



Trinity College Dublin

Coláiste na Tríonóide, Baile Átha Cliath

The University of Dublin

Hybrid Quantum Noise Model for Gaussian Quantum Channels: Development, Optimization, and Applications

PHD THESIS

TRINITY COLLEGE DUBLIN
THE UNIVERSITY OF DUBLIN
SCHOOL OF NATURAL SCIENCES

Author:

Mouli Chakraborty
19338026

Supervisor:

Dr. Subhash Chandra

Co-supervisor:

Dr. Avishek Nag

Submitted in 2025

*for the partial fulfillment of the degree of
Doctor in Philosophy*

Declaration of Work

I hereby declare that this dissertation is entirely my work and has not been submitted as an exercise for a degree at this or any other university.

I have read and understand the plagiarism provisions in the current year's General Regulations of the University Calendar, found at <http://www.tcd.ie/calendar>.

I have completed the Online Tutorial on avoiding plagiarism 'Ready Steady Write', at <http://tcd-ie.libguides.com/plagiarism/ready-steady-write>.

I consent to the examiner retaining a copy of the thesis beyond the examining period, should they so wish (EU GDPR May 2018).

I agree that this thesis will not be publicly available but will be available to TCD staff and students in the University's open-access institutional repository on the Trinity domain only, subject to Irish Copyright Legislation and Trinity College Library conditions of use and acknowledgment. **Please consult with your supervisor on this last item before agreeing, and delete if you do not consent.**

Signed: Mouli Chakraborty. Date: 28/02/2025

Acknowledgements

I extend my deepest gratitude to all those whose valuable support and encouragement have made this PhD journey possible. First and foremost, I am profoundly grateful to my supervisor, Professor Dr. Subhash Chandra, School of Natural Sciences, Trinity College Dublin, the University of Dublin, for his unwavering guidance, insightful mentorship, and constant encouragement. His vision, dedication, and meticulous approach have shaped my academic growth and instilled in me the discipline and perseverance necessary for rigorous research.

I sincerely thank my co-supervisor, Dr. Avishek Nag, School of Computer Science, University College Dublin, for his belief in my potential, even when I was at the earliest stage of my research career. His ability to provide clear direction while allowing room for exploration was instrumental in successfully structuring and completing this PhD. A heartfelt note of appreciation goes to Dr. Anshu Mukherjee, whose steadfast support from my first steps in Dublin to every phase of this journey has made this experience both rewarding and worthy.

I am also profoundly grateful to Professor Biswajit Basu and Professor Sara McCormack, Department of Civil, Structural, and Environmental Engineering, Trinity College Dublin, the University of Dublin, for their continued support and guidance. I extend my appreciation to the College GP Surgery, Counselling Service, and College Health Service at Trinity College Dublin, as well as Martin McAndrew, Postgraduate Student Support Officer at TCD for their assistance during challenging times.

I am indebted to Professor Siobhan Clarke, Co-Lead of the SFI Centre for Research Training in Advanced Networks for Sustainable Societies (SFI ADVANCE CRT), Trinity College Dublin, the University of Dublin, for her support from the beginning of my PhD. Thanks also to Luis Gómez de Membrillera, Senior Research Co-ordinator and CRT Program Manager at ADVANCE, and James Duggan, Research Support Officer for ADVANCE, University College Cork, for their guidance.

I gratefully acknowledge Professor Ioannis Krikidis, IEEE Fellow and Head of the IRIDA Research Laboratory for Communication Technologies, University of Cyprus, whose collaboration and mentorship in the doctoral internship played a pivotal role in shaping this research. Special thanks to the IRIDA Research Laboratory group for their generous support and insightful discussions. I remain indebted to Professor Krikidis, whose keen

intellect and invaluable feedback refined my research and inspired me to embark on this PhD journey. I would also like to thank Prof. Trung Q. Duong, IEEE Fellow, Canada Excellence Research Chair in Next Generation Communications Technologies and Full Professor, Faculty of Engineering and Applied Science, Memorial University of Newfoundland, Canada, and Professor, School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, Belfast, U.K, for his invaluable feedback and co-authorship in this research.

I acknowledge Trinity College Dublin, the University of Dublin, for providing the foundation that led me to this academic pursuit and fostering an environment of excellence and support. The Hamilton Library, Trinity College Dublin, has been instrumental in shaping my research path through its extensive book collection and reading support, which provided invaluable resources for my studies.

Finally, my deepest gratitude is reserved for my husband, parents, and family. Your sacrifices and unwavering support have been the cornerstone of my achievements. To my beloved husband, your insight, experience, and encouragement have been my most significant source of strength. Without you, this journey would not have been the same.

This PhD is not only a milestone but also a shared achievement with all who have supported, challenged, and believed in me throughout this journey.

Abstract

Quantum Gaussian channels are fundamental to the secure and efficient transmission of quantum information; however, quantum noise significantly impacts their performance in computing, cryptography, and communication. This research develops, optimizes, and validates a hybrid quantum noise model (HQNM) to enhance the understanding of quantum Gaussian channels. The study is structured into three parts: (I) Model Development and Analysis, where a hybrid quantum noise model combining Poissonian noise and classical additive white Gaussian noise (AWGN) is introduced. Closed-form capacity expressions are derived, confirming that Gaussian inputs achieve the highest data rates across different signal-to-noise ratios (SNR). The hybrid noise is modeled as a finite Gaussian mixture with Poisson-distributed weights, providing deeper insights into noise structure and optimization. Graphical representations enhance visualization, showing correlations between quantum Poissonian noise and classical AWGN. Additionally, entropy-based analysis refines the estimation of quantum channel capacity, offering more profound insights into entropy-driven noise effects. (II) Optimization and Validation incorporate machine learning (ML) techniques to improve quantum noise modeling. Hybrid noise is reformulated as a Gaussian mixture model (GMM), with the Expectation-Maximization (EM) algorithm dynamically updating channel parameters for optimal noise clustering. ML-based refinements significantly enhance capacity estimation and noise compensation, thereby improving signal accuracy across a range of SNR levels. (III) Applications in quantum key distribution (QKD) extend the HQN framework to satellite-based QKD, integrating quantum Poissonian noise and AWGN into a free-space quantum channel model. The study evaluates SKR performance under different reconciliation efficiencies, SNRs, and satellite altitudes, introducing a finite-regime QKD analysis. The findings establish a foundational framework for optimizing quantum communication, bridging the gap between theoretical noise models and real-world satellite quantum networks.

Contents

Declaration of Work	i
Acknowledgements	iii
Abstract	v
List of Figures	xii
List of Tables	xvii
List of Acronyms	xix
Nomenclature	xxiii
List of Publications	xxv
1 Introduction	1
1.1 Quantum Communication: A Mathematical and Physical Framework	2
1.2 Hybrid Quantum Noise in Quantum Communication Networks	5
1.3 Entropy of Quantum Channel	7
1.4 Optimization in Quantum Channel	9
1.5 Application of Hybrid Quantum Channel	11
1.6 Research Questions:	14
1.7 Aim and Objectives:	15
1.8 Thesis Structure	17
1.9 Conclusion	18
2 Background & Literature Review	19
2.1 Quantum Communication Networks	19
2.2 Noise in Quantum Channel	20
2.2.1 Entropy Estimation of Quantum Communication System	23
2.3 Optimization of Quantum Channel	26
2.4 Application of Quantum Channel in quantum key distribution (QKD)	29
2.4.1 Continuous-variable and Discrete-variable QKD	35
2.4.2 Direct Reconciliation and Reverse Reconciliation	36

2.4.3	Asymptotic QKD versus Finite Regime	37
2.5	Conclusion	39
3	Hybrid Quantum Noise Modeling for Quantum Channels	41
3.1	Introduction	41
3.2	System Model	44
3.2.1	Gaussian Quantum Channel	44
3.2.2	Qubit Model	45
3.3	Methodology	47
3.4	Quantum Noise Model	49
3.5	Quantum Signal Model for Gaussian Input	51
3.5.1	Quantum Transmitted Signal Model	52
3.5.2	Quantum Received Signal Model	52
3.6	Gaussian Mixture Model	57
3.6.1	Identifying Noise Model as GMM	59
3.6.2	Identifying Received Signal Model as GMM	59
3.7	Capacity for the Gaussian Input Quantum Channel	60
3.8	Quantum Signal Model for Non-Gaussian Input	62
3.9	Identifying Quantum Signal Models as Gaussian mixture model (GMM)s for Non-Gaussian Input	63
3.10	Capacity of the Quantum Channel for Non-Gaussian Input	64
3.11	Numerical Analysis	66
3.11.1	Noise Model Visualization	66
3.11.2	Output Signal Model's Visualization	67
3.11.3	Capacity Comparisons with respect to Signal-to-noise ratio	68
3.12	Conclusion	70
4	Hybrid Quantum Noise Approximation and Pattern Analysis	71
4.1	Introduction	71
4.2	System Model	72
4.2.1	hybrid quantum noise (HQN) Model Analysis	74
4.3	Numerical Analysis	76
4.3.1	HQN Model Visualization	76
4.4	Conclusion	78
5	Entropy Estimation of Hybrid Quantum Noise Channels	81
5.1	Introduction	81
5.2	System model	82
5.2.1	Quantum Entropies of Quantum Communication Channels	82
5.2.2	Entropy of Satellite Quantum Channel	84
5.3	Quantum Entropies of HQN Channel	86
5.3.1	Differential Entropy of HQN	87
5.3.2	Von Neumann Entropy of the HQN	89
5.3.3	Quantum Rényi Entropy of HQN	90

5.3.4	Hartley Entropy (Max-Entropy) of HQN	92
5.3.5	Quantum Collision Entropy of HQN	92
5.3.6	Min-Entropy of HQN	94
5.3.7	Quantum Unified Entropy of HQN	95
5.3.8	Quantum Tsallis Entropy of HQN	96
5.3.9	Quantum Mutual Information of Hybrid Quantum Noisy Channel	97
5.4	Application of Quantum Entropies in Quantum Tomography	98
5.5	Results and Analysis	101
5.6	Conclusion	109
6	Optimization of Hybrid Quantum Noise Model	111
6.1	System Model for the Quantum Communication Channel . .	112
6.1.1	Gaussian Quantum Channel Model	112
6.1.2	Hybrid Noise model	113
6.1.3	Quantum Transmitted Signal Model	113
6.2	Methodology of Quantum Noise Cluster Classification for Quantum Communication	114
6.2.1	Clustering with Gaussian Mixture Model	114
6.2.2	Maximization of log-likelihood to find optimal para- metric values for classifying the clusters:	119
6.2.3	Expectation-Maximization Algorithm (expectation-maximization (EM)):	121
6.2.4	The convergence of EM algorithm in the context of log-likelihood function	121
6.2.5	Discussion on selecting GMM in comparison to exist- ing machine learning (ML) models	122
6.2.6	Model Evaluation Metrics	124
6.3	Application in Maximization of Quantum Channel Capacity	125
6.4	Results and Numerical Analysis	127
6.4.1	Performance Comparison between Density-based spa- tial clustering of applications with noise (DBSCAN), K-means, and GMM-assisted EM Algorithm	128
6.5	Conclusion	140
7	Hybrid Noise Approach to Modeling of Free-Space Satellite Quantum Channel for CV-QKD	141
7.1	Introduction	141
7.2	System Model for Free-space Satellite Quantum Communi- cation	144
7.2.1	The Uplink and Downlink Scenarios in Quantum Satel- lite Communication	144
7.2.2	A Generalised CV-Gaussian Quantum Channel Model	145
7.2.3	The CV-Gaussian Quantum Channel Model for Satel- lite Quantum Communication	147

7.3	Methodology of Quantum Cryptography for Free-space Satellite Quantum Communication	149
7.3.1	Secret Quantum Key Distribution through free-space optics (FSO) Satellite Quantum Channel	149
7.3.2	Propagation Channel Model for FSO Satellite Quantum Communication	150
7.3.3	Analyzing the Transmission Efficiency for Satellite Quantum Channel	151
7.3.4	Received Signal Model for FSO Satellite Quantum Channel	152
7.3.5	Approximation of the Quantum Signal Models for Entropy Estimation	153
7.3.6	Capacity of FSO quantum satellite channel	155
7.3.7	Asymptotic Secret Quantum Key Rate Estimation for FSO Satellite Quantum Channel	157
7.3.8	A comparison study with finite-size secret key rate (SKR) for FSO satellite quantum channel	160
7.4	Results: Numerical Analysis	163
7.5	Conclusion	168
8	A Hybrid Noise Model for Satellite Quantum Channels: CV-QKD in the Finite-Size Regime	171
8.1	Introduction	171
8.2	System Architecture	172
8.2.1	Gaussian Quantum Channel and Noise Modeling	172
8.2.2	Finite-Size SKR in CV-QKD Systems	174
8.2.3	Aggregated Quantum SKR for Satellite Quantum Channel	175
8.2.4	Calculation of the Received Signal Model for FSO Satellite Quantum Channel	177
8.2.5	Feasible Zones and Geometric Considerations for Finite Regime SKR in continuous-variable quantum key distribution (CV-QKD) using Satellite Quantum Channels	180
8.2.6	The security analysis of collective attacks in the finite-key setting in Satellite-Based CV-QKD	185
8.3	Results and Numerical Analysis	187
8.4	Conclusion	194
9	Conclusion	197
9.1	Future Works:	198
	Appendix	201
A	Qubits Model	201

B Quantum Collision Entropy of Hybrid Quantum Noise Approximated as Differential entropy	205
C Proof of Lemma 1 and 2	207
C.0.1 Proof of Lemma 1	207
C.0.2 Proof of Lemma 2	208
C.0.3 The conditional density $f_{\mathbf{Z}}(\mathbf{z} t_k = 0)$ given that $\mathbf{z}$ does not belong to the k -th Gaussian component . . .	211
Bibliography	230

List of Figures

1.1	The flowchart of the research work.	16
3.1	The categorization of noise and capacity factor of the Gaussian quantum channel.	43
3.2	With feasible HQN power, the qubit remains within a torus-like object with a cuboid cross-sectional area inside the Bloch sphere after experiencing the HQN.	46
3.3	A noisy Quantum Channel: A schematic diagram showing a single quantum link between transmitter and receiver. H is the channel matrix, Z is the HQN as a convolution of quantum Poissonian noise Z_1 and additive white Gaussian noise Z_2 . The complete received signal can be modeled using the channel equation $Y = X + Z$, where X is the transmitted signal.	48
3.4	The block diagram explains the flow of the research methodology for Gaussian and non-Gaussian transmitted signals. . .	50
3.5	Quantum Noise model as a convolution of AWGN and Poissonian quantum noise	66
3.6	Received signal in case of Gaussian input, considered as a convoluted function of the quantum noise field and a Gaussian transmitted signal for the Gaussian quantum channel . .	67
3.7	Received signal in case of non-Gaussian input, considered as a convoluted function of quantum noise field and non-Gaussian transmitted signal for a Gaussian quantum channel	68
3.8	The channel capacity of the Gaussian quantum channel for the non-Gaussian input transmitted signal	69
3.9	The channel capacity of the Gaussian quantum channel for the Gaussian input transmitted signal	70
4.1	HQN model as a convolution of additive white Gaussian and quantum Poissonian noise with parameter $\lambda = 2$ and number of mixing components $R = 20$	73
4.2	A HQN model for $\lambda = 5$ and number of mixing components $R = 20$. Here, the Poisson parameter λ is adequately balanced by a sufficient number of Gaussian components.	74

4.3	A HQN model for $\lambda = 10$ and number of mixing components $R = 20$. This approximation is sufficient to capture the actual behaviour of the quantum noise and, hence, the entropy of the HQN.	75
4.4	HQN model for $\lambda = 20$ and number of mixing components $R = 20$. Here λ , it is not adequately balanced by a sufficient number of Gaussian components.	76
4.5	HQN model for $\lambda = 10$ and number of mixing components $R = 10$. This approximation fails to capture the actual behaviour of the quantum noise.	77
4.6	HQN model for $\lambda = 20$ and number of mixing components $R = 30$. Here, the Poisson parameter λ is adequately balanced by a sufficient number of Gaussian components; the approximation suffices to capture the actual behaviour of the quantum noise and hence the entropy of the HQN.	78
5.1	3D representation of Hybrid Quantum Noise using Gaussian Mixture Model (GMM).	100
5.2	The 3D representation of the differential entropic function of HQN. This entropic function's integration gives the required differential entropy of the HQN.	101
5.3	The 3D representation of the von-Neumann entropic function of HQN. This integration of the entropic function gives the required von Neumann entropy of the HQN.	102
5.4	The 3D representation of the quantum Rényi entropic function of HQN. This entropic function's integration gives the required quantum Rényi entropy of the HQN.	103
5.5	The 3D representation of the quantum Tsallis entropic function of HQN. This entropic function's integration gives the required quantum Tsallis entropy of the HQN.	104
5.6	The 3D representation of the quantum collision entropic function of HQN. This entropic function's integration gives the required quantum collision entropy of the HQN.	105
5.7	The 3D representation of the quantum tomographic entropic function of HQN. This entropic function's integration gives the required quantum tomographic entropy of the HQN.	106
5.8	The 3D representation of the quantum conditional entropic function of HQN. The integration of this entropic function yields the required quantum conditional entropy of the HQN and the received quantum data.	107
5.9	The 3D representation of the quantum mutual information function between transmitted quantum state data and the received quantum state data under HQN.	108

6.1	A generalized categorization of HQN data in two dimension space: (a) Original data (termed as Ground Truth) with specific cluster; (b) Unlabeled data for finding the original clusters; (c) GMM used for soft-clustering; (d) Responsibility of a cluster. Note that the x-coordinates and y-coordinates of the bi-variate data points are considered along the graphs' X-axis and Y-axis.	115
6.2	The process of updating channel parameters and finding optimal clusters of HQN using ML model.	118
6.3	The ground truth data of bivariate quantum noise sampling generated as a convolution of additive white Gaussian noise and Poissonian quantum noise. In our studies, the ground truth of the HQN data has been generated from the component GMMs.	126
6.4	HQN data clustering under DBSCAN.	127
6.5	Initial K-means setup: Five random centroids (eyes) define starting cluster means for HQN data points.	128
6.6	Clusters after 1st iteration under K-Mean.	129
6.7	After 12th iterations: Centroids shift toward data-dense regions with improved cluster separation.	129
6.8	Convergence at iteration 24th: Stabilized centroids minimize within-cluster variance, yielding five distinct clusters representing dominant quantum noise modes.	130
6.9	Initial Gaussian mixture clusters: Five colored spiral datasets with centroids (eyes) representing initial Gaussian component means.	131
6.10	After 10 iterations: Updated Gaussian mixture components for bivariate quantum noise clustering.	132
6.11	Final result at iteration 20: Converged Gaussian mixture clusters.	132
6.12	Log-likelihood convergence: EM algorithm convergence curves for $\lambda = 2$ and $\lambda = 5$, with curve saturation indicating cluster optimization completion.	133
6.13	Silhouette analysis: Identifies $K = 5$ as optimal cluster count with highest average silhouette score for HQN data.	134
6.14	Bayesian Information Criterion (BIC) and Akaike Information Criterion (AIC) analysis: Confirms $K = 5$ as optimal, optimizing the overfitting and underfitting while capturing underlying data structure.	135
6.15	The achievable rate of the general quantum channel.	136
6.16	The achievable rate of the satellite quantum channel with respect to signal-to-noise ratio (SNR).	137

7.1	A basic model for Quantum Satellite Communication can be replicated with multiple base stations or satellites for the feasibility of long-distance communication and QKD; it also forms a basis of the quantum internet.	144
7.2	A schematic diagram showing a single quantum link between transmitter and receiver under the satellite communication system.	146
7.3	The atmospheric turbulence with beam-wandering. Due to various atmospheric conditions, considering the beam-wandering model for uplinks and downlinks for satellites is useful, and it shows realistic scenarios in detecting the secret key rate. .	148
7.4	The beam-wandering model for laser direction. The red circle shows the position of the incoming beam on the receiver's aperture; the black circle represents the receiver's aperture. .	149
7.5	Impact of Reconciliation Efficiency on Quantum SKR. . . .	160
7.6	Impact of Electrical Noise on Quantum SKR.	161
7.7	Impact of Transmission Coefficient on Quantum SKR	162
7.8	Impact of Detection Efficiency on Quantum SKR	163
7.9	Impact of Transmission Efficiency on Quantum SKR	165
7.10	Impact of Excess Noise on Asymptotic Quantum SKR based on satellite altitude.	166
7.11	Impact of Quantum Poissonian Noise on Quantum SKR . .	167
7.12	Asymptotic Quantum SKR versus Finite-size Quantum SKR with respect to Satellite altitudes.	168
8.1	The diagram visually emphasizes how the satellite's position relative to the ground station affects the feasibility and efficiency of quantum communication. The central green region is crucial for secure QKD, while the other zones highlight the limitations imposed by satellite motion and atmospheric conditions.	173
8.2	Geometric configuration of satellite-to-ground communication. S represents the satellite, G the ground station, and O the Earth's center. The satellite altitude is denoted by h , the Earth's radius by R_E , and the slant range by R_S . The zenith angle θ and the elevation angle α are measured relative to the ground station. The parameter Z represents the satellite's position projected relative to the zenith. This diagram illustrates the key parameters affecting satellite communication geometry.	181
8.3	The relationship between the finite-size SKR and SNR for different values of reconciliation efficiency (β). The analysis explores how β influences the SKR in satellite quantum communication under varying SNR conditions.	188

8.4	The relationship between the finite-size SKR and satellite altitude for varying receiver telescope apertures a_r . The analysis demonstrates the impact of aperture size on the SKR performance in satellite-based quantum communication systems.	189
8.5	Variation of finite-size SKR with SNR for different transmission coefficients (T).	190
8.6	Variation of finite-size SKR with satellite altitude for different beam waist (w_0) values.	191
8.7	Dependence of finite-size SKR on effective communication time for different light source wavelengths.	192
8.8	Variation of finite-regime SKR with respect to the zenith angle for different SNR values.	193
8.9	Impact of detection efficiency η_{det} on finite-regime SKR at different satellite altitudes.	194
A.1	Case I: Representation of a pure state qubit on the Bloch sphere.	202
A.2	Case II: Representation of a mixed state qubit inside the Bloch sphere.	203

List of Tables

2.1	Comparative Summary of Key Literature in Quantum Communication and Hybrid Quantum Noise Modeling	33
6.1	Summary of Simulation Assumptions and Initializations . . .	138
6.2	Effect of Poisson Parameter λ on Cluster Weights and GMM Accuracy	138
6.3	Performance Comparison on HQN Clustering	139
8.1	Physical Parameter's Theoretical Value for QKD using Satellite Quantum Communication Channel	175

List of Acronyms

HQNM hybrid quantum noise model

HQN hybrid quantum noise

QEC quantum error correction

QBER quantum bit error rates

QMI quantum mutual information

QIP quantum information processing

s.d. standard deviation

RMS root mean square

RSA Rivest, Shamir and Adelman algorithm

ECC elliptic curve cryptography

LOQC linear optical quantum computing

CPTP completely positive trace-preserving

MAP maximum a posteriori

ML machine learning

DL deep learning

RL reinforcement learning

SVM support vector machines

PCA principal component analysis

KF Kalman filter

DBSCAN Density-based spatial clustering of applications with noise

GMDD Gaussian mixture density decomposition

WCSS within-cluster sum of squares

QML quantum machine learning

NN neural network

EM expectation-maximization

GM Gaussian mixture

p.d.f. probability density function

p.m.f. probability mass function

CDF cumulative distribution function

r.v. random variable

SNR signal-to-noise ratio

SPS single-source photon

GMM Gaussian mixture model

GMs Gaussian mixtures

BIC Bayesian Information Criterion

AIC Akaike Information Criterion

AWGN additive-white-Gaussian noise

OGS optical ground station

SKR secret key rate

QKD quantum key distribution

PNS photon number splitting

CV-QKD continuous-variable quantum key distribution

FSO free-space optics

MDI measure-device-independent

DV-QKD discrete-variable quantum key distribution

CV continuous variables

DV discrete variables

DR direct-reconciliation

RR reverse-reconciliation

CPTP completely positive, trace preserving

PM Prepare-and-Measure

PDTC probability distribution of transmission coefficient

PDTE probability distribution of transmission efficiency

S/C spacecraft

GS ground station

LDPC Low-Density Parity Check

LEO Low Earth Orbit

MEO Medium Earth Orbit

GEO Geostationary Earth Orbit

Eve eavesdropper

QE quantum entanglement

GMCS Gaussian-modulated coherent state

DRL deep reinforcement learning

ANN artificial neural network

CNN convolutional neural network

KNN K-nearest neighbours

MLP multilayer perceptron

DWDM dense wavelength-division multiplexing

AI artificial intelligence

AE autoencoder

KL Kullback-Leibler

MLE maximum likelihood estimation

A.R. achievable rate

Nomenclature

Symbol	Quantity
tr	The trace of a matrix
$\mathbf{T}(\cdot)$	Trace-preserving map $\mathbf{T}$
$\mathbf{A}^\dagger$	The adjoint of matrix $\mathbf{A}$
$\mathbf{A}^T$	The transpose of matrix $\mathbf{A}$
ν^*	The complex conjugate of ν
$\otimes$	The tensor product
$ \cdot\rangle$	The ket
$\langle\cdot $	The bra
$ \cdot $	The norm

List of Publications

1. M. Chakraborty, A. Mukherjee, A. Nag, and S. Chandra, "Hybrid Quantum Noise Model to Compute Gaussian Quantum Channel Capacity," in IEEE Access, vol. 12, pp. 14671-14689, 2024, doi: 10.1109/ACCESS.2024.3355789.
2. M. Chakraborty, A. Mukherjee, I. Krikidis, A. Nag, and S. Chandra, "Hybrid Quantum Noise Approximation and Pattern Analysis on Parameterized Component Distributions," 2024 IEEE Middle East Conference on Communications and Networking (MECOM), Abu Dhabi, United Arab Emirates, 2024, pp. 251-256, doi: 10.1109/MECOM61498.2024.10881051.
3. M. Chakraborty, A. Mukherjee, I. Krikidis, A. Nag and S. Chandra, "A Hybrid Noise Approach to Modeling of Free-Space Satellite Quantum Communication Channel for Continuous-Variable QKD," in IEEE Transactions on Green Communications and Networking, vol. 9, no. 3, pp. 1311-1325, Sept. 2025, doi: 10.1109/TGCN.2024.3525297.
4. M. Chakraborty, A. Mukherjee, I. Krikidis, A. Nag, and S. Chandra, "An Unsupervised Machine Learning to Optimize Hybrid Quantum Noise Clusters for Gaussian Quantum Channel," in IEEE Transactions on Green Communications and Networking, doi: 10.1109/TGCN.2025.3587144.

Publications under Review Process :

1. Chakraborty, M., Mukherjee, A., Duong, T. Q., Nag, A., and Chandra, S., 2025. A Hybrid Noise Model for Satellite Quantum Communication Channels: Continuous-Variable Quantum Key Distribution in the Finite-Size Regime. arXiv preprint arXiv:2501.0
2. Chakraborty, M., Mukherjee, A., Nag, A., and Chandra, S., 2024. Entropies in Satellite Quantum Communication: A Comprehensive Overview of the Hybrid Quantum Noisy Channel. arXiv preprint arXiv:2502.0

Chapter 1

Introduction

In the digital age, secure communication is no longer a luxury but a necessity. Protecting sensitive information has become paramount with the increasing reliance on internet-based transactions, cloud computing, and global data sharing. Traditional cryptographic methods, such as Rivest, Shamir and Adelman algorithm ([RSA](#)) and elliptic curve cryptography ([ECC](#)), have been the backbone of secure communication for decades [1]. However, the rapid advancements in quantum computing pose an existential threat to these classical encryption schemes, necessitating the search for alternative solutions. Current encryption systems heavily rely on mathematical problems that are computationally infeasible to solve using classical computers. For instance, [RSA](#) encryption is based on the difficulty of factoring large prime numbers, while [ECC](#) security is derived from the hardness of the discrete logarithm problem. However, with the development of quantum computers, these problems can be solved efficiently using algorithms like Shor's algorithm [2], rendering current cryptographic standards obsolete. Governments, businesses, and financial institutions face a critical challenge: maintaining secure communication in a future where quantum adversaries can break existing encryption schemes in polynomial time. The race to develop quantum-resistant security solutions is not just theoretical. It is urgent to safeguard digital infrastructure against the inevitable advent of large-scale quantum computing.

Quantum communication represents a paradigm shift in information transmission, holding significant potential to become a faster and highly secure communication technology. In quantum communication, the quantum states serve as information carriers. In contrast to classical communication, which relies on deterministic signal properties, quantum communication leverages the probabilistic and non-local nature of quantum mechanics to ensure the security and efficiency of information communication. Quantum mechanics' foundational principles, including superposition, entanglement, and the no-cloning theorem, provide the theoretical basis for applications such as quantum key distribution ([QKD](#)) [3], which offers encryption mechanisms immune to conventional eavesdropping techniques. Entanglement facilitates quantum teleportation, enabling the transfer of information from

one location to another without physically moving the particle or the information carriers.

Despite its promise, quantum communication faces significant challenges in implementation. Establishing long-distance networks requires advanced infrastructure, including satellite-based quantum communication or fiber-optic networks with quantum repeaters [4]. Additionally, practical challenges such as photon loss, noise, and the scalability of quantum technologies must be addressed before widespread adoption can be achieved. This is where the challenge becomes an opportunity. Integrating quantum communication with classical networks, developing quantum-resistant cryptographic protocols, and deploying multi-layered quantum communication architectures present a frontier for cutting-edge research. These challenges drive the need for interdisciplinary efforts spanning quantum physics, information theory, network engineering, and machine learning (ML) -driven optimization.

The motivation to explore quantum communication stems from the desire to create a secure information transfer through the digital communication network. The need to bridge the gap between classical and quantum communication, develop robust and scalable quantum cryptographic protocols, and integrate quantum security into real-world applications is more pressing than ever. The work in this field is not just about theoretical advancements—it is about pioneering solutions that will define the security of cryptographic systems in the future. From satellite-assisted quantum communication networks to artificial intelligence (AI)-driven optimization of QKD [5], the work in this domain has far-reaching implications for national security, financial transactions, and global data sovereignty. In a world where network threats continue to evolve, taking on the challenge of quantum-secured communication is not just an academic pursuit—it is a mission to safeguard the integrity of global communication network infrastructure. The transition to quantum communication is inevitable, and those who embrace it now will shape the future of secure communication in the quantum era.

1.1 Quantum Communication: A Mathematical and Physical Framework

Quantum communication is the process of transmitting quantum information using quantum states, typically leveraging principles such as superposition, entanglement, and quantum measurement [2]. A qubit is the fundamental unit of quantum information and is represented as a superposition of two basis states $|0\rangle$ and $|1\rangle$ given by [6],

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \text{where } \alpha, \beta \in \mathbb{C}, \quad |\alpha|^2 + |\beta|^2 = 1, \quad |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \quad (1.1)$$

The density matrix representation of a qubit is given by

$$\rho = |\psi\rangle\langle\psi| = \begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{bmatrix}. \quad (1.2)$$

Unlike classical communication, which transmits bits (0 or 1), quantum communication encodes information in qubits, which can exist in a superposition of states. This enables fundamentally new paradigms for secure communication, information transfer, and distributed quantum computing.

Quantum communication is fundamentally governed by the principles of quantum mechanics, which dictate how quantum information is generated, transmitted, and manipulated. In contrast to classical communication, where information is encoded in binary bits (0s and 1s), quantum communication uses qubits, which can exist in superposition states and exhibit entanglement. These quantum mechanical properties provide significant security and information transfer advantages, enabling protocols such as QKD and quantum teleportation [7]. To understand how quantum communication operates, it is essential to explore the foundational laws of quantum mechanics that govern its behaviour, including superposition, entanglement, the no-cloning theorem, and quantum measurement. One of the core principles of quantum mechanics is superposition [8], which allows a quantum system to exist in multiple states simultaneously.

This property enables quantum communication to encode and process more information per qubit than a classical bit, allowing for increased data efficiency in transmission. Entanglement is a uniquely quantum mechanical phenomenon in which two or more qubits become correlated, such that their quantum states cannot be described independently [9]. When two qubits are entangled, measuring the quantum state of one instantaneously determines the state of the other, regardless of the physical distance between them. It is a fascinating, counterintuitive phenomenon in which two subatomic particles remain deeply connected, even when separated by billions of light-years. This can help in quantum communication. This non-local correlation is a key resource in quantum communication protocols, particularly in QKD, where entanglement ensures that any eavesdropping attempt introduces detectable disturbances. A maximally entangled Bell state is given by,

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (1.3)$$

which means that if one qubit is measured as $|0\rangle$, the other must also collapse into $|0\rangle$, and similarly for $|1\rangle$. This property enables entanglement-based communication, where distant parties can share cryptographic keys with provable security.

In contrast to classical information, which can be copied without alteration, quantum information obeys the no-cloning theorem, which states that an arbitrary quantum state cannot be perfectly duplicated. Formally, if there existed a universal unitary operator U such that [10],

$$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle, \quad (1.4)$$

for all states $|\psi\rangle$, it would violate the linearity of quantum mechanics. This theorem is a cornerstone of quantum communication security, as it prevents an adversary from making perfect copies of transmitted qubits, ensuring that intercepted information cannot be stolen undetectably. This is particularly relevant for QKD, where eavesdropping inevitably disturbs the quantum states, alerting the communicating parties to the presence of an intruder.

Quantum communication is further constrained by the Heisenberg uncertainty principle [11], which states that specific pairs of quantum properties (e.g., position and momentum or different polarization bases) cannot be simultaneously measured with arbitrary precision. In the context of quantum communication, once a quantum state is measured, it collapses into a definite state, losing any prior superposition. This principle is exploited in QKD protocols, such as BB84 [7], where information is encoded in different polarization bases. Any unauthorized measurement by an eavesdropper disrupts the transmitted quantum states, leading to detectable anomalies in the key exchange process.

Quantum teleportation is a communication protocol that allows transferring an unknown quantum state from one location to another using entanglement and classical communication [12]. In contrast to the classical data transfer, where information physically propagates through a medium, quantum teleportation relies on shared entanglement between the sender and receiver. The process involves three main steps:

1. The sender, Alice, possesses an unknown quantum state $|\psi\rangle$ and an entangled pair shared with Bob.
2. Alice performs a joint Bell-state measurement on her qubit and part of the entangled pair, collapsing the system into one of four possible Bell states.
3. She sends the classical measurement results to Bob, who applies a corresponding unitary transformation to recover $|\psi\rangle$ on his side.

Mathematically, if Alice's unknown state is given by, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and she shares an entangled pair $|\Phi^+\rangle$, the teleportation process ensures that Bob's qubit is transformed into $|\psi\rangle$, despite the fact that the state itself was never physically transmitted. This protocol demonstrates the power of quantum communication, enabling long-distance transfer of quantum information without direct transmission of qubits.

A quantum channel is a mathematical representation of the physical process that governs the evolution of quantum states during transmission, storage, or interaction with an environment. It generalizes the concept of classical communication channels while incorporating the principles of quantum mechanics, such as superposition, entanglement, and decoherence. Formally, a quantum channel is a completely positive, trace preserving (CPTP) map that acts on the space of density matrices [2]. Let $\mathcal{H}$ be a Hilbert space associated with a quantum system. A quantum state is represented by a density matrix ρ , which satisfies, $\rho \geq 0$, $\text{Tr}(\rho) = 1$. A quantum channel $\mathcal{E}$ is a linear and CPTP map that transforms one density operator into

another [3],

$$\mathcal{E} : \mathcal{B}(\mathcal{H}) \rightarrow \mathcal{B}(\mathcal{H}), \quad (1.5)$$

where $\mathcal{B}(\mathcal{H})$ is the space of bounded operators on $\mathcal{H}$. The action of a quantum channel on a density matrix is commonly expressed using the Kraus representation,

$$\mathcal{E}(\rho) = \sum_i \mathbf{K}_i \rho \mathbf{K}_i^\dagger \quad (1.6)$$

where the operators $\mathbf{K}_i$ (called Kraus operators) satisfy the trace-preserving condition [13, 14],

$$\sum_i \mathbf{K}_i^\dagger \mathbf{K}_i = I. \quad (1.7)$$

This ensures that probabilities remain correctly normalized after the channel is applied. A unitary quantum channel represents the ideal, noise-free evolution of a quantum state. It is defined by a single Kraus operator, which is a unitary matrix $\mathbf{U}$ [10],

$$\mathcal{E}(\rho) = \mathbf{U} \rho \mathbf{U}^\dagger. \quad (1.8)$$

A more detailed description of quantum noisy channel [3, 6, 10] can be found in chapter 3 onwards.

1.2 Hybrid Quantum Noise in Quantum Communication Networks

Quantum communication has the potential to be of unmatched security and effectiveness in information transmission. In addition, it can address issues related to data and information security. Quantum communication involves transferring quantum information through a quantum channel among various entities using quantum-mechanical elements, such as photons. It facilitates functions such as quantum cryptography [15], quantum teleportation [16], and quantum networks [17]. Various approaches have been used to optimize the quantum channel using ML [18]. The inherent benefits of quantum communication are closely connected to addressing issues related to quantum noise, which arises from the interaction of quantum systems with their surroundings or during the measurement process and can significantly hinder the accuracy and dependability of quantum information transmission. Due to the high sensitivity of quantum systems to external interferences, quantum noise can result in the degradation of coherence and entanglement, which are vital aspects of quantum communication [6]. Approaches such as quantum error correction and decoherence-free subspaces aim to maintain the integrity of quantum information in the presence of inevitable noise [2].

Quantum noise comes in various forms, including quantum Poisson and classical noise, such as additive-white-Gaussian noise (AWGN) [19], [20]. Poisson noise is inherent to quantum systems due to the discrete nature

of light and matter, while **AWGN** originates from thermal fluctuations and electronic components in classical systems [11]. Managing these noise sources effectively is essential for maintaining the integrity of quantum communication channels, and hybrid noise models, combining both quantum and classical noise, are crucial for accurately capturing the full range of disturbances that affect such systems [18, 21, 22]. These models enable more realistic assessments of **QKD**, error rates, information capacity, and security, allowing for the optimization of quantum technologies [23, 24], [25].

Noise mitigation is crucial in determining the accuracy of information processing in the quantum channel. In this realm, the quantum channel's capacity is pivotal in determining the efficiency and accuracy of quantum information handling, with its performance being significantly influenced by channel noise. Quantum shot noise arises from the discrete nature of quantum particles, such as photons or electrons, and affects the transmission of quantum information [11]. It introduces uncertainty in the photon number, impacting quantum optical communication systems. A quantum shot noise channel is typically modeled using the phase-space representation of quantum mechanics, such as the Wigner function or the characteristic function approach [10]. The transformation of a quantum state due to shot noise can be represented by a Gaussian noise processing quadrature space.

For the photon-number-based model, let n be the number of received photons, which follows a Poisson distribution due to quantum fluctuations given by [11],

$$P(n) = \frac{(\lambda)^n e^{-\lambda}}{n!}, \quad (1.9)$$

where λ is the expected photon number at transmission.

The **AWGN** channel is a fundamental classical communication model where the transmitted signal is affected by additive Gaussian noise. It is widely used in quantum-classical hybrid systems, where quantum signals interact with classical noise. In an **AWGN** channel, the received signal Y is modeled as [18, 21, 22]

$$Y = X + N, \quad (1.10)$$

where X is the transmitted signal, N is a Gaussian noise with mean zero and variance σ given by [26, 27]

$$p(n) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-n^2/2\sigma^2}. \quad (1.11)$$

In the context of quantum optics, **AWGN** is modeled using heterodyne detection, where a coherent quantum state undergoes classical Gaussian noise.

A hybrid quantum-classical channel models the interplay between quantum noise (such as Poissonian shot noise) and classical noise (such as **AWGN**). This is particularly relevant in free-space quantum communication, where quantum signals are affected by both discrete quantum fluctuations and continuous classical noise sources. The hybrid quantum channel combines Poissonian shot noise (due to quantum uncertainty in photon detection)

and Gaussian noise(due to classical environmental disturbances) [26, 28]. The convolution of quantum Poissonian Shot Noise and classical [AWGN](#) gives the overall hybrid channel transformation on a quantum state ρ . This model is crucial for satellite-based quantum communication, where Poissonian shot noise arises due to the quantum nature of light and [AWGN](#) originates from atmospheric turbulence and electronic detection noise. The hybrid quantum channel represents a realistic model for quantum-classical communication systems, where quantum fluctuations and classical disturbances coexist. Understanding such channels is crucial for designing robust and secure quantum communication protocols, particularly in free-space optical and satellite quantum networks.

1.3 Entropy of Quantum Channel

Entropy, as a measure of the degree of uncertainty in a system, plays a central role in quantum mechanics and quantum information theory, in deciding the reliability of communication systems. Entropy in quantum communication quantifies uncertainty and information content, both of which are crucial for secure key distribution and error correction. It governs protocols like [QKD](#) by ensuring security through entropic uncertainty relations. Classical entropy concepts, such as Shannon entropy, have been extended to quantum systems to describe the complexity and randomness of quantum channels. Quantum entropy measures provide crucial insights into the properties of quantum channels, the efficiency of quantum communication protocols, and the impact of noise on quantum information processing. Understanding these entropy measures is fundamental in areas such as quantum computing, quantum cryptography, quantum networks, and quantum satellite communication.

Quantum entropy extends classical definitions to accommodate the probabilistic nature of quantum states. In contrast to classical probability distributions, quantum states are represented by density matrices, which necessitate alternative formulations of entropy measures. Several quantum entropy measures, including von Neumann entropy, Rényi entropy, Tsallis entropy, and differential entropy, have been developed to quantify different aspects of quantum uncertainty and information transfer.

The von Neumann entropy is a quantum analogue of Shannon entropy and is defined for a quantum state ρ as [6],

$$S(\rho) = -\text{Tr}(\rho \log \rho). \quad (1.12)$$

This entropy measure quantifies the mixedness of a quantum state. A pure state has zero entropy, while a maximally mixed state has the highest entropy. Von Neumann entropy is widely used in quantum communication to determine the efficiency of quantum channels and the degree of entanglement in multipartite systems. Studies have demonstrated that von Neumann entropy governs the transmission rates in quantum channels, influencing their capacity to transmit information securely. It also plays a

critical role in QKD and quantum error correction (QEC). In quantum satellite communication, von Neumann entropy helps evaluate the impact of decoherence due to environmental interactions.

Rényi entropy generalizes von Neumann entropy and introduces a tunable parameter α , defined as [29],

$$S_\alpha(\rho) = \frac{1}{1-\alpha} \log \text{Tr}(\rho^\alpha), \quad \alpha > 0, \alpha \neq 1. \quad (1.13)$$

Different values of α yield different entropy measures. For $\alpha = 1$, it reduces to von Neumann entropy, while for $\alpha = 0$, it corresponds to Hartley entropy. Rényi entropy has applications in quantum cryptography, where it provides insights into the security of key distribution protocols and quantum randomness extraction. Recent works have explored Rényi entropy in the context of HQN, where classical and quantum noise sources coexist. By adjusting the parameter α , Rényi entropy provides a flexible approach to assessing security levels in quantum networks.

Tsallis entropy is a non-extensive generalization of Shannon entropy, defined for a quantum state ρ as [29],

$$S_q(\rho) = \frac{1 - \text{Tr}(\rho^q)}{q - 1}, \quad q > 0, q \neq 1. \quad (1.14)$$

Unlike von Neumann entropy, Tsallis entropy captures non-linear correlations and long-range interactions in quantum systems. This entropy measure has been applied to quantum networks and error correction, where non-additivity properties become significant.

This fundamental concept underpins numerous aspects of quantum communication and networking. Different entropy measures—von Neumann, Rényi, Tsallis, differential, Hartley, and unified entropy—offer unique perspectives on information content and uncertainty in quantum systems [2]. The study of entropy in hybrid quantum noise environments is critical for optimizing quantum networks and ensuring the security and efficiency of quantum communication systems. Future work aims to refine entropy-based models to enhance the reliability of quantum internet infrastructure and satellite-based quantum communication.

In communication systems, entropy is used to assess the efficiency and reliability of signal transmission. The more uncertain or random the information source, the higher the entropy and the greater the challenges for effective and reliable communication. Entropy thus defines limits on the amount of information that can be transmitted over a communication channel, forming the backbone of error-correcting codes and data transmission protocols. In quantum systems, noise often introduces uncertainty, which can be quantified through the concept of entropy. Quantum noise arises from the interaction of quantum systems with their environments, resulting in decoherence and information loss. The entropy associated with quantum noise measures the degree to which the noise disrupts the system's coherence and fidelity, playing a key role in the design of QEC schemes.

1.4 Optimization in Quantum Channel

Clustering is a fundamental tool in data analysis, enabling the identification of patterns and relationships within complex datasets by grouping similar data points into clusters. In quantum noise modeling, clustering is essential because it allows us to separate overlapping noise sources—such as quantum shot noise and classical [AWGN](#) into meaningful categories. This distinction is crucial, as different noise patterns uniquely affect the quantum channel, influencing its capacity, performance, and the reliability of transmitted quantum information.

The hybrid quantum noise ([HQN](#)) model is inherently complex, involving a mixture of quantum and classical noise distributions. Without clustering, it becomes challenging to understand the structure of the noise and how various components contribute to the overall channel behaviour. The soft clustering methodology offered by the Gaussian mixture model ([GMM](#)) ensures that data points are not forced into a single cluster but can belong to multiple clusters with varying probabilities. This approach aligns with the probabilistic nature of quantum systems, where uncertainty and overlap are natural phenomena. The clustering can model these nuances effectively, leading to a deeper understanding of how noise behaves and interacts within the quantum channel [\[30\]](#).

In quantum noise modeling and communication systems, several advanced techniques beyond clustering offer alternative or complementary approaches. The deep learning ([DL](#)) models like neural network ([NN](#))s and autoencoder ([AE](#))s can uncover hidden patterns but demand high computational power [\[31\]](#). The reinforcement learning ([RL](#)) adapts to dynamic environments but requires extensive training and can be unstable. Bayesian Inference effectively handles uncertainty, but it is computationally intensive. The support vector machines ([SVM](#)) and kernel methods handle non-linear patterns well but struggle with large datasets. The principal component analysis ([PCA](#)) simplifies high-dimensional data but risks compromising information. Statistical signal processing techniques, such as Kalman filter ([KF](#)), focus on noise suppression but are less effective with irregular noise [\[32\]](#). The quantum machine learning ([QML](#)) promises an exponential speedup but is still experimental and hardware-dependent. Each technique has its pros and cons, and the choice depends on the specific needs of the quantum noise model, with some methods complementing clustering for enhanced performance and accuracy.

The clustering algorithms, such as K-means (centroid-based), Density-based spatial clustering of applications with noise ([DBSCAN](#)), hierarchical clustering, and distribution-based methods, are less suitable for this application [\[33\]](#). For instance: (I) Centroid-based clustering, e.g., K-means, is a popular clustering technique; it assumes that clusters are spherical and equally sized, which is a significant limitation in complex noise environments encountered in quantum systems. On the other hand, the [GMM](#) does not have this restriction and can model elliptical clusters with varying sizes. (II)

Density-based clustering, e.g., [DBSCAN](#), is an effective method for identifying arbitrarily shaped clusters; however, it is less effective when clusters are Gaussian-shaped and overlapping, as often observed in noise models. (III) Hierarchical clustering methods can capture nested clusters. They are computationally expensive and less efficient for high-dimensional data, making them impractical for real-time quantum noise classification. (IV) Distribution-based clustering, e.g., [GMM](#) combined with the expectation-maximization ([EM](#)) algorithm, provides a probabilistic approach particularly well-suited to the overlapping nature of quantum noise data. The literature has demonstrated that [GMM](#) with [EM](#) outperforms K-means and other clustering algorithms in terms of both flexibility and accuracy for mixed Gaussian data [30].

The use of [ML](#) techniques enables us to accurately determine the mathematical properties of the clusters, such as optimized means and variances, thereby facilitating better visualization and understanding of the hybrid noise model in higher-dimensional spaces. In [HQN](#) modeling, [GMM](#) plays a critical role in accurately representing complex noise distributions. Unlike traditional clustering techniques such as K-means and [DBSCAN](#), which assume spherical clusters of equal size with outliers, [GMMs](#) can model clusters with elliptical shapes and varying sizes. This flexibility is essential for quantum noise environments, where noise distributions are often irregular, overlapping, and multi-dimensional. In our model, [HQN](#) is formulated as the convolution of quantum shot noise, represented by a Poisson distribution, and [AWGN](#). [GMM](#) allows us to express this hybrid noise as a probabilistic mixture of multiple Gaussian distributions weighted according to a Poisson parameter λ . The ability to approximate the infinite mixture of Gaussians with a finite number of components ensures computational feasibility while retaining the essential characteristics of the noise. This enables effective visualization of the clusters and helps us analyze the underlying properties of the quantum channel more efficiently.

The [EM](#) algorithm is integral to optimizing the parameters of [GMMs](#), making it ideal for quantum noise modeling and channel capacity estimation. [EM](#) iteratively refines the parameters—such as the means, covariances, and mixing weights by maximizing the likelihood function, ensuring robust clustering even in high-dimensional and overlapping data. This is particularly advantageous in hybrid quantum noise models, where clusters are not distinct and often overlap. The [EM](#) algorithm’s ability to handle missing or incomplete data further strengthens its utility in noisy quantum environments. By using [EM](#) to optimize the [GMM](#) components, we achieve a more accurate estimation of the mutual information between the transmitter and receiver, resulting in a precise calculation of the quantum channel capacity. [EM](#) also enables soft clustering, which assigns probabilities to data points belonging to multiple clusters—an essential feature in quantum communication, where uncertainty is inherent. This balance of computational efficiency and accuracy makes the combination of [GMM](#) and [EM](#) particularly well-suited for real-time quantum noise classification and capacity estimation,

outperforming other clustering models, such as K-means and DBSCAN.

The overall aim is to improve the security and efficiency of satellite-based QKD by advancing noise modeling techniques, optimizing key rate computations, and introducing machine-learning-assisted error correction frameworks. The proposed methodologies seek to close the gap between theoretical QKD security proofs and their practical implementation in satellite quantum networks.

1.5 Application of Hybrid Quantum Channel

A satellite quantum channel is defined as a free-space optical communication link where quantum states of light—typically encoded in photon polarization or phase—are transmitted over vast distances through the Earth’s atmosphere and space. Due to atmospheric turbulence, beam diffraction, and satellite motion, the quantum signal experiences significant degradation, necessitating robust noise models and security analyses. The transmission coefficient T of the satellite quantum channel determines the fraction of photons successfully received and is given by multiple factors such as atmospheric losses, geometric losses due to beam divergence, the optical system efficiency, and the detector efficiency [23, 24].

The quantum signal transmission in a satellite quantum channel can be modeled as [26, 27, 34],

$$Y = TX + Z, \quad (1.15)$$

where T is the transmission coefficient incorporating various losses such as atmospheric (with the transmission efficiency $\tau = T^2$), geometric, optical, and detector losses, X represents the transmitted quantum state, Y is the received quantum state, and Z denotes the HQN comprising quantum Poissonian noise and classical AWGN. Satellite QKD enables long-distance secure communication by leveraging quantum mechanics to distribute encryption keys between distant parties. A satellite quantum channel enables optical laser-based quantum communication between ground stations and satellites, as well as inter-satellite links.

Several physical and environmental factors influence signal reliability in a quantum satellite communication channel, especially for QKD, significantly affecting the quantum secure key generation rates. Beam divergence and beam wandering, atmospheric turbulence, hybrid quantum noise, probability distribution of transmission coefficient (PDTC) [26], satellite altitude, zenith angle, finite-key effects, and day-night variations collectively influence the performance of quantum communication. The quantum optical beam from a satellite experiences beam divergence, characterized by the gradual widening of the beam as it propagates through space. Beam divergence results in a reduced photon density at the receiver, thereby decreasing the detection probability.

The PDTC represents the probability that a photon emitted from the satellite transmitter reaches and is successfully detected by the ground sta-

tion receiver. [PDTC](#) is crucial for long-distance quantum communication, which relies on entanglement. The transmission efficiency τ is characterized by a random variable that ranges between 0 and 1. The probability distribution of transmission efficiency ([PDTE](#)), τ aligns with the log-normal distribution, approximating the [PDTC](#) in entanglement distribution scenarios. The probability distribution of τ is given by [\[35, 36, 37, 38\]](#),

$$\mathcal{P}(\tau) = \frac{1}{\sqrt{2\pi\sigma\tau}} e^{-\frac{1}{2}\left(\frac{\ln\tau + \ln\tilde{\tau}}{\sigma}\right)^2}, \quad (1.16)$$

where τ represents the atmospheric transmittance, $-\ln\tilde{\tau}$ is the logarithm of the mean atmospheric transmittance, and σ is the variance of $-\ln\tau$, which characterizes the atmospheric turbulence. Additionally, beam wandering due to atmospheric turbulence results in a random lateral displacement of the beam centroid. Beam wandering can be statistically modeled as a Rayleigh-distributed displacement with a probability density function given by [\[26, 39\]](#),

$$P(r) = \frac{2r}{\sigma_b^2} \exp\left(-\frac{r^2}{\sigma_b^2}\right), \quad (1.17)$$

where r is the radial displacement from the optical axis, and σ_b is the beam wandering variance dependent on atmospheric turbulence strength and path length.

Quantum satellite channels inherently experience quantum noise, which combines classical background noise (such as sunlight scattering and detector dark counts) with quantum fluctuations. The atmospheric turbulence-induced noises that significantly affect [QKD](#), especially under daytime conditions, require rigorous spectral and spatial filtering techniques to enhance the [SKR](#). Satellite altitude and zenith angle further determine channel losses. Low Earth Orbit ([LEO](#)) satellites (500~1200 km altitude) offer lower free-space losses and shorter photon propagation delays, typically a few milliseconds. In contrast, Geostationary Earth Orbit ([GEO](#)) (35,786 km altitude) satellites suffer from higher losses and significantly larger propagation delays, making [LEO](#) preferable for high-rate [QKD](#). The zenith angle (θ_z) impacts the effective atmospheric path length, increasing turbulence effects and scattering at lower elevation angles. Finally, the adequate quantum communication time, governed by satellite passes over ground stations, differs significantly between day and night operations. Daytime [QKD](#) faces increased hybrid quantum noise due to solar background radiation, necessitating stringent filtering [\[4\]](#). In contrast, nighttime offers optimal conditions, reduced noise levels, and improved [PDTC](#), enhancing secure key generation rates substantially. The combined effects of beam divergence, beam wandering, atmospheric turbulence, [HQN](#), finite-key corrections, and channel geometry intricately determine the secure key rate and performance of satellite-based [QKD](#) systems. Addressing these factors through advanced adaptive optics, optimized link configurations, robust statistical analyses, and precise channel modeling is essential to realizing efficient global quantum communication networks.

The security of the satellite quantum channel for QKD is quantified using mutual information among the sender (Alice), receiver (Bob), and potential eavesdropper (Eve). The mutual information between Alice and Bob, $I(A : B)$, measures the amount of shared information, while $I(E : B)$ represents the information gained by Eve. The security of QKD systems is guaranteed by the laws of quantum physics rather than computational complexity, making them resilient to future quantum computing threats. A crucial metric for assessing security is the SKR, defined as [26, 34],

$$K = I(A : B) - I(E : B) \quad (1.18)$$

where $I(A : B)$ represents the mutual information between legitimate parties (Alice and Bob), and $I(E : B)$ denotes the mutual information between the eavesdropper (Eve) and Bob. Security is ensured when $I(A : B) > I(E : B)$, meaning that the legitimate parties share more information than an adversary can extract.

To counter potential quantum and classical attacks, security analyses typically involve key reconciliation, error correction, and privacy amplification. Satellite QKD introduces unique security challenges, including atmospheric turbulence, beam wandering, and satellite motion. In practical satellite QKD, the SKR is affected by hybrid quantum noise, which consists of both quantum Poissonian noise and AWGN. Hybrid quantum noise is modeled as [23, 24],

$$N_{\text{hybrid}} = N_{\text{Poisson}} + N_{\text{AWGN}}, \quad (1.19)$$

where N_{Poisson} represents shot noise originating from the quantum nature of light, and N_{AWGN} accounts for background noise from optical components and atmospheric scattering. The optimization of satellite QKD security involves mitigating the effects of HQN and improving the satellite channel efficiency. By refining transmission models and integrating adaptive noise suppression techniques, this chapter aims to enhance the resilience of quantum communication networks against environmental disturbances and eavesdropping attacks. The proposed methodologies aim to bridge the gap between theoretical QKD security proofs and real-world implementations, thereby ensuring the long-term viability of secure satellite-based quantum communication.

In QKD, collective attacks refer to a class of adversarial strategies where an Eve interacts with each transmitted quantum state in an identical but independent manner, storing all the intercepted quantum information in a quantum memory for later joint measurement and processing. Unlike individual attacks, where Eve measures each state separately, collective attacks allow the adversary to optimize their extraction of information by performing a global measurement on all stored states after classical post-processing between the legitimate parties.

In CV-QKD, where quantum information is encoded in quadrature variables of light (e.g., amplitude and phase), collective Gaussian attacks are considered optimal due to the extremality theorem. This means that the

most potent attacks in a Gaussian channel are those where [Eve](#) applies Gaussian-distributed operations, making security analysis against these attacks crucial. Security proofs in [CV-QKD](#) often rely on reverse-reconciliation ([RR](#)), where the secret key is extracted by the receiver rather than the sender, making the protocol more robust against loss and noise. However, hybrid quantum noise (combining quantum Poisson noise with classical additive white Gaussian noise) affects the security analysis, requiring refined entropy-based techniques to evaluate resilience against collective attacks.

This chapter demonstrates that hybrid quantum noise models provide a more realistic assessment of [CV-QKD](#) security under collective attacks. Entropy-based security analysis reveals how hybrid noise affects the mutual information between legitimate parties (Alice and Bob) and an [Eve](#), influencing the extractable [SKR](#). Hybrid noise affects error reconciliation by introducing additional noise sources that must be compensated to maintain secure key generation. Finite-key security considerations under collective attacks must account for quantum noise statistics, requiring advanced modeling techniques to ensure resilience in practical implementations. By incorporating hybrid quantum noise into the [CV-QKD](#) security framework, this chapter enhances our understanding of [CV-QKD](#)'s vulnerability to practical eavesdropping scenarios and paves the way for more robust and secure quantum communication protocols in real-world satellite-based quantum networks.

1.6 Research Questions:

The rapid advancement of quantum communication systems demands accurate modeling of real-world noise, which is inherently hybrid in nature, comprising both quantum and classical components. To bridge the gap between theoretical models and practical deployments, this thesis is guided by the following key research questions:

Q1. What methodologies can be employed to develop an [HQN](#) model that integrates classical and quantum noise, and how can such a model more accurately characterize quantum channel parameters such as achievable rates?

Q2: What validation techniques and optimization strategies are most effective for refining the [HQN](#) model to ensure accurate quantum channel modeling?

Q.3 How can the [HQN](#) model be applied to different quantum channels for practical applications such as satellite quantum communication, specifically in estimating [SKRs](#) and [SNRs](#), and satellite-based [QKD](#)?

1.7 Aim and Objectives:

This work aims to develop an **HQN** model that accurately characterizes the interplay between quantum and classical noise sources in satellite-based quantum communication systems. The model is designed to improve the characterization of quantum channel parameters, such as achievable rates, and enhance the performance of **QKD** protocols under realistic noise environments.

I. Development of the **HQN** Model

- *Formulate the **HQN** Model:* Develop a mathematical framework that integrates Poissonian quantum shot noise with classical **AWGN** to construct a realistic hybrid noise model for quantum communication.
- *Characterize Quantum-Classical Noise Interactions:* Employ **GMMs** and parametric estimation techniques to analyze the statistical interplay between classical and quantum noise, and evaluate their combined impact on quantum channel characteristics, especially channel capacity.
- *Entropy Estimation Framework:* Design a methodology to estimate the entropy of the hybrid noise system to gain deeper insight into the information-theoretic limits of the quantum channel under hybrid noise influence.

II. Validation and Optimization of the Model

- *Optimize the **HQN** Model using ML:* Apply **GMM-EM** algorithms, clustering, and other machine learning techniques to improve the accuracy and computational efficiency of the **HQN** model.
- *Evaluate Quantum Channel Capacity under Hybrid Noise:* Derive and validate an analytical formulation for mutual information between transmitter and receiver under hybrid noise conditions. Study capacity variations with **SNR** for both Gaussian and non-Gaussian input states.

III. Application to Satellite-Based Quantum Communication

- *Apply **HQN** Model to **CV-QKD** Systems:* Extend the validated **HQN** model to **CV-QKD** systems operating in satellite communication settings. Analyze performance under asymptotic and finite-size security regimes, considering practical factors such as altitude-dependent channel loss, atmospheric turbulence, and reconciliation efficiency.

These objectives collectively aim to deliver a robust, scalable, and practically applicable **HQN** framework that advances the state-of-the-art in quantum communication system modeling and performance analysis, especially in satellite-based **QKD** networks.

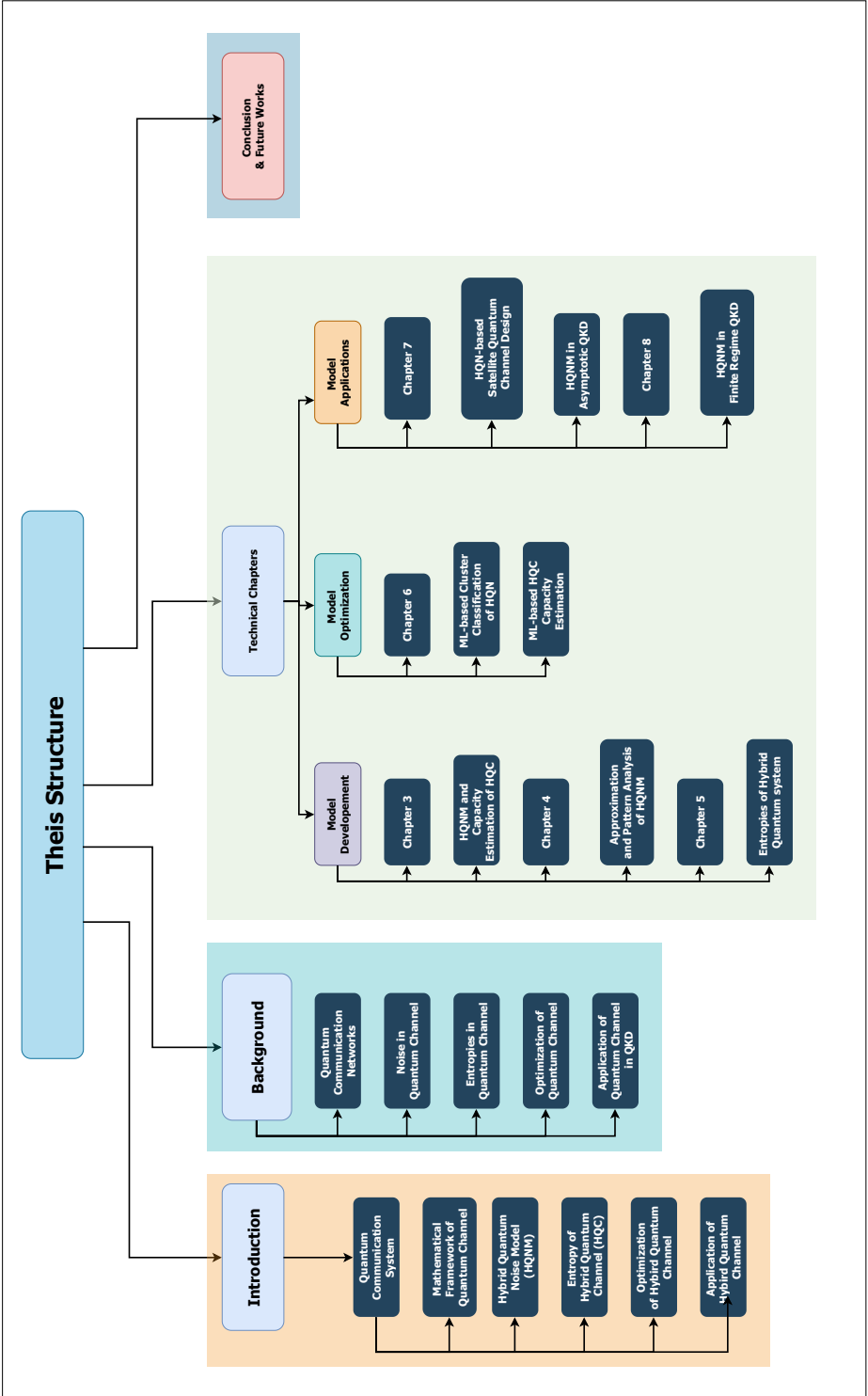


Figure 1.1: The flowchart of the research work.

