classical information theory. Finally, we review the specifics of quantum information with Gaussian variables.

2.1 Quantum mechanics postulates

2.1.1 Notations and basic definitions

A *quantum system* is a physical system whose evolution can be described by quantum mechanics. The first postulate of quantum mechanics is the *postulate of description* that gives the mathematical structure relevant to describe a quantum system. The *quantum state* of a system is a complete description of the system that allows us to predict the results of the experiments we can perform on the system. However, in quantum mechanics, only the probability distributions of the measurements outcomes can be accessed: quantum mechanics is *non-deterministic.*

Axiom 2.1.1.1 (Postulate 1)**.** *Any quantum system is completely described by a state vector, i.e. a unit vector in the system's state space, which is a Hilbert space $\mathcal{H}$.*

A Hilbert space is a complex inner product vector space (finite or infinite dimensional) that is also complete with respect to the distance induced by the inner product. The dimension of this Hilbert space corresponds to the number of degrees of freedom of the considered system. An element of $\mathcal{H}$ is usually written with the Dirac *ket* convention $|x\rangle \in \mathcal{H}$:

$$|x\rangle = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \tag{2.1}$$

in a Hilbert space $\mathcal{H}$ of dimension n. Dual forms in $\mathcal{H}$ are written with the *bra* notation $\langle y| : \mathcal{H} \to \mathbb{C}$:

$$|y\rangle = \begin{pmatrix} y_1^*, y_2^*, \ldots, y_n^* \end{pmatrix} \tag{2.2}$$

The scalar product of two vectors $|y\rangle$ and $|x\rangle$ is a complex number called *braket* and written $\langle y|x\rangle$:

$$\langle y|x\rangle = \begin{pmatrix} y_1^*, y_2^*, \ldots, y_n^* \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \sum_{i=1}^{n} y_i^* x_i \tag{2.3}$$

A *norm* $\|\cdot\|$ can be associated to the inner product of $\mathcal{H}$ and is defined as $\|x\| = \sqrt{\langle x|x\rangle}$. There exists an infinity of orthonormal basis in $\mathcal{H}$, that can be either countable $\{|x_i\rangle\}_{i\in I}$ and satisfy the relation:

$$\langle x_i|x_j\rangle = \delta_i^j \tag{2.4}$$

or uncountable $\{|x\rangle\}_{x\in J}$ and satisfy the relation:

$$\langle x|x^{'}\rangle = \delta(x - x^{'}) \tag{2.5}$$

In a finite-dimensional Hilbert space, any quantum state $|\psi\rangle$ can be decomposed on $\{|x_i\rangle\}_{i\in I}$:

$$|\psi\rangle = \sum_{i\in I} c_i \,|x_i\rangle \,, c_i = \langle x_i|\psi\rangle \,, \tag{2.6}$$

while in an infinite-dimensional Hilbert space, $|\psi\rangle$ can be decomposed on $\{|x\rangle\}_{x\in J}$:

$$|\psi\rangle = \int_J c(x)\,|x\rangle \,\mathrm{d}x, c(x) = \langle x|\psi\rangle \tag{2.7}$$

2.1.2 Quantum operators

The set of linear operators on $\mathcal{H}$ describes the possible evolutions of a quantum system. The identity operator is noted $\hat{\mathbb{1}}$ and *unitary* operators $\hat{U}$ satisfy the relationship $\hat{U}\hat{U}^{-1} = \hat{U}^{-1}\hat{U} = \hat{\mathbb{1}}$ where $\hat{U}^{-1}$ is the inverse of $\hat{U}$. According to the previous decomposition of any quantum state $|\psi\rangle$ in the orthonormal basis of a finite-dimensional Hilbert space $\mathcal{H}$ we have:

$$\sum_{i\in I} |x_i\rangle \langle x_i| \, |\psi\rangle = \sum_{i\in I} c_i \, |x_i\rangle = |\psi\rangle \tag{2.8}$$

One can deduce from this relationship the closure relation:

$$\sum_{i\in I} |x_i\rangle \langle x_i| = \hat{\mathbb{1}} \tag{2.9}$$

and that the projector on any vector $|x\rangle$ can be written $\hat{P}_{|x\rangle} = |x\rangle \langle x|$. A quantum operator $\hat{A}$ admits a matrix representation in any orthonormal basis $\{|x_i\rangle\}_{i\in I}$:

$$\hat{A} = \sum_{i,j\in I} A_{i,j} \, |x_i\rangle \langle x_j| \, , A_{i,j} = \langle x_i|\hat{A}|x_j\rangle \tag{2.10}$$

2.1.3 Composite systems

For complex physical systems involving several quantum systems, one must consider several Hilbert spaces to get a good description of the composite system. The second postulate of quantum mechanics aims at describing composite systems.

Axiom 2.1.3.1 (Postulate 2)**.** *The state space one has to consider to describe a composite physical system is the tensor product of the state spaces of the component physical systems. For a set of systems prepared in the states ψ_i, $1 \leq i \leq n$, the joint state of the composite system is $\otimes_{i=1}^{n}\psi_i$.*

In the case of a bipartite state AB described by the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, the tensor product of $\mathcal{H}_A$ and $\mathcal{H}_B$ defines the Hilbert space $\mathcal{H}_{AB}$ of the bipartite system:

$$\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B \tag{2.11}$$

If $\mathcal{H}_A$ and $\mathcal{H}_B$ have finite dimensions d_A and d_B and respective orthonormal bases $\mathcal{B}_A = \{a_1, \dots, a_{d_A}\}$ and $\mathcal{B}_B = \{b_1, \dots, b_{d_B}\}$, $\mathcal{H}_{AB}$ is finite-dimensional with dimension $d_{AB} = d_A d_B$ and an orthonormal basis for $\mathcal{H}_{AB}$ is $\mathcal{B}_{AB} = \{a_1 \otimes b_1, a_1 \otimes b_2, \dots, a_1 \otimes b_{d_B}, a_2 \otimes b_1, \dots, a_2 \otimes b_{d_B}, \dots, a_{d_A} \otimes b_1, \dots, a_{d_A} \otimes b_{d_B}\}$. A consequence of this tensor structure is the existence of physical systems that cannot be described by vectors. If a state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ can be written $|\psi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$, $|\psi_A\rangle \in \mathcal{H}_A$, $|\psi_B\rangle \in \mathcal{H}_B$, it is a *separable* state. Otherwise it is an *entangled* state, which means that one cannot consider separately its subsystems A and B.

Since in general a system is an unknown statistical mixture of vectors, one can introduce the *density operator* to describe the set of the possible states of the system. The density operator matrix $\hat{\rho}$ can be any positive semidefinite operator of norm unity on $\mathcal{H}$ ($\hat{\rho} \geq 0$ and $\|\hat{\rho}\| = \mathrm{Tr}(\hat{\rho}) = 1$). A density operator is pure if $\hat{\rho}^2 = \hat{\rho}$ and in this case it can be written $\hat{\rho} = |\psi\rangle \langle\psi|$ (another characterization of a pure density operator is that one of its eigen values is equal to one and the others are equal to zero). Any density operator that is not pure is called a mixed density operator.

2.1.4 Dynamics of a physical system

The two other postulates of quantum mechanics describe the dynamics of quantum states both with time and measurement processes. The third postulate concerns the time evolution of a quantum system.

Axiom 2.1.4.1 (Postulate 3)**.** *The evolution of a closed quantum system can be described by a unitary operator $\hat{U}$. The state $|\psi_1\rangle$ of the system at time t_1 is related to the state of the system at time t by the relationship:*

$$|\psi_1\rangle = \hat{U}\,|\psi\rangle \tag{2.12}$$

Another formulation of this postulate is Schrödinger equation for a closed quantum system:

$$i\hbar\frac{d\,|\psi\rangle}{dt} = \hat{H}\,|\psi\rangle\,, \tag{2.13}$$

where $\hat{H}$ is the Hamiltonian operator of the system.

The fourth postulate is relative to the measurement process.

Axiom 2.1.4.2 (Postulate 4)**.** *One can associate a set of measurement operators (also called Positive Operator Valued Measure) $\{M_i\}, i \in I$ to any measure on a quantum state $|\psi\rangle$ in a Hilbert space $\mathcal{H}$. The index i refers to the possible measurement outcomes of the experiment. The probability of getting the result i after the measurement M_i of the quantum state ψ is given by:*

$$p(i) = \langle\psi|M_i^\dagger M_i|\psi\rangle \tag{2.14}$$

The state $\psi^{'}$ of the system after the measurement is:

$$\psi^{'} = \frac{M_i\psi}{\sqrt{\langle\psi|M_i^\dagger M_i|\psi\rangle}}, \tag{2.15}$$

and the measurement operators satisfy the completeness relationship:

$$\sum_{i\in I} M_i^\dagger M_i = \hat{\mathbb{1}} \tag{2.16}$$

We have presented the basic postulates in quantum mechanics. In the next section, we briefly introduce some classical information theory concepts.

2.2 Classical Information Theory

Classical information theory was born in 1948 when Shannon introduced the notions of entropy and channel capacity in [125]. In this introduction, we give a basic description of these notions. The interested reader can refer to more complete references such as [25, 89].

2.2.1 Entropies

The Shannon *entropy* of a random variable X gives a measure of its uncertainty. It is defined as follows:

Definition 2.2.1.1 (Shannon entropy)**.** *Let X be a random variable taking values in the alphabet $\mathcal{X}$ and $p(x)$ be the probability associated with the realization $x \in \mathcal{X}$, then the Shannon entropy $H(X)$ of X is:*

$$H(X) = -\sum_{x\in\mathcal{X}} p(x)\log_2 p(x) \tag{2.17}$$

The joint entropy of two random variables taking values in the alphabets $\mathcal{X}$ and $\mathcal{Y}$ is:

$$H(X,Y) = -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log_2 p(x,y) \tag{2.18}$$

The choice of the base 2 for the logarithm corresponds to the fact that the information is measured in binary digits or bits. Let us illustrate this with the coin flipping game. Since the probability of each possible outcome of the game is one half, the Shannon entropy of the corresponding random variable is $-\log_2 1/2 = 1$. Indeed, flipping a coin gives one bit of information. For a biased coin that gives one outcome with probability one, the corresponding Shannon entropy is $-\log_2 1 = 0$: a certain outcome gives zero bit of information. In general, the entropy of a binary random variable X giving 1 with probability p and 0 with probability $1-p$ is:

$$H(X) = -p\log_2 p - (1-p)\log_2(1-p) = h(p) \tag{2.19}$$

The following theorem gives the useful properties of Shannon entropy that can be deduced from its definition:

Theorem 2.2.1.2 (Properties of the Shannon entropy)**.**

1. *$H(X) \geq 0$, $H(X) = 0$ iff there is no uncertainty on X.*
2. *$H(X,Y) \leq H(X)+H(Y)$, $H(X,Y) = H(X)+H(Y)$ iff X and Y are independent.*
3. *If $\mathcal{X}$ is finite and with n elements, $H(X) \leq \log_2 n$. $H(X) = \log_2 n$ iff X has a uniform distribution on $\mathcal{X}$.*

The operational meaning of the Shannon entropy was established by Shannon in [125]. The limits to possible *data compression* are given in the *source coding theorem*. It states that it is impossible to describe a random variable, also called the source, with a number of bits that is lower than the Shannon entropy of the source. If one tries to map the source to an alphabet whose cardinal is smaller than the Shannon entropy of the source, some information will be lost.

Theorem 2.2.1.3 (Shannon's source coding theorem)**.** *N independent and identically distributed (i.i.d.) random variables each with entropy $H(X)$ can be compressed into more than $NH(X)$ bits with negligible risk of information loss, as N tends to infinity; conversely, if they are compressed into fewer than $NH(X)$ bits it is virtually certain that information will be lost.*

Shannon entropy can be generalized to define a family of entropies parameterized by a parameter α. The Renyi entropy of order α of a random variable X is:

$$\forall\alpha \geq 0, \alpha \neq 1, H_\alpha(X) = -\frac{1}{1-\alpha}\log_2 \sum_{x\in\mathcal{X}} p(x)^\alpha \tag{2.20}$$

Some values of α are of particular interest:

- $\alpha = 0$: it is called *max-entropy* of X and is noted either $H_0(X)$ or $H_{max}(X)$. Its value is $H_0(X) = \log_2|X|$.
- $\alpha = 1$: $H_1(X) = H(X)$, the Shannon entropy of X.
- $\alpha = 2$: $H_2(X) = -\log_2\left(\sum_{x\in\mathcal{X}} p(x)^2\right) = -\log_2 P\left(X = X^{'}\right)$, where $X^{'}$ is a random variable independent from X but with the same law. It is called the collision entropy.

– $\alpha = \infty$: $H_\infty(X) = -\log_2 \sup_{x\in\mathcal{X}} p(x) = H_{min}(X)$ is the *min-entropy* of X and is related to the maximum probability of guessing the value of X.

The following inequality relates the min-entropy, entropy and max-entropy of a random variable X:

$$H_{min}(X) \leq H(X) \leq H_{max}(X) \tag{2.21}$$

the inequalities being saturated in the case of uniformly distributed random variable.

Conditional entropy is a powerful tool that allows us to characterize a random variable provided the knowledge of another random variable. For two random variables X and Y defined on the alphabets $\mathcal{X}$ and $\mathcal{Y}$, the conditional entropy of the random variable X given the random variable Y is:

$$H(X|Y) = -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log_2 p(x|y) \tag{2.22}$$

Conditioning with respect to a random variable reduces the entropy:

$$\forall X, Y, H(X|Y) \leq H(X) \tag{2.23}$$

with equality iff X and Y are independent random variables. The following chain rule property of the Shannon entropy is satisfied:

$$\forall X, Y, H(X,Y) = H(X) + H(Y|X) = H(Y) + H(X|Y) \tag{2.24}$$

which basically means that the uncertainty on the couple of random variables is equal to the uncertainty on the first random variable plus the uncertainty on the second random variable knowing the first random variable.

Another quantity of interest is the *mutual information* between the random variables X and Y. It basically gives a measure of the correlation between these random variables:

$$I(X:Y) = -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log_2 \frac{p(x,y)}{p(x)p(y)} \tag{2.25}$$

One can see that the mutual information between two independent random variables is zero and that mutual information is always non negative. One can also check the following relationships:

$$\begin{aligned} I(X:Y) &= H(X) - H(X|Y) && (2.26)\\ &= H(Y) - H(Y|X) && (2.27)\\ &= H(X) + H(Y) - H(X,Y) && (2.28)\end{aligned}$$

Conditional mutual information can be defined in the same way than for entropy:

$$I(X:Y|Z) = H(X|Z) - H(X|Y,Z) \tag{2.29}$$

Contrary to entropy, conditioning can either increase or decrease the mutual information.

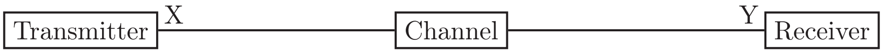


Figure 2.1: Shannon's coding theorem schematics.

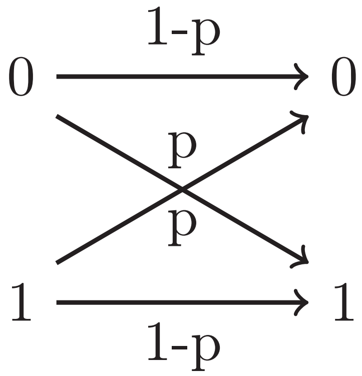


Figure 2.2: Binary symmetric channel transition probabilities.

2.2.2 Channels and Capacities

Another very important notion introduced by Shannon is the Shannon *capacity* of a communication channel. It corresponds to the theoretical maximum information transfer rate of the channel for a particular noise level. Let us consider the scheme of Figure 2.1 where a transmitter encodes messages using a discrete input alphabet $\mathcal{X}$ and a receiver receives messages that belong to a discrete output alphabet $\mathcal{Y}$ from the noisy channel. If the probability distribution of the output random variable Y only depends on the input random variable X at the same time, the channel is said to be *memoryless*. The capacity of the discrete memoryless channel is defined as:

$$C = \sup_{p(x)} I(X:Y) \tag{2.30}$$

where the supremum is taken over all possible choices of $p(x)$.

It is interesting to look at the capacities of some commonly studied channels. The *Binary Symmetric Channel* (BSC) is a channel where the input and output random variables are binary. When one tries to transmit a bit over this channel, it is changed with probability p and unchanged with probability $1-p$. The transition probabilities are represented in Figure 2.2. Let us compute the capacity of the BSC:

$$\begin{aligned} I(X:Y) &= H(Y) - H(Y|X) & (2.31)\\ &= H(Y) - \sum_{x\in\mathcal{X}} p(x) H(Y|X=x) & (2.32)\\ &= H(Y) - p\log_2 p - (1-p)\log_2(1-p) & (2.33)\\ &\leq 1 - h(p) & (2.34)\end{aligned}$$

where $h(p) = -p\log_2 p - (1-p)\log_2(1-p)$ is the binary entropy function. The last inequality comes from the fact that the entropy of a binary random variable is upper bounded by 1. It is saturated when the distribution of the

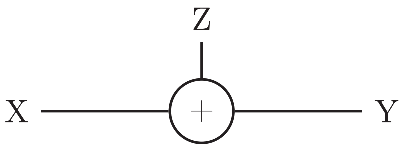


Figure 2.3: Additive white Gaussian noise channel schematics. A Gaussian noise Z is added to the input random variable X and the output random variable is $Y = X + Z$.

input random variable X is uniform. This shows that the capacity of the BSC is:

$$C_{\text{BSC}} = 1 - h(p) \tag{2.35}$$

which gives a capacity equal to 1 when no error occurs on the channel and a capacity equal to 0 when an error occurs with probability 1/2.

When one wants to deal with continuous variables, the concept of *differential entropy* must be used. For a random variable X defined on the continuous domain $\mathcal{X}$ and that admits a density function $p(x)$, the differential entropy $h(X)$ is:

$$H(X) = -\int_{x\in\mathcal{X}} p(x)\log_2 p(x)\,\mathrm{d}x \tag{2.36}$$

It is not hard to design examples of random variables for which the differential entropy does not exist. Furthermore, this quantity can be negative contrary to the discrete entropy.

Let us compute the differential entropy of a normal distribution Z of density $\phi(z) = \frac{1}{\sqrt{2\pi\sigma^2}}\exp -\frac{z^2}{2\sigma^2}$:

$$\begin{aligned} h(Z) &= -\int_z \phi(z)\ln\phi(z)\,\mathrm{d}z && (2.37)\\ &= -\int_z \phi(z)\left(-\frac{z^2}{2\sigma^2} - \frac{1}{2}\ln\left(2\pi\sigma^2\right)\right)\mathrm{d}z && (2.38)\\ &= \frac{E[Z^2]}{2\sigma^2} + \frac{1}{2}\ln\left(2\pi\sigma^2\right) && (2.39)\\ &= \frac{1}{2} + \frac{1}{2}\ln\left(2\pi\sigma^2\right) && (2.40)\\ &= \frac{1}{2}\ln\left(2\pi e\sigma^2\right) && (2.41)\\ &= \frac{1}{2}\log_2\left(2\pi e\sigma^2\right) && (2.42) \end{aligned}$$

where the last equality gives the result in bits. Let us use this result to compute the mutual information between the input X and the output Y of an *Additive White Gaussian Noise Channel* (AWGNC), which are related through $Y = X + Z$ with Z a Gaussian noise of variance σ^2 independent from the input (see Figure 2.3). Such a channel has an infinite capacity for a general output. When considering an input with a finite variance Σ^2, the capacity is finite. The mutual information is given by:

$$\begin{aligned} I(X:Y) &= h(Y) - h(Y|X) && (2.43)\\ &= h(Y) - h(X+Z|X) && (2.44)\\ &= h(Y) - h(X|X) - h(Z|X) && (2.45)\\ &= h(Y) - h(Z) && (2.46) \end{aligned}$$

where the last equality comes from the independence of X and Z. The variance of Y is:

$$E[Y^2] = E[(X+Z)^2] \tag{2.47}$$

$$= E[X^2] + E[Z^2] + 2E[X]E[Z] \tag{2.48}$$

$$= \Sigma^2 + \sigma^2 \tag{2.49}$$

since X and Z are independent and $E[Z] = 0$. Since the normal distribution maximizes the entropy for a given variance (see Theorem 9.6.5 of [25]), one can bound $h(Y)$:

$$h(Y) \leq \frac{1}{2} \log_2 2\pi e \left(\Sigma^2 + \sigma^2\right) \tag{2.50}$$

and we get:

$$I(X:Y) \leq \frac{1}{2} \log_2 \left(1 + \frac{\Sigma^2}{\sigma^2}\right) \tag{2.51}$$

Hence the capacity of the AWGNC, which is achieved for a normal input distribution is:

$$C_{\text{AWGNC}} = \frac{1}{2} \log_2 (1 + \text{SNR}) \tag{2.52}$$

where the *Signal to Noise Ratio* (SNR) is defined as SNR$= \Sigma^2/\sigma^2$.

Although the capacity of the AWGNC gives a tight upper bound on the information transfer rate of a channel that adds a Gaussian noise, this bound can never be achieved in practice because practical modulation schemes are limited to a finite alphabet and cannot use the entire set of real numbers. However, when studying the security of a CVQKD scheme with a Gaussian modulation we use the formula of the capacity of the AWGNC when we want to estimate the mutual information between Alice and Bob. We emphasize the fact that although this approximation leads to an optimistic value of the mutual information and therefore of the theoretical secret key rate, the practical implementation of the *discretized* Gaussian modulation directly leads to a mutual information that is lower than the theoretical mutual information with a perfect Gaussian modulation. Thus this does not result in an overestimation of the practical secret key rate.

Among the transmission schemes, the *binary input* modulation scheme is of particular interest. Indeed, we will see in Chapter 6 that it is particularly useful to build a *Binary Input Additive White Gaussian Noise Channel* (BIAWGNC) on top of the Gaussian channel. We give the analytical form of the capacity of the BIAWGNC:

$$C_{\text{BIAWGNC}} = \frac{1}{\sigma^2} - \int_{-\infty}^{\infty} \frac{e^{-\frac{x^2}{2}}}{\sqrt{2\pi}} \log_2 \cosh\left(\frac{1}{\sigma^2} + \frac{x}{\sigma}\right) \mathrm{d}x \tag{2.53}$$

2.2.3 Channel Coding

Now that we have defined the capacity of a noisy channel, we are interested in transmitting information reliably on a noisy channel. This can be done by adding *redundancy* to the data we want to transmit, which acts as a protection from noise. This can be easily understood considering the BSC and a particular information transfer scheme, the repetition scheme. Let us assume that we want to transmit one bit on a BSC of parameter $p = 0.1$. If we send directly this bit over the channel, information is lost with probability 0.1. Now, if we transmit this same bit three consecutive times and decide that the correct value for this bit is the most frequent value among received values, information is lost if two flips of three flips occurred which happens with probability $p^3 + 3 \times p^2 \times (1-p) = 0.028$. The probability of losing information has been reduced.

Mathematically, the repetition scheme we considered is a particular example of an *error-correcting code*, i.e. a mapping from a finite set, the source alphabet, to another finite set, the target alphabet. This can be extended to sequences of symbols in both alphabets. The goal of error-correcting codes is to recover reliably the information sent through the communication channel. They differ by their *rate* R, which is a measure of the amount of redundancy of a code. The rate of a code is defined by the ratio between the number of information bits and the length of the code word n:

$$R = \frac{\log_2 |\mathcal{X}|}{n} \tag{2.54}$$

For the previous repetition scheme the rate is 1/3 since one bit of information corresponds to three bits sent through the channel. The channel coding theorem stated by Shannon in 1948 gives the maximum possible efficiency of error-correcting codes with respect to the level of noise.

Theorem 2.2.3.1 (Shannon's channel coding theorem)**.** *For any $\epsilon > 0$ and for any rate R less than the channel capacity C, there exists an encoding and decoding scheme that can be used to ensure that the probability of decoding error is less than $\epsilon > 0$ for a sufficiently large block length. Also, for any rate greater than the channel capacity, the probability of error at the receiver goes to one as the block length goes to infinity.*

Although this theorem gives a fundamental limit to the maximum reliable transmission rate through a noisy channel, one still needs to design encoding and decoding schemes more subtle than the repetition scheme in order to achieve these limits. Among the commonly used code families, *Low Density Parity Check* (LDPC) codes provide a mathematical description [114] that makes them adaptable for different channels. We designed a particular type of LDPC codes, *multi-edge* LDPC codes, for the BIAWGNC in chapter 6 and explained how to use them to increase the range of CVQKD. In 2008, another family of codes that achieve the capacity for all discrete memoryless channels was introduced by Arıkan [8]. These are *polar codes.* In chapter 8, we designed polar codes for the BSC and the BIAWGNC and studied their use for both DVQKD and CVQKD. A particularity of currently known coding schemes is that their decoding complexity increases roughly when approaching the capacity. This results in a speed limitation in a practical QKD system. In chapter 8, we give our decoding performance results with both LDPC and polar codes and investigate the use of *Graphics Processing Units* (GPU) to increase the decoding speed of LDPC codes.

2.3 Single-mode Quantum Optics

We have seen that Hilbert spaces of potentially high dimension must be used to describe a quantum system, in particular when the quantum system involves several modes of the electromagnetic field. A mode is described by a polarization state, an energy level and a wave function. Fortunately, a N-mode quantum state can be decomposed over N Hilbert spaces, each one corresponding to one mode of the field. The tensor product of N one-mode *Fock spaces* $\mathcal{H}_i$ describes a N-mode quantum system $\mathcal{H}$:

$$\mathcal{H} = \otimes_{i=1}^{N} \mathcal{H}_i \tag{2.55}$$

Each Fock space can be described by a basis $\{|0\rangle, \ldots, |n\rangle, \ldots\}$ where the *Fock state* $|n\rangle$ corresponds to the state of n photons present in the mode described by this Fock space. In the following, we introduce the basic equations that are used when dealing with Fock states.

2.3.1 One-mode Fock States

The annihilation $\hat{a}$ and creation $\hat{a}^\dagger$ operators for a given mode are:

$$\hat{a}\,|n\rangle = \sqrt{n}\,|n-1\rangle\,, n > 0, \hat{a}\,|0\rangle = 0 \tag{2.56}$$

$$\hat{a}^\dagger\,|n\rangle = \sqrt{n+1}\,|n+1\rangle\,, n \geq 0 \tag{2.57}$$

where $|0\rangle$ corresponds to the state with no photon. These two operators are linked by the commutation relationship:

$$[\hat{a}, \hat{a}^\dagger] = 1 \tag{2.58}$$

By applying n times the operator $\hat{a}^\dagger$ to the vacuum state $|0\rangle$ that contains no photon we obtain:

$$|n\rangle = \frac{1}{\sqrt{n!}} \left(\hat{a}^\dagger\right)^n |0\rangle \tag{2.59}$$

An eigenstate $|n\rangle$ of the number operator $\hat{N} = \hat{a}^\dagger\hat{a}$ ($\hat{N}^\dagger = \hat{N}$) is called a Fock state (we also have $\hat{a}\hat{a}^\dagger = \hat{N}+1$) or a state with n photons in the mode defined by a frequency ω:

$$\hat{a}^\dagger\hat{a}\,|n\rangle = \hat{N}\,|n\rangle = n\,|n\rangle \tag{2.60}$$

A Fock state is also an eigen vector of the Hamiltonian:

$$H\,|n\rangle = \hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right)|n\rangle \tag{2.61}$$

$$= E_n\,|n\rangle \tag{2.62}$$

with the energy eigen value being $E_n = \hbar\omega\,(n + 1/2)$.

Quadratures operators

The quadratures of the electromagnetic field are linked to the annihilation and creation operators by:

$$\hat{x} = \frac{1}{\sqrt{2}}\left(\hat{a}^\dagger + \hat{a}\right) \tag{2.63}$$

$$\hat{p} = \frac{i}{\sqrt{2}}\left(\hat{a}^\dagger - \hat{a}\right) \tag{2.64}$$

They are Hermitian operators and are linked by the commutation relationship:

$$[\hat{x}, \hat{p}] = -i \tag{2.65}$$

Statistics

It is interesting to compute some basic statistics for the Fock states:

$$\langle n \rangle = \langle n|\hat{N}|n\rangle = n\,\langle n|n\rangle = n \tag{2.66}$$

$$\langle n^2 \rangle = \langle n|\hat{N}^2|n\rangle = n^2\,\langle n|n\rangle = n^2 \tag{2.67}$$

using the orthonormality of the Fock states basis. Then the variance is $(\Delta n)^2 = \langle n^2\rangle - \langle n\rangle^2 = n^2 - n^2 = 0$.

Let us do the same calculations with the quadratures $\hat{x}$ and $\hat{p}$:

$$\langle n|\hat{x}|n\rangle = \frac{1}{\sqrt{2}}\,\langle n|\hat{a}^\dagger + \hat{a}|n\rangle = \frac{1}{\sqrt{2}}\left(\sqrt{n+1}\,\langle n|n+1\rangle + \sqrt{n}\,\langle n|n-1\rangle\right) = 0 \tag{2.68}$$

$$\langle n|\hat{p}|n\rangle = \frac{i}{\sqrt{2}}\,\langle n|\hat{a}^\dagger - \hat{a}|n\rangle = \frac{i}{\sqrt{2}}\left(\sqrt{n+1}\,\langle n|n+1\rangle - \sqrt{n}\,\langle n|n-1\rangle\right) = 0 \tag{2.69}$$

where we used the orthonormality of the Fock states basis. We also have:

$$\langle n|\hat{x}^2|n\rangle = \frac{1}{2}\,\langle n|\hat{a}^\dagger\hat{a}^\dagger + \hat{a}^\dagger\hat{a} + \hat{a}\hat{a}^\dagger + \hat{a}\hat{a}|n\rangle = \frac{1}{2}\left(\hat{a}^\dagger\hat{a} + \hat{a}\hat{a}^\dagger\right) = \frac{2n+1}{2} \tag{2.70}$$

$$\langle n|\hat{p}^2|n\rangle = \frac{-1}{2}\,\langle n|\hat{a}^\dagger\hat{a}^\dagger - \hat{a}^\dagger\hat{a} - \hat{a}\hat{a}^\dagger + \hat{a}\hat{a}|n\rangle = \frac{1}{2}\left(\hat{a}^\dagger\hat{a} + \hat{a}\hat{a}^\dagger\right) = \frac{2n+1}{2} \tag{2.71}$$

Thus $(\Delta\hat{x})^2 = (\Delta\hat{p})^2 = \frac{2n+1}{2}$ and:

$$\Delta\hat{x}\Delta\hat{p} = \frac{2n+1}{2} \geq \frac{1}{2} \tag{2.72}$$

where the equality holds for the vacuum state.

2.3.2 Coherent States

Contrary to Fock states, coherent states do not have a precisely known number of photons. In addition to that, their phase is not completely random. Furthermore, the product of the uncertainty on the amplitude and the uncertainty on the phase corresponds to the minimum allowed by quantum mechanics. Thus they are the closest states to classical states.

Let us define the unitary displacement operator:

$$D(\alpha) = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}} \tag{2.73}$$

with α being an arbitrary complex number. The following theorems hold:

Theorem 2.3.2.1 (Disentangling theorem)**.** *For two operators such that* $[\hat{A},[\hat{A},\hat{B}]] = [\hat{B},[\hat{A},\hat{B}]] = 0$, *we have* $[\hat{A}, f(\hat{B})] = f^{'}(\hat{B})[\hat{A},\hat{B}]$.

and

Theorem 2.3.2.2. *For two non-commuting operators* $\hat{A}$ *and* $\hat{B}$ *such that* $[\hat{A},[\hat{A},\hat{B}]] = [\hat{B},[\hat{A},\hat{B}]] = 0$ *we have:*

$$e^{\hat{A}+\hat{B}} = e^{\hat{A}}e^{\hat{B}}e^{-[\hat{A},\hat{B}]/2} = e^{\hat{B}}e^{\hat{A}}e^{[\hat{A},\hat{B}]/2} \tag{2.74}$$

We can apply this theorem with $\hat{A} = \alpha\hat{a}^\dagger$ and $\hat{B} = -\alpha^*\hat{a}$ together with the relation $[\hat{a}, \hat{a}^\dagger] = 1$. Since $[\hat{A}, \hat{B}] = |\alpha|^2$, $[\hat{A}, [\hat{A}, \hat{B}]] = 0$ and $[\hat{B}, [\hat{A}, \hat{B}]] = 0$:

$$D(\alpha) = e^{-|\alpha|^2/2} e^{\alpha\hat{a}^\dagger} e^{-\alpha^*\hat{a}} \tag{2.75a}$$

$$D(\alpha) = e^{|\alpha|^2/2} e^{-\alpha^*\hat{a}} e^{\alpha\hat{a}^\dagger} \tag{2.75b}$$

The first equation corresponds to the normal form (the creation operator appears to the left of annihilation operators when the exponentials are written as power series) and the second equation to the anti-normal form. The hermitian conjugate of Eq. 2.75a is:

$$D^\dagger(\alpha) = e^{-|\alpha|^2/2} e^{-\alpha\hat{a}^\dagger} e^{\alpha^*\hat{a}} \tag{2.76}$$

thus by multiplying by Eq. 2.75b we get:

$$D(\alpha)D^\dagger(\alpha) = 1 \tag{2.77}$$

which proves that $D(\alpha)$ is a unitary operator.
Thus we have:

$$D^\dagger(\alpha) = e^{-|\alpha|^2/2} e^{-\alpha\hat{a}^\dagger} e^{\alpha^*\hat{a}} = D^{-1}(\alpha) = e^{|\alpha|^2/2} e^{\alpha^*\hat{a}} e^{-\alpha\hat{a}^\dagger} \tag{2.78}$$

$$= D(-\alpha) \tag{2.79}$$

where we used the previous theorem with $\hat{A} = -\alpha\hat{a}^\dagger$ and $\hat{B} = \alpha^*\hat{a}$ to get the last equality.

The Hadamard lemma gives:

$$e^{-\zeta\hat{A}}\hat{B}e^{\zeta\hat{A}} = \hat{B} - \zeta[\hat{A}, \hat{B}] + \frac{\zeta^2}{2!}[\hat{A}, [\hat{A}, \hat{B}]] - \frac{\zeta^3}{3!}[\hat{A}, [\hat{A}, [\hat{A}, \hat{B}]]] + \dots \tag{2.80}$$

Let us use $\hat{A} = -\alpha\hat{a}^\dagger$ and $\hat{B} = \hat{a}$. We have:

$$e^{\hat{A}} = e^{-\alpha\hat{a}^\dagger + \alpha^*\hat{a}} = D^{-1}(\alpha) \tag{2.81}$$

$$e^{-\hat{A}} = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}} = D(\alpha) \tag{2.82}$$

$$[\hat{A}, \hat{B}] = -\alpha[\hat{a}^\dagger, \hat{a}] = \alpha \tag{2.83}$$

and all higher order commutators are null. This gives:

$$D^{-1}(\alpha)\hat{a}D(\alpha) = \hat{a} + \alpha \tag{2.84}$$

$$D^{-1}(\alpha)\hat{a}^\dagger D(\alpha) = \hat{a}^\dagger + \alpha^* \tag{2.85}$$

The same technique gives:

$$D(\alpha)\hat{a}D^{-1}(\alpha) = \hat{a} - \alpha \tag{2.86}$$

$$D(\alpha)\hat{a}^\dagger D^{-1}(\alpha) = \hat{a}^\dagger - \alpha^* \tag{2.87}$$

A coherent state can be obtained from a displacement of the vacuum state in the phase space. When we apply a unitary operation by $D(\alpha)$ to the annihilation and creation operators, they are augmented by α and α^* respectively.

The coherent state $|\alpha\rangle$ is obtained by applying $D(\alpha)$ to the vacuum state $|0\rangle$:

$$|\alpha\rangle = D(\alpha)\,|0\rangle \tag{2.88}$$

Thus by applying $D^\dagger(\alpha)\hat{a}$ to previous equality we get:

$$D^\dagger(\alpha)\hat{a}\left|\alpha\right\rangle = D^\dagger(\alpha)\hat{a}D(\alpha)\left|0\right\rangle = (\hat{a}+\alpha)\left|0\right\rangle = \alpha\left|0\right\rangle \tag{2.89}$$

since $\hat{a}\left|0\right\rangle = 0$. Thus by multiplying by the unitary operator $D(\alpha)$ we get:

$$\hat{a}\left|\alpha\right\rangle = \alpha\left|\alpha\right\rangle \tag{2.90}$$

which proves that the coherent states are eigenstates of the annihilation operator $\hat{a}$.
The same technique can apply to the quadratures of the field and gives:

$$D^\dagger(\alpha)\hat{x}D(\alpha) = \hat{x} + \sqrt{2}\mathcal{R}\left(\alpha\right) \tag{2.91}$$
$$D^\dagger(\alpha)\hat{p}D(\alpha) = \hat{p} + \sqrt{2}\mathcal{I}\left(\alpha\right) \tag{2.92}$$

where $\mathcal{R}$ and $\mathcal{I}$ are the real and imaginary parts.

The power series expansion of an exponential operator gives:

$$e^{-\alpha^*\hat{a}}\left|0\right\rangle = \sum_n \frac{(-\alpha^*\hat{a})^n}{n!}\left|0\right\rangle = \left|0\right\rangle \tag{2.93}$$
$$e^{\alpha\hat{a}^\dagger}\left|0\right\rangle = \sum_n \frac{\left(\alpha\hat{a}^\dagger\right)^n}{n!}\left|0\right\rangle = \sum_n \frac{\alpha^n}{\sqrt{n!}}\left|n\right\rangle \tag{2.94}$$

thus:

$$\left|\alpha\right\rangle = D(\alpha)\left|0\right\rangle = e^{-\frac{|\alpha|^2}{2}}e^{\alpha\hat{a}^\dagger}e^{-\alpha^*\hat{a}}\left|0\right\rangle = e^{-\frac{|\alpha|^2}{2}}e^{\alpha\hat{a}^\dagger}\left|0\right\rangle \tag{2.95}$$
$$= e^{-\frac{|\alpha|^2}{2}}\sum_n \frac{\alpha^n}{\sqrt{n!}}\left|n\right\rangle \tag{2.96}$$

The number of photons of a coherent state is undefined but this allows them to have a phase relatively well defined contrary to Fock states that have a totally random phase. The probability distribution of photons in a coherent state is obtained by:

$$P(n) = |\left\langle n|\alpha\right\rangle|^2 = e^{-|\alpha|^2}\frac{|\alpha|^{2n}}{n!} \tag{2.97}$$

and the scalar product of two coherent states is:

$$\langle\beta|\alpha\rangle = \langle 0|D^\dagger(\beta)D(\alpha)|0\rangle = \langle 0|D(\alpha-\beta)|0\rangle = \langle 0|\alpha-\beta\rangle \tag{2.98}$$
$$= e^{-\frac{|\alpha|^2}{2}-\frac{|\beta|^2}{2}+\alpha\beta^*} = e^{-\frac{|\alpha-\beta|^2}{2}} \tag{2.99}$$

Thus two coherent states are never orthogonal though two states become approximately orthogonal in the limit $|\alpha-\beta| \gg 1$.

Statistics

For a coherent state:

$$\langle n\rangle = \langle\alpha|\hat{N}|\alpha\rangle = \alpha\left\langle\alpha|\hat{a}^\dagger|\alpha\right\rangle = |\alpha|^2 \tag{2.100}$$
$$\langle n^2\rangle = \langle\alpha|\hat{N}^2|\alpha\rangle = |\alpha|^4 + |\alpha|^2 \tag{2.101}$$

because $\langle\alpha|\hat{a}\hat{a}^\dagger|\alpha\rangle = |\alpha|^2 + 1$. The variance is $(\Delta n)^2 = \alpha^4 + \alpha^2 - \alpha^4 = \alpha^2$. For the quadrature operators, we have:

$$\langle\alpha|\hat{x}|\alpha\rangle = \frac{1}{\sqrt{2}}\langle\alpha|\hat{a}^\dagger + \hat{a}|\alpha\rangle = \frac{1}{\sqrt{2}}(\alpha^* + \alpha) \tag{2.102}$$

$$\langle\alpha|\hat{p}|\alpha\rangle = \frac{i}{\sqrt{2}}\langle\alpha|\hat{a}^\dagger - \hat{a}|\alpha\rangle = \frac{1}{\sqrt{2}}(\alpha^* - \alpha) \tag{2.103}$$

$$\langle\alpha|\widehat{x^2}|\alpha\rangle = \frac{1}{2}\langle\alpha|\hat{a}^\dagger\hat{a}^\dagger + \hat{a}^\dagger\hat{a} + \hat{a}\hat{a}^\dagger + \hat{a}\hat{a}|\alpha\rangle = \frac{1}{2}\left(\alpha^{*2} + 2\alpha^2 + 1 + |\alpha|^2\right) \tag{2.104}$$

$$\langle\alpha|\widehat{p^2}|\alpha\rangle = \frac{-1}{2}\langle\alpha|\hat{a}^\dagger\hat{a}^\dagger - \hat{a}^\dagger\hat{a} - \hat{a}\hat{a}^\dagger + \hat{a}\hat{a}|\alpha\rangle = \frac{1}{2}\left(\alpha^{*2} - 2\alpha^2 - 1 + |\alpha|^2\right) \tag{2.105}$$

Thus $(\Delta\hat{x})^2 = (\Delta\hat{p})^2 = \frac{1}{2}$ and $\Delta\hat{x}\Delta\hat{p} = \frac{1}{2}$.

2.3.3 Squeezed States

Squeezed states are a general class of minimum-uncertainty states. In general a squeezed state has less noise in one quadrature than a coherent state and consequently more noise in the other quadrature to satisfy the requirements of a minimum-uncertainty state (whereas coherent states have the same amount of noise in both quadratures).

Squeezed states can be generated with a squeezing operator defined by:

$$S(z) = e^{\frac{1}{2}\left(z\hat{a}^2 - z^*\hat{a}^{\dagger 2}\right)} \tag{2.106}$$

for a complex number $z = re^{-i\phi}$. This operator is hermitian and has the following properties:

$$S^\dagger(z) = S^{-1}(z) = S(-z) \tag{2.107}$$

We can apply Eq. 2.80 with $\hat{A} = \frac{-i}{2}\left(z\hat{a}^2 - z^*\hat{a}^{\dagger 2}\right)$:

$$\hat{t} = S(z)\hat{a}S^\dagger(z) = e^{i\hat{A}}\hat{a}e^{-i\hat{A}} \tag{2.108}$$

$$= \hat{a} + [i\hat{A}, \hat{a}] + \frac{1}{2!}[i\hat{A}, [i\hat{A}, \hat{a}]] + \frac{1}{3!}[i\hat{A}, [i\hat{A}, [i\hat{A}, \hat{a}]]] + \dots \tag{2.109}$$

The commutation relation $[\hat{a}, \hat{a}^\dagger] = 1$ gives:

$$[i\hat{A}, \hat{a}] = z^*\hat{a}^\dagger \tag{2.110}$$

$$\hat{t} = \hat{a} + z^*\hat{a}^\dagger + \frac{1}{2!}|z|^2\hat{a} + \frac{1}{3!}|z|^2 z^*\hat{a}^\dagger + \frac{1}{4!}|z|^4\hat{a} + \dots \tag{2.111}$$

$$= \hat{a}\left(1 + \frac{1}{2!}r^2 + \frac{1}{4!}r^4 + \dots\right) + \hat{a}^\dagger e^{i\phi}\left(r + \frac{1}{3!}r^3 + \dots\right) \tag{2.112}$$

$$= \hat{a}\cosh(r) + \hat{a}^\dagger e^{i\phi}\sinh(r) \tag{2.113}$$

and:

$$\hat{t}^\dagger = \hat{a}^\dagger\cosh(r) + \hat{a}e^{-i\phi}\sinh(r) \tag{2.114}$$

We have the commutation relation:

$$[\hat{t}, \hat{t}^\dagger] = 1 \tag{2.115}$$

and the transformations:

$$\begin{bmatrix} \hat{a} \\ \hat{a}^\dagger \end{bmatrix} = \begin{bmatrix} \cosh(r) & -e^{i\phi}\sinh(r) \\ -e^{-i\phi}\sinh(r) & \cosh(r) \end{bmatrix} \begin{bmatrix} \hat{t} \\ \hat{t}^\dagger \end{bmatrix} \tag{2.116}$$

and:

$$\begin{bmatrix} \hat{t} \\ \hat{t}^\dagger \end{bmatrix} = \begin{bmatrix} \cosh(r) & e^{i\phi}\sinh(r) \\ e^{-i\phi}\sinh(r) & \cosh(r) \end{bmatrix} \begin{bmatrix} \hat{a} \\ \hat{a}^\dagger \end{bmatrix} \tag{2.117}$$

Let us now apply the transformation with quadrature components $\hat{x}$ and $\hat{p}$ and $\phi = 0$:

$$\hat{t_1} = \frac{1}{\sqrt{2}}(\hat{t}^\dagger + \hat{t}) = \frac{1}{\sqrt{2}}(S(z)(\hat{a}^\dagger + \hat{a})S^\dagger(z)) \tag{2.118}$$

$$= \frac{1}{\sqrt{2}}(\hat{a}^\dagger + \hat{a})(\cosh(r) + \sinh(r)) = \hat{x}e^r \tag{2.119}$$

$$\hat{t_2} = \frac{i}{\sqrt{2}}(\hat{t}^\dagger - \hat{t}) = \frac{1}{\sqrt{2}}(S(z)(\hat{a}^\dagger - \hat{a})S^\dagger(z)) \tag{2.120}$$

$$= \frac{i}{\sqrt{2}}(\hat{a}^\dagger - \hat{a})(\cosh(r) - \sinh(r)) = \hat{p}e^{-r} \tag{2.121}$$

Let us denote by $(\hat{x}_{in}, \hat{p}_{in})$ and $(\hat{x}_{out}, \hat{p}_{out})$ the quadrature operators respectively before and after applying the previous transformation. We have:

$$\begin{bmatrix} \hat{x}_{out} \\ \hat{p}_{out} \end{bmatrix} = \begin{bmatrix} e^{-r} & 0 \\ 0 & e^r \end{bmatrix} \begin{bmatrix} \hat{x}_{in} \\ \hat{p}_{in} \end{bmatrix} \tag{2.122}$$

We can define the complex numbers τ and τ^*:

$$\tau = \alpha\cosh(r) + \alpha^* e^{i\phi}\sinh(r) \tag{2.123}$$

$$\tau^* = \alpha^*\cosh(r) + \alpha e^{-i\phi}\sinh(r) \tag{2.124}$$

and we have:

$$\tau\hat{t}^\dagger - \tau^*\hat{t} = \alpha\hat{a}^\dagger - \alpha^*\hat{a} \tag{2.125}$$

In a similar manner to the definition of coherent states we can define:

$$D(\tau) = e^{\tau t^\dagger - \tau^* t} = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}} = D(\alpha) \tag{2.126}$$

and the squeezed state $|\tau\rangle$ is generated from the vacuum by:

$$|\tau\rangle = D(\alpha)S(z)|0\rangle \tag{2.127}$$

We have by definition of t:

$$\hat{t}S(z) = S(z)\hat{a} = 0 \tag{2.128}$$

thus:

$$\hat{t}S(z)|0\rangle = S(z)\hat{a}|0\rangle = 0 \tag{2.129}$$

and $\hat{t}\,|0_t\rangle = 0$ with the squeezed vacuum state defined as:

$$|0_t\rangle = S(z)\,|0\rangle \tag{2.130}$$

A squeezed state can be generated from a squeezed vacuum state by applying the displacement operator:

$$|\tau\rangle = D(\tau)\,|0_t\rangle \tag{2.131}$$

We can derive exactly the same relations as with coherent states and τ is an eigenstate of $\hat{t}$. Let us now compute the variances of the quadratures for a squeezed state (with $\phi = 0$):

$$\begin{aligned}
\langle\tau|\hat{t_1}|\tau\rangle &= \frac{1}{\sqrt{2}}\,\langle\tau|\hat{t}^\dagger + \hat{t}|\tau\rangle = \frac{1}{\sqrt{2}}(\tau^* + \tau) && (2.132)\\
\langle\tau|\hat{t_1}^2|\tau\rangle &= \frac{1}{2}\,\langle\tau|\hat{t}^{\dagger 2} + \hat{t}^\dagger\hat{t} + \hat{t}\hat{t}^\dagger + \hat{t}^2|\tau\rangle = \frac{1}{2}(\tau^{*2} + 2|\tau|^2 + 1) && (2.133)\\
\left(\Delta\hat{t_1}\right)^2 &= \langle\tau|\hat{t_1}^2|\tau\rangle - \langle\tau|\hat{t_1}|\tau\rangle^2 = \frac{1}{2} && (2.134)\\
\left(\Delta\hat{t_2}\right)^2 &= \frac{1}{2} && (2.135)
\end{aligned}$$

Furthermore we have:

$$\begin{aligned}
\langle\tau|\hat{t_1}|\tau\rangle &= \langle\tau|\hat{x}|\tau\rangle\, e^{r} && (2.136)\\
\langle\tau|\hat{t_2}|\tau\rangle &= \langle\tau|\hat{p}|\tau\rangle\, e^{-r} && (2.137)\\
\langle\tau|\hat{t_1}^2|\tau\rangle &= \langle\tau|\hat{x}|\tau\rangle\, e^{2r} && (2.138)\\
\langle\tau|\hat{t_2}^2|\tau\rangle &= \langle\tau|\hat{p}|\tau\rangle\, e^{-2r} && (2.139)\\
& && (2.140)
\end{aligned}$$

which gives the variance of the quadratures for a squeezed state:

$$\begin{aligned}
(\Delta\hat{x})^2 &= \frac{1}{2}e^{-2r} && (2.141)\\
(\Delta\hat{p})^2 &= \frac{1}{2}e^{2r} && (2.142)
\end{aligned}$$

In the Fock basis the squeezed vacuum state is (with $\phi = 0$):

$$S(r)\,|0\rangle = \frac{1}{\sqrt{\cosh r}} \sum_{n=0}^{\infty} \frac{\sqrt{(2n)!}}{2^n n!} \tanh r^n\,|2n\rangle \tag{2.143}$$

One can compute the photon statistics of a squeezed state:

$$\langle n\rangle = \sinh^2 r \tag{2.144}$$

and

$$\begin{aligned}
\langle n^2\rangle &= \sinh^2 r(3\sinh^2 r + 2) && (2.145)\\
&= 3\,\langle n\rangle^2 + 2\,\langle n\rangle && (2.146)
\end{aligned}$$

2.4 Two-mode Squeezed States

Several devices, like non-degenerate optical parametric amplifiers for example, produce light which is correlated at two frequencies ω^+ and ω^-. The squeezing exists not in the individual modes but in the correlated state formed by the two modes. A two-mode squeezed state can be defined by:

$$|\alpha_+, \alpha_-\rangle = D_+(\alpha_+) D_-(\alpha_-) S(G) |0\rangle \tag{2.147}$$

where the displacement operator is:

$$D_{+,-}(\alpha) = e^{\alpha \hat{a}^\dagger_{+,-} - \alpha^* \hat{a}_{+,-}} \tag{2.148}$$

and the unitary two-mode squeeze operator is ($G = re^{i\theta}$):

$$S(G) = e^{G^* \hat{a_+} \hat{a_-} - G \hat{a_+}^\dagger \hat{a_-}^\dagger} \tag{2.149}$$

The squeezing operator transforms the annihilation operators as:

$$S^\dagger(G) \hat{a}_{+,-} S(G) = \hat{a}_{+,-} \cosh r - \hat{a}^\dagger_{-,+} e^{i\theta} \sinh r \tag{2.150}$$

This can be proven using the previous technique with the additional properties:

$$[\hat{a}_+, \hat{a}_-] = 0 \tag{2.151}$$

$$[\hat{a}_+, \hat{a}^\dagger_-] = 0 \tag{2.152}$$

$$[\hat{a}^\dagger_-, \hat{a}^\dagger_+] = 0 \tag{2.153}$$

In the Fock basis one can prove that the two-mode squeezed vacuum state reads:

$$S(r) |0,0\rangle = \frac{1}{\sqrt{\cosh r}} \sum_{n=0}^{\infty} \tanh^n r \, |n,n\rangle \tag{2.154}$$

where $|n,n\rangle = |n\rangle_1 \otimes |n\rangle_2$. If we trace out one of the two input modes, we obtain the mixed state:

$$\begin{aligned} \rho_1 &= \mathrm{Tr}_2\{|\Psi\rangle \langle\Psi|\} && (2.155) \\ &= \frac{1}{\cosh r} \sum_{n=0}^{\infty} \tanh^{2n} r \, |n\rangle_1 \langle n|_1 \qquad = |T\rangle && (2.156) \end{aligned}$$

This is a thermal state. One can compute its mean photon number:

$$\langle T|\hat{n}|T\rangle = \sinh^2 r \tag{2.157}$$

Thus we have:

$$\tanh^2 r = \frac{\langle n\rangle}{(\langle n\rangle + 1)} \tag{2.158}$$

which gives the decomposition of the thermal state:

$$\rho_{TH} = \sum_{n=0}^{\infty} \frac{\langle n\rangle}{(\langle n\rangle + 1)^{n+1}} |n\rangle \langle n| \tag{2.159}$$

We can also compute $\langle \hat{n}^2 \rangle$:

$$\langle T|\hat{n}^2|T\rangle = \langle n\rangle + 2\langle n\rangle^2 \tag{2.160}$$

For a quadrature $\hat{x}$ we have:

$$\langle T|\hat{x}|T\rangle = 0 \tag{2.161}$$

and

$$\langle T|\hat{x}^2|T\rangle = \frac{2\langle n\rangle + 1}{2} \tag{2.162}$$

Consequently, we have in the covariance matrix of the thermal state: $V = 2\langle n\rangle + 1$.