1.8 Thesis Structure

This doctoral thesis is broadly divided into three parts: (1) Development of a HQN Model, and (2) Optimization of the HQN Channel. Application of the hybrid quantum noise model in satellite quantum communication and quantum SKR estimation. The thesis is structured as follows, shown in Fig. 1.1:

Chapter 1: Introduction: This chapter provides an overview of quantum communication, the challenges associated with long-distance quantum transmission, and the motivation for developing a hybrid quantum noise model. The research's aim and objectives are clearly outlined.

Chapter 2: Background and Literature Review: A review of quantum communication principles, quantum noise models, and recent advancements in ML-optimized quantum communication. Additionally, recent works on satellite-based quantum communication in conjunction with QKD are presented. The limitations of existing noise models are discussed, highlighting the necessity of a hybrid quantum noise approach.

Chapter 3: HQN Modeling and Achievable Rate Estimation: This chapter introduces the proposed hybrid quantum noise model, formulated by convoluting Poisson-distributed quantum noise with classical AWGN. A mathematical expression for quantum channel capacity is derived, considering both Gaussian and non-Gaussian signal inputs. The model is analyzed using entropy-based metrics to determine its impact on the maximum achievable quantum information transfer. Simulations are performed to evaluate the capacity with respect to SNR for different input states.

Chapter 4: Parameterized Characterization of Hybrid Noise : The chapter explores the mathematical characterization of the hybrid quantum noise model using Gaussian and Poisson parametric analysis. It examines the relationship between Poisson distribution parameters and GMMs to efficiently approximate hybrid noise entropy. The chapter also discusses how, depending on Poissonian settings, an infinite mixture of Gaussians can be approximated by a finite mixture distribution.

Chapter 5: Quantum Entropies of HQN channel: This chapter provides a robust tool for quantifying the entropy associated with the quantum channel information, enhancing security in quantum communication. This study analyzes the equivalence and shared properties of various entropy measures under HQN. It mathematically explores conditions where these entropies coincide or relate closely, emphasizing their role in quantum information theory. The findings contribute to optimizing HQN in quantum networks.

Chapter 6: ML-Assisted Optimization for Noise Reduction: This chapter optimizes the hybrid noise model using ML-driven clustering techniques. The EM algorithm reduces the number of Gaussian clusters required for accurate noise representation. The results show how GMM-based noise modeling enhances the quantum channel's achievable rate by improving signal estimation and reducing computational complexity. The effectiveness of ML-driven quantum noise modeling is demonstrated through numerical sim-

ulations, particularly in satellite-based quantum communication for QKD.

Chapter 7: Application of HQN Model in FSO Satellite Quantum Communication: The hybrid quantum noise model is applied to FSO-based satellite quantum communication, where both quantum Poissonian shot noise and classical AWGN influence continuous variables (CV) Gaussian quantum channels. The chapter derives the QKD rate achievable under hybrid noise conditions, extending traditional Gaussian-only models to a more comprehensive noise framework. SKR analysis is performed under various altitude-dependent noise parameters, evaluating the impact of reconciliation efficiency, electrical noise, transmission coefficients, and detection efficiency. A comparative study of finite-size and asymptotic SKR is provided, offering a realistic assessment of quantum security in satellite networks.

Chapter 8: Finite-Size Effects on SKR in QKD : This chapter extends the hybrid noise model to analyze the finite-size SKR for CV-QKD systems. Unlike traditional Gaussian noise models, this approach accounts for the interactions between quantum and classical noise, providing a more nuanced understanding of SKR limitations under realistic conditions. The efficiency of finite-regime QKD under hybrid noise constraints is evaluated using covariance matrix formalism, revealing the interplay between channel parameters, noise sources, and environmental factors in practical satellite-based QKD implementations.

Chapter 9: Conclusion and Future Chapter: The final chapter summarizes key findings and contributions of the research, emphasizing the importance of hybrid noise modeling in advancing satellite-based quantum communication. It outlines potential future directions, including applying DL to optimize HQN channels with QEC techniques and the application of hybrid noise models in multi-layered satellite networks.

1.9 Conclusion

This chapter aims to develop a highly accurate and realistic model of hybrid quantum noisy channels while leveraging ML-assisted optimization to enhance their performance. The study applies this refined channel model to satellite-based quantum communication, strengthening the security and efficiency of satellite QKD through advanced noise modeling frameworks. By integrating cutting-edge techniques, the proposed methodologies enhance the QKD security proofs in satellite quantum networks, paving the way for more resilient and scalable quantum communication systems. In the next chapter, the reader will explore the background and existing research works, which will enable the identification of the research gap and this dissertation's aim and objective.

Chapter 2

Background & Literature Review

2.1 Quantum Communication Networks

Quantum communication is crucial for the next generation of secure communications and serves as a foundational and emerging component of the quantum internet [17]. Continued progress in capabilities like quantum repeaters and memories could lead to large-scale quantum communication networks and a quantum internet [40]. The progress of Quantum Internet and quantum networks achieves full functionality through stages like trusted repeater development, entanglement distribution, and memory enhancement, culminating in seamless integration with the existing Internet, including management aspects [41]. In quantum networks, routing is a significant problem, i.e., the problem of finding the shortest path in a network addressing the challenges of distributing quantum entanglement across a network of quantum repeaters with finite entangled qubit pairs and varying levels of entanglement fidelity [42]. Quantum sensing represents an advanced phase in integrated sensing, primarily focused on the trade-off between fundamental detection probability and achievable communication rates in communication systems [43].

Quantum cryptography marks a significant advancement over traditional cryptographic methods. QKD is a method that ensures secure communication by allowing the detection of eavesdropping attempts using quantum principles such as superposition and entanglement [44]. QKD protocols, such as BB84, exemplify this by using quantum properties to securely distribute encryption keys, making eavesdropping detectable due to the inherent nature of quantum states [16]. Quantum communication offers secure key exchange using QKD, utilizing the no-cloning theorem and properties such as photon polarization or phase [45], [46]. QKD, operational over hundreds of kilometres via optical fibres and quantum repeaters, detects eavesdropping and is superior to classical cryptography [47], [48]. Additionally, the scope of quantum communication extends beyond secure data transfer. It includes applications like quantum teleportation [49], which involves transferring quantum states between distant locations without the physical transfer of particles (qubits).

Beyond security, quantum communication is foundational to the establishment of quantum networks, which are envisaged to interconnect quantum computers [17]. These networks, facilitating the sharing of quantum information (qubits) across distances, are essential for distributed quantum computing, enabling computational tasks that are currently impractical with classical networks. Integrating quantum communication with quantum information processing is critical for this technological evolution. Quantum gates and circuits play a crucial role in transforming classical information into quantum states that can be processed more securely in a quantum information processing system across quantum networks [16]. Quantum communication focuses on the transmission of quantum information, while quantum information processing involves the manipulation and processing of this information [50]. The synergy between these fields is expected to develop powerful quantum computing networks, mirroring the Internet’s role for classical computers today.

However, quantum communication, including quantum information processing, faces several challenges, including the development of reliable quantum repeaters for long-distance communication and the management of quantum noise and decoherence. Efforts are also underway to integrate these quantum systems with existing infrastructure [51]. Despite these challenges, the continuous research in this domain promises substantial advancements in secure communication and the realization of global quantum networks and distributed quantum computing in the future.

2.2 Noise in Quantum Channel

Quantum noise, omnipresent in quantum computing, arises from various sources, including environmental interactions, qubit interactions, and imperfect controls, leading to errors such as dephasing and decoherence. Characterizing and understanding its impact is challenging but crucial for practical quantum computation[52]. Classical and quantum noises are integral to a quantum noisy channel, with quantum noise often indistinguishable from classical noise in functional scenarios [53]. Noise from vibrations and material fluctuations interferes with communication signals, causing information loss. Both types of noise are essential in modeling noisy quantum channels, with classical communication often affected by thermal and shot noise. A standard model is the additive white Gaussian noise, which imitates random natural processes and can distort signal integrity, necessitating noise generators for system response measurement. Quantum Poisson noises can be considerable as follows: photon-counting shot noise [54], electron shot noise [55], quantum projection noise [56], quantum walk fluctuations [57], and more noises can be found in [58, 59, 60, 61]. However, the classical noises that can be plugged into quantum noises are thermal noise [62], current shot noise [63], phase noise [64], amplifier noise [65], photodetector noise [66], and other ancillary noises are discussed in [67, 68, 69].

Entanglement brings noise into the quantum communication channel.

Entangled qubits decohere in noisy channels, losing entanglement through effects like sudden death [70]. Amplitude/phase damping also destroys correlations [71]. Furthermore, Gaussian states are vulnerable to thermal noise—adding photons [72], contaminating entanglement [73]. Quantum noise disturbs states, destroying information and entanglement through decoherence, dephasing, and photon loss. Decoherence can render channels useless by destroying the information they carry. The combined effect of these noises can significantly impact the accuracy and performance of the quantum channel, as well as the overall reliability of quantum communication. Decoherence can be linked to a form of quantum noise arising from interactions with the environment, causing errors and diminishing the reliability of quantum information in communication or computation [74]. Decoherence poses a significant challenge in quantum communication, where the accurate transmission and manipulation of quantum states are crucial.

Addressing decoherence in quantum communication is a crucial research effort. Several strategies and techniques are being developed to mitigate its effects [75], [76], [77], [78], [79]: Error correction codes and quantum error correction protocols are utilized to counteract the consequences of decoherence, protecting delicate quantum information and improving the dependability and effectiveness of quantum communication systems [80]. Quantum error correction codes that utilize entanglement are being developed to approach the quantum capacity [81]. The paper [82] introduces a decoding method for quantum stabilizer codes using the GRAND technique from classical codes, applied to quantum polar codes. [83] extends this to quantum random linear codes, using quantum noise statistics for efficient error correction. [84] compares classical and quantum error correction codes, detailing the construction of QEC codes from classical codes and their application to channel modeling. These works highlight the evolution of error correction methods in quantum computing, emphasizing adaptability and efficiency in handling quantum noise and error rates.

Matching ultrafast decoherence timescales with slower classical noise is a challenging task. Combining these mitigation strategies aims to improve robustness against decoherence in quantum communication. Approaches to match decoherence timescales: modeling via master equations [85], high-bandwidth colored noise [86], phase/frequency jitter noise, discrete femtosecond noise injection [87], fast physical noise sources, and modeling loss via short channel correlations [88]. Independent classical and quantum noise combine to a Gaussian distribution [89]. Adding equivalent sources, such as shot noise, preserves the power spectral density [90]. Uncorrelated noise sums in signal-to-noise ratio [91]. Correlated noise needs quantum treatment.

Combining classical and quantum noise poses challenges because of their distinct timescales and intensity scales. Numerical simulations with discrete time steps enable the concurrent influence of both types of noise [92]. Classical noise models employ analytical representations, while quantum noise uses Monte Carlo sampling [93] or Lindblad operators [94]. Independent

noise sources in the master / Langevin equations drive the evolution of the density matrix of the system [95],[96]. Classical parameters modulate the characteristics of quantum noise over time [50]. Decoherence must be considered, as it is a rapid quantum process that causes entanglement with the environment and the loss of quantum properties [74], [80].

Entanglement-based quantum communication, such as QKD for space communication, experiences a high loss during the terrestrial distribution of photons. This limits communications via the satellite links, where the loss is dominated by diffraction instead of absorption and scattering [97]. These noise types can disrupt quantum states, leading to the degradation of information through the loss of key quantum properties, such as superposition and entanglement [98]. Accurately modeling these quantum channels requires detailed characterization of noise parameters to mitigate their effects and maintain the integrity of transmitted quantum information. Quantum noise, distinct from classical noise, has a significant impact on quantum channels and necessitates analysis using density matrices and quantum operations. This requires a hybrid noise model that integrates both quantum and classical noise, employing statistical methods such as the Poisson distribution to capture the realistic behaviour of quantum channels effectively [11]. Quantum Poisson-distributed noises encompass disturbances such as photon-shot noise, electron-shot noise, quantum projection noise, and the spontaneous emission of photons from quantum states. These quantum noises can be combined with classical noises. This merging of noises highlights the interaction between quantum and classical noise sources in different scientific and engineering fields [21].

Modeling realistic quantum channels necessitates accounting for both quantum and classical noise sources due to their distinct characteristics and impacts on quantum communication systems. Quantum Poisson noise [11] is crucially linked to the uncertainty principle and photon counting, where photons, often carriers of quantum states, arrive at random, creating discrete noise events. These events are fundamental to quantum physics and have a significant impact on applications such as quantum information processing [99]. In contrast, classical AWGN [20], prevalent in many communication systems, features a continuous amplitude distribution, providing a contrasting noise profile with a zero mean and defined variance. Integrating quantum Poisson noise with classical AWGN captures random, discrete disruptions from quantum sources and continuous disturbances from classical sources. This hybrid noise model more accurately reflects the complex noise environment in quantum channels, facilitating the development of effective strategies to mitigate these interferences and enhance the reliability and security of quantum communications [100].

2.2.1 Entropy Estimation of Quantum Communication System

Entropy, as a concept, has found profound applications across various domains, particularly in quantum systems, information science, and communication theory. Originally formulated within thermodynamics, entropy quantifies disorder or uncertainty in physical systems. Its applications have expanded to quantum mechanics, where it plays a vital role in understanding quantum states and the behaviour of quantum systems. In quantum mechanics, entropy is crucial for characterizing the information content and uncertainty in a quantum system's state. Quantum entropy, particularly von Neumann entropy, measures the degree of mixedness of a quantum state, thus offering insights into the entanglement and coherence properties of quantum systems. This framework has become indispensable for studying quantum information and quantum thermodynamics. Differential entropy, introduced by Claude Shannon in 1948, revolutionized information theory by providing a mathematical measure for uncertainty or information content in data. It quantifies the average amount of information produced by a stochastic data source. In information science, entropy is a fundamental metric for data compression, error detection, and probabilistic modeling [2, 10].

Quantum communication channels, like their classical counterparts, are limited by entropy. However, in the quantum domain, quantum entropy (or von Neumann entropy) becomes a critical tool for analyzing the capacity and efficiency of these channels. The behaviour of entropy in quantum channels is closely related to concepts such as entanglement, superposition, and coherence, which enhance communication capabilities beyond classical limits. QKD leverages the principles of quantum mechanics to enable secure communication. Entropy is central to this process, as it quantifies the uncertainty or randomness in the generated key. The security of QKD protocols depends on ensuring that the entropy of the quantum key is maximized, minimizing the potential for interception or manipulation by adversaries [101].

Experimental data from the Micius satellite and other quantum communication projects reveal significant insights into the performance and reliability of quantum entropy-based protocols. These results underscore the importance of entropy measures in optimizing and securing quantum communication systems. Accurate state tomography is crucial for characterizing quantum gates and algorithms in quantum computing. Quantum entropies facilitate the evaluation of the performance and reliability of quantum computations. In quantum communication, ensuring the fidelity of quantum states is vital for secure information transfer [102]. Entropic measures help verify the integrity of quantum states used in protocols such as QKD. Quantum satellite communication leverages quantum entropies to enhance security and efficiency in data transmission over long distances. Entanglement-based protocols and QKD are integral to these systems, utilizing properties

of quantum entropies to ensure secure communication channels. Satellites with quantum communication technology can distribute entangled photon pairs over vast distances, overcoming terrestrial limitations. Entanglement distribution is quantified using measures like entanglement entropy, which assesses the degree of entanglement between quantum systems. QKD exploits the principles of quantum mechanics to generate secure cryptographic keys. The security of QKD protocols, such as BB84 and E91, relies on the properties of quantum entropies to detect eavesdropping and ensure the integrity of the key exchange process. Quantum tomography is also used in quantum metrology to characterize quantum sensors and improve measurement precision. Entropy-based assessments enhance the accuracy and reliability of quantum measurements.

Data from the Micius satellite and other quantum communication initiatives provide vital insights into the effectiveness and dependability of protocols based on quantum entropy. These findings highlight the significance of entropy metrics in refining and securing quantum communication networks. Precise state tomography is essential for defining quantum gates and algorithms in quantum computing. Quantum entropies play a key role in evaluating the effectiveness and stability of quantum computations. In quantum communications, maintaining the fidelity of quantum states is crucial for safe information exchange. Entropic measures aid in confirming the integrity of quantum states employed in protocols such as QKD [13]. Quantum satellite communication leverages quantum entanglement to enhance security and efficiency in data transfer over long distances. Integral to these systems, entanglement-based protocols and QKD utilize quantum entropy properties to secure communication lines. Satellites with quantum communication technology can transmit entangled photon pairs over extensive distances, overcoming terrestrial challenges. The entanglement distribution is assessed using metrics like entanglement entropy, which measures the level of entanglement between quantum systems. QKD takes advantage of quantum mechanics principles to create secure cryptographic keys. The safety of QKD methods, such as BB84 and E91, depends on quantum entropy properties to detect eavesdropping attempts and maintain the security of the key exchange process. Additionally, quantum tomography is employed in quantum metrology to define quantum sensors and enhance measurement accuracy, with entropy-based evaluations improving the precision and reliability of quantum measurements.

In quantum satellite communication, Tsallis entropy has been used to model the effects of non-Markovian noise, where memory effects influence the transmission of quantum states over long distances. This measure provides insights into optimizing quantum channel designs to counteract the effects of decoherence. Differential entropy extends Shannon entropy to continuous variables and is used to analyze continuous-variable quantum systems. It is particularly relevant for quantum optics, where Gaussian states are used in quantum communication protocols [103]. The entropy of continuous-variable quantum states, including squeezed and coherent states,

plays a crucial role in quantum information theory. Quantum networks utilizing [CV-QKD](#) rely on differential entropy measures to estimate security thresholds and optimize protocol performance. Hartley entropy is a special case of Rényi entropy at $\alpha = 0$, representing the logarithm of the number of non-zero eigenvalues of a quantum state. It quantifies the number of distinguishable states within a quantum system and has applications in quantum error correction and quantum resource management. In quantum networks, Hartley entropy helps assess the effective dimensionality of transmitted quantum states, guiding the selection of appropriate encoding schemes for quantum communication channels. Unified entropy provides a comprehensive framework encompassing Rényi, Tsallis, and other entropy measures [\[29\]](#). It allows for the flexible quantification of uncertainty in quantum systems under varying noise conditions. Hybrid quantum noise, where quantum and classical noise sources simultaneously affect a quantum state, necessitates a broader approach to entropy measures. Research on unified entropy in quantum satellite communication suggests that optimizing entropy parameters can enhance error correction techniques and improve the robustness of quantum links. Researchers can develop adaptive quantum communication protocols that dynamically adjust to different noise environments by leveraging unified measures of entropy.

Current research focuses on the applications of quantum entropy in quantum networks and the quantum internet. Quantum entropy measures are crucial in developing quantum networks and the quantum internet [\[34\]](#). Some key applications include (I) Quantum Channel Capacity Estimation: Von Neumann entropy and Rényi entropy help determine the maximum achievable communication rates in quantum channels. (II) Application in Security: Security proofs of [QKD](#) protocols often rely on Rényi entropy and Tsallis entropy to evaluate eavesdropping risks. (III) Application in [QEC](#): Entropy measures guide the development of quantum error-correcting codes by assessing the information loss due to noise. (IV) Quantum Satellite Communication: Entropy quantifies the decoherence effects in free-space quantum communication, optimizing quantum link designs. (V) Quantum Entanglement Detection: Various entropy measures indicate entanglement strength, which is essential for distributed quantum computing and teleportation protocols [\[3\]](#).

While entropy is defined differently in various contexts—thermodynamic, quantum, and information-theoretic—their commonality lies in their ability to quantify a system’s degree of uncertainty and disorder. A key study area is unifying these definitions under a common framework where the underlying principles remain consistent. The equivalence of different quantum entropies under specific conditions leads towards a unified definition of entropy that can be applied universally across quantum systems, classical communication, and information theory. Understanding entropy in these diverse contexts allows researchers to draw connections between classical and quantum systems, highlighting its versatility and foundational role in modern quantum communication networks.

2.3 Optimization of Quantum Channel

Optical cluster states [104] are critical in achieving quantum computational universality in linear optical quantum computing (LOQC) [105]. Since establishing direct entangling operations between photons is challenging due to the need for nonlinear effects, the probabilistic generation of entangled resource states offers a promising alternative approach. In LOQC, cluster states can be created using different methods, depending on how quantum information is encoded on a silicon photonic chip. Standard encoding options include spatial modes, where quantum information is encoded in photons' paths, and polarization, where the quantum state is defined by the orientation of the photons' electric fields [106]. The specific method of generating cluster states depends on the chosen encoding, which is vital for effectively operating quantum computing tasks. These states are essential building blocks for performing quantum gates [104] and operations in LOQC systems, driving advancements in photonic quantum computing.

As discussed earlier, quantum noise can disrupt quantum entanglement, leading to decoherence, which poses significant challenges for quantum communication and computing [107, 108]. Therefore, maintaining quantum coherence and minimizing decoherence (loss of quantum information) over long distances and timescales is challenging. ML algorithms can play a crucial role in the more efficient generation and detection of entangled states, which is vital for various quantum communication protocols [109], [110], thus improving the performance of quantum communication systems. A combined approach has been proposed to demonstrate how ML algorithms can enhance the generation of high-dimensional entangled states with higher fidelity and efficiency. This approach integrates quantum control techniques with ML algorithms to optimize generating entanglement [111]. Generative ML models can be utilized for quantum state tomography, including the identification of entangled states. This approach provides a more efficient and precise method for characterizing quantum states, especially those related to entanglement [112], [113], [114].

ML assists in improving the estimation and optimization of quantum channel parameters [115], error correction [116], resource allocation [117], and quantum information transmission. Progress has been notable in quantum communication technology for free-space satellites [118]. However, challenges related to quantum repeaters for long-distance quantum communications still need to be addressed to establish a global quantum network [119],[120]. Free-space quantum communication channels have encountered difficulties, including loss in the quantum channel, security issues, and limited data rates [121]. Conventional ML techniques offer a valuable approach to characterizing the features of free-space quantum channels [122]. In a recent study [123], supervised ML was employed to forecast the atmospheric strength of a free-space quantum channel. ML techniques play a crucial role in addressing quantum noise in communication systems. Clustering methods like GMM [124], which represent noise as a mixture of Gaussian compo-

nents, offer flexible and accurate noise modeling. The [EM](#) algorithm [125], calculating the maximum a posteriori ([MAP](#)) [126], used with [GMM](#), refines the model parameters iteratively to optimize noise clustering, thereby improving quantum channel capacity and noise management. This approach helps manage the probabilistic nature of quantum noise, enhances error correction, and boosts the precision of quantum communication protocols [127]. The [EM](#) algorithm is beneficial for modeling hybrid quantum noise in practical channels, including satellite-based [QKD](#) systems [23, 24]. It efficiently processes high-dimensional quantum data and optimizes parameters like means, variances, and weights in noise clusters, balancing model complexity with computational feasibility. This makes [EM](#) clustering essential for real-time quantum noise modeling, enhancing the performance and reliability of quantum communication systems [127].

The [EM](#) algorithm has relatively low computational complexity compared to more advanced machine learning techniques like [DL](#) or [RL](#). In each iteration, the [EM](#) algorithm performs the E-step (expectation) by estimating the likelihood of the data given the current parameters and the M-step (maximization) by refining the parameters to maximize the possibility. For [GMM](#), this involves basic linear algebra operations, such as matrix inversions and updating means and covariances [127]. While the complexity of each iteration depends on the number of data points and the number of clusters (or Gaussian components), it typically scales quadratically with the number of data points. This is manageable in most practical quantum communication scenarios, especially where real-time channel noise monitoring is required.

The computational burden of the [EM](#) algorithm in hybrid quantum noise modeling is significantly lower compared to alternative approaches such as [DL](#) or Bayesian inference. Although the [EM](#) algorithm is iterative, it generally converges in a reasonable number of iterations for most applications. However, it may face computational challenges with large-scale datasets or highly complex noise models, as each iteration involves recalculating parameters across all clusters. This could increase the computational burden in the context of high-dimensional quantum data, but it remains feasible for typical quantum communication channel modeling. The [GMM](#) approximation of hybrid quantum noise as finite mixtures reduces the computational cost associated with infinite mixtures of Gaussian components. This makes the [EM](#)-based approach more computationally efficient without sacrificing significant accuracy.

The feasibility of using the [EM](#) algorithm for hybrid quantum noise modeling in practical quantum channels is strong due to several factors, from manageable resource requirements to accurate parameter tuning. The [EM](#) algorithm, even with high-dimensional quantum data, can be executed efficiently with standard computational resources. This makes it feasible for real-world implementations where quantum channel noise needs to be modeled on-the-fly, such as in satellite-based [QKD](#) systems. The [EM](#) algorithm’s ability to optimize the parameters (means, variances, and weights)

of quantum noise clusters makes it a practical choice for refining noise models in free-space optical quantum communication systems. It balances model complexity and computational resource requirements, making it feasible for real-time deployment.

As a result, the [EM](#) algorithm’s balance between computational complexity, practical application, and efficiency makes it well-suited for hybrid quantum noise modelling. Its feasibility in handling quantum noise clustering and optimizing channel capacity without overwhelming computational burden positions it as an effective tool for current and future quantum communication technologies.

Estimating parameters in Gaussian quantum channels is a crucial task that involves identifying and optimizing variables essential for transmitting quantum states. A [GMM](#) represents a probability density function by a weighted sum of Gaussian component densities, providing a flexible representation of non-Gaussian densities. With sufficient components, [GMMs](#) can approximate any smooth function with arbitrary accuracy, making them suitable for representing multivariate densities in practical applications [128], [129]. The [EM](#) algorithm [30], [130], being a robust iterative technique, efficiently estimates the quantum channel parameters maximizing the likelihood function. The likelihood function in the context of the [EM](#) algorithm quantifies the probability of the observed data given the model parameters. It is used to iteratively update the parameters to maximize this probability, enhancing the model’s fit to the data. Maximum likelihood significantly improves Gaussian quantum channels by reducing noise and errors, thereby enhancing performance through the use of updated parametric values. By focusing on Gaussian states and operations, these channels can benefit from [ML](#) models trained to forecast their evolution, thus refining quantum communication protocols [131]. In hybrid quantum systems, [ML](#) aids in integrating Gaussian channels, facilitating the efficient exchange of classical and quantum information. [ML](#) techniques are essential for characterizing Gaussian quantum channels, identifying crucial attributes such as noise properties and entanglement effects, and detecting anomalies indicating external interference or unexpected noise [132]. [GMMs](#) further elucidate the hybrid quantum noise model of these channels [18, 21].

Furthermore, [ML](#) optimizes the preparation of the Gaussian state, enhancing transmission fidelity through precise squeezing and displacement [1],[19]. As parametric representations of the probability distribution of continuous measurements, these models are adept at forming smooth approximations of arbitrarily shaped densities, which is crucial for precise and reliable estimation of channel characteristics. This enhances the fidelity and performance of quantum state transmission. The iterative [EM](#) algorithm for calculating the [MAP](#) [126], [133] estimation of [GMM](#) parameters from training data is a widely accepted technique among researchers. This method significantly aids in estimating parameters for Gaussian quantum channels, optimizing the transmission of quantum states [134]. By leveraging [ML](#) algorithms, quantum communication channels can be optimized for

enhanced performance [111],[110],[109]. For example, the **GMM**, which represents noise distributions as a mixture of Gaussian components, provides a flexible and accurate method for modeling hybrid quantum noise. The **EM** algorithm, used in conjunction with **GMM**, iteratively refines the model’s parameters, optimizing the noise clustering to improve channel capacity and noise management. This combination enables the more effective handling of the probabilistic nature of quantum noise, providing valuable insights into its impact on quantum channels.

The role of **ML** extends beyond noise modeling, as it also plays a crucial part in optimizing quantum channel parameters, estimating noise characteristics, and improving error correction techniques. The use of **ML** techniques, such as **GMM** and **EM**, not only enhances the visualization of noise clusters but also improves the precision of quantum communication protocols. For instance, **ML** can be used to optimize entanglement generation and detection, which are vital for quantum communication systems. By incorporating **ML**-driven noise management into quantum communication systems, the overall performance and reliability of these channels are significantly improved [18]. The application of the **EM** algorithm for hybrid quantum noise modeling in practical quantum channels is rendered feasible by a confluence of factors, most notably the algorithm’s relatively modest resource requirements and its capacity for precise parameter tuning. Its inherent ability to efficiently process high-dimensional quantum data, even under standard computational constraints, underscores its practicality in real-world implementations. This becomes particularly significant in scenarios necessitating real-time quantum noise modeling, such as satellite-based **QKD** systems [24],[1]. By facilitating the optimization of key quantum noise cluster parameters (means, variances, and weights), the **EM** algorithm not only enhances the fidelity of noise models in free-space optical quantum communication systems but also adroitly navigates the trade-off between model complexity and computational overhead. Its adeptness at managing the intricacies of quantum noise clustering, coupled with its alignment with the demands of real-time deployment, positions the **EM** algorithm as an indispensable tool for advancing both the current and prospective landscapes of satellite quantum communication technologies.

2.4 Application of Quantum Channel in **QKD**

Integrating quantum communication with satellite technology has opened new frontiers in global secure communications, addressing the distance constraints inherent in terrestrial quantum networks [135, 136]. This synergy between quantum and satellite technologies promises to revolutionize fields such as cryptography, distributed computing, and precision timekeeping worldwide. Central to the advancement of quantum communication is the development of **QKD**, a cryptographic protocol that enables the secure exchange of encryption keys between distant parties [16]. Utilizing the unique properties of quantum states, Gaussian **CV QKD** allows two parties to es-

establish secret keys with security guaranteed by the laws of quantum physics rather than computational complexity [137],[135]. Satellite-based quantum communication systems leverage the vast reach of orbiting platforms to establish quantum links across continental scales, potentially enabling a global quantum internet using secure key sharing between the microsatellites and the portable optical ground station (OGS), paving the way for scalable, cost-effective global quantum networks [138]. Despite its potential, implementing QKD over extended ranges remains a challenge. However, noisy environments remain challenging for quantum channels, necessitating constant innovation and refinement to address real-world communication scenarios.

One of the promising approaches to overcoming these challenges involves space-based QKD solutions that employ satellites as relay nodes, creating a globally interconnected quantum network [139],[140]. The experimental foundations of QKD date back to seminal works that introduced protocols such as BB84 and its subsequent enhancements, incorporating decoy states and bit error rate optimizations [141]. These innovations have improved robustness against photon number splitting (PNS) cyber attacks and increased key generation rates. Space-based experiments have successfully demonstrated free-space BB84 QKD between ground stations separated by hundreds of kilometres and quasi-single-photon transmissions from satellites to Earth [142],[143]. Recent advancements include the SpeQtral-1 quantum satellite mission, which aims to establish ultra-secure communications via QKD. Additionally, ongoing work is being conducted on CubeSats specifically designed for spaceborne QKD protocols and their applications [144],[145].

Despite this progress, significant challenges persist in the field of satellite quantum communications. Optical transmission between satellites and ground-based platforms faces several limitations, including diffraction, systematic pointing errors, and atmospheric turbulence [146],[147]. These factors cause transmission losses by broadening the optical beam and introducing wavelength-dependent losses due to atmospheric absorption of photons [148]. Detector efficiencies need substantial improvement for efficient quantum key exchange [149]. Photon loss during propagation through atmospheric turbulence and background noise mitigation are critical areas of investigation [150]. While larger telescopes and shorter photon wavelengths can mitigate diffraction losses, a balance between telescope size, cost, and transmission performance is necessary [151],[149]. Atmospheric turbulence, caused by temperature-induced refractive index fluctuations, broadens and wanders the beam, introducing additional loss [152],[153]. Works like [154] have developed probability density functions (p.d.f.s) of transmittance for slant propagation paths, proposed models for atmospheric quantum channels with turbulence, and experimentally characterized distant FSO atmospheric channels. Addressing these challenges is essential for the seamless integration of QKD into existing satellite communication infrastructures, thereby enhancing the robustness and efficiency of global quantum networks

with the use of quantum repeaters [155]. Adaptive optical systems and optimal ground station selection can mitigate turbulence effects, particularly in uplink channels where turbulence is most significant [156],[28].

Quantum communication leverages quantum mechanics to facilitate secure information transfer, with QKD ensuring cryptographic security against computational attacks. Satellite quantum communication extends QKD beyond terrestrial fibre limitations, enabling global quantum networks via free-space optical links. Performance analysis distinguishes asymptotic and finite-size regimes: the asymptotic case assumes infinite key length, minimizing statistical fluctuations and optimizing theoretical key rates, while finite-size analysis accounts for practical constraints, including transmission losses, noise, and security parameter trade-offs. Understanding these regimes is crucial for optimizing satellite-based QKD, where finite-size effects significantly impact achievable key rates and real-world security assurances.

Finite-size QKD is critical for satellite quantum communication because it addresses the practical limitations and challenges inherent in real-world systems, which asymptotic SKR calculations fail to capture. One significant constraint in satellite-based communication is the limited number of quantum states that can be exchanged due to the short communication windows available during which a satellite passes over ground stations [157]. These limited data samples lead to statistical fluctuations in the measured parameters, which finite-size QKD explicitly accounts for, ensuring accurate and reliable SKR estimations. In contrast, asymptotic models assume an infinite number of exchanged quantum states, which is unrealistic in time-constrained satellite operations [143].

Real-world satellite communication channels introduce a variety of noise sources and imperfections that finite-size QKD is uniquely equipped to handle. Atmospheric turbulence, optical noise, beam divergence, and fading noise cause stochastic variations in satellite-to-ground links, which are often dynamic and unpredictable [158, 159]. Finite-size QKD incorporates these environmental variations into its calculations, ensuring robust key generation even under rapidly changing conditions. Additionally, hybrid noise effects, such as the combination of quantum Poissonian noise [11] and classical AWGN [160], are familiar in satellite channels [21]. While asymptotic models often rely on idealized noise assumptions, finite-size QKD provides a more realistic analysis, making it suitable for practical deployment [26].

Finite-size QKD enhances security in satellite quantum communication by ensuring composable security, making secret keys robust in real-world cryptographic systems [1]. It accounts for collective and coherent attacks, critical for protecting against advanced adversaries in quantum networks [161, 162]. Unlike asymptotic models, finite-size QKD incorporates practical constraints, such as satellite altitudes, zenith angles, and beam misalignments, making it more realistic [7]. It optimizes protocol design and hardware scalability by providing realistic performance benchmarks, ensuring secure and feasible global-scale quantum communication [163].

Satellite-based CV-QKD involves three essential stages [4, 23]:

1. Preparation: Encoding classical information into quantum states, leveraging the quadrature variables of the optical field for CV-QKD. This enables access to an infinite-dimensional Hilbert space, contrasting with the discrete states of discrete-variable quantum key distribution (DV-QKD), which rely on less efficient single-photon detectors [4].
2. Transmission: Propagation of quantum states through a quantum channel, such as FSO links, which must contend with atmospheric disturbances, including turbulence, refraction, and extinction, as well as finite-size statistical fluctuations.
3. Detection: Efficient decoding of received quantum states using homodyne or heterodyne detectors [1]. These detectors provide higher detection speeds and greater system simplicity compared to their DV-QKD counterparts, facilitating compact and robust implementations.

In satellite-based quantum communication, the finite-size SKR in CV-QKD is influenced by key parameters like zenith angle, satellite altitude, beam waist, reconciliation efficiency, transmission coefficient, receiver telescope aperture, detection efficiency, and light source wavelength. These parameters govern the performance and reliability of quantum communication under varying atmospheric conditions and finite-size effects [28]. The zenith angle and satellite altitude critically affect atmospheric losses, beam divergence, and the effective communication window. Lower zenith angles and altitudes reduce attenuation but increase the impact of turbulence and fading noise. The beam waist is pivotal in optimizing signal collection at the receiver, with larger beam waists improving photon capture efficiency but risking diffraction losses at higher altitudes.

Reconciliation efficiency and detection efficiency are essential for minimizing information loss and ensuring robust key generation. High reconciliation efficiency reduces the overhead in classical post-processing, while improved detection efficiency maximizes the detection of transmitted quantum states. Similarly, the transmission coefficient directly impacts the SKR by quantifying the proportion of transmitted signals that successfully reach the receiver, making it critical to mitigate losses due to atmospheric absorption and scattering. The wavelength of the light source influences SNR and atmospheric attenuation [164]. Shorter wavelengths reduce background noise and improve SNR but are more prone to atmospheric scattering. Receiver telescope aperture size also significantly impacts performance, with larger apertures improving photon collection but introducing potential mechanical and alignment challenges. Integrating hybrid noise models and precise parameter optimization ensures that finite-size SKR is maximized in all configurations, uplink, downlink, or hybrid. These approaches are crucial for advancing scalable and secure satellite quantum communication systems capable of addressing real-world environmental and technical challenges [19]. In [115], multiple tables have been introduced for the comparisons of AI/ML applications in QKD, quantum entanglement or teleportation, and quantum network schemes. ML based clustering techniques such as Gaussian mixture

density decomposition (GMDD) [165, 166] play a crucial role in addressing quantum noise in communication systems. Among different categories, clustering algorithms broadly include density-based methods like DBSCAN, partition-based methods such as K-means, and distribution-based methods exemplified by GMM [165]. The integration of secret-sharing techniques with K-means clustering enhances the efficiency and practicality of privacy-preserving secure three-party computation [167]. DBSCAN is unsuitable for datasets with varying regional densities, as it may incorrectly cluster such points, particularly under quantum computing protocols involving Gaussian states [168]. A summarizing table 2.1 has been provided in the following section.

Table 2.1: Comparative Summary of Key Literature in Quantum Communication and Hybrid Quantum Noise Modeling

Paper/ Works	Focus Area	ML Model	Methodology
Ou, Y., et al. [169], 2018	QKD, dense wavelength-division multiplexing (DWDM) fibre network	K-nearest neighbours (KNN)	To investigate and optimise the coexistence of hybrid quantum-classical channels in a QKD-integrated optical network
Cao et al. [170, 171], 2019	Hybrid quantum-classical networks	RL	To increase the number of achievable secret keys for securing data transfers in a multi-tenant QKD network architecture
Sharma, P., et al., [172], 2023	Optical networks	deep reinforcement learning (DRL)	Optimise routing and resource assignment problem in the quantum signal channel of QKD-secured optical network
Buchler, B., et al., [173], 2018	Quantum memory	artificial neural network (ANN)	To optimize a laser-cooled atomic ensemble to achieve ‘stopped and stationary light’ optical quantum memory with an efficiency of about 87%
Khatri, S., et al., [174], 2021	Quantum memory	RL	To develop the mathematical tools needed to perform reinforcement learning of entanglement distribution protocols in general quantum networks
Continued on next page			

Table 2.1 – continued from previous page

Paper/ Works	Focus Area	ML Model	Methodology
Yin, J., et al., [175], 2012	Quantum network	ML	To accurately and quickly predict the key rate for satellite-to-ground quantum communication channels via ML and stellar image recognition in quantum network
Reiß et al., [176] 2023	Quantum repeaters	DRL	To search for optimal solutions to memory storage time limits
Dong, Ye et al., [177] 2020	Secret sharing	Linear regression, multilayer perceptron (MLP), and convolutional neural network (CNN)	Improved the accuracy, reliability, security, and performance of privacy-preserving distributed ML based on secret sharing
Wei, W et al., [178] 2022	Secret sharing	K-means clustering	Enhanced the efficiency and practicality of a privacy-preserving secret-sharing-based secure three-party computation
Lu, S., et al., [179] 2018	quantum entanglement (QE)	Supervised learning	Demonstrated a reliable separability-entanglement classifier
Chen, Y., et al., [180] 2021	QE	Complex-valued neural network	Detected a quantum entanglement in high-dimensional and multipartite quantum systems and achieves a detection accuracy of 97.5%
Asif, N., et al., [181] 2023	QE	Supervised learning	Constructed a classifier by employing the relationship between coherence and entanglement
Wallnöfer, J., et al., [182] 2020	QE	RL, projective simulation	Discovered various quantum communication protocols, including quantum teleportation, quantum distillation, and end-to-end bipartite entanglement distribution along a chain of quantum repeaters
Continued on next page			

Table 2.1 – continued from previous page

Paper/ Works	Focus Area	ML Model	Methodology
Zhang, H., et al., [183] 2022	QE	Unsupervised learning	Trained an on-chip autoen- coder to encode 3-D quantum state onto 2-D quantum tele- portation, observing 3-D tele- portation
Xu, J., et al., [184] 2022	QE	KNN	Predicted the continuous- variable quantum teleporta- tion squeezing parameter and the satellite altitude
Chakraborty et al., 2024 [21, 22]	HQN Model- ing	GMM-based capacity estimation	Effectively models mixed noise types considering quantum Poissonian noise and AWGN
Chakraborty et al., 2025	Entropy Esti- mation	Differential, von Neu- mann, Rényi, Tsallis En- tropies	Offers diverse quantification of uncertainty in quantum states
Chakraborty et al., 2024 [18, 22]	Optimization in Quantum Channels	GMM for noise + EM clustering	Combining statistical learning with channel optimization
Chakraborty et al., 2024 [23]	Satellite CV-QKD	Asymptotic SKR	Satellite quantum channel modeling and parametric adaptability to changing free-space channel conditions
Chakraborty et al., 2024 [24]	Satellite CV-QKD	Finite-size SKR, collec- tive attack modeling	Realistic security under finite key length and satellite scenar- ios

2.4.1 Continuous-variable and Discrete-variable QKD

CV and discrete variables (DV) QKD represent two prominent approaches to implementing secure quantum communication. Both methods leverage the principles of quantum mechanics to ensure the secure exchange of cryptographic keys, but they differ in their encoding schemes, hardware requirements, and operational advantages. In DV-QKD, information is encoded in discrete quantum states, such as the polarization or phase of single photons. Protocols like BB84 and E91 are classic examples of DV-QKD, utilizing binary quantum states to establish secure keys. The primary advantage of DV-QKD lies in its inherent resistance to noise and its compatibility with single-photon detectors, which enable precise measurements. However, the reliance on single-photon sources and detectors can pose practical challenges, including limited detection efficiencies and higher costs associated

with specialized hardware.

Conversely, **CV-QKD** encodes information in continuous variables, such as the quadratures of the electromagnetic field. Protocols like Gaussian-modulated coherent state (**GMCS**) **QKD** utilize homodyne or heterodyne detection to measure the encoded quantum states. One of the significant advantages of **CV-QKD** is its compatibility with standard telecommunication infrastructure, including coherent detection systems and high-rate photodetectors [11]. This compatibility enables **CV-QKD** to achieve higher key rates over short and medium distances, making it suitable for metropolitan-scale quantum networks. The choice between **CV-QKD** and **DV-QKD** often depends on the specific application and the operational environment. **DV-QKD** excels in long-distance communication due to its robustness against loss and noise, particularly when paired with satellite-based platforms for global-scale secure communication. In contrast, **CV-QKD** is well-suited for short-distance, high-bandwidth applications, leveraging its compatibility with existing fibre-optic networks to enable cost-effective deployment [161].

Despite their differences, both **CV** and **DV-QKD** face common challenges, including the need for noise-resilient protocols, efficient error correction, and robust key reconciliation mechanisms. Hybrid **QKD** systems that integrate both **CV** and **DV** approaches are emerging as a promising direction, aiming to combine the strengths of both paradigms [1]. Such systems can leverage the high key rates of **CV-QKD** in short-range applications while utilizing the robustness of **DV-QKD** for long-range communication. Advancements in quantum technologies continue to refine the capabilities of both **CV** and **DV-QKD**. Innovations in photon source engineering, detector technologies, and noise mitigation strategies drive the scalability and practicality of **QKD** systems. **CV** and **DV-QKD** are poised to play complementary roles in realizing secure, global quantum communication networks as these technologies mature.

2.4.2 Direct Reconciliation and Reverse Reconciliation

The direct-reconciliation (**DR**) and **RR** are critical techniques in the context of satellite-based **QKD**, particularly for **CV-QKD** systems. These methods determine how the raw key data is processed to establish a secure and shared cryptographic key between communicating parties despite the presence of noise and potential eavesdropping [25]. In **DR**, the sender (typically referred to as Alice) encodes information onto a quantum state, and the receiver (Bob) measures this state. Bob's measurements are used to reconstruct Alice's original data during the reconciliation process. This method is intuitive and straightforward, but it has a significant limitation: its efficiency decreases as channel loss increases. High loss, common in satellite-to-ground communication links due to atmospheric turbulence and beam divergence, can lead to degraded reconciliation performance, making **DR** less suitable for long-distance or high-loss scenarios [185]. **RR**, on the other

hand, reverses the roles of Alice and Bob during the reconciliation process. Here, Bob’s measured data serves as the reference, and Alice adapts her data to match Bob’s. This approach is particularly advantageous in high-loss environments, such as satellite-based QKD, as it mitigates the impact of losses on the key rate. RR is often paired with advanced error-correction codes and noise mitigation techniques to further enhance its efficiency and robustness.

Satellite QKD systems, which operate over long distances and encounter varying loss conditions, typically benefit more from RR. The high loss inherent to free-space optical links makes RR essential for maintaining key rates and ensuring secure communication [25]. Additionally, RR enables lower-power quantum signals, reducing the risk of detection by eavesdroppers while maintaining compatibility with practical detector sensitivities. Implementing DR and RR in satellite QKD involves complex trade-offs between security, efficiency, and technological feasibility [185]. While DR is better suited for low-loss, short-distance applications, RR’s ability to handle high-loss channels makes it indispensable for satellite-based systems aiming for global-scale secure communication. Furthermore, the choice between these reconciliation techniques depends on the specific protocol and hardware configurations used in the QKD system.

Advancements in reconciliation algorithms, such as Low-Density Parity Check (LDPC) codes and turbo codes, have further optimized both DR and RR for satellite QKD. These developments enhance error-correction capabilities and improve reconciliation efficiency, paving the way for more scalable and robust quantum communication networks. As satellite QKD systems continue to evolve, integrating DR and RR techniques will remain central to their success, enabling secure and reliable key distribution across intercontinental distances.

2.4.3 Asymptotic QKD versus Finite Regime

In the satellite-based QKD, the distinction between asymptotic and finite regime scenarios plays a crucial role in understanding the practical and theoretical performance of QKD systems. Both approaches address the generation of secure cryptographic keys but differ in their treatment of resources, assumptions, and constraints. Asymptotic QKD refers to the idealized scenario where the number of transmitted quantum signals approaches infinity. In this regime, statistical fluctuations in the key generation process become negligible, allowing for the application of asymptotic security proofs. These proofs guarantee the unconditional security of the key based on the fundamental principles of quantum mechanics. Asymptotic QKD enables the calculation of key rates with high precision and provides insights into the theoretical limits of quantum communication systems. However, it assumes perfect operational conditions, such as an infinite number of signals and negligible error rates, which are impractical in real-world scenarios.

In contrast, the finite regime considers the practical constraints of real-

world QKD systems, where the number of transmitted quantum signals is limited. This scenario accounts for statistical fluctuations due to finite data samples, which can significantly impact the security and efficiency of key generation. Finite-size security proofs are more complex than their asymptotic counterparts because they must incorporate these statistical deviations to ensure robustness against potential attacks [162]. These proofs often require additional resources, such as more extensive error correction and privacy amplification, to achieve the same level of security as in the asymptotic case. The finite regime is particularly relevant for satellite QKD, where operational constraints such as limited satellite overpass time, atmospheric loss, and detector efficiency restrict the number of quantum signals that can be exchanged [26]. In such scenarios, finite-size effects are critical in determining the achievable key rates and the overall feasibility of secure communication. Addressing these effects requires careful protocol design, optimization of transmission parameters, and advanced reconciliation techniques to maximize the key generation efficiency within the finite resource constraints.

One of the key challenges in the finite regime is striking a balance between security and key rate. While strong security guarantees demand extensive data for statistical analysis, the limited number of signals in satellite QKD necessitates efficient use of available resources. Advanced techniques, such as parameter estimation and tight finite-size security bounds, are employed to mitigate these challenges and ensure the practicality of QKD protocols in finite scenarios. The interplay between the asymptotic and finite regimes highlights the trade-offs in satellite QKD. Asymptotic analyses provide valuable benchmarks and theoretical insights, while finite regime considerations ensure the practical viability of QKD systems under realistic conditions [37]. Future advancements in quantum technologies, including more sensitive detectors, higher-efficiency photon sources, and robust error correction protocols, are expected to bridge the gap between these two regimes, enabling satellite QKD systems to approach their theoretical performance limits while maintaining practical operability.

Despite this progress, significant challenges persist in satellite quantum communications. Optical transmission between satellites and ground-based platforms faces several limitations, including diffraction, systematic pointing errors, and atmospheric turbulence [146],[147]. These factors cause transmission losses by broadening the optical beam and introducing wavelength-dependent losses due to atmospheric absorption of photons [148]. Detector efficiencies need substantial improvement for efficient quantum key exchange [149]. Photon loss during propagation through atmospheric turbulence and background noise mitigation are critical areas of investigation [150]. While larger telescopes and shorter photon wavelengths can mitigate diffraction losses, a balance between telescope size, cost, and transmission performance is necessary [151],[149]. Atmospheric turbulence, caused by temperature-induced refractive index fluctuations, broadens and wanders the beam, introducing additional loss [152],[153]. Works like [154] have de-

veloped p.d.f.s of transmittance for slant propagation paths, proposed models for atmospheric quantum channels with turbulence, and experimentally characterized distant FSO atmospheric channels. Addressing these challenges is essential for the seamless integration of QKD into existing satellite communication infrastructures, thereby enhancing the robustness and efficiency of global quantum networks with the use of quantum repeaters [155]. Adaptive optical systems and optimal ground station selection can mitigate turbulence effects, particularly in uplink channels where turbulence is most significant [156],[28].

2.5 Conclusion

In conclusion, this chapter provides a comprehensive overview of the fundamental concepts of quantum communication, including quantum information theory, quantum noise models, and QKD systems. It explored the significance of quantum entropy in analyzing channel capacity and securing QKD. The discussion highlighted the limitations of existing noise models and emphasized the need for hybrid quantum noise modeling to achieve a more realistic representation of practical quantum channels. Additionally, it reviewed the role of machine learning in optimizing quantum signal processing and noise mitigation. The impact of hybrid noise on security frameworks, particularly under collective attacks, was examined to establish a strong foundation for analyzing quantum channel vulnerabilities. The insights from this chapter set the stage for developing a novel hybrid quantum noise model that enhances the efficiency and security of satellite-based quantum networks. This background serves as the theoretical and conceptual framework for the research in subsequent chapters.

In the next chapter, the reader will find an introductory discussion of the mathematical framework of HQN and a detailed discussion of the achievable rate of the hybrid quantum channel.

Chapter 3

Hybrid Quantum Noise Modeling for Quantum Channels

3.1 Introduction

Quantum information processing leverages the principles of quantum mechanics, utilizing qubits, to improve computational and communicative tasks. In this realm, the quantum channel's capacity is pivotal in determining the efficiency and accuracy of quantum information handling; its performance is influenced by quantum channel noise. This chapter developed a holistic [HQN](#) model that comprehensively integrated all the noises of the quantum channel to determine the quantum channel capacity. In this chapter, we formulated a mathematical expression for this capacity and conducted simulations for both Gaussian and non-Gaussian inputs. A hybrid noise model is constructed by the convolution of Poisson-distributed quantum noise with classical additive white Gaussian noise. The [GMM](#) has been utilized to characterize the quantum-classical noise and the density function of the received signal. The maximum amount of quantum information that can be reliably transmitted over a quantum channel (per use of the channel) has been determined by its capacity. Entropy and related quantities, such as mutual information between senders and receivers, play a role in calculating the channel's achievable rate. This formulation of quantum channel capacity is derived from the mutual information shared between the transmitter and receiver, encompassing the entropies of the information signals. The quantum channel presents a higher capacity with respect to [SNR](#) for Gaussian inputs than non-Gaussian ones.

This chapter developed a comprehensive hybrid noise model that combines classical and quantum noises, subsequently applied to estimate the capacity factor. It is considered a scenario of quantum communication where the sender and receiver are classical. Consider the architecture when both the sender and receiver use classical devices for communication, as this is a more practical scenario due to the limited availability of quantum computers. To achieve quantum security in communication links, classical information is encoded in quantum states (e.g., in the states of a photon); hence,

a single quantum channel is used to transport the quantum information. On the receiver side, the received signal, in the form of quantum information, is delivered, and the received quantum information is decoded into a classical signal through measurement procedures. The maximum achievable data rate, that is, the classical capacity of a quantum channel, will be calculated through this process. On the other hand, there is another use case where the sender and receiver communicate with quantum devices, and the channel between them is purely quantum. In that case, the investigated channel capacity is the quantum capacity of the quantum channel. The literature has reported [50] the classical capacity of the quantum channel, also known as the quantum capacity of a quantum channel. For that capacity, expression is derived from the density matrices of the qubit. However, the lack of a statistical formulation of the quantum channel has been noted [6], and simulating results, such as how capacity varies with SNR, have been unavailable so far [50]. The lack of models for the probability distribution function of HQN and quantum received signals was another motivation behind this research. Fig. 3.1 explains the direction of the study pictorially. The contributions of this chapter are many-fold, involving the introduction of the statistical theory of the HQN model, which considers both quantum Poissonian noise and classical AWGN, thereby providing the mathematical expression for the capacity of the Gaussian quantum channel. However, this chapter focuses on Gaussian quantum channels with Gaussian transmitted signals; however, the transmitted signal may exhibit non-Gaussian characteristics. To compare these two cases, it is essential to vary the input distribution to determine how capacity will fluctuate with respect to the SNR for the Gaussian and non-Gaussian input for the Gaussian quantum channel.

The main aspects of this chapter are (I) Designing a noisy quantum channel via modeling HQN by considering it as a combination of quantum Poissonian noise and classical additive white Gaussian noise, (II) Proposed a closed-form solution for the capacity of Gaussian quantum channel despite of Gaussian mixture (GM) Noise densities and GM output signal models, (III) Compare the results from the capacity tendency (the fluctuation of capacity or the growth / increasing/ decreasing nature of the capacity with respect to the signal-to-noise ration will be evaluated), for Gaussian and non-Gaussian inputs, (IV) The statistical interpretation of quantum channels has been introduced in this paper for the development of statistical quantum signal processing. It also analyzes the received signal models for a Gaussian variate transmitted signal and non-Gaussian inputs for the Gaussian quantum channel. The model is studied in detail in the current article, with particular emphasis on comparing capacities for Gaussian and non-Gaussian input to the quantum channel. In each case (Gaussian and non-Gaussian), the classical capacities of quantum channels have been derived throughout this literature.

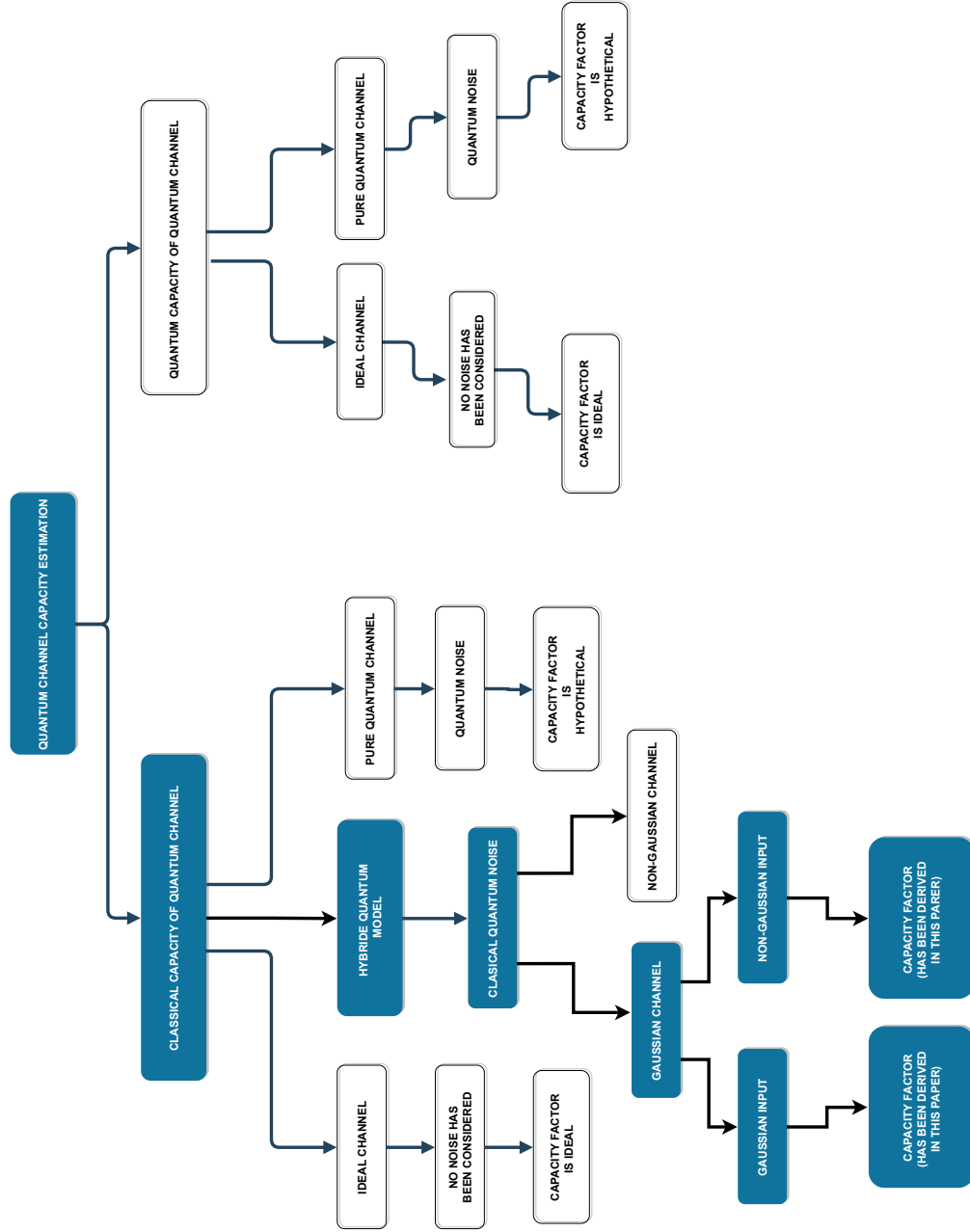


Figure 3.1: The categorization of noise and capacity factor of the Gaussian quantum channel.

3.2 System Model

The quantum information processing (QIP) is based on quantum states for data manipulation [50]. Unlike classical information processing, which uses classical bits based on macroscopic properties, QIP employs quantum states with qubits as basic units. These qubits are represented by quantum state vectors reflecting their probabilistic nature, hinging on quantum phenomena like superposition and entanglement. Various physical systems can generate quantum states, with light, consisting of photons, being ideal for long-distance communication. Entangled single- and two-photon states are desirable but challenging to prepare, making Gaussian states, such as coherent states [186], a more practical choice. Gaussian states, characterized by their Gaussian distribution in phase or Fock space, have proven robust for numerous QIP tasks. Quantum optical Gaussian states play a pivotal role in quantum information experiments, facilitating progress in both bright and weak Gaussian light contexts. Extending the theoretical and experimental successes of discrete quantum variables to continuous variables is a compelling endeavor [187], [188]. Gaussian states are central to this exploration, given the enhanced capabilities of quantum optical systems [189],[190]. They underpin properties, entanglement theory, communication protocols, and emerging directions such as Gaussian cluster states for quantum computing [191], [192].

3.2.1 Gaussian Quantum Channel

In mathematical terms, a quantum channel is defined as a completely positive trace-preserving map. $\rho \mapsto \mathbf{T}(\rho)$ That takes states, i.e., density operators ρ acting on some Hilbert space $\mathcal{H}$, into states. This chapter assumed that output and input Hilbert spaces are identical for simplicity. Every channel can be conceived as a reduction of unitary evolution in a larger quantum system. So for any channel $\mathbf{T}$ there exists a state ρ_E on a Hilbert space $\mathcal{H}_E$, and a unitary $\mathbf{U}$ such that.

$$\mathbf{T}(\rho) = \text{tr}_E[\mathbf{U}(\rho \otimes \rho_E)\mathbf{U}^\dagger] \quad (3.1)$$

The system labelled E serves as an environment, embodying degrees of freedom that include observation, inducing a decoherence process. The channel is then a local manifestation of the unitary evolution of the joint system. A Gaussian channel [193, 194, 195, 196, 197] is now a channel of the form as in Eq.(3.1), where $\mathbf{U}$ is a Gaussian unitary, determined by a quadratic Bosonic Hamiltonian, and ρ_E is a Gaussian state [194]. This restriction to a quadratic Hamiltonian gives a pretty good description of the physical system, such as the lossy optical fiber. In this study, the quantum channel is assumed to be Gaussian. However, the input states are not necessarily taken to be Gaussian.

The simplest Gaussian channel is a lossless unitary evolution governed

by a quadratic Bosonic Hamiltonian:

$$\rho \mapsto U \rho U^\dagger, U = e^{i/2 \sum_{k,l} \mathbf{H}_{kl} \mathcal{R}_k \mathcal{R}_l} \quad (3.2)$$

with $\mathbf{H}$ being a real and symmetric $2n \times 2n$ matrix, $\mathcal{R}$ represent s the canonical coordinates for the quantum system with n modes that is n canonical degrees of freedom [10, 198]. Such unitaries correspond to a representation of the real symplectic group $Sp(2n, \mathbb{R})$, formed by those real matrices for which $\mathbf{S} \sigma \mathbf{S}^t = \sigma$, where the matrix σ defines the symplectic scalar product [10, 198]. Such linear transformations preserve the commutation relations, the relation between such a canonical transformation in phase space and the corresponding unitary in Hilbert space is given by $\mathbf{S} = e^{\mathbf{H} \sigma}$. Gaussian unitaries are ubiquitous in physics, particularly in optics, which is why Gaussian channels play a crucial role. Notably, the action of ideal beam splitters, phase shifters, and squeezers corresponds to symplectic transformations.

Depending on the context, it is appropriate or transparent to formulate a Gaussian channel in the Schrodinger picture $\rho \mapsto \mathbf{T}_{\mathbf{A}, \mathbf{Z}}(\rho)$ or to define it as a transformation of covariance matrices

$$\rho \mapsto \mathbf{A}^t \rho \mathbf{A} + \mathbf{Z} \quad (3.3)$$

This is the most general form of a Gaussian channel. $\mathbf{A}$ serves the purpose of amplification, attenuation, and rotation in phase space, whereas the contribution $\mathbf{Z}$ is a noise term that may consist of quantum (required to make the mapped physical) and classical noise. Interestingly, $\mathbf{A}$ can be any real matrix, and therefore any map $\rho \mapsto \mathbf{A}^t \rho \mathbf{A}$ can be made approximately, as long as ‘sufficient noise’ is added [198], [10]. This model demonstrates that Gaussian channels can add noise to a system, ensuring the output remains a valid quantum state, which is essential for realistic quantum communication systems where both quantum and classical noises are considered additive.

3.2.2 Qubit Model

A qubit is characterised as superpositions of basis states $|0\rangle$ and $|1\rangle$, denoted as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, with complex coefficients fulfilling the normalization condition $|\alpha|^2 + |\beta|^2 = 1$. Density matrices represent both pure and mixed quantum states. Pure states correspond to single-state vectors, while mixed states signify probabilistic combinations of multiple-state vectors. For a qubit in a pure state $|\psi\rangle$, the density matrix ρ is given by $\rho = |\psi\rangle \langle \psi| = \begin{bmatrix} |\alpha|^2 & \alpha^* \beta \\ \alpha \beta^* & |\beta|^2 \end{bmatrix}$, where α^* and β^* are the complex conjugates of α and β , respectively. The density matrix for a mixed state, which is a probabilistic mixture of pure states $|\psi_i\rangle$ with probabilities p_i , is given by $\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i|$, with the condition that $\sum_i p_i = 1$.

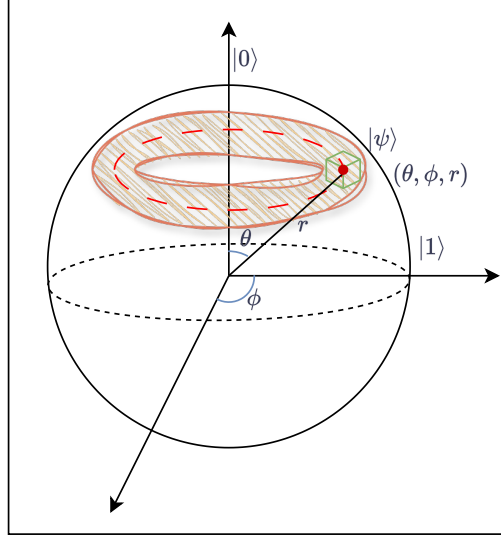


Figure 3.2: With feasible HQN power, the qubit remains within a torus-like object with a cuboid cross-sectional area inside the Bloch sphere after experiencing the HQN.

For a pure state, a qubit can be visualized as a point (θ, ϕ) on the surface of the Bloch sphere [3]. On the other hand, a qubit can also be described by a bivariate function $\zeta(\theta, \phi)$, where θ and ϕ are variables x_1 and x_2 respectively. Considering the restricted noise power assumption, the qubit stays within a strip on the Bloch sphere's surface. Specifically, if the qubit is rotated by varying θ while keeping ϕ constant, it traces a circular path. The strip centered on this path has a width of 2δ , with δ being the distance from the circle to the strip's edges. We propose that the qubit's position remains within this strip under feasible HQN power. Mathematically, this is described by $(\theta, \phi) \mapsto (\tilde{\theta}, \phi \pm \delta)$, where $\tilde{\theta} \in [0, 2\pi]$, and δ is sufficiently small for ϕ to be nearly constant with respect to θ [21, 22]. On the contrary, a mixed-state qubit ρ can be characterized by the point vector (θ, ϕ, r) inside the Bloch sphere, where r denotes its distance from the sphere's center. This qubit can be described by a multivariate function $\tilde{\zeta}(\theta, \phi, r)$, with θ , ϕ , and r as variables x_1 , x_2 , and x_3 respectively. Considering noise power, we assume the qubit remains within a torus-like object with a square cross-section inside the Bloch sphere. When rotating the qubit by varying θ while keeping ϕ and r constant, it follows a circular path shown in Fig. 3.2. The torus-like object's cross-section width is 2δ . Mathematically, under noise, the qubit's position changes as $(\theta, \phi, r) \mapsto (\tilde{\theta}, \phi \pm \delta, r \pm \delta)$ with $\tilde{\theta} \in [0, 2\pi]$. Assuming δ is small ϕ and r are nearly constant with respect to θ , simplifying to $(\theta, \phi, r) \mapsto (\tilde{\theta}, \phi, r)$. In summary, this approximation involves varying either θ or ϕ while holding the other variables constant. In our case, we varied θ , considering ϕ and r as constant. In either of the cases, a qubit ρ can be characterized by a scalar ρ [21, 22].

The theoretical treatment extends to imagining qubits navigating along

a circular path on the sphere, which can be as simple as a single rotation or as complex as multiple rotations akin to a spiral. This conceptual extension allows the qubit to be approximated by a single scalar ρ , simplifying its description to a one-dimensional random variable that effectively captures the probability distribution of quantum noise impacting the qubit. This approach reduces computational complexity while retaining the essence of the qubit's behavior under noise within the quantum framework.

The equation (3.3) represents the most comprehensive form of a Gaussian channel. Here, $\mathbf{A}$ functions to modulate the signal through amplification, attenuation, and rotational adjustments in phase space. Meanwhile, $\mathbf{Z}$ adds a noise component, which includes both quantum noise (necessary to render the transformation physically meaningful) and classical noise. Intriguingly, $\mathbf{A}$ can be any real matrix, allowing any transformation $\rho \mapsto \mathbf{A}^T \rho \mathbf{A}$ to be approximated, provided that adequate noise is incorporated. As detailed by equation (3.3), a simple quantum channel can be modeled as $\rho \mapsto \rho + \mathbf{Z}$, where $\mathbf{Z}$ includes both quantum and classical components of noise [21, 22]. Consider, $\mathbf{A} = \mathbf{I}_{2n}$ where $\mathbf{I}_{2n}$ is the identity matrix of order $2n \times 2n$ and n is the canonical degrees of freedom of the quantum system. $\mathbf{A}$ can be any real matrix; the transformation is valid as a quantum channel if enough noise is introduced [10]. In such a scenario, $\mathbf{A}^T \rho \mathbf{A}$ it becomes scalar. The noise $\mathbf{Z}$ added to the system is also treated as a scalar from the convolution of [AWGN](#) and quantum Poisson noise with both components of the noises in scalar representation [21, 22]. Hence, this setup can be equated to the basic formula in communication theory where $Y = X + Z$, representing the transmitted signal X , the received signal Y , and the [HQN](#) Z impacting the channel from various sources. In a practical quantum communication network handling classical information, it is presumed that the links are influenced by both quantum and classical noise. This noise is assumed to be additive, where $Z = Z_1 + Z_2$, with Z_1 being Poisson-distributed quantum shot noise and Z_2 representing Gaussian-distributed white classical noise [21, 22]. This concept is further illustrated in the referenced Fig. 3.3, which provides a schematic overview of the theory.

3.3 Methodology

In this section, a brief overview of the current chapter is provided. Starting with the channel equation $Y = X + Z$, where X , Y , and Z correspond to the random variables of the transmitted signal, received signal, and [HQN](#), the p.d.f. of the [HQN](#) will be the convolutional product of the component Quantum Poissonian noise and additive white Gaussian noise. This [HQN](#) model will be convoluted with the (I) Gaussian and (II) non-Gaussian input separately to get the received signal models of each setup shown in Fig. 3.4. In the meantime, the entropies of received signals and the [HQN](#) will be calculated to evaluate (I) the mutual information between the Gaussian transmitted signal and the corresponding received signal and (II) the mutual information between the non-Gaussian transmitted signal and the

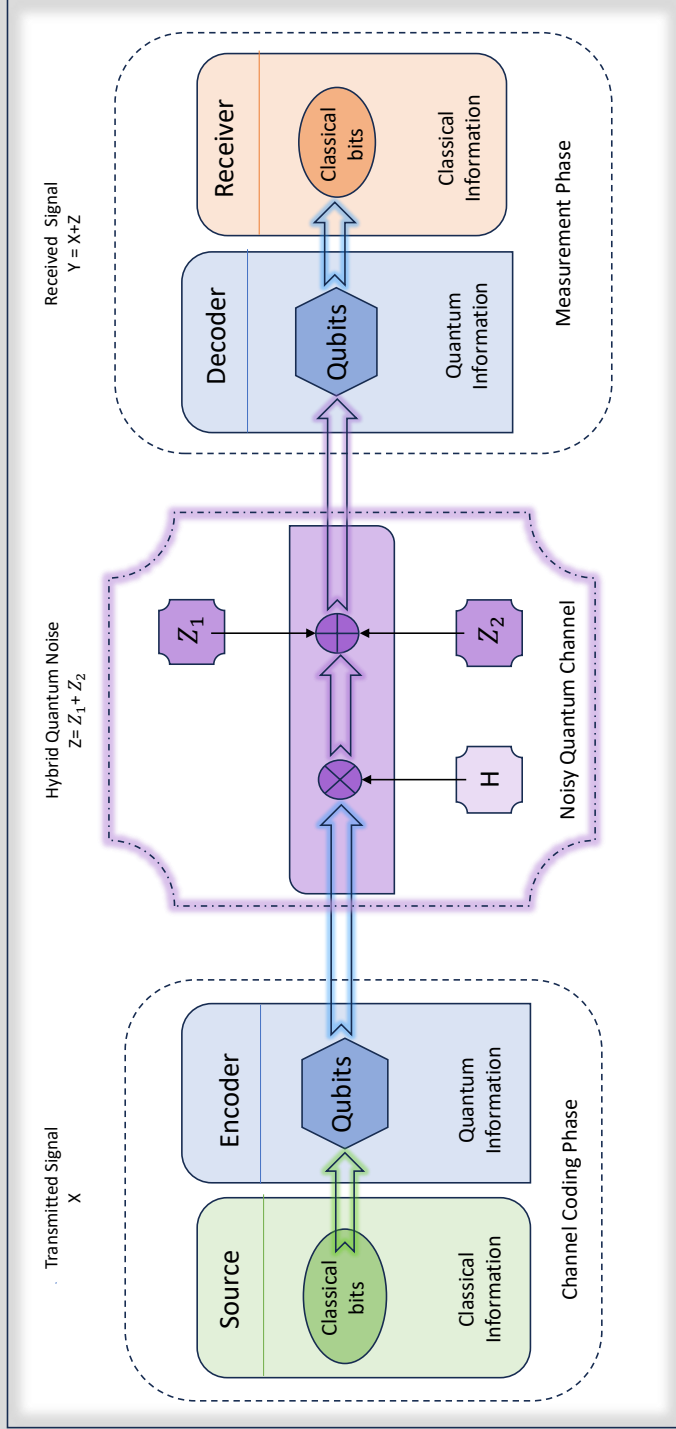


Figure 3.3: A noisy Quantum Channel: A schematic diagram showing a single quantum link between transmitter and receiver. H is the channel matrix, Z is the **HQN** as a convolution of quantum Poissonian noise Z_1 and additive white Gaussian noise Z_2 . The complete received signal can be modeled using the channel equation $Y = X + Z$, where X is the transmitted signal.

corresponding received signal. Finally, the capacity of the Gaussian channel will be calculated for (I) Gaussian and (II) non-Gaussian inputs separately to compare their trends to the signal-to-noise ratio.

3.4 Quantum Noise Model

In terms of mathematics, the classical additive white Gaussian noise and quantum Poisson noise are jointly described as $Z = Z_1 + Z_2$, where Z_1 is the noise arising from quantum fluctuations that have a Poissonian distribution and Z_2 is the classical counterpart, which has a Gaussian distribution. The statistical description of the hybrid classical-quantum noise Z is calculated considering it as a convolution product of Z_1 and Z_2 .

Quantum noise Z_1 follows a Poisson distribution with parameters λ , and classical noise Z_2 follows a normal distribution with parameters μ_{Z_2} and σ_{Z_2} . Mathematically, $Z_1 \sim \mathcal{P}(\lambda)$, $\lambda \geq 0$, $\lambda \in \{0, 1, 2, \dots\}$ and $Z_2 \sim \mathcal{N}(\mu_{Z_2}, \sigma_{Z_2}^2)$ where μ_{Z_2} and $\sigma_{Z_2}^2$ are the mean and variance of the distribution, respectively. The quantum-classical noise is modeled as a convolution product of Poisson and Gaussian distributions. The probability mass function (p.m.f.) of Z_1 is given by,

$$f_{Z_1}(k) = \frac{e^{-\lambda} \lambda^k}{k!} \quad (3.4)$$

where $\lambda \geq 0$ and $k \in \{0, 1, 2, \dots\}$. The p.d.f. of Z_2 can be expressed as,

$$f_{Z_2}(t) = \frac{1}{\sigma_{Z_2} \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{t - \mu_{Z_2}}{\sigma_{Z_2}} \right)^2} \quad (3.5)$$

where μ_{Z_2} and σ_{Z_2} are the mean and standard deviation (s.d.) of the corresponding distribution. Z_1 has a discrete distribution while Z_2 has a continuous distribution, but to develop the hybrid noise model, we need to calculate their joint distribution. This is done by expressing the p.m.f. of the discrete Poisson distribution in terms of the p.d.f. of a continuous distribution and then calculating the joint distribution of two continuous distributions.

The cumulative distribution function (CDF) of the discrete random variable (r.v.) Z_1 can be written as

$$F_{Z_1}(t) = \sum_{\forall k \in R_{Z_1}} P_{Z_1}(k) u(t - k) \quad (3.6)$$

where $R_{Z_1} = \{0, 1, 2, \dots\}$. Now, the p.d.f. of the above function can be written as

$$\begin{aligned} f_{Z_1}(t) &= \frac{dF_{Z_1}(t)}{dt} = \sum_{\forall k \in R_{Z_1}} P_{Z_1}(k) \frac{d}{dt} u(t - k) \\ &= \sum_{\forall k \in R_{Z_1}} P_{Z_1}(k) \delta(t - k) = \sum_{\forall k \in R_{Z_1}} \frac{e^{-\lambda} \lambda^k}{k!} \delta(t - k) \end{aligned} \quad (3.7)$$

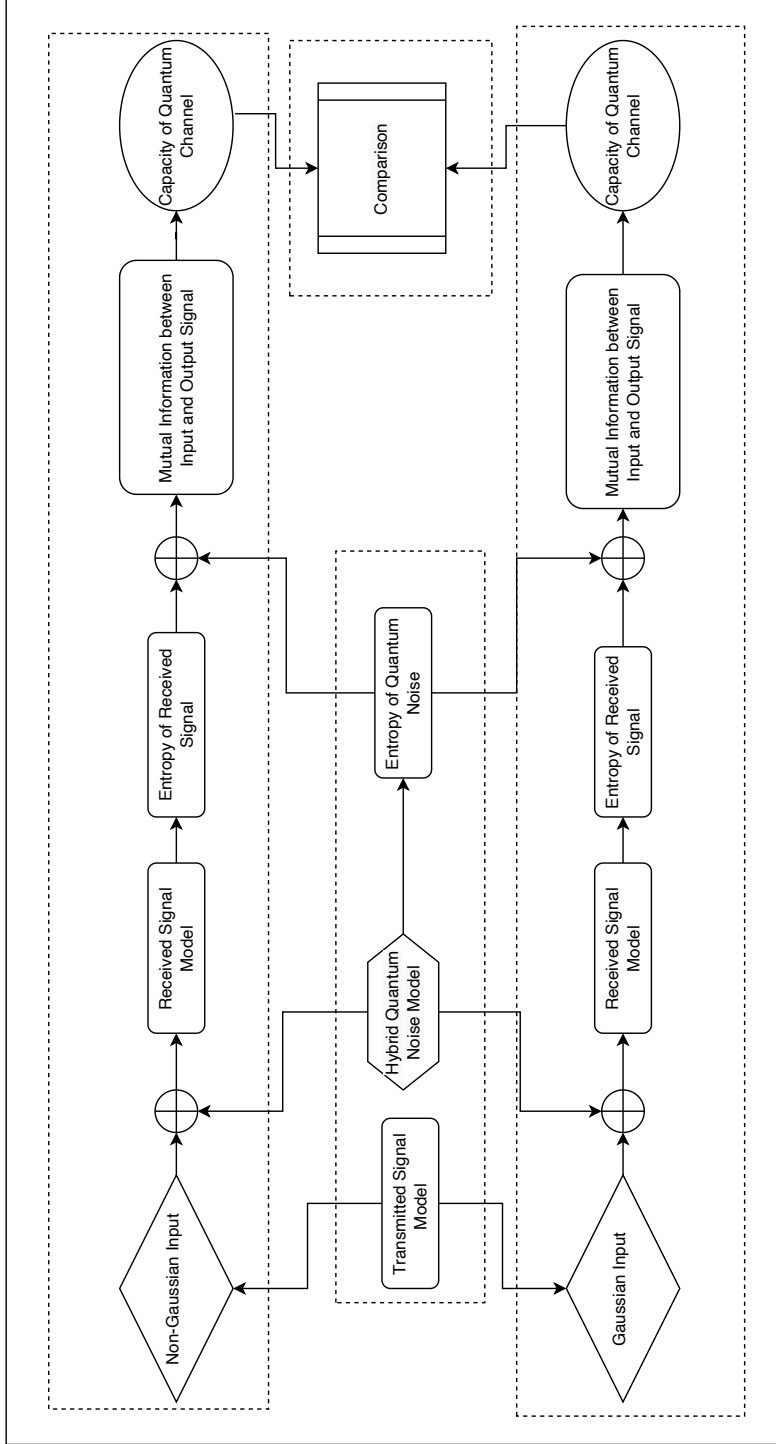


Figure 3.4: The block diagram explains the flow of the research methodology for Gaussian and non-Gaussian transmitted signals.

where $\delta(x) = \frac{d}{dx}u(x)$ is the Dirac delta function and $u(\cdot)$ is the unit step function. We know that if U is a discrete r.v. with p.m.f. $p_U : \chi \rightarrow [0, 1]$, and χ is a discrete set (maybe countably infinite), then the r.v. U can be thought of as a continuous r.v. with [p.d.f.](#)

$$f_U(u) = \sum_{\forall u_s \in \chi} p_U(u_s) \delta(u - u_s). \quad (3.8)$$

Now, if V is a continuous r.v., and $W = U + V$ is a hybrid r.v. then the [p.d.f.](#) of W can be computed from [p.d.f.s](#) of U and V . Assuming U and V are independent r.v.s, the p.d.f of W can be expressed as a convolution product of [p.d.f.s](#) f_U and f_V . Therefore,

$$f_W(w) = \sum_{\forall u_s \in \chi} p_U(u_s) f_V(w - u_s). \quad (3.9)$$

From the expressions (3.5) and (3.7) the [p.d.f.](#) of Z can be written as,

$$f_Z(z) = \sum_{\forall k \in R_{Z_1}} f_{Z_1}(k) f_{Z_2}(z - k) = \sum_{k=0}^{\infty} \frac{e^{-\lambda} \lambda^k}{k!} \frac{1}{\sigma_{Z_2} \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{z - k - \mu_{Z_2}}{\sigma_{Z_2}} \right)^2} \quad (3.10)$$

Hence, we evaluate the differential entropy of the r.v. Z given by the formula,

$$h(Z) = - \int_{\chi_Z} f_Z(z) \log_2 f_Z(z) dz \quad (3.11)$$

where χ_Z is the support of f_Z , i.e., the set on which f_Z is nonzero.

3.5 Quantum Signal Model for Gaussian Input

In quantum mechanics, a Fock state or number state is a quantum state that is an element of a Fock space with a well-defined number of particles (or quanta). These states are named after the Soviet physicist Vladimir Fock. In experimental practice, it is of general concern how robustly quantum states can be manipulated. A pure quantum state is symbolized by a ray in a Hilbert space over complex numbers [199]. However, density matrices can represent mixed states: positive semi-definite operators that act on Hilbert spaces [200]. In practice, the preparation of single-photon or two-photon entangled states (deterministically) is complex. Single-photon sources are light sources that emit light as individual photons. They are distinct from coherent light sources (e.g., lasers) and thermal light sources (such as incandescent light bulbs). The Heisenberg uncertainty principle conveys that a state with an exact number of photons of a single frequency cannot be created. However, the Fock states or number states can be observed for a system where the amplitude of the electric field is distributed over a narrow bandwidth. Fock states play an essential role in the second quantization formulation of quantum mechanics. In these circumstances, a single-photon source rises to an effectively one-photon-number state. Photons from an ideal single-photon source manifest quantum mechanical characteristics.

3.5.1 Quantum Transmitted Signal Model

Mathematically, a state is Gaussian if its distribution function in phase or its density operator in the Fock space is Gaussian. Examples of Gaussian functions include the well-known [p.d.f.](#) of the Normal distribution and the Wigner function, among others. Here, we began with the Normal distribution as the input distribution for [CV](#) quantum information processing. In our model, the input quantum signal X is in a Gaussian state, and it can be characterized by a Gaussian distribution with parameters μ_X and σ_X , $X \sim \mathcal{N}(\mu_X, \sigma_X^2)$ where μ_X and σ_X^2 are the mean and variance of the distribution respectively. The [p.d.f.](#) f_X of X can be expressed as,

$$f_X(x) = \frac{1}{\sigma_X \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{x - \mu_X}{\sigma_X} \right)^2} \quad (3.12)$$

where μ_X and σ_X are the mean and [s.d.](#) of the distribution. The received quantum signal can be calculated as the convolution product of the Gaussian-distributed transmitted signal and the quantum noise signal. As discussed above, important experiments of [QIP](#) are done with quantum light.

3.5.2 Quantum Received Signal Model

The distribution of the transmitted signal X and the hybrid quantum-classical noise Z are independent of each other, and their respective [r.v.s](#) are also independent. The input quantum signal is considered in a Gaussian state and follows the Gaussian distribution with [p.d.f.](#) f_X , it is continuous, as it is a probability density function. For considering [CV](#) signal processing, it modified discrete [p.m.f.](#) f_{Z_1} of Poisson quantum noise to a continuous distribution and plugged it with [p.d.f.](#) f_{Z_2} of classical Gaussian noise, which is also continuous; hence, the final convolution product f_Z is a continuous function. So both f_X and f_Z are continuous, and X and Z are independent of each other, having relation $Y = X + Z$. Therefore, the [p.d.f.](#) f_Y of Y can be written as the convolution of f_X and f_Z as follows:

$$f_Y(y) := \int_{-\infty}^{\infty} f_X(x) f_Z(y - x) dx \quad (3.13)$$

where the domain of X is given by $\mathcal{D}_X = (-\infty, \infty)$. Consider a range for qubits along a single direction on the surface of the Bloch sphere, such as $\mathcal{D}_X = [0, 2\pi]$ in some restriction. This topic is discussed in detail in the appendix. This is the same as the range $\mathcal{D}_X = [-\pi, \pi]$, which also represents a single complete rotation on the sphere's surface. However, this study extends this idea by considering this range as multiple rotations along the great circle; pictorially, it looks like a spiral or a Helix structure. For the theoretical range of the qubit on the Bloch sphere along a circular direction, we can use $\mathcal{D}_X = [-\pi, \pi]$ to represent a single rotation or $\mathcal{D}_X = (-\infty, \infty)$ for multiple rotations ($[-\pi, \pi] \times \text{number of rotations}$).

From using the expressions of (3.10) and (3.12) in (3.13), we have

$$\begin{aligned}
f_Y(y) &= \int_{-\infty}^{\infty} f_X(x) f_Z(y-x) dx \\
&= \int_{-\infty}^{\infty} \left(\frac{1}{\sigma_X \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{x-\mu_X}{\sigma_X} \right)^2} \right) \left(\sum_{k=0}^{\infty} \frac{e^{-\lambda} \lambda^k}{k!} \frac{1}{\sigma_{Z_2} \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{y-x-k-\mu_{Z_2}}{\sigma_{Z_2}} \right)^2} \right) dx \\
&= \int_{-\infty}^{\infty} \sum_{k=0}^{\infty} \frac{e^{-\lambda} \lambda^k}{k!} \left(\frac{1}{\sigma_X \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{x-\mu_X}{\sigma_X} \right)^2} \right) \left(\frac{1}{\sigma_{Z_2} \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{y-x-k-\mu_{Z_2}}{\sigma_{Z_2}} \right)^2} \right) dx
\end{aligned} \tag{3.14}$$

Let

$$f(x) := \frac{1}{\sigma_X \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{x-\mu_X}{\sigma_X} \right)^2} \tag{3.15}$$

and

$$g(x) = \frac{1}{\sigma_{Z_2} \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{y-x-k-\mu_{Z_2}}{\sigma_{Z_2}} \right)^2} = \frac{1}{\sigma_{Z_2} \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{x-(y-k-\mu_{Z_2})}{\sigma_{Z_2}} \right)^2} \tag{3.16}$$

Define $\mu_f := \mu_X$, $\sigma_f := \sigma_X$, $\mu_g := y-k-\mu_{Z_2}$, and $\sigma_g := \sigma_{Z_2}$. From (3.15) and (3.16) we can write

$$f(x) := \frac{1}{\sigma_f \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{x-\mu_f}{\sigma_f} \right)^2} \tag{3.17}$$

and

$$g(x) := \frac{1}{\sigma_g \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{x-\mu_g}{\sigma_g} \right)^2} \tag{3.18}$$

From (3.17) and (3.18) the product of functions f and g can be written as

$$f(x)g(x) = \frac{1}{2\pi\sigma_f\sigma_g} e^{-\left[\frac{(x-\mu_f)^2}{2\sigma_f^2} + \frac{(x-\mu_g)^2}{2\sigma_g^2} \right]} \tag{3.19}$$

Examine the term in the exponent in (3.19), Expanding the terms in quadratic, by collecting the terms in the power of x and dividing by the coefficient of x^2 gives,

$$\begin{aligned}
\beta &:= \frac{(x-\mu_f)^2}{2\sigma_f^2} + \frac{(x-\mu_g)^2}{2\sigma_g^2} \\
&= \frac{(\sigma_f^2 + \sigma_g^2)x^2 - 2(\mu_f\sigma_g^2 + \mu_g\sigma_f^2)x + \mu_f^2\sigma_g^2 + \mu_g^2\sigma_f^2}{2\sigma_f^2\sigma_g^2} \\
&= \frac{x^2 - 2\frac{\mu_f\sigma_g^2 + \mu_g\sigma_f^2}{\sigma_f^2 + \sigma_g^2}x + \frac{\mu_f^2\sigma_g^2 + \mu_g^2\sigma_f^2}{\sigma_f^2 + \sigma_g^2}}{\frac{2\sigma_f^2\sigma_g^2}{\sigma_f^2 + \sigma_g^2}}
\end{aligned} \tag{3.20}$$

Again, this is quadratic x ; therefore, (3.19) is a Gaussian function. Let us consider,

$$\epsilon = \frac{\left(\frac{\mu_f \sigma_g^2 + \mu_g \sigma_f^2}{\sigma_f^2 + \sigma_g^2}\right)^2 - \left(\frac{\mu_f \sigma_g^2 + \mu_g \sigma_f^2}{\sigma_f^2 + \sigma_g^2}\right)^2}{\frac{2\sigma_f^2 \sigma_g^2}{\sigma_f^2 + \sigma_g^2}} = 0 \quad (3.21)$$

Adding this term to β gives,

$$\begin{aligned} \beta &= \frac{x^2 - 2x \frac{\mu_f \sigma_g^2 + \mu_g \sigma_f^2}{\sigma_f^2 + \sigma_g^2} + \left(\frac{\mu_f \sigma_g^2 + \mu_g \sigma_f^2}{\sigma_f^2 + \sigma_g^2}\right)^2}{\frac{2\sigma_f^2 \sigma_g^2}{\sigma_f^2 + \sigma_g^2}} + \frac{\left(\frac{\mu_f^2 \sigma_g^2 + \mu_g^2 \sigma_f^2}{\sigma_f^2 + \sigma_g^2}\right) - \left(\frac{\mu_f \sigma_g^2 + \mu_g \sigma_f^2}{\sigma_f^2 + \sigma_g^2}\right)^2}{\frac{2\sigma_f^2 \sigma_g^2}{\sigma_f^2 + \sigma_g^2}} \\ &= \frac{\left(x - \frac{\mu_f \sigma_g^2 + \mu_g \sigma_f^2}{\sigma_f^2 + \sigma_g^2}\right)^2}{\frac{2\sigma_f^2 \sigma_g^2}{\sigma_f^2 + \sigma_g^2}} + \frac{(\mu_f - \mu_g)^2}{2(\sigma_f^2 + \sigma_g^2)} = \frac{(x - \mu_{fg})^2}{2\sigma_{fg}^2} + \frac{(\mu_f - \mu_g)^2}{2(\sigma_f^2 + \sigma_g^2)} \end{aligned} \quad (3.22)$$

where

$$\mu_{fg} = \frac{\mu_f \sigma_g^2 + \mu_g \sigma_f^2}{\sigma_f^2 + \sigma_g^2}, \sigma_{fg} = \sqrt{\frac{\sigma_f^2 \sigma_g^2}{\sigma_f^2 + \sigma_g^2}}. \quad (3.23)$$

Substituting (3.22) in (3.19) we get,

$$f(x)g(x) = \frac{1}{2\pi\sigma_f\sigma_g} e^{\left[-\frac{(x-\mu_{fg})^2}{2\sigma_{fg}^2}\right]} e^{\left[-\frac{(\mu_f-\mu_g)^2}{2(\sigma_f^2+\sigma_g^2)}\right]}. \quad (3.24)$$

Multiplying by $\frac{\sigma_{fg}}{\sigma_{fg}}$ and rearranging gives,

$$f(x)g(x) = \frac{1}{\sqrt{2\pi}\sigma_{fg}} e^{\left[-\frac{(x-\mu_{fg})^2}{2\sigma_{fg}^2}\right]} \frac{1}{\sqrt{2\pi(\sigma_f^2 + \sigma_g^2)}} e^{\left[-\frac{(\mu_f-\mu_g)^2}{2(\sigma_f^2+\sigma_g^2)}\right]} \quad (3.25)$$

Finally from (3.19) we have,

$$f(x)g(x) = \frac{S_{fg}}{\sqrt{2\pi}\sigma_{fg}} e^{\left[-\frac{(x-\mu_{fg})^2}{2\sigma_{fg}^2}\right]} \quad (3.26)$$

where

$$S_{fg} = \frac{1}{\sqrt{2\pi(\sigma_f^2 + \sigma_g^2)}} e^{\left[-\frac{(\mu_f-\mu_g)^2}{2(\sigma_f^2+\sigma_g^2)}\right]}, \mu_{fg} = \frac{\mu_f \sigma_g^2 + \mu_g \sigma_f^2}{\sigma_f^2 + \sigma_g^2}, \sigma_{fg} = \sqrt{\frac{\sigma_f^2 \sigma_g^2}{\sigma_f^2 + \sigma_g^2}}. \quad (3.27)$$

and the scaling factor S_{fg} is itself a Gaussian function on both μ_f and μ_g with Gaussian RMS width $\sqrt{(\sigma_f^2 + \sigma_g^2)}$. Note that the product fg is a Gaussian function. However, μ_{fg} and σ_{fg} need not be mean and s.d. of the distribution fg . The μ_f ($:= \mu_X$), σ_f ($:= \sigma_X$) and σ_g ($:= \sigma_{Z_2}$) are free from y

while only $\mu_g := y - k - \mu_{Z_2}$ depends on y . In the integrand below, it is necessary to be careful that both S_{fg} and μ_{fg} contain y and k . Using these expressions (3.17), (3.18), and (3.19) in (3.10) gives this result,

$$\begin{aligned} f_Y(y) &= \int_{-\infty}^{\infty} \sum_{k=0}^{\infty} \frac{e^{-\lambda} \lambda^k}{k!} \left(\frac{1}{\sigma_f \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{x - \mu_f}{\sigma_f} \right)^2} \right) \left(\frac{1}{\sigma_g \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{x - \mu_g}{\sigma_g} \right)^2} \right) dx \\ &= \int_{-\infty}^{\infty} \sum_{k=0}^{\infty} \frac{e^{-\lambda} \lambda^k}{k!} \frac{S_{fg}}{\sigma_{fg} \sqrt{2\pi}} e^{\left[-\frac{(x - \mu_{fg})^2}{2\sigma_{fg}^2} \right]} dx \end{aligned} \quad (3.28)$$

The expression of p.d.f. $f_Y(y)$ of the received signal Y can be further simplified to

$$\begin{aligned} f_Y(y) &= \int_{-\infty}^{\infty} \sum_{k=0}^{\infty} \frac{e^{-\lambda} \lambda^k}{k!} \frac{1}{\sigma_{fg} \sqrt{2\pi}} S_{fg} e^{\left[-\frac{1}{2\sigma_{fg}^2} \left(x - \frac{\mu_f \sigma_g^2 + \mu_g \sigma_f^2}{\sigma_f^2 + \sigma_g^2} \right)^2 \right]} dx \\ &= \int_{-\infty}^{\infty} \sum_{k=0}^{\infty} \frac{e^{-\lambda} \lambda^k}{k!} \frac{1}{\sigma_{fg} \sqrt{2\pi}} \frac{1}{\sqrt{2\pi(\sigma_f^2 + \sigma_g^2)}} e^{\left[-\frac{(\mu_f - \mu_g)^2}{2(\sigma_f^2 + \sigma_g^2)} \right]} \\ &\quad e^{\left[-\frac{1}{2\sigma_{fg}^2} \left(x - \frac{\mu_f \sigma_g^2 + (y - k - \mu_{Z_2}) \sigma_f^2}{\sigma_f^2 + \sigma_g^2} \right)^2 \right]} dx \\ &= \int_{-\infty}^{\infty} \sum_{k=0}^{\infty} \frac{e^{-\lambda} \lambda^k}{k!} \frac{1}{\sigma_{fg} \sqrt{2\pi}} \frac{1}{\sqrt{2\pi(\sigma_f^2 + \sigma_g^2)}} e^{\left[-\frac{(\mu_f - (y - k - \mu_{Z_2}))^2}{2(\sigma_f^2 + \sigma_g^2)} \right]} \\ &\quad e^{\left[-\frac{1}{2\sigma_{fg}^2} \left(x - \frac{\mu_f \sigma_g^2 + (y - k - \mu_{Z_2}) \sigma_f^2}{\sigma_f^2 + \sigma_g^2} \right)^2 \right]} dx \end{aligned} \quad (3.29)$$

Our target is to interchange the $\sum$ and $\int$. From (3.28) consider,

$$f_k(x) := \frac{e^{-\lambda} \lambda^k}{k!} \frac{S_{fg}}{\sigma_{fg} \sqrt{2\pi}} e^{\left[-\frac{(x - \mu_{fg})^2}{2\sigma_{fg}^2} \right]} \quad (3.30)$$

Therefore, we have,

$$f_Y(y) = \int_{-\infty}^{\infty} \sum_{k=0}^{\infty} f_k(x) dx \quad (3.31)$$

This is a special case of Fubini/Tonelli's theorem, where the measures are countable measures s on $\mathbb{N}$ and the Lebesgue measure on $\mathbb{R}$ (or, $[0, \infty)$). In a particular case, $\int_{-\infty}^{\infty} \sum_{k=0}^{\infty} f_k(x) dx$ with $f_k(x)$ being continuous functions $\forall k \in \{0, 1, 2, \dots\}$. In deriving the expression for f_Y , it will be easier if one

can interchange the integral and the summation in the above case. Another fundamental question is to determine if there are any necessary and sufficient conditions that allow swapping the integral and summation for the above expression. In particular, Tonelli's theorem says if $f_k(x) \geq 0 \forall k, x$ then

$$\int \sum f_k(x) dx = \sum \int f_k(x) dx \quad (3.32)$$

Without any further conditions needed. The monotone convergence theorem can be used to prove this. Fubini's theorem says that for a general function $f_k(\cdot)$, if $\int \sum |f_k(x)| < \infty$ or $\sum \int |f_k(x)| < \infty$ (by Tonelli the two conditions are equivalent), then $\int \sum f_k(x) = \sum \int f_k(x)$. The dominated convergence theorem can be used to prove this. We want to use the condition of Tonelli's theorem in (3.32). Hence, we only need to check if

$f_k(x) \geq 0 \quad \forall k, x$. We have $f_k(x) = \frac{e^{-\lambda} \lambda^k}{k!} \frac{S_{fg}}{\sigma_{fg} \sqrt{2\pi}} e^{\left[-\frac{(x-\mu_{fg})^2}{2\sigma_{fg}^2} \right]}$. The exponential function is always positive, $\therefore e^{\left[-\frac{(x-\mu_{fg})^2}{2\sigma_{fg}^2} \right]} \geq 0 \quad \forall x, k$. For the

part $\sigma_{fg} = \sqrt{\frac{\sigma_f^2 \sigma_g^2}{\sigma_f^2 + \sigma_g^2}}$, $\sigma_f (:= \sigma_X)$ and $\sigma_g (:= \sigma_{N_2})$ are s.d. of distributions X and N_2 respectively and $\therefore \sigma_f \geq 0$ and $\sigma_g \geq 0 \implies \sigma_{fg} \geq 0$. Similarly,

for the part $S_{fg} = \frac{1}{\sqrt{2\pi(\sigma_f^2 + \sigma_g^2)}} e^{\left[-\frac{(\mu_f - \mu_g)^2}{2(\sigma_f^2 + \sigma_g^2)} \right]}$, the expression $\frac{1}{\sqrt{2\pi(\sigma_f^2 + \sigma_g^2)}} \geq 0$

as $\sigma_f \geq 0$ and $\sigma_g \geq 0$ and the part $e^{\left[-\frac{(\mu_f - \mu_g)^2}{2(\sigma_f^2 + \sigma_g^2)} \right]} \geq 0$, being an exponential function. $\therefore S_{fg} \geq 0$. Let's define

$$A := \frac{e^{-\lambda} \lambda^k}{k!}, \quad B := \frac{S_{fg}}{\sqrt{2\pi} \sigma_{fg}}, \quad C := e^{\left[-\frac{(\mu_f - \mu_g)^2}{2(\sigma_f^2 + \sigma_g^2)} \right]} \quad (3.33)$$

Note that A and B do not contain x while only C contains x . Since $\lambda \geq 0, k \in \{0, 1, 2, \dots\}$,

$$\begin{aligned} A = \frac{e^{-\lambda} \lambda^k}{k!} \geq 0 \quad \forall k, \quad B = \frac{S_{fg}}{\sqrt{2\pi} \sigma_{fg}} \geq 0 \quad \forall k, \quad C = e^{\left[-\frac{(\mu_f - \mu_g)^2}{2(\sigma_f^2 + \sigma_g^2)} \right]} \geq 0 \quad \forall x, k \\ \implies f_k(x) = A \cdot B \cdot C \geq 0 \quad \forall x, k \end{aligned} \quad (3.34)$$

Hence, from Tonelli's theorem in (3.32), it can be concluded that the interchange of $\sum$ and $\int$ in (3.28) is possible. Hence, from (3.28), we can write,

$$f_Y(y) = \sum_{k=0}^{\infty} \frac{e^{-\lambda} \lambda^k}{k!} \frac{S_{fg}}{\sigma_{fg} \sqrt{2\pi}} \int_{-\infty}^{\infty} e^{\left[-\frac{(x-\mu_{fg})^2}{2\sigma_{fg}^2} \right]} dx \quad (3.35)$$

Remember both S_{fg} and μ_{fg} contain y and k . Now, for the part

$$\begin{aligned} \int_{-\infty}^{\infty} e^{-\left(\frac{x-\mu_{fg}}{\sqrt{2}\sigma_{fg}}\right)^2} dx &= \int_{-\infty}^{\infty} e^{-t^2} \sqrt{2}\sigma_{fg} dt \\ &= \sqrt{2}\sigma_{fg} \int_{-\infty}^{\infty} e^{-t^2} dt = \sqrt{2}\sigma_{fg}\sqrt{\pi} = \sqrt{2\pi}\sigma_{fg} \end{aligned} \quad (3.36)$$

where $t = \frac{x-\mu_{fg}}{\sqrt{2}\sigma_{fg}}$, $\sqrt{2}\sigma_{fg}t + \mu_{fg} = x$, $\sqrt{2}\sigma_{fg}dt = dx$ and $\int_{-\infty}^{\infty} e^{-t^2} dt = \sqrt{\pi}$. Finally, putting expression (8.12) in (3.35) we get,

$$\begin{aligned} f_Y(y) &= \sum_{k=0}^{\infty} \frac{e^{-\lambda}\lambda^k}{k!} \frac{S_{fg}}{\sigma_{fg}\sqrt{2\pi}} \sqrt{2\pi}\sigma_{fg} = \sum_{k=0}^{\infty} \frac{e^{-\lambda}\lambda^k}{k!} S_{fg} \\ &= \sum_{k=0}^{\infty} \frac{e^{-\lambda}\lambda^k}{k!} \frac{1}{\sqrt{2\pi(\sigma_f^2 + \sigma_g^2)}} e^{-\frac{1}{2(\sigma_f^2 + \sigma_g^2)}(\mu_f - \mu_g)^2} \\ &= \sum_{k=0}^{\infty} \frac{e^{-\lambda}\lambda^k}{k!} \frac{1}{\sqrt{2\pi(\sigma_X^2 + \sigma_{Z_2}^2)}} e^{-\frac{(y-k-\mu_X-\mu_{Z_2})^2}{2(\sigma_X^2 + \sigma_{Z_2}^2)}} \end{aligned} \quad (3.37)$$

In order to compare the p.d.f. of noise Z in 3.10 and p.d.f. of received signal Y in 3.37, it is worth noting that mathematically, both p.d.f.s have similar types of expression; moreover, one is a scaled version of the other. Finally, the differential entropy of the received signal Y is defined by

$$h(Y) = - \int_{\chi_Y} f_Y(y) \log f_Y(y) dy, \quad (3.38)$$

where χ_Y is the support of f_Y .

The following section shows the analytical derivations of the differential entropies for quantum noise and received signals. This leads to a closed-form solution of the mutual information, and hence, an analytical expression for the capacity. Meanwhile, the upper and lower bounds of the entropies of the received signal and joint quantum noise have been derived by focusing on the GMM for the noise and the received signal.

3.6 Gaussian Mixture Model

GMMs are weighted sums of Gaussian components that approximate arbitrary probability densities [130]. GMM parameters are estimated from data using EM or MAP [129]. GMMs model non-Gaussian uncertainties better than single Gaussians. With enough components, they can approximate any distribution [128]. Differential entropy of GMMs lacks a closed form, so bounds are proposed. A novel approximation calculates entropy bounds represented by Gaussian components [201]. Overall, GMMs flexibly model complex multivariate densities using Gaussian components. A GMM is a

weighted sum of M component Gaussian densities as given by the equation,

$$f(\mathbf{x}) = \sum_{i=1}^L w_i \mathcal{N}(\mathbf{x}, \mu_i, \mathbf{C}_i), \quad (3.39)$$

where w_i are non-negative weighting coefficients with $\sum_i w_i = 1$ and $\mathcal{N}(\mathbf{x}, \mu, \mathbf{C})$ is a Gaussian density mean vector μ , and covariance matrix $\mathbf{C}$.

For a continuous-valued random vector $\bar{x} \in \mathcal{R}^N$ with p.d.f. $f(\bar{x})$, the differential entropy is defined as

$$H(\bar{x}) = E[-\log f(\bar{x})] = - \int_{\mathcal{R}^N} f(\bar{x}) \log f(\bar{x}) d\bar{x}. \quad (3.40)$$

The entropy of Gaussian mixtures can not be calculated in closed form due to the logarithm of a sum of exponential functions. It can be visualized from the expression below

$$H_Z = - \int \sum_i w_i \frac{1}{\sigma \sqrt{2\pi}} e^{-\frac{1}{2}(x-\mu)^T C(x-\mu)} \left(\log_2 \sum_i w_i \frac{1}{\sigma \sqrt{2\pi}} e^{-\frac{1}{2}(x-\mu)^T C(x-\mu)} \right) dz \quad (3.41)$$

The exceptional case: For the special case of a single density, where entropy is

$$H(\bar{x}) = \frac{1}{2} \log_2 \left((2\pi e)^N \left| \sum \right| \right) \quad (3.42)$$

an approximate solution of (3.40). The expression (3.42) is an upper bound for all Gaussian mixture random vectors with some covariance matrix $\sum$ as in (3.42).

Independent of the entropy approximation method used, it is generally tricky or even impossible to quantify the deviation between the actual entropy value and its approximation. Providing a close lower and upper bound of the entropy value of a Gaussian mixture random vector makes it possible to decide whether the approximation is meaningful. Furthermore, as we will show, both bounds can be calculated in closed form. Thus, the bounds themselves can be used to efficiently approximate the actual entropy value [130].

Theorem 1 : A lower bound $H_L(\bar{x})$ of (3.40) is given by

$$H_L(\bar{x}) = - \sum_{i=0}^L w_i \log_2 \left(\sum_{j=0}^L w_j m_{i,j} \right) \quad (3.43)$$

with $m_{i,j} = \mathcal{N}(\bar{\mu}_i; \bar{\mu}_j, C_i + C_j)$ where μ_i is the mean vector and C_i is the covariance matrix of the corresponding component of Gaussian mixture $f(\bar{x})$.

Theorem 2 : An upper bound $H_U(\bar{x})$ of (3.40) is given by

$$H_U(\bar{x}) = \sum_{i=0}^L w_i \log_2 \left(-\log_2 w_i + \frac{1}{2} \log_2 \left((2\pi e)^N \left| C_i \right| \right) \right) \quad (3.44)$$

3.6.1 Identifying Noise Model as GMM

Consider the p.d.f. of joint noise Z in (3.10),

$$f_Z(z) = \sum_{i=0}^{\infty} \frac{e^{-\lambda} \lambda^i}{i!} \frac{1}{\sigma_{Z_2} \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{z-i-\mu_{Z_2}}{\sigma_{Z_2}} \right)^2} = \sum_{i=0}^{\infty} u_i \mathcal{N}(z, \mu_i^{(z)}, \sigma_i^{(z)^2}) \quad (3.45)$$

where $u_i = \frac{e^{-\lambda} \lambda^i}{i!}$, $\sum_{i=0}^{\infty} u_i = 1$, $u_i \geq 0 \quad \forall i$ and $\mathcal{N}(z, \mu_i^{(z)}, \sigma_i^{(z)^2})$ is Gaussian density in dummy variable z , mean $\mu_i^{(z)} = \mu_{Z_2} + i$, and $\sigma_i^{(z)^2} = \sigma_{Z_2}^2$ with s.d. $\sigma_i^{(z)}$ and variance $\sigma_i^{(z)^2}$. In (3.45), the approximation of $f_Z(z)$ is taken as

$$f_Z(z) = \sum_{i=0}^R \frac{e^{-\lambda} \lambda^i}{i!} \frac{1}{\sigma_{Z_2} \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{z-i-\mu_{Z_2}}{\sigma_{Z_2}} \right)^2} = \sum_{i=0}^R u_i \mathcal{N}(z, \mu_i^{(z)}, \sigma_i^{(z)^2}) \quad (3.46)$$

This is the Gaussian mixture in scalar variable z , the coefficient $u_i \geq 0 \quad \forall i$ and $\sum_{i=0}^R u_i \approx 1$ for large R . Corresponding Gaussian mixture in random vector $\bar{z} \in \mathbb{R}^M$ is

$$f_Z(\bar{z}) = \sum_{i=0}^R u_i \mathcal{N}(\bar{z}, \bar{\mu}_i^{(\bar{z})}, \sum_i^{(z)}) \quad (3.47)$$

where $\bar{z}$ is the random vector in $\mathbb{R}^M$, $\bar{\mu}_i^{(\bar{z})}$ is the mean vector, and $\sum_i^{(z)}$ is the covariance matrix of the corresponding Gaussian density $\mathcal{N}$.

3.6.2 Identifying Received Signal Model as GMM

Consider the p.d.f. of the received signal in (3.37) given by,

$$\begin{aligned} f_Y(y) &= \sum_{i=0}^{\infty} \frac{e^{-\lambda} \lambda^i}{i!} \frac{1}{\sqrt{2\pi(\sigma_X^2 + \sigma_{Z_2}^2)}} e^{-\frac{(y-i-\mu_X-\mu_{Z_2})^2}{2(\sigma_X^2 + \sigma_{Z_2}^2)}} \\ &= \sum_{i=0}^{\infty} \frac{e^{-\lambda} \lambda^i}{i!} \frac{1}{\sqrt{2\pi(\sigma_X^2 + \sigma_{Z_2}^2)}} e^{-\frac{1}{2} \left(\frac{y-(i+\mu_X+\mu_{Z_2})}{\sqrt{(\sigma_X^2 + \sigma_{Z_2}^2)}} \right)^2} \\ &= \sum_{i=0}^{\infty} v_i \mathcal{N}(y, \mu_i^{(y)}, \sigma_i^{(y)^2}) \end{aligned} \quad (3.48)$$

where $v_i = \frac{e^{-\lambda} \lambda^i}{i!}$, $\sum_{i=0}^{\infty} v_i = 1$, $v_i \geq 0 \quad \forall i$ and $\mathcal{N}(y, \mu_i^{(y)}, \sigma_i^{(y)^2})$ is Gaussian density in dummy variable y , mean $\mu_i^{(y)} = \mu_X + \mu_{Z_2} + i$, and s.d. $\sigma_i^{(y)} = \sqrt{(\sigma_X^2 + \sigma_{Z_2}^2)}$ with variance $\sigma_i^{(y)^2}$

In practical scenarios simulated over MATLAB, the p.d.f. of hybrid noise in (3.10) has been approximated as $\tilde{f}(z)$ in (3.46) and has been used to

formulate $f(y)$ which is given by,

$$\tilde{f}_Y(y) = \sum_{i=0}^R \frac{e^{-\lambda} \lambda^i}{i!} \frac{1}{\sqrt{2\pi(\sigma_X^2 + \sigma_{Z_2}^2)}} e^{-\frac{(y-i-\mu_X-\mu_{Z_2})^2}{2(\sigma_X^2 + \sigma_{Z_2}^2)}} = \sum_{i=0}^R v_i \mathcal{N}\left(y, \mu_i^{(y)}, \sigma_i^{(y)2}\right) \quad (3.49)$$

This is a Gaussian mixture in scalar variable y , and $v_i = \frac{e^{-\lambda} \lambda^i}{i!}$, $v_i \geq 0 \quad \forall i$, and $\sum_{i=0}^R v_i \approx 1$ for large R . Corresponding Gaussian mixture in random vector $\bar{y} \in \mathbb{R}^M$ is

$$f_Y(\bar{y}) = \sum_{i=0}^R v_i \mathcal{N}\left(\bar{y}, \bar{\mu}_i^{(y)}, \sum_i^{(y)}\right) \quad (3.50)$$

where $\bar{y}$ is the random vector in $\mathbb{R}^M$, $\bar{\mu}_i^{(y)}$ is the mean vector, and $\sum_i^{(y)}$ is the covariance matrix of the corresponding Gaussian density $\mathcal{N}$.

Since f_Z and f_Y are both Gaussian mixture densities, the closed-form solution of the corresponding entropies H_Z and H_Y of the noise and the received signal can not be calculated due to the logarithm of the sum and exponential function [130]. However, Theorems 1 and 2 provide the lower and the upper bounds for each entropy H_Z and H_Y . Let us call the upper and lower bounds of H_Z by U_Z and L_Z , and the upper and lower bounds of H_Y by U_Y and L_Y , respectively. That is

$$L_Z \leq H_Z \leq U_Z \quad (3.51)$$

and

$$L_Y \leq H_Y \leq U_Y \quad (3.52)$$

3.7 Capacity for the Gaussian Input Quantum Channel

In [25], the mutual information $I(X; Y)$ between transmitted signal X and received signal Y is defined as $I(X; Y) = H_X + H_Y - H(X, Y)$ and applying the chain rule for continuous variables, we have, $H(X, Y) = H(Y|X) + H_X$. Therefore, $I(X; Y) = H_Y - H(Y|X) = H_Y - H(X + Z|X) = H_Y - H(Z|X) = H_Y - H(Z) = H_Y - H_Z$ as transmitted signal X and noise Z are independent. We rename $H(Z)$ as H_Z for notational ease. Using (3.51) we will get,

$$-L_Z \geq -H_Z \geq -U_Z \quad (3.53)$$

$$H_Y - L_Z \geq H_Y - H_Z \geq H_Y - U_Z \quad (3.54)$$

$$U_Y - L_Z \geq H_Y - L_Z \geq H_Y - H_Z = I(X; Y) \quad (3.55)$$

Therefore,

$$I(X; Y) \leq U_Y - L_Z \quad (3.56)$$

Hence,

$$C = \max_{f(x)} I(X; Y) \leq U_Y - L_Z \quad (3.57)$$

From Theorem 1, let us calculate L_Z , the lower bound for H_Z , as follows:

$$L_Z = - \sum_{i=0}^R u_i \log_2 \left(\sum_{j=0}^R u_j \mathcal{N} \left(\bar{\mu}_i^{(z)}; \bar{\mu}_j^{(z)}, \sum_i^{(z)} + \sum_j^{(z)} \right) \right) \quad (3.58)$$

From Theorem 2, similarly we calculate U_Y , the upper bound for H_Y , as follows:

$$U_Y = \sum_{i=0}^R v_i \log_2 \left(-\log_2 v_i + \frac{1}{2} \log_2 \left((2\pi e)^M \left| \sum_i^{(y)} \right| \right) \right) \quad (3.59)$$

where $u_i = v_i = \frac{e^{-\lambda \lambda^i}}{i!} \forall i = 0(1)R$. From (3.56), using (3.58) and (3.59), we have,

$$\begin{aligned} U_Y - L_Z = & \sum_{i=0}^R \frac{e^{-\lambda \lambda^i}}{i!} \left(-\log_2 \left(\frac{e^{-\lambda \lambda^i}}{i!} \right) + \frac{1}{2} \log_2 \left((2\pi e)^M \left| \sum_i^{(y)} \right| \right) \right. \\ & \left. + \log_2 \left(\sum_{j=0}^R \frac{e^{-\lambda \lambda^j}}{j!} \mathcal{N} \left(\bar{\mu}_i^{(z)}; \bar{\mu}_j^{(z)}, \sum_i^{(z)} + \sum_j^{(z)} \right) \right) \right) \end{aligned} \quad (3.60)$$

From (7.22) and (7.25), the channel capacity would be,

$$\begin{aligned} C = & \sum_{i=0}^R \frac{e^{-\lambda \lambda^i}}{i!} \left(-\log_2 \left(\frac{e^{-\lambda \lambda^i}}{i!} \right) + \frac{1}{2} \log_2 \left((2\pi e)^M \left| \sum_i^{(y)} \right| \right) \right. \\ & \left. + \log_2 \left(\sum_{j=0}^R \frac{e^{-\lambda \lambda^j}}{j!} \mathcal{N} \left(\bar{\mu}_i^{(z)}; \bar{\mu}_j^{(z)}, \sum_i^{(z)} + \sum_j^{(z)} \right) \right) \right) \end{aligned} \quad (3.61)$$

This is the expression for the quantum channel capacity when the noise Z and the received signal Y are random vectors of dimension M . In scalar analogy, that is, when the noise Z and the received signal Y are random variables with p.d.f.s (3.46) and (3.49) respectively, the expression of capacity reduces to,

$$\begin{aligned} C = & \sum_{i=0}^R \frac{e^{-\lambda \lambda^i}}{i!} \left(-\log_2 \left(\frac{e^{-\lambda \lambda^i}}{i!} \right) + \frac{1}{2} \log_2 \left(2\pi e \sigma_i^{(y)} \right) \right. \\ & \left. + \log_2 \left(\sum_{j=0}^R \frac{e^{-\lambda \lambda^j}}{j!} \mathcal{N} \left(\mu_i^{(z)}; \mu_j^{(z)}, \sigma_i^{(z)^2} + \sigma_j^{(z)^2} \right) \right) \right) \end{aligned} \quad (3.62)$$

by putting $M = 1$, and replacing $\left| \sum_i^{(y)} \right|$ by $\sigma_i^{(y)}$, $\bar{\mu}_i^{(z)}$ by $\mu_i^{(z)}$, $\bar{\mu}_j^{(z)}$ by $\mu_j^{(z)}$, $\sum_i^{(z)}$ by $\sigma_i^{(z)^2}$ and $\sum_j^{(z)}$ by $\sigma_j^{(z)^2}$, where each vector is replaced by its scalar

analogue. Again $\mu_i^{(z)} = \mu_{Z_2} + i \forall i$, $\sigma_i^{(z)^2} = \sigma_{Z_2}^2 \forall i$, and $\sigma_i^{(y)^2} = \sigma_X^2 + \sigma_{Z_2}^2 \forall i$. Therefore, the capacity is given by,

$$\begin{aligned}
C &= \sum_{i=0}^R \frac{e^{-\lambda} \lambda^i}{i!} \left(-\log_2 \left(\frac{e^{-\lambda} \lambda^i}{i!} \right) + \frac{1}{2} \log_2 \left(2\pi e (\sigma_X^2 + \sigma_{Z_2}^2) \right) \right. \\
&\quad \left. + \log_2 \left(\sum_{j=0}^R \frac{e^{-\lambda} \lambda^j}{j!} \mathcal{N}(\mu_{Z_2} + i; \mu_{Z_2} + j, 2\sigma_{Z_2}^2) \right) \right) \\
&= \sum_{i=0}^R \frac{e^{-\lambda} \lambda^i}{i!} \left(-\log_2 \left(\frac{e^{-\lambda} \lambda^i}{i!} \right) + \frac{1}{2} \log_2 \left(2\pi e (\sigma_X^2 + \sigma_{Z_2}^2) \right) \right. \\
&\quad \left. + \log_2 \left(\sum_{j=0}^R \frac{e^{-\lambda} \lambda^j}{j!} \frac{1}{\sqrt{2\sigma_{Z_2}} \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{i-j}{\sqrt{2}\sigma_{Z_2}} \right)^2} \right) \right) \tag{3.63}
\end{aligned}$$

where $\mathcal{N}(\mu_{Z_2} + i; \mu_{Z_2} + j, 2\sigma_{Z_2}^2) = \frac{1}{\sqrt{2\sigma_{Z_2}} \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{\mu_{Z_2} + i - j - \mu_{Z_2}}{\sqrt{2}\sigma_{Z_2}} \right)^2}$.

3.8 Quantum Signal Model for Non-Gaussian Input

A Gaussian quantum channel does not necessarily imply that the input states are Gaussian [198], [10]. Considering this fact, we consider an arbitrary distribution for the transmitted signal. Hence, the input signal is approximated by its mean and s.d. $E[X]$ and σ_X , respectively. To invoke the role of the mean and s.d. of the input state's distribution in the actual scenario, the modified channel equation is considered as follows,

$$Y' = \mu_X + \sigma_X Z \tag{3.64}$$

where Y' and Z are the channel's received signal and HQN.

Mathematically, the sample space of X can be written as Sp_X and the random variable takes values $X = x_1, x_2, x_3, \dots$. Since an arbitrary distribution of the transmitted signal X has been considered, we approximate the transmit signal in terms of its point estimate (or mean), μ_X . But to replace the arbitrary input distribution f_X by its mean value is insufficient, as it will not specify the distribution. However, by fixing the mean and standard deviation, one can specify the unknown distribution [202] well. So we replaced the arbitrary input distribution by the mean $E[X]$ and s.d. σ_X . It is a useful method when considering an unknown distribution for calculations. However, replacing f_X by $E[X]$ is not meaningful as $E[X]$ ranges from sample space of X , which is $-(\infty, \infty)$, while the mean value of f_X comes from the range of f_X which is $[0, 1]$ as f_X is a p.d.f.. A solution to this problem could be replacing the sample space of the input signal by its expected value, that is, $x = E[X] = \mu_X, \forall x \in Sp_X$. This approximation

has been made to get a mathematical expression for the output signal and its visualization. Hence, starting with our channel equation,

$$Y' = \mu_X + \sigma_X Z \quad (3.65)$$

and from (3.10) we have the p.d.f. of the hybrid quantum-classical noise

$$f_Z(z) = \sum_{i=0}^{\infty} \frac{e^{-\lambda} \lambda^i}{i!} \frac{1}{\sigma_{Z_2} \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{z - i - \mu_{Z_2}}{\sigma_{Z_2}} \right)^2} \quad (3.66)$$

Theorem on Change of Variables: Given the probability density function, $f_Z(z)$, for z , p.d.f., $f_{Y'}(y')$ for $Y' = aZ + b$, ($a \neq 0$), is

$$f_{Y'}(y') = \frac{1}{|a|} f_Z\left(z = \frac{y' - b}{a}\right) \quad (3.67)$$

Putting $a = \mu_X$ and $b = \sigma_X$, we have the received signal model as,

$$\begin{aligned} f_{Y'}(y') &= \frac{1}{\sigma_X} f_Z\left(z = \frac{y' - \mu_X}{\sigma_X}\right) = \frac{1}{\sigma_X} \sum_{i=0}^{\infty} \frac{e^{-\lambda} \lambda^i}{i!} \frac{1}{\sigma_{Z_2} \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{\frac{y' - \mu_X}{\sigma_X} - i - \mu_{Z_2}}{\sigma_{Z_2}} \right)^2} \\ &= \sum_{i=0}^{\infty} \frac{e^{-\lambda} \lambda^i}{i!} \frac{1}{\sigma_X \sigma_{Z_2} \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{y' - \mu_X - \sigma_X i - \sigma_X \mu_{Z_2}}{\sigma_X \sigma_{Z_2}} \right)^2} \end{aligned} \quad (3.68)$$

The differential entropy of the received signal Y' is defined by

$$h(Y') = - \int_{\chi_{Y'}} f_{Y'}(y') \log f_{Y'}(y') dy' \quad (3.69)$$

where $\chi_{Y'}$ is the support of $f_{Y'}$.

3.9 Identifying Quantum Signal Models as GMMs for Non-Gaussian Input

Consider the p.d.f. of the received signal in (3.68) given by

$$f_{Y'}(y') = \sum_{i=0}^{\infty} \frac{e^{-\lambda} \lambda^i}{i!} \frac{1}{\sqrt{2\pi} \sigma_X \sigma_{Z_2}} e^{-\frac{1}{2} \left(\frac{y' - \mu_X - \sigma_X i - \sigma_X \mu_{Z_2}}{\sigma_X \sigma_{Z_2}} \right)^2} = \sum_{i=0}^{\infty} v_i \mathcal{N}\left(y', \mu_i^{(y')}, \sigma_i^{(y')^2}\right) \quad (3.70)$$

where $v_i = \frac{e^{-\lambda} \lambda^i}{i!}$, $\sum_{i=0}^{\infty} v_i = 1$, $v_i \geq 0 \quad \forall i$ and $\mathcal{N}(y, \mu_i^{(y')}, \sigma_i^{(y')^2})$ is Gaussian density in dummy variable y , mean $\mu_i^{(y')} = \mu_X + \sigma_X i + \sigma_X \mu_{Z_2}$, and s.d. $\sigma_i^{(y')} = \sigma_X \sigma_{Z_2}$ with variance $\sigma_i^{(y')^2}$.

In a practical scenario simulated in MATLAB, the p.d.f. of the hybrid noise in (3.45) can be approximated as $f_Z(z)$ in (3.46) and can be used to formulate $f_Y(y)$ which is given by

$$f_{Y'}(y') = \sum_{i=0}^R \frac{e^{-\lambda} \lambda^i}{i!} \frac{1}{\sqrt{2\pi} \sigma_X \sigma_{Z_2}} e^{-\frac{1}{2} \left(\frac{y' - \mu_X - \sigma_X i - \sigma_X \mu_{Z_2}}{\sigma_X \sigma_{Z_2}} \right)^2} = \sum_{i=0}^R v_i \mathcal{N}\left(y, \mu_i^{(y')}, \sigma_i^{(y')^2}\right) \quad (3.71)$$

This is a GM in the scalar variable y' , $v_i = \frac{e^{-\lambda} \lambda^i}{i!}$, $v_i \geq 0 \quad \forall i$, and $\sum_{i=0}^{\infty} v_i \approx 1$ for large R . The corresponding GM in a random vector is given by, $\bar{y}' \in \mathbb{R}^M$ is

$$f_Y'(\bar{y}') = \sum_{i=0}^R v_i \mathcal{N}\left(\bar{y}', \bar{\mu}_i^{(y')}, \sum_i^{(y')}\right) \quad (3.72)$$

where $\bar{y}'$ is the random vector in $\mathbb{R}^M$, $\bar{\mu}_i^{(y')}$ is the mean vector and $\sum_i^{(y')}$ is the covariance matrix of the corresponding Gaussian density $\mathcal{N}$. As f_Z and f_Y' are both densities of the GM, the closed-form solution of the corresponding entropies H_Z and H_Y' of noise and the received signal cannot be calculated due to the logarithm of the sum of an exponential function. However, Theorems 1 and 2 provide the lower and upper bounds for each of the entropies H_Z and $H_{Y'}$.

The upper bound and lower bound of H_Z are given by U_Z and L_Z in (3.51) and let the upper and lower bound of $H_{Y'}$ be given by $U_{Y'}$ and $L_{Y'}$, respectively. That is,

$$L_{Y'} \leq H_{Y'} \leq U_{Y'} \quad (3.73)$$

3.10 Capacity of the Quantum Channel for Non-Gaussian Input

The mutual information $I(X; Y')$ between the transmitted signal X and the received signal Y' is defined as, $I(X; Y') = H_X + H_{Y'} - H(X, Y')$ and applying the chain rule for CVs, we have, $H(X, Y') = H(Y'|X) - H_X$. Therefore, $I(X; Y') = H_{Y'} - H(Y'|X) = H_{Y'} - H(X + Z|X) = H_{Y'} - H(Z|X) = H_{Y'} - H(Z) = H_{Y'} - H_Z$ as transmitted signal X and noise Z are independent. For the sake of notational ease, we rename $H(Z)$ as H_Z . Using (3.73) and (3.51), we will get,

$$-L_Z \geq -H_Z \geq -U_Z \quad (3.74)$$

$$H_{Y'} - L_Z \geq H_{Y'} - H_Z \geq H_{Y'} - U_Z \quad (3.75)$$

$$U_{Y'} - L_Z \geq H_{Y'} - L_Z \geq H_{Y'} - H_Z = I(X; Y') \quad (3.76)$$

Therefore,

$$I(X; Y') \leq U_{Y'} - L_Z \quad (3.77)$$

Hence,

$$\tilde{C} = \max_{f(x)} I(X; Y') \leq U_{Y'} - L_Z \quad (3.78)$$

From Theorem 1, as we calculated L_Z , the lower bound for H_Z in (3.58),

$$L_Z = - \sum_{i=0}^R u_i \cdot \log_2 \left(\sum_{j=0}^R u_j \cdot \mathcal{N}(\bar{\mu}_i^{(z)}; \bar{\mu}_j^{(z)}, \sum_i^{(z)} + \sum_j^{(z)}) \right). \quad (3.79)$$

From Theorem 2, similarly calculate $U_{Y'}$, the upper bound for $H_{Y'}$,

$$U_{Y'} = \sum_{i=0}^R v_i \cdot \log_2 \left(-\log_2 v_i + \frac{1}{2} \log_2 \left((2\pi e)^M \left| \sum_i^{(y')} \right| \right) \right), \quad (3.80)$$

where $u_i = v_i = \frac{e^{-\lambda} \lambda^i}{i!} \forall i = 0(1)R$. From (3.58) and (3.80), we have,

$$\begin{aligned} U_{Y'} - L_Z = & \sum_{i=0}^R \frac{e^{-\lambda} \lambda^i}{i!} \left(-\log_2 \left(\frac{e^{-\lambda} \lambda^i}{i!} \right) + \frac{1}{2} \log_2 \left((2\pi e)^M \left| \sum_i^{(y')} \right| \right) \right. \\ & \left. + \log_2 \left(\sum_{j=0}^R \frac{e^{-\lambda} \lambda^j}{j!} \mathcal{N}(\bar{\mu}_i^{(z)}; \bar{\mu}_j^{(z)}, \sum_i^{(z)} + \sum_j^{(z)}) \right) \right). \end{aligned} \quad (3.81)$$

From (3.78) and (3.81), the channel capacity would be,

$$\begin{aligned} \tilde{C} = & \sum_{i=0}^R \frac{e^{-\lambda} \lambda^i}{i!} \left(-\log_2 \left(\frac{e^{-\lambda} \lambda^i}{i!} \right) + \frac{1}{2} \log_2 \left((2\pi e)^M \left| \sum_i^{(y')} \right| \right) \right. \\ & \left. + \log_2 \left(\sum_{j=0}^R \frac{e^{-\lambda} \lambda^j}{j!} \mathcal{N}(\bar{\mu}_i^{(z)}; \bar{\mu}_j^{(z)}, \sum_i^{(z)} + \sum_j^{(z)}) \right) \right). \end{aligned} \quad (3.82)$$

This is the expression for the quantum channel capacity when the noise Z and the received signal Y' are random vectors of dimension M .