2.5 Weyl Operator

The displacement operators can be generalized to the N-mode case. This is done by introducing the Weyl operator:

$$D_\xi = e^{ix\Omega\xi^T} \tag{2.163}$$

ξ being a vector in the 2N-dimensional phase space. For each mode one can use the quadratures representation ($\xi_x = \sqrt{2}\mathcal{R}(\alpha), \xi_p = \sqrt{2}\mathcal{I}(\alpha)$):

$$D_\alpha = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}} = e^{i(\xi_p\hat{x} - \xi_x\hat{p})} = D(\xi) \tag{2.164}$$

2.6 Phase-Space Representation

All the physical information about an N-mode state is contained in its quantum state represented by a density operator ρ, which is a trace-one positive operator acting on the corresponding Hilbert space. The space of density operators is called the state space. Instead of describing a quantum state ρ through its density matrix, one can refer to functions defined on the phase space. Let us introduce the Wigner characteristic function:

$$\chi_\rho(\xi) = \mathrm{Tr}[\rho D(\xi)] \tag{2.165}$$

Then an arbitrary ρ is equivalent to a Wigner characteristic function and by Fourier transform to a Wigner function:

$$\rho = \frac{1}{(2\pi)^{2N}} \int d^{2N}\xi \chi_\rho(-\xi) D_\xi \tag{2.166}$$

$$W(\xi) = \frac{1}{(2\pi)^{2N}} \int d^{2N}\zeta e^{i\xi^T\omega\zeta} \chi_\rho(\zeta) \tag{2.167}$$

In quantum physics, one cannot define the probability $f(x,p)$ to find the electric field in a small volume $\mathrm{d}x\,\mathrm{d}p$ close to the point (x,p) because of the uncertainty principle. However, it is possible to measure separately x, p or any combination $x_\theta = x\cos\theta + p\sin\theta$. These measures correspond to the projections of the probability distribution and one can build the object that produced these projections. The projections are the distributions of arbitrary projections $P_\theta(x_\theta)$ and the object that produced the projections is called Wigner function. The Wigner function is normalized to 1: $\int\int W(x,p)\,\mathrm{d}x\,\mathrm{d}p = 1$. The projections $P_\theta(x_\theta)$ give the optical density in x_θ when looking in the orthogonal direction p_θ.

Wigner functions are useful in practice for two reasons:

1. the Wigner function W is equivalent to the set of all the distributions $\{P_\theta\}$
2. the Wigner function contains all the information about the state, like the density matrix

2.7 Gaussian States

The most relevant quantities to define a quantum state are the statistical moments. A particular class of states can be entirely characterized with only two moments, hence we can write $\rho = \rho(mean, var)$. These states are the Gaussian states. By definition, Gaussian states are the states whose characteristic function, and equivalently Wigner function, is Gaussian. For an arbitrary quantum state ρ, we define the displacement vector d:

$$d = \langle \hat{r} \rangle = \text{Tr}[\rho \hat{r}] \tag{2.168}$$

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

$$\gamma_{i,j} = \text{Tr}[\rho\{(\hat{r_i} - d_i)(\hat{r_j} - d_j) + (\hat{r_j} - d_j)(\hat{r_i} - d_i)\}] \tag{2.169}$$

This definition comes from:

$$Cov(X_i, X_j) = \text{Tr}[\frac{1}{2}\{(X_i - m_i)(X_j - m_j) + (X_j - m_j)(X_i - m_i)\}\rho] \tag{2.170}$$

With these notations, the Gaussian states are the states whose characteristic function is:

$$\chi_\rho(\xi) = e^{-\frac{1}{4}\xi^T \Gamma \xi + iD^T \xi} \tag{2.171}$$

where $D = \Omega d$ and $\Gamma = \Omega \gamma \Omega$. The Wigner function of a Gaussian state is:

$$W(r) = \frac{1}{\pi^{2N}\sqrt{\det \gamma}} e^{-(r-d)^T \gamma^{-1}(r-d)} \tag{2.172}$$

Proof. One can use the identity: $e^{-\frac{y^2}{2} + iyx} = e^{-\frac{(y-ix)^2}{2} - \frac{x^2}{2}}$ and a change of variables. Since γ is symmetric it is diagonalizable. This allows to compute easily the determinant of the change of variables. □

The admissible covariance matrices for Gaussian states are the ones that satisfy the following condition:

$$\gamma + i\Omega \geq 0 \tag{2.173}$$

2.7.1 One mode Gaussian states

The general form of the covariance matrix is:

$$\gamma = \begin{bmatrix} a & c \\ c & b \end{bmatrix} \tag{2.174}$$

They are fully characterized by the displacement vector $d = (d_x, d_p)$ and the covariance matrix.

Vacuum and coherent states:

Their covariance matrix is the identity I. The vacuum state has null mean value $d = (0,0)$ whereas the coherent state has a non null displacement vector $d = (d_x, d_p)$.

Squeezed states:

Their covariance matrix is

$$\gamma = \begin{bmatrix} e^{-2r} & 0 \\ 0 & e^{2r} \end{bmatrix} \tag{2.175}$$

The squeezed vacuum state has null mean value whereas squeezed coherent states have a non null displacement vector.

Thermal states:

Their covariance matrix is

$$\gamma = \begin{bmatrix} V & 0 \\ 0 & V \end{bmatrix} \tag{2.176}$$

The thermal state has a null mean value. We have $V = 2\langle n \rangle + 1$ where $\langle n \rangle$ is the average number of photons contained in the thermal state. The vacuum state is a thermal state with $\langle n \rangle = 0$.

2.7.2 Two mode Gaussian states

They are fully characterized by a displacement vector $d = d_1 \otimes d_2$ and a covariance matrix:

$$\gamma = \begin{bmatrix} \gamma_1 & C \\ C & \gamma_2 \end{bmatrix} \tag{2.177}$$

where γ_1 and γ_2 are the covariance matrices of the first and second mode after tracing and C is the matrix giving the correlation between the two modes. Such a correlation can be either classical or quantum.

Tensor product state:

If $C = 0$ we have $\gamma_{12} = \gamma_1 \otimes \gamma_2$ and the state is a tensor product of one mode Gaussian states.

Two-mode squeezed state:

The mean is null and the covariance matrix is:

$$\gamma = \begin{bmatrix} \cosh 2rI & \sinh 2r\sigma_z \\ \sinh 2r\sigma_z & \cosh 2rI \end{bmatrix} \tag{2.178}$$

where

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{2.179}$$

and

$$\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{2.180}$$

2.8 Symplectic Analysis for Multimode Gaussian States

Williamson's theorem says that every positive-definite real matrix of even dimension can be put in diagonal form by a symplectic transformation. When applied to a N-mode covariance matrix it implies there exists a non-unique symplectic transformation S such that:

$$S^T \gamma S = \nu \tag{2.181}$$

where ν is a diagonal covariance matrix:

$$\nu = \bigotimes_{k=1}^{N} \nu_k I \tag{2.182}$$

ν is called the Williamson form of γ and the N positive quantities ν_k are called the symplectic eigenvalues of γ. The symplectic eigenvalues can be computed as the standard eigenvalues of the matrix $|i\Omega\gamma|$, where $|A|$ stands for $\sqrt{A^\dagger A}$. Since $|i\Omega\gamma|$ is hermitian, it is diagonalizable. Then one can take the modulus of its $2N$ real eigenvalues to get the N symplectic eigenvalues of γ. Eq. 2.173 is equivalent to:

$$\nu_k \geq 1, \forall k \in [1, N] \tag{2.183}$$

This bound is saturated only for pure Gaussian states where $\nu = I$.

2.8.1 One-mode normal decomposition

For a one-mode state of covariance matrix γ_1, one can compute the symplectic eigenvalues using the determinant. Indeed one has $\det \gamma_1 = \det(S\gamma_1 S^T)$ for any symplectic transformation S because $\det S = 1$. This gives for a one-mode system:

$$\nu_1 = \sqrt{\det \gamma_1} \tag{2.184}$$

2.8.2 Two-mode normal decomposition

Here we are concerned in finding the symplectic eigenvalues ν_1 and ν_2 of the two-mode covariance matrix

$$\gamma_{12} = \begin{bmatrix} \gamma_1 & C_{1-2} \\ C_{1-2}^T & \gamma_2 \end{bmatrix} \tag{2.185}$$

Another quantity Δ is left invariant under symplectic transformations:

$$\Delta = \det \gamma_1 + \det \gamma_2 + 2 \det C_{1-2} \tag{2.186}$$

Since we have $\det \gamma_{12} = \nu_1^2 \nu_2^2$ and $\delta = \nu_1^2 + \nu_2^2$ one only needs to compute the roots of the polynomial:

$$X^2 - \Delta X + \det \gamma_{12} \tag{2.187}$$

which gives:

$$\nu_{1,2}^2 = \frac{\Delta + - \sqrt{\Delta^2 - 4 \det \gamma_{12}}}{2} \tag{2.188}$$

2.8.3 Three-mode normal decomposition

Here we are concerned in finding the symplectic eigenvalues ν_1, ν_2 and ν_3 of the three-mode covariance matrix

$$\gamma_{123} = \begin{bmatrix} \gamma_1 & C_{1-2} & C_{1-3} \\ C_{1-2}^T & \gamma_2 & C_{2-3} \\ C_{1-3}^T & C_{2-3}^T & \gamma_3 \end{bmatrix} \tag{2.189}$$

The three symplectic invariants are:

$$\Delta_1^3 = \det \gamma_1 + \det \gamma_2 + \det \gamma_3 + 2 \det C_{1-2} + 2 \det C_{1-3} + 2 \det C_{2-3} \tag{2.190}$$

$$\Delta_2^3 = \det \gamma_{12} + \det \gamma_{23} + \det \gamma_{13} + 2 \det C_{12-23} + 2 \det C_{12-13} + 2 \det C_{23-13} \tag{2.191}$$

$$\Delta_3^3 = \det \gamma_{123} \tag{2.192}$$

where

$$C_{ij-kl} = \begin{bmatrix} C_{i-k} & C_{i-l} \\ C_{j-k} & C_{j-l} \end{bmatrix} \tag{2.193}$$

Since we have:

$$\Delta_1^3 \nu_1^2 + \nu_2^2 + \nu_3^2 \tag{2.194}$$

$$\Delta_2^3 = \nu_1^2 \nu_2^2 + \nu_2^2 \nu_3^2 + \nu_1^2 \nu_3^2 \tag{2.195}$$

$$\Delta_3^3 = \nu_1^2 \nu_2^2 \nu_3^2 \tag{2.196}$$

the symplectic eigenvalues are the roots of the polynomial:

$$x^3 - \Delta_1^3 x^2 + \Delta_2^3 z - \Delta_3^3 = 0 \tag{2.197}$$

2.9 Entropy of Gaussian States

2.9.1 Von Neumann entropy

The von Neumann entropy of a continuous-variable quantum system is:

$$S(\rho) = -\operatorname{Tr}[\rho \log \rho] \tag{2.198}$$

This quantity is finite on the compact set of states with bounded energy.

2.9.2 Entropy of Gaussian states

For every N-mode Gaussian state ρ_G, according to Williamson's theorem there exists a symplectic transformation S such that:

$$S \gamma S^T = \bigotimes_{k=1}^{N} \nu_k I \tag{2.199}$$

Then there exists a unitary transformation that maps the Gaussian state ρ_G to a product of N thermal states. Thus the entropy of ρ_G is equal to the sum of the entropy of the thermal states. Furthermore the variance ν_k of the thermal state k is linked to the number of photons in the mode k by:

$$\nu_k = 2 \langle n_k \rangle + 1 \tag{2.200}$$

Therefore we have:

$$S(\rho_G) = \sum_{i=1}^{N} S(\rho_{th}) \tag{2.201}$$

The Von Neumann entropy of a thermal state of density matrix:

$$\rho_{th} = \sum_{n=0}^{\infty} \frac{\langle n \rangle^n}{(\langle n \rangle + 1)^{n+1}} \left| n \right\rangle \left\langle n \right| \tag{2.202}$$

can be computed as:

$$S(\rho_{th}) = -\frac{1}{\langle n \rangle + 1} \sum_{k=0}^{\infty} \left(\frac{\langle n \rangle}{\langle n \rangle + 1} \right)^k \log_2 \left[\frac{1}{\langle n \rangle + 1} \left(\frac{\langle n \rangle}{\langle n \rangle + 1} \right)^k \right] \tag{2.203}$$

$$= \frac{\log_2 \langle n \rangle + 1}{\langle n \rangle + 1} \sum_{k=0}^{\infty} \left(\frac{\langle n \rangle}{\langle n \rangle + 1} \right)^k - \frac{\langle n \rangle}{(\langle n \rangle + 1)^2} \log_2 \frac{\langle n \rangle}{\langle n \rangle + 1} \sum_{k=1}^{\infty} k \left(\frac{\langle n \rangle}{\langle n \rangle + 1} \right)^k \tag{2.204}$$

$$= (\langle n \rangle + 1) \log_2 \langle n \rangle + 1 - \langle n \rangle \log_2 \langle n \rangle \tag{2.205}$$

2.9.3 Extremality of Gaussian states

Theorem 2.9.3.1 (Extremality of Gaussian states)**.** *Let $f : \mathcal{B}(H^{\otimes N}) \rightarrow R$ be a continuous functional, which is strongly sub-additive and invariant under local unitaries $f(U^{\otimes N} \rho U^{\dagger \otimes N}) = f(\rho)$. Then for every density operator ρ describing an N -partite system with finite first and second moments, we have that*

$$f(\rho) \geq f(\rho_G) \tag{2.206}$$

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

2.10 Gaussian Operations

Gaussian operations are the operations that map every Gaussian input state onto a Gaussian output state. What is very interesting about Gaussian operations is that they correspond to operations that can be performed easily with present technology.

Gaussian states being easy to characterize, there exists a large class of transformations acting on Gaussian states that are easy to characterize too: a Gaussian operation is entirely characterized by its action on the displacement vector d and the covariance matrix γ of a Gaussian state.

2.10.1 Gaussian unitary operations

They correspond to the set of operations generated by $U = e^{-i\hat{H}/2}$ from Hamiltonians $\hat{H}$ being second-order polynomials in the field operators:

$$\hat{H} = i(\hat{a}^\dagger \alpha + \hat{a}^\dagger F \hat{a} + \hat{a}^\dagger G \hat{a}^{\dagger T}) + h.c. \tag{2.207}$$

where $\alpha \in C^N$, F, G are $N \times N$ complex matrices and $h.c.$ stands for 'Hermitian conjugate'. A Gaussian unitary acts on the quadrature operator as an affine transformation:

$$\hat{x} - > S\hat{x} + d \tag{2.208}$$

where $d \in R^{2N}$ and S is a $2N \times 2N$ matrix.

Displacement operator:

The displacement D_ξ translates the mean of the Gaussian state $d_{out} = d_{in} + \xi$ and leaves invariant the covariance matrix. More generally, it does not modify the shape of the Wigner function of any quantum state of light.

A Gaussian state with mean $\langle x \rangle$ and covariance matrix γ is sent under the action of a Gaussian unitary characterized by a symplectic matrix S and a displacement vector d onto a Gaussian state with mean $\langle x^{'} \rangle$ and covariance matrix $\gamma^{'}$ given by:

$$\langle x^{'} \rangle = S \langle x \rangle + d \tag{2.209}$$

$$\gamma^{'} = S \gamma S^T \tag{2.210}$$

2.10.2 Passive transformations

These operations are the subset of symplectic transformation that are orthogonal. They are phase shifts and beamsplitters. They do not change the number of photons.

Phase shift:

A phase shift is a single mode operation corresponding to a rotation in the phase space. It is characterized by an angle θ and the corresponding rotation matrix $S_{PS}(\theta)$:

$$S_{PS}(\theta) = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \tag{2.211}$$

Beamsplitter:

The beamsplitter operation of transmittance T makes a coherent combination of two modes, characterized by the matrix S_{BS}:

$$S_{BS}(T) = \begin{bmatrix} \sqrt{T} I & \sqrt{1-T} I \\ -\sqrt{1-T} I & \sqrt{T} I \end{bmatrix} \tag{2.212}$$

Any passive transformation over N modes can be decomposed into a set of phase shifts and beamsplitters.

2.10.3 Active transformations

The complementary set of passive transformations inside symplectic transformations is called active transformations. These transformations are transformations that inject photons in the system.

Squeezing:

The squeezing operation with squeezing parameter s is characterized by a symplectic matrix S_{Sq}:

$$S_{Sq}(s) = \begin{bmatrix} e^{-s} & 0 \\ 0 & e^{s} \end{bmatrix} \tag{2.213}$$

Two-mode squeezing:

The two-mode squeezing operation with squeezing parameter s is characterized by a symplectic matrix S_{Sq2}:

$$S_{Sq2}(s) = \begin{bmatrix} \cosh sI & \sinh s\sigma_z \\ \sinh s\sigma_z & \cosh sI \end{bmatrix} \tag{2.214}$$

Partial measurements

Let us consider a general $(N_A + N_B)$-mode Gaussian state ρ_{AB} characterized by a displacement vector $d_{AB}^{in} = (d_A^{in}, d_B^{in})$ and a covariance matrix:

$$\gamma_{AB} = \begin{bmatrix} \gamma_A & C \\ C^T & \gamma_B \end{bmatrix} \tag{2.215}$$

The homodyne measurement on the B part of the state gives:

$$d_A^{out} = d_A^{in} + C(X\gamma_B X)^{MP}(m - d_B^{in}) \tag{2.216}$$

$$\gamma_A^{out} = \gamma_A - C(X\gamma_B X)^{MP}C^T \tag{2.217}$$

where $X = diag(1, 0, \dots, 1, 0)$ is the matrix of the measured quadratures and $m = (x_1, 0, x_2, 0, \dots, x_{N_B}, 0)$ is the result of the measurements x_i on the mode B_i. This result can be demonstrated by looking at the characteristic functions and applying a change of variables.

Chapter 3

Quantum Key Distribution with Continuous Variables

Contents

3.1 The Security of a QKD Protocol 42

3.1.1 Key Security Criterion 42

3.1.2 QKD Protocol Steps 43

3.2 A Brief History of QKD Protocols 43

3.3 Security Analysis of the Ideal GG02 Protocol . 44

3.3.1 Protocol Description 44

3.3.2 Some Potential Deviations to the Ideal GG02 Protocol 46

3.3.3 Security Proof against Collective Attacks 46

3.3.4 Security proof against General Attacks 49

3.4 Security Analysis of the Imperfect GG02 Protocol 49

3.4.1 Effect of an Imperfect Reconciliation Procedure . . 50

3.4.2 Effect of an Imperfect Homodyne Detection 51

3.4.3 Security of Gaussian Protocols with an Imperfect Modulation 53

3.4.4 Imperfect Calibration of the Detection Setup . . . 57

3.4.5 Improved Key Rate with Phase Noise Calibration . 61

3.5 Conclusion 66

In the previous chapter, we have introduced the mathematical tools that are useful to study the security of CVQKD. In this chapter, we start by explaining the criterion that characterizes the security of a QKD protocol and detail the different steps of a QKD protocol. Then, we briefly review the existing QKD protocols and focus on the GG02 [50] protocol that we implemented in chapter 4. As quantum key distribution becomes a mature technology, it appears clearly that some assumptions made in the security proofs cannot be justified in practical implementations. This might open the door to possible side-channel attacks. We examine several discrepancies between theoretical models and experimental setups in the case of continuous-variable quantum key distribution. We start with the most general security proof of GG02 protocol and study the impact of several imperfections on the secret key rate. We review how the finite efficiency of the error-correction procedure and an imperfect homodyne detection affect the secret key rate. Then, we study in particular the impact of an imperfect modulation on the security of Gaussian protocols and show that approximating the theoretical Gaussian modulation with a discrete one is sufficient in practice. We also address the issue of properly calibrating the detection setup, and in particular the value of the shot noise. Finally, we consider the influence of phase noise in the preparation stage of the protocol and argue that taking this noise into account can improve the secret key rate because this source of noise is not controlled by the eavesdropper.

3.1 The Security of a QKD Protocol

As we saw in chapter 1, the goal of QKD consists in establishing a secret key between two distant parties, i.e. a binary string that is unknown from any party except the two legitimate parties of the protocol, namely Alice and Bob. Once this key is obtained, it can be used to perform symmetric cryptography. A common scheme is the *One-Time Pad* (OTP) that consists in using one bit of secret key to encrypt and decrypt one bit of message using a *Exclusive Or* (XOR) operation. Such a scheme was proven to be *information-theoretically secure* by Shannon, which means that the encrypted message C provides no information about the plaintext M to any eavesdropper. Using the notations of chapter 2, this is expressed by $H(M) = H(M|C)$: conditioning on the knowledge of the ciphertext does not lower the uncertainty on the plaintext. However, OTP security has serious drawbacks:

- keys must be perfectly random
- keys must be as long as the message
- keys must never be reused

When either of these conditions is not satisfied, OTP security collapses very abruptly. Another possibility consists in using the keys produced by a QKD system to renew the keys of a non-information theoretically secure symmetric cipher, such as AES. Chapter 9 includes a demonstration of a cryptosystem combining a CVQKD system and an AES based encryptor. The notion of security of a key is of utmost importance. A particularity of a QKD protocol is that it is designed to abort if the key that it could produce is not secure with respect to a given security criterion.

3.1.1 Key Security Criterion

The universal definition of security used in modern QKD protocols was introduced by Renato Renner in [111]. It corresponds to the distance between the key S that is output by the QKD protocol and a perfectly randomly distributed secret key. The previous security definitions of QKD did not apply to joint attacks over QKD and the subsequent use of the key output by the protocol. Following [111], we can describe the joint state of the classical key S distributed according to a probability distribution $p(s)$ and the eavesdropper's quantum system, whose density matrix in the Hilbert space $\mathcal{H}_E$ is ρ_E^s given that S takes the value s for any element s of the key space $\mathcal{S}$, as:

$$\rho_{SE} = \sum_{s \in \mathcal{S}} p(s) \left| s \right\rangle \left\langle s \right| \otimes \rho_E^s \tag{3.1}$$

where $\{|s\rangle\}_{s\in\mathcal{S}}$ is an orthonormal basis of the Hilbert space $\mathcal{H}_S$ of the key. The key S is said to be ϵ-secure with respect to $\mathcal{H}_E$ if:

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

where $\rho_S = \sum_{s \in \mathcal{S}} \frac{1}{|\mathcal{S}|} |s\rangle \langle s|$ is the fully mixed state on $\mathcal{H}_S$ and ρ_E is any state of the eavesdropper. It means that an ϵ-secure key is uniformly distributed and independent from the eavesdropper's knowledge except with probability ϵ.

3.1.2 QKD Protocol Steps

A QKD protocol is divided into several successive steps:

– Quantum communication: Alice and Bob exchange quantum states through the quantum channel and perform some measurement on these states.

– Parameter estimation: Alice and Bob publicly announce at random a subset of the previously exchanged quantum signals. This step allows them to estimate the correlations between their quantum subsystems and therefore estimate the quantum information of the eavesdropper. They can abort the protocol at this stage if this amount of information is too large.

– Error-correction: the remaining quantum signals lead to partially identical bit strings on both Alice's and Bob's sides. Alice and Bob exchange public information on an authenticated classical channel and agree on a common bit string. This step increases the amount of information of the eavesdropper. Alice and Bob can abort the protocol at this stage if the total amount of information of the eavesdropper after all the previous steps is higher than the size of the common bit string.

– Privacy amplification: Alice and Bob extract from their common bit string a shorter bit string about which the eavesdropper knows a vanishing amount of information. This is done by applying a hashing function to their common bit string.

An incorrect implementation of any of these steps can threaten deeply the security of a QKD protocol. As we saw in chapter 1, the number of publications targeting incorrect implementations of QKD protocols and practical attacks on QKD systems has increased quickly over the past few years. In the rest of this chapter, we mainly consider CVQKD protocol imperfections related to the first two steps of this list.

3.2 A Brief History of QKD Protocols

Most implementations of QKD protocols and also the first commercial QKD systems [2, 3] correspond to DVQKD protocols and are based on photon counting techniques. While these systems feature rather long security distances (up to 40 dB losses [137] using superconducting single-photon detectors) and relatively high secret key rates (in the Mb/s range [30] at the time of writing), they suffer two major drawbacks that slow down their integration in network infrastructures: they require non-standard actively cooled components (the single-photon detectors) that might be hard to deploy in a server room environment and do not tolerate coexistence with other intense channels (with a power in the order of the mW) located at other wavelengths on the same optical fiber.

On the contrary, CVQKD uses only standard telecoms components (such as high efficiency PIN photodiodes optimized for the telecommunication industry) and feature an interesting intrinsic tolerance to the noise induced by wavelength multiplexed intense optical signals. This was firstly analyzed in [106] and we present further investigation in chapter 9.

Among CVQKD protocols, EPR-like entanglement protocols were first proposed [108, 109, 66, 18] but they were out of reach experimentally. Then, more practical versions of these protocols involved preparation and measurement of squeezed states, with either a discrete modulation [55, 27] or a Gaussian modulation [100]. This was a major improvement but the need for squeezed states still limited the practicality of these protocols. In 2002, Grosshans and Grangier [50] proposed the first CVQKD protocols using coherent states, which can easily be generated with a common laser source. This protocol consists in a Gaussian modulation of both quadratures of coherent states on Alice's side and applying a homodyne detection on Bob's side on one of the quadratures that is chosen at random. This protocol was limited to losses below 3 dB (that is a transmissivity of one half) because the mutual information between the eavesdropper and Alice's state was higher than the mutual information between Alice and Bob for higher losses. Several ideas were proposed to overcome this limitation: reverse reconciliation protocols [51, 49] that consist in establishing the secret key using Bob's measurements instead of Alice's prepared states, and post-selection protocols [130] which discard part of Alice's and Bob's data with a rule that leave them with data that are less noisy, i.e. less correlated to Eve. The security of this last category of protocols is far more difficult to establish due to the lack of a mathematical framework allowing us to analyze such a protocol which does not exhibit the same symmetries as protocols that do not use post-selection.

3.3 Security Analysis of the Ideal GG02 Protocol

Since we are mainly interested in improving the security and the performances of practical CVQKD protocols, we focus on the security proof of the GG02 protocol with reverse reconciliation in the rest of this chapter.

3.3.1 Protocol Description

We provide below a detailed description of the GG02 protocol with a reverse reconciliation:

1. Alice draws $2N$ random numbers $\{p_i\}_{1\leq i\leq N}$, $\{q_i\}_{1\leq i\leq N}$ according to a centered normal Gaussian distribution of variance V_A expressed in shot noise units.
2. Alice prepares and sends through the quantum channel N coherent states whose coordinates are $\{(p_i, q_i)\}_{1\leq i\leq N}$ in the phase space.
3. Bob draws N binary random numbers $\{b_i\}_{1\leq i\leq N}$.
4. Bob performs a homodyne measurement of either the Q or P quadrature depending on the value of $\{b_i\}_{1\leq i\leq N}$. He obtains N classical random variables $\{y_i\}_{1\leq i\leq N}$.
5. Bob sends to Alice on a public authenticated channel the values of the choice of quadratures $\{b_i\}_{1\leq i\leq N}$. Alice keeps the N values among its $2N$ values that correspond to Bob's choices of quadratures. These values are noted x_i. Alice and Bob now share a couple of N correlated classical variables $\{(x_i, y_i)\}_{1\leq i\leq N}$.

6. Alice (respectively Bob) draws $m = Nh(p)$ random bits for $0 \leq p \leq 1$ which allows them to select a subset of m values among their N couples of correlated random variables. The classical variables $\{(x_i, y_i)\}_{1 \leq i \leq m}$ from this subset are going to be revealed to estimate some parameters that characterize the quantum communication step. The value of p can be optimized depending on the number of values that are required to estimate the quantum transmission parameters with a good level of precision.
7. Alice (respectively Bob) sends on a public authenticated channel the m values selected at the previous step together with their position in their sequence of correlated data.
8. Bob (respectively Alice) computes an estimate of both the transmissivity $\hat{T}$ and the excess noise $\hat{\xi}$ of the quantum channel using $\{(x_i, y_i)\}_{1 \leq i \leq m}$ then uses these estimates to compute an estimate $\hat{\chi}(b : E)$ (the reconciliation being reverse here) of the upper bound on Eve's information and an estimate $\hat{I}(a : b)$ of the mutual information between Alice and Bob (a and b being Alice's and Bob's respective classical bits strings and E being Eve's quantum state). If $\hat{\chi}(b : E) > \beta\hat{I}(a : b)$ (where β corresponds to the effiency of the theoretical error correction procedure at this signal-to-noise ratio), Bob (respectively Alice) tells the other part to discard the $N - m$ remaining values.
9. Bob sends to Alice a bit string depending on his measurements on a public authenticated channel. According to Shannon's theory, the length of this bits string cannot be arbitrarily small and depends on the level of noise on the quantum channel.
10. Alice uses the received bits string to compute an estimate of Bob's measurements. If this error-correction procedure is correctly designed, the probability of Alice computing a correct value for the estimate of Bob's measurements is close to one. An optional step here consists in sending a short bit string that is a hash function of Alice's estimate from Alice to Bob on a public authenticated channel. Bob can compute the same hash function on its bit string and then compare the results. If they differ, he informs Alice so they can discard their respective classical bits strings.
11. Given $\hat{\chi}(b : E)$ and the length of the bits string disclosed at the previous step Alice (respectively Bob) computes an estimate of the number l of secret bits they can extract from their common partially secret bit string.
12. Alice (respectively Bob) draws a random hashing function that compresses a $N - m$ bit string into a l bit string. If they are using the two-universal hashing family *multiplication by a binary Toeplitz matrix*, the number of required random bits is $N - m + l - 1$.
13. Alice (respectively Bob) sends on a public authenticated channel the description of the drawn hashing function.
14. Alice and Bob apply this function to their respective bit strings. They obtain a secret bit string of size l.

We can see that such a description does not give a practical implementation of the protocol and makes use of rather theoretical objects such as the shot noise or the homodyne measurement.

3.3.2 Some Potential Deviations to the Ideal GG02 Protocol

Although this list does not intend to be exhaustive, it enumerates most of the practical imperfections that arise when trying to implement the GG02 protocol and therefore threaten its security:

– The practical discretized Gaussian modulation one can generate in an experiment might not be equivalent to the theoretical continuous Gaussian modulation. We study this imperfection in section 3.4.3 and in [63].
– The random numbers source that is required at different steps of the protocol might be predictable by an attacker.
– The states prepared by Alice might not be coherent states. The effect of preparing thermal states instead of coherent states was studied in [141].
– The detection apparatus might not measure perfectly a quadrature of the field.
– The Q and P quadratures that are supposed to be measured on Bob's side might not be orthogonal.
– The public channel might not be authentic.
– All the quantities used to estimate Eve's information might not be expressed correctly in shot noise units. As studied in chapter 5 and in [62], a fake shot noise estimation can be used to hide a full intercept and resend attack.

3.3.3 Security Proof against Collective Attacks

The security proof of the ideal GG02 protocol was established against collective attacks in [46, 99]. We review the sketch of this proof in this section.

The secret key rate against collective attacks in the asymptotic limit is given by:

$$K_{coll}^{asympt} = I(a:b) - S(b:E) \tag{3.3}$$

where $I(a;b)$ is the mutual information between Alice and Bob's classical bit strings after the quantum exchange and $S(b:E)$ if the Holevo quantity between Bob's classical bit string and Eve's quantum state. The proof proceeds by bounding the Holevo quantity between Eve and Bob using the optimality property of Gaussian states [153]:

Theorem 3.3.3.1 (Extremality of Gaussian states, Lemma 1 of [153])**.** *Let $f : \mathcal{B}(H^{\otimes N}) \to R$ be a continuous functional, which is strongly sub-additive and invariant under local unitaries $f(U^{\otimes N}\rho U^{\dagger\otimes N}) = f(\rho)$. Then for every density operator ρ describing an N-partite system with finite first and second moments, we have that*

$$f(\rho) \geq f(\rho_G) \tag{3.4}$$

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

In order to apply this theorem, let us show that $S(b:E) = f(\rho_{AB})$ where ρ_{AB} is the state shared by Alice and Bob. Since one can always write $\rho_E = \mathrm{tr}_{AB}(\rho_{ABE})$, it is possible to assume that ρ_{ABE} is pure. The property of the von Neumann entropy of a pure system gives $S(AB) = S(E)$.

Furthermore, after the projective homodyne measurement from B to b, the quantum system ρ_{AE} is still pure. Then $S(A|b) = S(E|b)$. By linearity $S(b : E) = S(E) - S(E|b)$ can be written as $f(\rho_{AB})$.

One can show that $f : \rho_{AB} \to f(\rho_{AB}) = S(b : E)$ satisfies the hypotheses of Theorem 3.3.3.1. Thus we have:

$$f(\rho_{AB}) \leq f(\rho_{AB}^{G}) \tag{3.5}$$

and we can compute the quantity $S(b : E)$ assuming that the state ρ_{AB} is Gaussian and this gives a general bound on $S(b : E)$. Then the secret key rate satisfies:

$$K_{coll}^{asympt} \geq I(a : b) - f(\rho_{AB}^{G}) \tag{3.6}$$

Once we have this result, let us see how to compute $S(b : E)$ for a two-mode Gaussian state. Since a Gaussian bivariate mixture of coherent states is a thermal state, in GG02 Alice prepares a thermal state of covariance matrix:

$$\gamma_A = \begin{bmatrix} V_A + 1 & 0 \\ 0 & V_A + 1 \end{bmatrix} \tag{3.7}$$

Furthermore, this thermal state can be obtained as a purification of a two-mode squeezed state (or EPR state) of covariance matrix:

$$\gamma_{EPR} = \begin{bmatrix} VI & \sqrt{V^2 - 1}\sigma_z \\ \sqrt{V^2 - 1}\sigma_z & VI \end{bmatrix} \tag{3.8}$$

where $V = V_A + 1$. The anti-diagonal sub-matrices exhibit the quantum correlations that characterize an EPR state. We still need to connect such a general covariance matrix to the real statistics of a practical CVQKD experiment which exhibit classical correlations.

In the general case, in the Prepare& Measure version of a CVQKD protocol, the covariance matrix related to Alice and Bob's measurements has the following form:

$$\gamma_{P\&M} = \begin{bmatrix} X_{11} & X_{12} & Z_{11} & Z_{12} \\ X_{21} & X_{22} & Z_{21} & Z_{22} \\ Z_{11} & Z_{12} & Y_{11} & Z_{12} \\ Z_{21} & Z_{22} & Z_{11} & Z_{12} \end{bmatrix} \tag{3.9}$$

which is the general form of a two-mode state covariance matrix. Intuitively, in an ideal version of the protocol, the quantum channel is supposed not to introduce any correlation between the Q and P quadratures. This justifies why all the non diagonal terms of the 2×2 sub-matrices should be equal to zero. Another theoretical justification is given in [73]: Alice and Bob could apply the same random orthogonal transformation to their respective data in order to symmetrize them. On the one hand, the Gaussian noise added by the channel is symmetric and therefore its law is not changed by such transformations, which implies that the same error-correction procedure can be applied whether we apply the symmetrization procedure or not. On the other hand, the symmetrization gives $X = \frac{X_{11}+X_{22}}{2}$, $Y = \frac{Y_{11}+Y_{22}}{2}$ and $Z = \frac{Z_{11}-Z_{22}}{2}$ and one can safely use the following symmetric covariance matrix in the equivalent entanglement-based version of the protocol:

$$\gamma_{sym} = \begin{bmatrix} XI & Z\sigma_z \\ Z\sigma_z & YI \end{bmatrix} \tag{3.10}$$

This form shows that Q and P play the same role and that Alice and Bob are simply left with estimating three parameters instead of ten. Furthermore, for a quantum channel of transmission T and excess noise ξ, Alice's modulated data $\{x_i\}_{1\leq i\leq N}$ and Bob's measurements $\{y_i\}_{1\leq i\leq N}$ are related by $y_i = tx_i + z_i$ where $z_i \sim \mathcal{N}(0,\sigma^2)$. This allows us to estimate these parameters:

$$\begin{cases} \langle x^2\rangle &= V-1 \\ \frac{\langle xy\rangle}{\langle x^2\rangle} &= \sqrt{T} \\ \langle y^2\rangle &= 1+T(V-1)+T\xi \end{cases} \tag{3.11}$$

Thus the covariance matrix of Alice and Bob's two-mode state can be written:

$$\gamma_{AB} = \begin{bmatrix} VI & \sqrt{T(V^2-1)}\sigma_z \\ \sqrt{T(V^2-1)}\sigma_z & (1+T(V-1)+T\xi)I \end{bmatrix} \tag{3.12}$$

One can note $\chi = (1-T)/T+\xi$ then we have:

$$\gamma_{AB} = \begin{bmatrix} VI & \sqrt{T(V^2-1)}\sigma_z \\ \sqrt{T(V^2-1)}\sigma_z & T(V+\chi)I \end{bmatrix} \tag{3.13}$$

Now one can compute $S^G(b:E)$ for the Gaussian state with covariance matrix γ_{AB}. The obtained value is a bound for $S(b:E)$. Since the system E can be written as a purifying system of ABE, the property of the von Neumann entropy of a pure composite system gives:

$$S(b:E) = S(E) - S(E|b) \tag{3.14}$$

$$= S(AB) - S(AB|b) \tag{3.15}$$

Then one just needs to compute the symplectic values of the matrices γ_{AB} and $\gamma_{AB|b}$. For a 4×4 matrix of the form:

$$\gamma_{AB} = \begin{bmatrix} aI & c\sigma_z \\ c\sigma_z & bI \end{bmatrix} \tag{3.16}$$

if we perform a measurement on the quadrature $\hat{x}$ of respective modes A and B we can apply the formula of the homodyne measurement respectively with $X_A = diag(1,0,0,0)$ and $X_B = diag(0,0,1,0)$ to get:

$$\gamma_{AB}^B = \begin{bmatrix} a-c^2/b & 0 \\ 0 & a \end{bmatrix} \tag{3.17}$$

and

$$\gamma_{AB}^A = \begin{bmatrix} b-c^2/a & 0 \\ 0 & b \end{bmatrix} \tag{3.18}$$

Then we have:

$$\gamma_{AB|b} = \begin{bmatrix} V-\frac{V^2-1}{V+\chi} & 0 \\ 0 & V \end{bmatrix} \tag{3.19}$$

The symplectic eigenvalue of $\gamma_{AB|b}$ is given by the product of the diagonal elements:

$$\nu_3^2 = V(V-\frac{V^2-1}{V+\chi}) \tag{3.20}$$

For γ_{AB} we have:

$$\Delta = a^2 + b^2 - 2c^2 = V^2(1-2T) + 2T + T^2(V+\chi)^2 \tag{3.21}$$

$$D = ab - c^2 = T(V\chi + 1) \tag{3.22}$$

and:

$$\nu_1^2 = \frac{1}{2}(\Delta + \sqrt{\Delta^2 - 4D^2}) \tag{3.23}$$

$$\nu_2^2 = \frac{1}{2}(\Delta - \sqrt{\Delta^2 - 4D^2}) \tag{3.24}$$

Finally, using the formula giving the entropy of a decomposition in thermal states we get:

$$S(b:E) = S(AB) - S(E|b) \tag{3.25}$$

$$= g\left(\frac{\nu_1 - 1}{2}\right) + g\left(\frac{\nu_2 - 1}{2}\right) - g\left(\frac{\nu_3 - 1}{2}\right) \tag{3.26}$$

Note that this quantity is exactly the same as in the protocol with squeezed states and homodyne measurement. However the key rate differs because of $S(A:B)$ which is different between the two protocols.

3.3.4 Security proof against General Attacks

The secret key rate against collective attacks converges to the secret key rate against coherent attacks in the asymptotic limit of infinite block lengths [112]. This is because a de Finetti's theorem [112] implies the optimality of collective attacks in the asymptotic limit. The optimality of Gaussian attacks [46, 99] among collective attacks allows us to conclude in this regime. However, because of the slow convergence, the analysis done in [112] does not allow us to compute useful bounds on the secret key rate in the finite-size regime, which is the scenario of interest for a practical implementation of a CVQKD protocol. A totally different security analysis makes use of an entropic uncertainty inequality [45] and allows us to compute bounds for practical values of exchanged signals. Unfortunately, the secret key rate obtained with this technique does not converge to the asymptotic secret key rate secure against collective attacks when considering an infinite number of signals. This results in a vanishing secret key rate after a few hundred meters. Another proof technique was introduced in [74] and improves the convergence speed of [112]. It consists in exploiting the symmetries of the protocol in phase space in order to obtain a tight bound on the effective dimension of the quantum state. Then, the so-called post-selection technique introduced in [23] for discrete-variables protocols can be applied [74] and gives better convergence results than the de Finetti's theorem used in [112]. The drawback of this last method is that it still lacks an analytical formula to compute an estimate of the secret key rate for a finite set of exchanged quantum signals [74].

3.4 Security Analysis of the Imperfect GG02 Protocol

The main argument in favor of QKD is its provable security based on the laws of quantum mechanics; it is therefore particularly important to make sure that the security proofs derived for theoretical protocols can be applied to real-world implementations. This is unfortunately never really the case because the security proofs usually assume idealized implementations, which do not take into account all possible experimental imperfections. This opens the door to potential security loopholes [121] that might be successfully exploited by an attacker. Such side-channel attacks have already been demonstrated against commercial QKD systems [155, 86].

There are basically two ways around side-channel attacks. A drastic solution consists in deciding that the systems held by Alice and Bob should not be trusted: this is the device-independent paradigm, based on the violation of a Bell inequality [31]. While being appealing in theory, this paradigm does not offer a practical solution since violating a Bell inequality in a loophole-free fashion has not been achieved until now. A more practical way to address side-channel attacks aims at refining the theoretical models used for security proofs in order to include various sources of experimental imperfections. This involves, for instance, developing better models for the state preparation, including the light source, the modulation, and the noise, and for the detection, including the quantum efficiency and the calibration of the noise.

In this section, we follow the second approach. We start by presenting two well-studied imperfections: the effect of the finite efficiency of the error-correction procedure on the secret key rate and how the finite efficiency and the electronic noise of an imperfect homodyne detection can be taken into account into the security proof. Then, we study three kinds of imperfections that occur in all implementations of this protocol and see how they affect its security and the secret key rate. The first imperfection concerns the modulation, which, in practice, can only approach the theoretical Gaussian modulation. Indeed, a Gaussian distribution is not only continuous but unbounded, and therefore cannot be exactly achieved since for instance, an infinite amount of randomness would be required. We show that the impact on security is not significant when the Gaussian distribution is replaced by a bounded, discrete approximation. However, deviations from a perfect discretized distribution degrade the security. The second source of imperfection comes from finite-size effects, and in particular from the calibration of the detection setup. While a first study in this direction has already considered statistical estimation of the transmittance and excess noise of the channel [77], it assumed that the quantum efficiency and the electronic noise of the detection, and more importantly, the shot noise level, were all perfectly calibrated. Here, we consider these effects in detail and examine their impact on the secret key rate and distance. Finally, we study the effect of phase noise in the preparation process of the protocol. This noise is unavoidable but one can safely assume that it is not controlled by the eavesdropper. We therefore show that by calibrating it properly, one can increase the secret key rate of the protocol.

3.4.1 Effect of an Imperfect Reconciliation Procedure

In this section we show that the effect of the imperfect reconciliation procedure is well understood and does not threaten the security of a CVQKD protocol if correctly performed. However, this step limited the range of CVQKD protocols with a Gaussian modulation for a long time. Chapter 6 shows how to overcome this limitation.

The theoretical secret key rate of Equation 3.3 can never be achieved in a practical implementation because only a fraction β of the mutual information between Alice and Bob can be recovered. In theory, according to Shannon's theorem, one can achieve the Shannon capacity of a channel which corresponds to the supremum of the mutual information between the input and the output over all the input distributions, with an error-correcting code of rate R equal to the capacity. In our Gaussian CVQKD protocol we are using a Gaussian modulation which is the probability distribution that maximizes the mutual information over the AWGNC. We require an error-correcting code of rate equal to the capacity of the AWGNC to extract all the mutual information between Alice and Bob. Unfortunately, such finite-length codes do not exist. The ratio between the rate of the code and the capacity of the channel gives the efficiency of the code with respect to the Shannon limit. The expression of the secret key rate taking into account an imperfect reconciliation efficiency reads:

$$K_{ECC}^{asympt} = \beta I(a:b) - S(b:E) \tag{3.27}$$

$$= \frac{R}{C_{AWGNC}} I(a:b) - S(b:E) \tag{3.28}$$

where $0 \leq \beta \leq 1$. In the limit of very large blocks, there exist codes that achieve the capacity and K_{ECC}^{asympt} converges towards K_{coll}^{asympt}.

Furthermore, when codes close to the channel capacity are available, usually the known iterative decoding algorithms are suboptimal and do not allow to correct errors at high repetition rates. In chapter 6, we give examples of LDPC codes that can perform close to the BIAWGNC capacity and in chapter 8 we study the use of polar codes for both DVQKD and CVQKD and give experimental speeds for both LDPC codes and polar codes.

3.4.2 Effect of an Imperfect Homodyne Detection

The efficiency of the homodyne detection is modeled by a beamsplitter of transmittance η and the electronic noise of the detection is modeled by a thermal noise of variance N added at the second input of the beamsplitter. Before Bob's homodyne measurement, the state received by Bob is mixed with a thermal state. The other output is called mode F and the other part of the thermal EPR pair is called mode G. We assume that FG is a pure state, i.e. Eve cannot interact with this state totally controlled by Bob. This seems justified because this state is produced in Bob's lab.