In scalar analogy, that is when the noise Z and the received signal Y' are random variables with p.d.f.s (3.46) and (3.71) respectively, the expression of capacity reduces to,

$$\begin{aligned} \tilde{C} = & \sum_{i=0}^R \frac{e^{-\lambda} \lambda^i}{i!} \left(-\log_2 \left(\frac{e^{-\lambda} \lambda^i}{i!} \right) + \frac{1}{2} \cdot \log_2 \left(2\pi e \sigma_i^{(y')} \right) \right. \\ & \left. + \log_2 \left(\sum_{j=0}^R \frac{e^{-\lambda} \lambda^j}{j!} \mathcal{N}(\mu_i^{(z)}; \mu_j^{(z)}, \sigma_i^{(z)^2} + \sigma_j^{(z)^2}) \right) \right), \end{aligned} \quad (3.83)$$

by putting $M = 1$, and replacing $\left| \sum_i^{(y')} \right|$ by $\sigma_i^{(y')}$, $\bar{\mu}_i^{(z)}$ by $\mu_i^{(z)}$, $\bar{\mu}_j^{(z)}$ by $\mu_j^{(z)}$, $\sum_i^{(z)}$ by $\sigma_i^{(z)^2}$ and $\sum_j^{(z)}$ by $\sigma_j^{(z)^2}$, where each vector is replaced by its scalar analogue. Again $\mu_i^{(z)} = \mu_{Z_2} + i \forall i$, $\sigma_i^{(z)^2} = \sigma_{Z_2}^2 \forall i$, and $\sigma_i^{(y')^2} = \sigma_X^2 \sigma_{Z_2}^2 \forall i$. Therefore, the capacity of a quantum channel in the case of a non-Gaussian transmitted signal is given by,

$$\begin{aligned} \tilde{C} = & \sum_{i=0}^R \frac{e^{-\lambda} \lambda^i}{i!} \left(-\log_2 \left(\frac{e^{-\lambda} \lambda^i}{i!} \right) + \frac{1}{2} \log_2 \left(2\pi e (\sigma_X^2 \sigma_{Z_2}^2) \right) \right. \\ & \left. + \log_2 \left(\sum_{j=0}^R \frac{e^{-\lambda} \lambda^j}{j!} \mathcal{N}(\mu_{Z_2} + i; \mu_{Z_2} + j, 2\sigma_{Z_2}^2) \right) \right) \end{aligned}$$

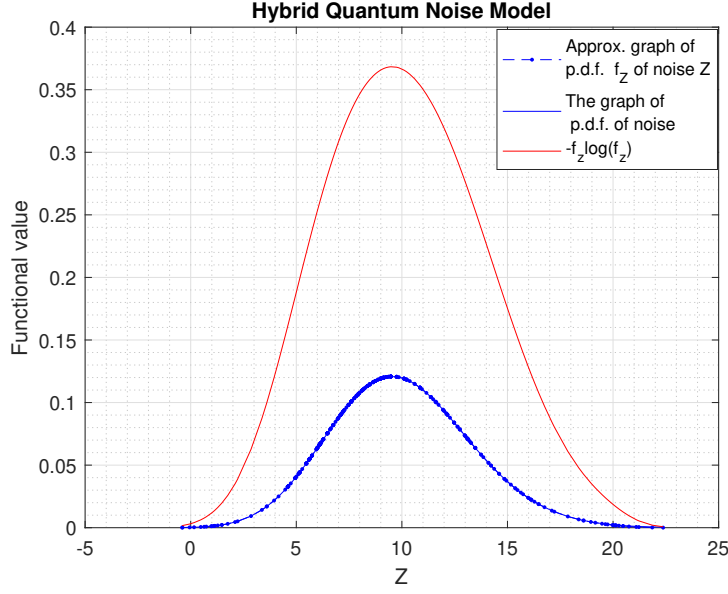


Figure 3.5: Quantum Noise model as a convolution of AWGN and Poissonian quantum noise

$$\begin{aligned}
&= \sum_{i=0}^R \frac{e^{-\lambda} \lambda^i}{i!} \left(-\log_2 \left(\frac{e^{-\lambda} \lambda^i}{i!} \right) + \frac{1}{2} \log_2 \left(2\pi e (\sigma_X^2 \sigma_{Z_2}^2) \right) \right. \\
&\quad \left. + \log_2 \left(\sum_{j=0}^R \frac{e^{-\lambda} \lambda^j}{j!} \frac{1}{\sqrt{2} \sigma_{Z_2} \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{i-j}{\sqrt{2} \sigma_{Z_2}} \right)^2} \right) \right)
\end{aligned} \tag{3.84}$$

$$\text{where } \mathcal{N}(\mu_{Z_2} + i; \mu_{Z_2} + j, 2\sigma_{Z_2}^2) = \frac{1}{\sqrt{2} \sigma_{Z_2} \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{\mu_{Z_2} + i - \mu_{Z_2}}{\sqrt{2} \sigma_{Z_2}} \right)^2}.$$

3.11 Numerical Analysis

3.11.1 Noise Model Visualization

To visualize the models, consider the following two functions,

$$f_Z(z) = \sum_{n=0}^{\infty} \frac{e^{-\lambda} \lambda^n}{n!} \frac{1}{\sigma_{Z_2} \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{z-n-\mu_{Z_2}}{\sigma_{Z_2}} \right)^2} \tag{3.85}$$

and

$$\tilde{f}_Z(z) = \sum_{n=0}^R \frac{e^{-\lambda} \lambda^n}{n!} \frac{1}{\sigma_{Z_2} \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{z-n-\mu_{Z_2}}{\sigma_{Z_2}} \right)^2} \tag{3.86}$$

Theoretically, the density function f_Z is the actual [p.d.f.](#) of Z and the function $\tilde{f}_Z$ is an approximated [p.d.f.](#) of Z shown in Fig. 3.5. The figure shows the [HQN](#) model for parameter $\lambda = 10$, and the sample sizes of the underlying component noises Z_1 and Z_2 are 20 for each distribution (Poisson and Gaussian). Each simulation in MATLAB randomly selects two sample

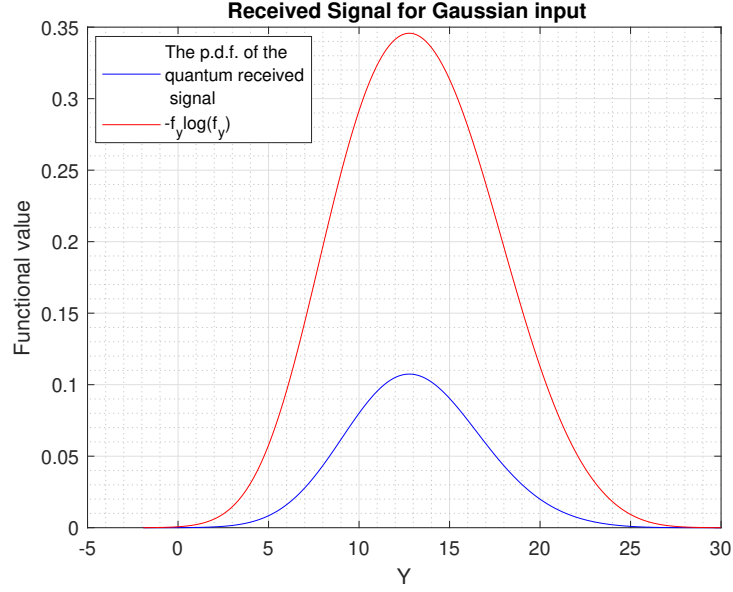


Figure 3.6: Received signal in case of Gaussian input, considered as a convoluted function of the quantum noise field and a Gaussian transmitted signal for the Gaussian quantum channel

spaces for the Poisson distribution (with parameter $\lambda = 10$) and the Gaussian distribution (with parameters $\mu_{Z_2} = 0$ and $\sigma_{Z_2} = 1$), returning a joint sample space for Z .

Let A and B be two sets, and $f : A \rightarrow B$ and $g : A \rightarrow B$ are two functions. Mathematically, two functions are identical if $f(a) = g(a) \forall a \in A$. In particular, the domains of the functions f_Z and $\tilde{f}_Z$ are the same as they are the same sample space of Z , and $f_Z(z) = \tilde{f}_Z(z) \forall z \in Z$. Therefore the actual p.d.f. f_Z of Z can be well approximated by the function $\tilde{f}_Z$ in Fig. 3.5. From here onwards, we will refer $\tilde{f}_Z$ by f_Z . Since the noise model is identified as GMM, we can infer that the p.d.f. can be approximated as a mixture of a finite number of Gaussian densities[130]. In Fig. 3.5, we characterize the joint quantum-classical noise by plotting the function $-f_Z(z) \log_2 f_Z(z)$ and $f_Z(z)$. This will be used to calculate the mutual information $I(X; Y)$, along with the entropy of the received signal Y and, hence, the channel capacity of the quantum channel.

3.11.2 Output Signal Model's Visualization

A. Received Signal Model's Visualization for Gaussian Distributed Transmitted Signal for Gaussian Quantum Channel:

The p.d.f. of the received signal f_Y is given in Fig. 3.6, which is the convolution product of the p.d.f.s of the Gaussian transmitted signal and HQN. Therefore, we computed the approximate density function for the received signal Y . Since the output signal model is identified as GMM, we can infer

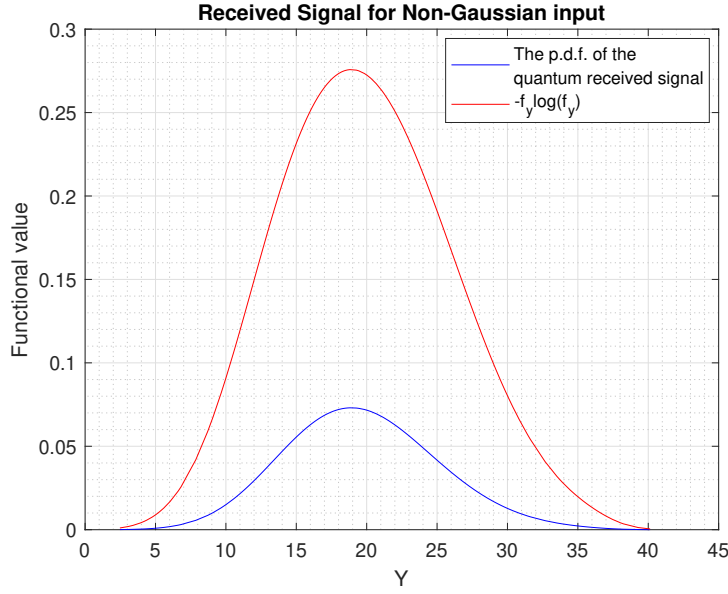


Figure 3.7: Received signal in case of non-Gaussian input, considered as a convoluted function of quantum noise field and non-Gaussian transmitted signal for a Gaussian quantum channel

that the p.d.f. can be approximated as a mixture of a finite number of Gaussian densities[130]. We also characterized the function $-f_Y(y) \log_2 f_Y(y)$ shown in Fig. 3.6 whose integral is the entropy of the received signal Y .

B. Received Signal Model's Visualization for a non-Gaussian distributed transmitted signal for a Gaussian Quantum Channel:

The p.d.f. of the received signal $f_{Y'}$ is given in Fig. 3.7, we approximated the probability distribution of the transmitted signal X by the mean of the sample space of X , and based on that we calculated the approximate density function for the received signal Y' . Since the received signal model is identified as GMM, we can infer that the p.d.f. can be approximated as a mixture of a finite number of Gaussian densities. We also characterized the function $-f_{Y'}(y') \log_2 f_{Y'}(y')$ shown in fig. 3.7 whose integral is the entropy of the received signal Y' .

3.11.3 Capacity Comparisons with respect to Signal-to-noise ratio

A. Visualization of the Capacity Trend with SNR for a Gaussian Quantum Channel in case of Non-Gaussian Distributed Transmitted Signal:

In Fig. 3.8, the capacity of the noisy quantum channel for the non-Gaussian distributed transmitted signal with respect to SNR and the logarithm of SNR ($\log_2(\text{SNR})$), are illustrated. As expected, the capacity increases with SNR and the logarithm of SNR. However, in the next section,

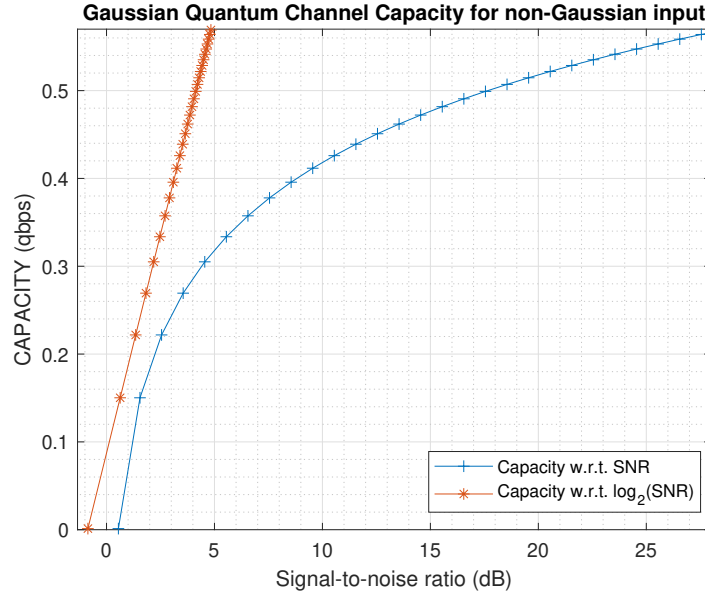


Figure 3.8: The channel capacity of the Gaussian quantum channel for the non-Gaussian input transmitted signal

we will visualize the tendency of the capacity of the Gaussian quantum channel in the case of a non-Gaussian input transmitted signal, and this will lead to a comparison of the capacities for Gaussian and non-Gaussian inputs for the Gaussian quantum channel.

B. Visualization of the Capacity Trend with SNR for Gaussian Quantum Channel in case of Gaussian Distributed Transmitted Signal:

Fig. 3.9 shows the capacity of the noisy quantum channel as a function of SNR and the logarithm of SNR in the case of Gaussian distributed input. It can be observed that the capacity increases with SNR and the logarithm of SNR , as expected. However, in the next section, we would like to compare the tendency of the capacities of the Gaussian quantum channels in either case of the Gaussian and the non-Gaussian transmitted signal.

C. Comparison of the Capacity Tendencies of Gaussian Quantum Channel in case of Gaussian and Non-Gaussian Distributed Transmitted Signal:

The capacity figures, Fig. 3.8 and Fig. 3.9, show the capacities of single Gaussian Quantum channels for non-Gaussian and Gaussian transmitted signals, respectively, with respect to (I) SNR and (II) the logarithm of SNR . To conclude, the Gaussian transmitted signal gives better capacity (the highest achievable data transmission rate) for the quantum channel shown in Fig. 3.9. Meanwhile, the non-Gaussian transmitted signal for the Gaussian channel gives a bit lesser capacity rate (shown in Fig. 3.8) than the Gaussian input transmitted signal with respect to SNR . In comparison to the logarithm of SNR , the Gaussian input signal gives better capacity

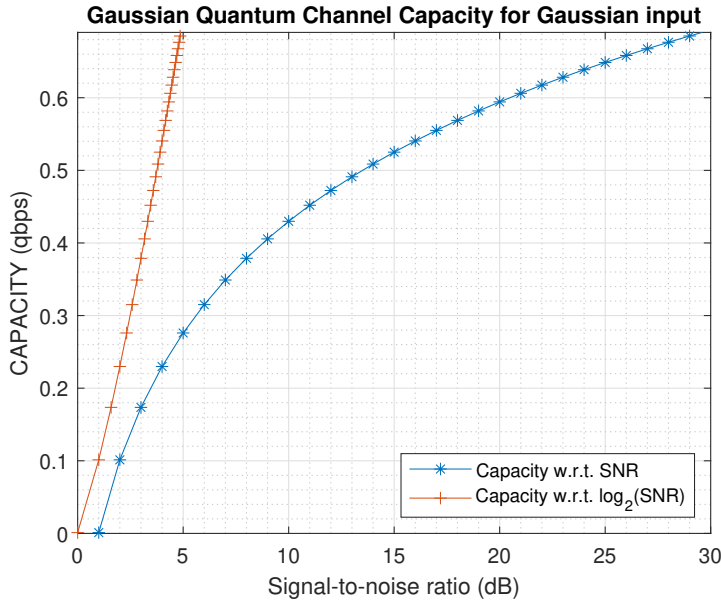


Figure 3.9: The channel capacity of the Gaussian quantum channel for the Gaussian input transmitted signal

than the non-Gaussian input for the same channel, and the Gaussian quantum channel matches standard results for capacity with respect to SNR for classical communication.

3.12 Conclusion

This chapter advances statistical quantum signal processing by modeling Gaussian quantum channels. It has developed representations for HQN channel models and output signals in these channels. Despite using Gaussian mixture models to characterize the quantum noise statistics, closed-form solutions are derived for the classical capacities of quantum channels with Gaussian and non-Gaussian inputs in the presence of HQN. The capacity expressions quantitatively demonstrate that Gaussian input distributions yield the highest achievable data rates for Gaussian quantum channels across varying SNRs. This research thus makes several vital contributions: (i) graphical depictions of HQN, (ii) statistical frameworks to describe quantum Gaussian channels, and (iii) analytical capacity solutions that confirm the advantage of Gaussian signaling in this setting. Overall, the modeling and analysis of quantum Gaussian channels from a statistical signal processing perspective provides new insights into optimizing information transfer through quantum networks. In the next chapter, the reader will explore the pattern analysis of HQN. It involves the component analysis of HQN based on the Poisson parameter and the number of Gaussian components. The Chapter 4 will focus on how these two parametric factors are interrelated and their effects on hybrid noise modeling.

Chapter 4

Hybrid Quantum Noise Approximation and Pattern Analysis

4.1 Introduction

Noise plays a vital role in determining the accuracy of quantum information processing in the quantum channel. In this chapter, classical noise effects are considered in conjunction with quantum noise sources to provide a more realistic model of quantum channels. A [HQN](#) model incorporating both quantum Poisson noise and classical [AWGN](#) has been interpreted as an infinite mixture of Gaussians with weightage from the Poisson distribution in Chapter 3. The entropy measure of such a convoluted function is difficult to calculate. This chapter developed how the infinite mixture can be well approximated by a finite mixture distribution depending on the Poisson parametric setting, compared to the number of mixture components. The mathematical analysis of [HQN](#) characterization has been demonstrated using Gaussian and Poisson parametric analysis. This chapter facilitates the study of parametric values in the component distribution and provides the mathematical framework for approximating hybrid noise entropy, thereby offering insight into [HQN](#).

In quantum channel modeling, accurately simulating quantum noise requires careful consideration of both Poisson and Gaussian parameters. The Poisson parameter, λ , is crucial as it quantifies the average photon count and captures the quantum mechanical nature of light, reflecting the random emission and detection processes in quantum optics [203, 204]. On the other hand, Gaussian components offer a probabilistic approach to modeling noise in quantum channels [205], effectively incorporating both quantum and classical noise effects. This integration enables a comprehensive representation of various noise sources that affect quantum states during transmission. Together, these models improve understanding of quantum noise complexities, facilitating the development of advanced error correction techniques and communication protocols designed to counteract the diverse

noise characteristics in quantum information transfer.

In Chapter 3, the HQN model [21], proposed initially, utilizes an approximation of an infinite mixture of Gaussian components, with mixing coefficients derived from a Poisson distribution. However, existing research omitted discussions on methods for approximating the primary p.d.f. with a secondary p.d.f. and also lacked formal proof establishing the new approximate function as a valid p.d.f. to work with. This chapter addresses these gaps by proving that the approximate function qualifies as p.d.f. In addition, this chapter introduces techniques for transitioning from an infinite mixture model to a finite number of mixture components, enhancing the practical applicability of the model [22].

The main aspects of this chapter are listed as follows:

- This chapter utilizes the framework of the HQN model that integrates quantum Poissonian noise with classical AWGN. This model is conceptualized as an infinite mixture of Gaussian distributions, with weights derived from Poisson distributions, which accurately represent the noise encountered in quantum communication systems, as discussed in Chapter 3. A pivotal aspect of this study is the influence of the photon count, indicated by the Poisson parameter, on this HQN model. This chapter examines the mathematical approach to approximating this complex noise model using a finite mixture of Gaussian distributions weighted by the Poisson distribution.
- This chapter's objective is to provide a method to simplify the HQN's p.d.f. into a finite number of Gaussian mixtures, contingent on the Poisson parameter, to estimate the entropy of the HQN. This analysis has not been provided in the existing work [21]. This chapter investigates how the Poisson parameter interrelates with the number of Gaussian mixture components necessary to simulate the HQN's original p.d.f.

Overall, this chapter presents the effect of Gaussian and Poisson parameters on HQN in emerging quantum communication systems.

4.2 System Model

In a practical scenario, quantum noise is indistinguishable from classical noise in quantum communication [206]. It is challenging to detect pure quantum noise in a real-world system separately from classical noise; therefore, one should consider both quantum and classical noise when modeling a noisy quantum channel. Mathematically, the combination of classical AWGN and quantum Poisson noise is represented by a random variable $Z = Z_1 + Z_2$. Quantum noise Z_1 follows a Poisson distribution with parameter λ [11], while classical AWGN Z_2 follows a Gaussian distribution with parameters μ_{Z_2} and σ_{Z_2} [20]. The HQN Z is statistically described by

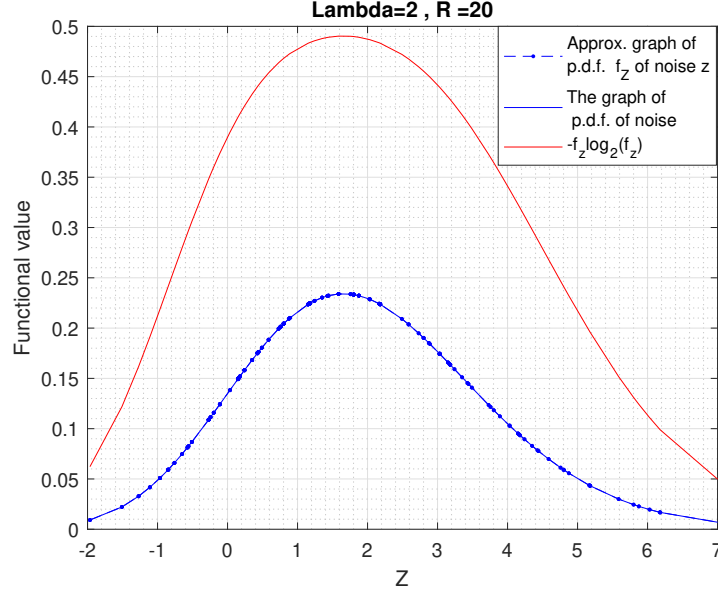


Figure 4.1: HQN model as a convolution of additive white Gaussian and quantum Poissonian noise with parameter $\lambda = 2$ and number of mixing components $R = 20$.

considering it as the convolution product of Z_1 and Z_2 as [21],

$$f_Z(z) = \sum_{i=0}^{\infty} w_i \mathcal{N}(z, \mu_i^{(z)}, \sigma_i^{(z)^2}), \quad (4.1)$$

where

$$\mathcal{N}(z, \mu_i^{(z)}, \sigma_i^{(z)^2}) = \frac{1}{\sigma_{Z_2} \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{z - i - \mu_{Z_2}}{\sigma_{Z_2}} \right)^2}, \quad (4.2)$$

is a Gaussian density with mean $\mu_i^{(z)} = i + \mu_{Z_2}$, standard deviation (s.d.) $\sigma_i^{(z)} = \sigma_{Z_2}$, and weightage $w_i = \frac{e^{-\lambda} \lambda^i}{i!}$, $\sum_{i=0}^{\infty} w_i = 1$, $w_i \geq 0 \quad \forall i = 0, 1, 2, \dots$. In the expression (4.1), the p.d.f. $f_Z(z)$ of HQN is an infinite mixture of Gaussians with weightage from the Poisson distribution. This infinite mixture is challenging to interpret in 1-dimension and multi-dimensions as well. It is possible to express the p.d.f. $f_Z(z)$ of HQN in a finite sum of the distributions of the underlying components. This research aims to determine the number of components that, in combination, can approximate the actual distribution.

Mathematically, the following function

$$\tilde{f}_Z(z) = \sum_{i=0}^R \frac{e^{-\lambda} \lambda^i}{i!} \frac{1}{\sigma_{Z_2} \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{z - i - \mu_{Z_2}}{\sigma_{Z_2}} \right)^2} = \sum_{i=0}^R w_i \mathcal{N}(z, \mu_i^{(z)}, \sigma_i^{(z)^2}), \quad (4.3)$$

will replace the p.d.f. in (4.1) depending on certain aspects, where R is the number of Gaussian components. Not every combination of values of λ and R can approximate the p.d.f. in a finite domain of the function. We find the number of components for which the value of R so that the function $\tilde{f}_Z(z)$

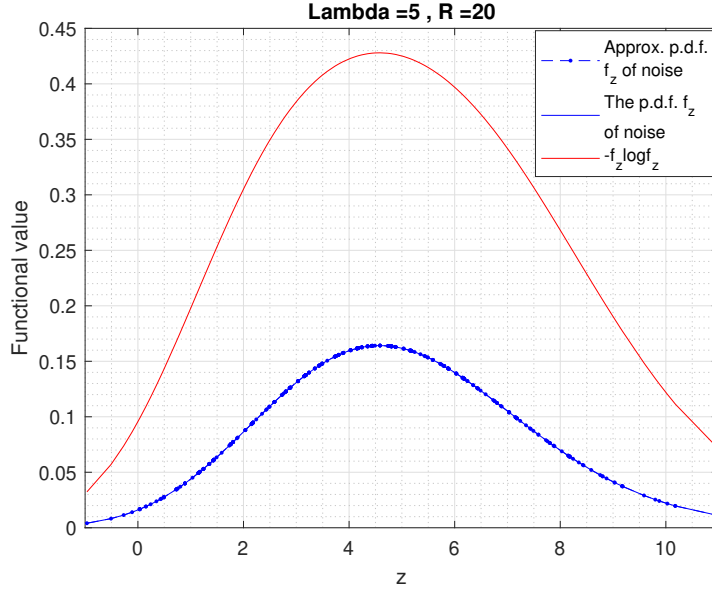


Figure 4.2: A HQN model for $\lambda = 5$ and number of mixing components $R = 20$. Here, the Poisson parameter λ is adequately balanced by a sufficient number of Gaussian components.

will serve the purpose of an approximation of $f_Z(z)$ in a finite domain. In (4.3), the function $\tilde{f}_Z(z)$ is the Gaussian mixture in the scalar variable z , the coefficient $w_i \geq 0 \quad \forall i$ and $\sum_{i=0}^R w_i \approx 1$ for large R . We will investigate how the number of components varies depending on the parametric value λ . The value of λ is interrelated with the number of components R in the finite summation expression (4.3), leading to the well-approximated p.d.f. of HQN. Once $\tilde{f}_Z(z)$ approximates $f_Z(z)$ in a finite domain, we will calculate the entropy of the HQN Z . To evaluate the differential entropy of Z , one can consider the formula [22, 130],

$$H(Z) = - \int_{\chi_Z} f_Z(z) \log_2 f_Z(z) dz,$$

where χ_Z is the support of f_Z , i.e., the set on which f_Z is nonzero.

4.2.1 HQN Model Analysis

Consider the HQN function in (4.1), to replace the infinite mixture with a finite number of components, one should expect that the new function will approximate the original function in the domain of the function, mathematically stating that the function $\tilde{f}_Z$ can reasonably approximate the original p.d.f. f_Z of HQN Z , depending on the parametric values of λ and the number of mixing components R . To do so, we have to prove the following [22]:

- The function $\tilde{f}_Z$ approximately represents a p.d.f., that is, $\tilde{f}_Z(z) \geq 0 \quad \forall z \in \mathcal{D}_Z$ and $\int_{\mathcal{D}_Z} \tilde{f}_Z(z) dz \approx 1$ where $\mathcal{D}_Z$ is the domain of f_Z .

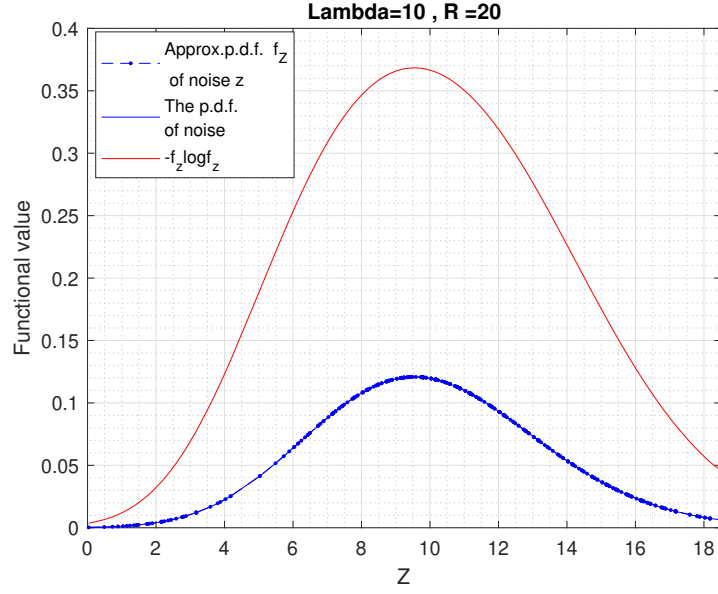


Figure 4.3: A HQN model for $\lambda = 10$ and number of mixing components $R = 20$. This approximation is sufficient to capture the actual behaviour of the quantum noise and, hence, the entropy of the HQN.

- $f_Z(z)$ and $\tilde{f}_Z(z)$ are identical on the domain of the functions, which is $f_Z(z) = \tilde{f}_Z(z) \forall z \in \mathcal{D}_Z \implies \tilde{f}_Z$ will approximate well the original p.d.f. of f_Z within the domain of functions. Mathematically, the two functions $f : A \rightarrow B$ and $g : A \rightarrow B$ are identical if $f(a) = g(a) \forall a \in A$.

It is important to note that, to do these, we need first to define the domain $\mathcal{D}_Z$ of the functions on which these functions can be replaced by each other. It is also essential to analyze how the parametric values of λ and the number of mixing components R are interdependent to approximate the p.d.f. of noise Z —starting the analysis by generating the domain $\mathcal{D}_Z$ of the functions. In the simulation, MATLAB randomly selects sample spaces for Gaussian noise based on specific parameters (mean & standard deviation) of the distribution, and depending on the parametric value λ , the sample space for Poisson noise has been generated, returning a joint sample space for HQN Z . We define both functions f_Z and $\tilde{f}_Z$ in the specified sample space, ensuring they are described in the same domain. This method is employed due to the lack of experimental HQN data and the limitation on the availability of pre-generated quantum noise data. Hence, we have the domain for these functions in which the functions can be compared.

Secondly, to prove the function $\tilde{f}_Z$ as a p.d.f., let compute the following

$$\begin{aligned} \int_{\mathcal{D}_Z} \tilde{f}_Z(z) dz &= \int_{\mathcal{D}_Z} \sum_{i=0}^R \frac{e^{-\lambda} \lambda^i}{i!} \frac{1}{\sigma_{Z_2} \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{z-i-\mu_{Z_2}}{\sigma_{Z_2}} \right)^2} dz \\ &= \sum_{i=0}^R \int_{\mathcal{D}_Z} \frac{e^{-\lambda} \lambda^i}{i!} \frac{1}{\sigma_{Z_2} \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{z-i-\mu_{Z_2}}{\sigma_{Z_2}} \right)^2} dz \end{aligned}$$

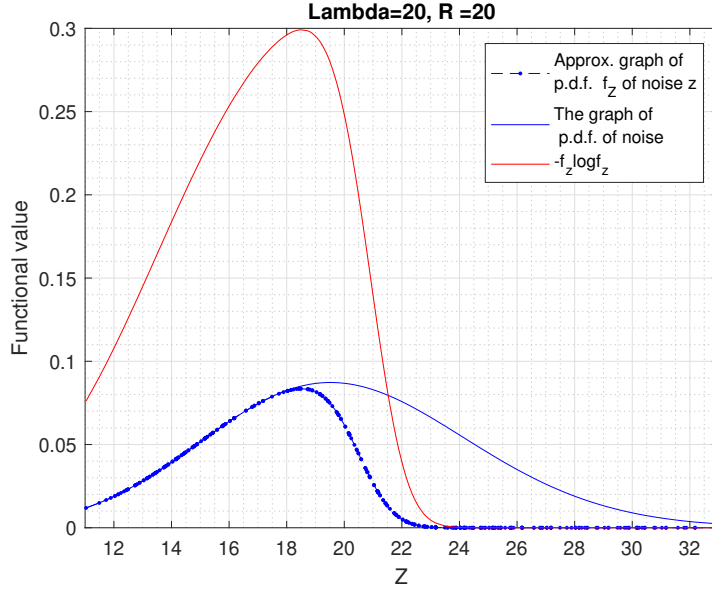


Figure 4.4: HQN model for $\lambda = 20$ and number of mixing components $R = 20$. Here λ , it is not adequately balanced by a sufficient number of Gaussian components.

$$= \sum_{i=0}^R w_i \int_{\mathcal{D}_Z} \mathcal{N}(z, \mu_i^{(z)}, \sigma_i^{(z)^2}) dz = \sum_{i=0}^R w_i = \sum_{i=0}^R \frac{e^{-\lambda} \lambda^i}{i!} \approx 1, \quad (4.4)$$

as $\mathcal{N}(z, \mu_i^{(z)}, \sigma_i^{(z)^2})$ is a Gaussian p.d.f. in random variable Z , hence $\int_{\mathcal{D}_Z} \mathcal{N}(z, \mu_i^{(z)}, \sigma_i^{(z)^2}) = 1$, and the mixing coefficient w_i coming from Poisson distribution, so $\sum_{i=0}^R w_i \approx 1$ depending on λ and R . Also note that $\tilde{f}_Z(z) \geq 0 \quad \forall z \in \mathcal{D}_Z$ as $\frac{e^{-\lambda} \lambda^i}{i!} \geq 0$ being an exponential function and $\lambda \geq 0$ and also $\frac{1}{\sigma_{Z_2} \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{z - i - \mu_{Z_2}}{\sigma_{Z_2}} \right)^2} \geq 0$ as $\frac{1}{\sigma_{Z_2} \sqrt{2\pi}} \geq 0$ and $e^{-\frac{1}{2} \left(\frac{z - i - \mu_{Z_2}}{\sigma_{Z_2}} \right)^2} \geq 0$. So, it is proved that $\tilde{f}_Z(z)$ satisfies the criteria of being a p.d.f. in the domain of the function $\mathcal{D}_Z$.

Third, by definition, $f_Z(z) = \tilde{f}_Z(z) \quad \forall z \in \mathcal{D}_Z$. Hence, it can be inferred that $\tilde{f}_Z$ can be an approximate p.d.f. depending on the parametric value λ and the mixing coefficient R . Thus, in the following paragraphs, we discuss how this approximation depends on λ and the mixing coefficient R , involving interesting results in the following numerical section.

4.3 Numerical Analysis

4.3.1 HQN Model Visualization

The research focuses on modeling HQN using a finite number of Gaussian components, aiming to replicate the behaviour of an infinite Gaussian mixture through discrete approximations. In MATLAB simulations, the p.d.f.s

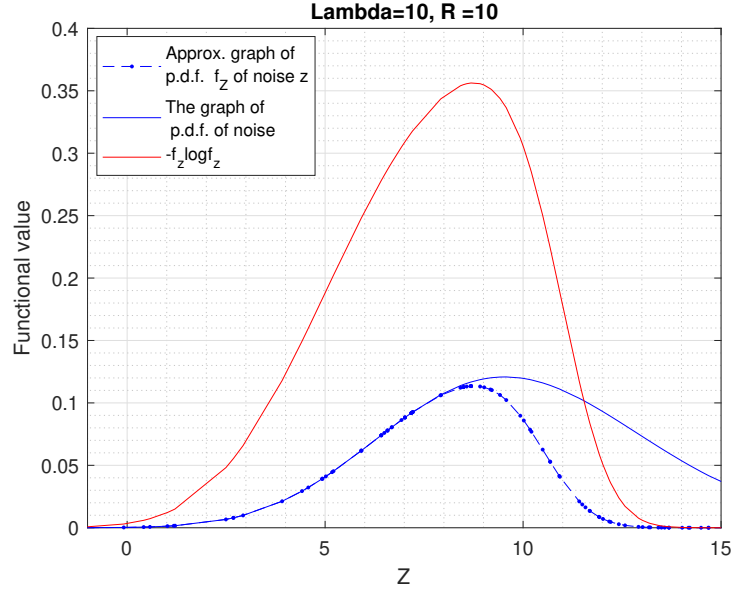


Figure 4.5: HQN model for $\lambda = 10$ and number of mixing components $R = 10$. This approximation fails to capture the actual behaviour of the quantum noise.

f_Z and $\tilde{f}_Z$ of the HQN Z are compared, where they share the same domain and demonstrate equivalence across all parameters studied. These functions are analyzed under varying conditions of the Poisson parameter λ and the number of Gaussian components R , with consistent Gaussian parameters $\mu_{Z_2} = 0$ and $\sigma_{Z_2} = 1$.

Through a series of figures, the relationship between λ and R is explored, providing insight into the impact of these parameters on the accuracy of the noise approximation. In particular, Fig. 4.1 shows how well $\tilde{f}_Z$ approximates f_Z for $\lambda = 2$ and $R = 20$, including an analysis of the entropy function that gives a detailed view of the noise characteristics in these settings. This methodological approach is consistent across various scenarios with different values of λ , as shown in the subsequent figures, Fig. 4.2 and Fig. 4.3.

As λ increases, discrepancies in the approximation accuracy become apparent, mainly when λ equals R , as shown in Fig. 4.4, where the model underperforms. This observation suggests that the number of Gaussian components R must exceed λ to ensure a reliable approximation of the HQN p.d.f. This principle is further tested in Fig. 4.5 and Fig. 4.6, where adjustments R are made to improve approximation fidelity, demonstrating that increasing R relative to λ can significantly enhance the model's accuracy.

The study reveals that the parameter λ , which represents the number of photons or the rate of quantum events per unit time, has a crucial influence on the fidelity of the noise model. If λ is not adequately balanced by a sufficient number of Gaussian components, the approximation fails to capture the actual behaviour of the quantum noise. This finding underscores the necessity of carefully choosing R based on the values of λ to ensure that the Gaussian mixtures effectively approximate the complex dynamics of HQN.

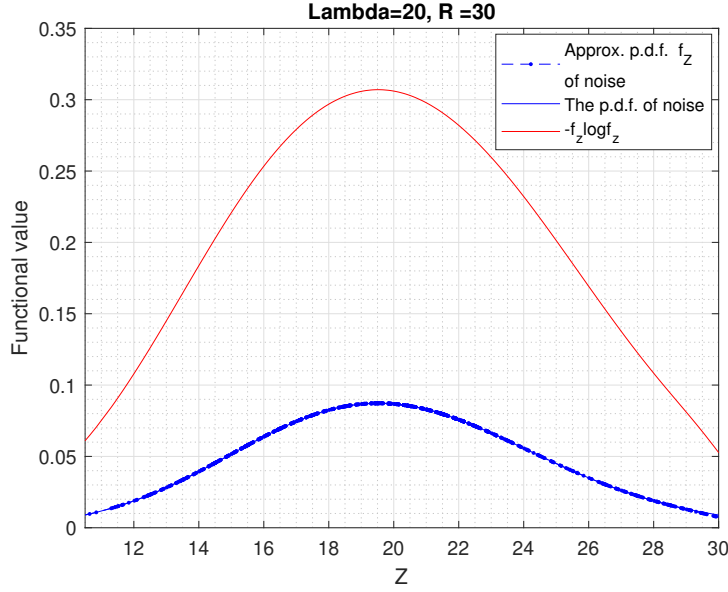


Figure 4.6: HQN model for $\lambda = 20$ and number of mixing components $R = 30$. Here, the Poisson parameter λ is adequately balanced by a sufficient number of Gaussian components; the approximation suffices to capture the actual behaviour of the quantum noise and hence the entropy of the HQN.

In general, this research advances the understanding of quantum noise modeling by establishing critical parameters that govern the effective simulation of quantum channels in communication systems. It highlights the importance of parameter selection in achieving accurate noise models and lays a foundation for future explorations into more sophisticated quantum communication technologies. The conclusion is that, for a precise simulation, the number of components of the Gaussian mixture must significantly exceed the Poisson parameter λ , as succinctly expressed by the inequality $\lambda < R$. This parameter interplay is crucial for developing reliable quantum communication systems, as it directly impacts the integrity and performance of quantum information processing.

4.4 Conclusion

This chapter significantly contributes to this area by mathematically modelling HQN in practical quantum communication channels. A novel aspect of this chapter is the calculation of the entropy of the hybrid noise, which provides deeper insight into the characteristics of the HQN, understanding, and impact. Its primary achievement is demonstrating how the p.d.f. of HQN can be effectively approximated using a finite number of component distributions. The study emphasized the necessity of considering the Poisson parameter related to the number of mixing components in the HQN. It articulates the correlation between the control of flying photons (or the clicks on a Geiger counter, denoted by the parameter) and the number of mixing components in the HQN. This relationship is crucial to improving

our understanding of practical noisy quantum channels, marking a significant advancement in the field. In Chapter 5, the reader will explore the estimation of entropy for HQN. Quantum entropies of HQN are key areas of study, providing essential insights into optimizing HQN in satellite quantum communication channels.

Chapter 5

Entropy Estimation of Hybrid Quantum Noise Channels

5.1 Introduction

Quantum entropies of [HQN](#) provide a robust framework for quantifying information in quantum systems, offering enhanced security and performance in communication protocols. The practical implementation challenges, such as decoherence and loss, must be addressed to realize the potential of quantum entropies in large-scale applications. This study examines the equivalence and shared properties of various quantum entropy measures such as differential entropy, von Neumann entropy, Rényi entropy, Hartley Entropy, Tsallis entropy, and Unified entropy in the presence of [HQN](#). It explores the conditions under which these entropies coincide or are closely related. Through mathematical proofs and in-depth discussions, the work highlights the similarities among the most commonly used quantum entropy measures, with a particular emphasis on their behaviour within the framework of quantum information theory. It contributes to the development of more efficient quantum entropy estimation techniques, enhances quantum memory and repeater technologies, and explores new applications of quantum entropies in emerging quantum networks and computing paradigms.

This chapter proposes an analysis of the various quantum entropies of [HQN](#) quantum channels. The [HQN](#) model for [CV](#) Gaussian quantum channel is adapted from our reported work [[18](#), [21](#), [22](#), [23](#), [24](#)]. The [HQN](#) model integrates both quantum Poissonian and classical [AWGN](#) components. This research is grounded in the mathematical modeling of [HQN](#), which considers both quantum and classical noise affecting the quantum channel. The quantum noise is statistically modeled as Poissonian, and the classical noise is considered as [AWGN](#). This idea is based on the fact that quantum noise is vulnerable to both quantum and classical noise. The key contributions of this research are listed as follows:

- This chapter provides a comprehensive mathematical analysis of various quantum entropy measures, including von Neumann entropy, Rényi entropy, Hartley entropy, Tsallis entropy, and Unified entropy,

in the context of HQN. It demonstrates the conditions under which these entropies converge or closely approximate each other, contributing to a unified understanding of entropy in quantum information theory.

- This work utilizes the HQN model to further develop an entropy estimation for a hybrid quantum noisy channel. This model is crucial for accurately representing the noise in satellite-based quantum communication channels, improving the estimation of quantum entropy in practical systems such as QKD and entanglement-based quantum communication networks.
- This chapter explores how entropy measures can be leveraged for quantum tomography, which is essential for state reconstruction in noisy quantum systems. Additionally, it examines the role of entropy in optimizing satellite-based quantum communication protocols, including error correction, secure key distribution, and entanglement verification, providing insights into improving the efficiency and robustness of quantum networks.

This chapter provides insights into the quantum entropies of HQN for the development of quantum communication systems.

5.2 System model

The HQN model used for this study is taken from [18, 21, 22, 23, 24].

Quantum entropy quantifies the uncertainty or disorder in a quantum state, playing a crucial role in quantum information theory and quantum tomography. The most widely used entropy measure is the von Neumann entropy, defined as $S(\rho) = -\text{Tr}(\rho \log \rho)$ where ρ is the density matrix of the quantum state. The von Neumann entropy generalizes the classical differential entropy to quantum systems and is a key indicator of quantum state purity. For two quantum states ρ and σ , the quantum relative entropy is given by $S(\rho||\sigma) = \text{Tr}(\rho \log \rho - \rho \log \sigma)$. This measure quantifies the distinguishability between ρ and σ , playing a fundamental role in quantum hypothesis testing and information geometry. For a bipartite quantum state ρ_{AB} , the quantum mutual information is defined as $I(A : B) = S(\rho_A) + S(\rho_B) - S(\rho_{AB})$ where $\rho_A = \text{Tr}_B(\rho_{AB})$ and $\rho_B = \text{Tr}_A(\rho_{AB})$ are the reduced density matrices of subsystems A and B . Quantum mutual information measures the total correlations between subsystems, capturing both classical and quantum correlations.

5.2.1 Quantum Entropies of Quantum Communication Channels

A quantum channel $\mathbf{N}$ is a CPTP map that transforms a density matrix ρ into another density matrix $D(\rho)$. Channels can introduce noise, loss, or

decoherence, impacting the transmitted quantum information. A quantum channel, $\mathbf{N}$, maps density matrices (quantum states) from one Hilbert space to another, $\mathbf{N}(\rho) = \sum_k E_k \rho E_k^\dagger$, where E_k are the Kraus operators that satisfy $\sum_k E_k^\dagger E_k = I$. Quantum noise refers to the effect of such a channel on a state, introducing decoherence, loss, or other transformations. Quantum entropy for channels or noise is not defined directly as a property of the channel itself but rather as the entropy of states modified by the channel or as measures of information loss associated with the channel.

Alternatively, a quantum communication channel can be represented by a completely positive unital map $\mathbf{N} : A_1 \rightarrow A$ between two finite quantum systems A_1 (input) and A (output). This mapping transforms an input state ρ of A_1 into an output state $\rho \circ \mathbf{N}$ of A , analogous to signal transmission in classical communication. The mutual entropy quantifies the amount of information correctly transmitted through the channel and depends on both the input state and the channel characteristics.

In quantum communication, the transmission process follows a scheme, $C_1 \xrightarrow{\gamma} A_1 \xrightarrow{\alpha} A \xrightarrow{\delta} C$ where C_1 and C represent classical input and output algebras, γ is the encoding map, δ decoding map, and $\mathbf{N}$ is the quantum channel responsible for signal transmission. The mutual entropy $I(\rho; \mathbf{N})$ of an input state ρ with respect to the channel $\mathbf{N}$ is defined as the supremum of relative entropy measures over all possible orthogonal decompositions. This measure captures the correlation between input and output states, providing insight into the efficiency of quantum information transmission. Stochastic Representations of the quantum channel can be described using a stochastic matrix with k rows and n columns, where each entry represents the probability of receiving an output given a specific input. This framework is analogous to classical communication channels, where information is encoded into symbols from an input set X , transmitted through the channel, and received as symbols from an output set Y . The transmission reliability is characterized by a probability distribution $W(y|Z)$, which determines the likelihood of receiving y given that x was sent.

Quantum channel entropy quantifies the uncertainty or disorder a quantum channel introduces, playing a crucial role in characterizing information flow and noise effects in quantum communication. Unlike classical channels, where entropy directly measures information loss, quantum entropy must account for quantum correlations, entanglement, and decoherence effects. Quantum channel entropy significantly influences error correction, entanglement-assisted communication, and the design of quantum networks. Understanding quantum channel entropy deepens our grasp of how noise and uncertainty impact quantum information transfer, guiding advances in quantum cryptography, satellite-based QKD, and fault-tolerant quantum networks.

For quantum communication, it is essential to model the realistic quantum noise of a quantum channel. Previous studies have shown that quantum noise is often represented as Poissonian noise [207, 208, 209]. However, a practical quantum link also suffers from noise sources that contribute

non-quantum noises, such as classical noise sources [62, 64, 65]. Classical noise is an integral part of the quantum channel and must be addressed to model a realistic quantum channel. A quantum channel is an **CPTP** map that transforms density operators ρ on a Hilbert space $\mathcal{H}$ into other states, represented as, $\rho \mapsto \mathbf{T}(\rho)$ [21, 22, 193, 194]. Assuming identical input and output spaces, a Gaussian quantum channel $\mathbf{T}$ can be expressed as, $\mathbf{T}(\rho) = \text{Tr}_E[\mathbf{U}(\rho \otimes \rho_E)\mathbf{U}^\dagger]$ Where $\mathbf{U}$ is a Gaussian unitary determined by a quadratic Bosonic Hamiltonian, and ρ_E is a Gaussian state [10, 21, 198]. For lossless unitary evolution, the channel is governed by, $\mathbf{U} = e^{\frac{i}{2} \sum_{k,l} \mathbf{H}_{kl} \mathcal{R}_k \mathcal{R}_l}$ where $\mathbf{H}_{kl}$ is a real symmetric matrix, $\mathcal{R}$ are canonical coordinates, and $\mathbf{U}$ belong to the symplectic group $Sp(2n, \mathbb{R})$ [10, 198]. Gaussian channels can be described in the Schrödinger picture as, $\rho \mapsto \mathbf{T}_{\mathbf{A}, \mathbf{Z}}(\rho)$ or equivalently via the transformation, $\rho \mapsto \mathbf{A}^T \rho \mathbf{A} + \mathbf{Z}$ [10, 21, 22, 23, 198]. $\mathbf{A}$ modulates the signal by performing amplification, attenuation, and phase-space rotation, and $\mathbf{Z}$ represents noise, comprising both quantum noise (ensuring physical consistency) and classical noise. Since $\mathbf{A}$ can be any real matrix, any transformation of the form, $\rho \mapsto \mathbf{A}^T \rho \mathbf{A}$ can be approximated by incorporating sufficient noise. In the simplest case, the transformation reduces to, $\rho \mapsto \rho + \mathbf{Z}$, where $\mathbf{Z}$ includes both quantum and classical noise [21, 22]. For $\mathbf{A} = \mathbf{I}_{2n}$, where $\mathbf{I}_{2n}$ is the identity matrix of order $2n \times 2n$ (with n denoting the quantum system's degrees of freedom), the added noise $\mathbf{Z}$ is originating from a convolution of Quantum Poisson noise and **AWGN** [21, 22].

This quantum channel model parallels classical communication, where, $Y = X + Z$ represents the transmitted signal X , the received signal Y , and the **HQN** Z . In quantum communication networks handling classical information, both quantum and classical noise influence transmission, where, $Z = Z_1 + Z_2$, Z_1 is the Quantum shot noise (Poisson-distributed) and Z_2 is the Classical white noise (Gaussian-distributed). A schematic representation of this hybrid quantum noisy channel is provided in Fig. 7.2, illustrating the interplay of quantum noise and classical interference in practical quantum networks.

5.2.2 Entropy of Satellite Quantum Channel

In optical communication, a photon quantum state carries quantum information. The optical signal, modulated by an input state, transforms a quantum channel, which is modeled as a completely positive map. The efficiency of optical communication relies on quantum mutual entropy, which evaluates how much information is preserved during transmission. Quantum noise and modulation techniques influence entropy dynamics, affecting channel capacity and error rates.

For multiple quantum channels with a standard input algebra, the entropy definition can be extended to n-tuples of channels, thereby forming a multi-channel model. This generalization is crucial for analyzing dynamic entropy, which captures information flow in time-dependent quantum systems. After sending the word $(x_1, x_2, \dots, x_n)$ from the alphabet

$\{1, 2, \dots, k\}$, the state of the quantum system evolves according to the channel $\mathbf{N} : M_m(\mathbb{C}) \rightarrow M_k(\mathbb{C})$, where the quantum states are represented by density matrices in the matrix algebra $M_m(\mathbb{C})$. The quantum channel transforms the input state ρ into an output state $\rho' = \mathbf{N}(\rho)$, capturing the probabilistic nature of quantum information transfer. In the asymptotic limit ($n \rightarrow \infty$), information transmission is analyzed using quantum channel capacity and error-correcting codes, ensuring that the probability of decoding errors remains small while maximizing reliable transmission rates. The study of entanglement-assisted communication and quantum error correction further refines this model, optimizing quantum signal transmission in practical scenarios, including optical and satellite-based quantum networks.

In such a quantum communication setup, the mutual entropy is crucial in quantifying the information transfer efficiency, particularly in the presence of noise and decoherence. Quantum information measures, including relative entropy, coherent information, and Holevo capacity, help characterize the fundamental limits of reliable quantum transmission. The study of quantum communication channels is central to quantum information theory, particularly in optical and satellite-based quantum communications. Mutual entropy is a fundamental measure of channel efficiency, guiding the development of robust quantum transmission protocols.

In the quantum probabilistic interpretation of a channel $\alpha : \mathfrak{B} \rightarrow \mathfrak{A}$, the algebra $\mathfrak{A}$ with a distinguished state ρ is regarded as a quantum probability space. The channel α acts as a random variable with state space $\mathfrak{B}$, and the transformed state $\rho \circ \alpha$ represents the distribution of this random variable. In some cases, a family of channels $\alpha_t : \mathfrak{B} \rightarrow \mathfrak{A}$, indexed by a parameter t , arises where all channels share the same input algebra. Such a collection is called a multiple channel (or a process in the probabilistic framework). This concept is crucial in quantum stochastic processes, where the dynamics of state transformations are analyzed over time, particularly in quantum information and open system dynamics. Let $(\alpha_i : A_i \rightarrow A)_{i=1}^n$ be a multiple quantum channel, and let $|\psi\rangle$ be a state of A . The entropy $H_{|\psi\rangle}(\alpha_1, \alpha_2, \dots, \alpha_n)$ satisfies several key properties that ensure its consistency as a measure of uncertainty in quantum systems. First, it is non-negative, ensuring that entropy never takes negative values. It exhibits monotonicity, meaning adding more independent channels does not decrease entropy. The subadditivity property states that the total entropy is, at most, the sum of the entropies of individual channels. Moreover, entropy is concave in the state $|\psi\rangle$, meaning that for a convex combination of states $|\psi\rangle = \sum_k p_k |\psi_k\rangle$, the entropy satisfies $H_{|\psi\rangle}(\alpha_1, \dots, \alpha_n) \geq \sum_k p_k H_{|\psi_k\rangle}(\alpha_1, \dots, \alpha_n)$. It is also invariant under unitary transformations, meaning that if the channels undergo a unitary transformation U , the entropy remains unchanged, i.e., $H_{|\psi\rangle}(\alpha_1, \dots, \alpha_n) = H_{|\psi\rangle}(\alpha_1^U, \dots, \alpha_n^U)$, where $\alpha_i^U(A) = U\alpha_i(A)U^\dagger$. Finally, in the classical limit, when operators commute, this entropy measure reduces to the differential entropy, ensuring consistency with classical information theory. These properties make

$H_{|\psi\rangle}(\alpha_1, \dots, \alpha_n)$ a robust tool for analyzing quantum correlations and information flow in quantum communication systems.

This section outlines the methodology for calculating the entropy over a fading satellite quantum channel. Alice generates a sequence of $2N$ real Gaussian-distributed random variables, $X_1, X_2, \dots, X_{2N} \sim \mathcal{N}(x; \mu_{X_k}, \sigma_{X_k}^2)$, with mean μ_{X_k} and standard deviation σ_{X_k} , representing N coherent states $|\mathbf{a}_1\rangle, |\mathbf{a}_2\rangle, \dots, |\mathbf{a}_N\rangle$, where each $\mathbf{a}_k = X_{2k-1} + iX_{2k} \in \mathbb{C}$. These states are transmitted through the quantum channel, and Bob performs homodyne detection, measuring both quadratures simultaneously. For the k th channel use, Bob obtains measurement results for the Y_{2k-1} and Y_{2k} , corresponding to Alice's transmitted values X_{2k-1} and X_{2k} , respectively. This process yields the raw key string $\mathbf{Y} = (Y_1, Y_2, \dots, Y_{2N})$, which serves as the foundation for key reconciliation, particularly under low transmission efficiency using reverse reconciliation. The analysis is extended to the asymptotic regime ($N \rightarrow \infty$), ensuring optimal performance in CV-QKD [26].

The parameter estimation process is crucial for predicting the expected outcomes for Alice and Bob within the given channel model. The quantum channel connecting them is modeled as a phase-insensitive, noisy Bosonic channel, requiring the consideration of the random variables X and Y within this framework. The relationship between Alice's transmitted signal X and Bob's received signal Y is given by

$$Y = TX + Z, \quad (5.1)$$

where T is the overall transmission coefficient for the atmospheric quantum channel use, with the transmission efficiency defined as $\tau = T^2$, and Z represents the HQN. So a state $\rho \mapsto \rho \circ \mathbf{N}$ for a satellite quantum channel $\mathbf{N}$ can be expressed in terms of the received symbols y as a function of transmitted symbols x . The hybrid noise Z is modeled as the sum of quantum Poissonian noise $Z^{(1)}$ and AWGN $Z^{(2)}$, such that

$$Z = Z^{(1)} + Z^{(2)}, \quad (5.2)$$

where the Poissonian noise $Z_k^{(1)}$ follows the p.m.f.,

$$f_{Z^{(1)}}(j) = \frac{e^{-\lambda} \lambda^j}{j!}, \quad \lambda \geq 0, \quad j \in \{0, 1, 2, \dots\}. \quad (5.3)$$

and the classical AWGN $Z^{(2)}$ is Gaussian-distributed with mean $\mu_{Z^{(2)}}$ and variance $\sigma_{Z^{(2)}}^2$. The convoluted p.d.f. represents the hybrid noise Z affecting the satellite quantum channel. Additionally, entropy measures are crucial in continuous-variable quantum systems for accurately estimating the channel's achievable rate.

5.3 Quantum Entropies of HQN Channel

The entropy quantification of the quantum channel extends to Rényi entropy, Tsallis entropy, and Unified entropy, which provide finer characteri-

zations of uncertainty, particularly in quantum cryptography and entanglement theory. The quantum conditional entropy and coherent information further quantify the flow of quantum information, which is crucial for analyzing quantum error correction and determining quantum channel capacity.

5.3.1 Differential Entropy of HQN

In our approach, we considered both quantum and classical noise to accurately represent the impact of HQN on the quantum channel. Quantum noise is statistically modeled using a Poisson distribution, while classical noise is treated as AWGN. This dual-noise modeling reflects that quantum channels are affected by both quantum and classical noise sources. The convolution of these two types of noise yields the HQN, represented by the following equation,

$$f_Z(z) = \sum_{i=0}^{\infty} \frac{e^{-\lambda} \lambda^i}{i!} \frac{1}{\sigma_{Z_2} \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{z-i-\mu_{Z_2}}{\sigma_{Z_2}} \right)^2} = \sum_{i=0}^{\infty} w_i \mathcal{N} \left(z; \mu_i^{(z)}, \sigma_i^{(z)^2} \right). \quad (5.4)$$

The coefficients $w_i = \frac{e^{-\lambda} \lambda^i}{i!}$ represents the weight of each Gaussian mixture component, with $w_i \geq 0$ and $\sum_{i=0}^{\infty} w_i = 1$. Each component $\mathcal{N}(z; \mu_i^{(z)}, \sigma_i^{(z)^2})$ is a Gaussian distribution with mean $\mu_i^{(z)} = \mu_{Z_2} + i$ and variance $\sigma_i^{(z)^2} = \sigma_{Z_2}^2$.

Due to the complexity of dealing with such an infinite mixture of Gaussian functions, we utilize a GMM to simplify calculations, such as entropy. It has been shown that the entropy of a GMM can be bounded within upper and lower limits, allowing us to derive a closed-form solution for quantum channel capacity. To further simplify our analysis, we approximate the infinite Gaussian mixture with a finite number of components using Poisson-distributed weights. The approximated HQN model is given by

$$f_Z(z) = \sum_{i=0}^R \frac{e^{-\lambda} \lambda^i}{i!} \frac{1}{\sigma_{Z_2} \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{z-i-\mu_{Z_2}}{\sigma_{Z_2}} \right)^2} = \sum_{i=0}^R w_i \mathcal{N} \left(z; \mu_i^{(z)}, \sigma_i^{(z)^2} \right). \quad (5.5)$$

The summation is truncated to R , with $\sum_{i=0}^R w_i \approx 1$ for sufficiently large R , ensuring the approximation closely matches the original model [22]. We also identified a relationship between the Poisson parameter λ and the number of Gaussian components, which plays a role in optimizing the model [23, 24].

Quantum channels facilitate the transfer of quantum states between two or more parties, forming the backbone of quantum communication and computation. Unlike classical communication channels, quantum channels must accommodate superposition, entanglement, and decoherence phenomena. Understanding the entropic characteristics of these channels is essential for evaluating their efficiency and reliability. This work examines the entropy measures relevant to quantum channels, including von Neumann entropy, differential entropy, Rényi entropy, Hartley Entropy, Tsallis entropy, Unified entropy, and Mutual information of quantum channels. This hybrid

noise model accurately represents the contributions of quantum and classical noise, which are crucial for analyzing quantum communication channels and optimizing key rate estimation in practical QKD systems [21]. This work presents a structured approach to exploring the entropy of the HQN modeled as a GMM. Such a representation encapsulates hybrid noise features from a quantum channel, combining classical and quantum probabilistic elements.

Entropies are invaluable in practical scenarios for modeling, understanding, and mitigating the effects of noise in hybrid quantum systems. They provide a mathematical framework for quantifying uncertainty and disorder, which is crucial for advancing the fields of quantum computing, quantum communication, and quantum information theory. For the CV Gaussian system, the differential entropy of HQN Z with p.d.f. $f_Z(z)$ on support χ_Z . The differential entropy of hybrid quantum noise Z is given by

$$H(Z) = \mathbb{E}[-\log f_Z(z)] = - \int_{\chi_Z} f_Z(z) \log f_Z(z) dz \quad (5.6)$$

Differential entropy measures the average surprisal for outcomes drawn from a continuous distribution. While entropy in quantum systems is traditionally defined via the density matrix ρ , this work focuses on a novel perspective describing quantum noise using random variables and analyzing their entropy. The goal is to investigate the equivalence (or lack thereof) between different forms of quantum entropy and the conditions under which they converge. Replacing (5.5) in (5.6), the entropy becomes,

$$H(Z) = - \int \left(\sum_{i=1}^R w_i \mathcal{N}(z; \mu_i, \sigma_i^2) \right) \log \left(\sum_{i=1}^R w_i \mathcal{N}(z; \mu_i, \sigma_i^2) \right) dz. \quad (5.7)$$

This involves integration over the weighted sum of Gaussian p.d.f. s, requiring approximations or numerical evaluation. The entropy reflects the uncertainty arising from the interplay of individual Gaussian components. Analytical evaluation is challenging due to the summation and logarithmic terms; numerical integration is typically employed. Quantum entropies of the HQN Z provide insights into its information-theoretic and thermodynamic properties.

Other important categories of quantum entropies are von Neumann entropy, Rényi Entropy, and Unified Entropy, which are discussed along the way. This study shows their equivalence in the case of HQN. For $\alpha \rightarrow 1$, Rényi entropy converges to differential entropy. Unified entropy generalizes Rényi entropies.

$$H_{q,r}(Z) = \frac{1}{1-r} \log \left(\int f_Z(z)^q dz \right), \quad q, r > 0, q \neq 1. \quad (5.8)$$

This measure is helpful for hybrid scenarios where noise exhibits multifaceted characteristics. Quantum entropy applied to channels and noise focuses on how these processes affect the entropy of quantum states, with

measures like coherent information, entropy generation, and relative entropy providing insights into their behaviour. These concepts are critical in assessing the efficiency and reliability of quantum communication and quantum computation systems.

This work focuses on identifying conditions for equivalence between these approaches. This study bridges classical and quantum perspectives on entropy, analyzing how random variables can characterize quantum noise. By comparing entropy measures across different paradigms, we aim to provide more profound insights into their interrelations and practical implications in quantum information theory.

5.3.2 Von Neumann Entropy of the HQN

Von Neumann entropy measures the mixedness of a quantum state. It is zero for pure states and positive for mixed states, reaching its maximum for the maximally mixed state. More intuitive in phase space formulation instead of the Hilbert space, where von Neumann entropy is defined as

$$S = - \int f_Z * \log_* f_Z, \quad (5.9)$$

which is the negative of the expected value of the $*$ -logarithm of the Gaussian function [2]. It quantifies the degree of mixedness of a quantum state, with higher values indicating more significant uncertainty.

For HQN Z with p.d.f. given by (5.6) in the quantum mechanical formalism, the differential entropy $H(Z)$ and von Neumann entropy $S(Z)$ are equivalent under $*$ -product of C^* -algebra. In the CV-QKD setting, the differential entropy of the HQN Z with density function $f_Z(z)$ is defined as (5.6). We start with the von Neumann entropy of HQN in density matrix representation $S(\rho_Z) = -\text{Tr}(\rho_Z \log \rho_Z)$, where ρ_Z is the density matrix representation of the probability density function $f_Z(z)$. The density matrix is diagonal on a continuous basis $|z\rangle$, hence,

$$\rho_Z = \int f_Z(z) |z\rangle \langle z| dz. \quad (5.10)$$

The logarithm of the density matrix is

$$\log(\rho_Z) = \int \log f_Z(z) |z\rangle \langle z| dz. \quad (5.11)$$

Now, substituting both expressions into the von Neumann entropy formula, we get

$$S(\rho_Z) = -\text{Tr}(\rho_Z \log \rho_Z). \quad (5.12)$$

Substituting the integral representations

$$S(\rho_Z) = -\text{Tr} \left(\left(\int f_Z(z) |z\rangle \langle z| dz \right) \left(\int \log f_Z(z') |z'\rangle \langle z'| dz' \right) \right). \quad (5.13)$$

Since these integrals involve projection operators $|z\rangle\langle z|$, the product $(\int f_Z(z)|z\rangle\langle z| dz)(\int \log f_Z(z')|z'\rangle\langle z'| dz')$, can be simplified further because $|z\rangle\langle z|$ are orthonormal projectors, the only nonzero contributions come when $z = z'$, allowing us to write the product as $\int f_Z(z) \log f_Z(z) |z\rangle\langle z| dz$. Thus, the trace operation, $\text{Tr}(\int f_Z(z) \log f_Z(z) |z\rangle\langle z| dz)$ reduces to an integral over the eigenvalues $f_Z(z)$, $\int f_Z(z) \log f_Z(z) dz$. Hence we obtain

$$S(\rho_Z) = - \int f_Z(z) \log f_Z(z) dz. \quad (5.14)$$

This is precisely the differential entropy of the probability distribution $f_Z(z)$, confirming that for a diagonal density matrix, the von Neumann entropy reduces continuously to the classical differential entropy.

5.3.3 Quantum Rényi Entropy of HQN

Quantum Rényi entropy is a differential entropy generalization which measures uncertainty or information content in a CV quantum system where HQN is described by density f_Z . It is parameterized by a non-negotiable number α . It is beneficial for analyzing different aspects of information theory, such as the diversity or concentration of a probability distribution. Quantum Rényi entropy can be treated as a generalization of the differential entropy as α approaches 1. In general, the α -order quantum Rényi entropy of HQN is given by

$$H_\alpha(Z) = \frac{1}{1-\alpha} \log \int f_Z(z)^\alpha dz, \quad (5.15)$$

where $0 \leq \alpha < \infty$, $\alpha \neq 1$, and α is a non-negative parameter that characterizes the entropy. It provides different perspectives on the noise's uncertainty depending on the value of α . For $\alpha > 1$, Rényi entropy gives more weight to the higher probabilities, which are less uncertain, while for $0 < \alpha < 1$, it emphasizes the lower probabilities, which means more uncertainty.

The connection between the quantum Rényi entropy of HQN and $\mathcal{P}$ -norms is interesting to explore. The $\mathcal{L}^\mathcal{P}$ spaces are also called function spaces, which leads towards a generalization of the $\mathcal{P}$ -norm for the finite-dimensional vector spaces. For a function $g \in \mathcal{L}^\mathcal{P}$, the Lebesgue integral of such a function can be defined as follows. $\|g\|_\mathcal{P} = \left(\int_\chi |g|^\mathcal{P} \right)^{1/\mathcal{P}}$. The entropy of HQN can be defined with the $\mathcal{P}$ -norm from (5.15) and the definition of this $\mathcal{P}$ -norm in function space as follows.

For the density function of HQN f_Z , define the $\mathcal{P}$ -norm of such function as

$$\|f_Z\|_\mathcal{P} = \left(\int f_Z^\mathcal{P} dz \right)^{1/\mathcal{P}} \quad (5.16)$$

since f_Z is a p.d.f. so it is always positive.

The α -norm which is a specific case of the $\mathcal{P}$ -norm, for $\mathcal{P} = \alpha$, so the α -norm of the HQN Z with p.d.f. f_Z defined by

$$\|f_Z\|_\alpha = \left(\int f_Z^\alpha dz \right)^{1/\alpha} \quad (5.17)$$

So, in terms of the $\mathcal{P}$ -norm, the quantum Rényi entropy of HQN Z can be derived as

$$\begin{aligned} H_\alpha(Z) &= \frac{1}{1-\alpha} \log \left(\int f_Z^\alpha dz \right) = \frac{\alpha}{1-\alpha} \frac{1}{\alpha} \log \left(\int f_Z^\alpha dz \right) \\ &= \frac{\alpha}{1-\alpha} \log \left(\int f_Z^\alpha dz \right)^{1/\alpha} = \frac{\alpha}{1-\alpha} \log \|f_Z\|_\alpha. \end{aligned} \quad (5.18)$$

About the $\mathcal{L}^\mathcal{P}$ spaces, the von Neumann algebra, or the so-called w^* -algebra of bounded operators on a Hilbert space of the quantum system, is a special type of C^* -algebra. For different values α , the $\mathcal{P}$ -norm highlights various aspects of the distribution $f_Z(Z)$, and thus, quantum Rényi entropy can provide a more nuanced understanding of the uncertainty in quantum noise Z . The α -norm captures how concentrated or spread out the distribution is. For higher α , the $\mathcal{P}$ -norm (and thus the quantum Rényi entropy) gives more weight to more significant components of the vector (i.e., the higher probabilities in the distribution), leading to a lower entropy. Quantum Rényi entropy with lower α values captures more of the overall diversity of the distribution. As α increases, the entropy measure becomes more sensitive to the most probable outcomes, thus reducing the perceived uncertainty. Different values α provide different perspectives on the state's uncertainty.

A. Differential Entropy as a special case of quantum Rényi Entropy ($\alpha \rightarrow 1$) for HQN

Differential entropy is the most common form of quantum entropy used in quantum information theory, given by (5.6). For $\alpha \rightarrow 1$, the quantum Rényi entropy gives,

$$\begin{aligned} H_1(Z) &= \lim_{\alpha \rightarrow 1} H_\alpha(Z) = \lim_{\alpha \rightarrow 1} \frac{\log \left(\int_{\chi_Z} f_Z^\alpha dz \right)}{1-\alpha} \\ &= \lim_{\alpha \rightarrow 1} \frac{\left(\int_{\chi_Z} f_Z^\alpha dz \right)^{-1} \left(\int_{\chi_Z} f_Z^\alpha \log f_Z dz \right)}{-1} \\ &= - \frac{\int_{\chi} f_Z \log f_Z dz}{\int_{\chi} f_Z dz} = - \int_{\chi} f_Z \log f_Z dz \end{aligned} \quad (5.19)$$

by using H'hospital rule and $\int_{\chi_Z} f_Z dz = 1$ as f_Z is a p.d.f.. Hence, the differential entropy merges with the quantum Rényi entropy ($\alpha \rightarrow 1$) for HQN.

Quantum Rényi entropy can be used in differential privacy to measure the privacy guarantees of randomized algorithms. This entropy is useful in feature selection and classification in quantum ML, where understanding the data distribution is crucial [22].

5.3.4 Hartley Entropy (Max-Entropy) of HQN

Hartley entropy (max entropy) quantifies a system's maximum uncertainty, assuming all outcomes are equally probable. It measures the logarithm of the number of possible outcomes and is derived by counting the non-zero probabilities in the distribution. Hartley entropy is a crude measure of uncertainty, insensitive to the actual probabilities, and focuses only on the number of possible outcomes. Under a CV system, the HQN Z Hartley entropy can be applied to Gaussian states. It can be defined as the logarithm of the practical support $f_Z(Z)$, which quantifies the region where $f_Z(Z)$ is non-zero or significantly non-negligible. The Hartley entropy of HQN can be defined as

$$H_{\text{Hartley}}(Z) = \log |\chi_Z|, \quad (5.20)$$

where $|\chi_Z|$ denotes the volume or measure of the support χ_Z in the domain of $f_Z(Z)$. Hartley entropy measures the amount of information when all outcomes are equally likely, providing a measure of the uncertainty based on the logarithm of the number of possible states. When $\alpha = 0$, the quantum Rényi entropy of HQN corresponds to the logarithm of the support of the density distribution, mathematically it is defined as

$$H_0(Z) = \log |\chi_Z| \quad (5.21)$$

However, note that from the definition of quantum Rényi entropy of HQN (associated with $\mathcal{P}$ -norm) (5.18), we can not directly substitute $\alpha = 0$ to deduce the Hartley Entropy/ Max-Entropy as the $\mathcal{L}^{\mathcal{P}}$ spaces are the norm linear space whenever $\mathcal{P} \geq 1$, that is for $0 \leq \mathcal{P} \leq 1$, $\|\cdot\|_{\mathcal{P}}$ is not a norm. So for $\alpha = 0$,

$$H_0(Z) = \log \int_{\chi} f_Z^0 dz = \log z|_{\chi_Z} = \log [\max \chi_Z - \min \chi_Z] = \log |\chi_Z| \quad (5.22)$$

as the set χ_Z is an interval on real line R .

5.3.5 Quantum Collision Entropy of HQN

The collision entropy of HQN is defined as

$$H_2(Z) = -\log \int f_Z(z)^2 dz \quad (5.23)$$

Quantum collision entropy is sensitive to the concentration of the probability distribution, providing a measure of the likelihood of a collision between two independent samples.

A. Quantum Collision Entropy as a special case of Quantum Rényi Entropy for $\alpha = 2$

Quantum Collision entropy, or the 2-Rényi entropy, quantifies the probability that two independent and identically distributed random variables are equal. It is useful in cryptographic contexts and is defined as for $\alpha = 2$, the quantum Rényi entropy gives,

$$H_\alpha(Z) = \frac{1}{1-\alpha} \log \left(\int_{\chi} f_Z^\alpha dz \right) = -\log \left(\int_{\chi} f_Z^2 dz \right) \quad (5.24)$$

f_Z is a GM so $f_Z^2 = f_Z \cdot f_Z$ is again a GM [18, 21, 22, 23, 24], hence for $\alpha = 2$, quantum Rényi entropy becomes quantum Collision entropy in case of HQN. The quantum collision entropy for the HQN can be expressed as

$$H_2(Z) = -\log \int \left(\sum_{i=1}^R w_i \mathcal{N}(z; \mu_i, \Sigma_i) \right)^2 dz \quad (5.25)$$

Squaring a sum introduces cross terms of the form,

$$\sum_{i,j} w_i w_j \int \mathcal{N}(z; \mu_i, \Sigma_i) \mathcal{N}(z; \mu_j, \Sigma_j) dz. \quad (5.26)$$

However, this integral does not simplify easily unless all Gaussians are identical or well separated.

In the particular case we have each Gaussian component $\mathcal{N}(z; \mu_i^{(z)}, \sigma_i^{(z)^2})$ with mean $\mu_i^{(z)} = \mu_{Z_2} + i$ and variance $\sigma_i^{(z)^2} = \sigma_{Z_2}^2$, this guarantees and shows those components distributions are identical and well separated hence can be applied for the HQN's distribution. Expanding the square term,

$$f_Z(z)^2 = \left(\sum_{i=1}^R w_i \mathcal{N}(z; \mu_i, \Sigma_i) \right) \cdot \left(\sum_{j=1}^R w_j \mathcal{N}(z; \mu_j, \Sigma_j) \right) \quad (5.27)$$

which leads to

$$f_Z(z)^2 = \sum_{i=1}^R \sum_{j=1}^R w_i w_j \mathcal{N}(z; \mu_i, \Sigma_i) \mathcal{N}(z; \mu_j, \Sigma_j). \quad (5.28)$$

Compute the integral,

$$I = \int f_Z(z)^2 dz = \int \sum_{i=1}^R \sum_{j=1}^R w_i w_j \mathcal{N}(z; \mu_i, \Sigma_i) \mathcal{N}(z; \mu_j, \Sigma_j) dz. \quad (5.29)$$

Interchanging summation and integration, we get

$$I = \sum_{i=1}^R \sum_{j=1}^R w_i w_j \int \mathcal{N}(z; \mu_i, \Sigma_i) \mathcal{N}(z; \mu_j, \Sigma_j) dz. \quad (5.30)$$

The integral of the product of two Gaussians gives [21]

$$\int \mathcal{N}(z; \mu_i, \Sigma_i) \mathcal{N}(z; \mu_j, \Sigma_j) dz = \mathcal{N}(\mu_i; \mu_j, \Sigma_i + \Sigma_j), \quad (5.31)$$

where the right-hand side is a Gaussian evaluated at μ_i under the distribution $\mathcal{N}(\mu_j, \Sigma_i + \Sigma_j)$, which simplifies to

$$\frac{e^{(-\frac{1}{2}(\mu_i - \mu_j)^T (\Sigma_i + \Sigma_j)^{-1} (\mu_i - \mu_j))}}{(2\pi)^{d/2} |\Sigma_i + \Sigma_j|^{1/2}}. \quad (5.32)$$

Thus, the integral simplifies to

$$I = \sum_{i=1}^R \sum_{j=1}^R w_i w_j \frac{e^{(-\frac{1}{2}(\mu_i - \mu_j)^T (\Sigma_i + \Sigma_j)^{-1} (\mu_i - \mu_j))}}{(2\pi)^{d/2} |\Sigma_i + \Sigma_j|^{1/2}}. \quad (5.33)$$

Taking the logarithm $H_2(Z) = -\log I$, which gives

$$H_2(Z) = -\log \sum_{i=1}^R \sum_{j=1}^R w_i w_j \frac{e^{(-\frac{1}{2}(\mu_i - \mu_j)^T (\Sigma_i + \Sigma_j)^{-1} (\mu_i - \mu_j))}}{(2\pi)^{d/2} |\Sigma_i + \Sigma_j|^{1/2}}. \quad (5.34)$$

The asymptotic equivalence of quantum collision and differential entropy for HQN modeled as a well-separated GMM has been shown in the Appendix. For a well-separated GMM representing HQN p.d.f., where the components are far apart relative to their covariances, the collision and differential entropy expressions become asymptotically equivalent under certain conditions.

5.3.6 Min-Entropy of HQN

In general, min-entropy is derived from the maximum probability in a distribution, focusing on the most certain outcome. Min-entropy provides the least uncertainty, serving as a lower bound for other entropy measures.

A. Min-Entropy as a special case of Renyi Entropy for $\alpha \rightarrow \infty$

Min-entropy represents the maximum probability of guessing the correct outcome due to the hybrid noise effect on the first attempt. It is a measure of the amount of uncertainty in the most likely outcome given by

$$H_{\min}(Z) = \min_i (-\log f_Z) \quad (5.35)$$

When $\alpha = \infty$, Rényi entropy gives,

$$\begin{aligned} H_{\infty}(Z) &= \lim_{\alpha \rightarrow \infty} H_{\alpha}(Z) = \lim_{\alpha \rightarrow \infty} \frac{\alpha}{1 - \alpha} \log \|f_Z\|_{\alpha} \\ &= \lim_{\alpha \rightarrow \infty} \frac{\alpha}{1 - \alpha} \sup_{z \in \chi_Z} f_Z(z) = -\log \sup_i f_Z \\ &= -\sup_i \log f_Z = \min_i (-\log f_Z) \end{aligned} \quad (5.36)$$

using L'Hospital rule $[\frac{\infty}{\infty}]$ and the supremum norm (Chebyshev norm/infinity norm) $\|f_Z\|_\infty = \sup\{|f_Z| : z \in \chi_Z\}$ does not involve any α and is a scalar. So $\alpha = \infty$, Rényi entropy converges to Min-Entropy. This focuses on the most probable event, providing insight into the 'worst-case' scenario.

5.3.7 Quantum Unified Entropy of HQN

Quantum unified entropy is a generalization of various entropy measures that captures the concept of uncertainty or disorder in a system. It connects different entropy formulations into a unified framework, like differential entropy, quantum Rényi entropy, and quantum Tsallis entropy. This entropy combines features of both Rényi and Tsallis entropies, being derived by incorporating parameters from both measures. Quantum unified entropy provides a flexible framework for analyzing uncertainty, capable of interpolating between different entropy measures. Quantum unified entropy generalizes both quantum Rényi and quantum Tsallis entropies.

The quantum unified entropy formula enables a smooth transition between different types of entropy of HQN by adjusting the value of α , thereby providing a flexible tool for measuring uncertainty across various contexts. For the density function f_Z the quantum unified (α, β) - entropy can be expressed as

$$S_\alpha^\beta(f_Z) = \frac{1}{(1-\alpha)\beta} \left[\left(\int_{\chi_Z} f_Z^\alpha(z) dz \right)^\beta - 1 \right] \quad (5.37)$$

For $\alpha \rightarrow 1, \beta = 1$, it recovers the differential entropy of HQN. For $\alpha \neq 1$, the formula generalizes to other quantum entropy measures such as quantum Tsallis and quantum Rényi entropy in the case of HQN.

A. Quantum Renyi Entropy as a special case of Quantum Unified Entropy of HQN with $\beta \rightarrow 0$

$$\begin{aligned} H_\alpha(f_Z) &= \lim_{\beta \rightarrow 0} H_\alpha^\beta(f_Z) = \lim_{\beta \rightarrow 0} \frac{\left(\int_{\chi_Z} f_Z^\alpha(z) dz \right)^\beta - 1}{(1-\alpha)\beta} \\ &= \lim_{\beta \rightarrow 0} \frac{\left(\int_{\chi_Z} f_Z^\alpha(z) dz \right)^\beta \log \left(\int_{\chi_Z} f_Z^\alpha(z) dz \right)}{(1-\alpha)} \\ &= \frac{1}{1-\alpha} \log \left(\int_{\chi} f_Z^\alpha d\mu \right) \quad (5.38) \end{aligned}$$

using L'Hospital rule with $[\frac{0}{0}]$ form and $\frac{d}{dx} a^x = a^x \log a$.

5.3.8 Quantum Tsallis Entropy of HQN

Quantum Tsallis entropy is another generalization of quantum entropies. The quantum Tsallis entropy of the HQN is defined by

$$S_\alpha(f_Z) = \frac{1}{(1-q)} \left[\left(\int_{\chi_Z} f_Z^q(z) dz \right) - 1 \right] \quad (5.39)$$

Tsallis entropy is non-extensive, meaning it does not necessarily add linearly for independent systems. The quantum Tsallis entropy of HQN, as a generalization of the differential entropy, is parameterized by q . The quantum Tsallis Entropy is a special case of Unified Entropy $\beta = 1$. The quantum Tsallis entropy is another generalization of differential entropy, parameterized by an actual number α , which is non-additive and used in non-extensive thermodynamics. It plays a crucial role in the study of systems with long-range interactions.

A. Differential entropy as a special case of Tsallis Entropy for HQN

As $q \rightarrow 1$,

$$\lim_{q \rightarrow 1} S_q(Z) = \lim_{q \rightarrow 1} \frac{1}{q-1} \left(1 - \left(\int_{\chi_Z} f_Z^q(z) dz \right) \right) \quad (5.40)$$

Using L'Hôpital's rule,

$$\begin{aligned} \lim_{q \rightarrow 1} \frac{1 - \left(\int_{\chi_Z} f_Z^q(z) dz \right)}{q-1} &= -\frac{d}{dq} \left(\int_{\chi_Z} f_Z^q(z) dz \right) \\ &= - \int_{\chi_Z} \left(\frac{d}{dq} f_Z^q(z) \right) \Big|_{q=1} dz = - \int f_Z(z) \log f_Z(z) dz. \end{aligned} \quad (5.41)$$

and $\frac{d}{dx} a^x = a^x \log a$. Therefore, the differential entropy is a special case of quantum Tsallis entropy for HQN.

Other types of quantum entropies can be calculated in the case of HQN, such as quantum tomographic entropy, conditional entropy, quantum cross-entropy, and entanglement entropy. Quantum tomographic entropy measures the informational completeness from HQN in terms of state reconstruction

$$H_T(Z) = 1 - \int_{\chi_Z} f_Z^2 dz. \quad (5.42)$$

This quantum entropy is derived from the purity of the reconstructed state transmitted through a hybrid quantum noisy channel. Quantum tomographic entropy reaches its maximum for pure states and decreases as the state becomes mixed, reflecting the loss of information in the reconstruction process.

Quantum conditional entropy is the quantum version of conditional entropy, measuring the amount of quantum information needed to describe a

part of a quantum system given another part. Quantum conditional entropy measures the amount of information necessary to describe the outcome of the random variable representing [HQN](#) Z , given that the random variable representing the received signal Y is known. It is defined as

$$H(Z|Y) = - \sum_{i,j} f(z_i, y_j) \log f(z_i|y_j). \quad (5.43)$$

Using the von Neumann entropy, the quantum conditional entropy measure is derived from the joint and marginal entropies of the system. Unlike its classical counterpart, conditional entropy can be damaging, indicating quantum entanglement. The quantum cross-entropy measures the difference between two probability distributions over the same set of events, often used in machine learning to define the loss function. It is defined as,

$$H(f_Z, f_Y) = - \sum_t f_Z(t) \log f_Y(t). \quad (5.44)$$

Topological entropy is used in dynamical systems to measure their complexity. It quantifies the rate at which information about the system's state is lost over time. Entanglement entropy is a key measure of quantum entanglement, providing insights into the quantum correlations between subsystems. The quantum entanglement entropy for a quantum channel is the von Neumann entropy of the reduced density matrix of the quantum channel.

These various entropy measures provide a comprehensive toolkit for analyzing the uncertainty, information content, and correlations in classical and quantum systems. Each entropy has unique properties and applications, contributing to our understanding of complex systems of quantum information science.

5.3.9 Quantum Mutual Information of Hybrid Quantum Noisy Channel

Mutual information in a communication channel quantifies the amount of information that can be obtained by observing the random variables of the transmitted signal, the received signal, and the noise in the channel. quantum mutual information ([QMI](#)) measures the total correlations between Alice and Bob, which can be defined in terms of quantum entropic measure [\[21\]](#), $I(X; Y) = H_X + H_Y - H(X, Y)$ and applying the chain rule for continuous variables, we have, $H(X, Y) = H(Y|X) + H_X$. Therefore, $I(X; Y) = H_Y - H(Y|X) = H_Y - H(X + Z|X) = H_Y - H(Z|X) = H_Y - H(Z) = H_Y - H_Z$ as transmitted signal X and noise Z are independent.

Quantum mutual information is always non-negative and quantifies classical and quantum correlations between the transmitter and receiver. This measure reflects the uncertainty about one part of the system, given knowledge of the other part. The key difference lies in the quantum context's handling of entanglement and nonclassical correlations. In summary, while

these entropies have different formulations and contexts, they exhibit equivalence or similar behaviour under certain conditions or limits, illustrating the interconnected nature of information measures in both classical and quantum domains.

This work examines whether the various quantum entropies mentioned are equivalent or share similar properties in the case of HQN. It has also discussed the conditions under which they coincide or approximate each other. This work provides mathematical proofs and discussions for the equivalence and similarities among the most commonly used quantum entropies of HQN, mainly focusing on their behaviour in the context of quantum information theory.

5.4 Application of Quantum Entropies in Quantum Tomography

Quantum tomography is a method for accurately reconstructing the transmitted signal from the received signal when it is affected by a hybrid quantum noisy channel. The process involves measuring the transmitted and received signals of the quantum communication network system and using these measurements to infer the density function that describes the HQN. The density function contains all the information needed to explain the input signal, including probabilities of different output signals and coherence between transmitted and received signals.

Quantum tomography is a key technique for reconstructing quantum states based on measurement, which is crucial for evaluating signal transmission through hybrid quantum noisy channels. Quantum entropies quantify uncertainty and information content, playing a vital role in assessing the accuracy of quantum state estimation. These entropy measures help analyze the fidelity of reconstructed states and refine estimation methodologies in the presence of noise effects. In quantum communication, tomography reconstructs the transmitted signal from the received signal, inferring the HQN density function. This function encodes information about output probabilities and coherence between transmitted and received signals. The fidelity of the reconstructed state is evaluated using quantum entropies, such as relative entropy and mutual information.

Quantum entropy aids in verifying and characterizing reconstructed states if an expected pure state exhibits nonzero entropy, it signals noise-induced errors. In multipartite systems, entropy measures help quantify entanglement properties. Process tomography further uses entropy to understand decoherence and noise characteristics, indicating information loss or gain. Additionally, relative entropy helps distinguish quantum states, providing insights into the impact of HQN. Quantum tomography enhances quantum communication by leveraging entropy measures, ensuring accurate state reconstruction and improved system performance. In quantum tomography, the fidelity of this reconstruction is crucial in quantum computing, quantum

communication, and quantum metrology, as it enables the reconstruction of a system's quantum state based on measurement data. Entropic measures play a crucial role in evaluating the accuracy of quantum state reconstruction, especially when the quantum system is exposed to HQN. In this scenario, we consider a hybrid noise model represented as a GMM weighted by a Poisson distribution. We describe the quantum state signal in terms of its p.d.f.

A transmitted quantum state X in phase space is represented by a p.d.f. $f_X(q, p)$, which satisfies

$$\int f_X(q, p) dq dp = 1 \quad (5.45)$$

where q, p are the quadratures of the quantum state. Under the influence of HQN, it is given by (5.4).

The observed quantum received state Y under a satellite hybrid quantum noisy channel is given by the convolution

$$f_Y(q, p) = \int T f_X(q', p') f_Z(q - q', p - p') dq' dp' \quad (5.46)$$

where $f_X(q', p')$ is the transmitted state distribution before HQN perturbation. To quantify the effects of HQN on state reconstruction, we analyze the entropy measures of the reconstructed density function $f_Y(q, p)$. The von Neumann entropy for a received quantum state Y represented by p.d.f. $f_Y(q, p)$ can be defined in the continuous-variable domain as

$$S(Y) = - \int f_Y(q, p) \ln f_Y(q, p) dq dp \quad (5.47)$$

A pure state X transmission implies $S(X) = 0$, whereas noise-induced mixed states increase entropy. In quantum tomography, if the reconstructed entropy $S(Y)$ is significantly larger than the actual entropy $S(W_{\text{true}})$, it indicates information loss due to hybrid noise. The relative quantum entropy (Kullback-Leibler (KL) divergence) between the actual X and the reconstructed quantum state signals Y measures the distinguishability of two probability distributions.

$$D_{\text{KL}}(f_X || f_Y) = \int f_X(q, p) \ln \frac{f_X(q, p)}{f_Y(q, p)} dq dp \quad (5.48)$$

A lower D_{KL} implies that the reconstructed quantum state Y closely approximates the actual quantum state X , while a higher value suggests significant deviation due to hybrid noise Z . Mutual information quantifies the amount of information preserved during the quantum tomography process.

$$I(f_X, f_Y) = S(f_X) - S(f_X | f_Y) \quad (5.49)$$

where $S(f_X | f_Y)$ represents the conditional entropy, accounting for uncertainties in reconstruction.

The Hybrid Quantum Noise (HQN) PDF in 3D

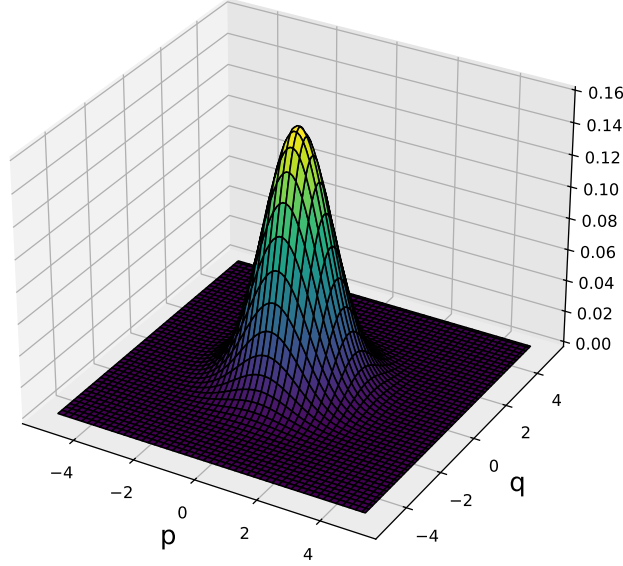


Figure 5.1: 3D representation of Hybrid Quantum Noise using Gaussian Mixture Model (GMM).

Quantum tomography and entropy measures provide a robust framework for evaluating and improving quantum state reconstruction under HQN. By leveraging entropy-based assessments such as von Neumann entropy, KL divergence, and mutual information, we can quantify the impact of Gaussian-Poisson noise models and optimize measurement strategies. These insights are crucial for quantum computing, secure quantum communication, and quantum metrology applications.

One standard method for state reconstruction is maximum likelihood estimation (MLE), which finds the state ρ_{MLE} that maximizes the likelihood of the observed data [18, 22]. Quantum entropies can evaluate the quality ρ_{MLE} by comparing its entropy to the actual state ρ_{true} . Bayesian inference is another approach that updates prior knowledge about the quantum state with measurement data to obtain a posterior distribution. Entropic measures, such as the KL divergence, can quantify the difference between the prior and posterior distributions, providing a measure of the information gained through the tomography process.

Quantum entropies provide a comprehensive framework for evaluating the performance and reliability of quantum state tomography. By quantifying the uncertainties and information content of reconstructed states, entropy measures enhance our understanding of the fidelity and efficiency of quantum state estimation. As quantum technologies advance, the inter-

The Differential Quantum Entropic Function for HQN

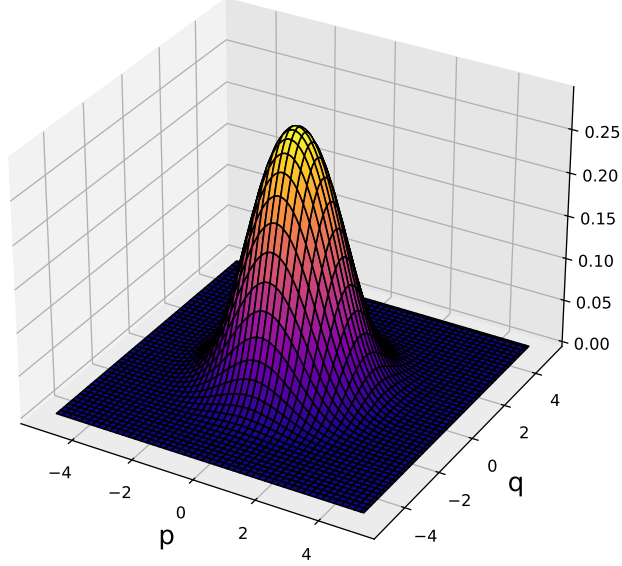


Figure 5.2: The 3D representation of the differential entropic function of HQN. This entropic function's integration gives the required differential entropy of the HQN.

play between quantum entropies and quantum tomography will continue to play a pivotal role in accurately characterizing and manipulating quantum systems.

5.5 Results and Analysis

We discussed earlier the graphical visualization of the different types of quantum entropies of HQN. Each entropy measure provides unique insights into the uncertainty and information content of quantum states, which are crucial for various applications in quantum information science. Analyzing quantum entropies in hybrid quantum noisy channels offers key insights into the performance of quantum communication. This section presents the results of the visual GMM representation of HQN.

This section analyses the graphical results of studying quantum entropies in hybrid quantum noisy channels. The visualizations illustrate how different entropy measures behave under the GMM representation of HQN, providing insights into quantum state uncertainty, coherence degradation, and entanglement characterization.

Fig. 5.1 shows the 3D representation of the HQN and the stochastic nature of the noise, which is modeled as a GMM with Poisson-distributed

The von Neumann Entropic Function for HQN

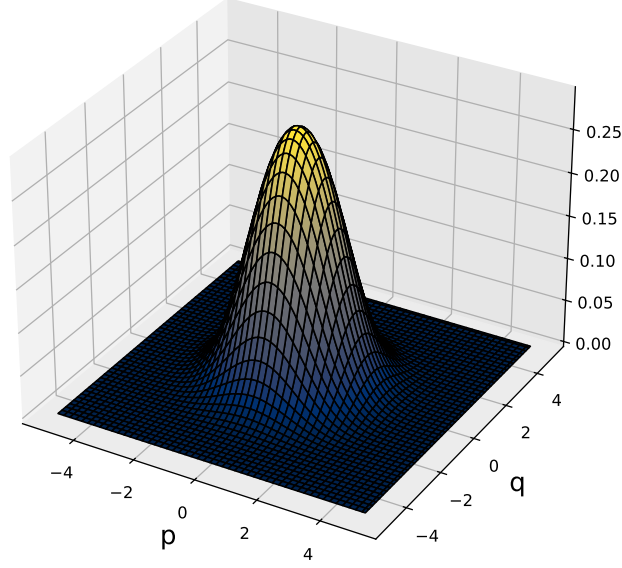


Figure 5.3: The 3D representation of the von-Neumann entropic function of HQN. This integration of the entropic function gives the required von Neumann entropy of the HQN.

weighting with $\lambda = 2$ and $R = 5$. This figure illustrates the [p.d.f.](#) of the [HQN](#), this representation captures the combined effect of Poisson-distributed quantum noise and [AWGN](#), which is crucial for modeling realistic quantum communication scenarios. The 3D visualization highlights the stochastic nature of the noise, with multiple Gaussian components contributing to the overall uncertainty.

In [Fig. 5.2](#), the differential entropy map for the [HQN](#) demonstrates how entropy varies across different regions of the noisy channel. Higher differential entropy values indicate regions of increased uncertainty, corresponding to areas where [HQN](#) significantly distorts the quantum state. The 3D structure suggests a complex interplay between quantum decoherence and classical noise contributions. This figure presents the differential entropy distribution over the [HQN](#). The entropy quantifies the uncertainty introduced by the GMM-based hybrid noise model. The results indicate that regions with higher noise variance exhibit increased differential entropy, suggesting a higher degree of disorder in the reconstructed quantum states.

[Fig. 5.3](#), the von Neumann entropy characterizes the mixedness of quantum states after passing through the hybrid noisy channel. The results reveal that regions of higher von Neumann entropy correspond to greater deco-

The Quantum Rényi Entropic Function for HQN ($\alpha=2$)

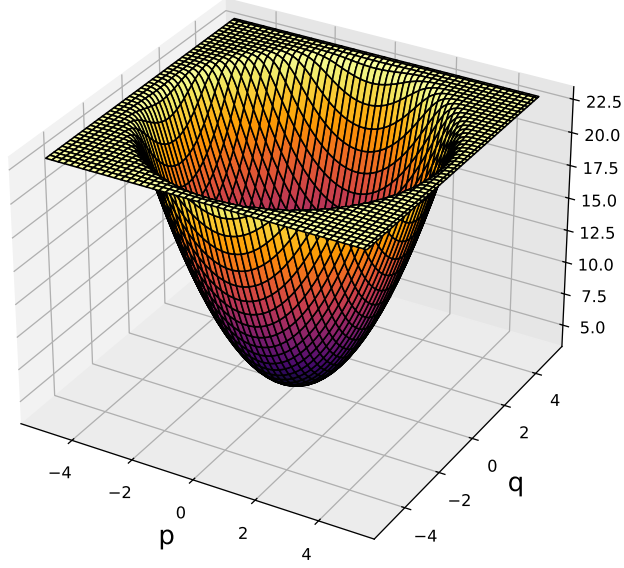


Figure 5.4: The 3D representation of the quantum Rényi entropic function of HQN. This entropic function's integration gives the required quantum Rényi entropy of the HQN.

herence and loss of quantum information. Compared to differential entropy, von Neumann's entropy provides additional insights into quantum state purity, making it essential for quantum tomography applications. This figure displays the von Neumann entropy computed from the density function of the GMM-based HQN. The von Neumann entropy of HQN provides a direct measure of the mixedness of the quantum state due to HQN perturbations. A comparison with differential entropy reveals that the von Neumann entropy exhibits a similar trend to the differential entropy of HQN, but it also accounts for quantum coherence properties. The results confirm that higher-entropy regions correspond to greater decoherence and information loss, which impacts QKD and entanglement-based communication.

Fig. 5.4, the Rényi entropy ($\alpha = 2$) highlights the effect of HQN on quantum information by emphasizing the contribution of dominant probability regions. The results indicate that Rényi entropy is more sensitive to noise fluctuations than differential entropy, making it a valuable measure for quantum error correction and QKD applications. This figure visualizes the function whose integration yields the Rényi entropy for $\alpha = 2$ in the case of HQN, offering an alternative perspective on uncertainty that emphasizes high-probability events more than differential entropy. The results show that the Rényi entropy of HQN is more sensitive to dominant Gaus-

The Quantum Tsallis Entropic Function for HQN ($q=2$)

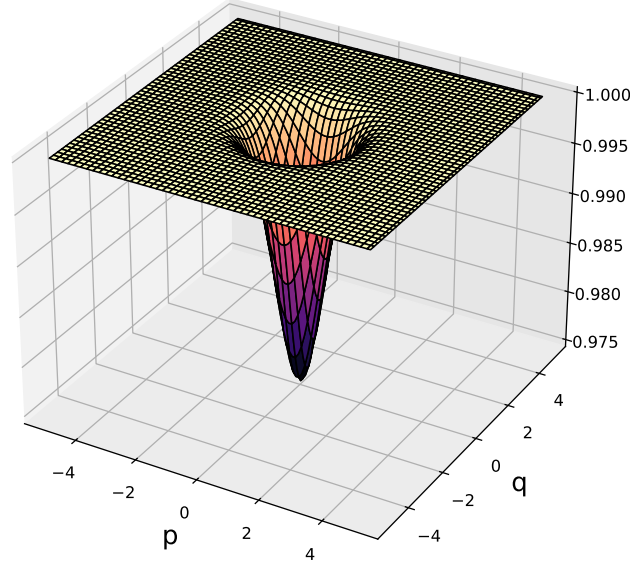


Figure 5.5: The 3D representation of the quantum Tsallis entropic function of HQN. This entropic function's integration gives the required quantum Tsallis entropy of the HQN.

sian components, making it helpful in evaluating entanglement security and noise suppression in quantum networks.

Tsallis entropy, a generalization of Shannon entropy, is crucial for quantifying uncertainty in quantum systems with non-extensive statistical properties. It provides insights into how HQN affects quantum communication channels under varying noise conditions. The 3D plot in Fig. 5.5 illustrates the Tsallis entropy distribution of HQN with parameter $q = 2$. The graph indicates that entropy is highly concentrated in specific regions of the phase space, suggesting that noise-induced uncertainty is not uniformly distributed throughout the phase space. This highlights the influence of structured noise patterns in quantum channels. Higher Tsallis entropy values indicate increased uncertainty in the evolution of quantum states due to hybrid noise. The entropy decreases in regions where noise-induced distortions are minimal, demonstrating the resilience of specific quantum states to noise interference. Compared to von Neumann entropy, Tsallis entropy emphasises rare events, making it a valuable tool for assessing worst-case noise scenarios in QKD and quantum error correction. Tsallis entropy helps identify optimal encoding schemes that minimise information loss under HQN conditions. It is instrumental in security analysis for QKD, where robustness against eavesdropping requires a precise understanding of entropy

The Quantum Collision Entropic Function for HQN

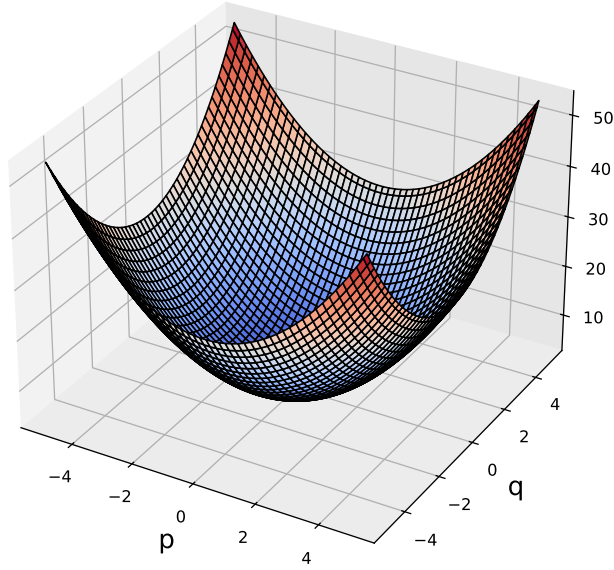


Figure 5.6: The 3D representation of the quantum collision entropic function of HQN. This entropic function's integration gives the required quantum collision entropy of the HQN.

fluctuations in the quantum channel. The results suggest that Tsallis entropy offers a more refined measure of noise-induced uncertainty, thereby enhancing quantum error mitigation strategies.

In Fig. 5.6, the collision entropy quantifies the likelihood of two randomly selected quantum states being identical in HQN. Higher entropy values indicate that the distinguishability of quantum states decreases due to noise interference. This trend has significant implications for quantum communication security, particularly in entanglement-based QKD protocols. This figure presents the function whose integration is the collision entropy of HQN, which quantifies the likelihood of two independently drawn quantum states being identical under hybrid noise conditions. The results reveal that higher noise variance leads to lower distinguishability between quantum states, impacting error rates in quantum communication.

Fig. 5.7, the tomographic entropy assesses the accuracy of quantum state reconstruction in noisy environments. Higher tomographic entropy values indicate increased information loss during the reconstruction process, making them a key metric for evaluating quantum tomography techniques under realistic noise conditions. This figure illustrates the function whose integration yields the tomographic entropy of HQN, evaluating the informational completeness of quantum state reconstruction. The observed patterns

The Quantum Tomographic Entropic Function for HQN

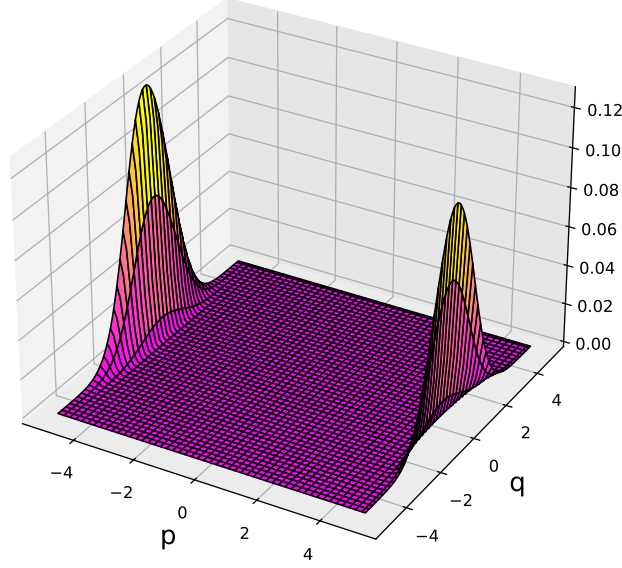


Figure 5.7: The 3D representation of the quantum tomographic entropic function of HQN. This entropic function's integration gives the required quantum tomographic entropy of the HQN.

suggest that higher-entropy regions correspond to increased errors in quantum tomography, underscoring the need for entropy-based noise mitigation strategies.

Fig. 5.8, the conditional quantum entropy measures the remaining uncertainty in a quantum state given prior knowledge of another correlated variable. The results reveal that higher entropy values correspond to more substantial quantum noise interference, suggesting reduced error correction and efficiency of entanglement distillation. This figure visualizes the function of the conditional quantum entropy of HQN and the received signal state, which quantifies the residual uncertainty of the quantum state given prior knowledge of another correlated variable. The results indicate that higher entropy values correspond to more substantial quantum noise interference, which reduces the efficiency of quantum error correction techniques.

The QMI quantifies the total correlation between two quantum subsystems, including both classical and quantum correlations. In the context of HQN, QMI provides a critical metric for evaluating the efficiency of information transfer. The 3D plot in Fig. 5.9 visualizes quantum mutual information between transmitted and received quantum states under HQN. The QMI function reveals how much information is preserved or lost due to noise interference. Higher QMI values correspond to regions where the im-

The Conditional Quantum Entropic Function for HQN

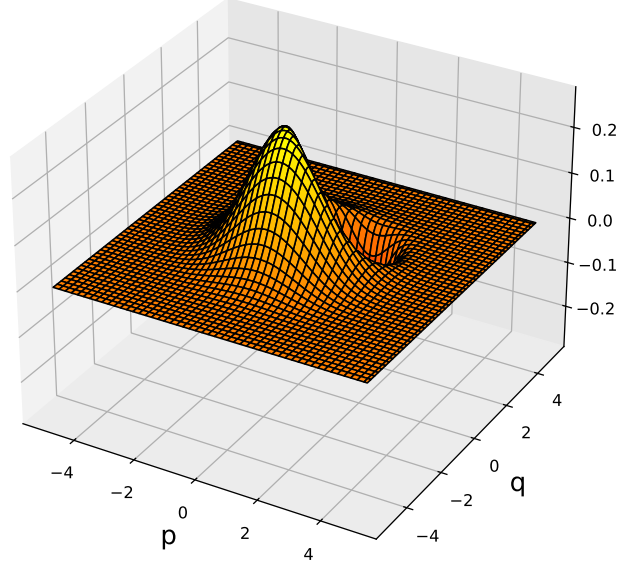


Figure 5.8: The 3D representation of the quantum conditional entropic function of HQN. The integration of this entropic function yields the required quantum conditional entropy of the HQN and the received quantum data.

pact of HQN is minimized, allowing for efficient quantum state transmission. In areas where QMI drops, quantum noise significantly affects the transmitted information, potentially degrading QKD performance. The results show that QMI is highly dependent on the SNR, with lower SNR values resulting in reduced information retention. A strong correlation between transmitted and received quantum states suggests that quantum entanglement can be better preserved under certain noise conditions. By analyzing QMI variations, optimal noise suppression techniques can be implemented to enhance quantum channel capacity. The study confirms that QMI is a powerful tool for characterizing the effects of HQN on secure quantum communication protocols, particularly in satellite-based QKD.

The results confirm that differential entropy converges to von Neumann entropy in the case of HQN under the continuous variable quantum regime, supporting the applicability of entropy reduction techniques for the satellite quantum channel in the context of quantum noise analysis. Higher entropy values indicate increased quantum bit error rates (QBER), which can compromise the security of CV-QKD protocols. The difference between von Neumann and differential entropy provides a quantitative measure of quantum state purity degradation, which is crucial for quantum tomography and entanglement verification. The entropy-based analysis offers a frame-

The Quantum Mutual Informatic Function for HQN

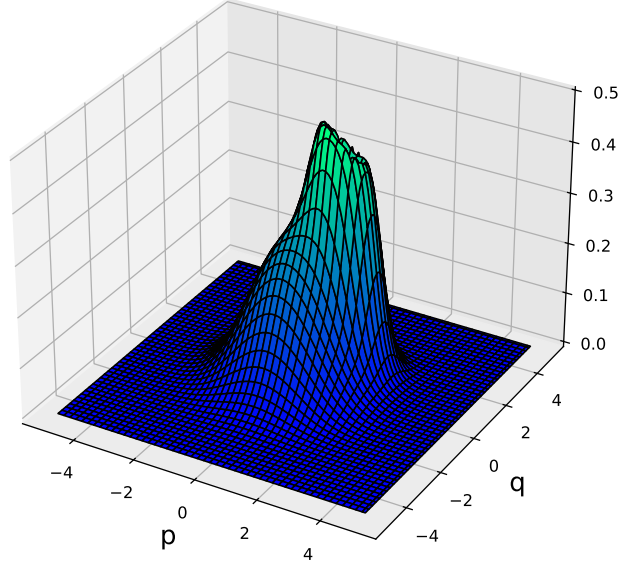


Figure 5.9: The 3D representation of the quantum mutual information function between transmitted quantum state data and the received quantum state data under HQN.

work for optimizing measurement strategies in quantum networks, ensuring robust transmission of quantum states with minimal decoherence. These quantum entropic analyses of the HQN system provide a refined understanding of noise-induced uncertainty, making them suitable for evaluating worst-case scenarios in quantum communication. Meanwhile, quantum mutual information serves as a crucial metric for assessing the reliability of quantum state transmission in the presence of HQN. These findings contribute to the development of optimized quantum communication protocols, ensuring more resilient and secure quantum networks. Future research should explore adaptive noise modeling techniques to enhance entropy-driven optimization in practical quantum communication systems.

In summary, the visualization and analysis of quantum entropy measures provide a comprehensive assessment of HQN effects on quantum communication and tomography. The results highlight the significance of entropy-based approaches in improving the optimization of quantum error correction, secure communication, and quantum state estimation techniques. Future research should focus on adaptive noise modeling techniques to mitigate entropy-induced quantum decoherence in practical quantum networks.

5.6 Conclusion

This chapter highlights the significance of entropy-based methods in improving [QBER](#), secure communication, and quantum state estimation techniques. Entropy visualizations offer invaluable insights into the impacts of [HQN](#) on quantum communication and quantum tomography. Utilizing these entropy metrics has led to notable progress in quantum satellite communication and [QKD](#), setting the foundation for a secure and effective quantum internet. Ongoing research and development in this domain are poised to unleash even more significant potential, revolutionizing how we transmit and safeguard information in the quantum age [99] [80] [15].

Future work should explore adaptive noise modeling strategies to minimize entropy-induced quantum decoherence in practical quantum networks. Leveraging these entropy measures has enabled significant advancements in quantum satellite communication and [QKD](#), paving the way for a secure and efficient quantum internet. Continued research and development in this field promise to unlock more significant water potential, transforming how we transmit and secure information in the quantum era [210] [24]. Chapter 6 explores the [HQN](#) cluster classification based on [GMM](#). It helps visualize [HQN](#) in higher dimensions and simplifies further calculations. Additionally, the [ML](#) algorithm updates the channel parameters and helps optimize the cluster and the achievable rate of a quantum channel.

Chapter 6

Optimization of Hybrid Quantum Noise Model

This chapter focuses on optimizing the hybrid quantum noise model (HQN) developed in Chapter 3, to improve the capacity of Gaussian quantum channels using ML generated clusters. The chapter leverages explicitly GMM and the EM algorithm to model the complex noise characteristics of quantum channels. HQN, which includes both quantum shot noise and classical AWGN, is modeled as an infinite mixture of Gaussian distributions weighted by Poissonian parameters. The chapter proposes a method to reduce the number of clusters within this noise model, simplifying visualization and improving the accuracy of channel capacity estimations without compromising essential noise characteristics. Key aspects include reducing Gaussian clusters while maintaining error tolerances and utilizing the EM algorithm to update quantum channel parameters, resulting in more accurate channel capacity estimates. The approach is validated through simulations, demonstrating that ML-enhanced quantum noise clustering significantly improves the channel's performance in satellite-based quantum communication systems, specifically for QKD. This chapter demonstrates that GMM and EM algorithms provide a practical solution for modeling quantum noise in real-time applications, advancing the optimization of quantum communication networks.

In this chapter, the proposed quantum channel optimization is highly effective for free-space optical satellite quantum communication, particularly in QKD. Chapter 4 has demonstrated that optimizing quantum noise components can be achieved through numerical optimization, which leads to ML-based clustering techniques. Leveraging optimised parameters significantly enhances quantum channel capacity and QKD rates, highlighting the practical relevance of this approach. An initial comparison with the K-Means algorithm was conducted, but the study primarily focused on the GMM-based EM algorithm for visualizing clustered datasets. Detailed analyses of clustering techniques, including the Elbow Method, Silhouette Analysis, and Gap Statistic, along with probabilistic approaches such as BIC and AIC, are discussed, emphasizing the evaluation of clustering qual-

ity and optimal cluster determination. The **GMM** framework, supported by the **EM** algorithm, was selected for its ability to iteratively optimize likelihood, handle missing data, and model overlapping clusters through soft probabilistic assignments. This makes it ideal for analyzing soft clustering in the **HQN** framework.

This chapter proposes an **ML** approach for visualizing **HQN** in higher dimensions. The previous chapters developed the **HQN** model and its approximation and visualized it in lower dimensions. This work validates the model and visualizes the **HQN** in 2 dimensions. In Chapter 3, the **HQN** model was expressed as an **GMM**, an infinite mixture of Gaussians with weights from a Poissonian distribution. In chapter 4, it has been described as a good approximation of the **p.d.f.** of the quantum noise that depends on the interrelation of the Poisson parameter and the number of Gaussian components [22]. In essence, the critical contributions of this chapter can be summarized in three main aspects:

- A **GMM-EM** based optimization framework for **HQN** clustering that achieves significant cluster reduction while preserving modeling accuracy and enabling effective noise visualization.
- Demonstration of achievable rate maximization in Gaussian quantum channels through optimized clustering and iterative parameter updates using the **EM** algorithm.
- Experimental validation showing superior performance of the proposed **GMM-EM** method compared to conventional machine learning approaches (K-means, DBSCAN) in quantum communication system optimization.

This chapter focuses on integrating **ML** techniques to optimize **HQN** clusters in quantum communication systems. This chapter enables the reduction of the noise model's complexity by utilizing **GMM** based **EM** algorithms, transforming an infinite mixture of Gaussians into a manageable finite model. This simplification allows for better visualization of quantum noise in higher dimensions and enhances the accuracy of quantum channel capacity estimation. In this work, we introduce a satellite quantum channel framework as a part of the application of the **HQN** channel in Section. However, a detailed discussion on **QKD** is considered for the future scope of this work.

6.1 System Model for the Quantum Communication Channel

6.1.1 Gaussian Quantum Channel Model

Let's return to the expression of a Gaussian channel, $\boldsymbol{\rho} \mapsto \mathbf{T}_{\mathbf{A}, \mathbf{Z}}(\boldsymbol{\rho})$, where $\mathbf{A}$ functions modulate the signal through amplification, attenuation, and rotational adjustments in phase space. Meanwhile, $\mathbf{Z}$ adds a noise component,

which includes both quantum noise (necessary to render the transformation physically meaningful) and classical noise. Intriguingly, $\mathbf{A}$ can be any real matrix, allowing any transformation $\rho \mapsto \mathbf{A}^T \rho \mathbf{A}$ to be approximated, provided that adequate noise is incorporated. As detailed, a simple quantum channel can be modeled as $\rho \mapsto \rho + \mathbf{Z}$, where $\mathbf{Z}$ includes both quantum and classical components of noise [21, 22]. Consider, $\mathbf{A} = \mathbf{I}_{2n}$ where $\mathbf{I}_{2n}$ is the identity matrix of order $2n \times 2n$ and n is the canonical degrees of freedom of the quantum system. $\mathbf{A}$ can be any real matrix; the transformation is valid as a quantum channel if enough noise is introduced [10]. In such a scenario, $\mathbf{A}^T \rho \mathbf{A}$ becomes scalar. The noise $\mathbf{Z}$ added to the system is also treated as a scalar from the convolution of [AWGN](#) and quantum Poisson noise with both components of the noises in scalar representation [21, 22]. Hence, this setup can be equated to the basic formula in communication theory where $Y = X + Z$, which represents the transmitted signal X , the received signal Y , and the [HQN](#) Z impacting the channel from various sources. In a practical quantum communication network handling classical information, it is presumed that the links are influenced by both quantum and classical noise. This noise is assumed to be additive, where $Z = Z_1 + Z_2$, with Z_1 being Poisson-distributed quantum shot noise and Z_2 representing Gaussian-distributed white classical noise [21, 22].

6.1.2 Hybrid Noise model

For quantum communication, it is essential to model the realistic quantum noise of a quantum channel. Previous studies have shown that quantum noise is often represented as Poissonian noise [207, 208, 209]. However, a practical quantum link also suffers from noise sources that contribute non-quantum noises, such as classical noise sources [62, 64, 65]. Classical noise is an integral part of the quantum channel and must be addressed to model a realistic quantum channel. In the semi-classical theory of photodetection, the shot noise level corresponding to Poissonian photoelectron statistics is the fundamental detection limit. Hence, the shot noise power level is often referred to as the quantum limit or the standard quantum limit of detection. Similarly, shot noise is often referred to as quantum noise [10, 11]. Considering the qubit noise as Poissonian and the classical noise as additive white Gaussian, one can expect a [HQN](#) represented by the following p.d.f. [21, 22],

$$f_Z(z) = \sum_{i=0}^{\infty} \frac{e^{-\lambda} \lambda^i}{i!} \frac{1}{\sigma_{Z_2} \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{z - i - \mu_{Z_2}}{\sigma_{Z_2}} \right)^2}. \quad (6.1)$$

6.1.3 Quantum Transmitted Signal Model

For the transmitted signal model, let us consider a Gaussian distributed signal for the [CV](#) system. Mathematically, a state is Gaussian if its distribution function in phase or its density operator in the Fock space is Gaussian

[21]. Examples of Gaussian functions are well-known [p.d.f.](#) of Normal distribution, Wigner function, etc. Important quantum information processing experiments are conducted using quantum light, which is described as being Gaussian distributed [10, 11]. In our model, the input quantum signal X in terms of qubits is in a Gaussian state, and it can be characterized by the scalar random variable X having a Gaussian distribution with parameters μ_X and σ_X , $X \sim \mathcal{N}(x; \mu_X, \sigma_X^2)$ the [p.d.f.](#) f_X of X can be expressed as [21, 22], $f_X(x) = \frac{1}{\sigma_X \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{x - \mu_X}{\sigma_X} \right)^2}$, where μ_X and σ_X are the distribution's mean and [s.d.](#).

6.2 Methodology of Quantum Noise Cluster Classification for Quantum Communication

6.2.1 Clustering with Gaussian Mixture Model

Let us start with the [HQN](#) model in (6.1),

$$f_Z(z) = \sum_{i=0}^{\infty} w_i \mathcal{N}(z; \mu_i^{(z)}, \sigma_i^{(z)^2}), \quad (6.2)$$

where $w_i = \frac{e^{-\lambda} \lambda^i}{i!}$ represent the weightage of the mixtures of Gaussians, $\sum_{i=0}^{\infty} w_i = 1$, $w_i \geq 0 \quad \forall i$ and $\mathcal{N}(z; \mu_i^{(z)}, \sigma_i^{(z)^2})$ is the Gaussian density in random variable Z , mean $\mu_i^{(z)} = \mu_{Z_2} + i$ and $\sigma_i^{(z)^2} = \sigma_{Z_2}^2$ with standard deviation $\sigma_i^{(z)}$ and variance $\sigma_i^{(z)^2}$. These lead to visualizing the noise model data in a scalar space or lower dimensions. In the meantime, this infinite mixture can be approximated by a finite number of components as

$$f_Z(z) = \sum_{i=0}^R w_i \mathcal{N}(z; \mu_i^{(z)}, \sigma_i^{(z)^2}). \quad (6.3)$$

This is the Gaussian mixture in the scalar variable Z , $w_i \geq 0 \quad \forall i$ and $\sum_{i=0}^R w_i \approx 1$ for large, R it depends on the Poisson parameter λ . However, a higher-dimensional approach is needed to visualize the original [HQN](#) data in the corresponding vector space as a scatter plot. This leads to the noise [p.d.f.](#) in a higher dimension given by the corresponding Gaussian mixture in a random vector $\mathbf{z} \in \mathbb{R}^D$ as

$$f_{\mathbf{Z}}(\mathbf{z}) = \sum_{i=0}^R w_i \mathcal{N}(\mathbf{z}; \boldsymbol{\mu}_i^{(z)}, \boldsymbol{\Sigma}_i^{(z)}), \quad (6.4)$$

where $w_i = \frac{e^{-\lambda} \lambda^i}{i!}$ represents the weightage of the Gaussian mixtures, $\mathbf{z}$ is the random vector in $\mathbb{R}^D$, D denotes the dimension of the vector $\mathbf{z}$, $\boldsymbol{\mu}_i^{(z)}$ is the mean vector, $\boldsymbol{\Sigma}_i^{(z)}$ is the covariance matrix of the corresponding Gaussian

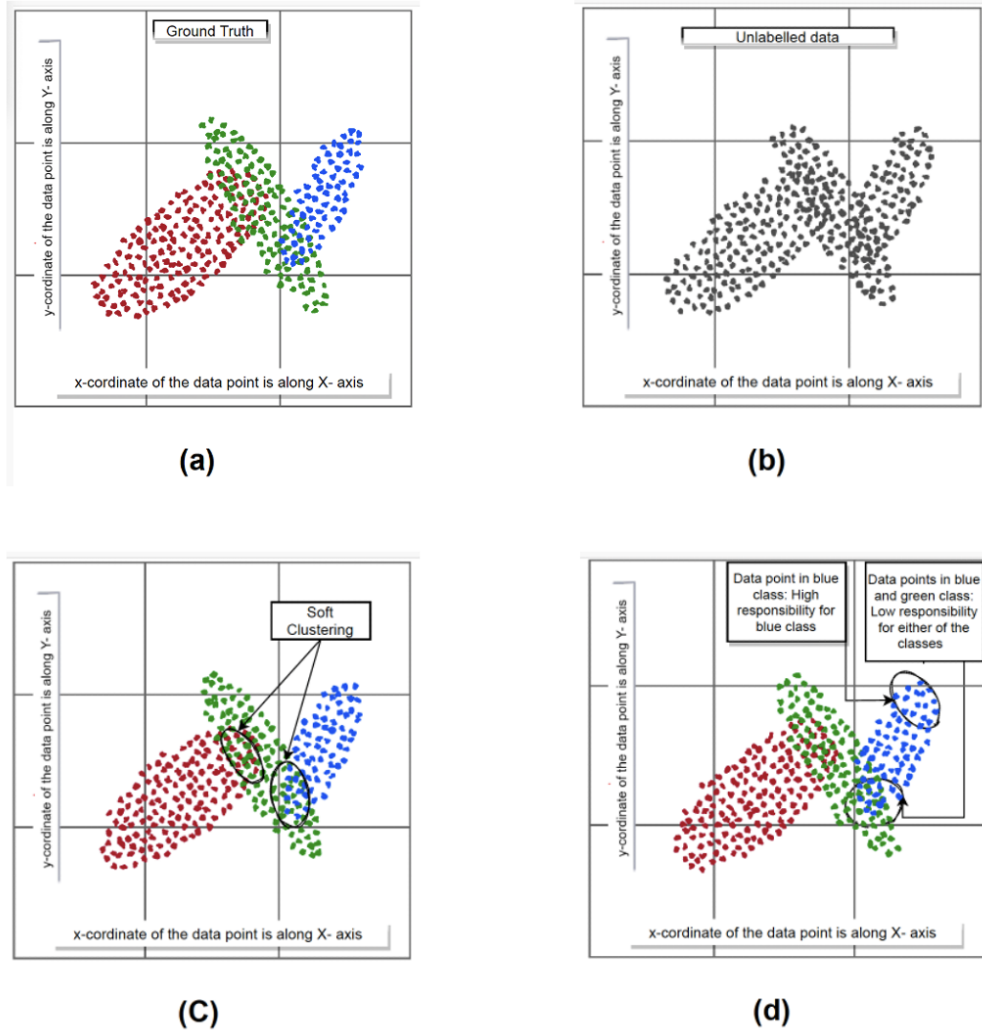


Figure 6.1: A generalized categorization of HQN data in two dimension space:
 (a) Original data (termed as Ground Truth) with specific cluster;
 (b) Unlabeled data for finding the original clusters;
 (c) GMM used for soft-clustering;
 (d) Responsibility of a cluster.

Note that the x-coordinates and y-coordinates of the bi-variate data points are considered along the graphs' X-axis and Y-axis.

density $\mathcal{N}$, and the multivariate Gaussian is given by $\mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)}) = \frac{1}{(2\pi)^{D/2} |\boldsymbol{\Sigma}_k^{(z)}|^{1/2}} e^{-\frac{1}{2}(\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)})^T \{\boldsymbol{\Sigma}_k^{(z)}\}^{-1} (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)})}$.

Consider the data set $\mathbf{Z} = \{\mathbf{z}_1, \mathbf{z}_2, \dots, \mathbf{z}_n\}$, $\mathbf{z}_i \in \mathbb{R}^D$, where D denotes the data points dimension, respectively. The primary purpose of this work is to understand the multidimensional HQN data set by partitioning it into K clusters, maximizing the likelihood of the probabilistic model. The HQN model in (6.4) can be expressed as $f_{\mathbf{Z}}(\mathbf{z}) = \sum_t f_{\mathbf{Z}}(\mathbf{z}, t) = \sum_t f_{\mathbf{Z}}(\mathbf{z}|t) f_{\mathbf{Z}}(t)$, where t is the latent variable, approximating the distribution with a Gaussian mixture. $f_{\mathbf{Z}}(\mathbf{z}|t)$ are Gaussian p.d.f., and $f_{\mathbf{Z}}(t)$ are mixing coefficients, these coefficients giving the weightage to the distribution $f_{\mathbf{Z}}(\mathbf{z}|t)$ with a particular probability of $f_{\mathbf{Z}}(t)$. Plugging over the $f_{\mathbf{Z}}(\mathbf{z}|t)$ with weightage $f_{\mathbf{Z}}(t)$, the resultant sum $\sum_t f_{\mathbf{Z}}(\mathbf{z}|t) f_{\mathbf{Z}}(t)$ represents the GMM, where $f_{\mathbf{Z}}(\mathbf{z}|t)$ is the posterior probabilities of the latent variable t given an observable $\mathbf{z}$. From (6.4), it guarantees the Gaussian distribution for each latent variable t 's conditional distribution $f_{\mathbf{Z}}(\mathbf{z}|t)$.