The system $ABFG$ where AB comes from the channel is a product state $\rho_{ABFG} = \rho_{AB} \otimes \sigma_{FG}$. Since we are computing a bound we can safely assume that ρ_{AB} is Gaussian. We also assume that the electronic noise is Gaussian thus the state ρ_{FG} is Gaussian. Therefore the system $ABFG$ is Gaussian and can be described by its covariance matrix γ_{ABFG} such that $\gamma_{ABFG} = \gamma_{AB} \otimes \gamma_{FG}$. The beamsplitter on Bob's side acts as a passive symplectic transformation described by the matrix $S = 1_A \otimes S_{BF} \otimes 1_G$ with:

$$S_{BF} = \begin{bmatrix} \sqrt{\eta} & \sqrt{1-\eta} \\ -\sqrt{1-\eta} & \sqrt{\eta} \end{bmatrix} \tag{3.29}$$

where B becomes B_1 and F becomes F_1 after coupling on the beamsplitter. Thus we have:

$$\gamma_{AB_1F_1G} = S\gamma_{AB} \otimes \gamma_{FG} S^T \tag{3.30}$$

We can rearrange the rows and the columns to get the matrix γ_{AFGB} and after measurement of the x quadrature of mode B we get:

$$\gamma_{AFG}^{x_b} = \begin{bmatrix} \gamma_A & \sigma_{AF} & \sigma_{AG} \\ \sigma_{AF}^T & \gamma_F & \sigma_{FG} \\ \sigma_{AG}^T & \sigma_{FG}^T & \gamma_G \end{bmatrix} \tag{3.31}$$

where

$$\gamma_A = \begin{bmatrix} a - \frac{c^2\eta}{b\eta+(1-\eta)N} & 0 \\ 0 & a \end{bmatrix} \tag{3.32}$$

$$\gamma_F = \begin{bmatrix} \frac{bN}{b\eta+(1-\eta)N} & 0 \\ 0 & b\eta + (1-\eta)N \end{bmatrix} \tag{3.33}$$

$$\gamma_G = \begin{bmatrix} N - \frac{(1-\eta)(N^2-1)}{b\eta+(1-\eta)N} & 0 \\ 0 & N \end{bmatrix} \tag{3.34}$$

$$\sigma_{AF} = \begin{bmatrix} \frac{-\sqrt{1-\eta}Nc}{b\eta+(1-\eta)N} & 0 \\ 0 & \sqrt{1-\eta}c \end{bmatrix} \tag{3.35}$$

$$\sigma_{AG} = \begin{bmatrix} \frac{-c\sqrt{(1-\eta)\eta(N^2-1)}}{b\eta+(1-\eta)N} & 0 \\ 0 & 0 \end{bmatrix} \tag{3.36}$$

$$\sigma_{FG} = \begin{bmatrix} \frac{\eta(N^2-1)}{b\eta+(1-\eta)N} & 0 \\ 0 & -\sqrt{\eta(N^2-1)} \end{bmatrix} \tag{3.37}$$

We note $\chi_D = \frac{1-\eta}{\eta}N$ which gives a reduced form for the symplectic invariants:

$$\Delta_1^3 = \frac{1}{b+\chi_D}(2b + aD + \chi_D(\Delta+1)) \tag{3.38}$$

$$\Delta_2^3 = \frac{1}{b+\chi_D}(b + 2aD + \chi_D(D^2+\Delta)) \tag{3.39}$$

$$\Delta_3^3 = \frac{D}{b+\chi_D}(a + \chi_D D) \tag{3.40}$$

that satisfy $P(x) = x^3 - \Delta_1^3 x^2 + \Delta_2^3 x - \Delta_3^3 = 0$. Since $P(1) = 0$ then one has to compute the roots of the polynomial $Q(x) = x^2 - (\Delta_1^3 - 1)x + \Delta_3^3$. Let us define $\chi_{tot} = \chi + \frac{\chi_D}{T}$, we can rewrite:

$$\Delta_1^3 = \frac{2T(V+\chi) + VD + \chi_D\Delta + \chi_D}{T(V+\chi_{tot})} \tag{3.41}$$

$$= \frac{VD + T(V+\chi) + \Delta\chi_D}{T(V+\chi_{tot})} + 1 = \alpha + 1 \tag{3.42}$$

$$\Delta_3^3 = \frac{VD + \chi_D D^2}{T(V+\chi_{tot})} = \beta \tag{3.43}$$

with:

$$\alpha = \frac{VD + T(V+\chi) + \Delta\chi_D}{T(V+\chi_{tot})} \tag{3.44}$$

$$\beta = \frac{VD + \chi_D D^2}{T(V+\chi_{tot})} \tag{3.45}$$

Finally the symplectic eigenvalues are:

$$\nu_3^2 = \frac{1}{2}(\alpha + \sqrt{\alpha^2 - 4\beta}) \tag{3.46}$$

$$\nu_4^2 = \frac{1}{2}(\alpha - \sqrt{\alpha^2 - 4\beta}) \tag{3.47}$$

$$\nu_5^2 = 1 \tag{3.48}$$

Then in the case of a noisy homodyne detection the Holevo quantity reads:

$$S(b:E) = g\left(\frac{\nu_1 - 1}{2}\right) + g\left(\frac{\nu_2 - 1}{2}\right) - g\left(\frac{\nu_3 - 1}{2}\right) - g\left(\frac{\nu_4 - 1}{2}\right) \tag{3.49}$$

3.4.3 Security of Gaussian Protocols with an Imperfect Modulation

We first consider an issue present in all implementations of CVQKD with a Gaussian modulation, namely that it is impossible to use an exact Gaussian modulation in practice. In the ideal scenario for the prepare-and-measure protocol, for each signal to be sent, Alice is supposed to draw two random normal variables $q, p \sim \mathcal{N}(0, V_A)$ and to prepare the coherent state $|q+ip\rangle$ centered on the point (q, p) in phase space. Unfortunately, in practice, ignoring phase noise, the coherent state really prepared by Alice is centered on (q', p') instead, where (q', p') is a point on a finite grid, approximating the ideal value of (q, p). This is unavoidable for several reasons. First, the analog-to-digital converters that drive the physical modulators used in practice produce discrete voltages; they typically have a bit depth of 10 like in [44]. Second, intensity modulators only work in some finite range of values, whereas the Gaussian distribution is unbounded. Another hardware constraint is the throughput of the physical Random Number Generators (for example Quantis, from ID Quantique, is limited to 16 Mbit/s). But there are also software limitations: one does not want to use too much randomness in order to draw the Gaussian variables q and p out of the uniform variables provided by the physical Random Number Generator because this requires computational power. For these reasons, it is useful to know how well the Gaussian modulation needs to be approximated in order to get a reasonably good level of security.

Intuitively, the presence of shot noise hides the small imperfections of the modulation and the security should not be compromised provided that the grid of (q', p') is sufficiently fine-grained compared to the value of the shot noise. Figure 3.1 illustrates how fine the grid needs to be compared to the shot noise.

In order to analyze the security of the practical protocol, it is convenient to look at the situation from Bob and Eve's points of view. In the theoretical protocol, the state sent by Alice to Bob should be a thermal state from Eve's perspective, that is a Gaussian mixture of coherent states. If Eve cannot distinguish the state sent in practice from a thermal state, then clearly the security of the protocol is not compromised by the approximated

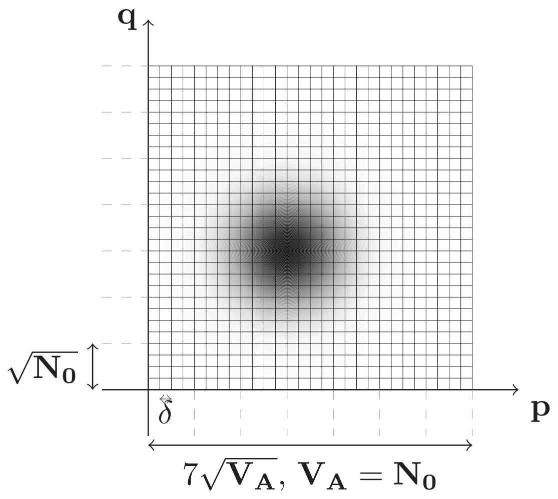


Figure 3.1: Discretization grid used to approximate a Gaussian modulation in phase space. The modulation variance V_A is chosen to be equal to the shot noise N_0. The distribution is truncated to 7 standard deviations and discretized in steps of $1/4^{\text{th}}$ of shot noise units. A coherent state of variance N_0 covers a large part of the grid, which results in hiding the small imperfections of the discretized modulation.

modulation. More precisely, if the trace distance between the ideal state and the actual state is bounded by ϵ_{prep}, and if the usual protocol (with perfect state preparation) is ϵ-secure, then the true protocol is $(\epsilon + \epsilon_{\text{prep}})$-secure. Therefore, one simply needs to ensure that ϵ_{prep} can be made quite small, that is on the order of 10^{-10} in a realistic implementation.

The quality of a Gaussian modulation

Let us write $\rho = \rho_{\text{th}} = \sum_{n=0}^{\infty} \frac{\overline{x}^n}{(\overline{x}+1)^{n+1}} |n\rangle\langle n|$ the ideal thermal state and $\sigma = \sum_k \omega_k |\alpha_k\rangle\langle\alpha_k|$ the state used in practice. Here ω_k corresponds to the probability of preparing the coherent state $|\alpha_k\rangle$.

We will compute the trace distance $||\rho - \sigma||_1$ between the two states, for two discretizations σ, either with a Cartesian or a polar grid. For both discretizations, we will use the gentle measurement lemma [152, 101]:

Lemma 3.4.3.1 (Gentle measurement)**.** *Let ρ be a state and Π be a projector. Then*

$$||\rho - \Pi\rho\Pi|| \leq 2\sqrt{1 - \operatorname{tr}(\Pi\rho\Pi)}. \tag{3.50}$$

Let us take $\Pi = |0\rangle\langle 0| + |1\rangle\langle 1| + \cdots + |Q-1\rangle\langle Q-1|$. The triangle inequality gives:

$$\begin{aligned}
||\rho - \sigma|| &\leq ||\rho - \Pi\rho\Pi|| + ||\Pi\rho\Pi - \Pi\sigma\Pi|| + ||\Pi\sigma\Pi - \sigma|| \\
&\leq \sum_{n=Q}^{\infty} \langle n|\rho|n\rangle + \left|\sum_{n,m=0}^{Q-1} \langle n|\rho|m\rangle - \langle n|\sigma|m\rangle\right| \\
&\quad +2\sqrt{1 - \mathrm{tr}\,(\Pi\sigma\Pi)} \\
&\leq \sum_{n=Q}^{\infty} \frac{\overline{x}^n}{(\overline{x}+1)^{n+1}} + \sum_{n=0}^{Q-1} \left|\frac{\overline{x}^n}{(\overline{x}+1)^{n+1}} - \langle n|\sigma|n\rangle\right| \\
&\quad +2 \sum_{0\leq n<m<Q} |\langle n|\sigma|m\rangle| + 2\sqrt{1 - \sum_{n=0}^{Q-1} \langle n|\sigma|n\rangle} \\
&\leq \left(\frac{\overline{x}}{\overline{x}+1}\right)^Q + \Delta_{\mathrm{diag}} + 2\Delta_{\mathrm{nondiag}} + 2\sqrt{R_\sigma} \qquad (3.51)
\end{aligned}$$

with $\Delta_{\mathrm{diag}} := \sum_{0\leq n<Q} \left|\frac{\overline{x}^n}{(\overline{x}+1)^{n+1}} - \langle n|\sigma|n\rangle\right|$, $\Delta_{\mathrm{nondiag}} := \sum_{0\leq n<m<Q} |\langle n|\sigma|m\rangle|$ and $R_\sigma := 1 - \sum_{0\leq n<Q} \langle n|\sigma|n\rangle$. These three quantities can be estimated from the terms $\langle n|\sigma|m\rangle, 0 \leq n, m < Q$.

Notice that $R_\rho := \left(\frac{\overline{x}}{\overline{x}+1}\right)^Q$ does not depend on the actual approximation used, but only on the mean photon number $\overline{x}$ of the ideal thermal state. When using a Gaussian modulation of variance V_A (in shot noise units), one has $\overline{x} = 2V_A$. This means that larger values of V_A require larger values of Q in order to obtain a good bound in Eq. (3.51). A typical range for V_A is $[1, 20]$. For $V_A = 20$, and $\epsilon_{\mathrm{prep}} = 10^{-10}$, one needs to have $Q \approx 1000$ to ensure that $R_\rho \leq \epsilon_{\mathrm{prep}}$. Furthermore one also needs $R_\sigma \leq \epsilon_{\mathrm{prep}}^2$, which puts additional constraints on Q.

Cartesian approximation

Here, we consider an approximation of the form

$$\sigma = \sum_{k=-N}^{N} \sum_{l=-N}^{N} \omega_k\, \omega_l\, |\alpha_{kl}\rangle\, \langle\alpha_{kl}| \qquad (3.52)$$

where $\omega_k = \frac{\gamma_k}{\sum_k \gamma_k}$, $\gamma_k = e^{-q_k^2/(2V)}$, $q_k = p_k = \frac{A}{N}k$, $\alpha_{kl} = q_k + ip_k$, and A, N are two parameters to be optimized. The $|\alpha_{kl}\rangle$ are coherent states: $|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$.

Therefore,

$$\begin{aligned}
\langle n|\sigma|m\rangle &= \sum_{k,l=-N}^{N} \omega_k\omega_l\, \langle n|\alpha_{kl}\rangle\, \langle\alpha_{kl}|m\rangle \\
&= \sum_{k,l=-N}^{N} \omega_k\omega_l\, e^{-|\alpha_{kl}|^2} \frac{\alpha_{kl}^n\, \alpha_{kl}^{*\,m}}{\sqrt{n!m!}}.
\end{aligned}$$

From this expression, Δ_{diag}, $\Delta_{\mathrm{nondiag}}$ and R_σ can be evaluated numerically for any choice of $\overline{x} = 2V_A, Q, A$ and N. Once A is chosen, N is typically set so that $\delta = A/N$, the discretization step, has some predetermined value. Given V_A, let us show that a low $\epsilon_{\mathrm{prep}} = ||\rho - \sigma||$ can be obtained with reasonable values of A and N. Assume $V_A = 20$, a rather large value corresponding to a Gaussian modulation of standard deviation $\sqrt{20}$; use (see Fig. 3.1)

- $A = 7\sqrt{V_A}$, meaning that the actual Gaussian distribution is truncated to 7 standard deviations;
- $N = \lceil 4A \rceil$, meaning that the distribution is discretized in steps of $1/4^{\text{th}}$ of shot noise units.

These choices can be used in practice: for $V_A = 20$, they require $2 \times \lceil 4 \times 7 \times \sqrt{V_A} \rceil + 1 = 253$ discretization steps, that is, an 8-bit discretization grid. The entropy of the corresponding pair of discretized Gaussian values is $2 \times 6.2 = 12.4$ bits. Source coding techniques enable to use on average no more than this randomness quantity when drawing them in practice.

For $Q = 2000$ (chosen to get a sufficiently low value of R_σ), a numerical evaluation yields

$$\Delta_{\text{diag}} \leq 1.02\ 10^{-11}, \tag{3.53}$$

$$\Delta_{\text{nondiag}} \leq 1.04\ 10^{-11}, \tag{3.54}$$

$$R_\sigma \leq 1.09\ 10^{-24}, \tag{3.55}$$

from which we deduce

$$||\rho - \sigma|| \leq 3.31\ 10^{-11}. \tag{3.56}$$

In the above discretization scheme, the mass lost because of the distribution cutoff is evenly distributed among the remaining coherent states. Let us give a similar result for a slightly different cutoff scheme where the lost mass is added to $\omega_{\pm N}$ only: $\omega_k = \frac{A}{N}\frac{1}{\sqrt{2\pi V}}e^{-q_k^2/(2V)}$ for $-N+1 \leq i \leq N-1$, and $\omega_{-N} = \omega_N = (1 - \sum_{i=-N+1}^{N-1} \omega_k)/2$. For this scheme with the same parameters as before, we find

$$||\rho - \sigma|| \leq 2.98\ 10^{-11}. \tag{3.57}$$

Polar approximation

The actual modulation devices implement a polar modulation because phase and intensity are modulated separately. It is therefore natural to investigate the discretization required in polar coordinates to obtain a good approximation of a thermal state.

Let us assume that the polar coordinates are discretized uniformly on $[0, R] \times [0, 2\pi]$. Let us note the discretized values as:

$$r_k = \left(k + \frac{1}{2}\right)\frac{R}{K}, k \in [\![0, K-1]\!], \tag{3.58}$$

$$\theta_l = \left(l + \frac{1}{2}\right)\frac{2\pi}{L}, l \in [\![0, L-1]\!]. \tag{3.59}$$

We consider then an approximation of the form

$$\sigma = \frac{1}{L}\sum_k \omega_k \sum_l |\alpha_{kl}\rangle\,\langle\alpha_{kl}|, \tag{3.60}$$

where $\omega_k = \frac{\gamma_k}{\sum_k \gamma_k}$, $\gamma_k = r_k e^{-r_k^2/(2V)}$ and $|\alpha_{kl}\rangle = e^{-r_k^2/2} \sum_{n=0}^{\infty} \frac{r_k^n e^{in\theta_l}}{\sqrt{n!}} |n\rangle$. Therefore,

$$\langle n|\sigma|m\rangle = \frac{1}{L} \sum_{k=0}^{K-1} \sum_{l=0}^{L-1} \omega_k \langle n|\alpha_{kl}\rangle \langle \alpha_{kl}|m\rangle \tag{3.61}$$

$$= \frac{1}{L} \sum_{k=0}^{K-1} \sum_{l=0}^{L-1} \omega_k \, e^{-r_k^2} r_k^{n+m} \frac{e^{i(n-m)2\pi l/L}}{\sqrt{n!m!}} \tag{3.62}$$

$$= U_{nm,L} \sum_{k=0}^{K-1} \omega_k \frac{e^{-r_k^2} r_k^{n+m}}{\sqrt{n!m!}} \tag{3.63}$$

with $U_{nm,L} = 1$ if L divides $n - m$, and $U_{nm,L} = 0$ otherwise.

Unfortunately, this polar discretization requires a finer discretization than the Cartesian one for the same approximation quality. For instance, with $V_A = 20$ as before, using $Q = L = 2000$ (thus eliminating the term Δ_{nondiag} altogether in Eq. (3.51)) and $R = 7\sqrt{V_A}$, a 17-bit discretization of the amplitude is required to obtain $|\langle 0|\rho|0\rangle - \langle 0|\sigma|0\rangle| \leq 10^{-10}$. Drawing values corresponding to this discretization uses 11 bits for the angle and 15.5 bits for the modulus on average. This situation can be improved by using instead of regularly spaced r_k, points placed according to the Gauss quadratures method, especially the Gauss-Hermite variant: an 9-bit amplitude discretization entropy is found to be sufficient for $\epsilon_{\text{prep}} \leq 10^{-10}$. This is still slightly worse than the Cartesian grid, but could be improved further by making the angle discretization depend on the amplitude, as less points are needed in the vicinity of the origin.

Robustness of bounds

An important question related to the discretization is the robustness of the bounds given in the previous sections when the discretization grid is disturbed by some small systematic error term. This can happen, for instance, because of calibration errors or because of complex discretization effects due to the experimental setup. For example, an amplitude modulator generally produces an amplitude $A = \cos(cV + \phi)$, where V is the voltage applied to it; since V is discrete, the modulated amplitude values are projected to a set that is the image of the discrete set of attainable voltages by the functional realized by the modulator. To model the effect of these errors, we added a small disturbance with Gaussian distribution of standard deviation σ_{error} to each point of the Cartesian grid, and numerically computed the resulting ϵ_{prep}. With parameters as in Section 3.4.3, we get $||\rho - \sigma|| \approx 0.1 \times \sigma_{\text{error}}$. This shows that obtaining $\epsilon_{\text{prep}} \leq 10^{-10}$ in practice may be difficult; it is more realistic to expect $\epsilon_{\text{prep}} \approx 10^{-4}$ or 10^{-5}.

It is true that the proof techniques used today force us to include ϵ_{prep} in the final security parameter of the key, but it is plausible that this is too pessimistic. Indeed, it is known that protocols with a non-Gaussian modulation are secure against all attacks corresponding to a linear channel between Alice and Bob [76]. This gives a hint that approximations of the order of 10^{-4} or 10^{-5} might be sufficient in practice.

3.4.4 Imperfect Calibration of the Detection Setup

We consider now finite-size effects related to the detection setup. We note that a proper calibration of Alice and Bob's devices is crucial to prove the security of the final key [58]. Our goal is to improve and expand the analysis of Ref. [77] concerning finite-size effects in CVQKD [1]. In particular, the values of the quantum efficiency and the electronic noise of Bob's *Homodyne Detection* (HD) can only be estimated up to some finite precision. These inaccuracies must be taken into account when computing a secret key rate compatible with a realistic scenario (where these sources of noise are not assumed to be controlled by Eve) while considering finite-size effects. In the same way, the modulation variance on Alice's side and the excess noise on Bob's side both need to be estimated, in shot noise units, when computing the secret key rate. This implies that any imperfect precision on the estimation of the shot noise has an impact on the secret key rate.

The effect of a noisy HD has already been taken into account in the security proofs [83, 44]. The efficiency of the detection is modeled by a beamsplitter of transmittance η and the electronic noise is modeled by a thermal noise of variance N_{el} added at the second input of the beamsplitter. That is, before Bob's HD, the state received by Bob is mixed with a thermal state of variance N_{el} on a beamsplitter of transmittance η. The variance of the electronic noise of the HD, v_{el}, is linked to N_{el} by $v_{\text{el}} = (1-\eta)(N_{\text{el}}-1)$. Interestingly, the final key rate depends only on one parameter, namely the added noise referred to the input of the measurement device, denoted as $\chi_{\text{hom}} = \frac{1-\eta}{\eta}N_{\text{el}} = \frac{1+v_{\text{el}}}{\eta} - 1$. Therefore, all the combinations of the parameters (η, v_{el}) that give the same χ_{hom} have the same impact on the secret key rate.

In [44], these parameters were supposed to be calibrated in a secure lab, which implies that no attacker can interfere with the calibration procedure. Since this calibration is not performed during a QKD run, the statistical noise due to the finite number of samples used for the estimation can be made arbitrarily small. However, both parameters are still known imperfectly because of the finite precision of the measurement apparatuses. Here we consider an imperfect knowledge of these parameters and its effect on the secret key rate.

In order to calibrate a fiber-based HD, like the one used in [44], one should in fact estimate three quantities:

- the interferometer mode matching η_{mod} with precision $\Delta\eta_{\text{mod}}$,
- the efficiency of the photodiodes η_{phot} with precision $\Delta\eta_{\text{phot}}$,
- the fiber optic transmittance η_{opt} with precision $\Delta\eta_{\text{opt}}$.

Then, the HD efficiency reads $\eta = \eta_{\text{mod}}^2\eta_{\text{phot}}\eta_{\text{opt}}$ [2] and the overall uncertainty is:

$$\Delta\eta = \eta\left(2\frac{\Delta\eta_{\text{mod}}}{\eta_{\text{mod}}} + \frac{\Delta\eta_{\text{phot}}}{\eta_{\text{phot}}} + \frac{\Delta\eta_{\text{opt}}}{\eta_{\text{opt}}}\right) \tag{3.64}$$

The interferometer mode matching efficiency η_{mod} is close to 99%, while a typical value for η_{phot} is 80% with the PIN photodiodes used in [44]. The fiber optic transmittance is usually low (around 80% for fiber-based HD since

[1] Note that finite-size effects are also considered in Ref. [45], where an entropic uncertainty relation is used to prove the security of an entanglement-based CVQKD protocol. Unfortunately, the bounds derived there are too pessimistic to be used in realistic experimental conditions.

[2] Note that η_{mod} is derived from a measurement of the visibility of the interference fringes on one arm of the HD when the Local Oscillator (LO) interferes with another classical signal of the same intensity. It is therefore the experimentally useful quantity to characterize mode mismatching in the interferometer, and is used as a reference for modeling the equivalent beamsplitter transmittance.

losses are usually applied on one arm of the interferometer to compensate for an unbalanced beamsplitter).

The electronic noise v_{el} is estimated as the variance of the HD electronic noise, i.e., the detection output variance when no optical signal enters the detection device. This noise is mainly due to the thermal noise introduced by the load resistance at the entrance of the amplifier circuit (the intrinsic noise of the photodiodes is typically negligible). A straightforward way to determine v_{el} is to measure it directly as the variance of the HD output when no light enters the homodyne detection. Alternatively, one can plot the relationship between the power of a light source entering one branch of the beamsplitter of a balanced shot-noise limited HD and the variance of the HD output, when the other entrance of the HD is disconnected. This relationship should be linear, the Y-intercept being the variance of the electronic noise. Experimentally, the latter method leads to less accurate values of the electronic noise. However, even with the direct method v_{el} can only be known up to a precision Δv_{el}.

The different uncertainties mentioned above can be evaluated depending on the measurement procedure and the precision of the measurement devices. In a practical CVQKD setup, Alice and Bob estimate the quantities required to compute the secret key rate through the sampling of $m = N - n$ pairs of correlated variables $(x_i, y_i)_{i=1\ldots m}$, where N is the total number of quantum signals sent through the quantum channel and n is the number of signals used for the key establishment.

More precisely, the parameter estimation is performed in two steps. First, after the state distribution and measurements, Alice and Bob need to roughly estimate the signal-to-noise ratio of their classical data in order to choose the proper error correcting code for the reconciliation [65]. This typically requires $m = O(\sqrt{N})$. Then, after the (reverse) reconciliation, Alice knows both her raw string and the one received by Bob. In practice, Alice and Bob would publicly compare a small hash of their final string to make sure that the reconciliation procedure succeeded. The size of these strings is N and the parameter estimation can be performed *on the whole string*. The results of this estimation will be used to compute a tight bound on Eve's information about Bob's string.

Since for CVQKD, it is sufficient to estimate the covariance matrix of the state shared by Alice and Bob, the only parameters that need to be estimated are the variance on Alice's and Bob's sides, respectively $\langle x^2 \rangle$ and $\langle y^2 \rangle$, and the covariance between Alice and Bob $\langle xy \rangle$ (assuming here that x and y are centered variables, that is, that $\langle x \rangle = \langle y \rangle = 0$). These values are linked to the key rate parameters through:

$$\langle x^2 \rangle = V_A \tag{3.65}$$

$$\langle y^2 \rangle = \eta T V_A + N_0 + \eta T \xi + v_{\text{el}} \tag{3.66}$$

$$\langle xy \rangle = \sqrt{\eta T} V_A, \tag{3.67}$$

where T is the quantum channel transmittance, V_A is the modulation variance, ξ is the excess noise, and N_0 is the shot noise (all expressed in their respective units and not in shot noise units as it is usually assumed).

Since η and v_{el} are calibrated beforehand, one has four unknown parameters (V_A, N_0, T, ξ) and only three equations. However, by forcing a quantum channel with zero transmittance, we get one more equation:

$$\langle {y_0}^2 \rangle = N_0 + v_{\text{el}}. \tag{3.68}$$

This can be done in Bob's laboratory by measuring the vacuum.

In order to compute confidence intervals for these parameters, we consider here a normal model for Alice and Bob's correlated variables $(x_i, y_i)_{i=1\dots N}$:

$$y = tx + z, \tag{3.69}$$

where $t = \sqrt{\eta T} \in \mathbb{R}$ and where z follows a centered normal distribution with unknown variance $\sigma^2 = N_0 + \eta T \xi + v_{\text{el}}$. Note that this normal model is an assumption justified in practice but not by *current* proof techniques, which show that the Gaussian assumption is valid once the covariance matrix is known [99, 46]. Exploiting symmetries of the protocol in phase-space might be a way to rigorously justify this assumption [73, 75]. The random variable x is a normal random variable with variance V_A in the case of a Gaussian modulation. Another set of Bob's data $({y_0}_i)_{i=1\dots N'}$ can be used to measure the noise when no signal is exchanged (one can take N' to be on the order of N):

$$y_0 = z_0 \tag{3.70}$$

where z_0 follows a centered normal distribution with unknown variance $\sigma_0^2 = N_0 + v_{\text{el}}$. Similarly to the analysis in [77], Maximum-Likelihood estimators $\hat{t}$, $\hat{\sigma}^2$ and $\widehat{\sigma_0}^2$ are known for the normal linear model:

$$\hat{t} = \frac{\sum_{i=1}^N x_i y_i}{\sum_{i=1}^N x_i^2}, \tag{3.71}$$

$$\hat{\sigma}^2 = \frac{1}{N}\sum_{i=1}^N (y_i - \hat{t}x_i)^2, \tag{3.72}$$

$$\widehat{\sigma_0}^2 = \frac{1}{N'}\sum_{i=1}^{N'} {y_0}_i^2, \tag{3.73}$$

$$\hat{V_A} = \frac{1}{N}\sum_{i=1}^N x_i^2. \tag{3.74}$$

The estimators $\hat{t}$, $\hat{\sigma}^2$, $\widehat{\sigma_0}^2$ and $\hat{V_A}$ are independent estimators whose distributions are:

$$\hat{t} \sim \mathcal{N}\left(t, \frac{\sigma^2}{\sum_{i=1}^N x_i^2}\right), \tag{3.75}$$

$$\frac{N\hat{\sigma}^2}{\sigma^2}, \frac{N'\widehat{\sigma_0}^2}{\sigma_0^2}, \frac{N\hat{V_A}}{V_A} \sim \chi^2(m-1) \tag{3.76}$$

where t, σ^2, σ_0^2 and V_A are the true values of the parameters. In the limit of large N, N', one can compute confidence intervals for these parameters:

$$t \in [\hat{t} - \Delta T, \hat{t} + \Delta T] \tag{3.77}$$

$$\sigma^2 \in [\hat{\sigma}^2 - \Delta\sigma^2, \hat{\sigma}^2 + \Delta\sigma^2] \tag{3.78}$$

$$\sigma_0^2 \in [\widehat{\sigma_0}^2 - \Delta\sigma_0^2, \widehat{\sigma_0}^2 + \Delta\sigma_0^2] \tag{3.79}$$

$$V_A \in [\hat{V_A} - \Delta V_A, \hat{V_A} + \Delta V_A], \tag{3.80}$$

where $\Delta T = z_{\epsilon_{\text{PE}}/2}\sqrt{\frac{\hat{\sigma}^2}{N V_A}}$, $\Delta\sigma^2 = z_{\epsilon_{\text{PE}}/2}\frac{\hat{\sigma}^2\sqrt{2}}{\sqrt{N}}$, $\Delta\sigma_0^2 = z_{\epsilon_{\text{PE}}/2}\frac{\widehat{\sigma_0}^2\sqrt{2}}{\sqrt{N'}}$, $\Delta V_A = z_{\epsilon_{\text{PE}}/2}\frac{\hat{V_A}\sqrt{2}}{\sqrt{N}}$ and $z_{\epsilon_{\text{PE}}/2}$ is such that $1 - \text{erf}(z_{\epsilon_{\text{PE}}/2}/\sqrt{2})/2 = \epsilon_{\text{PE}}/2$ (ϵ_{PE}, typically 10^{-10}, is the probability that the estimated parameters do not belong to the confidence region computed from the parameter estimation procedure). Here we have used the error function $\mathrm{erf}(x)$, defined as:

$$\mathrm{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt. \tag{3.81}$$

One can then estimate $T = \frac{\hat{t}^2}{\eta}$ and $\xi = \frac{\sigma^2 - \sigma_0^2}{\hat{t}^2}$ using the previous estimators and their confidence intervals. As regards the shot noise, it is known with a precision that depends both on the number of samples used to compute the estimator $\widehat{\sigma_0^2}$ and on the precision on the electronic noise Δv_{el}.

Once the parameters and their respective confidence intervals have been determined, one can in particular express in shot noise units all the quantities needed to compute $S_{\epsilon_{\mathrm{PE}}}(y : E)$, the maximal value of the Holevo information between Eve and Bob's classical data compatible with the statistics except with probability ϵ_{PE}. Thus, the secret key rate for collective attacks including all the finite-size effects and calibration imperfections discussed previously can be computed as:

$$K_{\mathrm{finite}} = \frac{n}{N}(\beta I(x : y) - S_{\epsilon_{\mathrm{PE}}}(y : E) - \Delta(n)), \tag{3.82}$$

where $\beta I(x : y)$ is the amount of mutual information Alice and Bob were effectively capable to extract through the reconciliation phase (β is the reconciliation efficiency which ranges from 0 when no information was extracted to 1 for a perfect reconciliation scheme) and $\Delta(n)$ is related to the security of the privacy amplification [122, 77].

Figure 3.2 gives the secret key rate for various values of the number of samples $N = N'$. It appears that even taking pessimistic confidence intervals for η and v_{el}, for example with $\Delta\eta = 0.1\eta$ and $\Delta v_{\mathrm{el}} = 0.1 v_{\mathrm{el}}$, the impact on the secret key rate is not significant. However, a high precision on the shot noise is required for long distances since $\eta T \xi$ must be known with a high precision as already observed in [77]. It is worth noting that even using 10^6 samples leads to a positive secret key rate for the Gaussian protocol unlike discrete modulation protocols for which at least 10^8 samples are required [77].

3.4.5 Improved Key Rate with Phase Noise Calibration

In order to obtain precise statements about the security of a given quantum key distribution (QKD) protocol, it is useful to carefully characterize the equipment of Alice and Bob. For CVQKD, this issue has already been addressed extensively for the detection stage. In particular, as was discussed in the previous section, in a calibrated device scenario, the detection model includes a finite quantum efficiency and a given level of electronic noise. Interestingly, both these imperfections act as sources of noise that can be trusted, in the sense that they are not controlled by Eve. This corresponds to the so-called realistic model, as opposed to the paranoid model where the eavesdropper is supposed to control all sources of noise. The realistic model allows one to derive a secret key rate that is actually better than the one obtained without this modeling for the imperfections of Bob's detection.

Concerning the preparation phase of the Gaussian CVQKD protocol that we are considering, recent work has addressed the issue of imperfections in Alice's state preparation. In particular, Refs [39, 141, 127] studied the situation where Alice in fact prepares thermal states instead of coherent

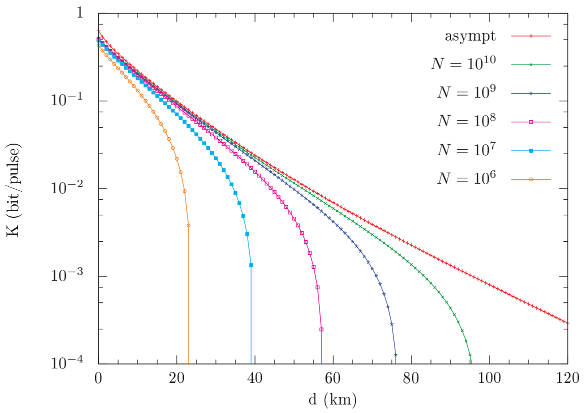


Figure 3.2: Secret key rate for collective attacks including finite-size effects and calibration imperfections with respect to the distance for different values of the number of samples. The transmittance T and distance d are linked with the expression $T = 10^{-\alpha d/10}$, where α is the loss coefficient of the optical fiber. $V_A = 2.5$, $\xi = 0.01$, $\eta = 0.6$, $v_{\mathrm{el}} = 0.01$, $\alpha = 0.2$ dB/km, $\beta = 95\%$, $\Delta\eta = 0.1\eta$, $\Delta v_{\mathrm{el}} = 0.1 v_{\mathrm{el}}$, $\epsilon_{\mathrm{PE}} = 10^{-10}$, $N = \mathrm{asympt}, 10^{10}, 10^{9}, 10^{8}, 10^{7}, 10^{6}$ from top to bottom.

states. In fact, it is even possible to achieve CVQKD in the microwave regime where the preparation of pure coherent states is impossible [146, 147]. One remark about these works is that they consider a specific kind of imperfection that can be efficiently dealt with experimentally (at least in the optical regime). Indeed, if Alice really prepares thermal states instead of coherent states, one simple solution is to increase the variance of modulation and then to strongly attenuate the resulting state in order to obtain something very close to a coherent state. For this reason, the problem of preparing thermal states instead of coherent states is not really an issue in a practical scenario.

A more relevant issue concerns non-Gaussian sources of noise. In particular, there always is some phase noise on the state prepared by Alice. A typical value for the variance of this noise is $10^{-4}N_0$ per photon in the pulse [84]. One cannot suppress this noise by increasing the variance of the modulation and then attenuating the state, as mentioned above. Studying this noise is therefore of particular theoretical interest and of importance for actual experiments.

An important property of this noise is that it leaves the global state $\rho_{B_0} = \mathrm{tr}_A \rho_{AB_0}$ sent by Alice in the quantum channel (and therefore seen by Eve) invariant. This is different from the thermal noise considered in [141, 127], which increases the variance of ρ_{B_0}. In particular, this means that this noise can be modeled as an imperfect measurement for Alice in the entanglement-based equivalent protocol. In that picture, Alice prepares two-mode squeezed vacuum states, sends one mode to Bob and measures the other one with a heterodyne detection. When modeling the noise, one can keep the preparation of two-mode squeezed vacuum states, and only Alice's detection will be noisy. This simply means that the *classical* data that she gets is noisy (with some phase noise). Therefore, the only consequence of this noise is that it degrades the mutual information shared between Alice and Bob, but it cannot increase Eve's information about Bob's measurement outcome, which is of interest in a reverse reconciliation scheme.

More specifically, in this case, the secret key rate against collective attacks is $K_{\text{asympt}} = \beta I(x:y) - \chi(y:E)$, where $\beta I(x:y)$ is defined as in the previous section and $\chi(y:E)$ is an upper bound on Eve's information on Bob's measurement outcomes. Because one can model phase noise as a local noise acting on Alice's system, it can only decrease the quantity $I(x:y)$ but cannot help the eavesdropper by increasing $\chi(y:E)$. In such a scenario, one can expect that the phase noise can be removed from the excess noise when computing Eve's information, leading to a realistic model for the preparation stage, similarly to the detection stage. This should lead to better secret key rates in practice.

Model for the phase noise

The phase noise can be modeled as applying a phase rotation $U(\theta) = \exp(i\theta a^\dagger a)$ on Alice's mode with a random phase θ characterized by some probability distribution $p(\theta)$. This means that when Alice tries to prepare some coherent state $|\alpha\rangle$ in the prepare-and-measure protocol, she actually prepares a state with a noisy phase: $\rho_\alpha = \int U(\theta)|\alpha\rangle\langle\alpha|U(\theta)^\dagger p(\theta)\mathrm{d}\theta$. Let us assume that Alice initially prepares an ideal two-mode squeezed vacuum state with a variance V_A. This state ρ_{ideal} has the following covariance matrix (for a displacement vector $[q_A, p_A, q_B, p_B]^T$):

$$\Gamma_{\text{ideal}} = \begin{bmatrix} V_A \mathbb{1}_2 & W\sigma_z \\ W\sigma_z & V_A \mathbb{1}_2 \end{bmatrix}, \tag{3.83}$$

where $W := \sqrt{V_A^2 - 1}$ and $\sigma_z = \mathrm{diag}(1, -1)$.

Applying a local phase shift $U(\theta)$ on Alice's mode gives a state with a covariance matrix $\Gamma(\theta)$ given by

$$\Gamma(\theta) = \begin{bmatrix} V_A & & W\cos\theta & W\sin\theta \\ & V_A & W\sin\theta & -W\cos\theta \\ W\cos\theta & W\sin\theta & V_A & \\ W\sin\theta & -W\cos\theta & & V_A \end{bmatrix}. \tag{3.84}$$

Finally, the state affected by the phase noise is a classical mixture of states with random phase shifts $\rho = \int (U_A(\theta) \otimes \mathbb{1}_B)\rho_{\text{ideal}}(U_A(\theta)^\dagger \otimes \mathbb{1}_B)p(\theta)\mathrm{d}\theta$, and its covariance matrix is

$$\Gamma_{\text{phase noise}} = \begin{bmatrix} V_A \mathbb{1}_2 & \sqrt{\kappa}W\sigma_z \\ \sqrt{\kappa}W\sigma_z & V_A \mathbb{1}_2 \end{bmatrix}, \tag{3.85}$$

where we assumed that the distribution θ is symmetric, and more precisely that $\int p(\theta)\sin\theta \mathrm{d}\theta = 0$, and introduced $\kappa := \left(\int p(\theta)\cos\theta\mathrm{d}\theta\right)^2 = (E[\cos\theta])^2$, where $E[X]$ is the expectation of the random variable X.

The interesting point is that from both Bob and Eve's points of view, it does not change anything whether a random phase shift is applied. In particular, the value of $\chi(y:E)$ quantifying the information that Eve can acquire about the raw key in a *reverse reconciliation* scenario does not depend on the value of the phase noise. Note that this statement would not be true in a direct reconciliation scenario where the raw key would correspond to Alice's noisy data.

Let us suppose that the quantum channel between Alice and Bob is characterized by its transmittance T and excess noise ξ. The covariance matrix Γ_{AB} of the bipartite state shared by Alice and Bob after the quantum channel is then given by:

$$\Gamma_{AB} = \left[\begin{array}{cc} V_A \mathbb{1}_2 & \sqrt{\kappa T} W \sigma_z \\ \sqrt{\kappa T} W \sigma_z & (T(V_A - 1) + 1 + T\xi) \mathbb{1}_2 \end{array} \right]. \tag{3.86}$$

If they were not taking phase noise into account (that is, if κ was equal to 1), Alice and Bob would estimate a transmittance T' and an excess noise ξ' such that

$$\left\{ \begin{array}{l} T' = T\kappa \\ T'(V_A - 1) + 1 + T'\xi' = T(V_A - 1) + 1 + T\xi \end{array} \right. \tag{3.87}$$

that is

$$\left\{ \begin{array}{ll} T & = T'/\kappa \\ \xi & = \xi' - (1-\kappa)(V_A - 1) \end{array} \right. \tag{3.88}$$

If the phase noise parameter κ is known, one can estimate the covariance matrix as usual, hence obtaining values (T', ξ') and use the formula above to deduce the parameters (T, ξ) that can be used instead to compute Eve's information $\chi(y : E)$.

For this technique to work, it is necessary to be able to measure $\kappa = (E[\cos\theta])^2$ experimentally. This is discussed in the next section.

Experimental evaluation of the phase noise

The evaluation of the phase noise can be performed with a phase sensitive apparatus which allows us to compute an estimate of the noise between a signal whose quadratures are modulated following a chosen sequence and the outputs of some chosen quadrature measurements. A homodyne or heterodyne detection can be used for this purpose.

Similarly to what is done on Bob's side when the homodyne detection efficiency and the variance of the electronic noise are calibrated, it is necessary to assume that the calibration of the phase noise is performed in a safe place, i.e. that Eve cannot interfere with Alice's apparatus during the phase noise measurement. The measurement can also be performed during a run of the protocol but one still needs to assume that Eve cannot interfere with Alice's device. This is crucial since overestimating the phase noise would lead to an overestimation of the secret key rate.

Here, we are interested in the phase noise in the prepare-and-measure version of the protocol. The procedure to estimate it goes as follows: Alice modulates as usual with a bivariate Gaussian distribution and she measures either one of the quadratures with a homodyne detection. Computing the variance of her measurement outcomes allows here to infer the quantity κ introduced above. Let us denote by ϕ the random variable corresponding to the angle between the modulated state and the measured quadrature and by B the random variable corresponding to the noise. This means for example that Alice prepared the state centered in $Ae^{i\phi}$ (with $A \geq 0$) and that the outcome of her q-quadrature measurement was $A\cos\phi + B$. This noise B can be decomposed into the sum of a component orthogonal to the signal and a component parallel to the signal:

$$B = B_{\parallel} \cos\phi + B_{\perp} \sin\phi, \tag{3.89}$$

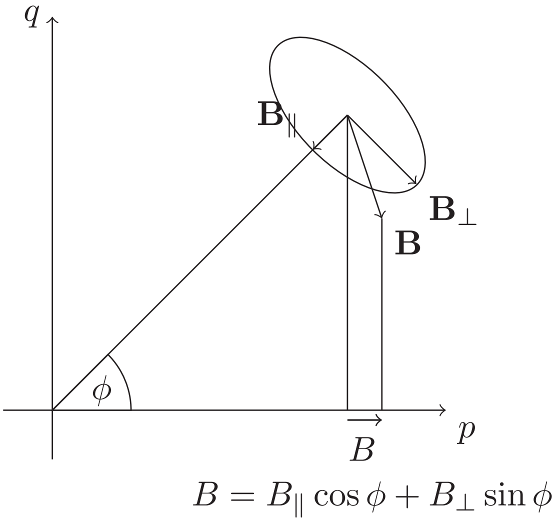


Figure 3.3: Experimental evaluation of the phase noise. The noise $\mathbf{B}$ before Bob's measurement can be decomposed into the sum of a component orthogonal to the signal $\mathbf{B}_{\perp}$ and a component parallel to the signal $\mathbf{B}_{||}$. The result of Bob's q-quadrature measurement is $A\cos\phi + B$ where Alice prepared the state centered in $Ae^{i\phi}$ with $A \geq 0$.

where we assume that $B_{||}$ and $B_{\perp}$ are independent of ϕ. Figure 3.3 gives an illustration of this decomposition. We can easily build estimators of $B_{||}$ and $B_{\perp}$ (in the following, $E[X]$ and $V[X]$ refer respectively to the expectation and variance of the random variable X):

$$\begin{aligned} V[B\cos\phi] &= V[B_{||}\cos^2\phi] + V[B_{\perp}\cos\phi\sin\phi] && (3.90)\\ &= V[B_{||}]E[\cos^4\phi] + V[B_{\perp}]E[\cos^2\phi\sin^2\phi] && (3.91)\\ &= 3/8V[B_{||}] + 1/8V[B_{\perp}] && (3.92)\\ V[B\sin\phi] &= 1/8V[B_{\perp}] + 3/8V[B_{||}] && (3.93) \end{aligned}$$

Since both $V[B\cos\phi]$ and $V[B\sin\phi]$ can be measured experimentally, one therefore has access to the values of $V[B_{\perp}]$ and $V[B_{||}]$. Here, we assume that the only sources of noise are the shot noise and the phase noise. We assume that $B_{\perp}$ can be fully described by the shot noise and the phase noise:

$$\begin{aligned} V[B_{\perp}] &= N_0 + V[A\sin\theta] = N_0 + E[\sin^2\theta]E[A^2] && (3.94)\\ E[\sin^2\theta] &= \frac{V[B_{\perp}] - N_0}{E[A^2]} = E_1 && (3.95) \end{aligned}$$

where A is the amplitude of the modulated signal and where we used $E[\sin\theta] = 0$. The assumption of a small phase noise, i.e. small values of θ, gives:

$$\begin{aligned} E[\cos\theta] &= E[1 - \theta^2/2] && (3.96)\\ &= 1 - \frac{1}{2}E_1 && (3.97) \end{aligned}$$

Figure 3.4 compares the so-called realistic and paranoid models. We consider a pessimistic scenario where the excess noise on Alice's side is about 2.5% of the shot noise (the detector quantum efficiency and electronic noise

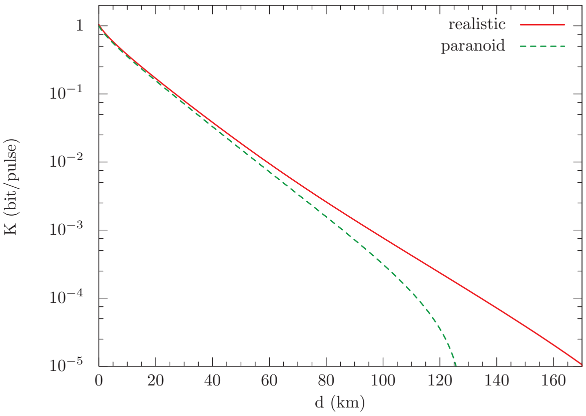


Figure 3.4: Secret key rate for collective attacks in the asymptotic regime. The plot at the top is obtained in the so-called realistic model where the phase noise is calibrated and is considered as a local noise useless to the eavesdropper. The plot at the bottom corresponds to the so-called paranoid model where all the sources of noise are attributed to the eavesdropper. The transmittance T and distance d are linked with the expression $T = 10^{-\alpha d/10}$, where α is the loss coefficient of the optical fiber. $V_A = 2.5$, $\xi = 0.025$, $\alpha = 0.2$ dB/km, $\beta = 95\%$, $E_1 = 3\ 10^{-3}$.

are not taken into account here, for clarity). For a modulation variance $V_A = 2.5$, we measured experimentally $E_1 = 3\ 10^{-3}$ with a system similar to the one described in [44]. This leads to a realistic value of the excess noise $\xi_{\text{real}} = 1.75\%$. The result on the secret key rate for collective attacks is an increased achievable distance by about 40 km.

3.5 Conclusion

In this chapter, we have analyzed several types of imperfections that appear in practical implementations of Gaussian continuous-variable QKD protocols. In particular, we studied a realistic approximate Gaussian modulation in the state preparation at Alice's site, the calibration of detection characteristics estimated with a finite precision at Bob's site, and the presence of intrinsic phase noise in the prepared states. In all cases, we provided a precise model of the imperfection and used this model to examine its effect on the security and performance of the protocol. These effects are more or less significant in practice: it is clear, for instance, that taking into account the phase noise in the security proof of a realistic scenario provides an important advantage in terms of secret key rate, while carefully approximating the ideal Gaussian modulation with respect to the shot noise values can minimize the impact of this imperfection. Finally, as expected, finite-size effects at all stages of the protocol should always be considered when calculating practical secret key rates.

This analysis demonstrates the importance of refining security proofs of QKD protocols to consider practical imperfections. In particular for CVQKD protocols, where potential side channels have not been yet widely studied, it provides specific ways to bypass attacks based on improperly modeled devices and procedures.

Chapter 4

Experimental Setup

Contents

4.1 Optical fibers 67

4.1.1 Waveguides 68

4.1.2 Transmission characteristics 68

4.1.3 Dispersion 69

4.1.4 Connections 70

4.2 Laser Source 70

4.3 Electro-optic Modulators 71

4.4 Light detection 74

4.4.1 Homodyne Detection Principle 74

4.4.2 Impact of the Imperfections on the Homodyne Detection 76

4.4.3 Electronics of the Homodyne Detection 77

4.5 Time and Polarization Multiplexing 77

4.6 Optical Component Characteristics Summary . 78

4.7 Acquisition and Control Cards 78

4.8 Random Numbers 80

4.9 Computing Power 84

In this chapter, we introduce the building blocks of our fiber-based experimental setup. We start by recalling some basic properties of optical fibers. Then, we successively detail the different optical components of our system: a standard telecom laser diode used in pulsed regime, electro-optic modulators, the homodyne detection of a quadrature of the electromagnetic field and a time and polarization multiplexing scheme. Finally, we consider the electronics part of our experiment, namely acquisition and control cards, random number generators and computing power.

4.1 Optical fibers

Most of quantum optics experiences are done in free space. This is because the physical properties of free space components together with the control of their alignment with a high precision allow for a better control of the losses and therefore the properties of the quantum states of interest. However, it is also harder to set up a free space experiment: the difficulties are mainly due to light alignment and mode coupling. While these implementation difficulties can be overcome in a lab, provided very stable optics tables, moving free space quantum key distribution experiments from optics

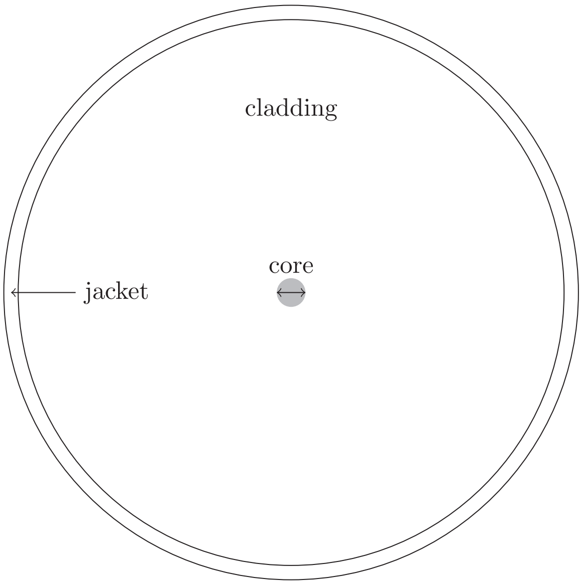


Figure 4.1: Generic optical fiber design. An optical fiber is composed of a high refractive index core surrounded by a low-index cladding. This design explains that the incident light is kept in the core by total reflection.

tables to rackable boxes located in server rooms is very challenging. Furthermore, although there have been several demonstrations, long-distance free-space QKD experiments [140, 123] suffer from laser aiming difficulties and transmission fluctuations due to atmospheric disturbance.

Optical fibers allow to get rid of light alignment and light guide difficulties. Fiber-based QKD products [2, 1, 4, 5] also benefit from well integrated components optimized for the telecommunications industry during several decades. Nevertheless, there are several drawbacks when using optical fibers and we describe in the following sections the optical fibers specific aspects that impact our experimental setup.

4.1.1 Waveguides

An optical fiber is a thin and flexible fiber made of silica or plastic. It is an optical *waveguide*, i.e. it conveys electromagnetic waves in the optical spectrum between its endpoints. The main particularity of optical fibers in comparison with other waveguides is the presence of a cylindrical axis of symmetry. Figure 4.1 shows the generic optical fiber design, which consists of a core of high refractive index surrounded by a low-index cladding. With such a design, incident light is kept in the core by total reflection. Some fibers support many propagation paths and are called *Multi-Mode Fibers* (MMF), these are fibers of large core (about 80 μm) and large numerical aperture. Other fibers only support a single mode and are called *Single Mode Fibers* (SMF). Single mode fibers at 1550 nm have a core of about 8 to 10 μm.