To use the EM algorithm for clustering components in the HQN dataset, a discrete random variable is introduced to assign data points to clusters (t , the t -th component of the mixture), ensuring that each cluster satisfies a Gaussian distribution with its parametric values. Ground truth in ML serves as the benchmark for training and evaluating models, ensuring accurate cluster assignments. In GMM-based clustering, the probability of a quantum data point $\mathbf{z}$ belonging to a specific cluster (e.g., red, green, or blue) is calculated. For classified data, points are colour-coded by cluster, as shown in Fig. 6.1(a), while unclassified data is shown in Fig. 6.1(b). When cluster assignment is uncertain, overlapping probabilities are represented by black circles (soft clustering) in Fig. 6.1(c). In this probabilistic framework, each data point is assigned a responsibility, the probability of belonging to a cluster, as depicted in Fig. 6.1(d). GMM excels in quantum-specific problems due to its soft probabilistic assignments ($[0, 1]$) compared to the complex classifications (0 or 1) of K-Means [33]. The EM algorithm is optimal for GMM, as it is tailored for probabilistic models and handles Gaussian-distributed data efficiently. This makes GMM and the EM algorithm ideal for quantum data classification, where soft clustering is preferred.

The p.d.f. of the GMM, which models the distribution of data points in a clustering scenario, is given by (6.4). The discrete latent variable $t_k \in \{0, 1\}$ for the K clusters is represented by the prior $f_{\mathbf{Z}}(t_k = 1) = \frac{e^{-\lambda} \lambda^k}{k!}$, $k \in [0, K]$, $\sum_{k=1}^K \frac{e^{-\lambda} \lambda^k}{k!} \approx 1$ for a sufficient choice of K . The clusters of the underlying components are Gaussians, with different parameters $f_{\mathbf{Z}}(\mathbf{z}|t_k = 1) = \mathcal{N}(\mathbf{z}; \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)})$. The quantity $t_k \in \{0, 1\}$ indicates whether the data point $\mathbf{z}$ belongs to the k -th class or not. Specifically, $t_k = 0$ means that $\mathbf{z}$ does not belong to the k -th class ($t_k \notin k$ -th class), and $t_k = 1$ means that $\mathbf{z}$ belongs to the k -th class ($t_k \in k$ -th class). The conditional density $f_{\mathbf{Z}}(\mathbf{z}|t_k = 0)$ is the density of $\mathbf{z}$ given that it does not belong to the k -th Gaussian component. The detailed calculation of $f_{\mathbf{Z}}(\mathbf{z}|t_k = 0)$ can be found in Appendix C. The probability that the data point $\mathbf{z}$

belongs to the k -th class is denoted by $f_{\mathbf{Z}}(t_k = 1)$. Consequently, the joint probability distribution of the data point $\mathbf{z}$ and the class membership t_k can be expressed as

$$f_{\mathbf{Z}}(\mathbf{z}, t_k = 1) = f_{\mathbf{Z}}(\mathbf{z}|t_k = 1)f_{\mathbf{Z}}(t_k = 1) = \frac{e^{-\lambda}\lambda^k}{k!}\mathcal{N}(\mathbf{z}; \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)}), \quad (6.5)$$

and the full generic model is given by

$$f_{\mathbf{Z}}(\mathbf{z}; w, \boldsymbol{\mu}, \boldsymbol{\Sigma}) = \sum_t f_{\mathbf{Z}}(\mathbf{z}, t) = \sum_k \frac{e^{-\lambda}\lambda^k}{k!}\mathcal{N}(\mathbf{z}; \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)}). \quad (6.6)$$

The posterior or conditional probability of t (the latent cluster) given a point $\mathbf{z}$ is

$$\begin{aligned} f_{\mathbf{Z}}(t_k = 1|\mathbf{z}) &= \frac{f_{\mathbf{Z}}(t_k = 1)f_{\mathbf{Z}}(\mathbf{z}|t_k = 1)}{f_{\mathbf{Z}}(\mathbf{z})} \\ &= \frac{f_{\mathbf{Z}}(t_k = 1)f_{\mathbf{Z}}(\mathbf{z}|t_k = 1)}{\sum_j f_{\mathbf{Z}}(t_j = 1)f_{\mathbf{Z}}(\mathbf{z}|t_j = 1)} = \frac{\frac{e^{-\lambda}\lambda^k}{k!}\mathcal{N}(\mathbf{z}; \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)})}{\sum_j \frac{e^{-\lambda}\lambda^j}{j!}\mathcal{N}(\mathbf{z}; \boldsymbol{\mu}_j^{(z)}, \boldsymbol{\Sigma}_j^{(z)})} = \gamma(z). \end{aligned} \quad (6.7)$$

After inferring a latent cluster for an observed point $\mathbf{z}$, probabilities can be assigned to this point that belongs to one of these unobserved clusters. $f_{\mathbf{Z}}(t_k = 1|\mathbf{z}) = \gamma(z)$ is the formula for obtaining the conditional posterior for the observed data point $\mathbf{z}$ that belongs to one of the latent clusters. Let's call $\gamma(z)$ the responsibility that class k takes to explain the data point $\mathbf{z}$.

The EM algorithm produced a set of these parametric values $w, \boldsymbol{\mu}^{(z)}, \boldsymbol{\Sigma}^{(z)}$ to infer the most optimal parameters and which parameters lead to the distribution that most likely explains the HQN data set. Therefore, it is necessary to define the log-likelihood function and to maximize it to find optimal parameters that describe the HQN dataset. The log-likelihood of the HQN can be expressed as

$$\ln f_{\mathbf{Z}}(\mathbf{z}; w, \boldsymbol{\mu}^{(z)}, \boldsymbol{\Sigma}^{(z)}) = \sum_{n=1}^N \ln \left(\sum_{k=1}^K \frac{e^{-\lambda}\lambda^k}{k!}\mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)}) \right), \quad (6.8)$$

where N is the total number of HQN data points named sample data. To maximize the log-likelihood function, in (6.8), the expression cannot be further simplified due to the logarithmic summation over the total number of clusters. However, one solution is to use the EM algorithm. One needs to improve the parameters and log-likelihood iteratively using this algorithm.

In Fig. 6.2, let's start with the HQN model p.d.f. $\rightarrow$ (1) Step: Ground Truth as quantum hybrid noise data generation using the p.d.f.. The next step will feed this data into the EM algorithm $\rightarrow$ (2) Step: Initialize the EM-algorithm with estimated values for the HQN parameters, and in the following stages, it delivers iteratively optimized parameters during the E-step and M-step. The algorithm's convergence gives the final optimized parametric values $\rightarrow$ (3). Step: Visualization of clusters gives the initial estimated clusters, followed by the intermediate and final optimized clusters.

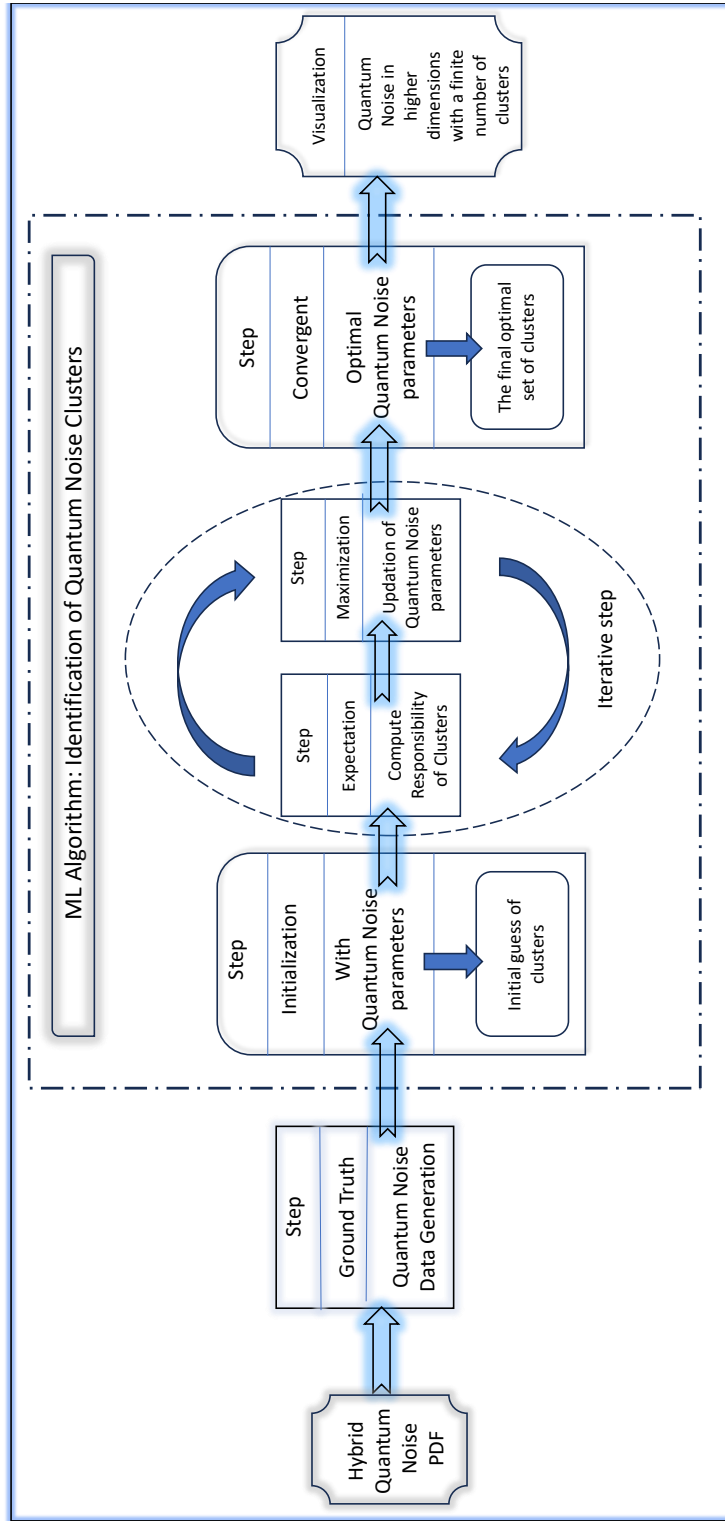


Figure 6.2: The process of updating channel parameters and finding optimal clusters of HQN using ML model.

6.2.2 Maximization of log-likelihood to find optimal parametric values for classifying the clusters:

It is necessary to maximize $\ln f_{\mathbf{Z}}(\mathbf{z}; w, \boldsymbol{\mu}^{(z)}, \boldsymbol{\Sigma}^{(z)})$ w.r.t. $\frac{e^{-\lambda}\lambda^k}{k!}, \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)} \forall k = 1(1)K$, where K is the total number of clusters. The problem is convex. Maximizing by looking for stationary points of logarithmic likelihood implies optimizing with respect to parameters $\frac{e^{-\lambda}\lambda^k}{k!}, \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)}$. Therefore, let's set the partial derivative of the log-likelihood function with respect to the mean vector $\boldsymbol{\mu}_k^{(z)}$ of the k -th class to zero $\frac{\partial}{\partial \boldsymbol{\mu}_k^{(z)}} \ln f_{\mathbf{Z}}(\mathbf{z}; w, \boldsymbol{\mu}^{(z)}, \boldsymbol{\Sigma}^{(z)}) = 0$, and solve it for $\boldsymbol{\mu}_k^{(z)}$. However, this equation does not have a closed-form solution. The stationary points depend on the posterior $\gamma(t_{n,k})$. It can find local minima using the so-called alternative update algorithm of the (expected) posterior iterative algorithm $\gamma(t_{n,k})$ and parameters maximization $\frac{e^{-\lambda}\lambda^k}{k!}, \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)}$.

If one takes the derivative of log-likelihood, it depends on the parameters $\boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)}$ and $\frac{e^{-\lambda}\lambda^k}{k!}$. Instead of this, one could write the solution for $\boldsymbol{\mu}_k^{(z)}$ as a function of responsibility $\gamma(t_{n,k})$, that is, $\frac{\partial}{\partial \boldsymbol{\mu}_k^{(z)}} \ln f_{\mathbf{Z}}(\mathbf{z}; \frac{e^{-\lambda}\lambda^k}{k!}, \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)}) = 0 \implies \boldsymbol{\mu}_k^{(z)}$ is a function of $\gamma(t_{n,k})$ and $\gamma(t_{n,k})$ depends on $\frac{e^{-\lambda}\lambda^k}{k!}, \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)}$. The proposed solution is to group all remaining parameters in this term of responsibility. Therefore, the term of responsibility still depends on other parameters $\frac{e^{-\lambda}\lambda^k}{k!}, \boldsymbol{\Sigma}_k^{(z)}$, even on $\boldsymbol{\mu}_k$. Using the EM algorithm to fix the posterior probability or the responsibility $\gamma(t_{n,k})$ and solve for the case $\boldsymbol{\mu}_k^{(z)}$ and all the other parameters, one can update the responsibilities and again iterate this solution for maximization and solve for the parameters.

Lemma 1 *The maximizing log-likelihood in (6.8) w.r.t. $\boldsymbol{\mu}_k^{(z)}$ by setting the derivative of the log-likelihood w.r.t. $\boldsymbol{\mu}_k^{(z)}$ to 0 that is $\frac{\partial}{\partial \boldsymbol{\mu}_k^{(z)}} \ln f_{\mathbf{Z}}(\mathbf{z}; w, \boldsymbol{\mu}^{(z)}, \boldsymbol{\Sigma}^{(z)}) = 0$, gives*

$$\boldsymbol{\mu}_k^{(z)} = \frac{\sum_{n=1}^N \gamma(t_{n,k}) \mathbf{z}_n}{\sum_{n=1}^N \gamma(t_{n,k})}. \quad (6.9)$$

Please refer to Appendix A.

Now, to maximize the log-likelihood with respect to the mixing coefficient, $\frac{e^{-\lambda}\lambda^k}{k!}$, we consider a constrained optimization problem using the Lagrange multiplier method. To maximize log-likelihood w.r.t. $\frac{e^{-\lambda}\lambda^k}{k!}$ let's set the derivative of the log-likelihood w.r.t. $\frac{e^{-\lambda}\lambda^k}{k!}$ to 0, under the constraint that the sum of the probabilities $\sum_{k=1}^K \frac{e^{-\lambda}\lambda^k}{k!}$, add up to one, that is, $\sum_{k=1}^K \frac{e^{-\lambda}\lambda^k}{k!} = 1$.

Let the Lagrange multipliers be denoted by

$$L(\frac{e^{-\lambda}\lambda^k}{k!}, \Lambda) := f(\mathbf{z}_n) + \Lambda(g(\mathbf{z}_n) - c), \quad (6.10)$$

where $f(\mathbf{z}_n) = \sum_{n=1}^N \ln f_{\mathbf{Z}}(\mathbf{z}_n; \frac{e^{-\lambda}\lambda^k}{k!}, \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)})$, $g(\mathbf{z}_n) = \sum_{k=1}^K \frac{e^{-\lambda}\lambda^k}{k!}$ and $c = 1$. Let us set the partial derivative of the Lagrange multipliers w.r.t.

$\frac{e^{-\lambda}\lambda^k}{k!}$ that is $\frac{\partial}{\partial w_k} L(w, \Lambda) = 0$ gives

$$\begin{aligned}
& \frac{\partial}{\partial \frac{e^{-\lambda}\lambda^k}{k!}} \left[\sum_{n=1}^N \ln f_{\mathbf{Z}}(\mathbf{z}_n; \frac{e^{-\lambda}\lambda^k}{k!}, \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)}) + \Lambda \left\{ \sum_{k=1}^K \frac{e^{-\lambda}\lambda^k}{k!} - 1 \right\} \right] = 0 \\
& \implies \sum_{n=1}^N \frac{\frac{\partial}{\partial \frac{e^{-\lambda}\lambda^k}{k!}} f_{\mathbf{Z}}(\mathbf{z}_n; \frac{e^{-\lambda}\lambda^k}{k!}, \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)})}{f_{\mathbf{Z}}(\mathbf{z}_n; \frac{e^{-\lambda}\lambda^k}{k!}, \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)})} + \Lambda \frac{\partial}{\partial \frac{e^{-\lambda}\lambda^k}{k!}} \left\{ \sum_{k=1}^K \frac{e^{-\lambda}\lambda^k}{k!} - 1 \right\} = 0 \\
& \implies \sum_{n=1}^N \frac{\frac{\partial}{\partial \frac{e^{-\lambda}\lambda^k}{k!}} \left[\sum_{k=1}^K \frac{e^{-\lambda}\lambda^k}{k!} \mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)}) \right]}{\sum_{k=1}^K \frac{e^{-\lambda}\lambda^k}{k!} \mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)})} + \Lambda \frac{\partial}{\partial \frac{e^{-\lambda}\lambda^k}{k!}} \left\{ \sum_{k=1}^K \frac{e^{-\lambda}\lambda^k}{k!} - 1 \right\} = 0 \\
& \implies \frac{e^{-\lambda}\lambda^k}{k!} = -\frac{1}{\Lambda} \sum_{n=1}^N \gamma(t_{n,k}).
\end{aligned} \tag{6.11}$$

Now let's solve it for Λ . For that, consider the constraint part $\sum_{k=1}^K \frac{e^{-\lambda}\lambda^k}{k!} = 1$. Now, setting derivative of the Lagrange multipliers w.r.t. Λ to zero, that is

$$\begin{aligned}
& \frac{\partial}{\partial \Lambda} L\left(\frac{e^{-\lambda}\lambda^k}{k!}, \Lambda\right) = 0 \implies \frac{\partial}{\partial \Lambda} \{f(\mathbf{z}_n) + \Lambda(g(\mathbf{z}_n) - c)\} = 0 \\
& \implies \sum_{k=1}^K \frac{e^{-\lambda}\lambda^k}{k!} - 1 = 0 \implies -\frac{1}{\Lambda} \sum_{n=1}^N \sum_{k=1}^K \gamma(t_{n,k}) = 1 \implies \Lambda = -N,
\end{aligned} \tag{6.12}$$

because $\sum_{k=1}^K \gamma(t_{n,k}) = \sum_{k=1}^K f_{\mathbf{Z}}(t_{n,k}|\mathbf{z}) = 1$, this is due to the sum of all classes. Finally, this gives us

$$w_k = \frac{1}{N} \sum_{n=1}^N \gamma(t_{n,k}). \tag{6.13}$$

Now let's calculate the expression for $\boldsymbol{\Sigma}_k^{(z)}$.

Lemma 2 *The maximization of the log-likelihood in (6.8) w.r.t. $\boldsymbol{\Sigma}_k^{(z)}$ by setting $\frac{\partial}{\partial \boldsymbol{\Sigma}_k^{(z)}} \ln f_{\mathbf{Z}}(\mathbf{z}; w, \boldsymbol{\mu}, \boldsymbol{\Sigma}) = 0$, gives*

$$\boldsymbol{\Sigma}_k^{(z)} = \frac{\sum_{n=1}^N \gamma(t_{n,k}) (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)}) (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)})^T}{\sum_{i=1}^N \gamma(t_{n,k})}. \tag{6.14}$$

Please refer to Appendix B. Now, define the effective number of points in cluster K by $N_k = \sum_{n=1}^N \gamma(t_{n,k})$. Hence, the solution for $\frac{e^{-\lambda}\lambda^k}{k!}, \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)}$

(dependent on the posterior) can be written as

$$\begin{aligned}
\boldsymbol{\mu}_k^{(z)} &= \frac{1}{N_k} \sum_{n=1}^N \gamma(t_{n,k}) \mathbf{z}_n, \\
\frac{e^{-\lambda} \lambda^k}{k!} &= \frac{N_k}{N}, \\
\boldsymbol{\Sigma}_k^{(z)} &= \frac{1}{N_k} \sum_{n=1}^N \gamma(t_{n,k}) (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)}) (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)})^T.
\end{aligned} \tag{6.15}$$

6.2.3 Expectation-Maximization Algorithm (EM):

The EM algorithm is a robust technique for estimating parameters in GMMs. This iterative algorithm comprises two primary steps: the expectation step (E-step) and the maximization step (M-step). Initially, the GMM parameters are established, which involve initialization of the means $\boldsymbol{\mu}_k^{(z)}$, covariances $\boldsymbol{\Sigma}_k^{(z)}$, and the probabilities of the mixture component expressed as $\frac{e^{-\lambda} \lambda^k}{k!}$ for each element k . In the E-step, the algorithm updates the expected posterior probabilities, or responsibilities $\gamma(z_{n,k})$, for each data point that concerns each mixture component. This step estimates the degree to which each component contributes to generating each data point. Subsequently, the M-step aims to maximize the model's log-likelihood given the current parameter estimates, adjusting $\boldsymbol{\mu}_k^{(z)}$, $\boldsymbol{\Sigma}_k^{(z)}$, and the probabilities based on the fixed posteriors established in the E-step. The algorithm alternates between these E and M steps until it meets a convergence criterion, such as a negligible change in the log-likelihood or after a specified number of iterations. This iterative process allows the EM algorithm to efficiently find local minima in the optimization landscape of the GMM parameter estimation problem. In our probabilistic framework, let's outline the EM algorithm within Algorithm 1.

6.2.4 The convergence of EM algorithm in the context of log-likelihood function

Convergence of the EM algorithm is typically understood in terms of the log-likelihood function of the observed data. In terms of monotonicity, the EM algorithm ensures that the log-likelihood function of the observed data does not decrease with each iteration [211]. Under general conditions, the EM algorithm converges to a local maximum (or saddle point in some cases) of the log-likelihood function. The convergence rate is typically linear but can slow near the maximum. The specific convergence rate can depend on the proximity of the initial parameter estimates to the actual values and the shape of the log-likelihood surface [212]. The convergence of the EM algorithm is guaranteed under certain regularity conditions, including certain log-likelihood function derivatives and the parameter space's boundedness. However, these conditions can sometimes only be strictly met in practice,

Algorithm 1: Expectation Maximization Algorithm for finding the optimal $\frac{e^{-\lambda}\lambda^k}{k!}, \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)}$

Input: $\lambda, \boldsymbol{\mu}_{k,0}^{(z)}, \boldsymbol{\Sigma}_{k,0}^{(z)}, k = 1(1)K$

Output: $\boldsymbol{\mu}_{k,m}^{(z)}, \boldsymbol{\Sigma}_{k,m}^{(z)}$

```

1  $m \leftarrow 1$ 
2 repeat
3   Calculate the responsibilities  $\gamma(z_{n,k,m})$  for each data point  $\mathbf{z}_n$ 
   and each component  $k$  according to
   
$$\gamma(z_{n,k}) = \frac{\frac{e^{-\lambda}\lambda^k}{k!}\mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)})}{\sum_{k=1}^K \frac{e^{-\lambda}\lambda^k}{k!}\mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)})};$$

4    $w_{k,m} = \frac{e^{-\lambda}\lambda^k}{k!} = \frac{1}{N} \sum_{n=1}^N \gamma(\mathbf{z}_{n,k,m});$ 
5    $\boldsymbol{\mu}_{k,m}^{(z)} = \frac{1}{N_k} \sum_{n=1}^N \gamma(\mathbf{z}_{n,k,m})\mathbf{z}_n;$ 
6    $\boldsymbol{\Sigma}_{k,m}^{(z)} = \frac{1}{N_k} \sum_{n=1}^N \gamma(\mathbf{z}_{n,k,m})(\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)})(\mathbf{z}_n - \boldsymbol{\mu}_{k,m}^{(z)})^T;$ 
7    $m \leftarrow m + 1;$ 
8 until convergence;
```

leading to convergence to local optima or, in rare cases, divergence if the assumptions are severely violated [125]. For practical considerations, the convergence of the EM algorithm is usually monitored by checking the change in the log-likelihood value or the change in parameter estimates between successive iterations.

6.2.5 Discussion on selecting GMM in comparison to existing ML models

In HQN modeling, GMM excels due to its flexibility, probabilistic approach, and ability to handle complex noise distributions. It effectively models overlapping clusters and multiple sub-populations, such as those influenced by quantum shot noise and classical AWGN [104]. Unlike K-means [33], which provides hard clustering, GMM's soft clustering assigns probabilities to each data point, accommodating the overlapping distributions standard in quantum noise. An initial comparison with the K-Means algorithm was performed in this article; however, the study primarily focused on the GMM-based EM algorithm for clustering visualization. Techniques such as the Elbow Method, Silhouette Analysis, Gap Statistic, and probabilistic approaches like BIC and AIC are explored for evaluating clustering quality and determining the optimal number of clusters. The GMM framework, combined with the EM algorithm, was chosen for its iterative likelihood optimization, ability to handle missing data, and effectiveness in modeling overlapping clusters with soft probabilistic assignments. The EM algorithm enhances GMM by iteratively optimizing parameters like means and variances, ensuring robust modeling of noisy or incomplete quantum data. Its computational efficiency and quadratic time complexity make it suitable for

real-time applications in quantum communication systems, such as satellite-based QKD [23, 24]. Compared to advanced ML techniques like DL or RL [31], or Bayesian inference [32], the EM algorithm offers a practical balance between complexity, computational demands, and accuracy, making it ideal for HQN modeling.

K-Means

K-Means is an unsupervised learning algorithm that partitions a dataset into K distinct, non-overlapping clusters. Each cluster is represented by the mean (centroid) of the points assigned to it. The algorithm aims to minimize the within-cluster sum of squares (WCSS), also known as the total intra-cluster variance [22].

Objective Function: Given a set of N quantum data points $\{z_1, z_2, \dots, z_N\} \subset \mathbb{R}^d$, the objective of K-Means is to minimize,

$$\arg \min_S \sum_{i=1}^K \sum_{z \in C_i} \|z - \mu_i\|^2 \quad (6.16)$$

where $C = \{C_1, C_2, \dots, C_K\}$ is the set of clusters, μ_i is the centroid of cluster C_i , defined as, $\mu_i = \frac{1}{|C_i|} \sum_{z \in C_i} z$, *Algorithm Steps:* (I) **Initialization:** Choose K initial centroids $\mu_1^{(0)}, \mu_2^{(0)}, \dots, \mu_K^{(0)}$ randomly. (II) **Assignment Step (E-Step):** (Assign each point z_j to the nearest centroid:) Assign z_j to cluster C_i where $i = \arg \min_i \|z_j - \mu_i\|^2$, (III) **Update Step (M-Step):** Recalculate the centroids using the current cluster members, $\mu_i = \frac{1}{|C_i|} \sum_{z \in C_i} z$, (IV) **Repeat:** Iterate steps 2 and 3 until convergence (i.e., no change in assignments or centroids).

In general, K-Means minimizes the squared Euclidean distance. It is sensitive to initial centroid selection and may converge to a local optimum. Assumes spherical, equally sized clusters. Fast and efficient, but not ideal for discovering complex or overlapping clusters.

DBSCAN

DBSCAN is a robust clustering algorithm that discovers clusters of arbitrary shape based on the density of data points. Unlike partitioning methods such as k -means, DBSCAN does not require the number of clusters to be specified a priori. It relies on two key parameters: ε , which defines the radius of a neighbourhood around a point, and $MinPts$, which specifies the minimum number of points required to form a dense region [22].

Given a point z_p in a dataset $\mathcal{D}$, the ε -neighborhood of z_p is defined as:

$$N_\varepsilon(z_p) = \{z_q \in \mathcal{D} \mid \|z_p - z_q\| \leq \varepsilon\} \quad (6.17)$$

A quantum data point z_p is called a *core point* if $|N_\varepsilon(z_p)| \geq MinPts$. If z_p is a core point and $z_q \in N_\varepsilon(z_p)$, then z_q is said to be *directly density-reachable* from z_p . Density-reachability is extended transitively: if there is a sequence

of points $z_1, z_2, \dots, z_n$ where each z_{i+1} is directly density-reachable from z_i , then z_n is *density-reachable* from z_1 .

However, density-reachability is not symmetric. To address this, **DBSCAN** defines two points z_p and z_q as *density-connected* if there exists a point z_o such that both z_p and z_q are density-reachable from z_o . Using these definitions, the algorithm clusters all density-connected points into the same group, and any point that is not density-reachable from any core point is labeled as noise.

The main strength of **DBSCAN** lies in its ability to discover clusters of arbitrary shape and to effectively handle outliers, which are treated as noise. Its performance, however, is sensitive to the selection of ε and *MinPts*, especially in datasets with varying density.

6.2.6 Model Evaluation Metrics

AIC, **BIC**, and the Silhouette Score are widely used metrics in statistical model selection and cluster evaluation. The **AIC** is a measure that evaluates the relative quality of a statistical model for a given dataset by balancing goodness-of-fit with model complexity. It is defined by the equation

$$\text{AIC} = 2\tilde{k} - 2\ln(\hat{L}), \quad (6.18)$$

where $\tilde{k}$ represents the number of estimated parameters in the model, and $\hat{L}$ denotes the maximized value of the likelihood function. A lower **AIC** value indicates a model that achieves a better trade-off between fit and simplicity. The **BIC** is similar in structure to **AIC** but introduces a more severe penalty for models with a larger number of parameters. It is given by

$$\text{BIC} = \tilde{k} \ln(N) - 2\ln(\hat{L}), \quad (6.19)$$

where N is the number of observations, $\tilde{k}$ is the number of parameters, and $\hat{L}$ is again the maximum likelihood of the model. The logarithmic dependency on N in the penalty term makes **BIC** more stringent, particularly as the sample size increases. In contrast to **AIC** and **BIC**, which are rooted in likelihood theory, the Silhouette Score is a geometric measure used for assessing the quality of clustering results. For each point i , the Silhouette Score is computed as

$$s(i) = \frac{b(i) - a(i)}{\max\{a(i), b(i)\}}, \quad (6.20)$$

where $a(i)$ is the average intra-cluster distance, i.e., the average distance between point i and all other points within the same cluster, and $b(i)$ is the minimum average distance from point i to all points in any other cluster, representing the nearest neighboring cluster. The score $s(i)$ ranges from -1 to 1 , with higher values indicating that the point is well-matched to its own cluster and poorly matched to neighbouring clusters. Collectively, these metrics provide a comprehensive toolkit for evaluating model fit and the coherence of clustering outcomes [22].

6.3 Application in Maximization of Quantum Channel Capacity

The interplay between the Poisson parameter and the [GMM](#) is fundamental to accurately simulating quantum noise in quantum channel modeling. The Poisson parameter, λ , quantifies the average photon count detected over a specific interval, highlighting the quantum nature of light and the stochastic process of photon emission and detection. This parameter is essential for modeling photon statistics in quantum optics [207, 208], where photon arrivals at a detector are typically Poisson distributed, reflecting the quantized nature of light. On the contrary, the [GMM](#) provides a probabilistic framework for modeling quantum noise, encompassing both quantum and classical noise influences on quantum states during transmission. This allows for a more comprehensive representation of various noise sources and their statistical behaviours in a quantum channel [11, 21, 22]. The connection between these two models lies in their joint capability to more accurately represent the complexity of quantum noise. Although the Poisson parameter λ captures the quantum mechanical aspects of the photon distribution, the [GMM](#) accounts for a broader range of noise scenarios, including classical noise effects such as thermal noise and detector inefficiencies [198]. This blend facilitates nuanced understanding and optimization of quantum channels, enabling the development of sophisticated error correction codes and communication protocols tailored to mitigate the specific noise characteristics encountered in quantum information transfer.

Taking into account [HQN](#) and the Gaussian transmitted signal model as discussed above [21, 22], the capacity of the quantum channel can be expressed as follows,

$$C = \sum_{i=0}^R \frac{e^{-\lambda} \lambda^i}{i!} \left(-\log_2 \left(\frac{e^{-\lambda} \lambda^i}{i!} \right) + \frac{1}{2} \log_2 \left((2\pi e)^M |\Sigma_i^{(y)}| \right) + \log_2 \left(\sum_{j=0}^R \frac{e^{-\lambda} \lambda^j}{j!} \mathcal{N}(\mu_i^{(z)}; \mu_j^{(z)}, \Sigma_i^{(z)} + \Sigma_j^{(z)}) \right) \right). \quad (6.21)$$

This formula delineates the capacity of the quantum channel for scenarios where both the noise $\mathbf{Z}$ and the received signal $\mathbf{Y}$ are represented as random vectors of dimension size M . In scalar analogy, that is, when the noise Z has scalar [p.d.f.](#), the expression of capacity is reduced to

$$C = \sum_{i=0}^R \frac{e^{-\lambda} \lambda^i}{i!} \left[-\log_2 \left(\frac{e^{-\lambda} \lambda^i}{i!} \right) + \frac{1}{2} \log_2 \left(2\pi e \sigma_i^{(y)} \right) + \log_2 \left(\sum_{j=0}^R \frac{e^{-\lambda} \lambda^j}{j!} \mathcal{N}(\mu_i^{(z)}; \mu_j^{(z)}, \sigma_i^{(z)^2} + \sigma_j^{(z)^2}) \right) \right], \quad (6.22)$$

by putting $M = 1$, and replacing $|\Sigma_i^{(y)}|$ by $\sigma_i^{(y)}$, $\mu_i^{(z)}$ by $\mu_i^{(z)}$, $\mu_j^{(z)}$ by $\mu_j^{(z)}$, $\Sigma_i^{(z)}$ by $\sigma_i^{(z)^2}$ and $\Sigma_j^{(z)}$ by $\sigma_j^{(z)^2}$, where each vector is replaced by its scalar

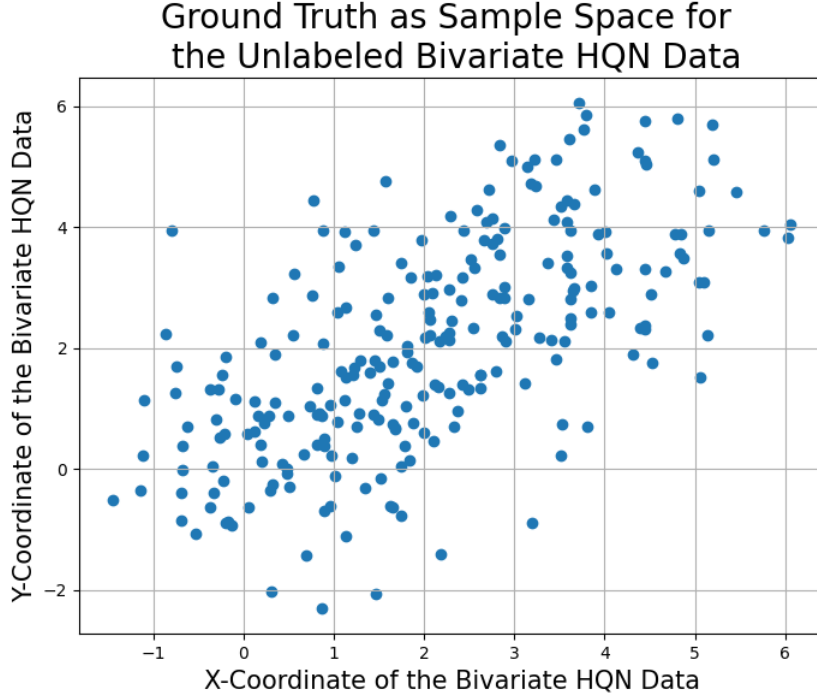


Figure 6.3: The ground truth data of bivariate quantum noise sampling generated as a convolution of additive white Gaussian noise and Poissonian quantum noise. In our studies, the ground truth of the HQN data has been generated from the component GMMs.

analogue [21, 22]. Again $\mu_i^{(z)} = \mu_{Z_2} + i \forall i$, $\sigma_i^{(z)^2} = \sigma_{Z_2}^2 \forall i$, and $\sigma_i^{(y)^2} = \sigma_X^2 + \sigma_{Z_2}^2 \forall i$. Therefore, the capacity of the quantum channel is given by,

$$C = \sum_{i=0}^R \frac{e^{-\lambda} \lambda^i}{i!} \left[-\log_2 \left(\frac{e^{-\lambda} \lambda^i}{i!} \right) + \frac{1}{2} \log_2 \left(2\pi e (\sigma_X^2 + \sigma_{Z_2}^2) \right) + \log_2 \left(\sum_{j=0}^R \frac{e^{-\lambda} \lambda^j}{j!} \frac{1}{\sqrt{2\sigma_{Z_2}} \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{i-j}{\sqrt{2\sigma_{Z_2}}} \right)^2} \right) \right]. \quad (6.23)$$

Application in Satellite Quantum Channel's Achievable Rate Enhancement

From this generalized description of a quantum channel, we can drive towards the atmospheric FSO satellite quantum channel model represented by the following equation [23, 26],

$$Y = TX + Z, \quad (6.24)$$

where the quantum channel transmitted signal is given by random variables X , representing Alice's inputs, and the received signal Y at Bob's side, Z is the HQN given by (6.1), where T is the overall transmission coefficient

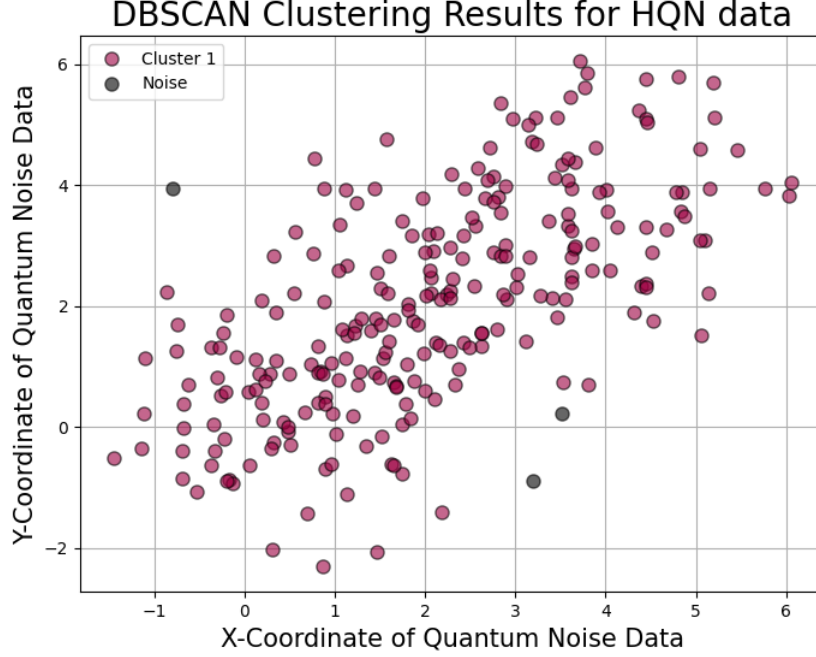


Figure 6.4: HQN data clustering under [DBSCAN](#).

for the single use of the quantum channel. The focus should be on the transmission coefficient T (with the transmission efficiency $\tau = T^2$). This model captures the complexity of satellite quantum communication, underscoring the importance of accounting for various noise sources and channel imperfections in ensuring secure communication.

Considering the [HQN](#) and the Gaussian transmitted signal model as discussed above, the achievable rate of the quantum channel can be expressed as follows [23, 24],

$$C_S = \sum_{j=0}^R \frac{e^{-\lambda} \lambda^j}{j!} \left(-\log_2 \left(\frac{e^{-\lambda} \lambda^j}{j!} \right) + \frac{1}{2} \log_2 \left(2\pi e (T^2 \sigma_X^2 + \sigma_{Z_2}^2) \right) \right. \\ \left. + \log_2 \left(\sum_{l=0}^R \frac{e^{-\lambda} \lambda^l}{l!} \cdot \frac{1}{\sqrt{2\sigma_{Z_2}} \sqrt{2\pi}} e^{-\frac{1}{2} \left[\frac{j-l}{\sqrt{2\sigma_{Z_2}}} \right]^2} \right) \right), \quad (6.25)$$

where

$$\mathcal{N}(\mu_{Z_2} + j; \mu_{Z_2} + l, 2\sigma_{Z_2}^2) = \frac{1}{\sqrt{2\sigma_{Z_2}} \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{\mu_{Z_2} + j - l - \mu_{Z_2}}{\sqrt{2\sigma_{Z_2}}} \right)^2}. \quad (6.26)$$

6.4 Results and Numerical Analysis

In this numerical section, we have visualized the implementation of the model. In the first part, we discussed how to visualize [HQN](#) in terms of

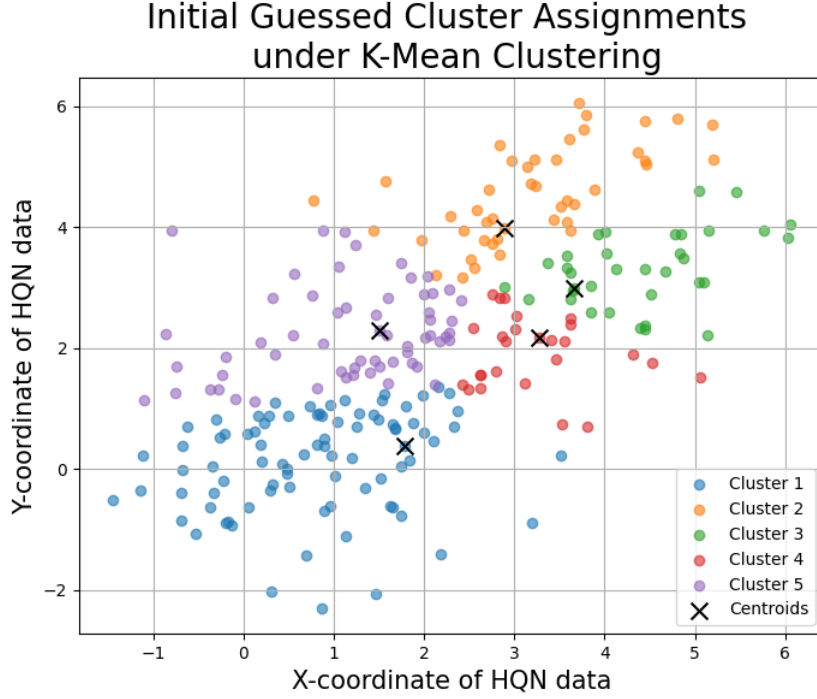


Figure 6.5: Initial K-means setup: Five random centroids (eyes) define starting cluster means for HQN data points.

Gaussian mixture clusters with weightage from a Poisson distribution and updated the parameters associated with the channel’s achievable rate. In the second part, we investigated how the achievable rate changes with updated parametric values in relation to the initial guess of parameters, leading to the final contribution of this work in terms of the improved achievable rate of the quantum channels.

Note that the Section 6.1, it considered the dimension reduction in the qubit. This representation leads to 1-D qubit and the corresponding scalar p.d.f.. However, to visualize the sample from vectorized p.d.f., we consider the bivariate quantum-noise data sampled from eq (6.4) shown in Fig. 6.3. The bivariate HQN data sample has been plotted, where the X-axis and Y-axis of the plots represent the X-coordinate and Y-coordinate of the bivariate qubit vectors.

6.4.1 Performance Comparison between DBSCAN, K-means, and GMM-assisted EM Algorithm

In Fig. 6.3, the ground truth of the HQN dataset is shown; the quantum noise samples are generated as a convolution of quantum Poisson noise and classical AWGN. These data points are inherently probabilistic, with overlapping distributions and varying densities, making them ideal candidates for soft clustering techniques. The goal is to identify meaningful clusters within this complex noise structure to better model quantum channel characteristics and ultimately enhance the communication achievable rate.

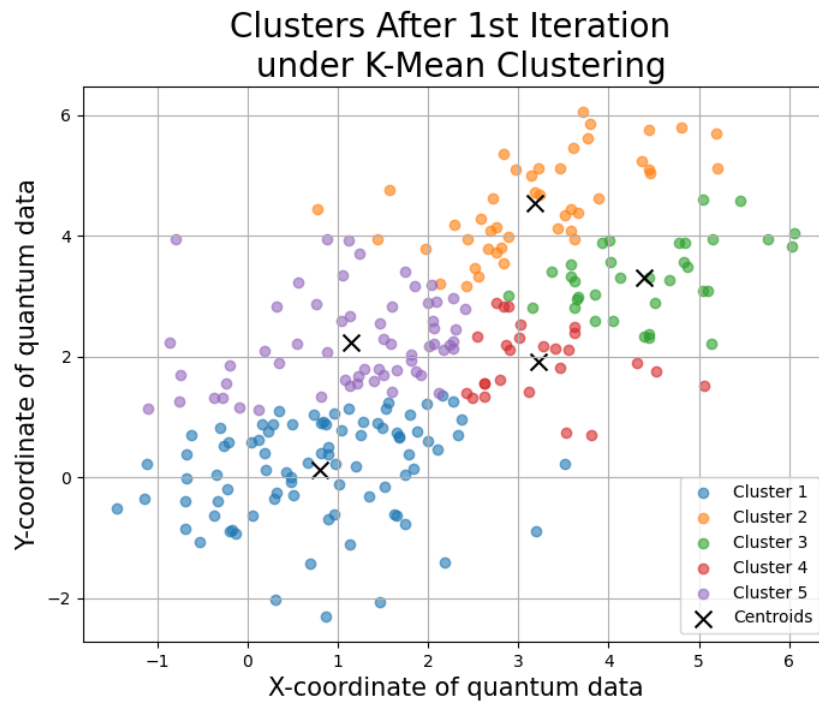


Figure 6.6: Clusters after 1st iteration under K-Mean.

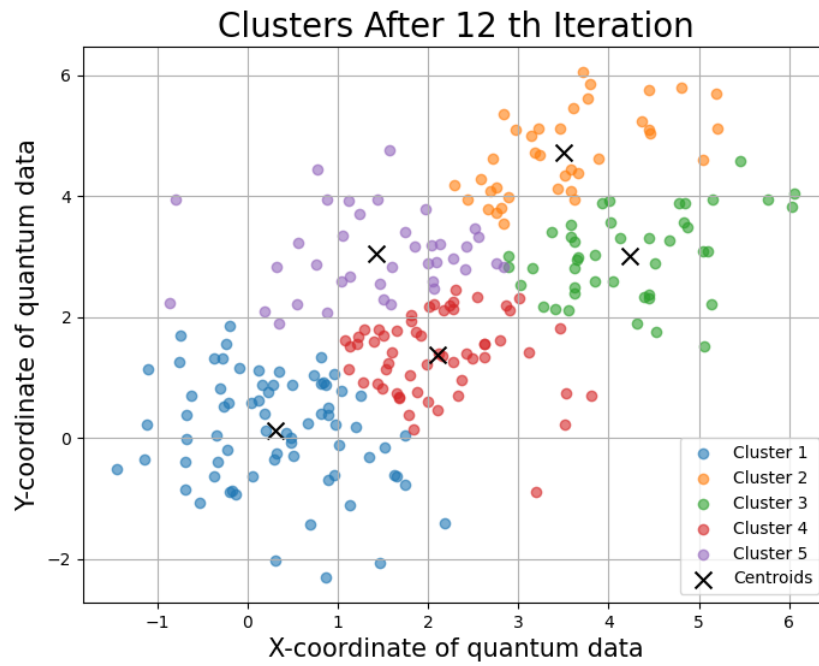


Figure 6.7: After 12th iterations: Centroids shift toward data-dense regions with improved cluster separation.

Final Clusters at 24 th Iteration under K-Mean Clustering

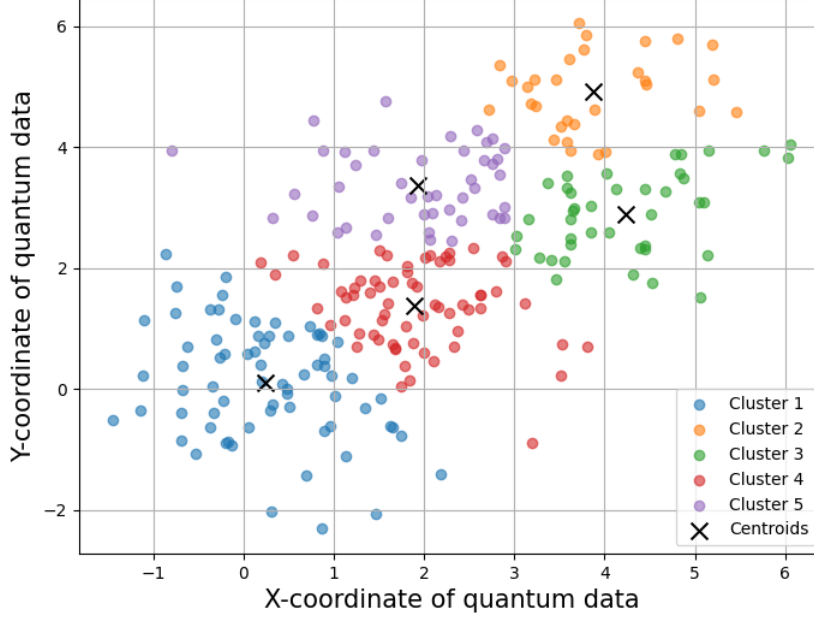


Figure 6.8: Convergence at iteration 24th: Stabilized centroids minimize within-cluster variance, yielding five distinct clusters representing dominant quantum noise modes.

The first approach attempted is [DBSCAN](#), a density-based clustering algorithm. It relies on two parameters: (the radius of the neighbourhood) and MinPts (the minimum number of points required to form a dense region). [DBSCAN](#) calculates the ϵ -neighborhood for each point and labels core points, reachable points, and outliers based on their density. However, when applied to the [HQN](#) dataset, [DBSCAN](#) fails to produce meaningful clusters, shown in Fig. 6.4. The reason for its failure lies in the inherent complexity and overlapping nature of quantum noise data. [DBSCAN](#) assumes uniform density across clusters and is highly sensitive to ϵ and MinPts. Because the [HQN](#) data exhibits non-uniform densities and high overlap among noise-induced distributions, [DBSCAN](#) either merges distinct clusters into one or labels a majority of points as noise, thereby failing to separate the quantum noise features effectively.

Next, the K-Means algorithm is applied, which partitions the dataset into 5 clusters by minimizing the within-cluster variance. The algorithm starts with an initial guess for centroids and iteratively assigns data points to the nearest centroid, recalculating the centroids in each iteration. While K-Means offers a more transparent structure than [DBSCAN](#), it fundamentally assumes that clusters are spherical and equally sized, shown in Fig. 6.5 to 6.8. As a result, it treats all clusters with equal importance and converges toward the geometric centre of each partition. This non-probabilistic approach proves inadequate for the [HQN](#) dataset. The [HQN](#) data contains clusters of varying density and overlapping boundaries, which K-Means cannot capture. Even when the number of clusters is correctly set to $K = 5$,

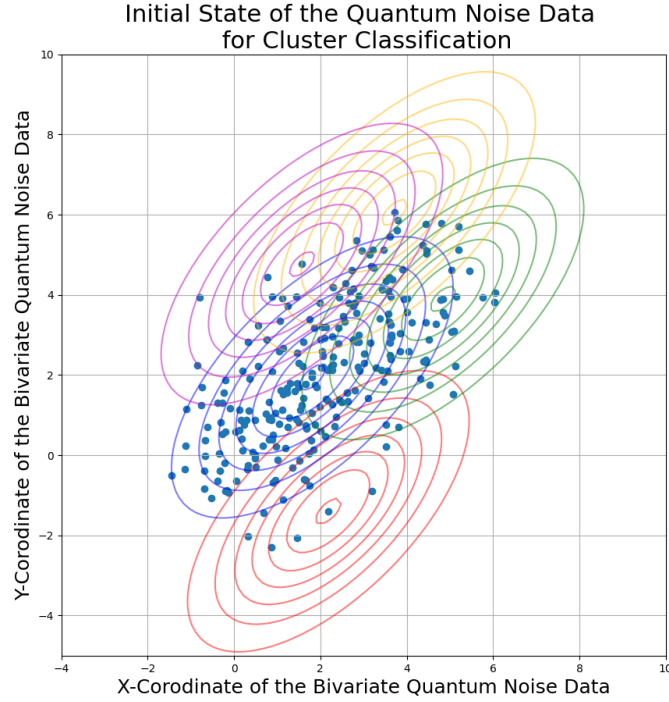


Figure 6.9: Initial Gaussian mixture clusters: Five colored spiral datasets with centroids (eyes) representing initial Gaussian component means.

as suggested by methods like the Elbow and Silhouette analyses, K-Means produces nearly equal-sized clusters without considering the actual statistical weight (e.g., Poissonian weightage) of each cluster. This results in a rigid partitioning that distorts the probabilistic nature of the HQN.

The comparison between K-Means and the GMM-assisted EM algorithm highlights the limitations of K-Means. While the Elbow Method and Silhouette Analysis suggest the optimal number of clusters as five in both models, probabilistic evaluation criteria such as the AIC and BIC strongly favour the GMM. K-Means lacks the statistical depth to accurately model varying cluster shapes and sizes, which is critical for quantum noise, where each Gaussian component is weighted according to a Poisson distribution. The key limitation of K-Means is its assumption of spherical, equally sized, and separable clusters. For the HQN dataset, where data points often fall into overlapping or skewed distributions, these assumptions do not hold. When K-Means is applied with $K = 5$, the resulting clusters are split evenly regardless of their true statistical significance, ignoring the underlying structure and leading to misleading interpretations.

In contrast, the GMM-based EM algorithm excels because it assigns probabilistic weights (responsibilities) to each data point relative to every cluster. This soft clustering approach allows it to model overlapping and variably weighted Gaussian components, making it ideal for HQN data where Poissonian weightage plays a critical role. GMM can refine cluster parameters (means, covariances, and weights) iteratively to better match the actual distribution, leading to significantly improved channel achievable rate estimations. Additionally, GMM integrates well with statistical model

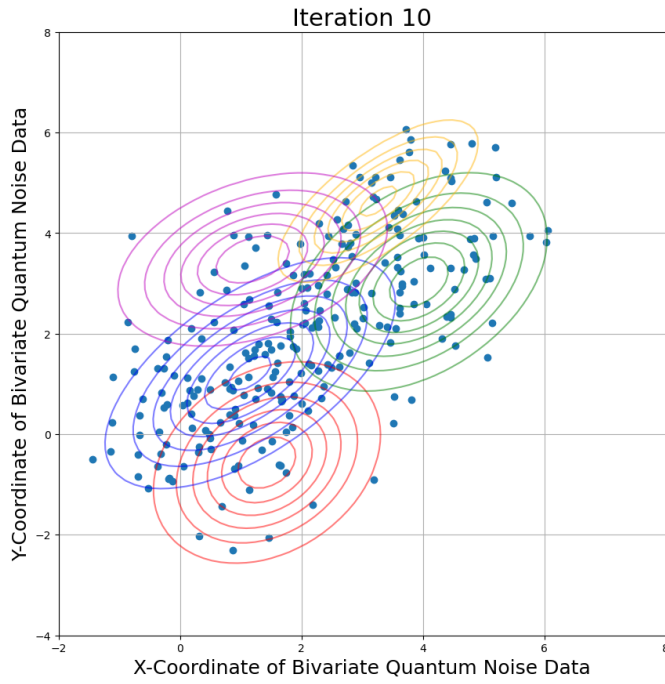


Figure 6.10: After 10 iterations: Updated Gaussian mixture components for bivariate quantum noise clustering.

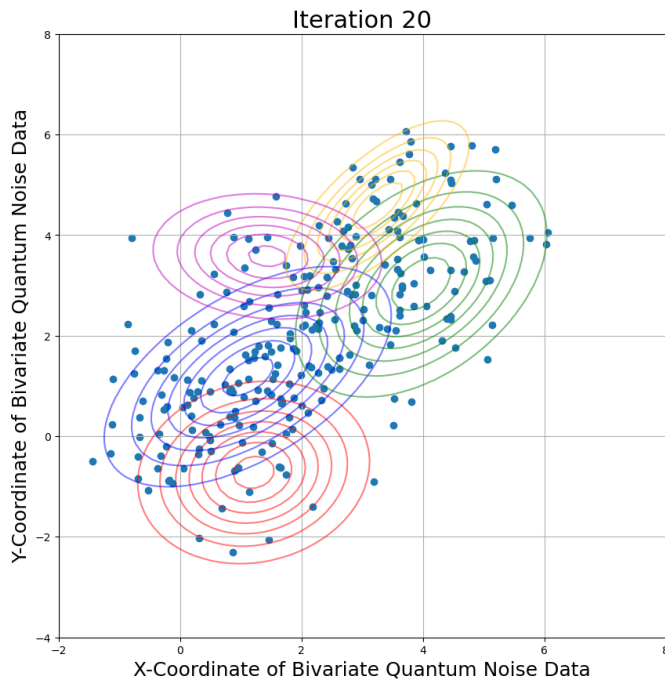


Figure 6.11: Final result at iteration 20: Converged Gaussian mixture clusters.

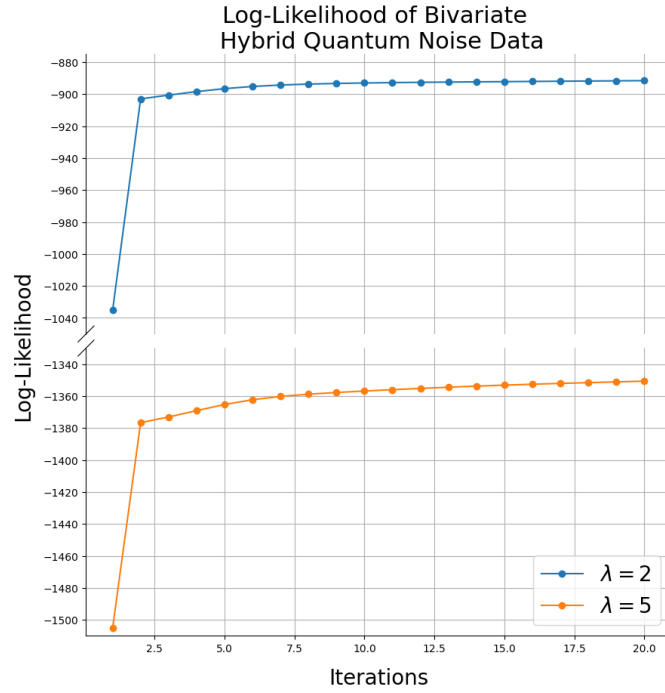


Figure 6.12: Log-likelihood convergence: EM algorithm convergence curves for $\lambda = 2$ and $\lambda = 5$, with curve saturation indicating cluster optimization completion.

selection tools like AIC and BIC to determine the optimal number of clusters while penalizing model complexity, a feature unavailable in K-Means and DBSCAN.

Regarding computational complexity, K-Means is the simplest, with linear time complexity $O(N \cdot K \cdot s)$, where N is the number of data points, K the number of clusters, and s the number of iterations. DBSCAN has a higher complexity, $O(N \log N)$, due to the spatial indexing required for neighbourhood queries, but is generally more robust for large datasets. GMM with EM has the highest complexity, typically $O(N \cdot K \cdot d^2 \cdot s)$, where d is the data dimensionality. Despite this, the GMM's superior performance in capturing complex, overlapping, and probabilistically weighted noise structures justifies its computational overhead, especially in applications involving quantum noise modeling where precision is paramount [165, 166, 213]. However, in the case of quantum datasets, the complexity of these algorithms is under investigation.

The optimal number of cluster identifications using different Machine learning evaluation metrics

Determining the optimal number of clusters (K) is a critical step in unsupervised learning, as it directly impacts the performance and interpretability of clustering algorithms. This study began with 10 initial clusters generated to represent the complexity of HQN data. Through a detailed analysis incorporating several established methods, it was determined that $K = 5$ was

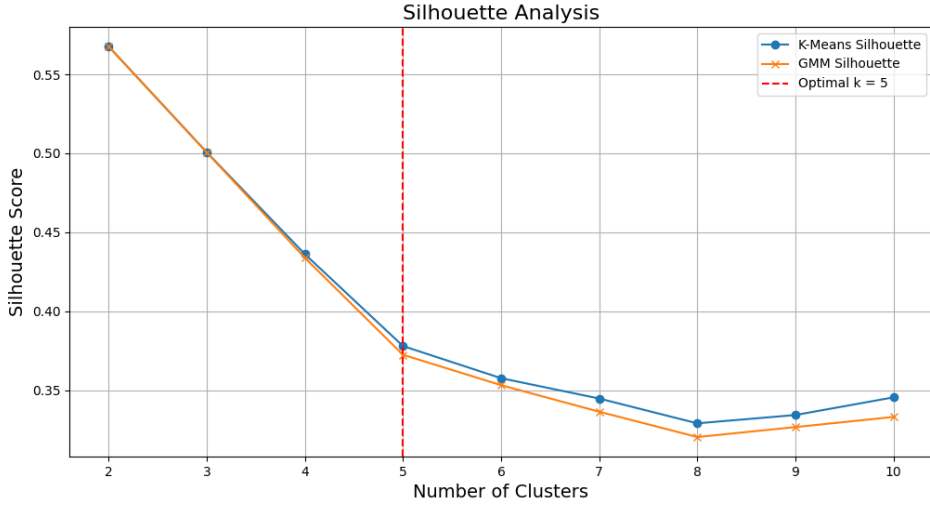


Figure 6.13: Silhouette analysis: Identifies $K = 5$ as optimal cluster count with highest average silhouette score for HQN data.

the optimal number of clusters, effectively capturing the underlying data structure while avoiding overfitting. The average silhouette score across all points provided a robust global measure, and the highest score corresponded to $K = 5$, indicating optimal separation and cohesion for this dataset, shown in Fig. 6.13. In addition to Silhouette Analysis, the Elbow Method, Gap Statistic, and probabilistic approaches such as AIC and BIC were employed to validate the results. The Elbow Method was identified $k = 5$ as the point where the rate of decrease in the WCSS slowed significantly, balancing compactness and overfitting. The Gap Statistic confirmed this result by comparing the clustering structure of the observed data to a null reference distribution. For the GMM used in this study, both AIC and BIC values were optimized at $K = 5$, shown in Fig. 6.14. Overfitting in these ML models can be detected when AIC and BIC values increase due to unnecessary complexity, indicating that the model is fitting noise rather than the signal. Conversely, underfitting occurs when both AIC and BIC are high, indicating a poor data fit, suggesting the model is too simple.

Simulation Assumptions, Initializations, and the Error Tolerance in HQN Cluster Size Reduction

The Table 6.1 indicates the summary of the initialization of the assumptions. In visualization of the HQN dataset in the vector field and investigate its properties based on the HQN model defined by (6.4), the model uses a GMM consisting of Gaussian components weighted by coefficients derived from a Poisson distribution, where the weights represent the prior probabilities of cluster membership. The weights are determined by $f_{\mathbf{Z}}(t_k = 1) = \frac{e^{-\lambda} \lambda^k}{k!}$, ensuring that $\sum_{k=1}^K \frac{e^{-\lambda} \lambda^k}{k!} \approx 1$ for a chosen accuracy level, typically $> 85\%$ ($|1 - \sum_{i=0}^R w_i| \leq 0.15 \implies$ error tolerance of 15%).

A detailed analysis of an effective number of clusters based on values of λ , is available in [22]. For this study, $\lambda = 2$ is used to focus on hybrid

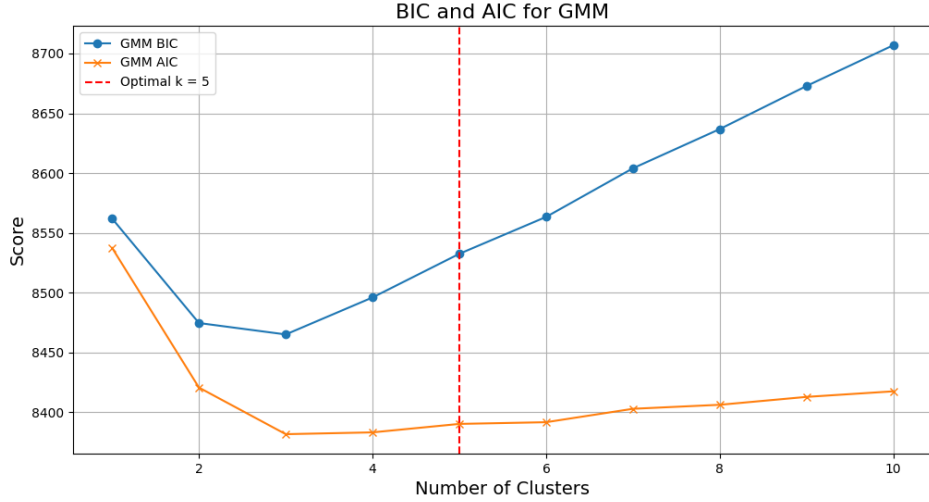


Figure 6.14: BIC and AIC analysis: Confirms $K = 5$ as optimal, optimizing the overfitting and underfitting while capturing underlying data structure.

noise clustering and the achievable channel rate. To satisfy the optimal number of clusters (K) with at least 85% accuracy, the most probable mixing coefficients for $\lambda = 2$ are chosen: $w_0 = 0.135$, $w_1 = 0.271$, $w_2 = 0.271$, $w_3 = 0.18$, and $w_4 = 0.09$. The sum $\sum_{i=0}^4 w_i = 0.947$, yield an accuracy of 95% and an error of 5%, within the tolerance limit. Thus, the optimal number of clusters is $K = 5$, satisfying the model's requirements. Similarly, with $\lambda = 5$, the weights 0.175, 0.175, 0.146, 0.140, 0.104, 0.084, 0.065 sum to 0.889, resulting in $K = 7$ clusters. However, using only the five highest weights from $\lambda = 5$ yields a sum < 0.85 , failing the initial condition. This illustrates how λ and the chosen accuracy influence the number of clusters. This analysis has been displayed in tabular format in 6.2.