4.1.2 Transmission characteristics

Attenuation is the reduction of intensity of the light signal as it travels through the fiber. It occurs due to fundamental scattering processes (mostly Rayleigh scattering), scattering caused by inhomogeneities introduced in the

	Window Range	Operating Wavelength
1^{st} Window	800 - 900 nm	850 nm
2^{nd} Window	1260 - 1310 nm	1310 nm
3^{rd} Window	1500 - 1600 nm	1550 nm

Table 4.1: Transmission windows ranges and operating wavelengths of optical fibers with a silica core.

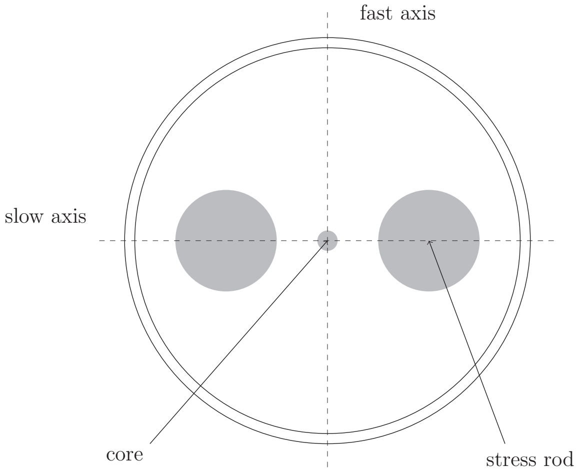


Figure 4.2: Cross section of a Panda type PM fiber. The cylindrical stress rods that run parallel to the fiber core create two different effective optical indexes along two orthogonal axis that are called the fast axis and the slow axis.

fabrication process and absorption of light by molecules. This limits the range of application of optical fibers at both short and long wavelengths. Table 4.1 gives the transmission windows of typical optical fibers with a silica core. The main transmission peak is at 1550 nm which explains why this wavelength is chosen for long-distance telecommunications.

4.1.3 Dispersion

Another source of limitation for long-distance communications with optical fibers is fiber *dispersion*, i.e. the variation of the propagation velocity with either optical frequency or path length. One source of dispersion is inter-modal dispersion in MMF: the arrival times of the different modes of the signal are not the same and the resulting shape is distorted, which limits the bandwidth of MMF. Dispersion is also caused by material dispersion due to variation of the refractive index of material with wavelength. Finally, waveguide dispersion is caused by the fiber geometry in SMF fibers: the chromatic dispersion of the input light results in different propagation speeds due to the boundary conditions of the waveguide.

SMF do not conserve polarization. Any twist of the fiber can introduce a *birefringence*, that is the property of having a refractive index that depends on the polarization and propagation direction of light. *Polarization-maintaining Fibers* (PMF) are optical fibers which maintain the polarization of linearly polarized light waves during propagation. The cross-coupling of optical power between the polarization modes is very low. Such fibers can be made by introducing stress rods of another material (typically boron for

Panda fibers) within the cladding. Stress rods induce an anisotropy that can be characterized by different effective optical indexes along two orthogonal axis called the fast axis and the slow axis ($\Delta n = 10^{-3}$ between the two axis). Panda style fibers are named based on the stress rods used. Stress rods are cylindrical and run parallel to the fiber core. These fibers have historically been used in telecoms applications, as it is easier to maintain uniformity in their cylindrical stress rods over very long lengths than with other stress shapes when manufacturing.

In our system, we used Panda PMF for all our components except for the delay lines, the Faraday mirrors, and the photodiodes, which use SMF.

4.1.4 Connections

Optical fibers can be connected to each other by optical fiber connectors or by splicing. Optical fiber connectors allow for a good flexibility as regards components replacement. They mechanically couple and align fiber cores so light can pass with high power transmission. There exists tens of standard type connectors. Good connectors do not lose much power because of fiber misalignments or reflections. We use *Ferrule Connectors* (FC) that were designed for use in high-vibration environments. The fiber end is embedded in a ferrule and the tip is polished to produce a rounded surface. Several grades of polish are available for the fiber tip: *Physical Contact* (PC), *Ultra Physical Contact* (UPC) or *Angled Physical Contact* (APC), where the fiber end is polished at an angle that prevents light coming from the reflection at the connection to travel back in the fiber. In the latter case, the angle causes the reflected light to leak out into the cladding. In our setup, we use only APC connectors for two main reasons. First, reflections could be exploited by an eavesdropper to probe the system by sending light into the output port and analyzing the reflected light and such a probing is harder to perform with APC connectors. Second, connection between APC connectors and non angled connectors result in high insertion loss.

4.2 Laser Source

The GG02 protocol we described in chapter 3 involves a Gaussian modulation of the light in phase space. Such a modulation cannot be achieved by direct modulation of the current of a laser. We will see in the next section that we can use fast optical modulators to perform this modulation.

Another optical signal is required to measure quadratures of the light, a classical local oscillator, i.e. a strong signal coherent with the quantum signal. In theory, this strong signal could be generated locally on Bob's side but locking its phase to the phase of the quantum signal is rather challenging experimentally. This is why in our experiment we chose to generate the local oscillator on Alice's side and send it through the quantum channel together with the quantum signal. We opted for a time and polarization multiplexing scheme as this will be detailed later. This implies that the local oscillator signal must be strongly attenuated during the signal pulses to avoid interference between them during the multiplexing step. A direct modulation of the laser allows us to do that: when the current that drives the laser diode is below the laser threshold a perfect extinction is achieved except for a low fluorescence incoherent with the quantum signal.

We use a *Distributed Feedback* (DFB) standard telecom laser at 1550 nm

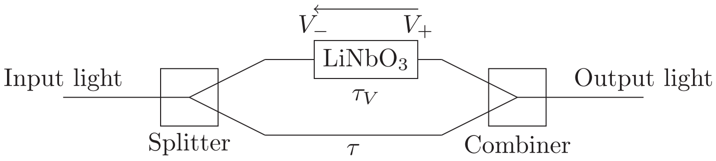


Figure 4.3: Schematics of the principle of a LiNBO_3 optical modulator. The input light if splitted into two optical beams. One travels through a length of LiNbO_3 crystal while the other experiences a fixed delay. After the light travels trhough these two paths, an optical combiner merges the two paths and the resulting light travels until the output of the component. A voltage-induced change in the refactive index is obtained on the LiNbO_3 path. As a result, the two light beams interfere constructively of destructively at the combiner depending on the applied voltage.

with a maximum output power of 30 mW and a spectral width of about 1 MHz when operated in the continuous regime. Our custom laser card can provide pulses with a duration between 10 ns and 100 ns and at a repetition rate between 500 kHz and 5 MHz. When using 100 ns pulses at a repetition rate of 500 kHz, the wavelength of the laser pulse varies by about 0.1 nm which corresponds to a spectral width of about 12.5 GHz.

4.3 Electro-optic Modulators

In our protocol, we modulate both the phase and the amplitude of the optical signal with *Electro-optic Modulators* (EOM) driven with an acquisition card. We benefit from lithium niobate (LiNbO$_3$) modulators optimized for high-speed telecommunications. They provide a high bandwidth and can be designed for zero-chirp operation contrary to direct modulation of a laser diode. Zero-chirp modulators help to minimize fiber dispersion effects in a telecommunication system. LiNbO$_3$ modulators also feature stable operation over temperature and low bias-voltage drift rates. These are desirable characteristics to operate them over long periods of time in a server room environment whose temperature is not perfectly controlled.

In a LiNbO$_3$ modulator, modulation is produced by a voltage-induced change in the refractive index. Since the index change is small, sufficient modulation can be obtained using either large voltages or long electrode lengths. Figure 4.3 shows the schematics of the principle of an optical modulator. The input light enters the modulator via the input fiber. Then the light is split into two fibers with an optical splitter and one fiber path travels through a length of LiNbO$_3$ crystal while the other fiber path experiences a fixed delay. After the light travels through these two paths, an optical combiner merges the two paths and the light travels until the output of the component. If the time delay through the crystal and the fixed fiber are equal, the two light beams interfere constructively at the combiner while they will interfere destructively if the delay through the crystal is changed by half of one wavelength. Figure 4.4 gives the measured voltage on Alice's photodiode with respect to the voltage applied to the amplitude modulator. A ramp voltage is applied to the amplitude modulator with a NI PCI-6115 acquisition card and for 2^{16} samples. The measurement of signal intensity using a photodiode and an amplifier circuit is a sinus function. The local

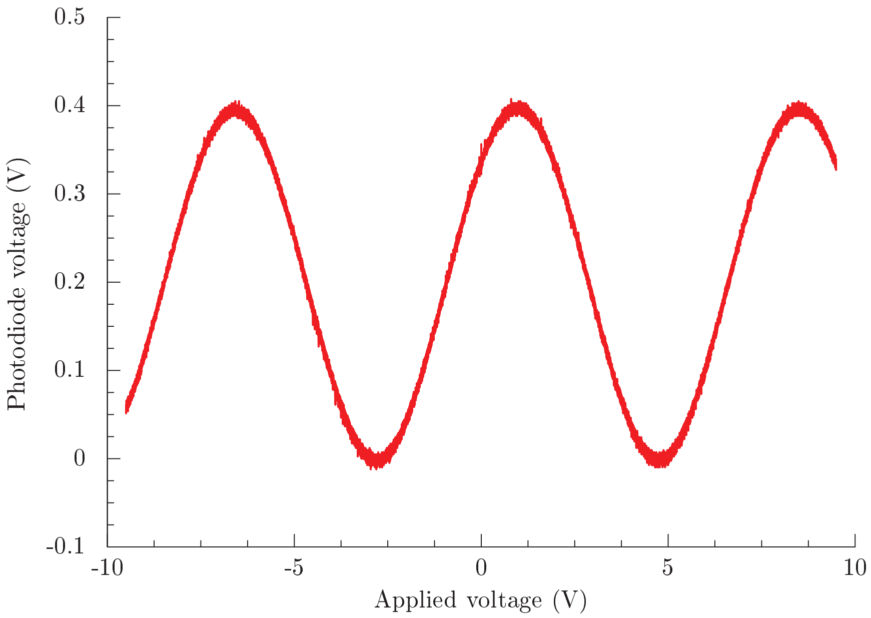


Figure 4.4: Measured voltage on Alice's photodiode with respect to the voltage applied to the amplitude modulator. A ramp voltage is applied to the amplitude modulator with a NI PCI-6115 acquisition card and for 2^{16} samples. The measurement of signal intensity using a photodiode and an amplifier circuit is a sinus function. The local minimum closest to a zero voltage is called V_{bias} while the voltage difference between a minimum and the next maximum is called V_{π}.

minimum closest to a zero voltage is called V_{bias} while the voltage difference between a minimum and the next maximum is called V_{π}.

$LiNbO_3$ material is subject to temperature variations. This results in a variation of the voltage that must be applied to the modulator to obtain the highest extinction ratio. Figure 4.5 shows the different responses to a ramp voltage that were obtained on Alice's photodiode at different moments during a 24 hour window. One can see that the answer is always a sinus function characterized by the same period but shifted along the x axis. When applying the bivariate Gaussian modulation of the GG02 protocol characterized by a variance V_A, such a drift in the amplitude modulator V_{bias} causes a variance variation, which results in a suboptimal secret key rate. Figure 4.6 shows how the statistics on Alice's photodiode are affected when no feedback control is performed on Alice's amplitude modulator. One can see that the V_{π} is quite stable while the V_{bias} varies notably. There are two basic possibilities to perform this feedback control. The first one consists in defining a set of calibration pulses that are used only to evaluate the amplitude modulator parameters and are discarded from the raw key. This method allows us to choose freely the amplitude and the number of the calibration pulses. However, it lowers the raw key rate and thus the secret key rate of the system. A second method consists in evaluating the amplitude modulator parameters directly on the modulated pulses. We chose to use this method that gives satisfactory results and does not penalize the secret key rate. Figure 4.7 shows the improvement on the photodiode statistics stability when using our feedback control.

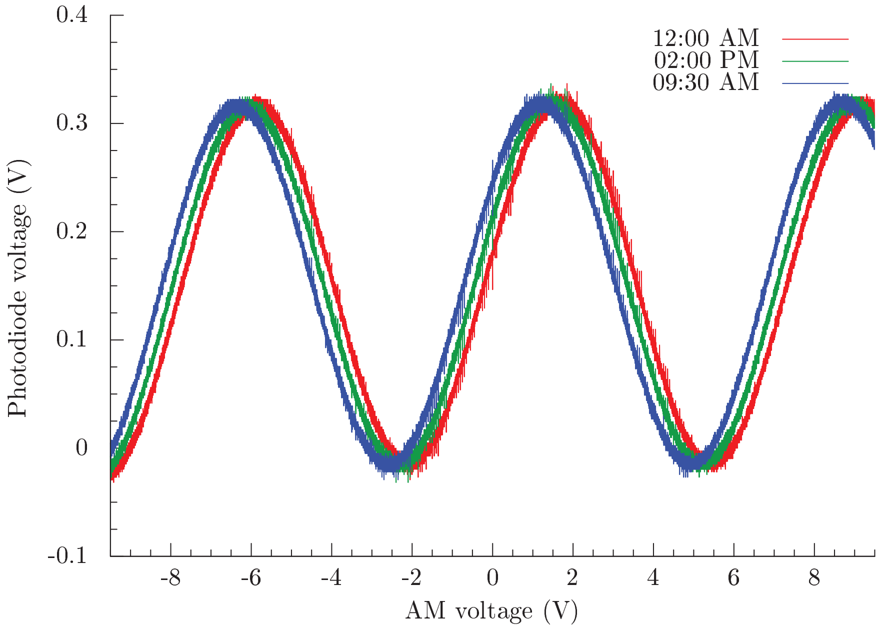


Figure 4.5: Alice's photodiode answer to a ramp voltage at selected times during a 24 hours period. This figure shows that the V_{bias} of an amplitude modulator cannot be assumed to be constant. Temperature drifts affect lithium niobate and the sinus function is displaced at different times of the day.

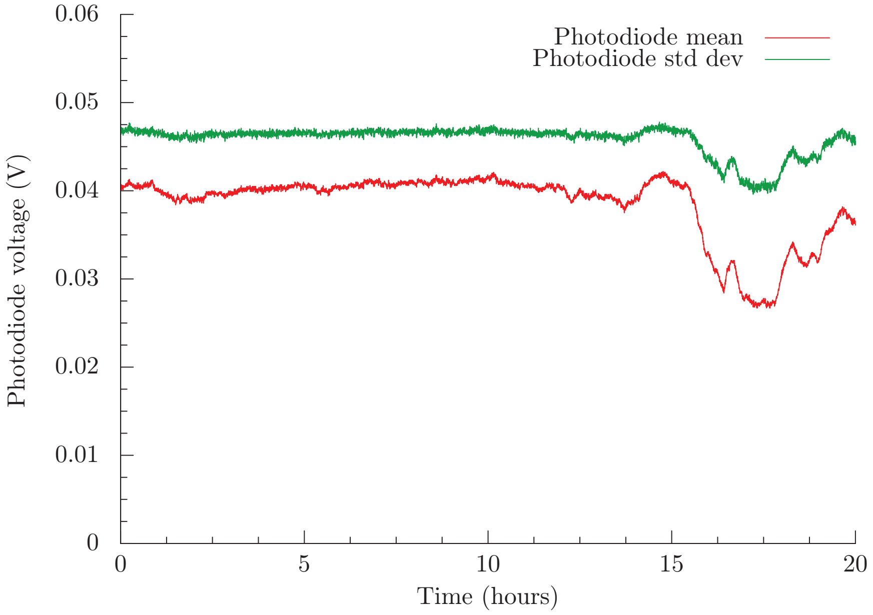


Figure 4.6: Alice's photodiode mean and standard deviation during 20 hours when no feedback control of Alice's amplitude modulator is used.

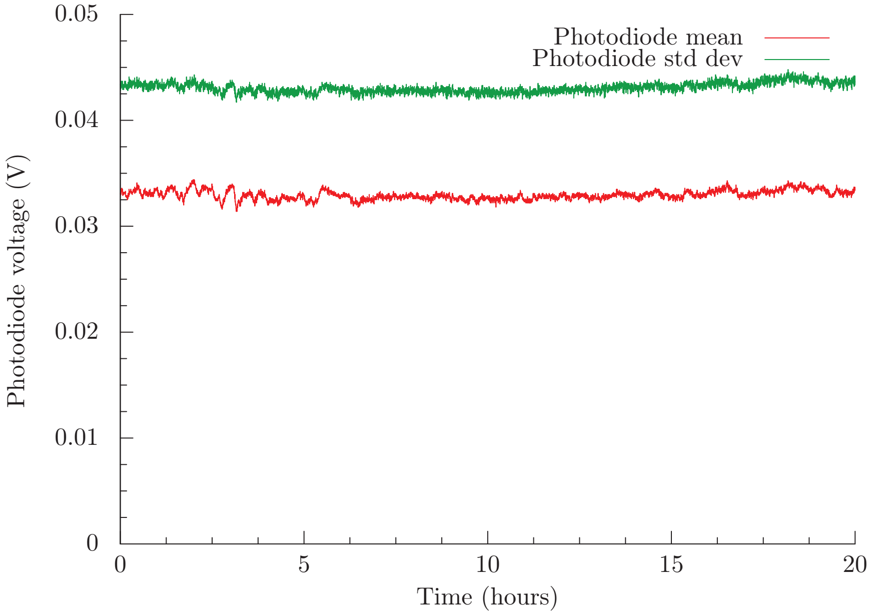


Figure 4.7: Alice's photodiode mean and standard deviation during 20 hours when Alice's amplitude modulator feedback control is used.

4.4 Light detection

We are interesting in measuring quadratures of the electromagnetic field. Such measurements cannot be done with a regular photodiode and its amplifier circuit for two reasons: such a system output a signal proportional to the intensity of the field or the number of photons of the field, which are quadratic quantities with respect to the field, and the oscillation frequency of the field is several order of magnitudes faster than the bandwidth of current photodiodes. Fortunately, interferences between a signal field and a synchronous reference field solve these two problems. They allow to measure a term proportional to the quadrature of the field and the interferences envelope fluctuates at a frequency that can be measured with an electronic circuit.

4.4.1 Homodyne Detection Principle

Figure 4.8 gives an illustration of the homodyne detection principle. The weak quantum signal and a strong classical signal coherent with the quantum signal are mixed on a beam splitter. The intensity of each output is measured with a high quantum efficiency photodiode. Then the photocurrents are subtracted to eliminate the mean intensities of each path and output an electronic signal proportional to the interference between the local oscillator (LO) and the signal. The LO plays both the role of an optical amplifier, that allows us to detect a weak signal with an appropriate electronics circuit, and of a phase reference. A phase modulator on the local oscillator path allows us to measure an arbitrary quadrature of the field.

Let us look at the theoretical equations that describe the homodyne detection. Each path of the homodyne detection is described by a monomode

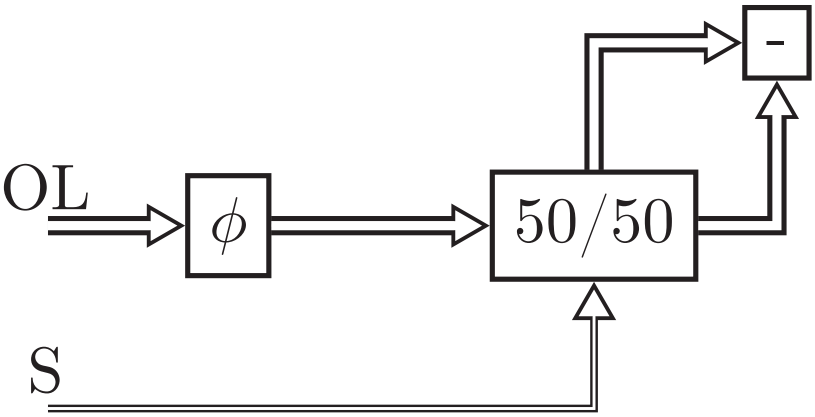


Figure 4.8: Principle of the homodyne detection. A strong signal called local oscillator (LO) interferes with a weak coherent signal on a balanced beam splitter. The LO plays both the role of an optical amplifier, that allows us to detect a weak signal with an appropriate electronics circuit, and of a phase reference. A phase modulator on the local oscillator path allows us to measure an arbitrary quadrature of the field. After the beam splitter, the difference of the two signals is performed with two photodiodes and an amplifier circuit.

annihilation operator $\hat{a}_\pm$:

$$\hat{a}_\pm = \frac{1}{\sqrt{2}}(\hat{a}_{ol} \pm \hat{a}_s) = \frac{1}{\sqrt{2}}(|\mathcal{E}_{ol}|e^{i\phi_{ol}} \pm \hat{a}_s) \tag{4.1}$$

where we neglected the quantum fluctuation of the local oscillator and considered it as a classic field equal to its mean intensity. Since the photocurrents of each path are proportional to the photon number operator we get:

$$\hat{I}_\pm = \hat{a}_\pm^\dagger \hat{a}_\pm = \frac{1}{2}|\mathcal{E}_{ol}|^2 + \frac{1}{2}\hat{a}_s^\dagger \hat{a}_s \pm \frac{1}{2}|\mathcal{E}_{ol}|(e^{-i\phi_{ol}}\hat{a}_s + e^{i\phi_{ol}}\hat{a}_s^\dagger) \tag{4.2}$$

After subtraction of the mean intensities, the difference of the photocurrents is proportional to $X_{s,\phi_{OL}}$ the component of the signal quadrature that is in phase with the local oscillator and defined by $\mathcal{E}_s = \frac{1}{2\sqrt{N_0}}(X_{s,\phi_{ol}} + iP_{s,\phi_{ol}})e^{i\phi_{ol}}$:

$$\Delta\hat{I} = |\mathcal{E}_{ol}|(e^{-i\phi_{ol}}\hat{a}_s + e^{i\phi_{ol}}\hat{a}_s^\dagger) = \sqrt{\frac{I_{ol}}{N_0}}X_{s,\phi_{ol}} \tag{4.3}$$

where $I_{ol} = |\mathcal{E}_{ol}|^2$ is the intensity of the field. This equation explains the observed proportionality between the variance of the measurements and the local oscillator intensity for a balanced homodyne detection whose signal input port is blocked. This gives an easy way to calibrate the standard noise reference N_0. However, the use of such a calibrated value for the shot noise in a QKD protocol might be targeted by an attacker as we explain in chapter 5. We proposed a countermeasure against such local oscillator calibration attacks that consists in calibrating this shot noise value in real-time during a QKD run.

4.4.2 Impact of the Imperfections on the Homodyne Detection

We considered an ideal model for the homodyne detection. In practice, several imperfections occur in an experimental implementation of an homodyne detection. Here, we consider the imbalance between the optical paths, the losses introduced by the homodyne detection and the effect of the quantum modelisation of the local oscillator beam.

The imbalance between the intensity of the two optical paths can be described by an imperfect beam splitter whose transmission T and reflectivity R are:

$$T = \frac{1}{2} + \epsilon \tag{4.4}$$

and

$$R = \frac{1}{2} - \epsilon \tag{4.5}$$

for small values of ϵ. In this case, one can compute the photocurrents values using a classical modelisation as:

$$\begin{aligned} I_+ &= |\sqrt{T}\mathcal{E}_{ol} + \sqrt{R}\mathcal{E}_s| && (4.6)\\ &= \frac{1}{2}(I_{ol} + I_s) + \epsilon(I_{ol} - I_s) + 2\sqrt{\frac{1}{4} - \epsilon^2}|\mathcal{E}_{ol}\mathcal{E}_s| \cos\phi_{ol} && (4.7)\end{aligned}$$

and

$$\begin{aligned} I_- &= |\sqrt{R}\mathcal{E}_{ol} - \sqrt{T}\mathcal{E}_s| && (4.8)\\ &= \frac{1}{2}(I_{ol} + I_s) - \epsilon(I_{ol} - I_s) - 2\sqrt{\frac{1}{4} - \epsilon^2}|\mathcal{E}_{ol}\mathcal{E}_s| \cos\phi_{ol} && (4.9)\end{aligned}$$

Since $\epsilon^2 \ll \frac{1}{4}$ and $I_s \ll I_{ol}$ we get:

$$\begin{aligned} \Delta I &= 2|\mathcal{E}_{ol}||\mathcal{E}_s| \cos\phi_{ol} + 2\epsilon I_{ol} && (4.10)\\ &= \sqrt{\frac{I_{ol}}{N_0}}(X_{s,\phi_{ol}} + 2\epsilon\sqrt{I_{ol}N_0}) && (4.11)\end{aligned}$$

This expression allows us to quantify the required precision concerning the balance of the homodyne detection. The imbalance becomes negligible when $\epsilon \ll \frac{1}{2\sqrt{I_{ol}}}$, i.e. $\epsilon \ll 5 \times 10^{-5}$ for local oscillator intensities of about 10^8 photons per pulse.

In quantum optics, the losses of the homodyne detection correspond to a coupling of the signal mode with the void on a beam splitter of transmission η. Therefore, losses do not only attenuate the signal but also add some noise. As explained in chapter 3, three main contributions to the homodyne detection losses can be identified: optical losses η_{opt}, the quantum efficiency of the photodetectors η_{phot} and imperfect mode matching η_{mod}. The output signal of the homodyne detection when taking into account the losses reads:

$$\Delta\hat{I} = \sqrt{\eta_{opt}\eta_{phot}\frac{I_{ol}}{N_0}}(\sqrt{\eta_{opt}\eta_{phot}\eta_{mod}^2}X_{s,\phi_{ol}} + \sqrt{1 - \eta_{opt}\eta_{phot}\eta_{mod}^2}X_{0,imperf}) \tag{4.12}$$

where $X_{0,imperf}$ is a void mode that regroups all the void modes introduced by the imperfections.

Finally, when considering a noisy local oscillator of intensity $I_{ol} + \delta I_{ol}$, one can show that the homodyne measurement becomes proportional to $\sqrt{I_{ol} + \delta I_{ol}}X_{s,ol}$. One can therefore neglect these fluctuations if $\delta I_{ol} \ll I_{ol}$.

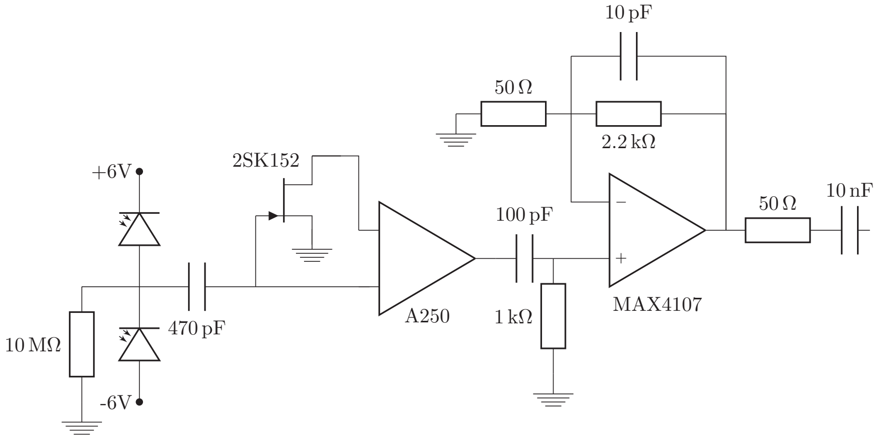


Figure 4.9: Schematics of the homodyne detection electronics. The photocurrents difference at the output of the photodiodes goes through a high pass filter composed of a 470 pF capacitance connected to the ground through a 10 MΩ resistivity. Then an Amptek A250 amplifier and its associated transistor FET 2SK152 constitute a first amplification stage specifically designed for weak currents low noise amplification. Since the decrease after each pulse is very slow, a derivative stage allows us to reduce it to 100 ns. Finally, another amplifying circuit using a MAX4107 amplifier allows us to achieve a higher level of amplification.

4.4.3 Electronics of the Homodyne Detection

Figure 4.9 represents the electronics of our homodyne detection. The photocurrents difference at the output of the photodiodes goes through a high pass filter composed of a 470 pF capacitance connected to the ground through a 10 MΩ resistivity. Then an Amptek A250 amplifier and its associated transistor FET 2SK152 constitute a first amplification stage specifically designed for weak currents low noise amplification. Since the decrease after each pulse is very slow, a derivative stage allows us to reduce it to 100 ns. Finally, another amplifying circuit using a MAX4107 amplifier allows us to achieve a higher level of amplification.

4.5 Time and Polarization Multiplexing

In the theoretical description of the GG02 [50] protocol, the measurement process, i.e. homodyne measurement of the quadratures of the quantum signal, is not described from an experimental point of view. There is no mention of the local oscillator and therefore to the need of sending it from Alice to Bob through the quantum channel. As presented in the previous section, in order to implement a homodyne detection, a classical signal coherent with the quantum signal is required. While this task is easy to perform locally by splitting the output of a laser beam into a weak beam and a strong beam before making them interfere on a balanced beam splitter, it becomes more challenging from a quantum communication point of view when the weak signal has to be sent through a quantum channel and undergoes both losses and noise.

As previously demonstrated in [83, 44], we chose to send the local oscillator together with the quantum signal through the quantum channel. When using a reasonably low time delay (a few hundreds of ns in our experiment) between these signals, they are submitted to almost the same fluctuations of the quantum channel and remain coherent after traveling through long distances. In addition to time multiplexing, we use polarization multiplexing: the local oscillator is polarized along the fast axis of our PM fibers while the signal propagates along the slow axis. The combination of these two methods is really useful: polarization multiplexing allows for an easy demultiplexing and time multiplexing solves the problem of leakage from the local oscillator into the signal.

In practice, time and polarization multiplexing is done on Alice's side using a *Polarization Beam Splitter* (PBS) together with a delay line and a Faraday mirror. Demultiplexing requires two stages on Bob's side. First, a *Dynamic Polarization Controller* (DPC) is used to find an optimal polarization state using the homodyne detection statistics. Second, another PBS together with a delay line and a Faraday mirror complete the demultiplexing.

4.6 Optical Component Characteristics Summary

Table 4.2 gives a summary of the optical losses and some other important characteristics of the different components used in our experimental setup. It is worth noting that losses on Alice's side do not have the same impact on the performances of the system as losses on Bob's side.

This is because the calibration of Alice's system is done at the output of the device. Consequently, losses on Alice's side do not have any impact on the theoretical secret key rate. The only limitation due to Alice's losses may be practical: for a given transmission channel, the intensity of both the local oscillator and the quantum signal at the output of Alice must be compatible with the establishment of the secret key. On the one hand, if the local oscillator power is not compatible with the homodyne detection linear regime, it is likely that no secret key will be obtained. On the other hand, if Alice's quantum signal variance cannot be adjusted to obtain a SNR on Bob's side that is compatible with the thresholds of the available error-correcting codes, no secret key can be obtained.

As regards Bob's losses one can distinguish two cases concerning the security model:

- the realistic mode: in this case the losses on Bob's signal path are assumed not to be due to the eavesdropper and do not impact strongly the theoretical secret key rate.
- the paranoid mode: Bob's signal path losses are dealt with in the same way as the quantum channel losses, which decreases the theoretical secret key rate.

4.7 Acquisition and Control Cards

As demonstrated in chapter 3, relatively high bit depths are required to drive the EOMs according to the Gaussian modulation of the GG02 protocol. Furthermore, we require two output channels on Alice's side for both amplitude and phase modulation and one input channel for the feedback on the amplitude modulation using a photodiode with an amplifier circuit. On Bob's side, we use two input channels, the homodyne detection and a signal proportional to the local oscillator power. Depending whether one of the

Components	Losses (dB)	Fiber	Comments
Laser Diode	-	PMF	30 mW power
Beam Splitter	0.3-0.5	PMF	99/1 to 50/50
Variable Attenuator	0.3-0.5	PMF	Up to 55 dB
Amplitude Modulator	3-5	PMF	30-50 dB
Phase Modulator	2-3	PMF	-
Polarization Beam Splitter	0.3-0.5	PMF	25-30 dB crosstalk
Polarization Controller	0.2-0.3	PMF	20 dB crosstalk
Photodiode	-	SMF	1 A/W efficiency
Faraday Mirror	0.2-0.4	SMF	-

Table 4.2: Components used in our experimental setup with their respective insertion losses excluding connection losses at 1550nm.

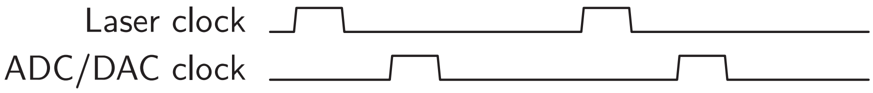


Figure 4.10: Alice's optical device clock signals. The laser clock is delayed in order to get a DAC/ADC clock allowing us to measure Alice's amplitude and set the amplitude and phase modulators at the same time.

countermeasures proposed in Chapter 5 is implemented, we use one or two output channels: one is always dedicated to the phase modulator allowing us to select any quadrature of the field, another might be used to drive either an amplitude modulator or an optical switch. We use National Instruments *Peripheral Component Interconnect* (PCI) 6110/6111/6115 cards. Any of these cards feature at least two input and two output 12 bits precision channels at 2.5 mega samples per second per channel.

These cards can be driven with an external trigger. On Alice's side, our trigger is generated by the laser card with a delay that allows us to use the same clock signal to set the states of the modulators and to perform a signal measurement on the photodiode. Figure 4.10 gives a timing diagram of Alice's optical device and Figure 4.11 shows the temporal relationship between the modulated and measured values of a clock cycle.

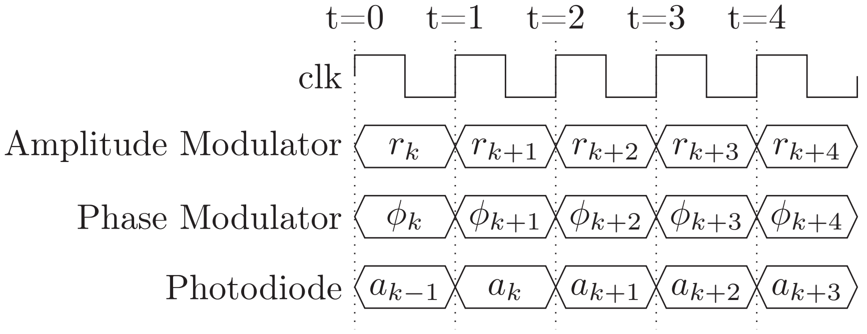


Figure 4.11: Alice's input and output data. Since a single clock is used to perform measurements on Alice's photodiode and to set Alice's modulators, the data sent to the acquisition card to set the modulators correspond to the pulse that is going to be measured at the next clock cycle.

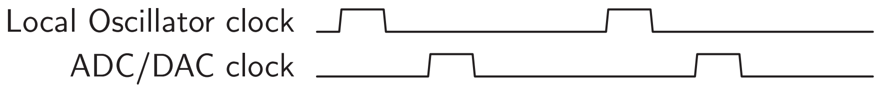


Figure 4.12: Bob's device clock signals. A clock is generated from the local oscillator signal. Then it is delayed in order to get a DAC/ADC clock allowing us to perform a quadrature measurement with the homodyne detection and set the phase modulator for the next pulse at the same time.

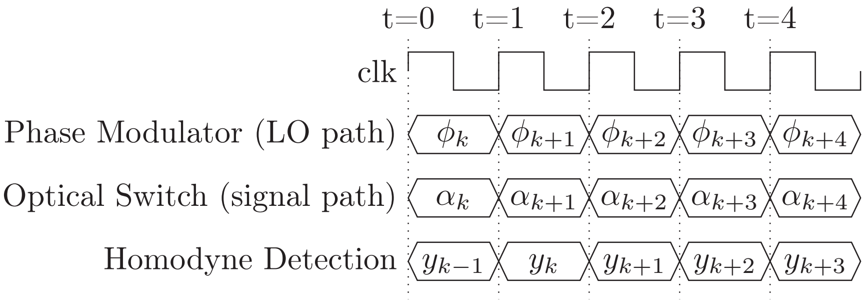


Figure 4.13: Bob's input and output data. Since a single clock is used to perform measurements on Bob's homodyne measurement and to set Bob's modulator, the data sent to the acquisition card to set the modulator correspond to the pulse that is going to be measured at the next clock cycle.

In the same way, on Bob's side, we generate a trigger out of the local oscillator signal at the input of Bob's system using a photodiode and an amplifier circuit. This trigger is then delayed and used to set the phase modulator (and the amplitude modulator or optical switch if the countermeasure proposed in Chapter 5 is implemented) and to perform the homodyne measurement. Figure 4.12 gives a timing diagram of Bob's optical device and Figure 4.13 shows the temporal relationship between the modulated and measured values of a clock cycle.

We also use a National Instruments PCI 6704 static control card on Bob's side in order to set the dynamic polarization controller four voltages. An optimal polarization state is found as a calibration step in an asynchronous way with respect to the quantum protocol.

4.8 Random Numbers

Random numbers are required at different stages of the protocol and on both Alice's and Bob's sides. The limiting factor as regards random numbers is of course the generation of the bivariate Gaussian modulation, which is performed on Alice's side. All the other random numbers can be drawn on Bob's side which can be interesting if the random numbers source has a limited throughput. The other steps that require random numbers are the following:

- Modulation: since our acquisition cards have only 12 bits of precision, no more than 24 random bits are required for modulating both the phase and the amplitude.
- Quadratures choice: in the GG02 protocol, Bob measures at random one of the two orthogonal quadratures X and P. This requires one bit

of randomness per pulse or more generally $h(p) = -p \log_2 p - (1 - p) \log_2 1 - p$ if they measure X on a fraction p of the pulses and P on a fraction $1 - p$ of the pulses.

- Sifting: in order to estimate the parameters that are necessary to compute the amount of secret key they can extract from their raw data, Alice and Bob must reveal at random a fraction $p \in \{0, 1\}$ of their correlated data. The amount of randomness required to perform this task is $h(p) = -p \log_2 p - (1 - p) \log_2 1 - p$.
- Privacy amplification: once Alice an Bob share a common corrected bit string of length n and know they can extract k bits of secret key from this string, they need to perform a privacy amplification step whose output is the final secret key. This is done by drawing a random $n \times k$ Toeplitz matrix with coefficients in GF(2), the finite field of two elements, and applying this matrix to the corrected bit string. A generic $n \times k$ Toeplitz matrix is described by $n+k-1$ coefficients. This implies that this step requires $n + k - 1$ random bits for a corrected string of length n. Since $k \leq n$ and assuming that $n \geq 1$, no more than two random bits per pulse are required for this step.
- Multidimensional reconciliation (optional): as explained in chapter 6, error correction with Gaussian modulation and Gaussian noise is hard to perform efficiently in the high noise regime, i.e. at long distances. This is why a multidimensional reconciliation protocol may be used at long distances. This allows us to deal with a modulation that is closed to a binary modulation and to benefit from efficient error-correcting codes that are available on the BIAWGNC. However, this procedure comes with an additional cost of drawing one random bit per pulse.
- Real time shot noise measurement (optional): in chapter 5, we detail a potential loophole in a CVQKD system, linked to the manipulation of the local oscillator during a QKD run and to the shot noise estimation procedure that is usually performed before the QKD run in a secure lab. We proposed a set of techniques allowing to deal with this potential attack. These techniques consist in measuring the shot noise in real time. One possible implementation is the introduction of an optical switch on Bob's signal path. This switch is used to define two set of pulses, one set being used for the shot noise measurement ant the other set for the usual key generation procedure. In the same manner as for the sifting procedure, Bob must attenuate at random a fraction $p \in 0, 1$ of their correlated data. The amount of required randomness for this task is again $h(p)$.

Table 4.3 summarizes the bounds on the amount of randomness that is required for our experimental setup:

Let us look at the bivariate Gaussian modulation into more detail. Its density probability is:

$$f(x, y) = \frac{1}{2\pi\sigma^2} e^{-\frac{x^2+y^2}{2\sigma^2}} \tag{4.13}$$

Since in our experiment, we can only act on the amplitude and the phase of the light, we are interested in their probability densities that can be obtained through a change of variables:

$$g(r) = \frac{r}{\sigma^2} e^{-\frac{r^2}{2\sigma^2}} \tag{4.14}$$

Protocol Step	Alice	Bob
Modulation	24	0
Quadratures Choice	0	1
Sifting	0	1
Privacy Amplification	0	2
Multidimensional Protocol	0	1
Real Time Shot Noise Measurement	0	1
Total	24	6

Table 4.3: We assumed $p = 0.5$ for the fraction of pulses used for the quadratures choice, the sifting and the real time shot noise measurement. This corresponds to the worst case as regards random numbers consumption.

and

$$h(\phi) = \frac{1}{2\pi} \tag{4.15}$$

where $r = \sqrt{x^2 + y^2}$ is the amplitude of the field and ϕ is the phase of the field. The phase has a uniform distribution in $[0, 2\pi]$ and therefore can be drawn directly using the uniform random numbers output by random numbers generator. However, drawing the amplitude distribution is more challenging. On the one hand, this distribution is unbounded, on the other hand, a method allowing to generate this distribution out of the uniform bits output by the random number generator is required.

A common method consists in generating a bivariate Gaussian distribution and use a change of variable to get the corresponding polar coordinates. The bivariate Gaussian distribution can be drawn using Box Muller method that generates two Gaussian random variables out of two uniform random variables. However, since each uniform random variable output by the random numbers generator corresponds to 16 bits of randomness, Box Muller method requires 32 bits of randomness per pulse. At a frequency of 1 MHz and using about 15% of synchronization pulses, this corresponds to about 27.2 Mb/s only for the Gaussian modulation. Such a rate is not possible with well known commercial products such as Quantis from IdQuantique [2]. We used an entropic coding method that allows us to use exactly the amount of randomness that is necessary to generate a random distribution. It is called range coding.

Furthermore, for frequencies above 1 MHz, we chose to use a Bull Mountain RNG from Intel. It includes a 3 Gb/s physical source and a post-processing stage. They present the advantage to be available on standard Intel Ivy bridge x86 CPUs and are FIPS SP800/90, FIPS-140-3 compliant. One could wonder why a post-processing stage is implemented on a device that includes a physical source of randomness. The reason for that is that physical devices can fail. Figures 4.14 and 4.15 give the bytes statistics over a 1 Gb dataset for Salsa *Pseudo-random Numbers Generator* (PRNG) and for an aged physical RNG. One can see that the deviations from the uniform distribution are far more important with the aged physical RNG than with the PRNG. Such a failure would not be noticed with a proper post-processing stage.

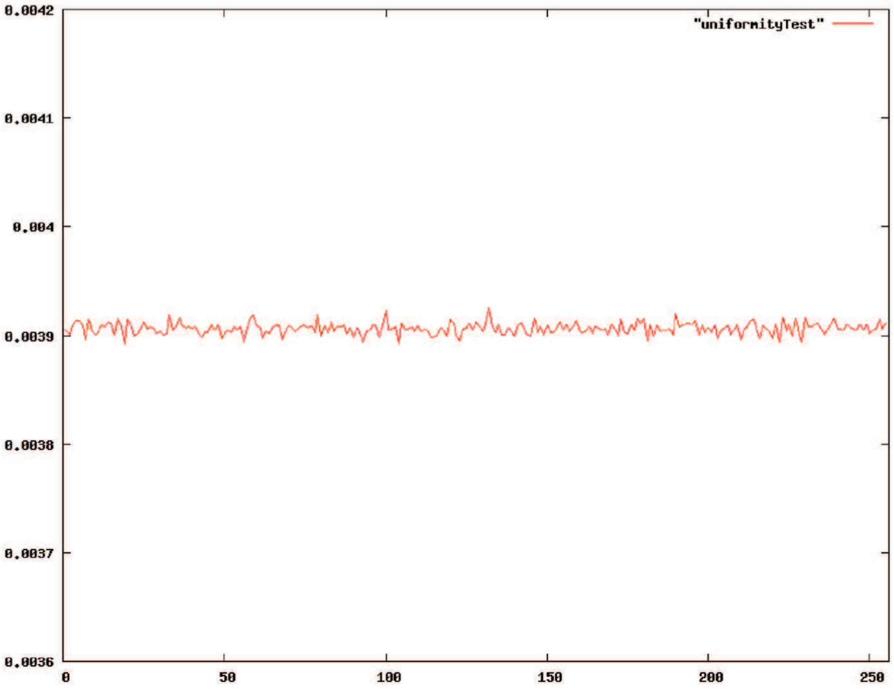


Figure 4.14: Bytes statistics with Salsa PRNG for a 1 Gb dataset.

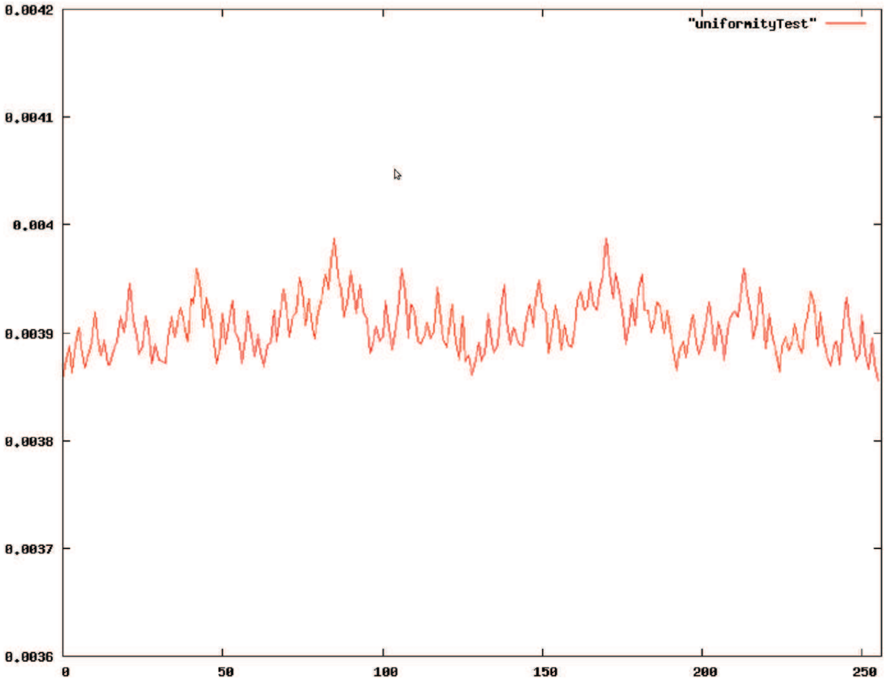


Figure 4.15: Bytes statistics with an aged physical RNG for 1 Gb dataset.

4.9 Computing Power

We end this chapter by emphasizing on the need for important computing resources for CVQKD post-processing. This is because the error-correction step needs to be performed close to Shannon's bound in order to get a positive secret key rate. In addition to that, current iterative decoding algorithms fail to converge quickly when operating close to a LDPC code threshold. We could solve this problem in chapter 8 using GPUs. We also proposed to use polar codes that feature efficient recursive decoding on modern CPUs.

Chapter 5

Preventing Calibration Attacks on the Local Oscillator in Continuous-Variable Quantum Key Distribution

Contents

5.1 Theoretical Security vs Practical Attacks 85
5.2 Security assumptions and calibration techniques 86
5.3 Description of the local oscillator calibration attack 88
5.4 Analysis of the excess noise 90
5.5 A quantitative example 92
5.6 Countermeasure: real-time shot noise measurement techniques 92
5.7 Conclusion 94

Establishing an information-theoretic secret key between two parties using a quantum key distribution (QKD) system is only possible when an accurate characterization of the quantum channel and proper device calibration routines are combined. Indeed, security loopholes due to inappropriate calibration routines have been shown for discrete-variable QKD. In this chapter, we propose and provide experimental evidence of an attack targeting the local oscillator calibration routine of a continuous-variable QKD system. The attack consists in manipulating the classical local oscillator pulses during the QKD run in order to modify the clock pulses used at the detection stage. This allows the eavesdropper to bias the shot noise estimation usually performed using a calibrated relationship. This loophole can be used to perform successfully an intercept-resend attack. We characterize the loophole and suggest possible countermeasures.

5.1 Theoretical Security vs Practical Attacks

The two communicating parties of a quantum key distribution (QKD) protocol [120], Alice and Bob, can in principle share an information-theoretic secret key after the exchange of a large number of quantum signals through a physical channel, known as quantum channel, which is subject to eavesdropping, and additional information sent on a public but authenticated classical channel. After Alice and Bob have agreed on a set of non-commuting quantum operators, they can safely encode the key into these variables: any eavesdropping attempt disturbs the transmitted quantum states and is discovered after random sampling of a fraction of Alice and Bob's correlated data. However, deviations of the practical implementation of a QKD protocol from the underlying theoretical model can be exploited by an eavesdropper.

In most commonly used QKD systems, the key information is encoded on discrete variables, such as the polarization of a single photon, and thus specific components for single-photon detection are required. Exploiting imperfections of such devices has led to powerful attacks, namely the time-shift attack [159], the phase-remapping attack [155], and the remote control of single-photon detectors using tailored bright illumination [86]. Other attacks proposed against discrete-variable QKD systems include Trojan horse [47], device calibration [58], and wavelength dependent beamsplitter [80] attacks. The latter have also been adapted to continuous-variable QKD (CVQKD), where the key information is encoded on continuous variables [148], such as the quadratures of coherent states [50]. In CVQKD systems, measurements are performed using standard coherent detection techniques, in particular homodyne detection when the protocol requires the measurement of a single quadrature of the electromagnetic field or heterodyne detection when both quadratures need to be measured. Wavelength dependent beamsplitter attacks targeting CVQKD schemes using heterodyne detection have recently been studied [56, 87]. Finally, attacks specific to CVQKD [38, 88] typically involve manipulation of the power of the local oscillator, which is the phase reference classical signal required for the coherent detection and is usually sent from Alice to Bob together with the quantum signal [64].

Here, we consider device calibration attacks against continuous-variable QKD. These attacks arise from a subtle link between the local oscillator calibration procedure and the clock generation procedure in practical CVQKD setups using Gaussian modulation of coherent states and homodyne detection. We show that combining this security loophole with intercept-resend attacks can compromise the security of continuous-variable QKD in the absence of appropriate countermeasures. With recent advances in this technology, which allows for long-distance key distribution using standard telecommunication components and with strong security guarantees [64], assuring the practical security of all aspects of the implementation, and specifically of the ubiquitous calibration procedure, is of utmost importance.

5.2 Security assumptions and calibration techniques

A standard assumption when designing and implementing a CVQKD system is that the local oscillator cannot be manipulated by an eavesdropper. This cannot, however, be verified in practice since the local oscillator is a classical, and therefore intense, signal, and thus the no-cloning theorem does not apply. This means that the local oscillator can be measured and regenerated, or directly amplified, without adding any additional disturbance.

Current security proofs do not explicitly take into account the local oscillator, which is not required at a theoretical level to define the exchanged states and the performed measurements [99, 46, 74]. In particular, all the

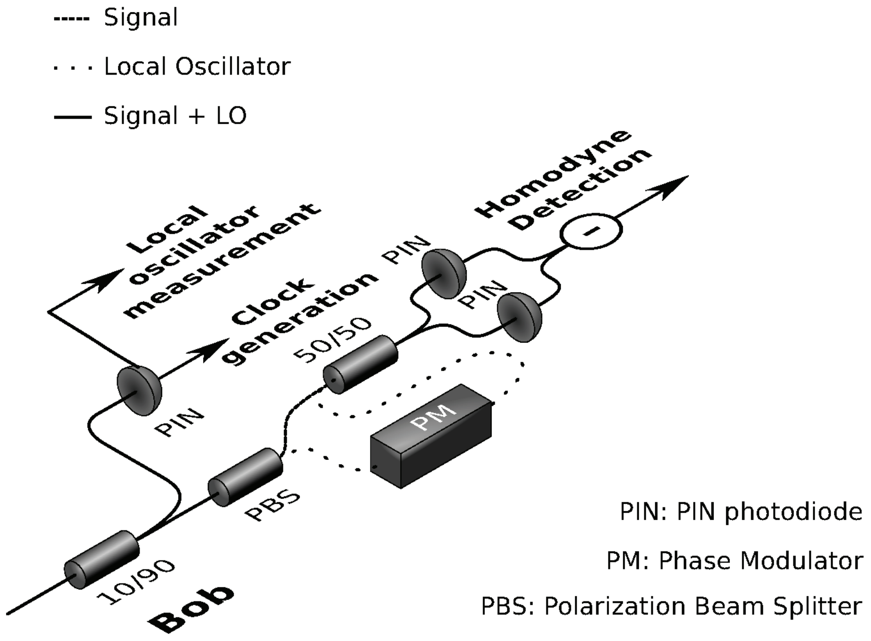


Figure 5.1: Local oscillator experimental measurement procedure. Here a PIN photodiode is used for two purposes: generating a clock on Bob's side and generating a signal proportional to the local oscillator power.

quantities that are used in the calculation of the secret key generation rate are expressed in shot noise units. Knowledge of the shot noise is therefore required. In principle, the shot noise variance can be evaluated using a balanced homodyne detector, as the variance of the interference between the local oscillator and the vacuum mode. This measurement method incurs some statistical uncertainty due to the finite size of the data, as was studied in [63]. Alternatively, the linear relationship between the variance of this measurement and the input power of the local oscillator signal on the homodyne detector can be used to estimate the shot noise during the quantum transmission, provided that the local oscillator power is known.

A standard calibration technique, used for instance in [61], consists in establishing in a secure laboratory, before the QKD run, the aforementioned linear relationship between the shot noise and the local oscillator power. During the QKD run, the local oscillator power is measured either with a power meter or with a photodiode followed by an integration circuit, at the input of Bob's site. In either case, a signal proportional to the intensity of the local oscillator over a time period that should be equal to the homodyne detection integration window is available. The previously established linear relationship can then be used to deduce the shot noise level used for the secret key rate calculation. This approach, however, has two shortcomings. First, it is not possible to trust the power of the signal entering Bob's device, since an eavesdropper can easily add another classical signal (for instance, at a different wavelength) into the quantum channel. Second, in a practical CVQKD system, the local oscillator is not only used as an intense signal coherent with the weak quantum signal and therefore allowing us to measure its quadratures; it is also used to generate the clock signal that is necessary to perform the measurements, as shown in Fig. 5.1. Therefore, the local oscillator signal can be suitably modified by an eavesdropper such that the

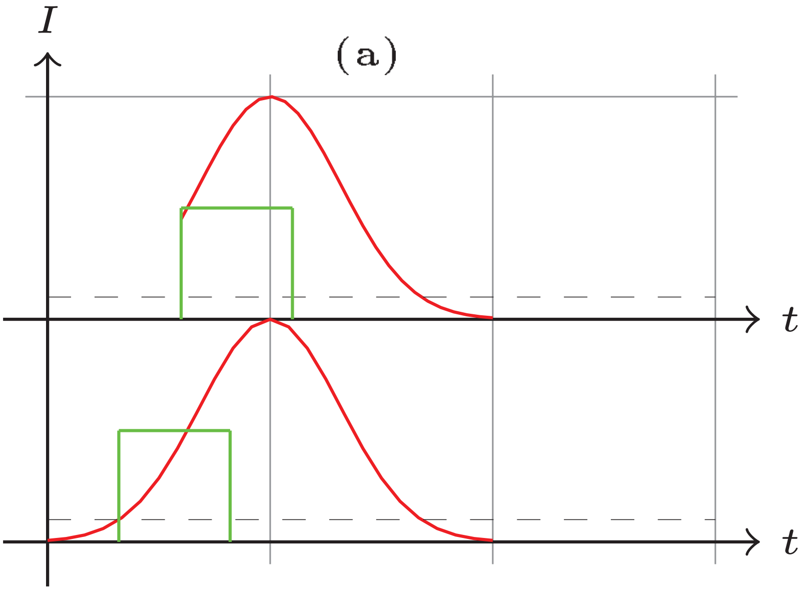


Figure 5.2: Profile of the trigger signal generated at Bob's site depending on the shape of the local oscillator pulse.

trigger signal generated by the clock circuit is also altered.

In the following, we describe how the interplay between the local oscillator calibration and the clock generation procedures can be exploited to perform an eavesdropping attack.

5.3 Description of the local oscillator calibration attack

The basic principle of the attack is illustrated in Figs. 5.2, 5.3 and 5.4. In particular, as shown in Fig. 5.2, the clock circuit is usually designed to output a rising trigger signal when the intensity entering the photodiode is above a certain threshold. Subsequently, this trigger is delayed such that the value of the signal at the output of the homodyne detection is maximized. A potential attack for an eavesdropper consists in attenuating the beginning of the local oscillator pulse, which induces a delay of the trigger used for the measurements. Note that this was also suggested in [21] as a potential source of loophole. Figure 5.4 shows experimental results illustrating the relationship between the variance of the measurement on the homodyne detection and the local oscillator power for different trigger signals. These results were obtained using the setup of Fig. 5.1, which corresponds to a simplified version of Bob's setup employed for long-distance continuous-variable QKD using Gaussian modulation of coherent states [64]. The experiment shows that a delayed trigger results in a decrease of the detection response slope. This is because a homodyne measurement is usually performed by integrating the differential photocurrent during a period Δ using an integrator circuit: after this period Δ, the capacitor discharges exponentially, which implies that the maximum measurement variance is obtained when the trigger coincides with the end of the period Δ, as shown in Fig. 5.3. As

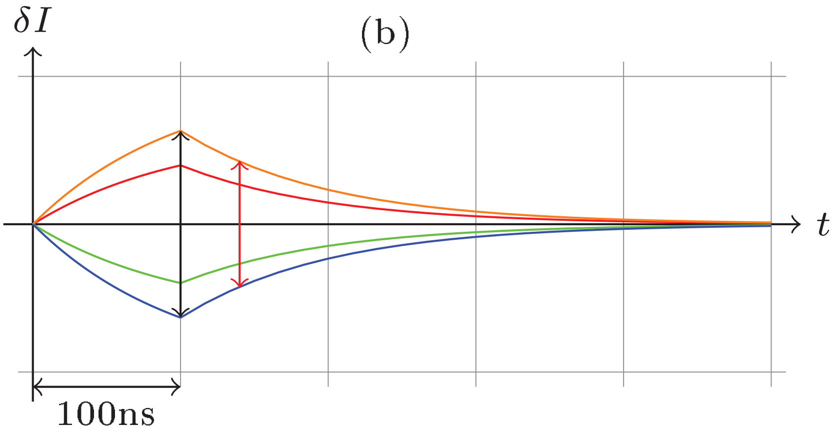


Figure 5.3: Differential signal obtained by the homodyne detector for several modulated quadratures. After an integration period of $\Delta = 100$ ns, the capacitor discharges exponentially. Depending on the time of the measurement, the variance of the measurement of the homodyne detection is different.

a result, if Alice and Bob use the previously calibrated relationship to evaluate the shot noise based on the measured local oscillator power, they will use a false value, if the trigger signal has been delayed during the QKD run. In particular, they will overestimate the value of the shot noise, and consequently underestimate the excess noise present in the setup. This creates an important loophole in the security of the implementation.

Based on this loophole, we propose the following practical attack. It is important to note that this attack can be implemented with current technology, without any need, for instance, for a quantum memory.

- The eavesdropper, Eve, introduces a phase-independent attenuator in the quantum channel and applies an attenuation factor α $(0 \leq \alpha \leq 1)$ on a fraction ν $(0 \leq \nu \leq 1)$ of the local oscillator pulses in order to modify their shape. The trigger used to perform the homodyne measurement relative to these pulses is delayed by δ.
- Eve introduces a beam splitter in the quantum channel and for a fraction μ $(0 \leq \mu \leq 1)$ of the input signal pulses she measures both quadratures and prepares the appropriate quantum state, whereas for a fraction $1 - \mu$ of the input signal pulses she just eavesdrops using the beamsplitter. This so called partial intercept-resend attack was implemented experimentally in [82].

When Eve increases the fraction μ of signal pulses over which she performs an intercept-resend attack, she introduces more noise, which lowers the amount of secret key that Alice and Bob can extract from the quantum transmission. The fraction ν of local oscillator pulses attenuated by Eve and the attenuation factor α are two free parameters that play the same role: they scale the variance of the measurements made by Bob while his shot noise estimation remains unchanged. This leads Alice and Bob to conclude that no noise has been introduced in the quantum channel and hence they establish a key without detecting the presence of Eve.

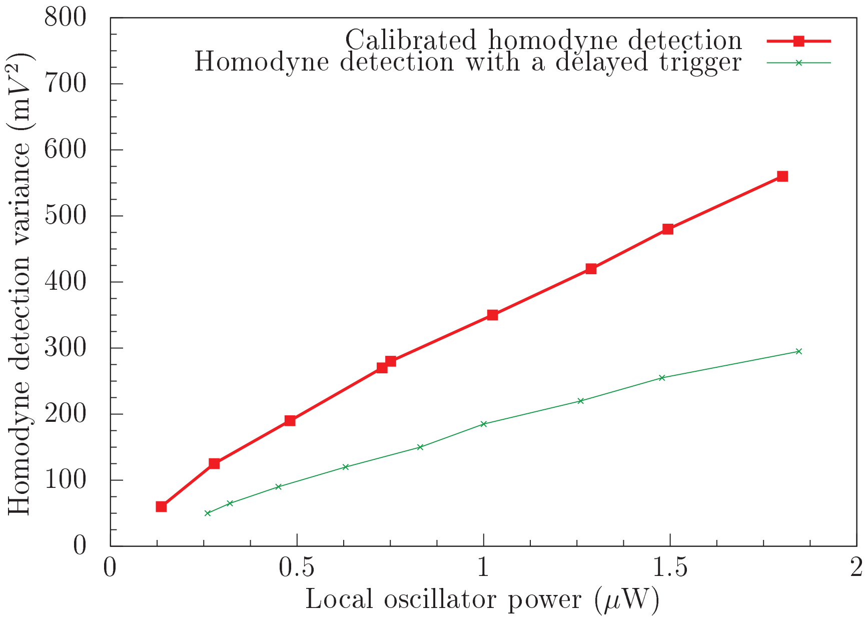


Figure 5.4: In red, the calibrated linear relationship between the variance of the homodyne detection measurements and the local oscillator power. In green, the linear relationship we obtain when delaying the trigger of the homodyne detection by 10 ns.

5.4 Analysis of the excess noise

To assess the impact of our attack on the security of continuous-variable QKD, we detail the parameter estimation procedure that is necessary for the derivation of the secret key and how this procedure is altered when the attack is implemented. In a practical CVQKD setup, Alice and Bob estimate the quantities required to compute the secret key rate by sampling $m = N - n$ couples of correlated variables $(x_i, y_i)_{i=1...m}$, where N is the total number of quantum signals sent through the quantum channel and n is the number of signals used for the key establishment. Since for CVQKD it is sufficient to estimate the covariance matrix of the state shared by Alice and Bob, the only parameters that need to be estimated are the variance on Alice's and Bob's sites, $\langle x^2\rangle$ and $\langle y^2\rangle$, respectively, and the covariance between Alice and Bob, namely $\langle xy\rangle$ (assuming here that x and y are centered variables, that is, that $\langle x\rangle = \langle y\rangle = 0$). Then, the following estimators are used during the QKD run:

$$\langle x^2\rangle = V_A, \langle xy\rangle = \sqrt{\eta T}V_A \tag{5.1}$$

$$\langle y^2\rangle = \eta T V_A + N_0 + \eta T\xi + v_{\text{el}} \tag{5.2}$$

In the above expressions, T is the quantum channel transmittance, V_A is the modulation variance, ξ is the excess noise, N_0 is the shot noise, η is the efficiency of the homodyne detector, and v_{el} is the electronic noise (all expressed in their respective units).

Here we assume that the electronic noise does not change between the QKD run and the calibration procedure. In theory, an eavesdropper may also try to modify the value of the electronic noise, for example by changing the temperature operating conditions of the electronic circuit of the homodyne detection between the calibration and the QKD run. However, the impact of such an attack would be less significant since the value of the electronic noise is typically between 10 and 20 dB below the shot noise.

In order to compute confidence intervals for these parameters, we consider a normal model for Alice and Bob's correlated variables $(x_i, y_i)_{i=1\dots m}$, namely $y = tx + z$, where $t = \sqrt{\eta T} \in \mathbb{R}$, and z follows a centered normal distribution with unknown variance $\sigma^2 = N_0 + \eta T\xi + v_{\text{el}}$. Note that this normal model is an assumption justified in practice but not by current proof techniques, which show that the Gaussian assumption is valid once the covariance matrix is known [74].

Maximum-Likelihood estimators $\hat{t}$, $\hat{\sigma}^2$ and $\hat{V}_A$ are known for the normal linear model:

$$\hat{t} = \frac{\sum_{i=1}^m x_i y_i}{\sum_{i=1}^m x_i^2}, \hat{\sigma}^2 = \frac{1}{m}\sum_{i=1}^m (y_i - \hat{t}x_i)^2, \hat{V}_A = \frac{1}{m}\sum_{i=1}^m x_i^2$$

These are independent estimators with distributions:

$$\hat{t} \sim \mathcal{N}\left(t, \frac{\sigma^2}{\sum_{i=1}^m x_i^2}\right), \frac{m\hat{\sigma}^2}{\sigma^2}, \frac{m\hat{V}_A}{V_A} \sim \chi^2(m-1),$$

where t, σ^2 and V_A are the true values of the parameters. Using the previous estimators and their confidence intervals together with the shot noise value from the calibration N_0', it is then possible to estimate $T = \hat{t}^2/\eta$ and $\xi = (\hat{\sigma}^2 - N_0' - v_{\text{el}})/\hat{t}^2$.

If the eavesdropper can change the slope of the homodyne detection response as previously explained, the equality $N_0' = N_0$ is not verified. This leads to the following estimation for the excess noise when a calibration attack occurs:

$$\hat{\xi}_{\text{calib}} = \hat{\xi} + \frac{N_0' - N_0}{\hat{t}^2}, \tag{5.3}$$

where $\hat{\xi}$ is the estimate without the attack. In order to compute a secret key rate, the excess noise must be expressed in shot noise units, hence we have:

$$\frac{\hat{\xi}_{\text{calib}}}{N_0'} = \frac{N_0}{N_0'}\left[\frac{\hat{\xi}}{N_0} + \frac{1}{\hat{t}^2}\left(1 - \frac{N_0'}{N_0}\right)\right] \tag{5.4}$$

Next, we consider the excess noise introduced by a partial intercept-resend (PIR) attack alone. According to the analysis of [82], in this case, the probability distribution of Bob's measurements is the weighted sum of two Gaussian distributions with a weight of μ for the intercepted and resent data and a weight of $1 - \mu$ for the transmitted data:

$$\langle y^2 \rangle_{\text{IR}} = \eta T(V_A + 2N_0) + N_0 + \eta T\xi + v_{\text{el}} \tag{5.5}$$

$$\langle y^2 \rangle_{\text{BS}} = \eta T V_A + N_0 + \eta T\xi + v_{\text{el}}, \tag{5.6}$$

where ξ is the technical excess noise of the system. The excess noise introduced by this attack can then be computed as:

$$\hat{\xi}^{\text{PIR}} = \hat{\xi} + 2\mu N_0 \tag{5.7}$$

In practice, when a full intercept-resend attack is implemented ($\mu = 1$), the excess noise is dominated by the second term in the above expression due to the noise introduced by Eve's measurements.

If, additionally, the eavesdropper performs the local oscillator calibration attack, then the excess noise introduced by the partial intercept-resend attack is computed, in shot noise units, as:

$$\frac{\hat{\xi}^{\mathrm{PIR}}_{\mathrm{calib}}}{N_0'} = \frac{N_0}{N_0'}\left[\frac{\hat{\xi}^{\mathrm{PIR}}}{N_0} + \frac{1}{\hat{t}^2}\left(1 - \frac{N_0'}{N_0}\right)\right] \tag{5.8}$$

5.5 A quantitative example

When the eavesdropper implements a full intercept-resend attack ($\mu = 1$), and with a typical value of $\xi/N_0 = 0.1$, we find from Eq. (5.7) that the noise introduced by the attack is $\xi^{\mathrm{PIR}}/N_0 = 2.1$. This noise value is above the entanglement breaking limit, hence no secret key can be exchanged, independently of the communication distance. However, if Eve implements additionally the local oscillator calibration attack, then Alice and Bob will estimate the excess noise using Eq. (5.8). For example, for a transmission $T = 0.5$ and a homodyne detection efficiency $\eta = 0.5$, we find:

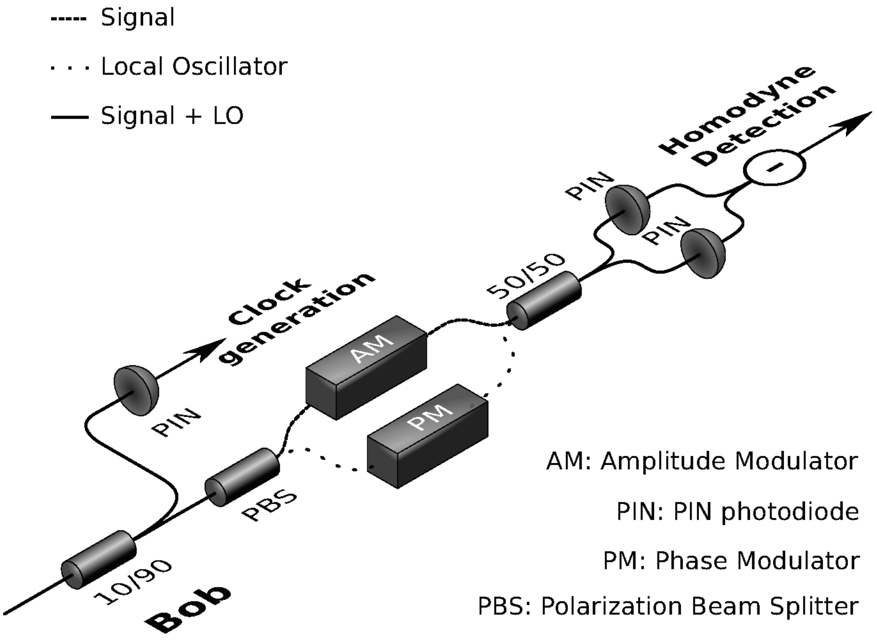
$$\frac{\hat{\xi}^{\mathrm{PIR}}_{\mathrm{calib}}}{N_0'} = \frac{N_0}{N_0'}\left[2.1 + \frac{1}{0.5 \times 0.5}\left(1 - \frac{N_0'}{N_0}\right)\right] \tag{5.9}$$

Then, for $N_0'/N_0 \approx 1.5$, which is a realistic value as shown in Fig. 5.4, the excess noise estimated by Alice and Bob will be close to zero, hence they will conclude they can share a secret key. The security of the protocol is thus entirely compromised.

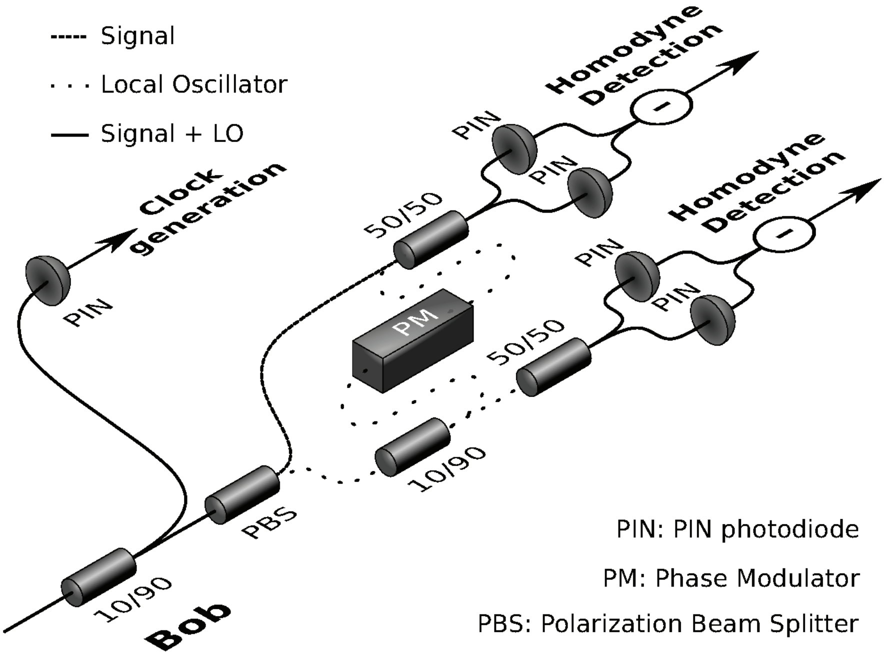
5.6 Countermeasure: real-time shot noise measurement techniques

In practice, it is possible to show that a calibrated linear relationship between the shot noise level and local oscillator power cannot be used in the presence of an eavesdropper (see Appendix for a detailed analysis). Therefore, a countermeasure for the proposed attack consists in devising techniques allowing us to measure the shot noise in real time. One such technique consists in applying a strong attenuation on Bob's signal path to a randomly chosen set of pulses, using, for instance, an optical switch or an amplitude modulator. Alternatively, an additional homodyne detector dedicated to the real-time shot noise measurement can be used: a beam splitter is introduced in Bob's local oscillator path and the relative sensitivity of the two homodyne detectors is calibrated. A schematic representation of the two techniques is shown in Fig. 5.5. In both methods, two noise measurements on two sets of pulses allow us to extract the shot noise and the signal noise by inverting a linear system. To the best of our knowledge, none of these techniques has been proposed or implemented in CVQKD.

In Fig. 5.6, we compare the theoretical secret key rates against collective attacks [99, 46] for a CVQKD system that does not implement any countermeasure against the local oscillator calibration attack we proposed and for a system that uses the countermeasure of Fig. 5.5(a) with an optical switch on Bob's signal path. In the latter case, the impact of the countermeasure on the secret key rate is twofold. First, the number of pulses that can be used to extract a secret key is diminished by the fraction of pulses chosen at random to compute an estimate of the shot noise; in our numerical analysis,



(a)



(b)

Figure 5.5: Real-time shot noise measurement procedures protecting a CVQKD system against a local oscillator calibration attack. (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.

we chose to discard 10% of the pulses. Second, the efficiency of Bob's measurement apparatus η is reduced because of the 2.7 dB losses introduced by the optical switch. For realistic values of all the parameters, we find that the maximum secure distance drops from 80 km to 70 km when implementing this countermeasure.

5.7 Conclusion

We proposed a powerful and realistic calibration attack for continuous-variable QKD systems, by which an eavesdropper can make Alice and Bob negotiate a key even for an introduced noise that is above the entanglement breaking limit at which no secret key can be exchanged at any distance. Preventing this attack involves real-time measurement of the shot noise, which is possible but not trivial. Given the relevance of CVQKD technology for high-performance secure communications, this work highlights the importance of rigorously testing the practical security of current implementations.

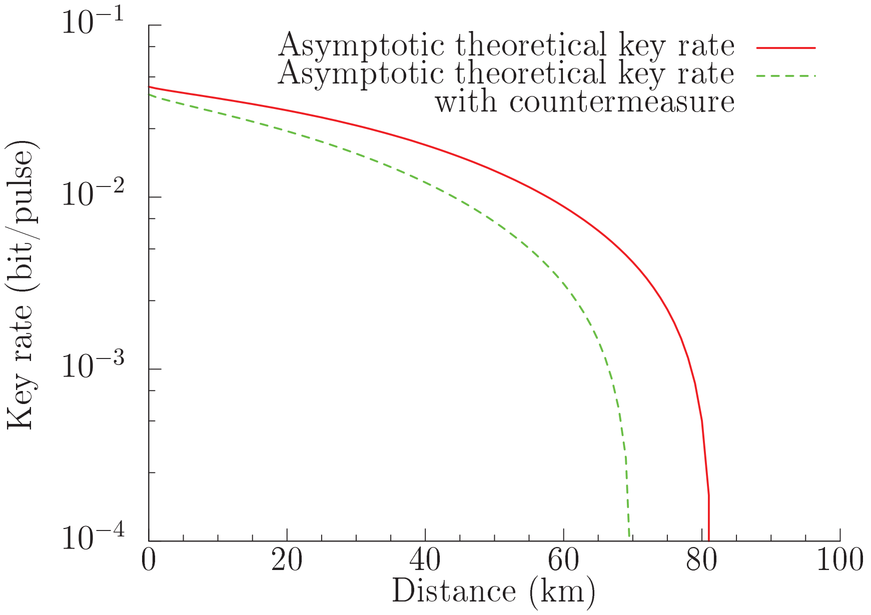


Figure 5.6: Secret key rate for collective attacks in the asymptotic regime. Both plots are obtained in the so-called realistic model where the electronic noise and the efficiency of the homodyne detection are calibrated and cannot be altered by the eavesdropper. The red upper plot corresponds to the secret key rate computed without implementing any countermeasure against the local oscillator calibration attack. The green lower plot is obtained when inserting an optical switch with typical losses of 2.7 dB on Bob's signal path and discarding 10% of the pulses on Bob's side at random to perform a real-time shot noise measurement. The transmittance T and distance d are linked with the expression $T = 10^{-\alpha d/10}$, where $\alpha = 0.2$ dB/km is the loss coefficient of the optical fiber. The modulation variance of Alice V_A is adjusted to maintain a signal-to-noise ratio of 0.075 on Bob's side, which allows for a reconciliation efficiency of $\beta = 94.8\%$ [64]. The excess noise on Bob's side is $\xi_{\text{Bob}} = 0.001$, and the electronic noise of the homodyne detection is $v_{el} = 0.01$. For the upper plot, the efficiency of the homodyne detection is assumed to be $\eta = 0.6$ while the lower plot corresponds to an efficiency $\eta_{\text{calib}} = 0.32$ when taking into account the losses of the optical switch on Bob's signal path.

Chapter 6

Increasing the Range of CVQKD

Contents

6.1 Theory of Reconciliation of Gaussian Variables . . . 98

6.2 Reconciliation of Gaussian Variables: Implementation with LDPC Codes . . . 99

6.2.1 Simulation Results with Rotations . . . 101

6.2.2 Use of rotations in higher dimension spaces . . . 102

6.2.3 Dealing with a continuous range of SNR with puncturing, shortening and repetition . . . 104

6.3 Practical use for a continuous-variable quantum key distribution system . . . 105

6.4 A rate 1/50 multi-edge LDPC code . . . 107

6.5 Puncturing / shortening performance . . . 108

6.6 Conclusion . . . 108

In the standard protocol [50], one needs to prepare Gaussian modulated coherent states and to measure them with a homodyne or a heterodyne [145] detection which requires only standard telecommunication parts. With the current proof techniques, using a Gaussian modulation is optimal as regards the theoretical secret key rate. In particular, security against collective attacks is well understood [46, 99], even in the finite-size regime [78], and collective attacks are known to be asymptotically optimal [112]. However, since the efficiency of the current reconciliation protocols for Gaussian variables drops dramatically in the regime of low signal-to-noise ratios (SNRs), new protocols using specific non-Gaussian modulations, either discrete [71] or continuous [76], have been developed. The idea of these modulations is that they are compatible with high-performance error correction, making possible for the protocol parties to extract efficiently the information available in their raw data. This is in strong contrast with the Gaussian modulation for which no efficient reconciliation procedure was available until now. In theory, protocols with a non-Gaussian modulation therefore increase the achievable secure distance of CVQKD. They have, however, not yet been demonstrated experimentally. Indeed, for long distances, that is low transmission of the quantum channel, the optimal modulation variance is typically lower for non-Gaussian modulations (in particular for the four-state protocol [71]) than for a Gaussian modulation. This makes the design of a stable continuous-variable system able to operate at large distances difficult. Even if this effect is mitigated for the eight-dimension protocol [76], the modulation allowing for the largest variance remains the Gaussian one [50].

In this chapter, we present high-efficiency error correcting codes which can be combined with a multidimensional reconciliation scheme [70]. This allows, for the first time, to distill a secret key from a CVQKD protocol with a Gaussian modulation in the regime of very low SNR, and paves the way for future experimental demonstrations of CVQKD over much larger distances than the current record of 30 km [83, 44].

In Section 6.1, we explain how the problem of reconciling Gaussian variables can be translated into a channel coding problem on the Binary Input Additive White Gaussian Noise Channel (BIAWGNC), for which we describe very low rate error correcting codes in Section 6.2. Combining these tools, we are able to efficiently reconcile data at low SNRs. Finally, we show in Section 6.3 the consequences of these new developments on the performance of the Gaussian protocol over long distances.

6.1 Theory of Reconciliation of Gaussian Variables

The data reconciliation step is critical in CVQKD: the distance of the chosen error-correction scheme to the Shannon bound affects both the key rate and the range of the protocol. Of considerable importance is the problem of the reconciliation of correlated Gaussian variables. This is indeed the scenario considered in the GG02 protocol [50] where Alice's coherent states are modulated with a bivariate Gaussian distribution in phase space. Different approaches have been explored to increase the reconciliation efficiency for a Gaussian modulation, especially in the regime of low SNR.

A first approach called *Slice Reconciliation* was proposed in [143, 14] and implemented in [83, 44] but the efficiency of this method currently limits the protocol range to about 30 km. Another method is to encode the information on the sign of the Gaussian modulated value. However, since we deal with centered Gaussian variables, the uncertainty on the sign increases at low SNRs because most values have small amplitude. Another class of protocols use *post-selection* [130, 98, 69, 54] by working only with high-amplitude data but the security is not proven against general collective attacks.

In [70], the idea of reducing the Gaussian variables reconciliation problem to the channel coding problem is introduced. One first uses a d-dimensional rotation to build a virtual channel close to the BIAWGNC from the physical Gaussian channel. This means that d consecutive instances of the physical channel are mapped to d approximate copies of a virtual BIAWGN channel, which are used to perform the error correction and eventually distill the actual secret. The final reconciliation efficiency one obtains with such a scheme depends on two things:

- The intrinsic efficiency of the error correcting code used on the virtual channel *on the BIAWGNC* (such an efficiency is given for example in Table 6.1).
- The quality of the approximation between the virtual channel and the BIAWGNC (for the scheme given in [70], the quality of this approximation increases with the dimension d).

One can therefore improve the reconciliation efficiency of the global scheme by working on two things: designing codes with higher efficiencies on the BIAWGNC and increasing the dimension of the scheme.

Let us now explain in more details the setting defined in [70]: Alice, the sender, and Bob, the receiver, are given two n-dimensional real vectors $\mathbf{x}$ and $\mathbf{y}$ and can use a public authenticated channel to agree on a common bit string $\mathbf{u}$. For this, one of the parties (say Alice in the direct reconciliation scheme) sends to the other additional information describing a function f such that $f(\mathbf{x}) = \mathbf{u}$; the other party (Bob) applies this function to his data to get $\mathbf{v} := f(\mathbf{y})$; this way, a virtual communication channel with input $\mathbf{u}$ and output $\mathbf{v}$ is defined. The explicit construction of [70] aims at creating a virtual channel that is close to the BIAWGNC since very efficient codes are available for that channel.

Alice and Bob are given two d-uplets $\mathbf{x}$ and $\mathbf{y}$ corresponding to correlated Gaussian vectors (this is valid for CVQKD with a Gaussian modulation and a Gaussian optimal attack). This means that one can introduce constants t, t' and σ, σ' such that one has $\mathbf{y} = t\mathbf{x}+\mathbf{z}$ with $\mathbf{x} \sim \mathcal{N}(0,1)^d$, $\mathbf{z} \sim \mathcal{N}(0,\sigma^2)^d$ in the direct reconciliation case and $\mathbf{x} = t'\mathbf{y}+\mathbf{z}'$ with $\mathbf{y} \sim \mathcal{N}(0,1+\sigma^2)^d$, $\mathbf{z}'^d \sim \mathcal{N}(0,\sigma'^2)^d$ in the reverse reconciliation case. Since the two scenarios are similar, we consider without loss of generality only the direct reconciliation one here. Furthermore, up to a simple renormalization, one can fix $t = 1$.

Alice chooses a random element $\mathbf{u} \in \{-1/\sqrt{d}, 1/\sqrt{d}\}^d$ with the uniform distribution on the d-dimensional hypercube and sends $\mathbf{r} = \mathbf{u}.\mathbf{x}^{-1}$ to Bob through the public channel (a "multiplication" and its inverse "division" operator are assumed to exist on d-dimensional vectors - more on this below). Then Bob computes $\mathbf{v} := \mathbf{r}.\mathbf{y}$. Let us analyze the noise $\mathbf{w}$ on this virtual channel:

$$\begin{aligned} \mathbf{w} &:= \mathbf{v} - \mathbf{u} \\ &= \mathbf{r}\mathbf{y} - \mathbf{u} \\ &= \mathbf{u}.\mathbf{x}^{-1}\,(\mathbf{x}+\mathbf{z}) - \mathbf{u} \\ &= \mathbf{u}\frac{\mathbf{z}}{\mathbf{x}} \sim \mathbf{u}\frac{\mathbf{z}}{||\mathbf{x}||} \end{aligned}$$

where the last equality holds in law and is due to the spherical symmetry of the distributions of $\mathbf{z}$ and $\mathbf{x}$ and their independence. Since the norm of $\mathbf{x}$ is transmitted, the channel considered is a Fading Channel with Known Side Information as defined in [114], the fading coefficient being the norm of $\mathbf{x}$, which follows a $\chi(d)$ distribution with d degrees of freedom. Since the distribution $\chi(d)$ gets closer to a Dirac distribution when d goes to infinity, one should use the highest dimension possible in order to obtain the degenerate version of the Fading Channel with Known Side Information where all the fading coefficients are equal to 1, that is, the BIAWGNC. Unfortunately, the required division operator only exists in dimensions 1, 2, 4 and 8 (where it can be built from the algebraic structure of $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ and $\mathbb{O}$ respectively), so that it is not possible to use the above algorithm in arbitrary dimension.

6.2 Reconciliation of Gaussian Variables: Implementation with LDPC Codes

Low Density Parity Check (LDPC) codes (or Gallager codes) are linear error-correcting codes with a sparse parity check matrix. A good reference about general coding theory and LDPC codes is [114]. LDPC codes can be represented as bipartite graphs, one set of the nodes being the check nodes representing the set of parity-check equations which define the code; the other, the variable nodes which represent the elements of the codewords. Variables nodes and check nodes are connected through edges. LDPC codes are commonly used in telecommunications since they perform very close to Shannon limit and can be decoded with a fast iterative message-passing decoder called Belief Propagation (BP) (in such a decoding scheme, information is propagated between variable and check nodes that are connected by edges). These codes are designed for a given channel and a given SNR. The rate of a code is defined as the ratio between the information bits and the total number of transmitted bits on the channel. A low rate code is therefore a code with a lot of redundancy bits. Correcting errors at very low SNRs implies to design codes with low rates since adding redundancy allows to correct more errors.

A standard way to characterize LDPC codes is the probabilistic method: an ensemble of LDPC codes $\mathcal{C}$ is characterized by the node degrees and one proves that good codes occur with high probability within this ensemble. A specific code is simply drawn randomly from this set. Then one can modify the node degrees and their probabilities of occurrence to improve the performance of the codes of the ensemble. A well known method to optimize LDPC codes for a given rate and a given channel is to use a genetic algorithm called *Differential Evolution*. This method has been successfully applied for a wide range of channels: the Binary Erasure Channel (BEC) [128], the BIAWGNC [115] and the Binary Symmetric Channel (BSC) [32]. The cost function that is maximized using this algorithm is defined as the threshold value for the channel (*i.e.* the maximal value of the noise that can be corrected with a given code, e.g. the standard deviation σ of the noise for the BIAWGNC or the probability of error ϵ for the BSC) and *Discretized Density Evolution* is used to compute the threshold.

In CVQKD, we need low-rate and high-efficiency codes for the BIAWGNC since errors must be efficiently corrected at very low SNRs to increase the secure distance. *Multi-edge-type LDPC codes* [113] give simple structures allowing to operate very close to Shannon limit at very low SNRs (for another construction of low rate LDPC codes refer to [7]). In the multi-edge setting, several edge classes are defined on the bipartite graph; then every node is defined by its number of sockets in each class. Whereas for standard LDPC ensembles the graph connectivity is constrained only by the node degrees, the multi-edge-type setting allows a greater control over the graph because only sockets of the same class can be connected together. Unlike standard LDPC ensembles, this framework provides for example the possibility to use degree-1 edges which improves significantly the threshold.

Every known reconciliation technique for CVQKD with a Gaussian modulation achieves an efficiency less than or equal to 90% [14, 83, 142]. This efficiency parameter β (defined by $\beta(s) = R/C(s)$ for a SNR s where R is the code rate used for the reconciliation and C is the capacity of the Additive White Gaussian Noise Channel (AWGNC)) is critical since the asymptotic secure key rate in the reverse reconciliation scheme is given by $K = \beta I(x;y) - \chi(y;E)$, where both $I(x;y)$ (the mutual information between the two protagonists bit strings x and y) and $\chi(y;E)$ (the Holevo information between the eavesdropper and the receiver's data) are large compared to K. One should especially pay attention to the dependency of β on the SNR. In [14, 83, 142], the good efficiency values are obtained only for SNRs higher than 1 which is incompatible with long distances. In [70], a 90% efficiency is obtained for a 0.5 SNR which allows to extend the secure distance

R	s_{DE}	C_{th}	β_{DE}
0.1	0.156	0.10429	95.9%
0.05	0.074	0.05144	97.2%
0.02	0.029	0.02038	98.1%

Table 6.1: Multi-edge LDPC codes asymptotic efficiencies. SNR asymptotic thresholds (s_{DE}) on the BIAWGNC, corresponding channel capacities (C_{th}) and efficiencies (β_{DE}) given by Density Evolution for low rate multi-edge LDPC codes of rate R.

R	s	$s_{d=1}$	$s_{d=2}$	$s_{d=4}$	$s_{d=8}$
0.1	0.271	0.187	0.169	0.163	0.161
0.05	0.123	0.082	0.077	0.076	0.075
0.02	0.047	0.030	0.029	0.029	0.029

Table 6.2: SNR thresholds on the BIAWGNC for low rate multi-edge LDPC codes (size 2^{20}) using the multidimensional reconciliation scheme ($d = 1, 2, 4, 8$).

from 30 km to 50 km. Here, we obtain higher efficiencies for even lower SNRs which allows secure key distribution over longer distances.

Let us now review low rate LDPC codes with a good efficiency available in literature. In [113], table IX, a 95.9% efficiency, rate 1/10 code for the BIAWGNC is described. This efficiency can be further improved through an optimization of the distribution coefficients as mentioned in [113]. Starting from the structure of this code we designed codes with lower rates and with higher asymptotic thresholds. Table 6.1 sums up the performances of this original code together with our set of new multi-edge LDPC codes (the actual structure of the rate 0.02 code is described as an example in Appendix 6.4). In this table, R is the rate of the considered code, s_{DE} is the SNR threshold given by Discretized Density Evolution, C_{th} is the theoretical channel capacity for this level of noise and β_{DE} is the efficiency of the code. These results are valid in the asymptotic regime, *i.e.* for codes of infinite length. However, the efficiency that is obtained with codewords of length 2^{20} is within 1% of the asymptotic efficiency.

6.2.1 Simulation Results with Rotations

Let us discuss the simulation results we obtained applying the multidimensional reconciliation scheme on S^1, S^3 and S^7 with the previous codes for a dimension $d = 2$, $d = 4$ and $d = 8$, for the sign coding technique ($d = 1$) and without using any additional information, *i.e.* when we try to use a code designed for the BIAWGNC with a Gaussian modulation.

Tables 6.2 and 6.3 summarize the efficiencies we obtained with respect to the Gaussian channel capacity with our multi-edge LDPC codes for a block size of 2^{20}. We obtained a quite high Frame Error Rate (FER) (about 1/3) but a null Bit Error Rate (BER) on the blocks where the decoding succeeded. This means that concatenating our codes with very high rate codes like BCH codes to remove the residual errors (as was done in [83, 44]) is not necessary here.

Since the channel obtained with rotations is not exactly a BIAWGNC, the efficiencies β are always lower than the efficiencies predicted by density evolution on the BIAWGNC. However, increasing the dimension d of the

R	β	$\beta_{d=1}$	$\beta_{d=2}$	$\beta_{d=4}$	$\beta_{d=8}$
0.1	57.9%	80.8%	88.7%	92.1%	93.1%
0.05	59.7%	88.3%	93.5%	94.8%	95.8%
0.02	60.0%	93.1%	96.3%	96.6%	96.9%

Table 6.3:

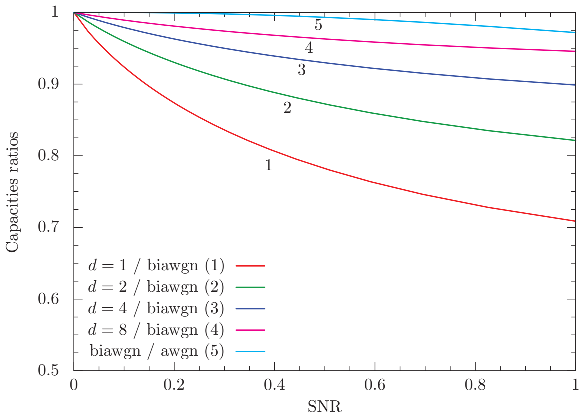


Figure 6.1: Ratios between the capacities of the multidimensional channels ($d = 1, 2, 4, 8$) and the BIAWGNC and between the BIAWGNC and the AWGNC with respect to the SNR.

rotations allows to get closer to the efficiency of the code on the BIAWGNC. This is expected since the norm of the input vector $u^d||x^d||$ of the virtual channel follows a distribution $\chi(d)$ (where d is the number of degrees of freedom), which gets closer to a Dirac when d tends to infinity.

Figure 6.1 compares the capacities of the BIAWGNC and the multidimensional virtual channels for $d = 1, 2, 4, 8$ as a function of the SNR.

6.2.2 Use of rotations in higher dimension spaces

As was explained in the previous section, the multidimensional reconciliation scheme is limited to dimensions $1, 2, 4$ and 8 because these are the only ones compatible with a division structure [70].

In [70], the following construction applicable to arbitrary dimension d is proposed. In the direct case, with the same notations as in paragraph 6.1 (where Alice has a vector $\mathbf{x}$, Bob a vector $\mathbf{y}$, and Alice uses $(\mathbf{x}, \mathbf{r})$ to 'virtually' send $\mathbf{u}$ to Bob), a random orthogonal transformation Q on $\mathbb{R}^d$ is drawn according to the Haar measure, then Q is composed with the reflection S across the mediator hyperplane of $\mathbf{x}' = Q(\mathbf{x})$ and $\mathbf{u}$. The resulting matrix $R = S \circ Q$ sends $\mathbf{x}$ to $\mathbf{u}$ and $\mathbf{y}$ to a point close to $\mathbf{u}$, because R preserves the euclidean distance; R is revealed by Alice and plays the same role as the vector $\mathbf{r}$ in section 6.1. The randomization provided by Q ensures that R does not reveal more information on $(\mathbf{x}, \mathbf{u})$ than the relation $R(\mathbf{x}) = \mathbf{u}$; in particular, all $\mathbf{u}$ are equally likely given R.

Q is built, for instance, as the orthogonal ('Q') part of the QR decomposition of a $d \times d$ matrix G of Gaussian normalized random values. This method has complexity $\mathcal{O}(d^3)$. All other known methods to draw random orthogonal matrices have the same complexity.

We propose a method that allows to reduce the complexity to $\mathcal{O}(d^2)$. Let us observe first that we have the choice of the encoding of R: we do not need to reveal it in matrix form. However, the encoding must not reveal anything about $\mathbf{u}$ except that R satisfies $R(\mathbf{x}) = \mathbf{u}$. For instance, with the first method, revealing separately Q and S instead of $R = S \circ Q$ is not a good idea since S leaks information about u: indeed, in high dimension d, two random independent vectors are approximately orthogonal and therefore their mediator hyperplane forms and angle of about $\pi/4$ with either vector.

Let us examine first how an orthogonal transform Q can be drawn according to the Haar measure with complexity $\mathcal{O}(d^2)$, using an adequate representation, the Householder decomposition. An orthogonal basis $\mathbf{e}_1, \ldots, \mathbf{e}_d$ is fixed. Let E (resp. F) be the span of $\mathbf{e}_1, \ldots, \mathbf{e}_d$ (resp. $\mathbf{e}_2, \ldots, \mathbf{e}_d$).

If $d = 1$, choose $+1$ or -1. If $d > 1$, choose a random vector $\mathbf{g}$ uniformly on $\mathcal{S}^{d-1}$, the unit sphere in $\mathbb{R}^d$ (it can be constructed as $\mathbf{g} = \mathbf{h}/||\mathbf{h}||$ where $\mathbf{h}$ has independent normalized Gaussian coordinates), and draw recursively a random orthogonal matrix Q' of dimension $d-1$, viewed as a transform of F. Q' is extended to E by setting $Q'(\mathbf{e}_1) = \mathbf{e}_1$. Let S be the reflection that sends $\mathbf{e}_1$ on $\mathbf{g}$, and define $Q = S \circ Q'$. Q' is itself a composition of $d-1$ reflections in spaces of dimensions $d-1, \ldots, 1$. Describing each reflection by its corresponding eigenvector for the eigenvalue -1, Q is described by d vectors of dimensions $d, d-1, \ldots, 1$, for a total of $\frac{d(d+1)}{2}$ coefficients. The decomposition is unique. Note that $Q(\mathbf{e}_1) = \mathbf{g}$.

This process can be adapted when a constraint $Q(\mathbf{x}) = \mathbf{u}$ is added, with $||\mathbf{x}|| = ||\mathbf{u}||$. If $d = 1$, choose $+1$ or -1 depending on $\mathbf{x} = \mathbf{u}$ or $\mathbf{x} = -\mathbf{u}$. Assuming $d > 1$, $\mathbf{g}$ is chosen uniformly at random among unit vectors s.t.

$$\mathbf{u} \cdot \mathbf{g} = \mathbf{x} \cdot \mathbf{e}_1 \tag{6.1}$$

where $\cdot$ is the dot product. This relation is required for Q to satisfy both $Q(\mathbf{x}) = \mathbf{u}$ and $Q(\mathbf{e}_1) = \mathbf{g}$. Starting from a Gaussian normalized vector $\mathbf{h}$, α is chosen uniformly so that $(\mathbf{h} + \alpha\mathbf{u}) \cdot \mathbf{u} = (\mathbf{x} \cdot \mathbf{e}_1) \times ||\mathbf{h} + \alpha\mathbf{u}||$ (this is a quadratic equation that has at least one solution except if $\mathbf{h}, \mathbf{u}$ span the same line, and $\mathbf{e}_1, \mathbf{x}$ do not, which happens with probability 0). $\mathbf{g} = \frac{\mathbf{h}+\alpha\mathbf{u}}{||\mathbf{h}+\alpha\mathbf{u}||}$ is computed in linear time and satisfies (6.1).

For an arbitrary vector $\mathbf{v}$, write its decomposition on F, e_1 as $\mathbf{v} = \mathbf{v}_F + \mathbf{v}_{F^\perp}$. Q' is drawn recursively, satisfying $Q'(\mathbf{x}_F) = S(\mathbf{u})_F$. This is possible because $\mathbf{x} \cdot \mathbf{e}_1 = \mathbf{u} \cdot \mathbf{g} = \mathbf{u} \cdot S(\mathbf{e}_1) = S(\mathbf{u}) \cdot \mathbf{e}_1$ implies $\mathbf{x}_{F^\perp} = S(\mathbf{u})_{F^\perp}$ and $||\mathbf{x}_F|| = ||S(\mathbf{u})_F||$. Then as $Q'(e_1) = e_1$, $Q'(\mathbf{x}) = S(\mathbf{u})$.

Define $Q = S \circ Q'$ as before: $Q(\mathbf{x}) = S(Q'(\mathbf{x})) = \mathbf{u}$.

The algorithm still runs in $\mathcal{O}(d^2)$, and the decomposition does not reveal any side information because it is unique. Since the added constraint (6.1) is required for the relation $Q(\mathbf{x}) = \mathbf{u}$ to hold, one sees recursively that the process yields the correct distribution on O_d. Finally, given the d reflection vectors, computing $Q(\mathbf{z})$ for any $\mathbf{z}$ is also done in time $\mathcal{O}(d^2)$. Hence by revealing these vectors instead of Q in matrix form, one gets the desired $\mathcal{O}(d^2)$ algorithm.

Let us now consider the rate 1/2 multi-edge LDPC code given in Table VI of reference [113]. The SNR threshold given by Discretized Density Evolution is $s^* = 1.074$. The corresponding efficiency on the BIAWGNC is 98.2%. When using a Gaussian modulation, table 6.4 shows the effect of the dimension d on the efficiency β of the reconciliation scheme. We can see that increasing the dimension above 8 when operating at a high SNR

d	s	β
2	1.644	76.3%
4	1.336	85.7%
8	1.194	91.7%
16	1.144	94.3%
32	1.108	96.2%
64	1.097	96.9%

Table 6.4: SNR thresholds and channel efficiencies on the BIAWGNC for a rate 1/2 multi-edge LDPC code with respect to the dimension of the multidimensional reconciliation scheme. The description of this code can be found in in Table VI of ref. [113]

enables to increase significantly the efficiency, and therefore the key rate in QKD applications.

6.2.3 Dealing with a continuous range of SNR with puncturing, shortening and repetition

We designed good efficiency codes for a finite set of rates so far; we are going to show how to deal with a continuous range of SNRs with this finite set. Since we designed low rate codes with good efficiencies, we can apply the simple technique of repetition codes mentioned in [72]. It is shown that starting from a code of rate R achieving an efficiency $\beta(s)$ for a SNR s on the BIAWGNC, one can use a repetition scheme of length k to build a new code of rate $R^{'} = R/k$ achieving an efficiency β' for a SNR $s' = s/k$ given by

$$\beta'(s/k) = \beta(s)\ \frac{\log_2(1+s)}{k\log_2(1+s/k)}$$

For example, using a repetition scheme of length 3 with our code of rate 0.02 and efficiency 98% for a SNR of 0.03, we can build a code of efficiency $\beta(0.01) = 0.98\frac{\log_2(1.03)}{3\log_2(1.01)} = 97\%$. We applied this technique with repetition factors of 2 and 4 with our code of rate 0.02 to obtain the codes of rates 0.01 and 0.005 given in Table 6.5.