Channel parameter updation based on GMM-EM algorithm

We reformulate our noise probability density function using a GMM with five components: $f_{\mathbf{Z}}(\mathbf{z}) = \sum_{k=0}^4 w_k \cdot \mathcal{N}(\mathbf{z}; \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)})$. Our goal is to determine the optimal parameters w_k , $\boldsymbol{\mu}_k^{(z)}$, and $\boldsymbol{\Sigma}_k^{(z)}$ for $k = 0, 1, 2, 3, 4$. While a typical GMM with five components requires 15 parameters (five each for weights, means, and covariances), we demonstrate that fewer parameters are sufficient for this representation. The simulation, conducted in an Anaconda Jupyter Notebook with Python, employed the EM algorithm to optimize the parameters and classify clusters in a hybrid quantum-classical dataset. The initial parameters were defined as follows: $w_0 = 0.135$, $w_1 = 0.271$, $w_2 = 0.271$, $w_3 = 0.18$, $w_4 = 0.09$, $\boldsymbol{\mu}_k^{(z)} = (\mu_{Z_2} + k)\mathbf{I}_{2 \times 1}$, where $\mu_{Z_2} = 0$, $k = 0, 1, 2, 3, 4$, $\boldsymbol{\Sigma}_k^{(z)} = \sigma_{Z_2}^2 \mathbf{I}_{2 \times 2}$, where $\sigma_{Z_2}^2 = 1$, $k = 0, 1, 2, 3, 4$. Fig. 6.9-6.11 illustrate the dataset and intermediate cluster estimations using GMM, visualizing the initial quantum noise distribution, while subsequent figures depict the evolution of clusters during iterations. Convergence is confirmed in Fig. 6.12, where the logarithmic likelihood stabilizes for each of the cases $\lambda = 2$ and $\lambda = 5$, affirming optimal parameter values. The final parameter

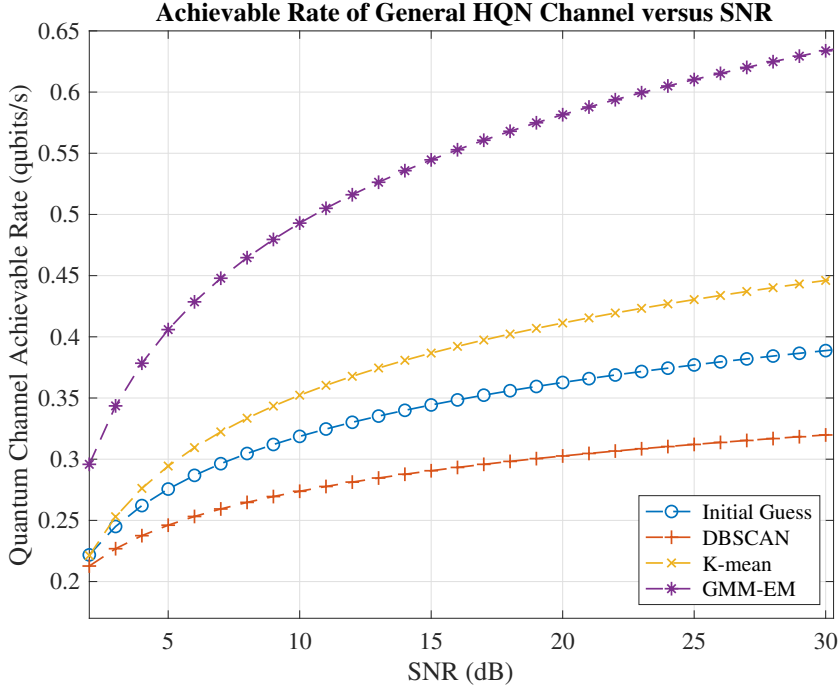


Figure 6.15: The achievable rate of the general quantum channel.

values after 20 iterations are: $w'_0 = 0.1871, w'_1 = 0.3321, w'_2 = 0.2916, w'_3 = 0.1487, w'_4 = 0.0403$, $\mu'_0 = \begin{bmatrix} 0.4180 \\ 0.0895 \end{bmatrix}$, $\Sigma'_0 = \begin{bmatrix} 0.8910 & -0.1011 \\ -0.1011 & 0.9452 \end{bmatrix}$. These results validate the algorithm's ability to optimize Gaussian components while preserving the Poissonian parameter $\lambda \approx 2$, corresponding to photon counts in the system. The updated parameters will be instrumental in analyzing the achievable rate of the quantum channel for Gaussian signals.

Therefore, as a verification, this application of the EM algorithm for finding the optimal cluster in the classification of bivariate hybrid-quantum data can update the optimal parametric values of Gaussian components and helps to identify the optimal clusters but does not affect the Poissonian parameter λ , which is the number of photon counts in the system. However, the iterative EM algorithm has successfully updated the other two channel parameters. We will use the updated parameters to compare the achievable rate of the quantum channel for the Gaussian transmitted signal.

Consider the expression of the general quantum channel achievable rate in (6.23), and the satellite quantum channel achievable rate in (6.25), respectively. These equations involve the channel parameter σ_{Z_2} only to reflect any change in achievable rate, as we have shown that there is no change in the value of λ , and μ_{Z_2} does not involve the expression. Now, let us compare the achievable rate with respect to the SNR for the following case studies: (I) In Fig. 6.15, we have plotted the benchmark result as the achievable rate of the general quantum channel with respect to SNR for the number of components 5, the variance of Gaussian noise, $\sigma_{Z_2}^2$, has been used based on initial guess, and the updated values corresponding to DBSCAN,

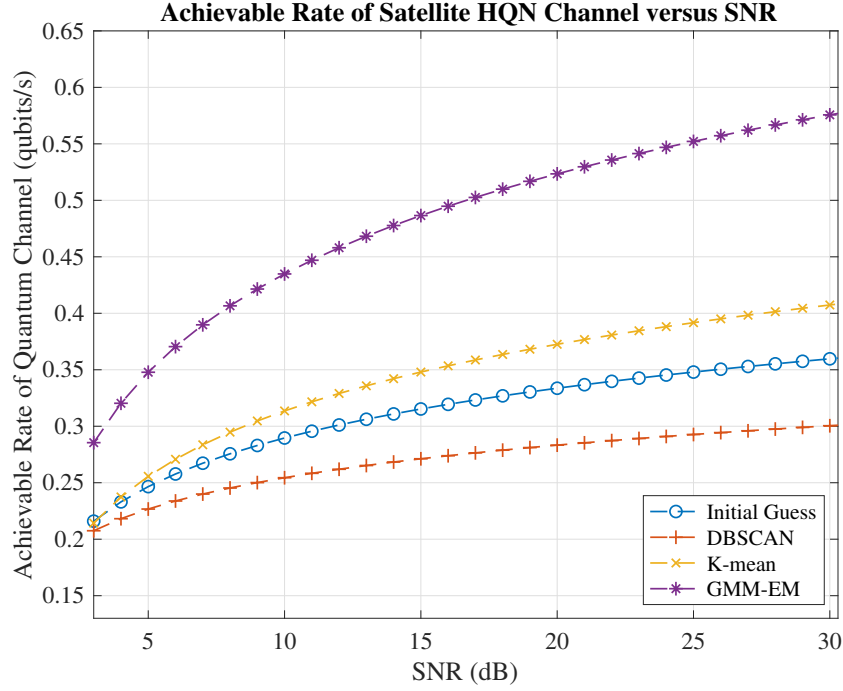


Figure 6.16: The achievable rate of the satellite quantum channel with respect to SNR.

K-means, and GMM-EM respectively. This reflects that the GMM-EM gives the best achievable rate among the other comparative methods. (II) Fig. 6.16, we plot the achievable rate of the satellite quantum channel with respect to the SNR for the number of components 5 and the noise variance $\sigma_{Z_2}^2$ is used based on initial guess, and the updated values corresponding to DBSCAN, K-means, and GMM-EM respectively. GMM-EM-optimized parameters give a better achievable rate (A.R.) estimation result than the initial estimated parameters and other ML benchmark methods in the case of a satellite quantum link.

The Table 6.3 shows that the GMM-EM method achieves the highest achievable rate in both cases of general quantum channel and satellite quantum channel, indicating its superiority in accurately modeling the hybrid Poisson-Gaussian noise structure. It helps achieve reasonable performance but requires significantly higher computational complexity due to EM and model selection overhead (AIC and BIC). K-means shows limited performance and low achievable rates, especially in high-noise-overlap regimes. DBSCAN fails to adapt to the variable densities of the hybrid model, leading to inconsistent clustering and the lowest achievable rate estimations. The Table 6.1 indicates the summary of the initialization of the assumptions.

Table 6.1: Summary of Simulation Assumptions and Initializations

Parameter/Setting	Assumption / Initialization Details
Hybrid Noise Model	Convolution of Quantum Poisson Noise and Classical AWGN
Poisson Parameter (λ)	Set to values such as 2 and 5 to represent low mean photon numbers
Gaussian Noise Parameters	Mean $\mu_{Z_2} = 0$, Variance $\sigma_{Z_2}^2 = 1$ initially; later optimized during EM iterations
Number of Gaussian Components (R)	Initially chosen to satisfy accuracy threshold $\geq 85\%$; e.g., $R = 10$ for $\lambda = 2$
Initial GMM Weights (w_k)	Derived from truncated Poisson distribution: $w_k = \frac{e^{-\lambda} \lambda^k}{k!}$
Initial Means ($\mu_k^{(z)}$)	$(\mu_{Z_2} + k) \cdot I_{2 \times 1}$, $k = 0, 1, \dots, R - 1$
Initial Covariances ($\Sigma_k^{(z)}$)	$\sigma_{Z_2}^2 \cdot I_{2 \times 2}$, where $\sigma_{Z_2}^2 = 1$
Data Dimensionality	Bivariate quantum noise samples ($\mathbb{R}^2$)
Clustering Algorithm	Gaussian Mixture Model (GMM) with Expectation-Maximization (EM)
Initialization Method	Random initialization of component means and Poisson-weighted cluster probabilities
Convergence Criterion	Log-likelihood improvement threshold or fixed number of iterations (e.g., 20 iterations)
Error Tolerance in Weight Sum	$ 1 - \sum_{k=0}^{R-1} w_k \leq 0.15$ (i.e., at least 85% approximation accuracy)
Evaluation Metrics	Silhouette Score, Elbow Method, AIC , BIC used to validate optimal number of clusters
Software Environment	Python (Anaconda Jupyter Notebook); GMM implemented using Scikit-learn

Table 6.2: Effect of Poisson Parameter λ on Cluster Weights and [GMM](#) Accuracy

λ	Cluster Size R	Top K Weights (Rounded)	Cumulative Weight (c.w.)	Threshold Met (if c.w. $> 85\%$)
2	5	0.271, 0.271, 0.135, 0.180, 0.090	94.7%	✓
5	7	0.175, 0.175, 0.146, 0.140, 0.104, 0.084, 0.065	88.9%	✓
5	5	0.175, 0.175, 0.146, 0.140, 0.104	74.0%	X
3	4	0.224, 0.224, 0.168, 0.149	76.5%	X
4	5	0.195, 0.195, 0.156, 0.146, 0.104	79.6%	X

Table 6.3: Performance Comparison on HQN Clustering

Method	Clusters R	Variance	Achievable Rate of unity GQC (qubit/s) at SNR 25 dB	Achievable Rate of unity SQC (qubit/s) at SNR 25 dB	Silhouette	AIC / BIC	Complexity of cluster- ing
K-means	5	0.743	0.446	0.407	0.385	N/A	Low, hard clusters with equal weigh- tage
GMM-EM	5	0.687	0.633	0.575	0.375	Low	High, soft probabilistic clusters
DBSCAN	1	2.891	0.319	0.300	-	N/A	Low, single cluster

6.5 Conclusion

This chapter focuses on optimizing HQN clustering to enhance the achievable rate of Gaussian quantum channels through advanced ML techniques. Specifically, the study utilizes GMM and the EM algorithm to capture the intricate noise characteristics of quantum channels. HQN, consisting of quantum shot noise and classical AWGN, is represented as an infinite mixture of Gaussian distributions weighted by Poisson parameters. A key innovation of this chapter lies in reducing the number of clusters in the noise model and streamlining visualization while maintaining accuracy in channel achievable rate estimation without sacrificing the core properties of the noise. Notable contributions include minimizing the number of Gaussian clusters within acceptable error tolerances and applying the EM-algorithm to update quantum channel parameters, which results in improved channel achievable rate. The proposed method is validated through simulations, revealing that GMM-EM enhanced quantum noise clustering significantly boosts performance in satellite-based quantum communication systems, particularly in maximization of the achievable rate, while outperforming other well-known clustering ML methods such as K-means and DBSCAN. This study demonstrates that GMM and EM-algorithm offer a practical and efficient solution for modeling complex quantum noise in real-time applications, thereby advancing the optimization of quantum communication networks.

In Chapter 7, readers explore the application of the HQNM in free-space satellite-based quantum communication. Based on the HQNM, an architecture has been proposed for satellite-assisted quantum communication channels. As shown in that chapter, this model has been used for long-distance QKD as an application of this hybrid quantum channel in satellite communication. The achievable rate of the satellite quantum channels has been calculated with the quantum SKR based on different parameter settings.

Chapter 7

Hybrid Noise Approach to Modeling of Free-Space Satellite Quantum Channel for CV-QKD

7.1 Introduction

QKD is a crucial technology for secure communication. Quantum satellite communication offers a promising approach to implementing QKD over long distances. However, noise and environmental disturbances significantly impact the performance of QKD in satellite-based systems. This chapter proposes to use the HQN model to enhance the robustness and efficiency of QKD in quantum satellite communication. The HQN model integrates classical noise models with quantum noise effects, addressing key challenges such as photon loss, atmospheric turbulence, and decoherence. The proposed model is analyzed through simulations to demonstrate its effectiveness in improving key generation rates and security against eavesdropping.

This chapter introduces the application of HQN in QKD utilizing FSO satellite quantum channel. It proposes an innovative satellite quantum channel model and derives the quantum SKR achievable through this channel. Unlike existing models that approximate the noise in quantum channels as merely Gaussian distributed, this model incorporates a hybrid quantum noise analysis, accounting for both quantum Poissonian noise and classical AWGN. This hybrid approach acknowledges the dual vulnerability of CV Gaussian quantum channels to both quantum and classical noise under collective attack with RR setting, thereby offering a more realistic assessment of the quantum SKR. This chapter delves into the variation of asymptotic SKR with the SNR and satellite altitudes under various influencing parameters. The critical factors such as reconciliation efficiency, electrical noise, transmission coefficient, detection efficiency, transmission efficiency, excess noise, and the quantum Poissonian noise parameter impacting the SKR have been identified and analysed. These parameters are pivotal in determining the asymptotic SKR in FSO satellite quantum channels, highlighting the challenges of satellite-based quantum communication. A comparative study

has been provided based on the finite-size and asymptotic SKR. It provides a comprehensive framework for understanding and optimizing asymptotic SKR in satellite-based QKD systems, paving the way for more efficient and secure quantum communication networks.

This chapter addresses the limitations of current QKD systems by proposing a novel free-space atmospheric satellite quantum channel model. The proposed model uniquely incorporates quantum Poissonian noise and classical AWGN, providing a realistic representation of the noise characteristics that impact quantum channels. It identifies and analyses critical parameters influencing the asymptotic SKR, including reconciliation efficiency, electrical noise, transmission coefficient, detection efficiency, transmission efficiency, excess noise, and the quantum Poissonian noise parameter. By examining how asymptotic SKR varies with SNR and satellite altitudes under different conditions, this chapter provides valuable insights into the potential and limitations of satellite-based quantum communication systems.

An introductory comparison with finite quantum key size has provided for the analysis of the asymptotic quantum SKR. However, this study was limited to the CV system with asymptotic quantum SKR under collective attack. However, a detailed analysis of finite-size key rate estimation using the HQN model approach is considered an extended work, as provided in Chapter 8 [24]. The CV system was considered the base model, however DV framework needed extensive study with this HQN model. In this chapter considers RR framework with homodyne detection. However, it is interesting to investigate the DR setting with this HQN model under heterodyne detection. In CV-QKD with RR, homodyne detection is often preferred because it minimizes excess noise and maximizes the measured quadrature's SNR. Additionally, studies related to the receiver aperture radius and beam size are considered as a multiplication factor under the total transmission coefficient. This current system model primarily considered CV with RR systems for investigating asymptotic quantum SKR under different atmospheric conditions, utilizing the HQN framework. Also noted, it is considered that Eve's accessible information or optimal attack is Gaussian.

A comprehensive analysis of atmospheric and environmental factors, combined with advanced quantum communication protocols, underscores the robustness and high potential of quantum satellite communications for global-scale secure networks. This chapter demonstrates the efficacy of the HQN model in enhancing free-space quantum satellite communication technologies, presenting new solutions to address the challenges of quantum noise in quantum channels.

This chapter focuses on QKD through a quantum channel model for free-space satellite communication. Previous works, such as those by [26], have proposed atmospheric quantum satellite communication channel models that consider noise as AWGN, typically expected in classical channels [214]. Building on this, [21, 22] introduced a mathematical model incorporating HQN to depict the quantum channel accurately. It extends these

models to propose an accurate estimation of the [SKR](#) for free-space satellite quantum communication. In essence, the critical aspects of this chapter can be summarized as follows :

- This chapter proposes the application of the [HQN](#) model that was developed, analyzed, and optimized in prior chapters [18, 21, 22]. The [HQN](#) framework is used for the first time in the satellite-[CV-QKD](#) system. The chapter emphasizes the integration of quantum Poissonian noise alongside classical [AWGN](#) to form a hybrid noise model, which has not been comprehensively explored in prior chapter works, specifically in the context of satellite-based [CV-QKD](#).
- This chapter introduces a pioneering free-space atmospheric satellite quantum channel model that integrates quantum Poissonian noise and classical [AWGN](#). This hybrid noise approach significantly advances over traditional models that typically consider only Gaussian noise. By acknowledging the dual vulnerabilities of continuous-variable Gaussian quantum channels to both quantum and classical noise, the proposed model offers an accurate and realistic representation of the capacity of the satellite-based [FSO](#) quantum channel. This innovation enhances the accuracy of the channel's capacity, making it a crucial contribution to satellite-based quantum communication.
- This chapter substantially contributes to the practical asymptotic [QKD](#) rates in satellite-based communication. This chapter provides valuable insights into optimizing quantum communication systems by exploring how the asymptotic [SKR](#) varies with the [SNR](#) and satellite altitudes under various parametric conditions. It advances theoretical models and provides a robust framework for the practical design and implementation of [QKD](#) systems, making it an exemplary study in quantum communications.
- This chapter thoroughly examines factors like reconciliation efficiency, electronic noises, detection efficiency, excess noise, transmission coefficient, transmission efficiency, satellite altitude, and the quantum Poissonian noise parameter. It excels in identifying and analyzing key parameters that influence the [CV](#) asymptotic [SKR](#) in free-space atmospheric satellite quantum channels. This finding underscores the challenges of satellite-based quantum communication and the need for careful optimization of system parameters.

This comprehensive approach and findings advance the enhanced design and implementation of robust, efficient, and secure global quantum communication networks.

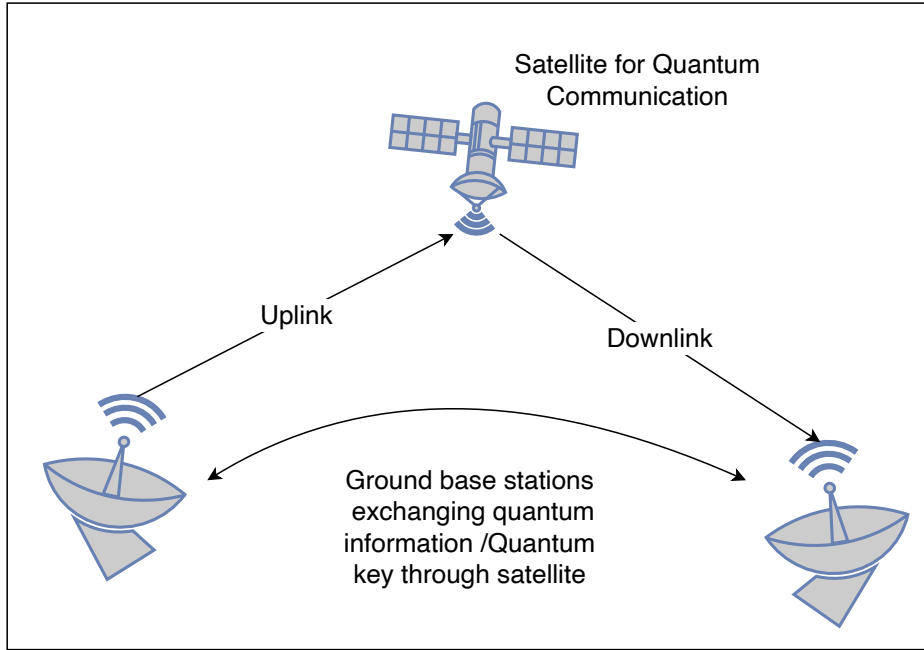


Figure 7.1: A basic model for Quantum Satellite Communication can be replicated with multiple base stations or satellites for the feasibility of long-distance communication and QKD; it also forms a basis of the quantum internet.

7.2 System Model for Free-space Satellite Quantum Communication

7.2.1 The Uplink and Downlink Scenarios in Quantum Satellite Communication

In satellite-based quantum communication, there are two primary channels: uplink (ground-to-satellite) and downlink (satellite-to-ground). The ground station transmits signals to the satellite receiver in the uplink channel. In contrast, the satellite transmits signals to the ground station receiver in the downlink channel, as shown in Fig. 7.1. In this setup, complex quantum engineering components are confined to the ground stations, where one station acts as the source of quantum states and the other as the receiver. Although reflecting quantum states via a satellite is a sophisticated engineering task, it avoids the need for onboard generation of quantum communication information. Deploying quantum technology at the ground stations offers practical advantages such as lower-cost maintenance and rapid upgrades as new technology matures. Several possible architectures and schemes for implementing satellite-based quantum communication depend on the types of links utilized, as illustrated and studied in the existing literature in terms of [CV-QKD](#). For example, some schemes involve higher

complexity and deployment of quantum technology on the satellite [4]. Some schemes have the source of quantum states onboard the satellite, with both ground stations acting as receivers [4]. Another example is a scheme that involves both ground stations transmitting quantum states to the satellite, where quantum measurements are performed on the received states [4]. The classical measurement results are then communicated back to the ground stations. These measurement results support entanglement swapping and measure-device-independent (MDI) protocols, facilitating QKD between the two ground stations.

7.2.2 A Generalised CV-Gaussian Quantum Channel Model

The CV Gaussian quantum channel model used in this chapter is adapted from the previous chapters [21, 22], [18], and for additional insights, it is presented briefly in this section. Quantum communication involves the transfer of quantum states via a quantum channel and consists of three main steps: (I) preparation of quantum states where classical information is encoded into quantum states; (II) transmission of these quantum states over a quantum channel, such as optical fiber or free-space optical FSO channel; and (III) detection where the received states are decoded using quantum measurement to yield classical information. This configuration is shown in Fig. 7.2. Quantum states in communication are represented using DV and CV descriptions. DV technology encodes information into discrete features, such as photon polarization, using single-photon detectors [4].

A qubit, the fundamental unit of DV quantum information, is a superposition of two orthogonal quantum states $|\psi\rangle = c_1|0\rangle + c_2|1\rangle$, where c_1 and c_2 are complex coefficients satisfying $|c_1|^2 + |c_2|^2 = 1$. Quantum states, whether pure or mixed, are described by density matrices. For a pure state qubit $|\psi\rangle$, the density matrix is $\rho = |\psi\rangle\langle\psi|$, while mixed states are represented as probabilistic mixtures of pure states [193, 194]. In contrast, CV encoding maps information onto the optical field's quadrature variables, spanning an infinite-dimensional Hilbert space. CV QKD offers higher efficiency by utilizing a broader range of quantum states, enabling more compact and robust systems. In contrast, DV QKD typically requires more complex setups and has lower key rates due to the limited nature of the quantum states used. Detection of CV states often involves homodyne or heterodyne detectors, which are faster and more efficient than single-photon detectors. Homodyne detection is simpler and more cost-effective, as it requires only one local oscillator, making it easier to implement in practical systems. In contrast, heterodyne detection requires two local oscillators and a more complex setup, increasing system complexity and cost.

A quantum channel is defined as a CPTP map, which transforms density operators ρ within a Hilbert space $\mathcal{H}$. This transformation can be described as $\rho \mapsto \mathbf{T}(\rho)$. For any quantum channel $\mathbf{T}$, a corresponding state exists ρ_E

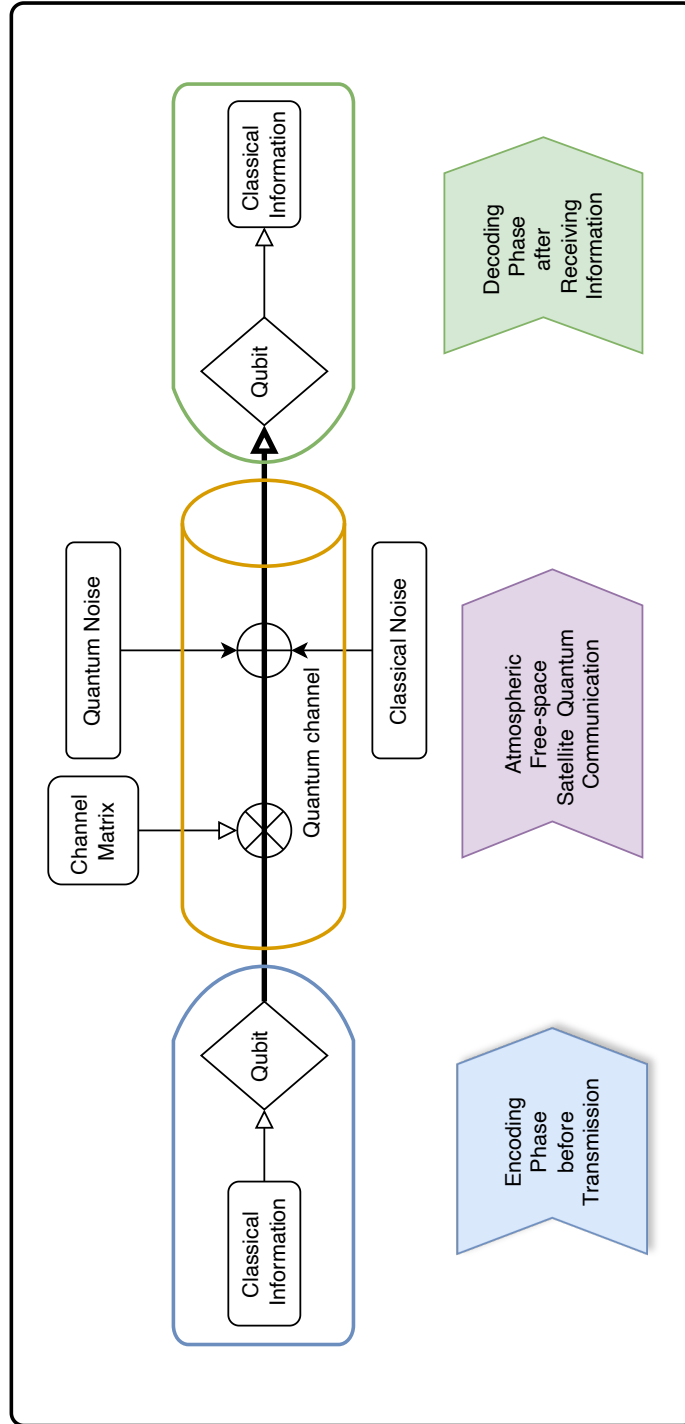


Figure 7.2: A schematic diagram showing a single quantum link between transmitter and receiver under the satellite communication system.

in an environment Hilbert space $\mathcal{H}_E$ and a unitary operation $\mathbf{U}$, satisfying $\mathbf{T}(\boldsymbol{\rho}) = \text{tr}_E[\mathbf{U}(\boldsymbol{\rho} \otimes \boldsymbol{\rho}_E)\mathbf{U}^\dagger]$, where the environment E drives the decoherence process [195, 197]. In Gaussian channels, the transformation can be expressed as $\boldsymbol{\rho} \mapsto \mathbf{A}^t \boldsymbol{\rho} \mathbf{A} + \mathbf{Z}$, where $\mathbf{A}$ modulates the signal, and $\mathbf{Z}$ accounts for both quantum and classical noise. In special cases when $\mathbf{A} = \mathbf{I}_{2n}$, where n is the degrees of freedom of the corresponding quantum system, the channel can be simplified to $\boldsymbol{\rho} \mapsto \boldsymbol{\rho} + \mathbf{Z}$, and the transformation remains valid as a quantum channel if sufficient noise is introduced. A qubit, represented as a point vector (θ, ϕ, r) on the Bloch sphere, can be treated as a scalar variable θ under hybrid noise constraints [18, 21, 22]. Under this scalar transformation, the scalar variable representing the qubit can be mapped in the following way $\theta \mapsto \theta + Z$ where Z is the random variable representing the HQN Z consists of quantum Poisson noise and classical AWGN. Hence, the generalized quantum channel equation can be written from the above as $Y = X + Z$ where X and Y are the transmitted and the received signal, respectively [18, 21]. The channel equation has been derived in the following section for the special case of the satellite quantum channel.

7.2.3 The CV-Gaussian Quantum Channel Model for Satellite Quantum Communication

This chapter examines a quantum satellite communication model comprising a ground station and a satellite, enabling bidirectional transmission. Let's designate the sender as Alice and the receiver as Bob, regardless of location, and include an eavesdropper, Eve, who may intercept transmissions anywhere along the path. Alice prepares quantum states, typically qubits or CV states encoded as photons, which are transmitted via a satellite-based free-space optical channel. This channel is subject to free-space diffraction, atmospheric turbulence, and thermal noise, affecting signal quality differently in uplink and downlink scenarios.

The satellite serves as an intermediary relay between Alice and Bob. Upon receiving the quantum states, Bob may employ homodyne, heterodyne, or single-photon detection methods depending on the nature of the transmitted quantum states. Bob's ability to accurately decode the information depends on the fidelity of the received quantum states, which is influenced by the noise and losses introduced by the satellite channel. Quantum mechanical principles constrain an eavesdropper's (Eve's) potential interception attempts, although she may employ sophisticated strategies to covertly extract information. This model allows for a comprehensive analysis of quantum communication protocols and security scenarios in satellite-based systems, addressing the unique challenges of long-distance, free-space quantum transmission under various environmental conditions and potential security threats.

From this generalized description of a quantum channel, let's drive towards the atmospheric FSO satellite quantum channel model represented

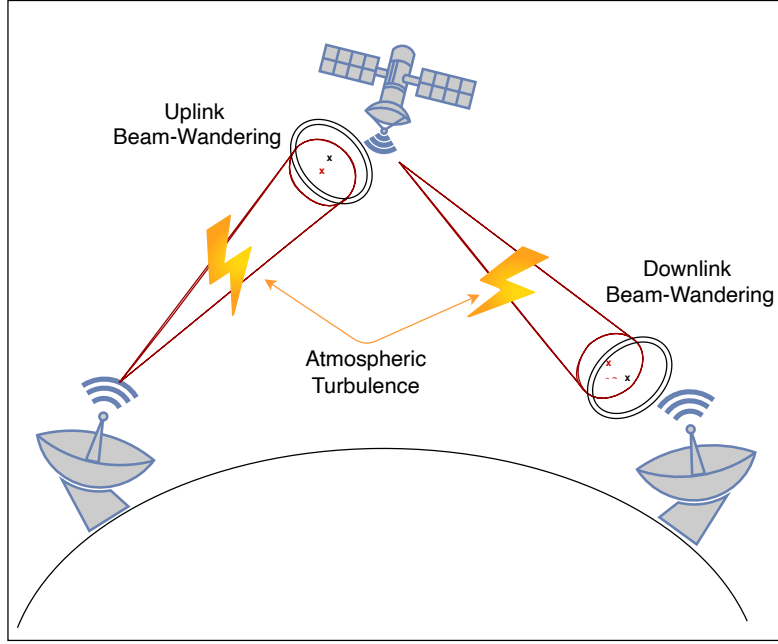


Figure 7.3: The atmospheric turbulence with beam-wandering. Due to various atmospheric conditions, considering the beam-wandering model for uplinks and downlinks for satellites is useful, and it shows realistic scenarios in detecting the secret key rate.

by the following equation [26]

$$Y = TX + Z, \quad (7.1)$$

where the quantum channel transmitted signal is given by random variables X , representing Alice's inputs, and the received signal Y at Bob's side, Z is the HQN, where T is the overall transmission coefficient for the single use of the quantum channel. The focus should be on the transmission coefficient T (with the transmission efficiency $\tau = T^2$). The goal is to maximize the SKR that Alice and Bob can extract while minimizing the information that Eve can gain. This model captures the complexity of satellite quantum communication, underscoring the importance of accounting for various noise sources and channel imperfections in ensuring secure communication.

In FSO, losses arise from diffraction, absorption, scattering, and atmospheric turbulence. Diffraction causes beam spreading, leading to divergence losses, while absorption and scattering depend on wavelength. Weather conditions like fog or rain can significantly reduce channel transmissivity, challenging FSO communication, especially for quantum communication models [4]. These scenarios are pictorially shown in Fig. 7.3.

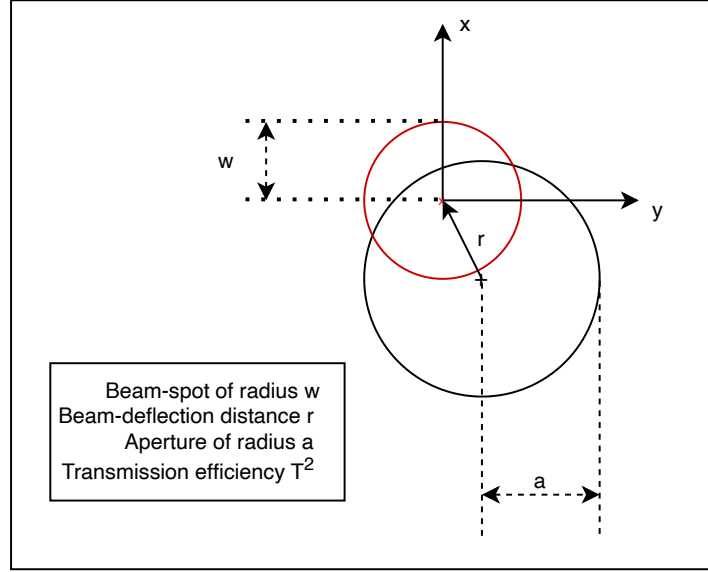


Figure 7.4: The beam-wandering model for laser direction. The red circle shows the position of the incoming beam on the receiver's aperture; the black circle represents the receiver's aperture.

7.3 Methodology of Quantum Cryptography for Free-space Satellite Quantum Communication

7.3.1 Secret Quantum Key Distribution through FSO Satellite Quantum Channel

This section outlines the methodology for calculating the key generation rate across a fading channel. To initiate the process, Alice generates a sequence of $2N$ real random variables $X_1, X_2, \dots, X_{2N}$ that are Gaussian distributed with variance $\sigma_{X_k}^2$, expressed as $X_k \sim \mathcal{N}(x; \mu_{X_k}, \sigma_{X_k}^2)$, with the associated p.d.f. given by [26],

$$f_{X_k}(x) = \frac{1}{\sigma_{X_k} \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{x - \mu_{X_k}}{\sigma_{X_k}} \right)^2}, \quad (7.2)$$

where μ_{X_k} and σ_{X_k} are the mean and s.d. of the distribution, respectively. These $2N$ random variables $X_1, X_2, \dots, X_{2N}$ correspond to N coherent states given by $|\mathbf{a}_1\rangle, |\mathbf{a}_2\rangle, \dots, |\mathbf{a}_N\rangle$, where $\mathbf{a}_k = X_{2k-1} + iX_{2k} \in \mathbb{C}$ and $i = \sqrt{-1}$. Each state is sent through the quantum channel to Bob, who performs homodyne detection, simultaneously measuring both quadratures. For the k th use of the channel, Bob obtains two results, Y_{2k-1} and Y_{2k} , corresponding to X_{2k-1} and X_{2k} , respectively. The raw key string $\mathbf{Y} = (Y_1, Y_2, \dots, Y_{2N})$ is obtained, which is particularly useful under low transmission efficiency with reverse reconciliation. The asymptotic values are considered in the limiting case $N \rightarrow \infty$. In general, RR is superior to

DR in quantum satellite communication because it enables the trusted receiver (e.g., a ground station) to dictate the key generation process, thereby making it more resilient to the high channel loss and noise typically experienced in satellite-to-ground links. This approach improves the achievable secure key rate under adverse channel conditions. The formula traditionally used to calculate the asymptotic value of the SKR, particularly under reverse reconciliation, is known as the Devetak-Winter bound [26, 36],

$$K_{WD} = \beta I_{AB} - \chi_{BE}, \quad (7.3)$$

where βI_{AB} measures the correlation between Alice and Bob's datasets, incorporating the inefficiency of the error correction process through the parameter β (≤ 1). Meanwhile, χ_{BE} indicates the amount of information Eve has about the raw key derived from Bob's data.

7.3.2 Propagation Channel Model for FSO Satellite Quantum Communication

To assess the efficacy of a QKD protocol over a specific quantum channel, one must calculate the mutual information βI_{AB} and the Holevo quantity χ_{BE} . These quantities are essential for determining the SKR. The parameter estimation process must be modeled to predict the expected outcomes for Alice and Bob within the given channel model. The quantum channel connecting Alice and Bob can be represented as a phase-insensitive, noisy Bosonic channel. This formulation requires that the random variables X_k and Y_k be considered within this framework. The relationship between X_k and Y_k is given by,

$$Y_k = T_k X_k + Z_k, \quad (7.4)$$

Where T_k is the overall transmission coefficient for the k -th channel use, with the transmission efficiency of k -th channel $\tau_k = T_k^2$, and Z_k represents the HQN. The distribution of the HQN Z_k is given by [21]

$$f_{Z_k}(z) = \sum_{j=0}^{\infty} \frac{e^{-\lambda} \lambda^j}{j!} \frac{1}{\sigma_{Z_k^{(2)}} \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{z - j - \mu_{Z_k^{(2)}}}{\sigma_{Z_k^{(2)}}} \right)^2} = \sum_{j=0}^{\infty} u_j^{(Z_k)} \mathcal{N} \left(z; \mu_j^{(Z_k)}, \sigma_j^{(Z_k)^2} \right), \quad (7.5)$$

where $u_j^{(Z_k)} = \frac{e^{-\lambda} \lambda^j}{j!}$, $\sum_{j=0}^{\infty} u_j^{(Z_k)} = 1$, and $u_j \geq 0 \quad \forall j$. The term $\mathcal{N}(z; \mu_j^{(Z_k)}, \sigma_j^{(Z_k)^2})$ represents a Gaussian density with mean $\mu_j^{(Z_k)} = \mu_{Z_k^{(2)}} + j$, variance $\sigma_j^{(Z_k)^2} = \sigma_{Z_k^{(2)}}^2$ and standard deviation $\sigma_j^{(Z_k)}$. The HQN Z_k is a combination of quantum Poissonian noise $Z_k^{(1)}$ and classical additive white Gaussian noise $Z_k^{(2)}$, such that $Z_k = Z_k^{(1)} + Z_k^{(2)}$. Quantum Poissonian Noise $Z_k^{(1)}$ follows the p.m.f. given by $f_{Z_k^{(1)}}(j) = \frac{e^{-\lambda} \lambda^j}{j!}$, where $\lambda \geq 0$, $\lambda \in \{0, 1, 2, \dots\}$, and $j \in \{0, 1, 2, \dots\}$.

The classical [AWGN](#) $Z_k^{(2)}$ follows Gaussian distribution with the mean $\mu_{Z_k^{(2)}}$ and variance $\sigma_{Z_k^{(2)}}^2$.

7.3.3 Analyzing the Transmission Efficiency for Satellite Quantum Channel

This section explores the critical aspects of transmission efficiency in free-space quantum communication channels, with a specific focus on satellite-based systems. The transmission efficiency τ_k is characterized by a random variable that ranges between 0 and 1. The probability distribution of τ_k aligns with the log-normal distribution, approximating the [PDTC](#) in entanglement distribution scenarios. The probability distribution of τ_k is given by [35, 36, 37, 38]

$$\mathcal{P}(\tau_k) = \frac{1}{\sqrt{2\pi\sigma\tau_k}} e^{-\frac{1}{2}\left(\frac{\ln \tau_k + \ln \tilde{\tau}_k}{\sigma}\right)^2}. \quad (7.6)$$

Here, τ_k represents the atmospheric transmittance, $-\ln \tilde{\tau}_k$ is the logarithm of the mean atmospheric transmittance, and σ is the variance of $-\ln \tau_k$, which characterizes the atmospheric turbulence. The primary effects of atmospheric turbulence on quantum communication include beam spreading, scintillation, and beam wandering [4, 215]: (I) Beam Spreading occurs when the beam width is significantly larger than the eddies' radius in the turbulent layer. (II) Scintillation dominates when the beam width and eddies' radius are comparable, which is especially significant for satellite downlink. (III) Beam Wandering is common in both uplinks and downlinks. It involves time-dependent random lateral shifts in the beam's position. The beam wandering effect, shown in Fig. 7.3, is influenced by how atmospheric turbulence causes lateral shifts in the beam's position.

The Weibull distribution is employed to measure the pointing error of the spacecraft ([S/C](#)) given by the [p.d.f.](#) $P(r, \sigma_r) = \frac{r}{\sigma_r^2} e^{-\left(\frac{r}{\sqrt{2}\sigma_r}\right)^2}$, where σ_r represents the standard deviation, and r is the displacement distance from the receiver's center. The [PDTC](#) statistical model represents the transmission efficiency T received at the ground station ([GS](#)) [4, 37] $T^2 = T_0^2 e^{-\left(\frac{r}{R_1}\right)^{\kappa_1}}$, where $T_0^2 = 1 - e^{-2\frac{a^2}{W^2}}$, and κ_1 and R_1 are the shape and scale parameters given by,

$$\kappa_1 = 8 \frac{a^2}{W^2} \frac{e^{-4\frac{a^2}{W^2}} I_1\left(4\frac{a^2}{W^2}\right)}{1 - e^{-4\frac{a^2}{W^2}} I_0\left(4\frac{a^2}{W^2}\right)} \left[\ln \left(\frac{2T_0^2}{1 - e^{-4\frac{a^2}{W^2}} I_0\left(4\frac{a^2}{W^2}\right)} \right) \right]^{-1} \quad (7.7)$$

and

$$R_1 = a \left[\ln \left(\frac{2T_0^2}{1 - e^{-4\frac{a^2}{W^2}} I_0\left(4\frac{a^2}{W^2}\right)} \right) \right]^{-1/\kappa_1}, \quad (7.8)$$

where a is the receiver aperture radius, W is the beam size, and I_0 and I_1 are the modified Bessel functions of the first kind.

Consider the **PDTC** and beam wandering, and account for the **S/C**'s off-axis pointing behaviour. Assuming the beam fluctuates around the aperture's centre, one can calculate the **PDTC** (P) as follows, [37]

$$P(T) = \frac{2R_1^2}{\sigma_r^{\kappa_1} T} \left(2 \ln \left(\frac{T_0}{T} \right) \right)^{\frac{2}{\kappa_1} - 1} e^{-\frac{1}{2\sigma_r R_1^2} \left(2 \ln \left(\frac{T_0}{T} \right) \right)^{\frac{2}{\kappa_1}}}. \quad (7.9)$$

PDTC is crucial for long-distance quantum communication, which relies on entanglement. This model, focused on beam wandering, underpins expansions into quantum free-space channels, suggesting that fluctuating losses may better preserve quantum properties, such as entanglement and squeezing, than constant losses. This preservation is vital for successful free-space quantum communication.

7.3.4 Received Signal Model for **FSO** Satellite Quantum Channel

In quantum communication, accurately calculating the key rate over fading channels is crucial, particularly in free-space satellite communication, where atmospheric turbulence has a significant impact on transmission efficiency. Considering the impact of atmospheric turbulence, the transmission coefficient T_k varies but is assumed to be stable over short periods. The transmission coefficient remains stable during back-to-back uses, allowing Alice and Bob to adjust error correction strategies, assuming approximate knowledge of T_k . Therefore, it is worth considering a fixed value of T_k during the consecutive transmission through the quantum channel and writing T_g instead of T_k , where T_g is an aggregated transmission coefficient, however, for each group g the aggregated transmission coefficient T_g can take constant value.

Aggregated secret key rate: Analyzing transmission coefficients (T) for varying satellite-to-ground distances optimizes satellite optical communication systems. For altitudes from 400 km (LEO) to 22,000 km (MEO/GEO), slant range variations significantly impact T , with lower altitudes experiencing more noise. A mitigation strategy groups transmission coefficients into clusters based on expected transmittance intervals, minimizing fading noise. Each group is independently analyzed to determine the secret key rate per group ($K_{fad}(PDTE(g))$), which is aggregated into a total key rate, $K_{agg} = \sum_g P(\tau_g \in PDTE(g)) K_{fad}(PDTE(g))$. Here, τ_g represents the estimated aggregated channel transmission efficiency. This approach ensures accurate channel transmittance estimation, even during fast-fading processes, improving the precision of group classifications. This study divides transmission values $T(\leq 1)$ uniformly, ranging from single-group analysis to 100 equally spaced intervals, approaching the asymptotic limit. This strategy highlights the importance of optimizing the transmission coefficient

to maximize secure key rates and address practical challenges in satellite optical communication systems. The modified channel equation becomes [26, 28],

$$Y_k = TX_k + Z_k, \quad (7.10)$$

where T varies over 0.3 to 1 equally divided into 100 subgroups. For a given transmitted signal $X_k \sim \mathcal{N}(x; \mu_{X_k}, \sigma_{X_k}^2)$, the scaled signal $TX_k \sim \mathcal{N}(s; T\mu_{X_k}, T^2\sigma_{X_k}^2)$. The p.d.f. of TX_k is given by,

$$f_{TX_k}(s) = \frac{1}{T\sigma_{X_k}\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{s-T\mu_{X_k}}{T\sigma_{X_k}}\right)^2}. \quad (7.11)$$

The hybrid noise Z_k is given in (7.5), hence the p.d.f. of the received signal Y_k is obtained in convolution of f_{TX_k} and f_{Z_k} given by,

$$\begin{aligned} f_{Y_k}(y) &= \sum_{j=0}^{\infty} \frac{e^{-\lambda}\lambda^j}{j!} \frac{S_{pq}}{\sigma_{pq}\sqrt{2\pi}} \sqrt{2\pi}\sigma_{pq} = \sum_{i=0}^{\infty} \frac{e^{-\lambda}\lambda^i}{i!} S_{fg} \\ &= \sum_{i=0}^{\infty} \frac{e^{-\lambda}\lambda^i}{i!} \frac{1}{\sqrt{2\pi(\sigma_f^2 + \sigma_g^2)}} e^{-\frac{1}{2(\sigma_f^2 + \sigma_g^2)}(\mu_f - \mu_g)^2} \\ &= \sum_{i=0}^{\infty} \frac{e^{-\lambda}\lambda^i}{i!} \frac{1}{\sqrt{2\pi(\sigma_X^2 + \sigma_{Z_i^{(2)}}^2)}} e^{-\frac{(T\mu_X - y + i + \mu_{Z_k^{(2)}})^2}{2(T^2\sigma_X^2 + \sigma_{Z_i^{(2)}}^2)}} \\ &= \sum_{j=0}^{\infty} \frac{e^{-\lambda}\lambda^j}{j!} \frac{1}{\sqrt{2\pi(T^2\sigma_{X_k}^2 + \sigma_{Z_j^{(2)}}^2)}} e^{\left[-\frac{(y - j - T\mu_{X_k} - \mu_{Z_k^{(2)}})^2}{2(T^2\sigma_{X_k}^2 + \sigma_{Z_j^{(2)}}^2)} \right]} \\ &= \sum_{j=0}^{\infty} v_j^{(Y_k)} \mathcal{N}\left(y; \mu_j^{(Y_k)}, \sigma_j^{(Y_k)^2}\right), \end{aligned} \quad (7.12)$$

where $v_j^{(Y_k)} = \frac{e^{-\lambda}\lambda^j}{j!}$, $\sum_{j=0}^{\infty} v_j^{(Y_k)} = 1$, $v_j^{(Y_k)} \geq 0 \quad \forall j \in \{0, 1, 2, \dots\}$ and $\mathcal{N}(y; \mu_j^{(Y_k)}, \sigma_j^{(Y_k)^2})$ is Gaussian density in dummy variable y , with mean $\mu_j^{(Y_k)} = T\mu_{X_k} + \mu_{Z_k^{(2)}} + j$, s.d. $\sigma_j^{(Y_k)} = \sqrt{(T^2\sigma_{X_k}^2 + \sigma_{Z_k^{(2)}}^2)}$ and variance $\sigma_j^{(Y_k)^2}$.

Now, let's derive the p.d.f. of the received signal in free-space quantum communication channels by assuming a stable transmission coefficient over short periods and analyzing the HQN. This enables us to understand the key generation rate and the impact of various noise components, ultimately aiding in the design of efficient QKD protocols.

7.3.5 Approximation of the Quantum Signal Models for Entropy Estimation

This section analyses the channel's entropy by approximating the HQN and received signal as finite Gaussian mixtures (GMs). In the next section, we

derive upper and lower entropy bounds, providing a robust framework for the capacity of the satellite quantum channel.

The probability distribution of the HQN Z_k is given by in (7.5), the approximation of $f_Z(z)$ is taken as [21],

$$f_{Z_k}(z) = \sum_{j=0}^R \frac{e^{-\lambda} \lambda^j}{j!} \frac{1}{\sigma_{Z_k^{(2)}} \sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{z - j - \mu_{Z_k^{(2)}}}{\sigma_{Z_k^{(2)}}} \right)^2} = \sum_{j=0}^R u_j^{(Z_k)} \mathcal{N}\left(z; \mu_j^{(Z_k)}, \sigma_j^{(Z_k)^2}\right), \quad (7.13)$$

where $u_j^{(Z_k)} = \frac{e^{-\lambda} \lambda^j}{j!}$, $\sum_{i=0}^R u_i^{(Z_k)} \approx 1$ for large R , and $u_j^{(Z_k)} \geq 0 \quad \forall j$. The term $\mathcal{N}(z; \mu_j^{(Z_k)}, \sigma_j^{(Z_k)^2})$ represents a Gaussian density with mean $\mu_j^{(Z_k)} = \mu_{Z_k^{(2)}} + j$ and variance $\sigma_j^{(Z_k)^2} = \sigma_{Z_k^{(2)}}^2$, with standard deviation $\sigma_j^{(Z_k)}$. This is the Gaussian mixture in the scalar variable Z_k , and the corresponding Gaussian mixture in random vector $\bar{Z}_k \in \mathbb{R}^M$ is

$$f_{\bar{Z}_k}(\bar{z}) = \sum_{i=0}^R u_i^{(\bar{Z}_k)} \mathcal{N}\left(\bar{z}; \bar{\mu}_i^{(\bar{Z}_k)}, \Sigma_i^{(\bar{Z}_k)}\right), \quad (7.14)$$

where $\bar{z}$ is the random vector in $\mathbb{R}^M$, $\bar{\mu}_i^{(\bar{Z}_k)}$ is the mean vector, and $\Sigma_i^{(\bar{Z}_k)}$ is the covariance matrix of the corresponding Gaussian density $\mathcal{N}$.

Consider the p.d.f. of the received signal Y_k given by in (8.13), the approximation of $f_{Y_k}(y)$ is taken as,

$$\begin{aligned} f_{Y_k}(y) &= \sum_{j=0}^R \frac{e^{-\lambda} \lambda^j}{j!} \frac{1}{\sqrt{2\pi(T^2 \sigma_{X_k}^2 + \sigma_{Z_k^{(2)}}^2)}} e^{\left[-\frac{(y - j - T\mu_{X_k} - \mu_{Z_k^{(2)}})^2}{2(T^2 \sigma_{X_k}^2 + \sigma_{Z_k^{(2)}}^2)} \right]} \\ &= \sum_{j=0}^R v_j^{(Y_k)} \mathcal{N}\left(y; \mu_j^{(Y_k)}, \sigma_j^{(Y_k)^2}\right), \end{aligned} \quad (7.15)$$

where $v_j^{(Y_k)} = \frac{e^{-\lambda} \lambda^j}{j!}$, $\sum_{i=0}^R u_i^{(Y_k)} \approx 1$ for large R , $\mu_j^{(Y_k)} = T\mu_{X_k} + \mu_{Z_k^{(2)}} + j$, and $\sigma_j^{(Y_k)} = \sqrt{T^2 \sigma_{X_k}^2 + \sigma_{Z_k^{(2)}}^2}$. This is the Gaussian mixture in scalar variable Y_k , and the corresponding Gaussian mixture in random vector $\bar{Y}_k \in \mathbb{R}^M$ is,

$$f_{\bar{Y}_k}(\bar{y}) = \sum_{i=0}^R u_i^{(\bar{Y}_k)} \mathcal{N}\left(\bar{y}; \bar{\mu}_i^{(\bar{Y}_k)}, \Sigma_i^{(\bar{Y}_k)}\right), \quad (7.16)$$

where $\bar{y}$ is the random vector in $\mathbb{R}^M$, $\bar{\mu}_i^{(\bar{Y}_k)}$ is the mean vector, and $\Sigma_i^{(\bar{Y}_k)}$ is the covariance matrix of the corresponding Gaussian density $\mathcal{N}$. The detailed calculations and approximation methodology of p.d.f.s have been showcased in [18].

For a continuous-valued random vector $\bar{x} \in \mathcal{R}^D$ with p.d.f. $f(\bar{x})$, the differential entropy is [21]

$$H(\bar{x}) = E[-\log f(\bar{x})] = - \int_{\mathcal{R}^D} f(\bar{x}) \log f(\bar{x}) d\bar{x}. \quad (7.17)$$

Now, if p.d.f. $f(\cdot)$ is a GMM, which means it can be represented as a weighted sum of L component Gaussian densities as given by the expression, $f(\bar{x}) = \sum_{i=1}^L w_i \mathcal{N}(\bar{x}; \bar{\mu}_i, \Sigma_i)$, where w_i are non-negative weighting coefficients with $\sum_i w_i = 1$ and $\mathcal{N}(\bar{x}; \bar{\mu}_i, \Sigma_i)$ is a Gaussian density mean vector $\bar{\mu}_i$, and covariance matrix $\Sigma_i \forall i = 1(1)L$. The differential entropy of the HQN $\bar{Z}_k$ is $H(\bar{Z}_k) = - \int_{\chi_{\bar{Z}_k}} f_{\bar{Z}_k}(\bar{z}) \log f_{\bar{Z}_k}(\bar{z}) d\bar{z}$, and for the received signal $\bar{Y}_k$, the differential entropy is $H(\bar{Y}_k) = - \int_{\chi_{\bar{Y}_k}} f_{\bar{Y}_k}(\bar{y}) \log f_{\bar{Y}_k}(\bar{y}) d\bar{y}$, where $\chi_{\bar{Z}_k}$ is the support of $f_{\bar{Z}_k}$ and $\chi_{\bar{Y}_k}$ is the support of $f_{\bar{Y}_k}$. The entropy cannot be directly calculated for Gaussian mixtures due to the logarithm of a sum of exponential functions, but it can be approximated using the following bounds. The entropy of Gaussian mixtures, although complex due to the logarithm of a sum of exponentials, can be approximated for practical purposes. In the QKD context, accurate entropy calculation is crucial for determining the key rate. Entropy approximation methods often face challenges in quantifying the deviation between actual and approximated values. Therefore, establishing tight lower and upper bounds for the entropy of the GM random vector is essential. These bounds can provide a meaningful approximation and be calculated in the closed form [21, 130].

The lower bound $H_L(\bar{x})$ of the entropy $H(\bar{x})$ is given by, [21, 130]

$$H_L(\bar{x}) = - \sum_{i=0}^L w_i \log_2 \left(\sum_{j=0}^L w_j m_{i,j} \right), \quad (7.18)$$

where $m_{i,j} = \mathcal{N}(\bar{\mu}_i; \bar{\mu}_j, \Sigma_i + \Sigma_j)$, $\bar{\mu}_i$ is the mean vector, and Σ_i is the covariance matrix of the corresponding component of the Gaussian mixture $f(\bar{x})$.

The upper bound $H_U(\bar{x})$ of the entropy $H(\bar{x})$ is given by [21, 130],

$$H_U(\bar{x}) = \sum_{i=0}^L w_i \log_2 \left(-\log_2 w_i + \frac{1}{2} \log_2 ((2\pi e)^D |\Sigma_i|) \right). \quad (7.19)$$

7.3.6 Capacity of FSO quantum satellite channel

Since $f_{\bar{Z}_k}$ and $f_{\bar{Y}_k}$ are both Gaussian mixture densities, the closed-form solution of the corresponding entropies $H_{\bar{Z}_k}$ and $H_{\bar{Y}_k}$ of the hybrid quantum noise and the received signal can not be calculated due to the logarithm of the sum and exponential function [21, 130]. However, (7.18) and (7.19) provide the lower and the upper bounds for each entropy $H_{\bar{Z}_k}$ and $H_{\bar{Y}_k}$. Let us call the upper and lower bounds of $H_{\bar{Z}_k}$ by $U_{\bar{Z}_k}$ and $L_{\bar{Z}_k}$, and the upper and lower bounds of $H_{\bar{Y}_k}$ by $U_{\bar{Y}_k}$ and $L_{\bar{Y}_k}$, respectively, given by

$L_{\bar{Z}_k} \leq H_{\bar{Z}_k} \leq U_{\bar{Z}_k}$ and $L_{\bar{Y}_k} \leq H_{\bar{Y}_k} \leq U_{\bar{Y}_k}$. In [25], the mutual information $I(\bar{X}_k; \bar{Y}_k)$ between transmitted signal $\bar{X}_k$ and received signal $\bar{Y}_k$ is defined as, $I(\bar{X}_k; \bar{Y}_k) = H(\bar{X}_k) + H(\bar{Y}_k) - H(\bar{X}_k, \bar{Y}_k)$, and applying the chain rule for continuous variables, one would get, $H(\bar{X}_k, \bar{Y}_k) = H(\bar{Y}_k | \bar{X}_k) + H(\bar{X}_k)$. Therefore,

$$\begin{aligned} I(\bar{X}_k; \bar{Y}_k) &= H(\bar{Y}_k) - H(\bar{Y}_k | \bar{X}_k) = H(\bar{Y}_k) - H(\bar{X}_k + \bar{Z}_k | \bar{X}_k) = H(\bar{Y}_k) - H(\bar{Z}_k | \bar{X}_k) \\ &= H(\bar{Y}_k) - H(\bar{Z}_k) = H(\bar{Y}_k) - H(\bar{Z}_k), \quad (7.20) \end{aligned}$$

as transmitted signal $\bar{X}_k$ and noise $\bar{Z}_k$ are independent. Let's rename $H(\bar{Z}_k)$ as $H_{\bar{Z}_k}$ for notational ease, and the bound for mutual information can be calculated as follows

$$\begin{aligned} -L_{\bar{Z}_k} &\geq -H_{\bar{Z}_k} \geq -U_{\bar{Z}_k} \implies H_{\bar{Y}_k} - L_{\bar{Z}_k} \geq H_{\bar{Y}_k} - H_{\bar{Z}_k} \geq H_{\bar{Y}_k} - U_{\bar{Z}_k} \\ &\implies U_{(\bar{Y}_k)} - L_{(\bar{Z}_k)} \geq H_{(\bar{Y}_k)} - L_{(\bar{Z}_k)} \geq H_{(\bar{Y}_k)} - H_{(\bar{Z}_k)} = I(\bar{X}_k; \bar{Y}_k). \quad (7.21) \end{aligned}$$

Hence,

$$C = \max_{f_{\bar{X}_k}(\bar{x})} I(\bar{X}_k; \bar{Y}_k) \leq U_{\bar{Y}_k} - L_{\bar{Z}_k}. \quad (7.22)$$

From (7.18), the lower bound $L_{\bar{Z}_k}$ of entropy $H_{\bar{Z}_k}$, can be calculated as

$$L_{\bar{Z}_k} = - \sum_{j=0}^R u_j^{(\bar{Z}_k)} \log_2 \left(\sum_{l=0}^R u_l^{(\bar{Z}_k)} \mathcal{N}(\bar{\mu}_j^{(\bar{Z}_k)}; \bar{\mu}_l^{(\bar{Z}_k)}, \Sigma_j^{(\bar{Z}_k)} + \Sigma_l^{(\bar{Z}_k)}) \right). \quad (7.23)$$

From (7.19), similarly lets calculate $U_{\bar{Y}_k}$, the upper bound for $H_{\bar{Y}_k}$, as

$$U_{\bar{Y}_k} = \sum_{j=0}^R v_j^{(\bar{Y}_k)} \log_2 \left(-\log_2 v_j^{(\bar{Y}_k)} + \frac{1}{2} \log_2 \left((2\pi e)^M \left| \Sigma_j^{(\bar{Y}_k)} \right| \right) \right), \quad (7.24)$$

where $u_j^{(\bar{Z}_k)} = v_j^{(\bar{Y}_k)} = \frac{e^{-\lambda} \lambda^j}{j!} \forall j = 0(1)R$. Hence,

$$\begin{aligned} U_{(\bar{Y}_k)} - L_{(\bar{Z}_k)} &= \sum_{j=0}^R \frac{e^{-\lambda} \lambda^j}{j!} \left(-\log_2 \left(\frac{e^{-\lambda} \lambda^j}{j!} \right) + \frac{1}{2} \log_2 \left((2\pi e)^M \left| \Sigma_j^{(\bar{Y}_k)} \right| \right) \right. \\ &\quad \left. + \log_2 \left(\sum_{l=0}^R \frac{e^{-\lambda} \lambda^l}{l!} \mathcal{N}(\bar{\mu}_j^{(\bar{Z}_k)}; \bar{\mu}_l^{(\bar{Z}_k)}, \Sigma_j^{(\bar{Z}_k)} + \Sigma_l^{(\bar{Z}_k)}) \right) \right). \quad (7.25) \end{aligned}$$

From (7.22) and (7.25), the k -th quantum channel capacity is defined as the channel capacity at the k -th transmission of the key given by

$$\begin{aligned} C_k &= \sum_{j=0}^R \frac{e^{-\lambda} \lambda^j}{j!} \left(-\log_2 \left(\frac{e^{-\lambda} \lambda^j}{j!} \right) + \frac{1}{2} \log_2 \left((2\pi e)^M \left| \Sigma_j^{(\bar{Y}_k)} \right| \right) \right. \\ &\quad \left. + \log_2 \left(\sum_{l=0}^R \frac{e^{-\lambda} \lambda^l}{l!} \mathcal{N}(\bar{\mu}_j^{(\bar{Z}_k)}; \bar{\mu}_l^{(\bar{Z}_k)}, \Sigma_j^{(\bar{Z}_k)} + \Sigma_l^{(\bar{Z}_k)}) \right) \right). \quad (7.26) \end{aligned}$$

This is the expression for the quantum channel capacity when the noise $\bar{Z}_k$ and the received signal $\bar{Y}_k$ are random vectors of dimension M . In scalar analogy, that is when the noise Z_k and the received signal Y_k are random variables with p.d.f.s (7.5) and (8.13) respectively, the expression of the capacity reduces to

$$C_k = \sum_{j=0}^R \frac{e^{-\lambda} \lambda^j}{j!} \left(-\log_2 \left(\frac{e^{-\lambda} \lambda^j}{j!} \right) + \frac{1}{2} \log_2 \left(2\pi e \sigma_j^{(Y_k)} \right) + \log_2 \left(\sum_{l=0}^R \frac{e^{-\lambda} \lambda^l}{l!} \mathcal{N} \left(\mu_j^{(Z_k)}; \mu_l^{(Z_k)}, \sigma_j^{(Z_k)^2} + \sigma_l^{(Z_k)^2} \right) \right) \right), \quad (7.27)$$

by putting $M = 1$, and replacing $|\Sigma_j^{(\bar{Y}_k)}|$ by $\sigma_j^{(Y_k)}$, $\bar{\mu}_j^{(\bar{Z}_k)}$ by $\mu_j^{(Z_k)}$, $\bar{\mu}_l^{(\bar{Z}_k)}$ by $\mu_l^{(Z_k)}$, $\Sigma_j^{(\bar{Z}_k)}$ by $\sigma_j^{(Z_k)^2}$ and $\Sigma_l^{(\bar{Z}_k)}$ by $\sigma_l^{(Z_k)^2}$, where each vector is replaced by its scalar analogue. Again $\mu_j^{(Z_k)} = \mu_{Z_k^{(2)}} + j$, $\sigma_j^{(Z_k)^2} = \sigma_{Z_k^{(2)}}^2$ and $\sigma_j^{(Y_k)^2} = T^2 \sigma_{X_k}^2 + \sigma_{Z_k^{(2)}}^2$, $\forall j = 0(1)R$.