However, this technique allows a low efficiency loss only for very small SNRs. For higher SNRs, other techniques must be applied if we want to keep very good efficiencies. Puncturing and shortening for LDPC codes are a good way to adapt the rate of a code [33]. Let us start with a (n, k) code, *i.e.* a code of length n with $n-k$ bits of redundancy; the rate is $R = k/n$. Puncturing consists in deleting a predefined set of p symbols from each word, converting a (n, k) code into a $(n-p, k)$ code. Shortening means deleting a set of s symbols from the encoding process (or revealing s message bits in addition to the syndrome in each codeword), converting a (n, k) code into a $(n-s, k-s)$ code. With a combination of these techniques the rate obtained is

$$R = \frac{k-s}{n-p-s} \quad .$$

The loss of efficiency incurred is small for small relative variations of the code rate. Typically, one can achieve a decrease of 5% (though shortening) and an increase of 10% (through puncturing) of the code rate with an efficiency loss smaller than 1%.

R	β	s
0.5	93.6%	1.097
0.1	93.1%	0.161
0.05	95.8%	0.075
0.02	96.9%	0.029
0.01	96.6%	0.0145
0.005	95.9%	0.00725

Table 6.5: SNR thresholds and channel efficiencies on the AWGNC of the multi-edge LDPC codes mentioned in this chapter.

6.3 Practical use for a continuous-variable quantum key distribution system

In this section, we apply the techniques developed in the previous sections to CVQKD in order to increase the secure distance achievable. We have to take into account that our quantum channel is Gaussian so that code efficiencies must be computed w.r.t. this channel capacity:

$$\beta = \frac{R}{C_{AWGNC}}$$

where R is the rate of the code and C_{AWGNC} is the capacity of the AWGNC. As we can see on Figure 6.1, the capacity of the BIAWGNC is very close to the capacity of the AWGNC for small values of the SNR. We give the efficiencies we can achieve on the AWGNC for different SNRs in Table 6.5.

Our set of codes allows us to correct errors with an efficiency of about 95% for some fixed low SNRs. Let us plot the secret key rate as a function of the SNR on Bob side for a given distance and assuming a fixed error correction efficiency β. This enables to determine for which particular SNR it is relevant to design error-correcting code in order to maximize the secret key rate. We do not consider here finite-size effects [78], meaning that our figures represent the key rate in the regime of infinite block length. In order to take finite-size effects into account two approaches are possible: a theoretical one consists in improving the proofs and the bounds on the secret key rate [12], a more practical one consists in designing systems with sufficient hardware stability in order to compute keys on large blocks.

The modulation variance is restricted within the interval $[1, 100]$ (in shot noise units) since lower values make the experimental setup much more complex. Indeed, a very low modulation variance is not compatible with brighter synchronization and phase tracking signals, because of the limited extinction ratios of the optical modulators (30dB for the most common models). An attenuation of 0.2dB/km is assumed. The homodyne detection efficiency is set to 0.6, and a value of 1% of the shot noise is taken for the electronic noise of the homodyne detection [83, 44]. A conservative value of 4% of the shot noise as in the European project SECOQC (Secure Communication based on Quantum Cryptography) [44] is used for the excess noise in Figure 6.4 while a more optimistic figure of 1% is used in Figures 6.2, 6.3 and 6.5. This second value is also typical of a realistic CVQKD system citeLBG07.

Figure 6.2 shows the optimal variance modulation on Alice side with respect to the key rate as a function of the distance. Achieving a good reconciliation efficiency at any SNR allows to work with a high modula-

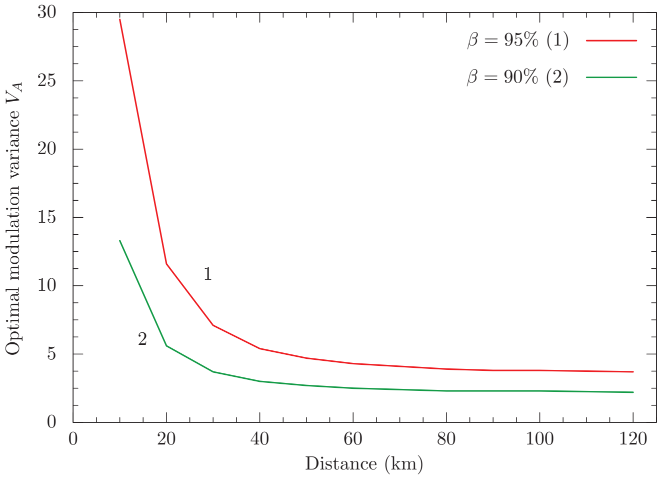


Figure 6.2: Optimal modulation variance with respect to the distance. $\eta = 0.6$, $V_{elec} = 0.01$, $\xi = 0.01$, $\alpha = 0.2dB/km$, $\beta = 95\%$ and $\beta = 90\%$ from top to bottom.

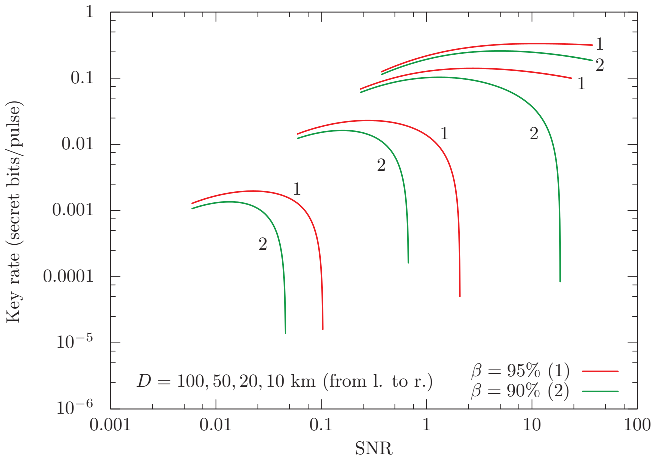


Figure 6.3: Secret key rate for collective attacks with respect to the SNR. $\eta = 0.6$, $V_{elec} = 0.01$, $\xi = 0.01$, $\alpha = 0.2dB/km$, $V_A \in \{1, 100\}$, $\beta = 95\%$ and $\beta = 90\%$, $D = 10, 20, 50, 100$ km.

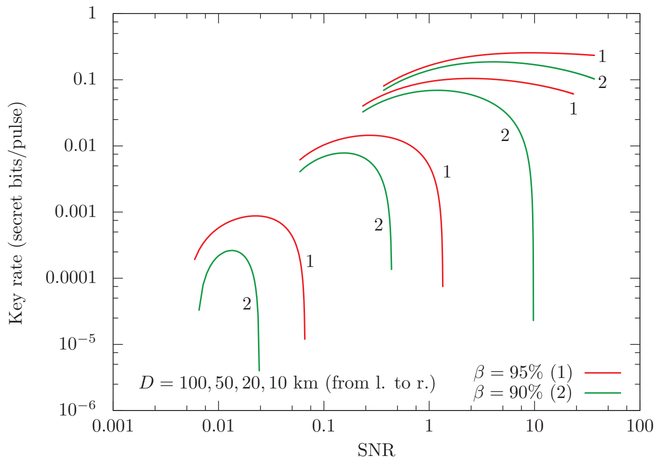


Figure 6.4: Secret key rate for collective attacks with respect to the SNR. $\eta = 0.6$, $V_{elec} = 0.01$, $\xi = 0.04$, $\alpha = 0.2dB/km$, $V_A \in \{1, 100\}$, $\beta = 95\%$ and $\beta = 90\%$, $D = 10, 20, 50, 100$ km.

tion variance. This compares favorably to previous schemes with a discrete modulation which require modulation variances 10 times lower than the ones shown here.

Figure 6.3 and 6.4, plotted respectively for an excess noise of 1% and 4% of the shot noise, show that an improvement on the reconciliation efficiency yields at any distance a wider range of SNR with a close-to-optimum secret key rate. Conversely, the range of distances where a given error-correcting code working close to its threshold SNR can be used to get an almost optimal key rate is increased.

Given these large distance ranges where an error-correcting code is usable, it becomes feasible to use a small family of error-correcting codes to perform the reconciliation step at *any* distance and *without* using rate-tuning techniques such as puncturing or shortening. Figure 6.5 shows the key rate and the maximum secure distance obtained with this simple approach and the codes of Table 6.5. With an excess noise of 1% of the shot noise, a secure distance above 150 km is obtained (with an excess of noise of 4% and the same codes, the secure distance is above 140 km). This is a significant improvement over previous reconciliation techniques since a reconciliation efficiency of 90% for a SNR of 0.5 only allows a secure distance of about 50 km with a Gaussian modulation [70].

6.4 A rate 1/50 multi-edge LDPC code

Below is the description of a multi-edge LDPC ensemble of codes of rate $R = 0.02$ ($\sigma^* = 5.91$ on the BIAWGNC). The left half of the array describes the multi-degree distributions of variable nodes, and the right half the distribution of check node multi-degrees. m stands for a multi-degree distribution of probability ν_m at the variable nodes and μ_m at the check nodes. For instance, with probability 0.0225, a variable node has multi-degree [2, 57, 0], *i.e.* it has 2 sockets for edges of type 0, 57 sockets for edges of type 1, and no socket of type 2. Check node probabilities sum to $1 - R = 0.98$ since there is 0.98 check node for 1 variable node.

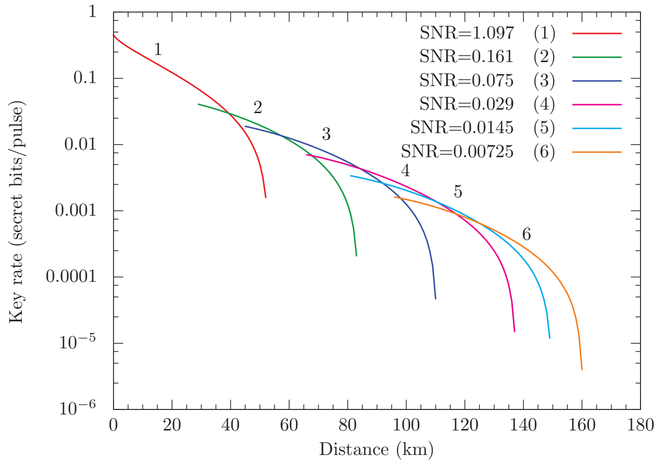


Figure 6.5: Secret key rate for collective attacks with respect to the distance. $\eta = 0.6$, $V_{elec} = 0.01$, $\xi = 0.01$, $\alpha = 0.2 dB/km$, $V_A \in \{1, 100\}$, $SNR = 1.097, 0.161, 0.075, 0.029, 0.0145, 0.00725$, $\beta = 93.6\%, 93.1\%, 95.8\%, 96.9\%, 96.6\%, 95.9\%$ from left to right.

ν_m	m			μ_m	m		
0.0225	2	57	0	0.010625	3	0	0
0.0175	3	57	0	0.009375	7	0	0
0.96	0	0	1	0.6	0	2	1
				0.36	0	3	1

6.5 Puncturing / shortening performance

Figure 6.6 gives the efficiency of a rate 0.5 LDPC code on the BIAWGNC with respect to noise. Modifications of the rate of the code with puncturing and shortening techniques allow us to maintain a high efficiency over a wide SNR range. This implies that a finite set of codes is sufficient to cover the whole useful SNR range for CVQKD.

6.6 Conclusion

We designed high-efficiency error-correcting codes allowing to distribute secret keys with a continuous-variable quantum key distribution system using a Gaussian modulation over long distances. Our results give a secure distance above 150 km against collective attacks (in the asymptotic regime) and can be implemented with only software modifications in the experimental setups of [83] and [44].

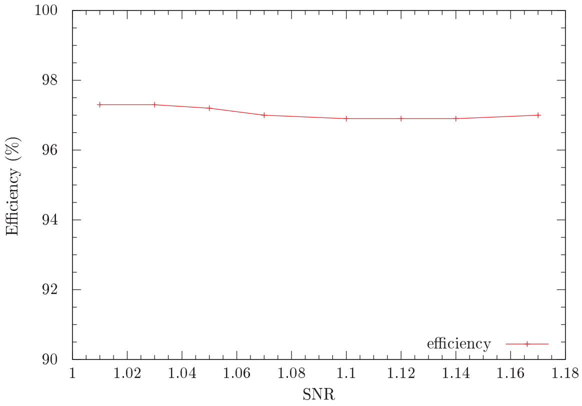


Figure 6.6: Efficiency of a LDPC code on the BIAWGNC with respect to noise. Modifications of the rate of the code with puncturing and shortening techniques allow us to maintain a high efficiency over a wide SNR range. This implies that a finite set of codes is sufficient to cover the whole useful SNR range for CVQKD.

Chapter 7

Experimental Demonstration of Long-distance CVQKD

Contents

7.1 Outlook of the Experiment 113

7.2 Experimental Results 114

7.3 Security Conditions 117

7.4 Multidimensional Reconciliation 117

7.5 Local Oscillator Manipulation 117

7.6 Hardware Stability 118

7.7 Post-processing Performance 118

7.8 Conclusion and Perspectives 119

Distributing secret keys with information-theoretic security is arguably one of the most important achievements of the field of quantum information processing and communications [120]. The rapid progress in this field has enabled quantum key distribution (QKD) in real-world conditions [104, 119] and commercial devices are now readily available. QKD systems based on continuous variables [148] present the major advantage that they only require standard telecommunication technology. However, these systems were considered up till now unsuitable for long-distance communication [44, 28, 61]. Here, we overcome all previous limitations and demonstrate for the first time continuous-variable quantum key distribution over 80 km of optical fiber. All aspects of a practical scenario are considered, including the use of finite-size data blocks for secret information computation and key distillation. Our results correspond to an implementation guaranteeing the strongest level of security for QKD reported to date for such long distances and pave the way to practical applications of secure quantum communications.

Long-distance experiments in quantum information science, and in particular for quantum key distribution (QKD), are of utmost importance for future technological applications. Such experiments will allow the integration of quantum devices in current secure infrastructures and in future networks based on quantum repeaters [17]. The quest for long-distance QKD in the last years has led to several successful demonstrations [137, 117, 133, 29], however improving security guarantees and performance in practical conditions in these implementations remains an issue. These experiments use discrete-variable or distributed-phase-reference protocols [120], where the key information is encoded on properties of single photons. Alternatively,

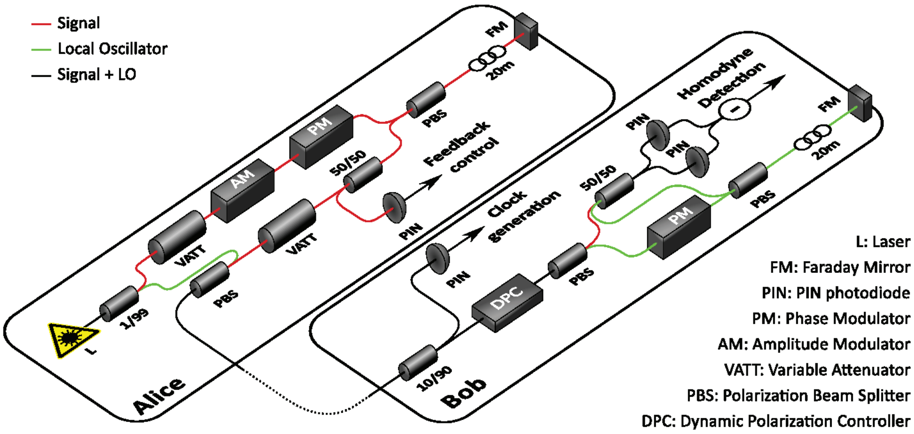


Figure 7.1: Optical layout of the long-distance CVQKD prototype. Alice sends to Bob 100 ns coherent light pulses generated by a 1550 nm telecoms laser diode pulsed with a frequency of 1 MHz. These pulses are split into a weak signal and a strong local oscillator (LO) with an unbalanced coupler. The signal pulse is modulated with a centered Gaussian distribution using an amplitude and a phase modulator. The variance is controlled using a coarse variable attenuator and the amplitude modulator. The signal pulse is 200 ns delayed with respect to the LO pulse using a 20 m delay line and a Faraday mirror. Both pulses are multiplexed with orthogonal polarization using a polarizing beamsplitter (PBS). The time and polarization multiplexed pulses are then sent through the channel. They are demultiplexed on Bob's side with another PBS combined with active polarization control. A second delay line on Bob's side allows for time superposition of signal and LO pulses. After demultiplexing, the signal and LO interfere on a shot-noise limited balanced pulsed homodyne detector. A phase modulator on the LO path allows for random choice of the measured signal quadrature. Alice and Bob are situated in the same laboratory and separated by fiber spools. The maximum operating distance of the experiment is 80 km.

in the continuous-variable (CV) QKD protocols, light carries continuous information such as the value of a quadrature component of a coherent state. Such protocols have been implemented in various situations [49, 107, 83, 136, 44, 28, 126, 61]. Their key feature is that dedicated photon-counting technology can be replaced by homodyne detection techniques that are widely used in classical optical communications. CVQKD schemes, however, require complex post-processing procedures, mostly related to error correction. These have hindered their operation over more than 25 km of optical fiber [44, 28, 61], a communication span that may be insufficient for network cryptographic applications. Furthermore, implementations so far were based on security proofs valid in the limit of infinitely large data blocks, while the finite size of real data must be taken into account according to more complete security proofs [122, 63].

Here we demonstrate the distribution of secret keys over a distance of 80 km, using continuous variables and security proofs compatible with the use of finite-size data blocks for the generation of the secret key. This remarkable range improvement was made possible by a system operation in a regime of signal-to-noise ratios (SNR) between one and two orders of magnitude lower than in earlier implementations. It was previously overlooked that techniques developed for error correction of Gaussian signals can perform close to the optimal bounds for low SNR. Implementing such error-correction codes at high speed and in an optical environment featuring excellent stability, which enabled the acquisition of large data blocks, allowed us to reach parameter regions that were previously inaccessible. This was a key element for the present experiments.

7.1 Outlook of the Experiment

In the experimental setup, shown in Figure 7.1, we implement the standard GG02 coherent-state CVQKD protocol [50]. The sender, Alice, prepares coherent states with a Gaussian modulation and sends them to the receiver, Bob, who measures one of the quadratures with a homodyne detection system. A reverse reconciliation scheme, in which Alice and Bob use Bob's data to establish the secret key [49], is used.

Our experiment is a one-way implementation, where Alice sends to Bob coherent light pulses with a 100 ns duration and 1 MHz repetition rate generated by a 1550 nm pulsed telecoms laser diode. These pulses are split into a weak signal and a strong local oscillator (LO) with an unbalanced coupler. The implemented protocol uses Gaussian modulation of coherent states [50]: the signal is randomly modulated in both quadratures using an amplitude and a phase modulator. The signal pulses are then attenuated by a variable attenuator such that the signal power belongs to a range allowing to control the variance of the Gaussian distribution exiting Alice's device using a photodiode and an appropriate feedback algorithm. A second variable attenuator lowers the signal level to a few shot noise units.

The signal and LO are then transmitted through the optical fiber without overlap using time and polarization multiplexing. Delay lines of 200 ns, composed of a 20-m single-mode fiber followed by a Faraday mirror, are used for the time multiplexing. Polarization multiplexing is achieved using polarization beam splitters. After demultiplexing, the signal and LO interfere on a shot-noise limited balanced pulsed homodyne detector. The electric signal coming from the detector is proportional to the signal quadrature X_ϕ, where ϕ is the relative phase between the signal and the LO, which can be controlled using the phase modulator on Bob's LO path according to the Gaussian protocol [50].

Feedback controls are implemented to allow for a stable operation of the system over a large number of pulses ($\geq 10^8$). Polarization drifts occurring in the quantum channel are corrected using a dynamic polarization controller. The beamsplitter placed at the entrance of Bob's apparatus aims at generating from the LO pulse a clock signal that is independent of the polarization state. Then, the homodyne detection statistics and an appropriate algorithm allow us to maintain an optimal polarization state at the output of the channel. The photodiode on Alice's signal path is used for amplitude modulator feedback to correct alterations of the required voltage settings induced by temperature variations. On Bob's side, the homodyne detection output is sensitive to phase and can be used to control Alice's and Bob's phase modulators.

The security of the implemented protocol is well established against collective attacks, both in the asymptotic [46, 99] and in the finite-size regime [63]. Moreover, collective attacks have been shown to be asymptotically optimal [112, 74]. Here, we consider security proofs pertaining to such attacks, taking also into account finite-size effects. The Gaussian modulation used in the implemented protocol maximizes the mutual information between Alice and Bob, thus offering an optimal theoretical key rate. However, it is hard to reconcile correlated Gaussian variables, especially at low signal-to-noise ratios, which are inherent in long-distance experiments. Indeed, the secure distance of previous demonstrations of fiber-based CVQKD [44, 61] was limited to 25 km because no efficient error-correction procedure was available at low SNR. Here, we use a multidimensional reconciliation protocol[70], which transforms a channel with a Gaussian modulation into a virtual binary modulation channel, with a capacity loss that is very low at low SNR. This enables the use of error-correction codes designed for the Binary Input Additive White Gaussian Noise Channel, whose typical efficiencies for arbitrarily low SNR are of 0.95 extracted bit per theoretically available bit [65]. This leads to a significant extension of the secure distance.

Let us now look at the parameters that are relevant for the extraction of the secret key. Due to the Gaussian optimality theorem[46, 99], Alice and Bob's two-mode state at the output of the quantum channel is fully characterized by Alice's modulation variance V_A, the channel transmission T and the excess noise ξ, which is added by the channel. Both V_A and ξ are expressed in shot noise units. These parameters, together with the shot noise, are estimated in real time using a parameter estimation process, during which a fraction of the samples is randomly revealed. The other parameters used to compute an estimate of the secret information that can be extracted from the shared data, namely the electronic noise v_{el} and the efficiency of the homodyne detection η, are assumed not to be accessible to Eve and are measured during a secure calibration procedure that takes place before the deployment of the system. For simplicity, we make the standard assumption that Eve does not tamper with the local oscillator, but we emphasize that countermeasures against such tampering have been proposed (see Supplementary Information for details). The modulation variance is adjusted in real time in order to be at all times as close as possible to the SNR corresponding to the threshold of an available code.

Privacy amplification allows extracting the secret information from the identical strings shared by Alice and Bob after error correction. In addition to the amount of data revealed during error correction, we compute an upper bound on the eavesdropper's information on the corrected string for collective attacks in both the asymptotic regime, where all the experimental parameters are assumed to be known with an infinite precision, and in the finite-size regime, where the parameters are estimated over large data pulse sets. The stability of our system allows us to obtain a positive secret key rate at long distances in both regimes.

7.2 Experimental Results

Long-distance secret key generation results are shown in Figure 7.2. Secret keys were produced by the experimental system at 25 km, 53 km, and 80.5 km of standard optical fiber. The key rate was computed during 24 hours at all distances. A sifting procedure reveals 50% of the raw key for parameter estimation, while 50% of the optical pulses have also been discarded for shot noise estimation. The fraction of light pulses effectively used for generating the key is thus 25%. The error correction is performed using Low Density Parity Check codes with a Graphic Processing Unit decoder (see Supplementary Information for details). The obtained secret key

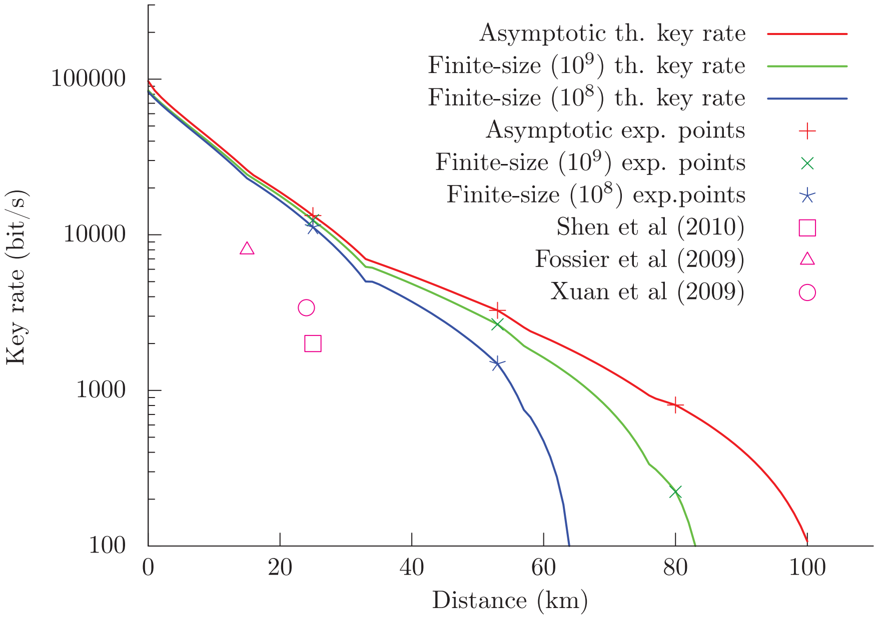


Figure 7.2: These figures are obtained with a SNR of 1.1 on Bob's side at 25 km (5.0 dB losses), a SNR of 0.17 at 53 km (10.6 dB losses), and a SNR of 0.08 on Bob's side at 80.5 km (16.1 dB losses). In red, the rate is calculated assuming an eavesdropper able to perform collective attacks in the asymptotic regime. This rate is also valid against arbitrary attacks. In green (resp. blue), the rate is calculated assuming an eavesdropper able to perform collective attacks taking into account finite-size effects with block size 10^9 (resp. 10^8) and security parameter $\epsilon = 10^{-10}$. The odd shape of the curves results from the use of a small set of error-correcting codes optimized to perform data reconciliation in specific ranges of SNR. The homodyne detection is characterized by an efficiency $\eta = 0.552$, known with uncertainty $\Delta\eta = 0.025$, and an electronic noise variance $v_{el} = 0.015$, known with uncertainty $\Delta v_{el} = 0.002$. For comparison, previous state-of-the-art experimental results are shown [83, 44, 28]: they are all restricted to distances below 25 km, and do not take finite-size effects into account.

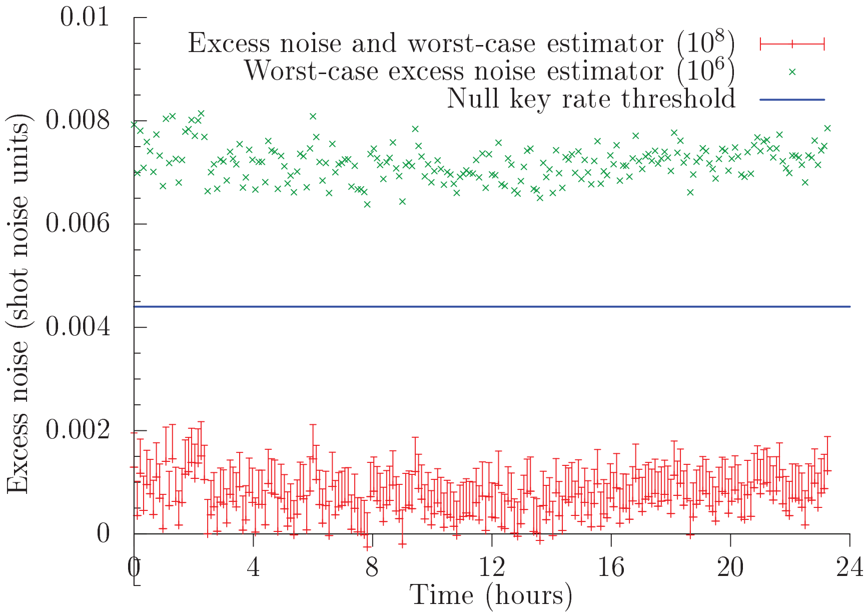


Figure 7.3: Experimental excess noise measured during 24 hours with a SNR of 0.17 on Bob's side. For this measurement we used 53 km of standard optical fiber corresponding to 10.6 dB losses. The red + correspond to measurements performed on blocks of size 10^8, each one corresponding to roughly 6 minutes of data acquisition, and indicate the experimental measured excess noise (lower point) as well as the worst-case estimator for the excess noise (upper point) compatible with this data. The probability that the true value of the excess noise is underestimated by the estimator because of statistical fluctuations is less than 10^{-10}, assuming that the noise is Gaussian. This worst-case estimator is the value used to compute the secret key rate when finite-size effects are taken into account. For comparison, the green × correspond to the worst-case estimator if the estimation was performed on blocks of size 10^6. The blue line indicates the maximal value of excess noise that allows for a positive secret key rate. Even without any experimental noise, no secret key could be extracted at 53 km with a parameter estimation on blocks of size 10^6.

rates are lower than those obtained with discrete-variable QKD [29]. This is mainly due to the lower clock rate of our experiment.

The results corresponding to the finite-size regime are of particular interest because of their relevance for practical applications. Indeed, obtaining an infinite precision in parameter estimation as required in the asymptotic case is, in practice, impossible. We can further elucidate these results by investigating the impact on the secret key rate of the uncertainty on the excess noise value. Figure 7.3 shows the experimental excess noise measured on blocks of size 10^8 during 24 hours at a 53-km distance. For each data point, a worst-case estimator of the excess noise compatible with the experimental data is also indicated. For comparison, the worst-case estimator for a block size of 10^6 is displayed and is clearly incompatible with the extraction of a secret key rate, thus showing that a very large block size is required to achieve long-distance QKD. These results illustrate the significance of the excess noise estimation for system performance. They also confirm the excellent stability of our system, since the excess noise maintains low values, even in this very low SNR regime required by the security proof, and with very large data blocks.

7.3 Security Conditions

Collective attacks against the implemented protocol have been shown to be asymptotically optimal, thanks to an infinite-dimensional version of de Finetti's theorem [112]. Furthermore, security proofs combining arbitrary attacks and finite-size effects are presently actively studied [74, 45].

The implemented protocol requires an exact Gaussian modulation, which is impossible to achieve. In practice, this is approximated by a truncated discretized modulation with parameters compatible with a security proof against collective attacks. This is performed with almost optimal randomness consumption using source coding techniques.

The efficiency and the variance of the electronic noise of the homodyne detection are assumed to be calibrated in a secure laboratory. This corresponds to the standard realistic assumption for CVQKD implementations, according to which Eve cannot entangle herself with the losses or electronic noise of the homodyne detection. Under this assumption, we evaluate confidence intervals for these values and we compute the eavesdropper's corresponding information taking calibrated value uncertainties into account [63]. Note that in the so-called "paranoid" or "uncalibrated-device" scenario [120], where Eve can exploit the homodyne detection parameters, no secret key would be obtained beyond 35 km.

7.4 Multidimensional Reconciliation

The error-correction step is divided into two parts. First, Bob divides his data into vectors y of size 8 and for each, draws a binary vector u of the same size at random; u is the reference for the key after the error correction. Then Bob computes $r = y \cdot u$ (where the vectors are interpreted as octonions, see [70] for details) and sends it to Alice who obtains $v = x^{-1} \cdot r = x^{-1} \cdot y \cdot u$, that is a noisy version of Bob's binary modulated vector u, with a noise close to a Gaussian noise. Interestingly, it can be shown that the classical data r, available to Eve, does not leak any information about the binary vector u [70]. The second step of the error-correction protocol consists in forming vectors of size 2^{20} on Alice's and Bob's sides (corresponding to 2^{17} pairs of such vectors u, v) and to use multi-edge Low Density Parity Check (LDPC) codes to correct all the errors [65]. The amount of data revealed during this step is subtracted from the secret information previously computed. We use Graphics Processing Unit (GPU) decoding to obtain a decoding speed compatible with real-time data-processing.

7.5 Local Oscillator Manipulation

In the main text we have made the standard assumption that Eve does not tamper with the local oscillator. The simplest example of such tampering would be for Eve to manipulate the intensity of the LO, and a simple countermeasure (implemented in the experiment) is to monitor continuously the LO intensity [38]. More sophisticated tampering may be possible, and deserves more studies. An example of such a calibration attack involving

LO manipulation is given in chapter 5. All LO attacks can be fixed in principle by “reconstructing” the LO at Bob’s site, but this is currently not implemented.

7.6 Hardware Stability

Hardware stability over a long period of time is necessary to extract secret keys from blocks of size greater than 10^9, as is required to take into account finite-size effects for distances above 50 km [63]. A limitation to the long-term hardware stability in [44, 61] was the clock reliability on the receiver’s side, because of its dependence on the polarization control. We use a splitter and a dedicated electronic circuit and obtain a considerably less noisy and hence more reliable clock.

The hardware stability is also linked to the fraction of pulses that are used for parameter estimation. In particular, for blocks of size 10^9, which are required to perform parameter estimation at long distances, the ratio between the number of pulses used for the parameter estimation and the number of pulses used to extract the key was 1. It is possible to change this ratio; however, if for example we use a ratio 0.1 instead of 1, the parameters need to remain stable during a period corresponding to $(1/0.1 + 1) \times 10^9$ pulses. More generally, the hardware stability needs to be improved in order to sacrifice a vanishing fraction of symbols. We found that the ratio of 1 offers a good trade-off between the amount of symbols we have to sacrifice (and thus are not used to extract the key) and the stability of our experimental parameters.

7.7 Post-processing Performance

The error-correction is performed using low signal-to-noise ratio (SNR) multi-edge Low Density Parity Check (LDPC) codes [65]. High efficiencies are obtained when operating very close to the maximum amount of noise a code can correct. We achieve speeds up to several Mbits/s [60] using an OpenCL implementation of Belief Propagation with flooding schedule on an AMD Tahiti Graphics Processor Unit (GPU). The huge parallelism provided by GPUs allows to overcome the computational complexity of CVQKD [158].

When several codes are available with the modulation variance V_A in its allowed range (between 1 and 10 shot-noise units on Alice’s side), the one corresponding to the higher key rate is chosen. Puncturing and shortening of LDPC codes allow to modify the rate of a code while maintaining a high efficiency over a wide SNR range. We use a technique [94] that consists in adapting the code rate with the sum of punctured and shortened bits equal to a constant value determined as the maximum number of punctured bits one can use with a given code without any significant efficiency loss (approximately 10% of the code length). This is particularly convenient since the input size of the error correction is constant; only the output size of the corrected key depends on the number of shortened bits. The failure probability of the error correction is roughly 10%. In case of failure, the whole block is discarded, whereas all accepted blocks (9 over 10 on average) are error-less.

Privacy amplification is performed by multiplying by random Toeplitz matrices aggregated corrected key blocks. This can be done very efficiently with input blocks of size 10^9: a throughput above 40 Mbits/s is obtained with one core of a Core i7-920 processor for a rate of 10^{-3} secret key bit per raw key bit.

7.8 Conclusion and Perspectives

To conclude, let us discuss possible further improvements of our implementation. The current repetition rate of 1 MHz can be increased by shortening the pulse duration and the time-multiplexing period, as well as the homodyne detection data sampling period, using high-speed and high-precision data acquisition cards. Current error-correction techniques can deal with raw key rates of up to 10 Mbits/s, and better rates are possible using multiple devices. However, both the sifting procedure and the multidimensional reconciliation scheme require transmitting a large amount of classical data between Alice and Bob, so increasing the optical rate too much would lead to network link saturation. Finally, the ultimate secure distance that can be reached by our system is determined by the excess noise present in the setup. In this respect, recent protocols using “noiseless amplification” [13] or its “virtual” implementation [43, 144] might be promising.

Chapter 8

Increasing the Speed of CVQKD

Contents

8.1 Effect of an imperfect error correction step in QKD . . . 121

8.1.1 Secret key rate and error correction . . . 122

8.1.2 Previous work . . . 124

8.2 Polar codes for QKD: efficiency vs. block sizes 124

8.3 Decoding speed: numerical results . . . 126

8.4 Privacy amplification . . . 128

8.5 Network Bandwidth Consumption . . . 129

8.6 Several Bits per Pulse . . . 130

In this chapter, we are concerned with the speed limitations that affect a CVQKD system. For a long time, post-processing was the bottleneck that limited CVQKD systems speed. In chapter 6, we designed high-efficiency LDPC codes that allowed us to overcome the distance limitation. Here, after emphasizing on the effect of an imperfect error correction step in QKD, we propose the use of polar codes for both DVQKD and CVQKD and compare their decoding speeds on CPUs with LDPC codes ones on both GPUs and CPUs. We also present our speed results as regards privacy amplification. Finally, we consider network bandwidth consumption in a real implementation of a CVQKD system.

8.1 Effect of an imperfect error correction step in QKD

Two families of QKD technologies exist: Discrete Variables QKD and Continuous Variables QKD. In both cases, the transmission of a binary message, the *raw key*, on a quantum noisy channel is at the heart of the protocol. Errors resulting from this transmission have to be corrected for Alice and Bob to be able to compute the same key. The quantum channels of DVQKD and CVQKD have different error distributions: in the DVQKD case, the channel is a BSC whose probability of error is the *Quantum Bit Error Rate* (QBER). For CVQKD, it is a Gaussian channel with both a transmission T, and a Gaussian noise, composed of a quantum noise, the shot noise, and other classical noises which form the excess noise.

When linear, non-interactive, error-correcting codes are used, the error correction algorithm uses the fact that the string sent satisfies some predefined set of linear equations where some linear combinations of message bits, or *parity bits*, are equal to zero. Transmission is therefore preceded by an *encoding step* where the message to be transmitted is transformed into a string that satisfies these equations. However, in the QKD setting, contrary to the usual setup of error-correcting codes, a noiseless classical channel is available alongside the quantum noisy channel. Using this channel, the encoding step can be avoided: the message and the string sent are equal, and the values of the parity bits are revealed on the classical channel. Therefore the performance of the encoding step is not considered in our case.

The limitations the error correction step introduces in the implementation of a QKD system are two-fold. First, the number of raw key bits or linear combination of raw key bits revealed during the error correction step must be subtracted from the final key size during the *privacy amplification* step [111]. Therefore efficient codes, i.e. codes with thresholds close to the Shannon Bound, are needed. Secondly, the throughput of the error-correction, which is usually not high because of the aforementioned efficiency constraints, may limit the final key rate below what is allowed by the optics. On the other hand, cost, power consumption, and latency constraints are much less of an issue than in typical error-correction applications.

We propose to examine the relevance for QKD of a new family of codes, *polar codes*, introduced by Arıkan [8]. Based on our previous discussion, we will look at their distance to Shannon bounds and the decoding speed. For a given block size N and a fixed channel, the polar decoding algorithm is deterministic. Its execution time provably scales in $O(N \log N)$; it also has a simple recursive structure which gives good practical performance. However, we will see that very large blocks are required to achieve the high efficiencies needed for QKD on the BSC or the Binary Input Additive White Gaussian Noise Channel (BIAWGNC).

The next sections are organized as follows: in section 8.1 the impact of the imperfection of the error-correction procedure in both DVQKD and CVQKD is detailed and the previous work is reviewed. In section 8.2 the usage of polar codes to correct errors in a QKD setup is laid out. Finally the performances of polar codes and LDPC codes are compared in section 8.3.

8.1.1 Secret key rate and error correction

Key rate and distance of error correction to Shannon bounds

In a classical DVQKD setup, Alice encodes a classical bit onto the phase or the polarization of a photon and sends this photon to Bob who measures it with a Single Photon Detector (SPD) and gets a bit value. As regards CVQKD, Alice encodes continuous information onto the quadratures of the electromagnetic field and sends weak light pulses to Bob who performs either a homodyne measurement on one single quadrature or a heterodyne measurement on both quadratures. In both cases, Bob ends up with a bit string, like in a DVQKD setup, because of the finite precision of its measurement apparatus. Since this step is repeated many times, Alice and Bob are given two bit strings x and y after the quantum exchange.

The eavesdropper, Eve, has a quantum state E, generally correlated to x and y. If we assume Alice is chosen as the reference for the establishment of a secret key, the maximal secret information shared by Alice and Bob is given by $S(x|E)$, which is the Von Neumann entropy of the variable x conditionally to Eve's knowledge (which is in general quantum). In order to compute an information-theoretic secret key rate, all the information corresponding to the errors between x and y, $H(x|y)$ that is the conditional Shannon entropy of x given y, is assumed to be known by Eve and is subtracted from the final key. Thus the theoretical secret key rate reads:

$$K_{th} = S(x|E) - H(x|y) \tag{8.1}$$

This expression can be rewritten in terms of mutual informations as:

$$K_{th} = I(x:y) - S(x:E) \tag{8.2}$$

According to the information theory, one can never extract the exact amount of mutual information $I(x:y)$ between Alice and Bob with a finite error-correcting code. That is why one introduces a factor β which represents the reconciliation efficiency and ranges from 0 when no information is extracted to 1 in the theoretical perfect reconciliation scheme:

$$K_{real} = \beta I(x:y) - S(x:E) \tag{8.3}$$

Thus an imperfect reconciliation scheme results in a reduction of the secret key rate and a limitation of the range of the protocol. With all known protocols $I(x,y) - S(x:E)$ decreases faster with the distance than $I(x,y)$ and $S(x:E)$ individually, so that the effect of $\beta < 1$ is most severe at large distances. This last effect limited the range of CVQKD protocols for a long time before specific error correcting codes were proposed [70, 65].

Key rate and error correction computation time

Long-range QKD therefore needs error-correcting codes and decoding schemes enabling operation as close to the Shannon limit $\beta = 1$ as possible. However, decoding close to the Shannon limit can be a computationally demanding task; the computation time may then limit the throughput of a QKD experiment. In [83], the raw optical repetition rate is 500 kHz and the raw data rate reduces to 350 kHz because some pulses are used for synchronization purposes and parameters estimation. Since the best reconciliation algorithm available in [83] is limited to about 63 000 symbols per second, only 18% of the available symbols can be used to extract secret keys. More generally, the key rate of a practical system is affected by a factor $\alpha = D_{ECCout}/D_{ECCin}$ where D_{ECCout} stands for the error-correction output rate (63 kb/s in our example) and D_{ECCin} stands for the data output rate of the system used as an input for the error-correction (350 kb/s in our example).

$$K_{sys} = \alpha\left(\beta I(x:y) - S(x:E)\right) \tag{8.4}$$

Key rate and error correction frame error rate

The frame error rate (FER), or the probability for a message to be incorrectly decoded, is usually one of the most regarded characteristics of an error-correcting code, since failure to decode a message is usually associated with data loss in conventional data transmission scenarios, at best causing retransmission delays. However, in the quantum key distribution setting, raw key blocks incorrectly decoded are simply discarded by both the sender and the receiver. As a result, the raw key rate and final key rate are affected by a factor (1 − FER). Frame error rates that are unacceptable in conventional error correction applications are therefore sufficient in the QKD case. Besides, accepting a high FER enables faster error correction. Our target figure in the rest of this article is a FER of 0.1.

Taking into account all the previously discussed imperfections of ECC in the QKD case, the final key rate is

$$K = \alpha(1 - \mathrm{FER})\left(\beta I(x:y) - S(x:E)\right) \tag{8.5}$$

8.1.2 Previous work

Most of the error-correction algorithms designed especially for DVQKD, such as Cascade [16, 26, 134], Winnow [154] or Liu's algorithm [118] suffer latency problems because they are highly interactive. Although the latest ones exhibit less interactivity than Cascade, it remains the algorithm most used in DVQKD experiments because it exhibits an efficiency higher than 96% [32] over the range $[0; 0.11]$ for the error probability of a standard Binary Symmetric Channel (BSC), which is the admissible range for the QBER to distribute a secret in DVQKD. The maximum reported Cascade speed is about 5.5Mb/s with 4 threads on a quad-core processor [119].

Low Density Parity Check (LDPC) codes have also been developed for DVQKD experiments and have efficiencies similar with Cascade over the range $[0; 0.02]$ while they present a significant improvement for bit error rates above 0.02[32]. As regards interactivity, LDPC codes require only one exchange contrary to Cascade which is highly interactive. Since LDPC codes are optimized for a given probability error, puncturing and shortening techniques [35] can be used to extend their efficiency to a wider range and protocols allowing to reconcile information while maintaining a low interactivity have been proposed [33, 34, 93]. However, high-efficiency LDPC error-correction speed has not been investigated a lot except for CVQKD where the authors of [83] report a 40kb/s speed on CPU and a 60kb/s speed on GPU.

Modern coding techniques have mainly been used for continuous variables with Turbo-codes or LDPC codes. The main difficulty as regards continuous variables is that the best protocols known require a Gaussian modulation while the noise added by the channel is Gaussian too. Thus, one has to deal with an Additive White Gaussian Noise Channel (AWGNC) and high-efficiency error-correction is particularly hard at low Signal to Noise Ratios (SNRs) which correspond to a long operating distance for CVQKD. However, in [70], the authors proposed a technique allowing to encode the information in binary variables which allows us to deal with a Binary Input (BI) AWGNC instead of the usual AWGNC. Low-rate high-efficiency multi-edge LDPC codes can be designed for this channel [65, 113] which results in a considerably extended achievable distance for CVQKD with a Gaussian modulation.

8.2 Polar codes for QKD: efficiency vs. block sizes

The use of polar codes has been previously considered for other scenarii. In [90], the authors show that the secrecy capacity of classical wiretap channels can be achieved using polar codes. This work was extended to quantum wiretap channels with a classical eavesdropper in [151]. In [110], polar codes are used to transmit quantum information and an efficient decoder is provided for both Pauli channels and erasure channels. In [52], it is shown that the Holevo capacity of lossy optical channels can be achieved with polar codes but an implementation of a quantum successive cancellation decoder is far beyond what can be experimentally realized today with quantum states.

The QKD and wiretap channel scenarii are nevertheless different: in QKD, Alice and Bob's correlations are directly used to compute an upper bound on Eve's information without making any assumption on the channel between Alice and Eve, whereas in the wiretap channel scenario, the channel between Alice and Eve is assumed to be characterized.

Polar codes exhibit some specificities that make them suitable for QKD error correction. First, they are easily employed in a rateless setup where the noise of the channel can change over time. Secondly, they enable non-interactive error correction, similarly to LDPC codes, and contrary to two-way protocols like Cascade. In this section, we evaluate the block sizes needed to obtain the efficiencies required for QKD. This impacts the decoding throughputs that can be obtained in practical implementations.

In polar codes, individual copies of symmetric Binary Discrete Memoryless Channels (BDMC) are combined recursively in order to form a new set of channels composed of more and more differentiated channels, such that in the asymptotic limit channels are either error-free or completely noisy, with a fraction of error-free channels equal to the code capacity. This phenomenon is called channel polarization: each channel becomes either noiseless or noisy as the block length goes to infinity. In the asymptotic limit, the capacity of the BDMC can be achieved by sending the information bits through the noiseless channels, while in practice, only a fraction of this capacity is achieved using the bits with almost zero error probability for finite block lengths. The convergence speed of channels into noiseless or noisy channels is called polarization speed.

We used the polar codes construction method described in [92] to compute the decoding error probabilities on symmetric binary memoryless channels for the BSC and the BIAWGNC. For a given noise level on a given channel, Density Evolution allows us to compute the capacities of the different bits of the code. Some of the bits corresponding to channels with lowest capacities are simply revealed and are called the frozen bits of the code. As explained in [92], this selection rule for frozen bits also gives us an upper bound on the decoding error probability of a block (also called the Frame Error Rate or FER). Since in QKD it is not crucial to lose some blocks (they will just be thrown away at the verification step), we select sets of frozen bits that give an upper bound of 0.1 on the FER. It appears that the polarization speed is highly dependent on the channel for polar codes [67]. Figure 8.1 gives the polarization speed we obtained for the BSC. It shows that polar codes have an efficiency above 95% over almost the entire probability error range $[0; 0.11]$, which is the range of interest in DVQKD, for block lengths starting from 2^{24}. Even smaller block lengths can be used if one does not need to cover the entire probability error range. The situation is definitely worse in Figure 8.2 for CVQKD. We studied the polarization speed for the SNRs described in [65] because high efficiency multi-edge LDPC codes have been designed to deal with such noise levels [65, 113]. The results show that

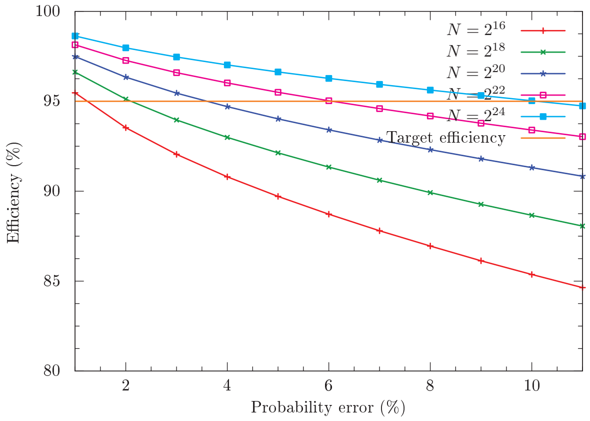


Figure 8.1: Polar codes efficiency for the BSC for probability errors from 1% to 11% with a 1% step. The method described in [92] is used to compute the capacities of each channel for a given noise level and the frozen bits are chosen in order to upper bound the FER by 0.1 according to this method. From the bottom to the top we used the following block sizes: 2^{16}, 2^{18}, 2^{20}, 2^{22}, 2^{24}. We can see that the efficiency is higher than the target efficiency of 95% over almost the entire range for block sizes equal to 2^{24}.

Channel	QBER / SNR	Size	β	Speed (Mb/s)	FER
BSC	2.0%	2^{16}	93.5%	10.9	0.09
BSC	2.0%	2^{20}	96.3%	9.5	0.11
BSC	2.0%	2^{24}	98.0%	8.3	0.08
BIAWGNC	1.097	2^{24}	95.2%	8.0	0.10
BIAWGNC	0.161	2^{27}	92.8%	7.3	0.09

Table 8.1: The efficiencies correspond to a block error rate of 0.1 when selecting the frozen bits according to the method described in [92]. These figures were obtained with one core of an Intel Core i5 670 3.47GHz processor.

only a 90% efficiency can be achieved with polar codes for blocks of size 2^{27} whereas efficiencies of about 95% are achieved in [65] with LDPC codes. However long distance CVQKD is still possible using polar codes. Furthermore, there is still some hope to improve the polarization speed for polar codes for the BIAWGNC, for example by changing the recursive method used to combine channels, as proposed in [97].

8.3 Decoding speed: numerical results

An interesting feature of polar codes is their regular recursive structure. This allows us to implement a recursive, successive-cancellation decoder that achieves a speed of about 10Mb/s on modern CPUs (Intel Core i5 670 3.47 GHz in the simulations). The main optimization in this decoder is to use fixed-point arithmetic and a table-lookup implementation of the function $\varphi(x) = \log(\tanh(x/2))$ used to update log-likelihood ratios (LLRs). Other techniques have been proposed for efficient polar codes decoding and could improve the decoding speeds given in Table 8.1: in [157], the authors propose look-ahead techniques that allow to reduce the decoding latency of successive cancellation by 50% while in [138, 79, 20], some variants of list decoding for polar codes are introduced.

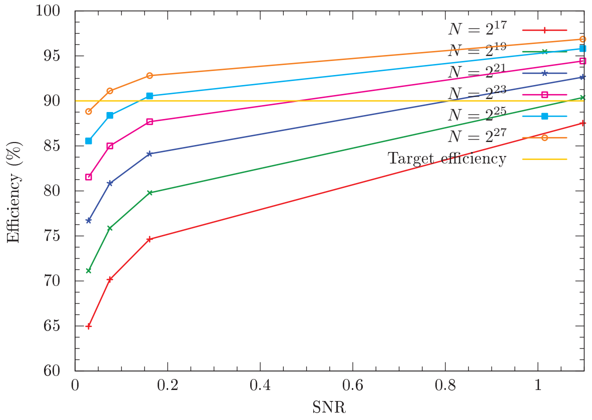


Figure 8.2: Polar codes efficiency for the AWGNC for the SNRs 1.097, 0.161, 0.075, 0.029 from [65]. The method described in [92] is used to compute the capacities of each channel for a given noise level and the frozen bits are chosen in order to bound the FER by 0.1 according to this method. From the bottom to the top we used the following block sizes: 2^{17}, 2^{19}, 2^{21}, 2^{23}, 2^{25}, 2^{27}. We can see that the efficiency is higher than the target efficiency of 90% over almost the entire range for block sizes equal to 2^{27}.

Channel	QBER / SNR	Size	β	Speed (Mb/s)	FER
BSC	2.0%	2^{17}	92.9%	7.3	0.01
BIAWGNC	1.097	2^{20}	96.9%	6.5	0.09
BIAWGNC	0.161	2^{20}	93.1%	7.1	0.04

Table 8.2: LDPC codes decoding speeds with LDPC codes described in [32] for the BSC and in [113] for the BIAWGNC. The maximum number of iterations was fixed to 20 for the first code, and respectively to 160 and 100 for the next two codes. These figures were obtained with an AMD Tahiti Graphics Processor.

The polar decoding performance has to be compared with the speed of a LDPC decoder based on BP. The speed of such a decoder dramatically lowers when approaching the capacity of the code used because BP requires more iterations to converge. Thus LDPC decoding speed is limited to about 800kb/s using one core of a modern CPU. The LDPC CPU decoder uses fixed-point arithmetic and the same implementation of φ as in the polar code case. It is a shuffle decoder with an early termination strategy where bits are considered to be known (and their LLR ceases to be updated) when the absolute value of their LLR passes a threshold; when no bit is updated for a sufficient number of iterations, decoding is considered to be over and is stopped. Because the regime explored is close to the Shannon limit, simplified BP algorithms such as min-sum or its variants cannot be used. Finally, the maximum number of iterations is controlled to adjust the FER to the target value 0.1. This control is imprecise however, since small variations of the maximum allowed number of iterations result in large FER changes. The maximum number of iterations used for LDPC codes are given in Table 8.2 and Table 8.3 legends.

GPUs provide a huge amount of parallelism that allows us to achieve speeds of 10Mb/s (figures are given for an AMD Tahiti Graphics Processor). The GPU LDPC decoder is different from the CPU implementation:

Channel	QBER / SNR	Size	β	Speed (Mb/s)	FER
BSC	2.0%	2^{17}	93.1%	0.82	0.03
BIAWGNC	1.097	2^{20}	96.9%	0.09	0.03
BIAWGNC	0.161	2^{20}	93.1%	0.12	0.04

Table 8.3: LDPC codes decoding speeds with LDPC codes described in [32] for the BSC and in [113] for the BIAWGNC. The maximum number of iterations was fixed to 15 for the first code, and respectively to 100 and 50 for the next two codes. These figures were obtained with one core of an Intel Core i5 670 3.47GHz processor.

it is a floating-point, flood decoder running in a fixed number of iterations and using both 'external' parallelism (several vectors are decoded concurrently) and 'internal' parallelism (for a single BP execution corresponding to one message being decoded, several messages are propagated concurrently). This was experimentally found to be optimal on GPU architectures because they have much more floating point computational power than CPUs, but are slowed down by complex control logic. No competitive GPU decoder for polar codes was implemented, as successive cancellation is inherently sequential, and therefore only external parallelism can be used.

Table 8.1 gives the decoding speeds obtained with polar codes for the BSC and the BIAWGNC for characteristic noise levels in DVQKD and CVQKD. Table 8.3 and Table 8.2 give the corresponding speeds with LDPC codes respectively with a GPU and a CPU.

8.4 Privacy amplification

Privacy amplification allows to extract a secret bit string from the identical correlated bit strings shared by Alice and Bob after the error-correction step. This step cannot be done with a single function without revealing some information about the output string. This is why Alice and Bob must consider families of hashing functions and use a new function for each key extraction. A hashing functions family is *universal* if for any couple of input messages B_1 and B_2, the collision probability $f(B_1) = f(B_2)$ is bounded by 2^{-k} where k is the size of the output message. It appears that the multiplication of binary vector by a random binary matrix is a universal hashing function. However, a generic matrix-vector multiplication is not very efficient computationally and describing a generic $n \times k$ matrix requires nk binary coefficients, which costs both random numbers and network bandwidth.

We implemented the universal hashing function "multiplication by a random Toeplitz matrix". Such $n \times k$ matrices are described by only $n + k - 1$ coefficients and feature a structure that allows for high speed implementation on modern CPUs. We give in Figure 8.3 our throughput results for different input and output sizes. The obtained speeds range from tens to hundreds of Mbits per second on one core of CPU, which clearly demonstrates that privacy amplification is not a limiting factor for CVQKD.

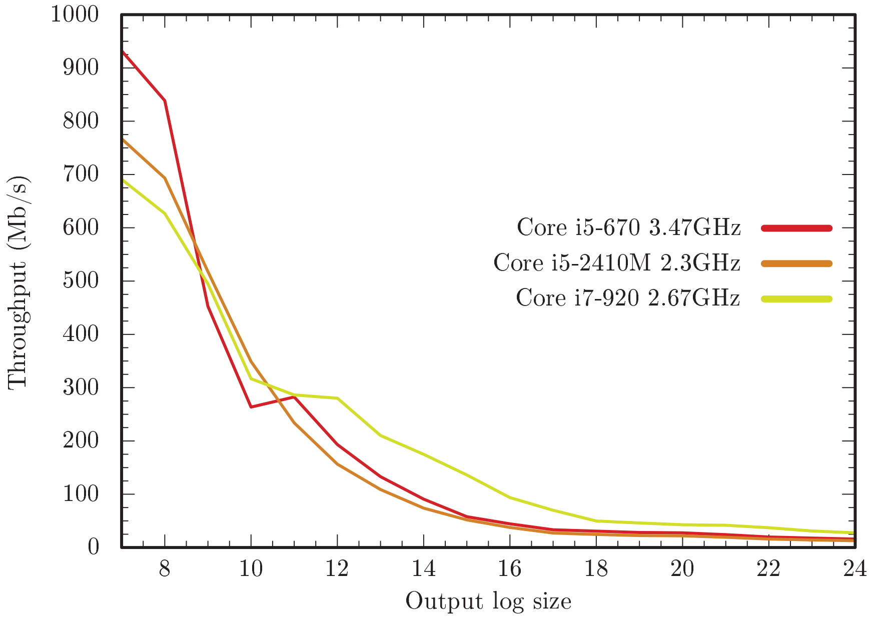


Figure 8.3: Privacy amplification performance on recent CPUs for the implementation of the universal hash family ”multiplication by a random Toeplitz matrix”.

8.5 Network Bandwidth Consumption

Network bandwidth might become a limiting resource in future implementations of CVQKD. Indeed, dealing with continuous variables requires to encode continuous data in potentially long bit strings. We recall in this section the size of the different messages that are exchanged in our CVQKD protocol. All these values are summarized in table 8.4:

- synchronization step: Alice modulates blocks of size 2^{16} that are sent through the quantum channel. Bob has to find Alice’s pulses numeration in order to compute statistics such as the correlation between their respective data. For each received block where he detected the synchronization pattern, Bob sends the index of the beginning of the received pulses to Alice. It is a number encoded on 64 bits. Alice tells Bob if he must keep or discard this data block.
- sifting step: for each modulated pulse Alice reveals one of the modulated quadratures to Bob, which is encoded into 1 bit, and reveals the 12 bits used for the modulation of the revealed quadrature. Bob replies with an estimation of the signal-to-noise ratio, which is a float of 32 bits. At this stage they work with blocks of 2^{20} bits since this size allows for a high-efficiency error-correction.
- error-correction step: Bob sends to Alice a set of parity check equations (the syndrome), whose size depends on the rate of the selected code and thus on the observed signal-to-noise ratio. Since we are using the multidimensional protocol for the reconciliation, a real value must be revealed for each measured pulse. However, since our measured values are encoded into 12 bits, we reveal 12 bits per measured value for the multidimensional protocol. Bob also sends a hashed value of his reference string. After having performed the decoding step, Alice computes her own hash of her corrected string and compares it with

Protocol Step	Size	A to B (bits)	B to A (bits)
Synchronization	2^{16}	1	2^6
Sifting	2^{20}	$2^{20} \times (12+1)$	2^5
Error Correction	2^{20}	1	$2^{20} \times ((1-R)+12)+2^4$
Privacy Amplification	2^{24}	1	$2^{24} \times (1+K)+2^6$
Final Key	$2^{24} \times K$	-	-

Table 8.4: Network traffic for the Gaussian CVQKD protocol used in Cygnus.

the received hash. She then sends to Bob 1 bit of information that corresponds to the success or the failure of the error-correction.

– privacy amplification: in order to have a limited uncertainty on the transmission parameters and therefore a high value of the secret key rate, Alice and Bob perform this step over large blocks of size 2^{24}. Bob draws a random Toeplitz matrix and send it to Alice. The number of bits used to describe such a matrix depends on the number of secret bits Alice and Bob can extract from their data. After having applied this compression function to his data, Bob send the first 64 bits of this string to Alice together with the matrix description. Then, Alice applies this same function to her data and compares the first 64 bits of her hashed string with the hash received from Bob. She finally announces the success or the failure of the key distillation to Bob.

8.6 Several Bits per Pulse

When the first continuous variable protocols were designed, the main selling point of these protocols was that CVQKD should feature higher secret key rates than DVQKD because of the possibility to extract several bits per pulse. In this thesis, we mainly focused on the extraction of secret keys at long distances, i.e. with signal to noise ratios lower than 1. In such regimes it is not possible to extract more than one bit per pulse. Furthermore, in the meantime, single photon dectectors operating at GHz frequencies were developed, which allowed DVQKD laboratory systems to demonstrate secret key rates up to 1 Mb/s [30], which is still higher than the best key rates reported using CVQKD.

We believe that CVQKD can obtain secret key rates up to a few Mb/s and compare favorably with DVQKD at short distances. This should be possible using error-correction procedures like *Slice Reconciliation*, which was proposed in [143, 14] and implemented in [83, 44], and GPU decoding as proposed in this chapter. Note that the repetition rate of CVQKD can also be increased if low noise balanced homodyne detectors are available [21].

Chapter 9

Integration of CVQKD in Optical Networks

Contents

9.1 QKD and Network Infrastructures 131

9.2 SEQURE demonstration field test 134

9.2.1 Structure of the demonstration 134

9.2.2 The quantum layer 136

9.3 Security considerations 138

9.4 Performance of the quantum layer 139

9.4.1 Events 139

9.4.2 Excess noise 139

9.4.3 Secret key rate 142

9.5 Performance of the encryption layer 142

9.6 SEQURE Demonstration Conclusion and Perspectives 142

9.7 Analysis of the Noise Contributions in a WDM Setup 143

9.7.1 Leakage from Classical Channels 144

9.7.2 Four-wave Mixing 145

9.7.3 Spontaneous Anti-Stokes Raman Scattering 145

9.8 Noise Photons in Local Oscillator Matched Mode 145

9.9 Experimental Results 146

9.10 Concluding Remarks 147

In this chapter, we consider the use of CVQKD as a practical security primitive in current network architectures. First, we demonstrate the combination of CVQKD and classical symmetric encryptors within a long-term point-to-point field deployment where two fibers are used, one for the classical traffic, the other for the quantum channel. Second, we overcome the dark fiber limitation of CVQKD and demonstrate possible coexistence of a quantum channel with intense DWDM channels.

9.1 QKD and Network Infrastructures

Quantum Key Distribution (QKD) [120] is among the first industrial applications of the field of quantum information processing. Its natural commercial target is network security, since this technology allows two distant parties to share a secret key through the exchange of quantum states even in the presence of an eavesdropper, provided that the parties share an auxiliary authenticated classical communication channel. Contrary to all known classical schemes, the security of the established key can be proven without making any assumption on the capacities of the eavesdropper (for example computational power, knowledge of efficient algorithms, amount of memory). In theory, this key can be combined with an information-theoretically secure encryption method, the one-time pad (OTP), which requires a key that has to be as long as the message. However, the latest long-term field demonstrations, the Tokyo QKD network [119] and the SwissQuantum network [132], report a secret key rate lower than 1 Mbit/s, which makes OTP incompatible with most of practical applications that require key rates above 1 Gbit/s. If high bit rates are required, a practical solution is to use the keys issued from QKD to renew keys used in classical symmetric algorithms like the FIPS Advanced Encryption Standard (AES) [41]. Since each QKD key is completely independent of keys generated earlier, renewing keys forces an attacker to perform a new attack to obtain the key after each renewal. This *forward secrecy* property cannot be achieved with classical symmetric schemes. It can, however, be achieved with classical asymmetric schemes but only under some complexity assumptions [68, 57].

In order to become an essential part of current network infrastructures, QKD systems have to pass integrability and reliability tests. Systems that rely on encoding the information on discrete variables, such as the phase or the polarization of single photons, have been widely tested. Commercial products based on such systems have been developed by ID Quantique [2] and MagiQ Technologies [3]. AES key renewal was demonstrated in [37], where the ID Quantique QKD system was combined with an AES-based encryptor allowing to encrypt 1 Gbit/s communications, while the long-term reliability of this technology was tackled in [132]. In comparison with QKD based on discrete variables, continuous-variable QKD (CVQKD), relies on encoding the information on continuous variables such as the quadratures of coherent states [50], that has been implemented in a great variety of situations [49, 69, 85, 83, 139, 107, 136, 44, 36, 28, 135, 126] (for a review of quantum information with continuous variables see [148]). This has important practical advantages: the homodyne detection hardware does not require any specific component, such as actively cooled single-photon detectors, and exhibits a better compatibility with a Wavelength Division Multiplexing (WDM) environment [106]. As recently created companies, Quintessence Labs [4] and SeQureNet [5], pursue the development of a new generation of CVQKD technologies, it is imperative to demonstrate the integrability and reliability of CVQKD in a long-term field deployment.

We report here on the design and performances of the *Symmetric Encryption with QUantum key REnewal* (SEQURE) project demonstration. In the context of this project, a point-to-point classical symmetric encryption link using keys provided by a CVQKD system was installed in a production environment and ran during six months. This is the first demonstration of the long-term stability of CVQKD.

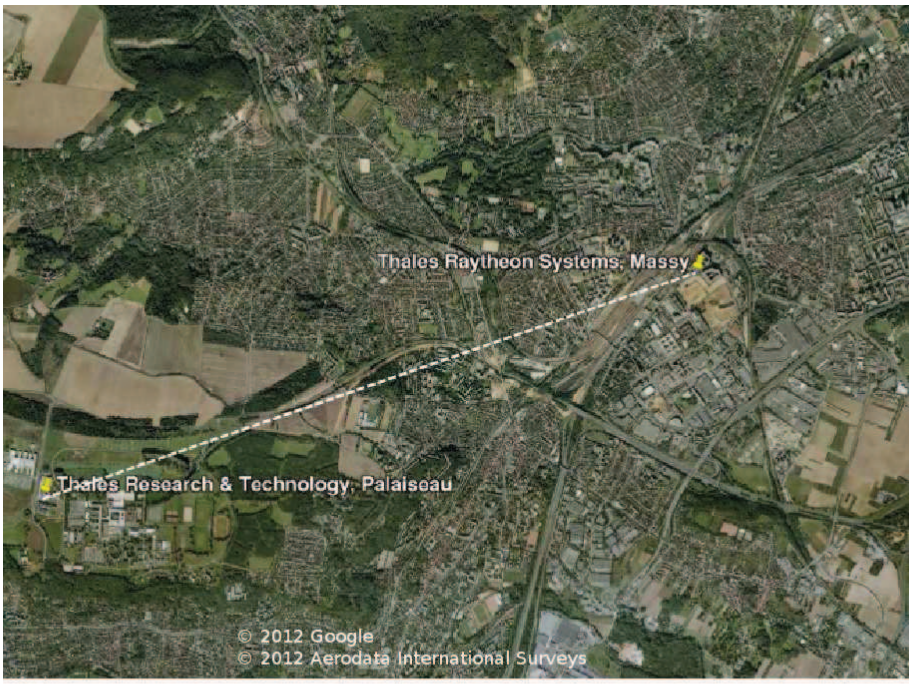

Thales Raytheon Systems, Massy
Thales Research & Technology, Palaiseau
© 2012 Google
© 2012 Aerodata International Surveys

Figure 9.1: Map of the SEQURE demonstration. The two nodes are located in the cities of Massy and Palaiseau in the southwest of Paris. The dashed line shows the 5 km straight path between the two sites, whereas the actual length of the fiber is 17.7 km. ©Google Maps – 2012

Table 9.1: SEQURE demonstration link characteristics.

Length of fibre (km)	Optical loss (dB)
17.7	5.6

9.2 SEQURE demonstration field test

9.2.1 Structure of the demonstration

We first discuss several important features of the SEQURE demonstration. The demonstration involves two nodes located in:

- Palaiseau (Thales Research & Technology France)
- Massy (Thales Raytheon Systems)

The characteristics of the link are summarized in table 9.1 and a map is given in Fig. 9.1. For the generation and management of the secret keys, we used the layered architecture (see Fig. 9.2) that was employed in the SECOQC FP6 European project network [104]. Note that the Tokyo QKD network [119] and the SwissQuantum network [132] also used the same architecture. Its main feature is that a layer of abstraction, the key management layer, is added between the physical medium used for the QKD and the application layer that uses the produced keys to secure classical communications. Then, it is straightforward to replace a QKD technology with another and, in our case, to extend the SEQURE demonstration point-to-point setup to a multipoint configuration.

In more detail, the SEQURE demonstration layers are the following:

- a quantum layer implemented with a CVQKD point-to-point link (developed jointly by Thales Research & Technology and Institut d'Optique/CNRS [83, 44])
- a key management layer allowing to authenticate the reconciliation traffic of the quantum layer and to provide symmetric keys to the application layer (this software [1] was developed by the Austrian Institute of Technology (AIT, formerly Austrian Research Center ARC) during the SECOQC project [104])
- an application layer where the keys coming from the key management layer are used by end users to encrypt their communications with a classical symmetric encryptor Mistral Gigabit (developed by Thales Communications)

The physical layer of the link is composed of one pair of dark fibres. One fibre is used as a quantum channel (note that in a CVQKD system there are two time-multiplexed physical channels on the optical fibre since a classical signal, namely the local oscillator, is transmitted on the same fiber as the quantum signal) and the other one is used to transmit all the classical channels. In the SEQURE demonstration there were several types of classical channels:

- the channel for the reconciliation protocol of the QKD system
- the channel for cryptographic applications
- the channel for the monitoring of all the devices

A diagram of the components of the system is shown in Fig. 9.3.

Since all the above classical channels need to operate in both directions, they are multiplexed using WDM techniques. The wavelengths used are 1490nm (uplink) and 1310nm (downlink). Standard GigaBit Interface Converters (GBIC) were used to convert Ethernet optical signals propagating in fibres into Ethernet electric signals propagating in copper cables. The

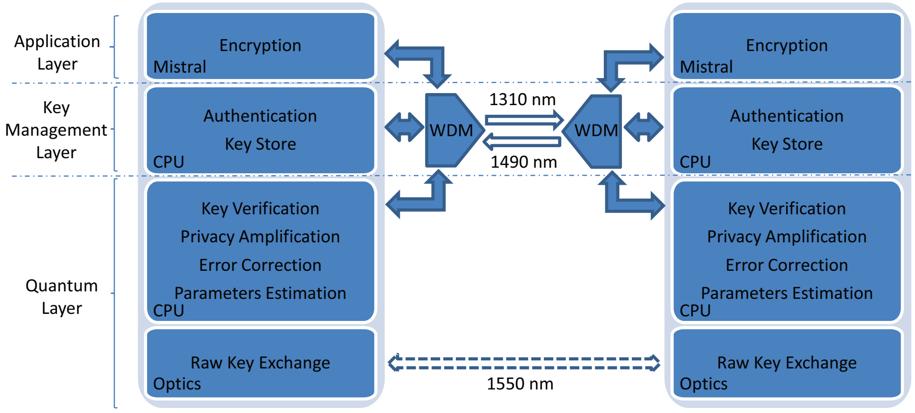


Figure 9.2: Layer structure of the SEQURE demonstration. The dashed bidirectional arrow represents the fibre used for the Local Oscillator (LO) and the quantum signal, while the plain arrow stands for the wavelength multiplexed classical signals: the reconciliation part of the CVQKD, the key management layer and the encrypted traffic.

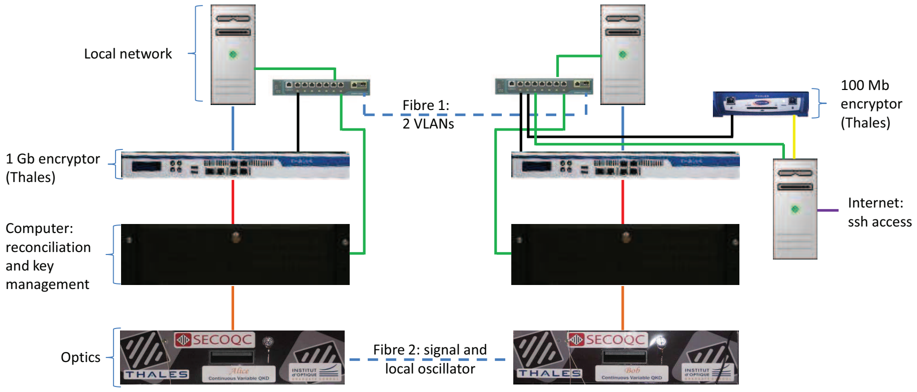

Local network
1 Gb encryptor (Thales)
Computer: reconciliation and key management
Optics
Fibre 1: 2 VLANs
Fibre 2: signal and local oscillator
100 Mb encryptor (Thales)
Internet: ssh access
SECOQC
THALES

Figure 9.3: Structure of the SEQURE demonstration. The dashed lines correspond to the two fibres. Fibre 1 is used for multiplexed classical communications, fibre 2 transmits the physical pulses that are used to establish the raw key. The colors correspond to the different types of traffic: blue is plain text, black is the encrypted traffic VLAN, red is key renewal, orange is optics control and raw key traffic, yellow is the control of Mistral products configuration, purple is the Internet link, green is the monitoring traffic VLAN.

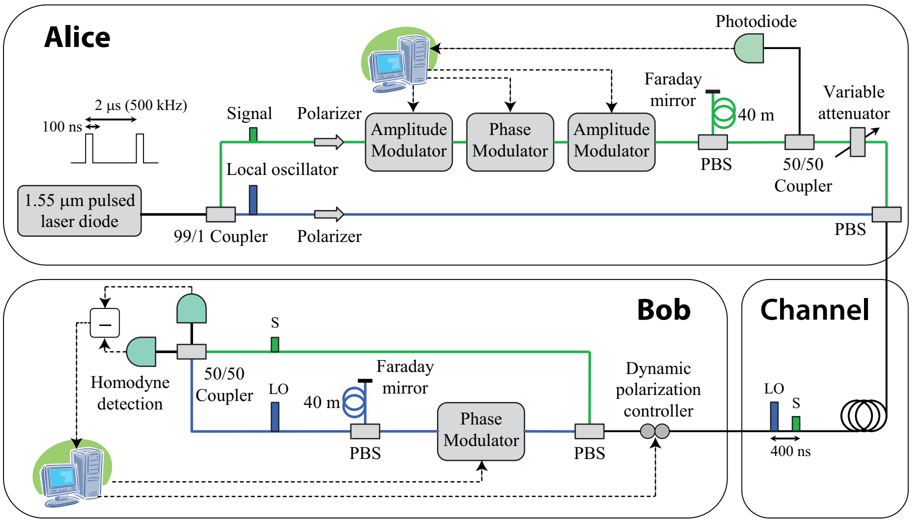


Figure 9.4: Optical layout of the CVQKD prototype. Alice sends to Bob 100 ns coherent light pulses generated by a 1550 nm telecoms laser diode pulsed with a frequency of 500 kHz. These pulses are split into a weak signal and a strong local oscillator (LO) with an unbalanced coupler. The signal pulse is modulated with a centered Gaussian distribution using an amplitude and a phase modulator. The variance is controlled using a coarse variable attenuator and a finely tuned amplitude modulator. The signal pulse is 400 ns delayed with respect to the LO pulse using a 40 m delay line and a Faraday mirror. Both pulses are multiplexed with orthogonal polarization using a polarizing beamsplitter (PBS). The time and polarization multiplexed pulses are then sent through the channel. They are demultiplexed on Bob's side with another PBS combined with active polarization control. A second delay line on Bob's side allows for time superposition of signal and LO pulses. After demultiplexing, the signal and LO interfere on a shot-noise limited balanced pulsed homodyne detector. A phase modulator on the LO path allows for random choice of the measured signal quadrature.

optical fibres carrying the classical channels exhibited significant losses in the L-band; therefore Small Form-Pluggable (SFP or Mini-GBIC) modules specified for a 40-km link (Prolabs GLC-BX-D/U) were used. These modules were inserted into 8-port Cisco switches (WS-C2960G-8TC-L) with one dual port. The different classical channels were realized using only one classical link and multiplexing via Virtual Local Area Networks (VLANs). One VLAN is used for the reconciliation and the encrypted traffic, another VLAN is used to monitor all the devices.

The VLAN developed to monitor the demonstration was connected to a Management Center located in Thales Research & Technology in Palaiseau. Remote accessibility to this management center was provided by secure shell (ssh) connections allowed only for legitimate users.

In case of power cuts, rack-mounted remote-control power switches (ePowerSwitch) could be used. They provide a secure web server interface allowing to switch on and off specific devices.

9.2.2 The quantum layer

The quantum link is composed of a pair of optical devices, whose hardware description is given in Fig. 9.4. This is a one-way implementation, where Alice sends to Bob 100 ns coherent light pulses generated by a 1550 nm telecoms laser diode pulsed at a frequency of 500 kHz. These pulses are split into a weak signal and a strong local oscillator (LO) with an unbalanced coupler. The implemented protocol uses Gaussian modulation of coherent states [50]: the signal is randomly modulated following a centred Gaussian modulation in both quadratures, using an amplitude and a phase modulator. The random numbers used for this modulation are provided by Quantis, a physical Random Number Generator (RNG) from ID Quantique [2]. The signal pulses are then attenuated roughly by a variable attenuator and finely by a second amplitude modulator, allowing to control the variance of the Gaussian distribution exiting Alice's device.

The signal and LO are then transmitted through the optical fiber without overlap using time and polarization multiplexing. One 400 ns delay line, composed of a 40-m single-mode fibre followed by a Faraday mirror, is inserted into Alice's signal path for the time multiplexing. Polarization multiplexing is achieved by a polarization beam splitter (PBS) on Alice side. Both pulses propagate through the fibre with orthogonal polarizations and a 400 ns time delay. They are demultiplexed on Bob's side with another PBS combined with active polarization control. A second delay line on Bob's side allows for time superposition of signal and LO pulses.

After demultiplexing, the signal and LO interfere on a shot-noise limited balanced pulsed homodyne detector (HD). The electric signal coming from the HD is proportional to the signal quadrature X_ϕ, where ϕ is the relative phase between the signal and the LO. Following the protocol, by applying a $\pi/2$ phase shift, the phase modulator on Bob's LO path allows one to measure randomly either X_0 or $X_{\pi/2}$.

Finally, feedback controls are implemented to allow for a stable operation of the system over several months. Polarization drifts occurring in the quantum channel are corrected using a dynamic polarization controller that finds an optimal polarization state at the output of the channel. Temperature drifts affect lithium niobate, the active material used in the amplitude and phase modulators, therefore the voltages that need to be applied to reach the target modulation vary with temperature. The photodiode on Alice's signal path is used for the feedback control of the amplitude modulators while the HD output is sensitive to phase and can be used to control the phase modulators.

It is important to note that the Gaussian modulation used in the implemented protocol [50] maximizes the mutual information between Alice and Bob, thus offering an optimal theoretical key rate against either individual [49] or collective [46, 99] attacks. However, it is hard to reconcile correlated Gaussian variables with low signal-to-noise ratios (SNRs). The limited efficiency of the error-correcting codes (typically 0.90 bit extracted per bit theoretically available) results in a limit of the secure distance in the order of 30 km in our case. However, new ideas have been proposed [70] and recently combined with new error-correcting codes [65] to increase the secret bit rate and secure distance, still keeping the Gaussian modulation which has presently the most robust security proofs [46, 99].

With respect to the classical communication, four steps are required (see Fig. 9.2). First, a Parameter Estimation (PE) step is needed to compute estimates of the physical parameters linked to the exchange of quantum states through the quantum channel. These parameters are the modulation variance V_A, the transmission of the quantum channel T, and the excess noise

ξ. Half of the raw key data is chosen at random and revealed to perform PE over blocks of 50 000 measures. For some measured transmission and excess noise the modulation variance V_A is adjusted in order to optimize the secret key rate for a set of pairs (SNR, β) (where SNR is the Signal to Noise Ratio and β is the efficiency of the error-correction procedure) corresponding to the set of available error-correcting codes [83]. The other parameters used to compute an estimate of the secret information that can be extracted from the shared data, the electronic noise v_{el} and the efficiency of the homodyne detection η, are measured during a calibration procedure that takes place before the deployment of the system and that is assumed to be performed in a secure environment. For the SEQURE demonstration, the second step, which is the error correction procedure, was based on a multilevel reconciliation algorithm using Low Density Parity Check Codes (LDPC). This data reconciliation algorithm is explained in detail in [83]. The amount of data revealed during this step is subtracted from the secret information previously computed. The privacy amplification step described in [83] allows us to extract the secret information from the identical strings shared by Alice and Bob after the error correction procedure. Finally, a key verification step ensures with an overwhelming probability (10^{-60}) that Alice and Bob secret keys are identical. This is simply done by revealing a small part of the final bits (200 bits) chosen at random.

9.3 Security considerations

The authentication of the classical channel needed for the QKD protocol is performed by the cryptographic engine provided by the AIT software. A point-to-point authenticated channel is created by the Q3P protocol. It is based on the Wegman-Carter scheme [150, 149]. This authentication protocol, like other QKD implementations, requires an initial common secret. The key consumption of the authentication is roughly 10 bits/s [104], that is about 2% of the secret key rate produced by our system.

As for other families of QKD systems, some attacks can be implemented on a CVQKD system exploiting the imperfections of the setup. For example, the presence of excess noise, which is noise in excess of the shot noise, opens the possibility for partial intercept-resend attacks as demonstrated in [82]. This is why the shot noise level on the receiver side must be precisely known. Monitoring the physical parameters of the channel allows to upper-bound the information available to Eve. An efficient way to perform quantum hacking (see [120]) on a QKD system consists in exploiting side-channels. In our setup, a linear relationship between the LO level and the shot noise is determined during the system calibration. Then the LO level is continuously monitored with one photodiode of the HD and the shot noise level is computed with the help of the previously calibrated relationship. It is used to convert in shot noise units all the physical quantities needed to compute the amount of generated secret data. Generally, the LO, which is a classical signal that can be manipulated by an eavesdropper, is a potential vulnerability [38, 53]. Monitoring the LO level is a counter-measure to such attacks. This monitoring should be good enough so that any undesired change in the shot noise variance is below the measured excess noise variance, of order 1% of the shot noise. Since the shot noise variance is proportional to the LO intensity, this intensity has to be monitored with a slightly better accuracy, for example 0.1%. More details on that monitoring are given in references [38, 53].

9.4 Performance of the quantum layer

9.4.1 Events

The system was stable and ran continuously during more than 6 months, from the end of July 2010 to the beginning of February 2011. The optical part did not require any human intervention during the full period of the demonstration. We list below the most significant problems experienced during the demonstration:

- September 23 to September 29: the motherboard of Alice's computer in Massy failed and had to be changed (these two dates correspond to the two first marks on Fig. 9.5 and Fig. 9.6). Error correction is the most demanding task in terms of computing power and is performed on Alice's side.
- October 1 to October 31: the server room in Massy (Alice's side) was unavailable so the experiment had to be interrupted until it was started again in a new location (these two dates correspond to the two last marks on Fig. 9.5 and Fig. 9.6).
- November 1: the system was restarted but the experimental conditions became continuously changing because of a lack of thermal regulation. However, the results could still be exploited.

9.4.2 Excess noise

The excess noise was recorded during the full period of the experiment and is reported in Fig. 9.5. On a daily scale, it is subject to variations linked to statistical fluctuations and experimental conditions like fibre vibrations. Since our detection scheme relies on an interferometer, phase noise in the transmission creates excess noise. Most of the low frequency phase noise is eliminated by constantly tracking the phase. However, this tracking cannot be done with a perfect accuracy and the high frequency part of the phase noise causes excess noise. Keys are mainly produced with low values of the excess noise, while no keys are produced on blocks with a large excess noise because of the limited efficiency of the error correction scheme (about 90%, see [83]). The system operation was rather stable during the 6 months but we can notice a significant difference in performance when the experiment at one site was transferred from the server room to the room with no thermal regulation. In fact, the excess noise obtained with the equipment in these degraded experimental conditions does not allow to obtain a positive secret key rate against collective attacks for the line transmission [46, 99]. As a result, a secret key rate against individual attacks [49] only was produced by the system during the second part of the demonstration. This illustrates the importance of monitoring continuously the excess noise in order to evaluate the security of the keys [82]. It is important to note that this kind of problem is typical of an external environment and would not occur in laboratory conditions. Our system was still able to produce keys in those degraded conditions, although with an inferior performance. This illustrates the maturity of our setup.

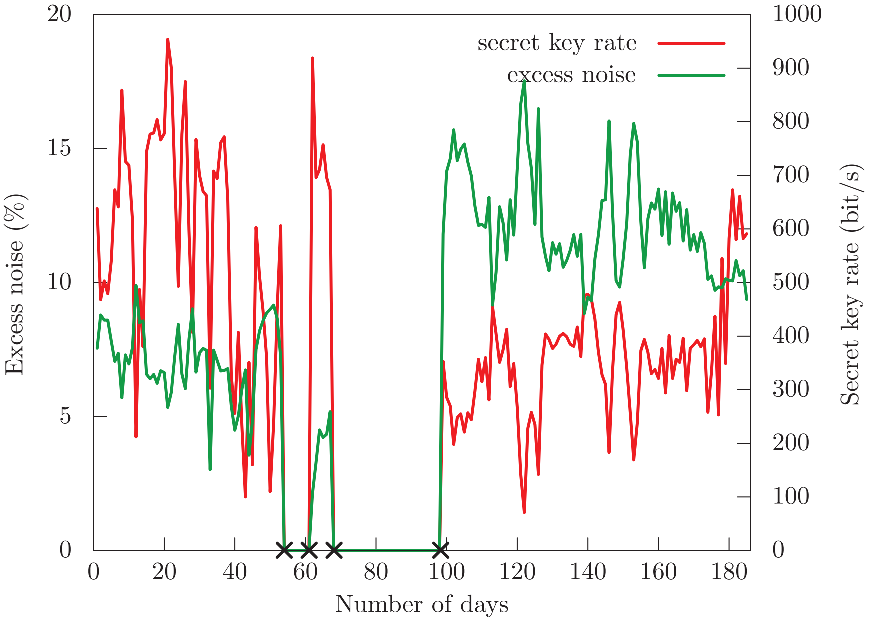


Figure 9.5: Secret key rate and excess noise during the SEQURE demonstration. In red, the secret key rate produced during the SEQURE demonstration. The given secret key rate corresponds to the key rate produced by the system after key distillation and privacy amplification assuming an eavesdropper able to perform collective attacks in the first part and limited to individual attacks in the second part. In green, the measured excess noise during the SEQURE demonstration. During the first part (server room), this excess noise can be mainly attributed to the acoustic noise in the server room. In the second part, an additional excess noise occurred, that is attributed to thermal fluctuations due to the lack of thermal regulation in the room. The black marks correspond to the events listed in the section 9.4.1.

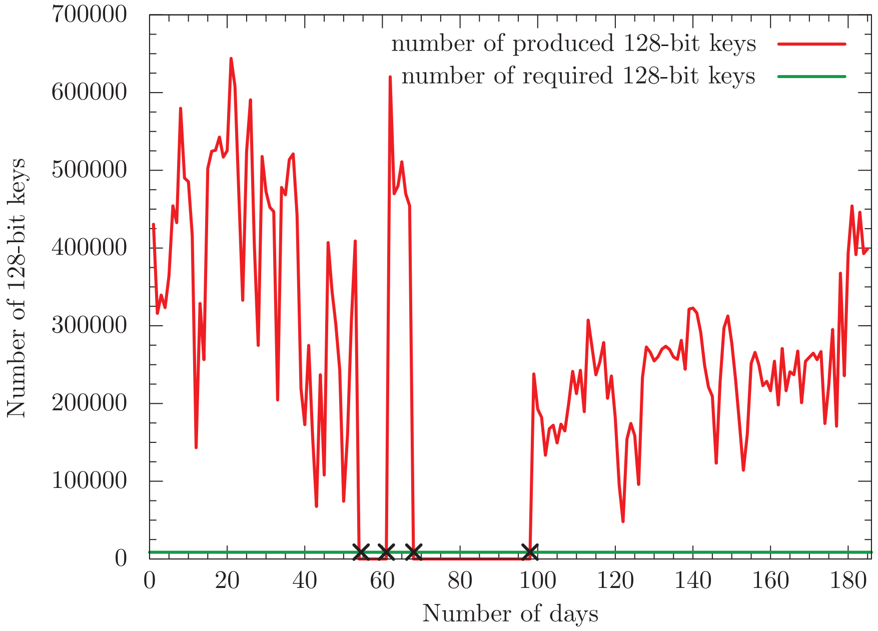


Figure 9.6: Keys produced during the SEQURE demonstration. In red, number of 128-bit keys per day produced during the SEQURE demonstration. The given secret key rate corresponds to the key rate produced by the system after key distillation and privacy amplification assuming an eavesdropper able to perform collective attacks in the first part and limited to individual attacks in the second part. In green, number of 128-bit keys per day required for a key renewal every 10 seconds. The number of produced keys largely exceeds this limit. Before day 100, the keys were produced assuming collective attacks from an eavesdropper. After day 100, they were produced assuming only individual attacks because the excess noise was significantly higher. The black marks correspond to the events listed in the section 9.4.1.

9.4.3 Secret key rate

The keys generated by the quantum layer were used to refresh the Thales Mistral encryptors' 128-bit AES keys. The renewal period was 10 seconds, thus the quantum layer had to be able to generate 8640 128-bit keys per day, which is roughly 1 Mbit of key material. Then, a 13 bit/s secret key rate would be sufficient. This rate is much lower than the rate up to 2 kbit/s that our setup can produce with comparable line transmission and excess noise conditions [83]. The ultimate performances of our system were obtained using a multi-thread data processing architecture with 2 cores devoted to the reconciliation and 1 core dedicated to the management of the hardware part [44]. In the present case only one core is required to perform the reconciliation, which results in an improved stability of the software and an improved stability of the overall system over long periods. Figure 9.6 shows that the SEQURE demonstration was largely above this threshold. Figure 9.5 shows that the key rate was about 600 bit/s (against collective attacks) during the first part of the demonstration and 400 bit/s key rate (against individual attacks) during the second part. In both parts of the experiment, the given secret key rate corresponds to the key rate produced by the system after key distillation and privacy amplification, assuming an eavesdropper able to perform collective attacks in the first part and limited to individual attacks in the second part.

9.5 Performance of the encryption layer

Several tests were performed in order to ensure that the key renewal did not affect the operation of the encryptors. As no specific adaptation of the Thales Mistral products was performed for the project, it was clear that the encryptors could not deal with a key renewal period lower than 3 seconds. A 10 second period, as mentioned in the previous paragraph, was therefore chosen as a security margin. This period could seem arbitrary but it ensures that no more than 2^{35} bits are encrypted with the same key if we consider 1Gb/s data communications. This can be compared with the best known attack [95] on the former encryption standard, the Data Encryption Standard (DES), which requires 2^{43} plaintext - ciphertext pairs, that is 2^{49} bits of observed traffic with known plaintext.

Classical networking applications like big files transfers (more than 1 Gbyte), disk sharing and persistence of the network link were tested. In all cases, the performance of the Mistral Gigabit was not affected by the key renewal.

9.6 SEQURE Demonstration Conclusion and Perspectives

The SEQURE demonstration that we have presented shows that continuous-variable QKD can compare well with discrete-variable QKD with respect to robustness and reliability in a server room environment, whose operating conditions are harder to cope with than laboratory ones. Furthermore, it shows that CVQKD can be integrated easily with off-the-shelf network equipments such as symmetric encryptors as a part of a more complex network infrastructure. Integration into WDM networks could be also eased by tolerance of the CVQKD homodyne detection scheme to incoherent noise

[106]. Moreover, if CVQKD WDM compatibility is confirmed in real optical network deployments, it will imply a significant decrease of the operational costs, which can stimulate further interest for this technology. The sequel of this chapter is dedicated to preliminary experiments concerning CDQKD WDM compatibility.

The operating distance of the implemented system can be improved by the recent developments of better error-correcting codes [65] without any hardware modification. These codes would also allow to produce keys secure against collective attacks even with the high values of the excess noise obtained during the second part of the demonstration. For distances higher than 100 km, the key management layer developed within the SECOQC project can still be used to share keys between two sites connected through several links.

As regards to the key rate, the current limitation of the system is not the optical part but the error correction speed which can be drastically improved using Graphics Processing Units (GPU) [83, 60]. Furthermore, in order to take into account finite-size effects it is necessary to process large blocks ($\geq 10^8$ pulses) to extract the final key [77, 63]. Then improving the error-correction speed allows to deal with finite-size effects without dramatically increasing the key production latency.

Finally, in a setting where QKD is used together with computational high-speed symmetric encryption like in SEQURE, it is not unreasonable to use a scheme based on minimal assumptions about the security of symmetric cryptography, like the Lamport signature scheme, instead of using an initial secret key. This enables to initialize QKD with an exchange of *authentic* values, which is easier to perform than an exchange of secret values. The security properties of QKD are unaffected provided the Lamport scheme is instantiated with a function that can be considered to be collision-resistant on the timescale of the first QKD session (such as cryptographic hash functions); then, as soon as common secret values are available, sessions are authenticated using unconditional means as usual. For a more detailed security analysis, see [68].

9.7 Analysis of the Noise Contributions in a WDM Setup

Another challenge in order to widen QKD deployments is to integrate QKD into classical communication networks. WDM architectures allow to share the use of one single optical fiber to transport several data channels at different wavelengths. This allows us to linearly reduce the infrastructure costs linked to fiber deployment. WDM compatibility would thus imply a significant improvement for QKD in terms of cost-effectiveness and compatibility with existing optical infrastructures. Extra noise due to the photon leakage from classical channels into the quantum channel however lowers QKD performance and must be controlled. While optical noise can be efficiently filtered when its wavelength is sufficiently far from the quantum channel, non-linear processes such as Raman scattering can generate photons at the wavelength of the quantum channel. Coping with Raman noise induced by classical channel is a major problem for QKD systems, especially for DVQKD that relies on photon counting: Raman spectrum is 200 nm broad and Raman scattering induced by one 0 dBm channel typically

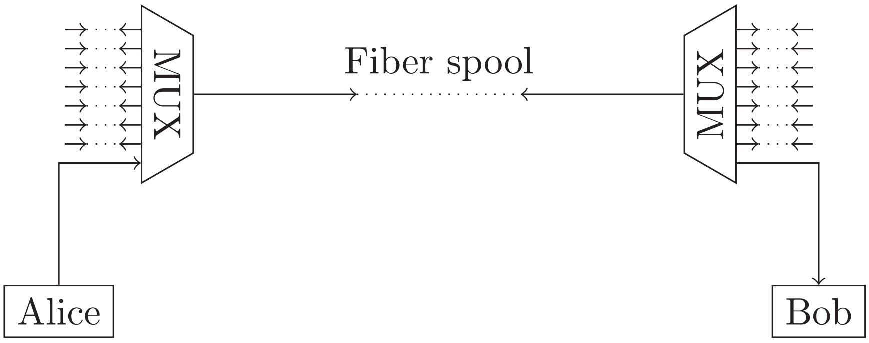


Figure 9.7: Generic WDM setup. 7 out of the 8 input channels of a MUX are used for classical optical signals while Alice's output is connected to the last channel. All the signals are multiplexed and travel over a unique fiber. On the receiver's side, they are demultiplexed with the corresponding DEMUX and the signal signal sent by Alice enters Bob's system.

higher than 0.1 noise photon per nm per ns, cannot be removed by wavelength filters. The coexistence in DVQKD with classical signals on a DWDM network relying on photon counting has been studied in [105] where no key could be established at 25 km for an input power higher than -3 dBm. Several DVQKD experiments tried to circumvent this limitation. In [37], four classical channels where multiplexed with a DVQKD system and 50 km operation was demonstrated. However, the intensity of the classical channels was attenuated to the smallest possible power compatible with the sensitivity limit of the optical receiver (around -20 dBm). This technique was also used in [103], where the temporal filtering technique developed in [22] was applied to obtain an extended range of 90 km for DVQKD operation in DWDM environment. Nevertheless, these two important results have been obtained with strongly attenuated classical channels and cannot realistically be translated to deployed DWDM networks.

As analyzed in [106], the coherent detection used in CVQKD to measure the field quadratures acts as a natural and extremely selective filter whose acceptance is equal to the spectral width of the local oscillator (LO). As a consequence, CVQKD, although less suited for very long distance operation, is intrinsically more resilient to WDM-induced noise photons than DVQKD. In this section, we review Bing Qi et al's analysis [106] of the different noise contributions when putting one weak quantum signal and several strong classical signals together on a single optical fiber. We consider successively leakage from classical channels and photons generated by nonlinear processes such as *Four-wave Mixing* (FWM) and *Spontaneous Anti-Stokes Raman Scattering* (SASRS).

9.7.1 Leakage from Classical Channels

Any practical laser source has a broadband noise background. Although the classical signal wavelength is not the same as the quantum signal one, a non negligible fraction of the classical signal can leak into the quantum channel due to the finite isolation of the *Demultiplexer* (DEMUX). The mean number of photons contributed by a classical signal C reads:

$$N^C_{leak} = \frac{\xi_2 P^C_{out}}{h\nu^C} \tag{9.1}$$

where ξ_2 is the cross channel isolation of the DEMUX, P^C_{out} is the power of the classical signal C at the input of the DEMUX and ν^C is the frequency of the classical signal C.

Typical values of the parameters are: $\xi_2 = 10^{-8}$, $P^C_{out} = 0$dBm, $\nu^C = c/\lambda^C$ ($\lambda^C = 1550$nm).

9.7.2 Four-wave Mixing

Four-wave mixing is generated by the interaction between two or more pump fields and the $\chi^(3)$ nonlinearity of the optical fiber. Three optical signals at different frequencies mix and create a new wave whose frequency is a linear combination of the three others. FWM can become the major source of noise for short distances but is dominated by the Raman effect for metropolitan fiber length[105]. Furthermore, this effect can be mitigated for example using wide channel spacing between classical channels of skipping a signal between the QKD signal and classical signals as suggested in [105]. For these reasons we neglect FWM in our analysis.

9.7.3 Spontaneous Anti-Stokes Raman Scattering

When putting the quantum channel at a shorter wavelength than the classical channel, SASRS is the dominant nonlinear process that generates photons at the wavelength of the quantum channel. The mean photons number contributed by SASRS is given by:

$$N^C_{SASRS} = \frac{\lambda^3}{hc^2} P^C_{out} \beta z \eta_{DEMUX} \tag{9.2}$$

where λ is the wavelength of the classical signal C, P^C_{out} is the power of the classical signal C at the input of the DEMUX, β is the spontaneous Raman scattering coefficient, z is the fiber length, η_{DEMUX} is the insertion loss of the DEMUX. Typical values of the parameters are: $\lambda = 1550$nm, $P^C_{out} = 0$dBm, $\beta = 3 \times 10^{-9} (km.nm)^{-1}$, $z = 1 - 100$km, $\eta_{DEMUX} = 0.89$(0.5 dB loss).

9.8 Noise Photons in Local Oscillator Matched Mode

The advantage brought by CVQKD over DVQKD in a setup where the quantum channel coexists with multiple classical channels setup is related to the homodyne detection. The strong local oscillator coherent with the quantum signal acts as a mode filter. The noise photons that are not in the same spatiotemporal and polarization mode as the local oscillator do not interfere with it. This reduces considerably the number of noise photons. The case where a large number of noise photons are unmatched with the local oscillator cannot be dealt with this way. Indeed, if this number is comparable to the number of photons of the local oscillator these signals create their own shot noise statistics on the homodyne detection and their contributions cannot be neglected.

Table 9.2: Parameters used for the computation of the secret key rate against collective attacks in the realistic model in a WDM setup.

λ^C (nm)	1550
β	3×10^{-9}
η_{Bob}	0.552
η_{DEMUX}	0.89

Based on the previous noise analysis, we assume that the quantum signal wavelength is shorter than the classical channel wavelength. In this setting, the total number of noise photons that are matched with the local oscillator at the entrance of Bob's system reads:

$$N^C = \frac{1}{2}(\eta_{ch}\eta_{DEMUX}N^C_{leak} + N^C_{SASRS}) \tag{9.3}$$

where the $\frac{1}{2}$ factor corresponds to the polarization selection of the local oscillator. The excess noise contributed by these noise photons after the homodyne detection of efficiency η is:

$$\epsilon^C = 2\eta N^C \tag{9.4}$$

Let us simulate the secure distance we should achieve assuming this noise model and the experimental parameters of chapter 7. Table 9.2 summarizes the experimental parameters we used for our simulation. We assume a 100 GHz width for MUX and DEMUX, which corresponds to a 0.8 nm width for the channels. A typical laser background noise within a 0.8 nm window is -60 dBm. Then the number of photons per mode with a DEMUX of isolation ξ_2 is significantly smaller than Raman photons. Figure 9.8 gives the excess noise created on the homodyne detection by Raman noise photons for an input power of 1 mW. It appears that this noise is comparable to the level of noises obtained in chapter 7. Consequently, it is in theory possible to maintain the secret key rates obtained in chapter 7, even in the presence of a strong classical channel at another wavelength.

9.9 Experimental Results

It appears that measuring the Raman noise induced by a classical channel at another wavelength than the quantum channel with the setup of chapter 7 cannot be done accurately without any modification. This is because the Raman photons do not affect only signal pulses but also local oscillator pulses. Furthermore, noise photons at other wavelengths than the local oscillator wavelength will be detected by the homodyne detection. This leads to two important remarks: the shot noise level depends on the Raman noise and the calibrated relationship that links the local oscillator level to the shot noise evaluation cannot be used safely.

We chose to solve this problem by implementing one of the real-time shot noise measurement techniques proposed in chapter 5. We introduced an optical switch on Bob's signal path. This technique allows us to define two sets of pulses on Bob's side. A maximum extinction is applied on one set of pulses while a minimum extinction is applied on the other set. From these two sets of pulses statistics, one can estimate the shot noise and the excess noise. However, this technique still adds an intrinsic noise that prevents us

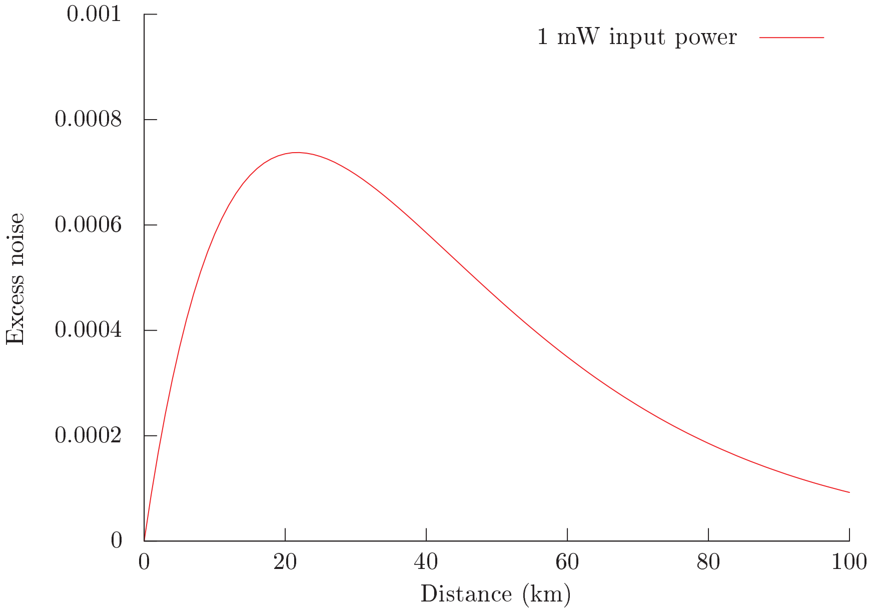


Figure 9.8: Theoretical noise induced by a 1 mW classical channel on the homodyne detection.

Table 9.3: Experimental parameters of the experimental demonstration of the coexistence between a classical channel and CVQKD on a single optical link.

λ^C	channel 29 and 33
λ^Q	channel 34
η_{Bob}	0.30
MUX losses	3.22 dB
ADM losses	0.59 dB
Channel losses	5.15 dB

from achieving the same excess noise levels as in chapter 7. The noise level of our system using this technique currently limits the maximum secure distance we can achieve in our WDM setup. Table 9.3 summarizes the experimental values of the parameters of our WDM setup and table 9.4 gives our excess noise measurements. On Bob's side, due to the extra losses of our DEMUX, we used an *Add Drop Module* (ADM) to reduce losses. Our excess noise levels are above the ones obtained in chapter 7 because of the new shot noise measurement procedure. These high excess noise values do not allow us to characterize the Raman induced noise. However these noise levels still allow us to obtain a positive secret key rate against collective attacks at 25 km.

9.10 Concluding Remarks

In this chapter, we showed that the maturity level of our setup is compatible with long-term field deployments using real optical fibers. Our demonstration consisted in renewing AES keys from symmetric encryptors with QKD generated keys. Future work includes combining QKD keys with asymmetric keys using a simple XOR as already done in [132] for DVQKD and

Table 9.4: Experimental excess noise measurements on Bob's side for a varying classical channel input power. The cases of an adjacent and a non-adjacent classical channel are reported.

Power (dBm)	channel 29	channel 33
0	6×10^{-3}	6×10^{-3}
3	6.5×10^{-3}	7.6×10^{-3}
5	6.7×10^{-3}	2.1×10^{-2}

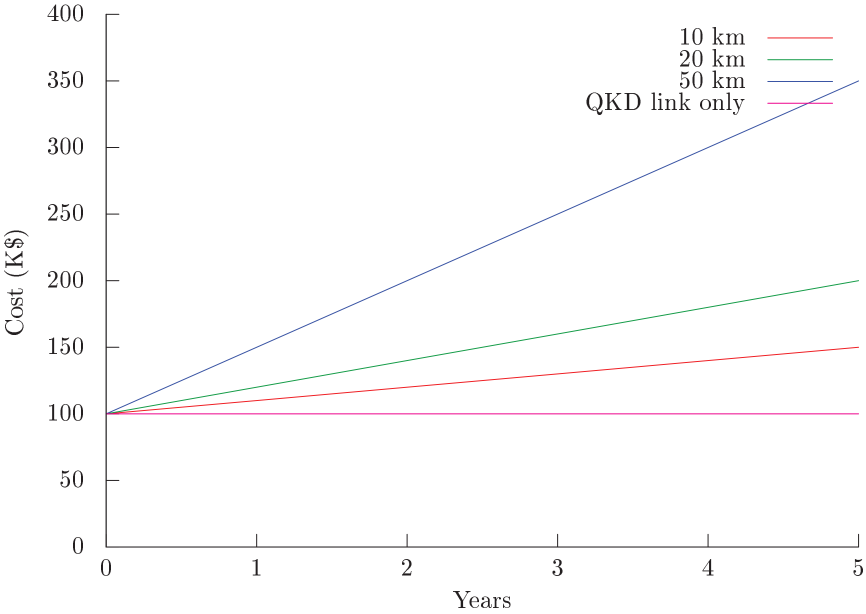


Figure 9.9: Operational cost of a QKD deployment over the lifespan of an equipment. We assumed a price of 100 K$ for a QKD link and a renting price of 1K$ per km and per year for the optical link. We plot the evolution of the operational cost of a QKD link for practical distances of 10, 20 and 50 km. We also plot the price of the QKD link only which is the deployment cost of a WDM compatible QKD system.

exploring schemes that benefit from the high volume of keys provided by QKD. A possible scheme consists in renewing AES sub-keys (that are used for each round of the AES) using QKD keys instead of deriving these sub keys from the AES key. Another step towards better synergy between classical and quantum cryptography is to encrypt QKD traffic with classical encryptors. In [68], we propose several other ways to enhance QKD security using symmetric cryptography primitives in a context where QKD is combined with symmetric encryptors.

We also demonstrated experimentally the combination of CVQKD and intense optical channels at other wavelengths on the same optical fiber. The coexistence of the quantum channel with classical channels is very important to increase the number of deployment scenarii for QKD. Indeed, as shown in figure 9.9, the operational cost of a QKD deployment is dominated by the renting price of the fiber link when the QKD system requires a dark fiber. WDM compatibility allows a QKD user to save the renting fiber cost which is proportional to the fiber length.

Conclusion and Perspectives

In this thesis, we studied the performance and security of continuous-variable quantum key distribution. At the beginning of this thesis, although some continuous-variable quantum key distribution protocols featured promising characteristics like laboratory implementations using only off-the-shelf components optimized for the telecommunication industry, they were clearly outperformed by discrete variables protocols both in terms of performance and security. Indeed, discrete variables commercial products were already on the market and benefited from both more mature security analyses and higher secure distances.

The main achievement of this thesis was to bridge the gap between these technologies. On the performance aspect, we were able to increase the secure distance of the coherent state protocol with a Gaussian modulation from 25 km to 80 km. This was possible because of high-efficiency error-correction techniques in the low signal-to-noise ratios regime. Furthermore, we implemented these error-correcting codes on state-of-the art Graphics Processing Units. As a result, post-processing speed is not the bottleneck of this technology any more and higher speeds might be achieved in the near future.

As regards security, we focused on several practical imperfections of our experimental setup and took them into account in the security proof. This includes computing security parameters over large data blocks, which requires enhanced hardware stability. We built an experimental setup from scratch and developed efficient feedback controls that allowed us to get stable experimental parameters over long periods of time. We also imagined possible attacks against our system and designed proper countermeasures. We strongly believe that real-time shot noise measurement techniques should be implemented in any CVQKD setup in order to claim a high level of security. More generally, we have initiated work concerning side-channel attacks that target CVQKD (Trojan horse attacks and wavelength attacks are currently being studied) and we aim at reaching security levels that qualify our system to pass the first quantum system certification evaluations.

We also worked towards CVQKD integration in optical networks. First, we demonstrated the combination of CVQKD with classical symmetric encryptors as it had already been done with DVQKD. Such a combination seems to be the most realistic QKD deployment scenario in the next few years. Second, we ran preliminary experiments that demonstrated the compatibility of CVQKD with intense optical signals propagating on the same fiber in a DWDM configuration. Given that the cost of a QKD system is dominated by the cost of fiber optic infrastructures over the lifespan of a product, DWDM compatibility is expected to significantly increase perspectives of QKD deployments. Finally, we commercialized the first CVQKD product, based on this thesis work. It features high hardware stability and

	2010	2013
range	25 km	80 km
rate	10 kb/s	100 kb/s
security proof	asymptotic	finite-size effects
practical security	imperfect detection	imperfect modulation
side channels	- - -	+
stability	- - -	+ + +
WDM integration	+	+ +

Table 9.5: This table compares CVQKD security and performance in 2010 and 2013.

long-distance key agreement capability.

We expect this is not the end of the story as regards CVQKD improvements! Perspectives include improved DWDM compatibility over longer distances and improved key rate performance. Our secure distance is currently limited by the excess noise of our setup. This limitation could be overcome using virtual noiseless amplification or other protocols more resistant to the excess noise such as heterodyne-based detection protocols. Higher speed is now possible by improving the hardware repetition rate. We believe the point in doing that is more to diminish the impact of finite size effects by estimating parameters over larger blocks than to increase the secret key rate since one-time-pad at state-of-the-art telecoms speeds should remain an elusive goal. On the theoretical side, the main concern is to get a security proof against coherent attacks in the finite-size regime. Finally, perspectives offered by silicon photonics both in terms of miniaturization and costs are expected to broaden CVQKD market. Indeed, on the one hand replacing current bulk versions of CVQKD systems by silicon chips would ease CVQKD integration in data centers, on the other hand the cost of the optics should drop by an order of magnitude.

Appendix A

Matrix Representation of the Octonions

We used the following matrix representation of the octonions to implement the multidimensional protocol described in chapter 6:

$$A_0 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$A_1 = \begin{bmatrix} 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$$A_2 = \begin{bmatrix} 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \end{bmatrix}$$

$$A_3 = \begin{bmatrix} 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \end{bmatrix}$$

$$A_4 = \begin{bmatrix} 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$A_5 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$A_6 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$A_7 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Appendix B

Local Oscillator Power Measurement and Clock Signal Generation

Here, we discuss the feasibility of measuring the local oscillator power and generating a trigger signal from the local oscillator without compromising the security of the system.

Reasonable trigger generation functions are of the following form:

$$U_1(t) = \mathbf{1}_{s(t-r)>x} \tag{B.1}$$

$$U_2(t) = \mathbf{1}_{s(t-r)-s(t-r-\delta)>0} \tag{B.2}$$

The function U_1 outputs a positive value at time t if and only if the signal measurement is above the threshold value x at time $t-r$. This corresponds to detecting the beginning of a pulse (when its value is above the threshold x) and then delaying the trigger with a chosen delay r. The function U_2 outputs a positive value at time t if and only if the difference between the signal and the signal delayed of one pulse duration δ is positive. This presents the advantage of being independent from the signal level but requires to know the pulse duration δ. This cannot be assumed in the context of an active eavesdropper. Both U_1 and U_2 are of the form $\mathbf{1}_{\phi(s)}$ where ϕ is a linear functional of the signal.

Reasonable power measurement functions are of the following form:

$$P = \int_0^\delta s(t-s)\alpha^{-s}ds \tag{B.3}$$

where α is some nonnegative integration constant. P is a linear form of the local oscillator signal. Since P is not a multiple of ϕ for the trigger examples above, there are signals that can be added to the local oscillator signal that do not change the output of P but that change ϕ. A closer look to this problem shows that it is indeed possible to change U_i, $i = 1$ or 2, without changing P.

A simple example is given in Fig. B.1. Both local oscillator pulses have the same energy but the rising time of the trigger does not coincide with the end of the pulse.

This analysis shows that, in practice, a calibrated linear relationship between the shot noise level and local oscillator power cannot be used in the presence of an eavesdropper, who will always be able to modify the linear relationship during the QKD run.

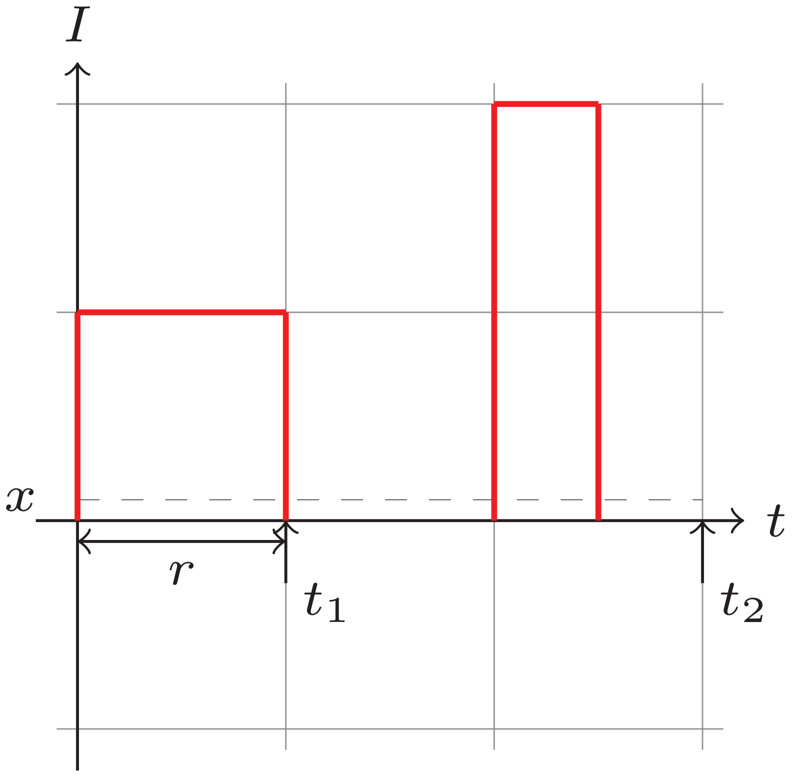


Figure B.1: Trigger generation with respect to pulses shapes. This figure shows how two pulses of same energy generate two different trigger signals of rising time t_1 and t_2.

Appendix C

Post-processing Scheduling

When doing a CVQKD experiment with post-processing, there are basically two possibilities. The first one consists in accumulating raw data during the quantum exchange and then stopping the quantum exchange and performing post-processing over the accumulated data. Such a method bounds the time required by the system to extract secret key from a given data size by the sum of the optics time to generate raw data and the post-processing time to process these raw data. The second method allows us to make an optimal use of both optical and computing power resources. It consists in using *multi-threading* in order to post-process raw data on the fly while the optics is still running. We used C++11 threads to share computing power demanding tasks into several execution threads. With this parallelism, the time required by the system to extract secret key from a given data size is only bounded by the maximum of the optics time and the post-processing time.

In figure C.1, we represent our post-processing flow diagram. Each rectangle represents an execution thread. Vertical arrows represent messages passing between local threads and horizontal arrows are for network messages passing between Alice and Bob. SOme further details are given below:

- **Alice Hardware** thread generates the Gaussian modulation, sends control data to the acquisition card and receives values coming from Alice's output photodiode. Both values are transmitted to **Alice Data Processing**. **Bob Hardware** thread performs quadrature selection by sending phase values to the acquisition card and receives measurements coming from the homodyne detection. Both sets of values are transmitted to **Bob Data Processing**.
- **Alice Data Processing** controls the quality of the Gaussian modulation, estimates amplitude modulator parameters and performs an adjustment of these parameters if required. Then data are transmitted to **Regroup Intervals**. **Bob Data Processing** tries to find Alice's synchronization pattern and can compute some statistics such as the correlation between Alice and Bob once this pattern is detected. Then data are transmitted to **Compute Intervals**.
- On Bob's side **Compute Intervals** computes the offset of the current data block in Alice's modulation sequence and sends it to Alice through the network. If no synchronization pattern has been found, the data block is thrown away and Alie is informed about that. On Alice's side, **Regroup Intervals** uses Bob's offset to create a data block in phase with Bob's block out of two successive blocks. If Alice is not able to do that because of errors on her side, data is discarded

and she informs Bob. Otherwise, she discloses at random a fraction of this block quadratures and send them to Bob.

– On Bob's side, **Filter Intervals** is used to discard Bob's block is he is informed by Alice that data concerning this block should not be considered (because of modulation errors for example). In the opposite case, Alice's sifted data are transferred to **Regroup ECC** together with Bob's data. Here, data are accumulated until the size of an error-correction block is reached (2^{20} in our setup). **Prepare ECC** does the same thing on Alice's side.
– On Bob's side **Select Code** computes an estimate of the SNR thanks to Alice's sifted data and selects an error-correcting code with eventually some puncturing and shortening parameters. Then he computes a set of parity-check bits, the syndrome, and sends it to Alice, together with the description of some rotations corresponding to the multi-dimensional protocol described in chapter 6. On Alice's side, Alice uses the description of the rotations to prepare her data for the error-correction in **Prepare ECC**. Then Alice performs the error-correction in **Error Correction**.
– After the error-correction, Bob accumulates error-corrected keys in **Regroup and Init PA** until he has enough data to perform the privacy amplification over a block large enough, which allows to diminish the uncertainty on the transmission parameters and to achieve a higher value of the secret key rate. Once this is done, he draws a random binary Toeplitz matrix and multiplies his corrected binary string by this matrix. Then he sends Alice the description of this matrix together with some check bits that allow them to know with high probability if they share a common key after privacy amplification. On Alice's side, error-corrected binary strings are accumulated in the same way and Alice applies privacy amplification on her vector with the matrix description sent by Bob. Then she compares her check bits with the check bits sent by Bob and she informs him on the success of the failure of the key extraction.
– On both sides, if a final key was successfully extracted, this key is transmitted to a **Key Broker** thread which is in charge of delivering this key to some users according to the defined security policy.

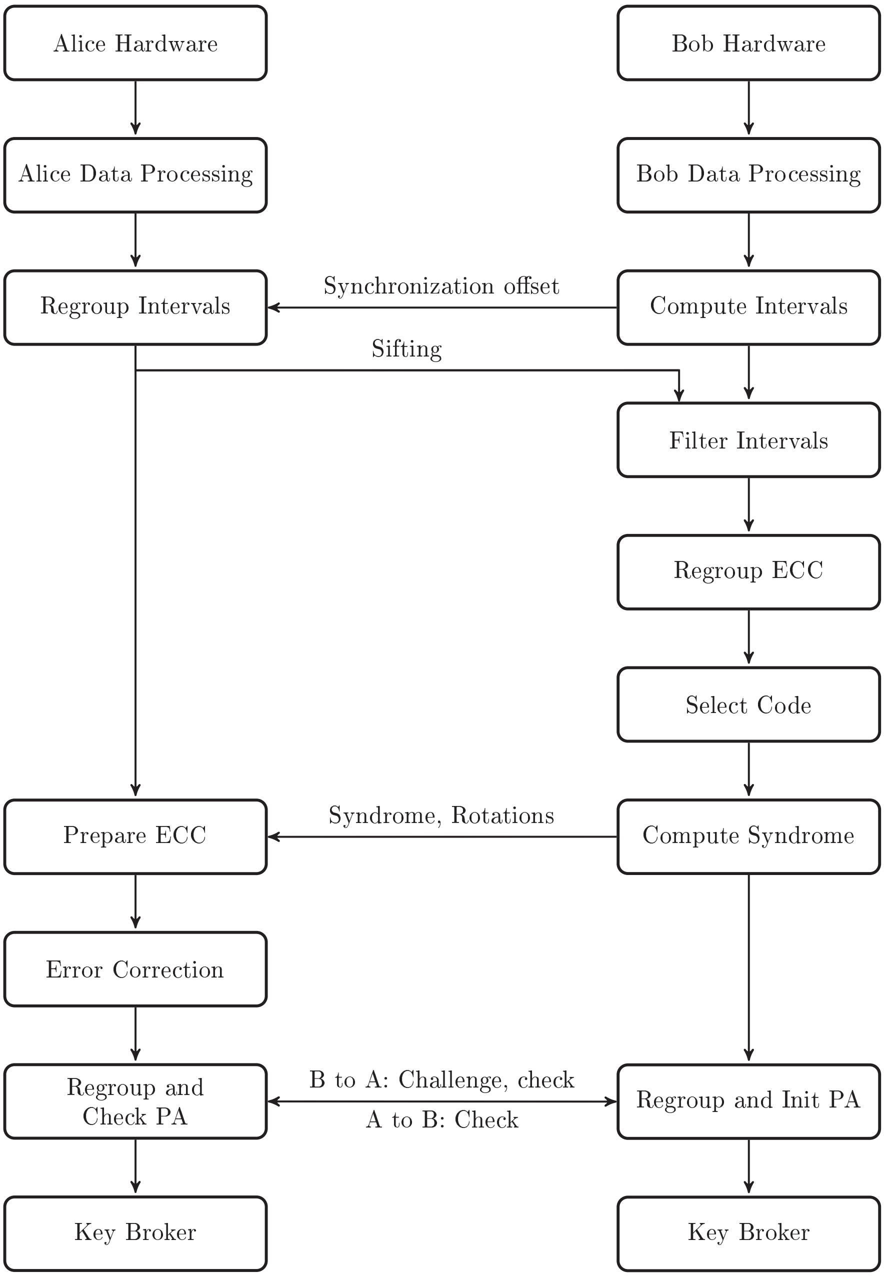


Figure C.1: Flow diagram of Alice and Bob post-processing. Each step runs in a separate C++11 thread. All the data structures are created once in memory at the launch of the program and data are then moved between threads using typed buffers. Races between threads to access data are dealt with thanks to *mutex* from the standard C++11 library.

List of Abbreviations

ADM	Add Drop Module
AES	Advanced Encryption Standard
APC	Angled Physical Contact
AWGNC	Additive White Gaussian Noise Channel
BIAWGNC	Binary Input Additive White Gaussian Noise Channel
BSC	Binary Symmetric Channel
CVQKD	Continuous Variables Quantum Key Distribution
DEMUX	Demultiplexer
DFB	Distributed Feedback
DPC	Dynamic Polarization Controller
DVQKD	Discrete Variables Quantum Key Distribution
DWDM	Dense Wavelength Division Multiplexing
EOM	Electro-optic Modulator
FC	Ferrule Connector or Fiber Channel
FWM	Four-wave Mixing
GPU	Graphics Processing Unit
HD	Homodyne Detection
IP	Internet Protocol
LDPC	Low Density Parity Check
MMF	Multi-Mode Fibers
OTP	One-Time Pad
PBS	Polarization Beam Splitter
PC	Physical Contact
PCI	Peripheral Component Interconnect
PKI	Public Key Infrastructure
PMF	Polarization-maintaining Fibers
POVM	Positive Operator Valued Measure
PRNG	Pseudo-random Numbers Generator
QBER	Quantum Bit Error Rate

QKD	Quantum Key Distribution
QRNG	Quantum Random Number Generator
RSA	Rivest Shamir Adleman
SASRS	Spontaneous Anti-Stokes Raman Scattering
SECOQC	Secure Communication based on Quantum Cryptography
SEQURE	Symmetric Encryption with QUantum key REnewal
SMF	Single Mode Fibers
SNR	Signal to Noise Ratio
UPC	Ultra Physical Contact
XOR	Exclusive Or

Bibliography

[1] Austrian Institute of Technology. https://sqt.ait.ac.at/software/.

[2] ID Quantique. http://www.idquantique.com.

[3] MagiQ Technologies. http://www.magiqtech.com.

[4] Quintessence Labs. http://www.quintessencelabs.com.

[5] SeQureNet. http://www.sequrenet.com.

[6] Andris Ambainis. A new protocol and lower bounds for quantum coin flipping. *J. Comput. Syst. Sci.*, 68:398–416, 2004.

[7] I. Andriyanova and J.P. Tillich. On a Low-Rate TLDPC Code Ensemble and the Necessary Condition on the Linear Minimum Distance for Sparse-Graph Codes. *CoRR*, abs/1010.1911, 2010.

[8] E. Arikan. Channel polarization: A method for constructing capacity-achieving code. In *Information Theory, 2008. ISIT 2008. IEEE International Symposium on*, pages 1173–1177, july 2008.

[9] C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179, New York, 1984. IEEE Press.

[10] Guido Berlin, Gilles Brassard, Felix Bussières, and Nicolas Godbout. Loss-tolerant quantum coin flipping. *Phys. Rev. A*, 80:062321, 2009.

[11] Guido Berlin, Gilles Brassard, Felix Bussières, Nicolas Godbout, Joshua Slater, and Wolfgang Tittel. Experimental loss-tolerant quantum coin flipping. *Nat. Commun.*, 2:561, 2011.

[12] M. Berta, F. Furrer, and V. B. Scholz. The Smooth Entropy Formalism on von Neumann Algebras. *CoRR*, abs/1107.5460, 2011.

[13] R. Blandino, A. Leverrier, M. Barbieri, J. Etesse, P. Grangier, and R. Tualle-Brouri. Improving the maximum transmission distance of continuous-variable quantum key distribution using a noiseless amplifier. *Phys. Rev. A*, 86:012327, 2012.

[14] M. Bloch, A. Thangaraj, and S. W. McLaughlin. Efficient Reconciliation of Correlated Continuous Random Variables using LDPC Codes. *CoRR*, abs/cs/0509041, 2005.

[15] Manuel Blum. Coin flipping by telephone: a protocol for solving impossible problems. In *Advances in Cryptology; a Report on CRYPTO'81*, volume 82, pages 11–15, Santa Barbara, California, USA, 1981.

[16] G. Brassard and L. Salvail. Secret-key reconciliation by public discussion. pages 410–423. Springer-Verlag, 1994.

[17] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.*, 81:5932–5935, 1998.

[18] G. Leuchs Ch. Silberhorn, N. Korolkova. Quantum key distribution with bright entangled beams. *Phys. Rev. Lett.*, 88:167902, 2002.

[19] André Chailloux and Iordanis Kerenidis. Optimal quantum strong coin flipping. In *50th Annual Symposium on Foundations of Computer Science, FOCS 2009, October 25-27, 2009, Atlanta*, IEEE Computer Society, 2009.

[20] K. Chen, K. Niu, and J. R. Lin. List successive cancellation decoding of polar codes. *Electronics Letters*, 48(9):500–501, 2012.

[21] 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 J. Phys.*, 13(1):013003, 2011.

[22] Iris Choi, Robert J Young, and Paul D Townsend. Quantum information to the home. *New J. Phys.*, 13(6):063039, 2011.

[23] Matthias Christandl, Robert König, and Renato Renner. Postselection technique for quantum channels with applications to quantum cryptography. *Phys. Rev. Lett.*, 102:020504, Jan 2009.

[24] R.J. Clarke, P.J.and Collins, V. Dunjko, E. Andersson, J. Jeffers, and G. S. Buller. Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light. *Nature Communications*, 3(1174), 2012.

[25] Thomas M. Cover and Joy A. Thomas. *Elements of information theory.* Wiley-Interscience, New York, NY, USA, 1991.

[26] C. Crépeau. Réconciliation et distillation publiques de secret, 1995.

[27] J. Preskill D. Gottesman. Secure quantum key distribution using squeezed states. *Phys. Rev. A*, 63:022309, 2001.

[28] Q. Dinh Xuan, Z. Zhang, and P.L. Voss. A 24 km fiber-based discretely signaled continuous variable quantum key distribution system. *Opt. Express*, 17(26):24244–24249, 2009.

[29] 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. *Appl. Phys. Lett.*, 96:161102, 2010.

[30] 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. *Appl. Phys. Lett.*, 96(16):161102–161102–3, 2010.

[31] A.K. Ekert. Quantum cryptography based on bell?s theorem. *Phys. Rev. Lett.*, 67(6):661–663, 1991.

[32] D. Elkouss, A. Leverrier, R. Alléaume, and J. Boutros. Efficient reconciliation protocol for discrete-variable quantum key distribution. In *Proceedings of the 2009 IEEE international conference on Symposium on Information Theory - Volume 3*, ISIT'09, pages 1879–1883, Piscataway, NJ, USA, 2009. IEEE Press.

[33] D. Elkouss, J. Martínez-Mateo, D. Lancho, and V. Martin. Rate Compatible Protocol for Information Reconciliation: An application to QKD. *CoRR*, abs/1006.2660, 2010.

[34] D. Elkouss, J. Martinez-Mateo, and V. Martin. Secure rate-adaptive reconciliation. In *Information Theory and its Applications (ISITA), 2010 International Symposium on*, pages 179–184, 2010.

[35] D. Elkouss, J. Martínez-Mateo, and V. Martin. Untainted puncturing for irregular low-density parity-check codes. *IEEE Wireless Communications Letters*, 1:585–588, 2012.

[36] D Elser, T Bartley, B Heim, Ch Wittmann, D Sych, and G Leuchs. Feasibility of free space quantum key distribution with coherent polarization states. *New J. Phys.*, 11(4):045014, 2009.

[37] P. Eraerds, N. Walenta, M. Legre, N. Gisin, and H. Zbinden. Quantum key distribution and 1 gbps data encryption over a single fibre. *New J. Phys.*, 12(6):063027, 2010.

[38] A. Ferenczi, P. Grangier, and F. Grosshans. Calibration attack and defense in continuous variable quantum key distribution. In *IQEC Conf. Digest*, volume IC 13, 2007.

[39] Radim Filip. Continuous-variable quantum key distribution with noisy coherent states. *Phys. Rev. A*, 77:022310, Feb 2008.

[40] Digital Signature Standard (DSS). FIPS PUB 186-3, National Institute for Standards and Technology, 2009.

[41] Advanced Encryption Standard (AES). FIPS PUB 197, National Institute for Standards and Technology, 2001.

[42] Data Encryption Standard (DES). FIPS PUB 46-3, National Institute for Standards and Technology, 1999.

[43] J. Fiurasek and N. J. Cerf. Gaussian postselection and virtual noiseless amplification in continuous-variable quantum key distribution. *Phys. Rev. A*, 86:060302(R), 2012.

[44] 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 J. Phys.*, 11:045023, 2009.

[45] 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.

[46] R. Garcia-Patron and N.J. Cerf. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.*, 97(050903), 2006.

[47] 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.

[48] Daniel Gottesman and Isaac L. Chuang. Quantum digital signatures. Technical report, 2001.

[49] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N.J. Cerf, and P. Grangier. Quantum key distribution using gaussian-modulated coherent states. *Nature*, 421(6920):238–241, 2003.

[50] Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.*, 88(5):057902, 2002.

[51] Frédéric Grosshans and Philippe Grangier. Reverse reconciliation protocols for quantum cryptography with continuous variables, April 2002.

[52] Saikat Guha and Mark M. Wilde. Polar coding to achieve the holevo capacity of a pure-loss optical channel. *CoRR*, abs/1202.0533, 2012.

[53] Hauke Häseler, Tobias Moroder, and Norbert Lütkenhaus. Testing quantum devices: Practical entanglement verification in bipartite optical systems. *Phys. Rev. A*, 77:032303, Mar 2008.

[54] M. Heid and N. Lütkenhaus. Security of coherent-state quantum cryptography in the presence of Gaussian noise. *Phys. Rev. A*, 76(2):022313, 2007.

[55] Mark Hillery. Quantum cryptography with squeezed states. *Phys. Rev. A*, 61:022309, Jan 2000.

[56] Jing-Zheng Huang, Christian Weedbrook, Zhen-Qiang Yin, Shuang Wang, Hong-Wei Li, Wei Chen, Guan-Can Guo, and Zheng-Fu Han. Quantum hacking on continuous-variable quantum key distribution system using a wavelength attack. *Arxiv preprint arXiv:1302.0090 [quant-ph]*, 2013.

[57] L. M. Ioannou and M. Mosca. A new spin on quantum cryptography: Avoiding trapdoors and embracing public keys. *CoRR*, abs/1109.3235, 2011.

[58] Nitin Jain, Christoffer Wittmann, Lars Lydersen, Carlos Wiechers, Dominique Elser, Christoph Marquardt, Vadim Makarov, and Gerd Leuchs. Device calibration impacts security of quantum key distribution. *Phys. Rev. Lett.*, 107:110501, Sep 2011.

[59] D. Johnson and A. Menezes. The Elliptic Curve Digital Signature Algorithm (ECDSA). Technical Report CORR 99-34, University of Waterloo, 1999.

[60] P. Jouguet and S. Kunz-Jacques. High performance error correction for quantum key distribution using polar codes. *Preprint at http://arxiv.org/abs/1204.5882*, 2012.

[61] P. Jouguet, S. Kunz-Jacques, T. Debuisschert, S. Fossier, E. Diamanti, R. Alléaume, R. Tualle-Brouri, P. Grangier, A. Leverrier, P. Pache, and P. Painchault. Field test of classical symmetric encryption with continuous variables quantum key distribution. *Opt. Express*, 20:14030–14041, 2012.

[62] P. Jouguet, S. Kunz-Jacques, and E. Diamanti. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. *Phys. Rev. A*, 87:062313, Jun 2013.

[63] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier. Analysis of imperfections in practical continuous-variable quantum key distribution. *Phys. Rev. A*, 86:032309, 2012.

[64] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature Photonics*, doi:10.1038/nphoton.2013.63, 2013.

[65] 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.

[66] A. Jankovic K. Bencheikh, T. Symul and J.A. Levenson. Quantum key distribution with continuous variables. *J. Mod. Opt.*, 48:1903, 2001.

[67] S.B. Korada, A. Montanari, I.E. Telatar, and R. Urbanke. An empirical scaling law for polar codes. In *Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on*, pages 884–888, 2010.

[68] S. Kunz-Jacques and P. Jouguet. Using Hash-Based Signatures to Bootstrap Quantum Key Distribution. *CoRR*, abs/1109.2844, 2011.

[69] 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, 2005.

[70] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier. Multidimensional reconciliation for a continuous-variable quantum key distribution. *Phys. Rev. A*, 77(4):42325, 2008.

[71] A. Leverrier and P. Grangier. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Phys. Rev. Lett.*, 102(18):180504, 2009.

[72] A. Leverrier and P. Grangier. Continuous-variable Quantum Key Distribution protocols with a discrete modulation. *arxiv preprint:1002.4083*, Feb 2010.

[73] A. Leverrier, E. Karpov, P. Grangier, and NJ Cerf. Security of continuous-variable quantum key distribution: towards a de finetti theorem for rotation symmetry in phase space. *New J. Phys.*, 11:115009, 2009.

[74] 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.

[75] 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.

[76] Anthony Leverrier and Philippe Grangier. Continuous-variable quantum-key-distribution protocols with a non-gaussian modulation. *Phys. Rev. A*, 83:042312, Apr 2011.

[77] Anthony Leverrier, Frédéric Grosshans, and Philippe Grangier. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A*, 81:062343, Jun 2010.

[78] Anthony Leverrier, Frédéric Grosshans, and Philippe Grangier. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A*, 81:062343, 2010.

[79] Bin Li, Hui Shen, and D. Tse. An adaptive successive cancellation list decoder for polar codes with cyclic redundancy check. *Communications Letters, IEEE*, 16(12):2044–2047, 2012.

[80] 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.

[81] H.-K. Lo and H. F Chau. Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica D*, 120:177–187, 1998.

[82] J. Lodewyck, T. Debuisschert, R. García-Patrón, R. Tualle-Brouri, N.J. Cerf, and P. Grangier. Experimental implementation of non-gaussian attacks on a continuous-variable quantum-key-distribution system. *Phys. Rev. Lett.*, 98:030503, Jan 2007.

[83] 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(4), 2007.

[84] Jérôme Lodewyck, Thierry Debuisschert, Rosa Tualle-Brouri, and Philippe Grangier. Controlling excess noise in fiber-optics continuous-variable quantum key distribution. *Phys. Rev. A*, 72:050303, Nov 2005.

[85] S. Lorenz, J. Rigas, M. Heid, U. L. Andersen, N. Lütkenhaus, and G. Leuchs. Witnessing effective entanglement in a continuous variable prepare-and-measure setup and application to a quantum key distribution scheme using postselection. *Phys. Rev. A*, 74:042326, Oct 2006.

[86] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*, 4(10):686–689, 2010.

[87] Xiang-Chun Ma, Shi-Hai Sun, Mu-Sheng Jiang, and Lin-Mei Liang. Improved wavelength attack on practical continuous variables quantum key distribution system with heterodyne protocol. *Arxiv preprint arXiv:1303.6039 [quant-ph]*, 2013.

[88] 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 system. *Arxiv preprint arXiv:1303.6043 [quant-ph]*, 2013.

[89] David J. C. Mackay. *Information Theory, Inference and Learning Algorithms.* Cambridge University Press, first edition edition, June 2003.

[90] Hessam Mahdavifar and Alexander Vardy. Achieving the secrecy capacity of wiretap channels using polar codes. *IEEE Trans. Inf. Theor.*, 57(10):6428–6443, October 2011.

[91] Vadim Makarov. Controlling passively quenched single photon detectors by bright light. *New J. Phys.*, 11(6):065003, 2009.

[92] Ryuhei Mari and Toshiyuki Tanaka. Performance and construction of polar codes on symmetric binary-input memoryless channels. In *Proceedings of the 2009 IEEE international conference on Symposium on Information Theory - Volume 3*, ISIT'09, pages 1496–1500, Piscataway, NJ, USA, 2009. IEEE Press.

[93] J. Martinez-Mateo, D. Elkouss, and V. Martin. Interactive reconciliation with low-density parity-check codes. In *Turbo Codes and Iterative Information Processing (ISTC), 2010 6th International Symposium on*, pages 270–274, 2010.

[94] J. Martinez-Mateo, D. Elkouss, and V. Martin. Blind reconciliation. *Quant. Inf. Comp.*, 12(9–10):791–812, 2012.

[95] Mitsuru Matsui. Linear cryptanalysis method for des cipher. In *Workshop on the theory and application of cryptographic techniques on Advances in cryptology*, EUROCRYPT '93, pages 386–397, Secaucus, NJ, USA, 1994. Springer-Verlag New York, Inc.

[96] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.*, 78(17):3414–3417, 1997.

[97] R. Mori and T. Tanaka. Non-binary polar codes using reed-solomon codes and algebraic geometry codes. In *IEEE Information Theory Workshop (ITW)*, 2010.

[98] R. Namiki and T. Hirano. Practical Limitation for Continuous-Variable Quantum Cryptography using Coherent States. *Phys. Rev. Lett.*, 92(11):117901, 2004.

[99] Miguel Navascués, Frédéric Grosshans, and Antonio Acín. Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography. *Phys. Rev. Lett.*, 97(19):190502, 2006.

[100] G. Van Assche N.J. Cerf, M. Levy. Quantum distribution of gaussian keys using squeezed states. *Phys. Rev. A*, 63:052311, 2001.

[101] T. Ogawa and H. Nagaoka. A new proof of the channel coding theorem via hypothesis testing in quantum information theory. In *Proceedings of IEEE International Symposium on Information Theory*, page 73, Lausanne, Switzerland, 2002. IEEE, IEEE Press.

[102] A. Pappa, P. Jouguet, T. Lawson, A. Chailloux, M. LegrÃ©, P. Trinkler, I. Kerenidis, and E. Diamanti. Experimental plug & play quantum coin flipping. *Arxiv preprint arXiv:1306.3368 [quant-ph]*, 2013.

[103] 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.

[104] 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 J. Phys.*, 11:075001, 2009.

[105] 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 1550ânm qkd with strong classical channels in reconfigurable networking environments. *New J. Phys.*, 11(4):045012, 2009.

[106] B. Qi, W. Zhu, L. Qian, and H.K. Lo. Feasibility of quantum key distribution through a dense wavelength division multiplexing network. *New J. Phys.*, 12(10):103042, 2010.

[107] 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.

[108] T. C. Ralph. Continuous variable quantum cryptography. *Phys. Rev. A*, 61:010303(R), 2000.

[109] M.D. Reid. Quantum cryptography with a predetermined key, using continuous variable einstein-podolsky-rosen correlations. *Phys. Rev. A*, 62:010303, 2000.

[110] Joseph M. Renes, Frédéric Dupuis, and Renato Renner. Efficient polar coding of quantum information. *Phys. Rev. Lett.*, 109:050504, Aug 2012.

[111] R. Renner. *Security of Quantum Key Distribution.* Phd thesis, ETH Zurich, Switzerland, 2005.

[112] R. Renner and J. I. Cirac. de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography. *Phys. Rev. Lett.*, 102(11):110504, 2009.

[113] T. Richardson and R. Urbanke. Multi-edge type LDPC codes. presented at the Workshop honoring Prof. Bob McEliece on his 60th birthday, California Institute of Technology, Pasadena, California, May 2002.

[114] T. Richardson and R. Urbanke. *Modern Coding Theory.* Cambridge University Press, New York, NY, USA, 2008.

[115] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke. Design of capacity-approaching irregular low-density parity-check codes. *IEEE Trans. Inform. Theory*, 47:619–637, 2001.

[116] R. Rivest, A. Shamir, and L. M. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21(2):120 – 126, 1978.

[117] D. Rosenberg, C. G. Peterson, J. W. Harrington, P. R. Rice, N. Dallmann, K. T. Tyagi, K. P. McCabe, S. Nam, B. Baek, R. H. Hadfield, R. J. Hughes, and J. E. Nordholt. Practical long-distance quantum key distribution system using decoy levels. *New J. Phys.*, 11:045009, 2009.

[118] H. C. A. V. Tilborg S. Liu and M.V. Dijk. A practical protocol for advantage distillation and information reconciliation. *Des. Codes Cryptography*, 30(1):39–62, august 2003.

[119] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, 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*, 19:10387–10409, 2011.

[120] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev. The Security of Practical Quantum Key Distribution. *Reviews of Modern Physics*, 81(3):1301, 2009.

[121] V. Scarani and C. Kurtsiefer. The black paper of quantum cryptography: real implementation problems. *Arxiv preprint arXiv:0906.4547v2 [quant-ph]*, 2012.

[122] Valerio Scarani and Renato Renner. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Phys. Rev. Lett.*, 100:200501, May 2008.

[123] 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.

[124] C. P. Schnorr. Efficient Identification and Signatures for Smart Cards. In B. Brassard, editor, *Advances in Cryptology – Crypto'89*, volume 435 of *LNCS*, pages 239 – 252. Springer-Verlag, 1990.

[125] Claude E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27:379–423, 623–656, July, October 1948.

[126] 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.

[127] Yujie Shen, Xiang Peng, Jian Yang, and Hong Guo. Continuous-variable quantum key distribution with gaussian source noise. *Phys. Rev. A*, 83:052304, May 2011.

[128] M. A. Shokrollahi and R. Storn. Design of Efficient Erasure Codes with Differential Evolution. In *Proceedings of the 2000 IEEE international conference on Symposium on Information Theory*, 2000.

[129] P. W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[130] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs. Continuous variable quantum cryptography: Beating the 3 dB loss limit. *Phys. Rev. Lett.*, 89:167901, 2002.

[131] Robert Spekkens and Terry Rudolph. Quantum protocol for cheat-sensitive weak coin flipping. *Phys. Rev. Lett.*, 89(22):1–4, 2002.

[132] D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat, J-B. Page, D. Perroud, G. Ribordy, A. Rochas, S. Robyr, J. Tavares, R. Thew, P. Trinkler, S. Ventura, R. Voirol, N. Walenta, and H. Zbinden. Long-term performance of the swissquantum quantum key distribution network in a field environment. *New J. Phys.*, 13(12):123001, 2011.

[133] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten. High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New J. Phys.*, 11:075003, 2009.

[134] T. Sugimoto and K. Yamazaki. A study on secret key reconciliation protocol "cascade". *IEICE Trans. Fundamentals*, E83-A(10):1987–1991, october 2000.

[135] T. Symul, V. Sharma, T. C. Ralph, and Ping Koy Lam. Coherent state quantum key distribution with continuous-wave laser beams. In *Optical Fiber Communication Conference*, page OWC6. Optical Society of America, 2010.

[136] Thomas Symul, Daniel J. Alton, Syed M. Assad, Andrew M. Lance, Christian Weedbrook, Timothy C. Ralph, and Ping Koy Lam. Experimental demonstration of post-selection-based continuous-variable quantum key distribution in the presence of gaussian noise. *Phys. Rev. A*, 76:030303, Sep 2007.

[137] H. Takesue, S.-W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto. Quantum key distribution over a 40-db channel loss using superconducting single-photon detectors. *Nature Photon.*, 1:343–348, 2007.

[138] I. Tal and A. Vardy. List decoding of polar codes. In *IEEE International Symposium on Information Theory*, pages 1–5, 2011.

[139] Shingo Tokunaga, Kazuya Shirasaki, and Takuya Hirano. Free-space continuous-variable quantum cryptography. In *CLEO/Europe and IQEC 2007 Conference Digest*, volume IC 5. Optical Society of America, 2007.

[140] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Omer, M. Furst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger. Entanglement-based quantum communication over 144 km. *Nature Physics*, 3(7):481–486, June 2007.

[141] Vladyslav C. Usenko and Radim Filip. Feasibility of continuous-variable quantum key distribution with noisy coherent states. *Phys. Rev. A*, 81:022318, Feb 2010.

[142] G. Van-Assche. *Quantum Cryptography and Secret-Key Distillation.* Cambridge University Press, New York, NY, USA, 2006.

[143] G. Van Assche, J. Cardinal, and N. J. Cerf. Reconciliation of a Quantum-Distributed Gaussian Key. *IEEE TRANS.INFORM.THEORY*, 50:394, 2004.

[144] N. Walk, T. Symul, P.-K. Lam, and T. C. Ralph. Gaussian post-selection for continuous variable quantum cryptography. *Preprint at http://arxiv.org/abs/1206.0936*, 2012.

[145] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam. Quantum Cryptography Without Switching. *Phys. Rev. Lett.*, 93:170504, 2004.

[146] C. Weedbrook, S. Pirandola, S. Lloyd, and T.C. Ralph. Quantum cryptography approaching the classical limit. *Phys. Rev. Lett.*, 105(11):110501, 2010.

[147] C. Weedbrook, S. Pirandola, and T.C. Ralph. Continuous-variable quantum key distribution using thermal states. *Phys. Rev. A*, 86:022318, Aug 2012.

[148] 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.

[149] M. N. Wegman and L. Carter. New Hash Functions and Their Use in Authentication and Set Equality. *Journal of Computer and System Sciences*, 22(3):265–279, June 1981.

[150] Mark N. Wegman and Larry Carter. New classes and applications of hash functions. In *FOCS*, pages 175–182, 1979.

[151] M. M. Wilde and S. Guha. Polar codes for classical-quantum channels. *IEEE Transactions on Information Theory*, 59(2):1175 – 1187, 2013.

[152] A. Winter. Coding theorem and strong converse for quantum channels. In *IEEE Transactions on Information Theory*, volume 45, pages 2481–2485, Piscataway, NJ, USA, 1999. IEEE Press.

[153] Michael M. Wolf, Geza Giedke, and J. Ignacio Cirac. Extremality of gaussian quantum states. *Phys. Rev. Lett.*, 96:080502, Mar 2006.

[154] S.K. Lamoreaux J.R. Torgerson G.H. Nickel C.H. Donahue W.T. Buttler and C.G. Peterson. Fast, efficient error reconciliation for quantum cryptography. *Phys. Rev. A*, 67:052303, may 2003.

[155] F. Xu, B. Qi, and H.K. Lo. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New J. Phys.*, 12:113026, 2010.

[156] Nelly Ng Huei Ying, Siddarth K. Joshi, Chia Chen Ming, Christian Kurtsiefer, and Stephanie Wehner. Experimental implementation of bit commitment in the noisy storage model. *Nature communications*, 3(1326), 2012.

[157] B. Zhang, C. Yuan and K. Parhi. Reduced-latency sc polar decoder architectures. In *Proceedings of IEEE International Conference on Communications*, 2012.

[158] Y-B. Zhao, Y-Z. Gui, J-J. Chen, Z-F. Han, and G-C. Guo. Computational complexity of continuous variable quantum key distribution. *IEEE Trans. Inf. Theor.*, 54(6):2803–2807, June 2008.

[159] 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.

Sécurité et performance de dispositifs de distribution quantique de clés à variables continues

Paul JOUGUET

RESUME : L'objet de cette thèse est l'étude de la distribution quantique de clés, une primitive cryptographique qui permet à deux utilisateurs distants de générer une quantité arbitraire de clé secrète et cela y compris en présence d'un espion, sous réserve qu'ils partagent un secret initial. Nous restreignons notre étude aux protocoles employant des variables continues et démontrons expérimentalement une implémentation entièrement fibrée fonctionnant à 80 km sur une fibre dédiée en prenant en compte toutes les imperfections expérimentales connues. Pour atteindre une telle distance de fonctionnement, nous avons mis au point des codes correcteurs d'erreurs spécifiques fonctionnant près de la limite théorique de Shannon dans des régimes de faible rapport signal à bruit. Nous envisageons également la possibilité d'attaques par canaux cachés qui ne sont donc pas prises en compte dans la preuve de sécurité du système et proposons des contre-mesures. Enfin, nous étudions la compatibilité de notre système avec des canaux de communication intenses qui se propagent sur la même fibre optique.

MOTS-CLEFS : cryptographie quantique, cryptographie classique, distribution quantique de clés, optique quantique, théorie de l'information, codes correcteurs d'erreurs, communications quantiques, canaux cachés, attaques sur les systèmes quantiques, multiplexage en longueur d'onde.

ABSTRACT : This thesis focuses on a cryptographic primitive that allows two distant parties to generate an arbitrary amount of secret key even in the presence of an eavesdropper, provided that they share a short initial secret message. We focus our study on continuous-variable protocols and demonstrate experimentally an all-fiber system that performs distribution of secret keys at 80 km on a dedicated fiber link while taking into account all known imperfections. We could extract secret keys at such a distance by designing specific error correcting codes that perform very close to Shannon's bound for low signal to noise ratios. We also consider side-channel attacks that are not taken into account into the system security proof and propose some countermeasures. Finally, we study our system compability with intense communication channels that propagate on the same optical fiber.

KEY-WORDS : quantum cryptography, classical cryptography, quantum key distribution, quantum optics, information theory, error correcting codes, quantum communications, side channels, quantum hacking, wavelength division multiplexing.