Therefore, for a fixed Gaussian quantum channel, the quantum received signal can be calculated as the convolution product of the Gaussian distributed transmitted signal and the quantum noise signal. Considering the HQN and the Gaussian transmitted signal model as discussed above, the capacity of the quantum channel can be expressed as follows

$$\begin{aligned} C_k &= \sum_{j=0}^R \frac{e^{-\lambda} \lambda^j}{j!} \left(-\log_2 \left(\frac{e^{-\lambda} \lambda^j}{j!} \right) + \frac{1}{2} \log_2 \left(2\pi e (T^2 \sigma_{X_k}^2 + \sigma_{Z_k^{(2)}}^2) \right) \right. \\ &\quad \left. + \log_2 \left(\sum_{l=0}^R \frac{e^{-\lambda} \lambda^l}{l!} \mathcal{N} \left(\mu_{Z_k^{(2)}} + j; \mu_{Z_k^{(2)}} + l, 2\sigma_{Z_k^{(2)}}^2 \right) \right) \right) \\ &= \sum_{j=0}^R \frac{e^{-\lambda} \lambda^j}{j!} \left(-\log_2 \left(\frac{e^{-\lambda} \lambda^j}{j!} \right) + \frac{1}{2} \log_2 \left(2\pi e (T^2 \sigma_{X_k}^2 + \sigma_{Z_k^{(2)}}^2) \right) \right. \\ &\quad \left. + \log_2 \left(\sum_{l=0}^R \frac{e^{-\lambda} \lambda^l}{l!} \frac{1}{\sqrt{2}\sigma_{Z_k^{(2)}}\sqrt{2\pi}} e^{-\frac{1}{2} \left[\frac{j-l}{\sqrt{2}\sigma_{Z_k^{(2)}}} \right]^2} \right) \right), \end{aligned} \quad (7.28)$$

where

$$\mathcal{N} \left(\mu_{Z_k^{(2)}} + j; \mu_{Z_k^{(2)}} + l, 2\sigma_{Z_k^{(2)}}^2 \right) = \frac{1}{\sqrt{2}\sigma_{Z_k^{(2)}}\sqrt{2\pi}} e^{-\frac{1}{2} \left(\frac{\mu_{Z_k^{(2)}} + j - \mu_{Z_k^{(2)}}}{\sqrt{2}\sigma_{Z_k^{(2)}}} \right)^2}. \quad (7.29)$$

7.3.7 Asymptotic Secret Quantum Key Rate Estimation for FSO Satellite Quantum Channel

Revisiting the asymptotic SKR derivation from the non-asymptotic perspective is also beneficial. According to the asymptotic perspective, the secret

keys remain secure against general attacks, even in the finite-size regime. The determination of the asymptotic SKR given by [26],

$$K = \lim_{N \rightarrow \infty} \left\{ \frac{1}{N} \left(H(Y^{(N)}) - leak_{EC}^{(N)} \right) - \Psi(\Gamma^{(N)}) \right\} = \beta I_{AB} - \chi_{BE}, \quad (7.30)$$

where

$$\beta I_{AB} = \lim_{N \rightarrow \infty} \left\{ \frac{1}{N} \left(H(Y^{(N)}) - leak_{EC}^{(N)} \right) \right\}, \quad \chi_{BE} = \lim_{N \rightarrow \infty} \Psi(\Gamma^{(N)}). \quad (7.31)$$

Here $H(Y^{(N)})$ represents the empirical entropy of the sequence $Y^{(N)}$, with the superscript N explicitly indicating the dependence of these variables on the block length, the term $leak_{EC}^{(N)}$ denotes the number of bits disclosed during the error correction process, wherein Bob provides auxiliary information to Alice, facilitating her accurate prediction of Y . Furthermore, $\Psi(\Gamma^{(N)})$ measures Eve's accessible information denoted by χ_{BE} , which will be elucidated upon subsequently. This detail underlines the focus on the asymptotic behaviour of the SKR, allowing us to overlook discretization effects for this analysis. The utility of (7.30) lies in its guidance on calculating βI_{AB} and χ_{BE} as per the Devetak-Winter bound. This equation simplifies the determination of these critical parameters, which are essential for evaluating the efficiency and security of QKD systems in the context of quantum cryptography [28].

While the calculations of βI_{AB} and $\Psi(\Gamma)$ are relatively straightforward for a fixed Gaussian channel with consistent transmission efficiency and excess noise [140, 216], they become more complex for fading quantum channels, leading to varied findings in existing work. Specifically, employing Gaussian modulation allows for approaching the channel capacity, factoring in a reconciliation efficiency factor β , leading to [214],

$$\beta I_{AB} = \beta \frac{1}{N} \sum_{k=1}^N C_k, \quad (7.32)$$

where C_k is given by (7.28) $\forall k = 1(1)N$.

Apart from the generic HQN, the free-space satellite channel suffers from associated noise referred to as excess noise, denoted by ϵ . Furthermore, consider imperfections in Bob's detectors through two specific parameters, e.g., the detection efficiency η and the electronic noise ν_{ele} . The quantum channel is characterized by its transmission coefficient $T \leq 1$ and excess noise ϵ . The total added noise refers to the quantum channel's input due to losses $1/T - 1$, and the excess noise ϵ (in shot noise units) is given by $\chi_{line} = 1/T - 1 + \epsilon$ [140]. The signal then reaches Bob's detector, which is modeled by assuming that a factor further attenuates the signal η , the detection losses mixed with some thermal noise, specifically electronic noise ϑ_{ele} added by the detection electronics, expressed in shot noise units. The noise introduced by the realistic homodyne detector is $\chi_{hom} = (1 + \vartheta_{ele})/\eta - 1$ [140]. The total cumulative noise added between Alice and Bob specifically for the free-space quantum satellite channel is given by $\chi_{tot} = \chi_{line} + \chi_{hom}/T$, referred to as the channel input keys [140].

Now, focusing on the component χ_{BE} , the term $\Psi(\Gamma^{(N)})$ assesses the information Eve could potentially access. Specifically, $\Gamma^{(N)}$ provides a conservative estimation of the (average) covariance matrix associated with the state that Alice and Bob would theoretically share in an entanglement-based rendition of their protocol. The function Ψ is characterized as, $\Psi(\Gamma) = S(\boldsymbol{\rho}_{AB}) - S(\boldsymbol{\rho}_E^b)$, where $S(\boldsymbol{\rho})$ is defined as the von Neumann entropy of the quantum state $\boldsymbol{\rho}$ [140]. For an n -mode Gaussian state ρ , this entropy is expressed as $S(\boldsymbol{\rho}) = \sum_j G\left(\frac{\lambda_j - 1}{2}\right)$, where $G(x) = (x + 1) \log_2(x + 1) - x \log_2 x$, and λ_j are the symplectic eigenvalues of the covariance matrix $\boldsymbol{\gamma}$ characterizing $\boldsymbol{\rho}$ [216],[217]. For the sake of simplicity, let us consider the average variance of all transmitted signals $\sigma_X = \frac{1}{2N} \sum_{k=1}^{2N} \sigma_{X_k}$, where σ_{X_k} is given by (7.2) $\forall k = 1(1)2N$.

The entropy $S(\boldsymbol{\rho}_{AB})$ is calculated from the symplectic eigenvalues λ_1, λ_2 of the covariance matrix $\boldsymbol{\gamma}_{AB} = \begin{bmatrix} \gamma_A & \sigma_{AB} \\ \sigma_{AB}^t & \gamma_B \end{bmatrix}$, and the symplectic eigenvalues of $\boldsymbol{\gamma}_{AB}$ are given by

$$\lambda_{1,2}^2 = \frac{1}{2} \left[A \pm \sqrt{A^2 - 4B} \right], \quad (7.33)$$

where $A = \sigma_X^2(1 - 2T) + 2T + T^2(\sigma_X^2 + \chi_{line})^2$, and $B = T^2(\sigma_X^2 \chi_{line} + 1)^2$. Similarly, the entropy $\boldsymbol{\rho}_E^b$ is determined from the symplectic eigenvalues $\lambda_3, \lambda_4, \lambda_5$ of the covariance matrix characterizing the state $\boldsymbol{\rho}_E^{Y_B}$ of Eve's system conditional on Bob's measurement outcome Y_B . The symplectic eigenvalues λ_3, λ_4 are given by

$$\lambda_{3,4}^2 = \frac{1}{2} \left[C \pm \sqrt{C^2 - 4D} \right], \quad (7.34)$$

where

$$C = \frac{\sigma_{X_k}^2 \sqrt{B} + T(\sigma_X^2 + \chi_{line}) + A\chi_{hom}}{T(\sigma_X^2 + \chi_{tot})}, \quad D = \sqrt{B} \frac{\sigma_X^2 + \sqrt{B}\chi_{hom}}{T(\sigma_X^2 + \chi_{tot})}, \quad (7.35)$$

and the last symplectic eigenvalue is $\lambda_5 = 1$. The Holevo information bound is given by [36, 140],

$$\chi_{BE} = G\left(\frac{\lambda_1 - 1}{2}\right) + G\left(\frac{\lambda_2 - 1}{2}\right) - G\left(\frac{\lambda_3 - 1}{2}\right) - G\left(\frac{\lambda_4 - 1}{2}\right), \quad (7.36)$$

and from (7.30), (8.31) and (7.36) the SKR is given as,

$$\begin{aligned} K &= \beta I_{AB} - \chi_{BE} \\ &= \beta \frac{1}{N} \sum_{k=1}^N C_k - \left[G\left(\frac{\lambda_1 - 1}{2}\right) + G\left(\frac{\lambda_2 - 1}{2}\right) - G\left(\frac{\lambda_3 - 1}{2}\right) - G\left(\frac{\lambda_4 - 1}{2}\right) \right]. \end{aligned} \quad (7.37)$$

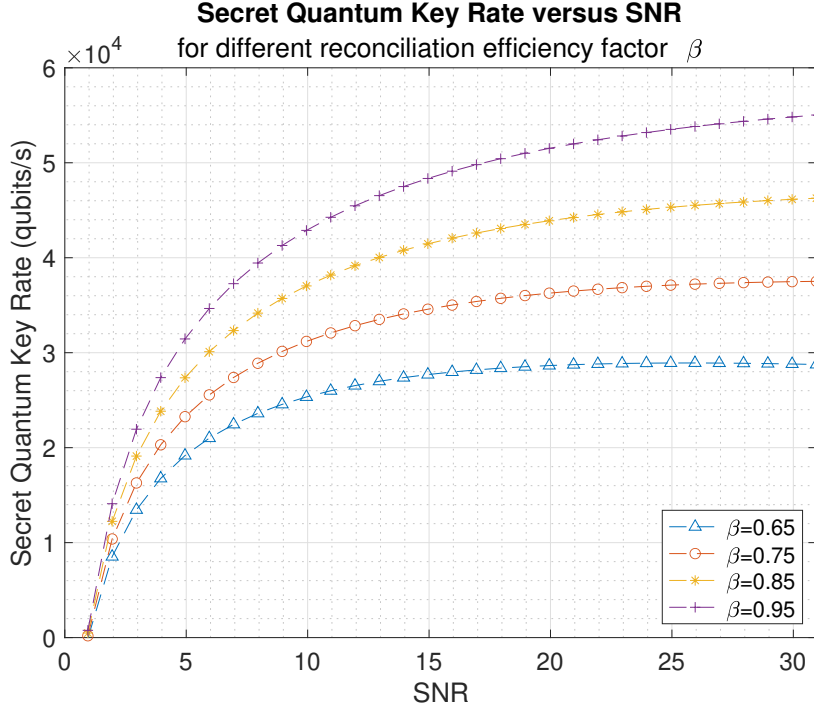


Figure 7.5: Impact of Reconciliation Efficiency on Quantum SKR.

7.3.8 A comparison study with finite-size SKR for FSO satellite quantum channel

The security analysis of collective attacks in the finite-key setting for RR-CV-QKD is discussed. In practical implementations, finite-size effects introduce constraints on the SKR due to statistical uncertainties in parameter estimation. For a block size N of pulses, $N - n$ pulses are allocated for channel parameter estimation, with the remaining n pulses used for key generation. The finite-size analysis of CV-QKD under collective attacks refines the expression for the SKR. The finite-key SKR K_{fin} , under reverse reconciliation, is expressed as

$$K_{fin} = \frac{n}{N} (\beta I_{AB} - \chi_{BE} - \Delta(n)) = \frac{n}{N} [\beta I(a : b) - S_{\epsilon_{PE}}(b : E) - \Delta(n)], \quad (7.38)$$

where $\Delta(n)$ the correction parameter accounts for finite-size effects, $S_{\epsilon_{PE}}(b : E)$ is Eve's conditional entropy about Bob's key, adjusted for parameter estimation inaccuracies with a failure probability ϵ_{PE} . The correction term $\Delta(n)$, which encapsulates finite-size effects, decreases as n increases. The correction term is expressed as

$$\Delta(n) = (2 \dim \mathcal{H}_X + 3) \sqrt{\frac{\log_2(2/\bar{\epsilon})}{n}} + \frac{2}{n} \log_2 \left(\frac{1}{\epsilon_{PA}} \right), \quad (7.39)$$

where $\dim \mathcal{H}_X = 2$ is the dimensionality of the Hilbert space for the raw key variable x , and $\bar{\epsilon}$ and ϵ_{PA} are set to 10^{-10} to balance security and practicality. The first term governs the convergence speed of the smooth

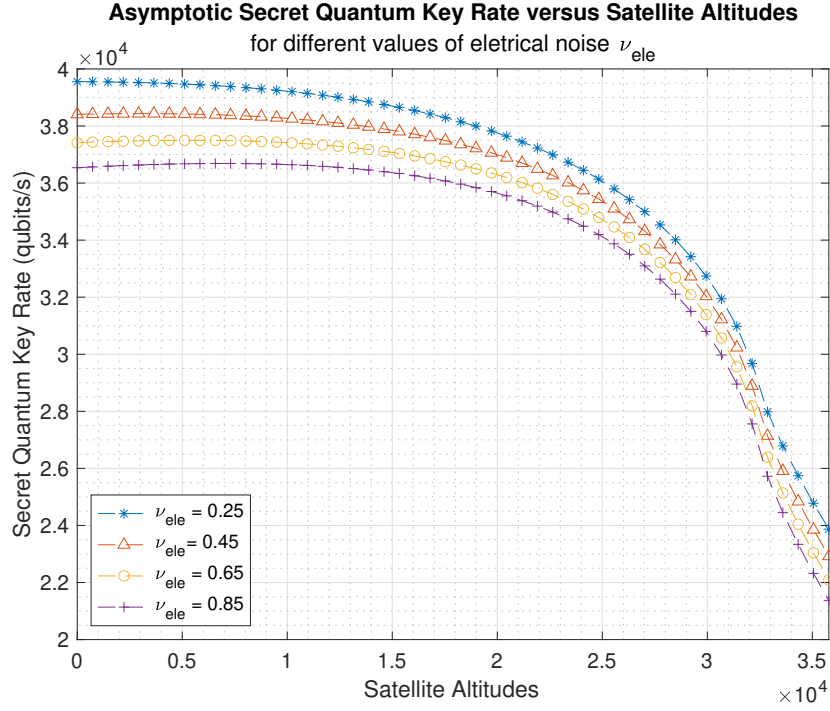


Figure 7.6: Impact of Electrical Noise on Quantum SKR.

minimum entropy, while the second term accounts for the probability of private key amplification failure. These terms highlight the influence of finite-size effects on the SKR, stressing the importance of optimizing n and N for both security and efficiency. The correction parameter $\Delta(n)$ is approximated as $\Delta(n) \approx 7 \cdot \sqrt{\log_2 \left(\frac{2/\bar{\epsilon}}{n} \right)}$ where $\bar{\epsilon}$ the smoothing parameter is set to 10^{-10} . By incorporating finite-size effects into the analysis, the gap between theoretical predictions and practical implementations is addressed. This addition reveals the trade-offs between security and performance, ensuring that the results apply to satellite-based CV-QKD operations, where practical constraints such as orbital mechanics, power limitations, and data transfer windows must be considered.

It is proven that for all bipartite quantum states ρ_{AB} with covariance matrix γ_{AB} , the secret key rate $K(\rho_{AB})$ satisfies the inequality, $K(\rho_{AB}) \geq K(\rho_{G_{AB}})$. This implies that $K(\rho_{G_{AB}})$ serves as a lower bound on the secret key rate for any protocol, including non-Gaussian ones, under collective attacks (including non-Gaussian attacks). The key requirement for this result to hold is that Alice and Bob rely on the second-order moments of the quadratures to compute this bound. Specifically, for the Gaussian-CV setting, Eve's optimal attack is Gaussian, and in this case, the bound is saturated, meaning $K(\rho_{AB}) = K(\rho_{G_{AB}})$. This results in the following lower bound on the overall secure key rate, expressed as a weighted sum of the key rates from individual segments $K = \sum_i \max \left(0, \frac{n_i}{N} [bI_{AB} - \chi_{BE} - \Delta(n_i)] \right)$. Here, n_i represents the number of events in segment i , and N is the total number of segments. The expression ensures that only positive contribu-

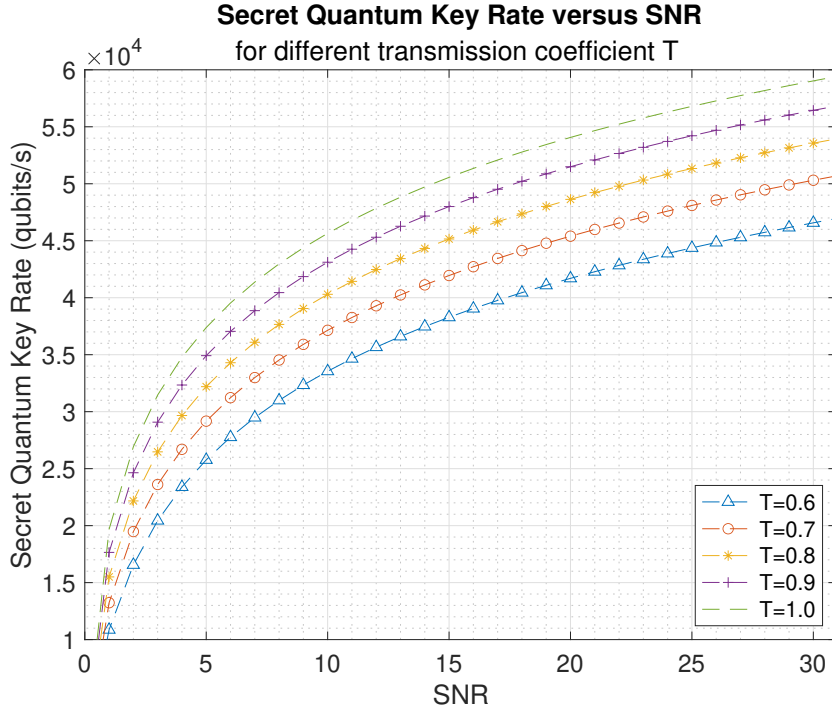


Figure 7.7: Impact of Transmission Coefficient on Quantum SKR

tions to the key rate are considered, with the sum taken over all segments. In this case, n_i represents the raw key length for segment i , with N_i being the number of data points for that segment such that, $\sum_i N_i = N$. Out of the N_i data points, $N_i - n_i$ are used for segment channel estimation. The weight for each segment is determined by the relative size of n_i/N , where N is the overall block size for a given satellite pass. This weight reflects the contribution of each segment to the total secure key rate, ensuring that larger segments (with more data points) have a proportionally greater influence on the overall key rate.

This work scrutinizes practical asymptotic QKD rates by introducing a hybrid quantum channel model tailored for free-space satellite quantum communication. This model is tailored to the fading properties present in satellite-to-ground links while considering the satellite's dynamic orbit. These security analyses include considering asymptotic and finite-size QKD and computable security under collective attack, which is crucial for practical implementations.

This chapter expands the theoretical foundation and practical application of quantum communications via satellite links, extending existing analyses from ground-based free-space settings to the more complex scenario of ground-to-satellite communications. This transition involves longer travel distances of optical signals through the atmosphere, which must account for variable altitudes and zenith angles, whether in uplink or downlink configurations. Crucially, this environment includes additional atmospheric disturbances, such as refraction, extinction, and turbulence, alongside varied sources of background noise, including planetary albedos and sky bright-

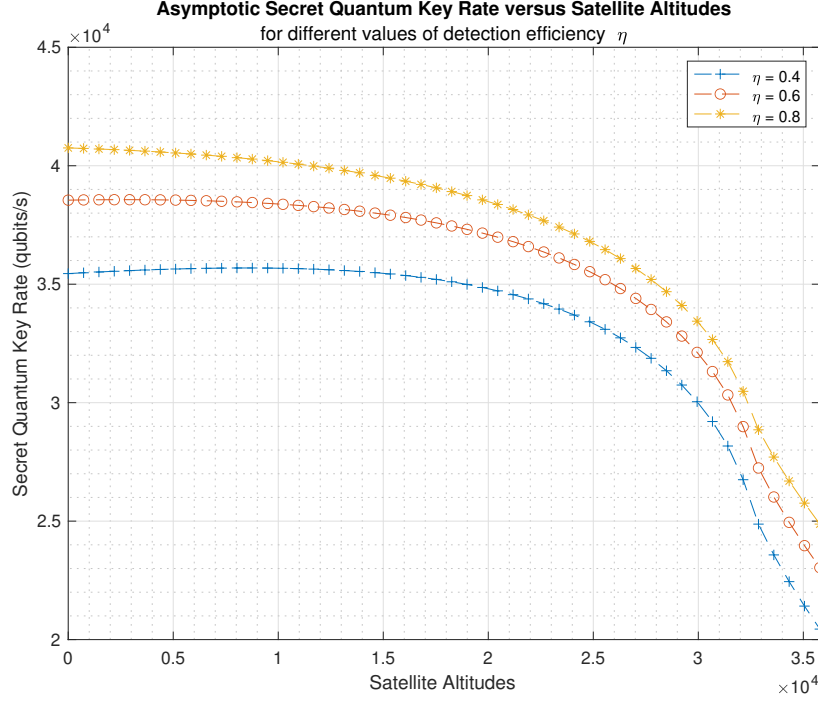


Figure 7.8: Impact of Detection Efficiency on Quantum SKR

ness. These elements are crucial in modeling the conditions under which quantum communication occurs, offering a detailed understanding of the potential for secure key generation and entanglement distribution using satellites, regardless of the time of day or link direction. It demonstrates that asymptotic QKD via CV RR systems is feasible and highly effective for downlink and uplink configurations operating during daytime and nighttime. Furthermore, it highlights the superiority of satellite-based quantum key distribution over traditional existing networks.

7.4 Results: Numerical Analysis

The section delves into the analysis of asymptotic quantum SKR in free-space atmospheric satellite quantum channels, focusing on its relationship with the SNR and satellite altitude. The study explores how various channel parameters, including reconciliation efficiency, electrical noise, transmission coefficient, transmission efficiency, excess noise, detection efficiency, and quantum Poissonian noise, influence the asymptotic SKR in the context of free-space atmospheric satellite quantum channels. The findings offer a comprehensive understanding of the factors affecting the performance of QKD in satellite-based systems.

Reconciliation efficiency β is a crucial factor that impacts the asymptotic quantum SKR. This efficiency measures the effectiveness of error correction between the sender (Alice) and the receiver (Bob). Fig. 7.5 illustrates the dependence of quantum SKR on different β values from 0.65, 0.75, 0.85, and

0.95, keeping other parametric values fixed with $\lambda = 2$, $\epsilon = 0.63$ shot noise units, $T = 1$, $\eta = 0.66$, and $\nu_{ele} = 0.41$ shot noise units. The sensitivity of **SKR** to β is significant because it directly affects the amount of mutual information that can be converted into a secure key. A higher β value indicates more efficient reconciliation, leading to a higher **SKR**, as fewer bits are lost during error correction. Conversely, a lower β reduces the **SKR**, even under ideal channel conditions, because a larger portion of shared information must be discarded. The results underscore the importance of optimizing β to maximize **SKR** in satellite-based quantum channels.

Electrical noise ν_{ele} represents the classical noise introduced by detection and electronic processing systems at the receiver's end. Fig. 7.6 illustrate the dependence of asymptotic quantum **SKR** on different ν_{ele} values ranging from 0.25, 0.45, 0.65 and 0.85 shot noise units, with $\lambda = 2$, $\epsilon = 0.005$ shot noise units, $\beta = 0.95$, $\eta = 0.606$, and T varies from 0.3 to 1 in decreasing order over the satellite altitude. The variations ν_{ele} within its permissible range significantly impact the **SKR**. This indicates that electrical noise is a primary limiting factor for **SKR** in these channels with respect to satellite altitudes. The analysis reveals that within its permissible range, ν_{ele} , it has a significant effect on the **SKR** under different ranges of satellite altitudes. This suggests that the system is designed to function effectively even with typical levels of electrical noise encountered in free-space atmospheric satellite channels. The sensitivity of **QKD** protocols to moderate levels of electrical noise due to error correction and privacy amplification steps explains this impact on the asymptotic **SKR** of the satellite-based quantum channels. However, if ν_{ele} exceeds the permissible range, it could degrade the **SKR** by increasing the error rate beyond what can be corrected, thereby reducing the amount of secure key generated. This highlights the importance of maintaining low electrical noise levels while emphasizing the system's resilience within the tested parameters.

The transmission coefficient T is a vital parameter influencing the asymptotic quantum **SKR**. T reflects the fraction of quantum states successfully transmitted from Alice to Bob through the terrestrial quantum channel. A higher transmission coefficient improves **SKR** by ensuring that more quantum states are transmitted to the receiver. The **SKR**'s sensitivity to T is substantial because it encapsulates the effects of absorption, scattering, and other losses during quantum state transmission. In free-space quantum communication, atmospheric conditions and distance significantly impact T , particularly on satellite channels. Fig. 7.7 illustrates the dependence of quantum **SKR** on different T values ranging from $T = 0.6, 0.7, 0.8, 0.9$ up to 1 with setting other parametric values as $\lambda = 2$, $\epsilon = 0.63$ shot noise units, $\beta = 0.95$, $\eta = 0.606$ and $\nu_{ele} = 0.41$ shot noise units. The higher transmission coefficients lead to better **SKR** performance, as fewer quantum states are lost in transit. Optimizing T is, therefore, critical for enhancing **SKR**, especially in satellite-based **QKD** systems where atmospheric conditions and distance can greatly influence transmission efficiency.

Detection efficiency η is crucial for accurately measuring quantum states.

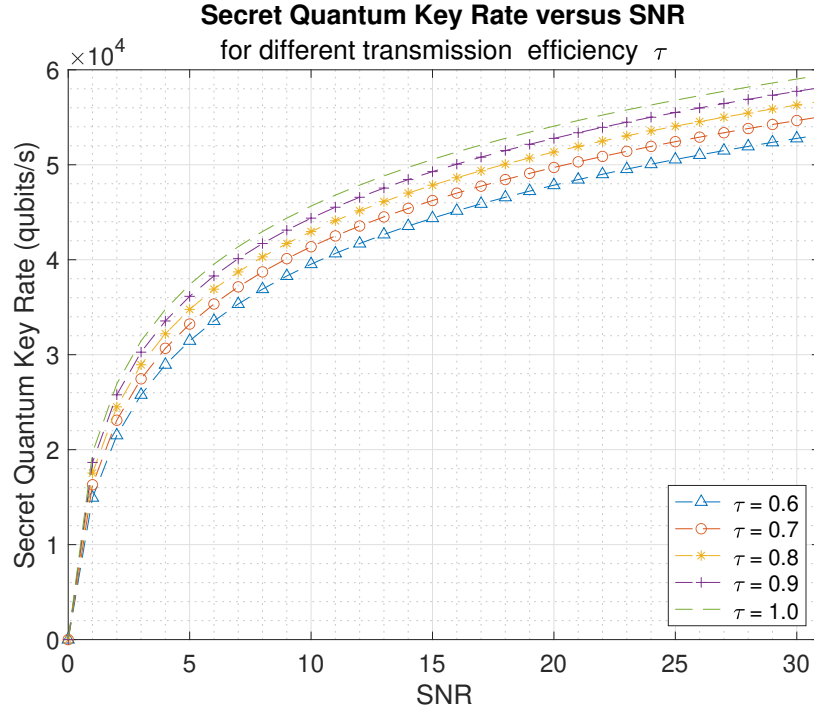


Figure 7.9: Impact of Transmission Efficiency on Quantum SKR

It determines the fraction of incoming quantum states that are successfully detected and measured. Fig.7.8 illustrates the dependence of asymptotic quantum SKR on different η values ranging from 0.4, 0.6 and 0.8, with $\lambda = 2$, $\epsilon = 0.35$ shot noise units, $\beta = 0.95$, $\nu_{ele} = 0.41$ shot noise units, and T varies from 0.3 to 1 in decreasing order over the satellite altitude. The SKR's insensitivity to η the observed range implies that the detection mechanism in the system is robust and reliable. Within the studied range, most transmitted states that reach the receiver are successfully detected, leaving the SKR largely unaffected by variations in η . However, if η were significantly lower, it would decrease the detected signal, reducing the SKR. This work illustrates that changes in η do not substantially impact the SKR, indicating the system's reliability under varying conditions.

Transmission efficiency τ is another critical factor affecting the asymptotic quantum SKR. This parameter measures the effectiveness with which quantum states are transmitted through the channel without being lost due to absorption, scattering, or diffraction. Fig.7.9 demonstrates the variation of SKR with different τ values ranging from $\tau = 0.6, 0.7, 0.8, 0.9$ up to 1, and $T = \sqrt{\tau}$ with setting other parametric values as $\lambda = 2$, $\epsilon = 0.35$ shot noise units, $\beta = 0.95$, $\eta = 0.606$ and $\nu_{ele} = 0.41$ shot noise units. The SKR is highly sensitive to τ because higher transmission efficiency means more quantum states reach the receiver, increasing the likelihood of successful QKD and, consequently, a higher SKR. Conversely, lower τ results in more quantum states being lost in transit, reducing the usable data for key generation and decreasing the SKR. It emphasizes the importance of optimizing τ to enhance SKR in FSO satellite-based quantum channels.

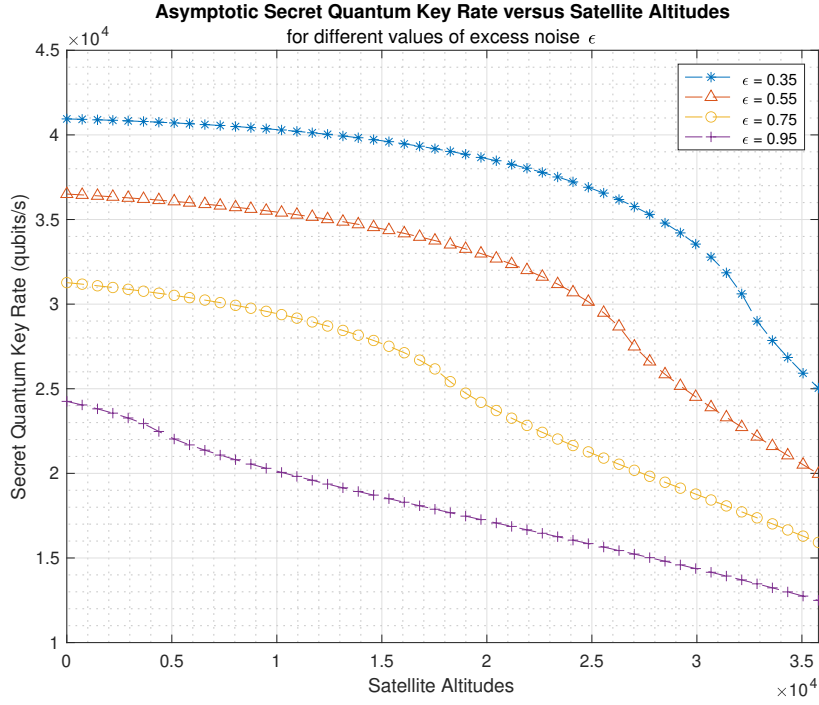


Figure 7.10: Impact of Excess Noise on Asymptotic Quantum SKR based on satellite altitude.

Excess noise ϵ represents the noise in the quantum channel beyond what is expected from quantum mechanical limits. Fig. 7.10 demonstrate the variation of asymptotic SKR with different ϵ values 0.35, 0.55, 0.75, and 0.95 shot noise units, with setting other parametric values as $\lambda = 2$, $\beta = 0.95$, $\eta = 0.606$, $\nu_{ele} = 0.041$ shot noise units, and T varies from 0.3 to 1 in decreasing order over the satellite altitude. The SKR shows high sensitivity to ϵ within its permissible range of satellite altitudes, indicating that modern QKD protocols are vulnerable against reasonable noise levels. However, if ϵ exceeds certain thresholds, it would introduce additional errors that could not be reconciled, reducing the SKR. This work demonstrates that excess noise has a significant impact on the SKR within the permissible satellite altitude range. This suggests that the system needs to be robust to tolerate typical environmental and instrumental noise levels without significant degradation in performance.

Quantum Poissonian noise λ significantly influences the asymptotic quantum SKR. This parameter represents the level of quantum Poissonian noise in the channel, originating from the random nature of photon emission in quantum communication systems. Fig. 7.11 illustrates the dependence of quantum SKR on different λ values ranging from 2, 3, 4, 5 and 6, with $\epsilon = 0.43$ shot noise units, $\beta = 0.95$, $\nu_{ele} = 0.41$ shot noise units, $\eta = 0.606$, and $T = 1$. A larger λ increases the number of noise photons present, raising the error rate and reducing the SKR, as more signals may be confused with noise rather than legitimate quantum states. Conversely, a smaller λ implies fewer noise photons, thereby improving the SKR by increasing the

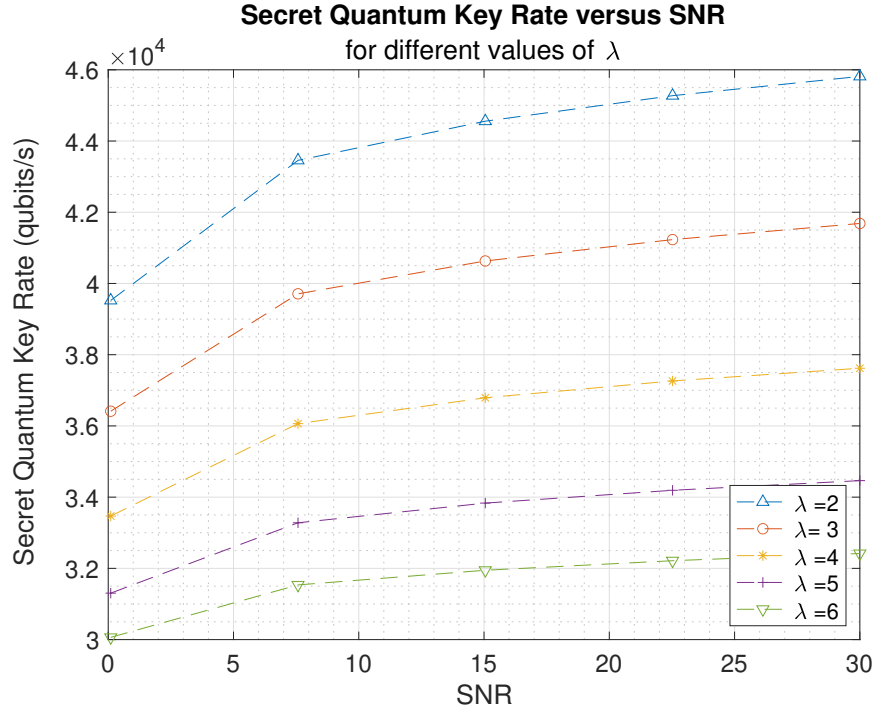


Figure 7.11: Impact of Quantum Poissonian Noise on Quantum SKR

SNR and making it easier to distinguish between quantum states carrying key information and noise. This work demonstrates how different λ values can substantially affect the SKR. Optimizing λ is essential for achieving high SKR in free-space atmospheric satellite channels.

Finally, the analysis examines how the finite size affects quantum SKR. This analysis involves the comparison of asymptotic SKR with finite-size quantum SKR that varies over satellite altitudes h . For the finite-size regime, the block size n has been considered as 10^6 , 10^8 , 10^{10} , respectively, and for the asymptotic size $N = 10^{20}$ has been considered. Fig. 7.12 shows that the asymptotic and finite-size quantum SKRs decrease as satellite altitudes increase considering transmission efficiency τ as a function of satellite altitudes, setting the primary parametric values as $\epsilon = 0.35$ shot noise units, $\beta = 0.95$, $\nu_{ele} = 0.41$ shot noise units, $\eta = 0.606$, and $\lambda = 2$. As satellite altitudes increase, the transmission efficiency τ decreases due to atmospheric attenuation, beam divergence, and other losses over high altitudes. This reduction in τ leads to a lower SKR as fewer quantum states reach the receiver. For CV satellite quantum channel, the findings underscore the importance of optimizing transmission efficiency and noise management strategies to ensure effective quantum communication over extended altitudes, where losses are more pronounced.

This chapter comprehensively analyses the factors influencing the asymptotic quantum SKR in free-space atmospheric satellite quantum channels. The study highlights the significant impact of reconciliation efficiency β , electrical noise ν_{ele} , transmission coefficient T , detection efficiency η , transmission efficiency τ , excess noise ϵ , and quantum Poissonian noise λ on

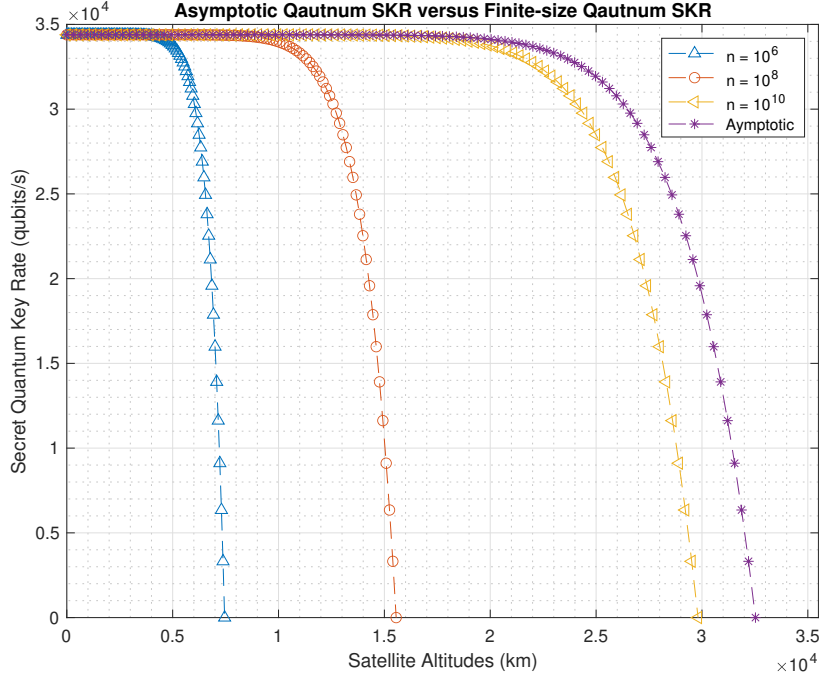


Figure 7.12: Asymptotic Quantum SKR versus Finite-size Quantum SKR with respect to Satellite altitudes.

satellite-based quantum SKR. In line with this, the asymptotic SKR has been compared with finite-size SKR within the permissible ranges of satellite altitudes. The results emphasize optimizing these parameters to maintain high SKR levels, particularly as satellite altitudes increase. This investigation lays the groundwork for future work to enhance the performance of satellite-based quantum communication systems, ensuring the secure and efficient transmission of quantum information across global distances.

7.5 Conclusion

This work advanced the application of asymptotic QKD in free-space atmospheric satellite-based quantum communication. It has developed a novel free-space atmospheric satellite quantum channel model based on an HQN architecture and investigated the critical parameters influencing the asymptotic quantum SKR of such channels. Unlike existing models that consider noise in quantum channels as purely Gaussian distributed, this model incorporates a hybrid noise framework that includes both quantum Poissonian noise and classical AWGN. This approach acknowledges the dual vulnerabilities of quantum channels to quantum and classical noise, providing a more realistic assessment of the asymptotic SKR. The chapter identifies several critical parameters significantly impacting the asymptotic SKR in free-space atmospheric satellite quantum channels. These parameters include reconciliation efficiency β , electrical noise ν_{ele} , transmission coefficient T , detection efficiency η , transmission efficiency τ , excess noise ϵ ,

and quantum Poissonian noise λ . These findings highlight that optimizing these parameters is essential for maximizing the SKR and ensuring robust quantum communication. Furthermore, the work concludes that finite-size SKR decreases more rapidly than asymptotic quantum SKR with increasing satellite altitude. This declination is attributed to increased losses and reduced signal strength over longer distances, underscoring the importance of maintaining high transmission efficiency and effective noise management strategies in satellite-based QKD systems. This work contributed to the field by proposing a more realistic quantum channel model and identifying the influential factors affecting the asymptotic quantum SKR using a free-space atmospheric CV satellite quantum communication channel under collective attack with the RR framework. The knowledge generated in this chapter work enhances the performance and security of satellite-based quantum communication systems, facilitating the global transmission of quantum information. In Chapter 8, the HQN model has been applied to the finite-regime QKD in satellite-based quantum communication. In that chapter, it has been discussed how the finite-regime QKD depends on various parametric factors, such as the total time of effective communication and zenith angle, under a satellite-based quantum communication system.

Chapter 8

A Hybrid Noise Model for Satellite Quantum Channels: CV-QKD in the Finite-Size Regime

8.1 Introduction

This chapter develops a hybrid quantum channel model tailored for finite-regime QKD in free-space satellite quantum communication. The model addresses the fading characteristics of satellite-to-ground links while incorporating the dynamics of satellite orbits. By conducting a comprehensive security analysis under finite-size effects and collective attacks, the research bridges the theoretical and practical aspects of satellite-based QKD. Critical parameters, such as reconciliation efficiency, transmission coefficient, detection efficiency, receiver telescope aperture, beam waist, and adequate communication time, are systematically investigated to optimize the secret key rate. The study reveals key trade-offs between the influence of satellite altitude on communication windows, noise levels, and synchronization, which significantly impact quantum channel efficiency. The model improves the accuracy of free-space quantum channel evaluations by presenting a hybrid noise framework that combines quantum Poissonian noise with classical AWGN. This chapter's numerical results demonstrate the feasibility and robustness of finite-regime QKD for uplink and downlink configurations in various atmospheric conditions, highlighting the superiority of satellite-based quantum communication over conventional networks.

A novel hybrid satellite quantum channel model is proposed for finite-size key quantum key distribution, integrating a hybrid noise framework that accounts for quantum Poissonian noise and classical AWGN. Leveraging the broader range of quantum states available in CV-QKD, the model significantly enhances SKR performance under finite-size effects. Understanding the interplay between orbital geometry, atmospheric losses, and finite-size effects is critical for deploying CV-QKD in satellite-based networks. Atmo-

spheric attenuation and beam divergence, coupled with satellite dynamics like changing zenith angles and communication windows, pose significant challenges.

The findings contribute to understanding the critical parameters influencing CV-QKD systems, such as reconciliation efficiency, transmission coefficient, detection efficiency, and beam waist. This approach addresses the challenges posed by finite-size effects and sets the stage for scalable and secure satellite-based quantum communication, bridging the gap between theoretical advancements and practical deployment in global quantum networks. The main aspects of this chapter are summarized as follows,

- Proposed hybrid quantum channel model accounts for the fading characteristics of finite-regime QKD utilizing free-space satellite links, including the zenith angle, satellite altitude, and communication time. This chapter incorporates finite-size effects and composable security under collective attacks, bridging gaps between theory and practice in satellite-based quantum communication.
- This chapter examines key parameters, including reconciliation efficiency, transmission coefficient, detection efficiency, receiver telescope aperture, and beam waist. The chapter's theme highlights trade-offs, including the impact of varying satellite altitudes and light source wavelengths on secure key rates, optimizing performance for practical satellite-based CV-QKD systems.
- The chapter's framework models atmospheric turbulence, beam divergence, and fading noise, providing a realistic analysis of transmission coefficient fluctuations and improving the feasibility of secure global quantum communication.

8.2 System Architecture

In this chapter, the Gaussian quantum channel model for CV QKD builds on foundational works [18, 21, 22, 23], offering a detailed framework for finite-size SKR calculations. The model, briefly summarized here, emphasizes its critical role in characterizing and optimizing finite-size CV-QKD systems.

8.2.1 Gaussian Quantum Channel and Noise Modeling

The CV Gaussian quantum channel model utilized in this study builds upon the foundational framework established in our previous works [18, 21, 22, 23]. Readers seeking a comprehensive understanding are encouraged to refer to these prior studies for in-depth insights.

Finite-size CV-QKD implementations are susceptible to statistical fluctuations due to the limited sample size of quantum states used for parameter estimation. The noise model of the quantum channel is critical for accurately deriving achievable key rates in this regime. Under hybrid noise

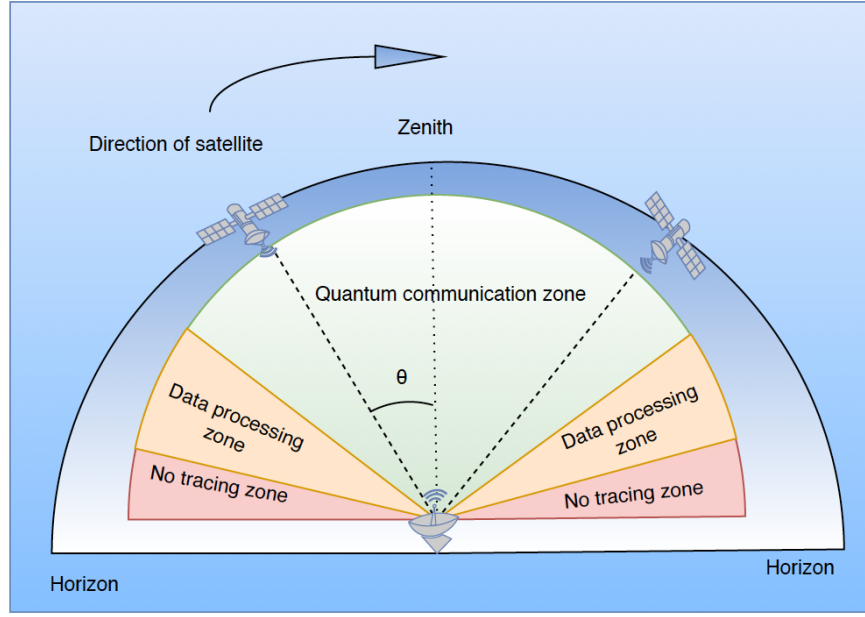


Figure 8.1: The diagram visually emphasizes how the satellite’s position relative to the ground station affects the feasibility and efficiency of quantum communication. The central green region is crucial for secure QKD, while the other zones highlight the limitations imposed by satellite motion and atmospheric conditions.

constraints, the generalized quantum channel equation is, $Y = X + N$, where X is the transmitted quadrature variable, Y is the received quadrature, and N , the total noise, is expressed as: $N = N^{(1)} + N^{(2)}$, with $N^{(1)}$ representing quantum Poisson shot noise and $N^{(2)}$ denoting classical AWGN [18, 21]. This additive noise formulation precisely captures the hybrid noise characteristics, enabling detailed modeling of quantum channels in finite-size analyses. By leveraging this comprehensive noise model, this study provides crucial insights into the interplay of quantum and classical noise in CV-QKD systems, laying a robust foundation for optimizing secure key generation under real-world constraints.

In satellite-based CV-QKD systems, several noise sources impact signal quality and channel efficiency. Diffraction causes optical beam spreading, leading to divergence losses, which can be mitigated by optimising receiver apertures or using shorter wavelengths, though this increases cost and alignment sensitivity. Atmospheric turbulence induces beam wandering and scintillation, degrading signal quality, especially in uplink scenarios, while downlink turbulence is less severe due to reduced atmospheric interaction. Thermal noise, more prominent in downlink transmissions, varies with diurnal conditions. Hybrid noise combines quantum noise (e.g., photon loss) and classical additive noise (e.g., thermal fluctuations), complicating SKR optimisation. Precise modelling of these effects, integrating quantum and classical noise, is crucial to designing robust quantum communication

protocols for realistic atmospheric quantum channels.

8.2.2 Finite-Size SKR in CV-QKD Systems

Alice generates a sequence of $2M$ Gaussian-distributed real random variables, $X_1, X_2, \dots, X_{2M}$, each with variance σ_X^2 , to represent M coherent states $|\alpha_m\rangle$, where $\alpha_m = X_{2m-1} + iX_{2m}$. These variables define M coherent states, $|\alpha_1\rangle, |\alpha_2\rangle, \dots, |\alpha_M\rangle$, transmitted through a quantum channel. Each coherent state's amplitude and phase are encoded by the real and imaginary components of $\alpha_m \in \mathbb{C}$, with $i = \sqrt{-1}$. The quantum channel delivers these states to Bob, who performs homodyne detection, simultaneously measuring both quadratures of the received signal. For the m th channel use, Bob obtains two measurements, Y_{2m-1} and Y_{2m} , corresponding to the transmitted quadratures X_{2m-1} and X_{2m} . This results in a raw key string $\mathbf{Y} = (Y_1, Y_2, \dots, Y_{2M})$. This protocol is particularly effective in low-transmission-efficiency scenarios, particularly when using [RR](#). The hybrid quantum noise N_m associated with the m th channel is modeled as a combination of quantum Poissonian noise $N_m^{(1)}$ and classical [AWGN](#) $N_m^{(2)}$, expressed as $N_m = N_m^{(1)} + N_m^{(2)}$, for $m \in \{1, \dots, M\}$.

The quantum Poissonian noise follows the [p.m.f.](#), $f_{N_m^{(1)}}(j) = \frac{e^{-\lambda} \lambda^j}{j!}$, where $\lambda \geq 0$, $\lambda, j \in \{0\} \cup \mathbb{N}$, and $\mathbb{N}$ denotes the set of natural numbers. The classical [AWGN](#) $N_m^{(2)}$ follows a Gaussian distribution with mean $\mu_{N_m^{(2)}}$ and variance $\sigma_{N_m^{(2)}}^2$. To evaluate the finite-size [SKR](#) in a [CV-QKD](#) system over fading channels, this chapter incorporates finite-size effects and realistic channel conditions. The analysis emphasises the interplay between channel fading and hybrid noise, presenting a robust model to address practical challenges.

This chapter explores a quantum satellite communication framework enabling bidirectional transmission between a ground station and a satellite. Within this setup, Alice acts as the sender, encoding information into quantum states—either [CV](#) states or qubits—transmitted via a satellite-based [FSO](#) channel. Bob, as the receiver, decodes these states, irrespective of the sender's or receiver's location. Eve, the eavesdropper, attempts to intercept transmissions at any point along the channel. Environmental factors, such as free-space diffraction, atmospheric turbulence, and thermal noise, significantly impact the [FSO](#) channel, introducing unique challenges in both uplink (ground-to-satellite) and downlink (satellite-to-ground) configurations. This comprehensive modeling approach provides valuable insights into mitigating these challenges to ensure robust and secure quantum communication.

The [FSO](#) satellite channel is mathematically modeled as [\[23, 26\]](#),

$$Y = \sqrt{\tau}X + N, \quad (8.1)$$

where X is Alice's transmitted quantum signal, Y is the signal received by Bob, N represents hybrid noise comprising both quantum and classical

Table 8.1: Physical Parameter's Theoretical Value for QKD using Satellite Quantum Communication Channel

Physical parameter	Symbol	Value
Poisson parameter	λ	2
Reconciliation efficiency	β	0.95
Electronic noise	ν_{ele}	0.041
Detection efficiency	η_{det}	0.606
Receiver telescope aperture	ϵ	0.005
Satellite altitude	h	2000 km
Photon temporal width	t	3 ns
Beam waist	w_0	5 cm
Signal-to-noise ratio	SNR	40 dB
Transmitter telescope aperture	a_s	10 cm
Receiver telescope aperture	a_r	30 cm
Wavelength	w	800 nm
Gravitational constant	G	$6.674 \times 10^{-11} Nm^2/kg^2$
Earth's mass	M_E	$5.972 \times 10^{24}kg$

components, and τ denotes the channel's overall transmission efficiency. The transmission coefficient, $T = \sqrt{\tau}$, is a critical parameter influencing the achievable SKR. In CV-QKD, the primary objective is to maximize the SKR shared between Alice and Bob while minimizing the information accessible to Eve, despite the presence of noise and channel imperfections.

Atmospheric transmittance is probabilistically modeled using a log-normal distribution [23], as expressed:

$$\mathcal{P}(\tau) = \frac{1}{\sqrt{2\pi\sigma\tau}} e^{-\frac{1}{2}\left(\frac{\ln \tau + \ln \tilde{\tau}}{\sigma}\right)^2}, \quad (8.2)$$

where $-\ln \tilde{\tau}$ represents the logarithm of the mean atmospheric transmittance, σ is the variance of $-\ln \tau$, characterizing atmospheric turbulence, and the zenith angle contributes significantly to atmospheric transmittance. Accurate modeling of fading channels is essential for calculating key rates in free-space satellite communication, where atmospheric turbulence strongly impacts transmission efficiency.

8.2.3 Aggregated Quantum SKR for Satellite Quantum Channel

Analyzing the transmission coefficient (T) across varying satellite-to-ground distances is pivotal for optimizing satellite optical communication systems. Given the variability of atmospheric turbulence, the transmission coefficient

T_k fluctuates but is assumed to remain stable over short intervals [23, 26]. This stability enables Alice and Bob to adapt error correction strategies based on an approximate knowledge of T_k . For consecutive uses of the quantum channel, it is practical to assume a fixed value of T_k , denoted as T_g , representing an aggregated transmission coefficient for a specific group g . For each group, the aggregated transmission coefficient T_g is treated as a constant, simplifying the analysis and adjustment of quantum communication protocols. This approach ensures robustness in error correction and key extraction, despite the dynamic nature of the free-space channel. For altitudes ranging from 400 km (LEO) to 22,000 km (Medium Earth Orbit (MEO) / GEO), variations in slant range significantly influence the transmission coefficient [218]. Lower altitudes are prone to greater noise due to pronounced fluctuations in satellite distance. To mitigate this, a clustering-based approach groups observed transmission coefficients (T_k) into intervals based on expected transmittance, referred to as $PDTE(g)$. This strategy minimizes fading noise by associating quantum symbols with specific transmittance groups, facilitating more accurate and robust analysis. Each transmission group is independently analyzed to derive its secret key rate, $K_{fad}(PDTE(g))$, which is aggregated into a total key rate,

$$K_{agg} = \sum_g P(\tau_g \in PDTE(g)) K_{fad}(PDTE(g)), \quad (8.3)$$

where τ_g represents the estimated aggregated channel transmission efficiency. This method enhances channel transmittance estimation, particularly under fast-fading conditions, ensuring precise classification of transmission coefficients. The transmission values $T(\leq 1)$ are uniformly divided into intervals, ranging from single-group analysis to 100 equally spaced intervals, approaching the finite-regime limit. This refined approach highlights the critical role of T optimization in maximizing secure key rates and addressing practical challenges in satellite optical communication systems.

Transmission efficiency is further treated as a function of satellite altitude to simplify and evaluate convolutions, as detailed in [23]. For a transmitted signal $X_m \sim \mathcal{N}(x; \mu_{X_m}, \sigma_{X_m}^2)$, the scaled signal $\sqrt{\tau}X_m \sim \mathcal{N}(s; \sqrt{\tau}\mu_{X_m}, \tau\sigma_{X_m}^2)$. The p.d.f. of $\sqrt{\tau}X_m$ is expressed as,

$$f_{\sqrt{\tau}X_m}(s) = \frac{1}{\sqrt{\tau}\sigma_{X_m}\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{s - \sqrt{\tau}\mu_{X_m}}{\sqrt{\tau}\sigma_{X_m}}\right)^2}. \quad (8.4)$$

This formulation provides a robust framework for understanding and optimizing transmission dynamics in quantum satellite communication, ensuring precise modeling and enhanced system performance.

8.2.4 Calculation of the Received Signal Model for FSO Satellite Quantum Channel

The [p.d.f.](#) of the received signal Y_m is obtained from the convolution of [p.d.f.](#) of f_{X_m} and the hybrid quantum noise f_{N_m} . Mathematically,

$$f_{Y_m}(y) = \int_{-\infty}^{\infty} f_{\sqrt{\tau}X_m}(s) f_{N_m}(y-s) ds. \quad (8.5)$$

Substituting $f_{\sqrt{\tau}X_m}(s)$ and $f_{N_m}(y-s)$ into the convolution integral yields the [p.d.f.](#) of the received signal written as

$$\begin{aligned} f_{Y_m}(y) &= \int_{-\infty}^{\infty} \left(\frac{1}{\sqrt{\tau}\sigma_{X_m}\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{s-\sqrt{\tau}\mu_{X_m}}{\sqrt{\tau}\sigma_{X_m}}\right)^2} \right) \\ &\quad \left(\sum_{j=0}^{\infty} \frac{e^{-\lambda}\lambda^j}{j!} \frac{1}{\sigma_{N_m^{(2)}}\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{y-s-j-\mu_{N_m^{(2)}}}{\sigma_{N_m^{(2)}}}\right)^2} \right) ds \\ &= \int_{-\infty}^{\infty} \sum_{j=0}^{\infty} \frac{e^{-\lambda}\lambda^j}{j!} \left(\frac{1}{\sqrt{\tau}\sigma_{X_m}\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{s-\sqrt{\tau}\mu_{X_m}}{\sqrt{\tau}\sigma_{X_m}}\right)^2} \right) \left(\frac{1}{\sigma_{N_m^{(2)}}\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{y-s-j-\mu_{N_m^{(2)}}}{\sigma_{N_m^{(2)}}}\right)^2} \right) ds \\ &= \int_{-\infty}^{\infty} \sum_{j=0}^{\infty} \frac{e^{-\lambda}\lambda^j}{j!} \frac{1}{2\pi\sigma_p\sigma_q} e^{-\left[\frac{(s-\mu_p)^2}{2\sigma_p^2} + \frac{(s-\mu_q)^2}{2\sigma_q^2}\right]} ds, \quad (8.6) \end{aligned}$$

where $\mu_p := \sqrt{\tau}\mu_{X_m}$, $\sigma_p := \sqrt{\tau}\sigma_{X_m}$, $\mu_q := y - j - \mu_{N_m^{(2)}}$, and $\sigma_q := \sigma_{N_m^{(2)}}$. Let's examine the term in the exponent in (8.6), consider

$$\Delta := \frac{(s-\mu_p)^2}{2\sigma_p^2} + \frac{(s-\mu_q)^2}{2\sigma_q^2} = \frac{(s-\mu_{pq})^2}{2\sigma_{pq}^2} + \frac{(\mu_p-\mu_q)^2}{2(\sigma_p^2+\sigma_q^2)}, \quad (8.7)$$

where $\mu_{pq} = \frac{\mu_p\sigma_q^2+\mu_q\sigma_p^2}{\sigma_p^2+\sigma_q^2}$, $\sigma_{pq} = \sqrt{\frac{\sigma_p^2\sigma_q^2}{\sigma_p^2+\sigma_q^2}}$. Substituting (8.7) in (8.6) one get,

$$\begin{aligned} f_{Y_m}(y) &= \int_{-\infty}^{\infty} \sum_{j=0}^{\infty} \frac{e^{-\lambda}\lambda^j}{j!} \frac{1}{\sqrt{2\pi}\sigma_{pq}} e^{-\left[\frac{(s-\mu_{pq})^2}{2\sigma_{pq}^2}\right]} \frac{1}{\sqrt{2\pi(\sigma_p^2+\sigma_q^2)}} e^{-\left[\frac{(\mu_p-\mu_q)^2}{2(\sigma_p^2+\sigma_q^2)}\right]} ds \\ &= \int_{-\infty}^{\infty} \sum_{j=0}^{\infty} \frac{e^{-\lambda}\lambda^j}{j!} \frac{S_{pq}}{\sigma_{pq}\sqrt{2\pi}} e^{-\frac{(\mu_p-\mu_q)^2}{2\sigma_{pq}^2}} ds, \quad (8.8) \end{aligned}$$

where the scaling factor $S_{pq} = \frac{1}{\sqrt{2\pi(\sigma_p^2+\sigma_q^2)}} e^{-\frac{(\mu_p-\mu_q)^2}{2(\sigma_p^2+\sigma_q^2)}}$ is itself a Gaussian function on both μ_p and μ_q with Gaussian root mean square (RMS) width $\sqrt{(\sigma_p^2+\sigma_q^2)}$. Note that μ_p , σ_p and σ_q are free from y while only μ_q depends on y . In the integrand above, it is necessary to be careful that both S_{pq}

and μ_{pq} contain y and j . Our target is to interchange the summation and integration in (8.8), and for that, consider

$$\phi_j^m(s) := \frac{e^{-\lambda\lambda^j}}{j!} \frac{S_{pq}}{\sigma_{pq}\sqrt{2\pi}} e^{-\frac{(s-\mu_{pq})^2}{2\sigma_{pq}^2}}, \quad (8.9)$$

Hence express

$$f_{Y_m}(y) = \int_{-\infty}^{\infty} \sum_{j=0}^{\infty} \phi_j^m(s) ds. \quad (8.10)$$

This formulation represents a specific application of Fubini's and Tonelli's theorems, where the measures considered are a countable measure over the natural numbers $\mathbb{N}$ and the Lebesgue measure over the real numbers $\mathbb{R}$ (or the non-negative real numbers $[0, \infty)$). In particular, $\int_{-\infty}^{\infty} \sum_{j=0}^{\infty} \phi_j^m(s) ds$ is valid because the functions $\phi_j^m(s)$ are continuous for all $j \in \{0, 1, 2, \dots\}$. This continuity ensures the well-defined interchangeability of the integral and summation under the conditions of these theorems.

In deriving the expression for f_{Y_m} , it is advantageous to interchange the integral and the summation in this case. An important question to consider is whether any necessary and sufficient condition exists that allows for the interchange of the integral and summation in the above expression. According to Tonelli's theorem, if $\phi_j^m(s) \geq 0$ for all j and s , then $\int \sum_j \phi_j^m(s) ds = \sum_j \int \phi_j^m(s) ds$ without any additional conditions. This can be proven using the monotone convergence theorem. Fubini's theorem states that for a general function $g_j(\cdot)$, if $\int \sum |g_j(s)| < \infty$ or $\sum \int |g_j(s)| < \infty$ (and by Tonelli's theorem, these two conditions are equivalent), then $\int \sum_j \phi_j^m(s) = \sum_j \int \phi_j^m(s)$. This can be proven using the dominated convergence theorem. To use the conditions of Tonelli's theorem as stated above, it suffices to verify whether $\phi_j^m(s) \geq 0 \quad \forall j, s$.

In the specific case of (8.9), being the exponential function, the part $e^{-\frac{(s-\mu_{pq})^2}{2\sigma_{pq}^2}}$ is always non-negative for all s and j . The standard deviations σ_p and σ_q , defined as $\sigma_p = T\sigma_{X_m}$ and $\sigma_q = \sigma_{N_m^{(2)}}$, are non-negative, which implies $\sigma_{pq} \geq 0$. Similarly, for the expression $S_{pq} = \frac{1}{\sqrt{2\pi(\sigma_p^2 + \sigma_q^2)}} e^{-\frac{(\mu_p - \mu_q)^2}{2(\sigma_p^2 + \sigma_q^2)}}$, both $\frac{1}{\sqrt{2\pi(\sigma_p^2 + \sigma_q^2)}}$ and the exponential component are non-negative, which ensures that $S_{pq} \geq 0$. Note that, $\frac{e^{-\lambda\lambda^j}}{j!}$ and $\frac{S_{pq}}{\sqrt{2\pi}\sigma_{pq}}$ do not depend on s , while only $e^{-\frac{(\mu_p - \mu_q)^2}{2(\sigma_p^2 + \sigma_q^2)}}$ involves s . Given that $\lambda \geq 0$ and $j \in \{0, 1, 2, \dots\}$, one have $\frac{e^{-\lambda\lambda^j}}{j!} \geq 0 \quad \forall j$, $\frac{S_{pq}}{\sqrt{2\pi}\sigma_{pq}} \geq 0 \quad \forall j$, $e^{-\frac{(\mu_p - \mu_q)^2}{2(\sigma_p^2 + \sigma_q^2)}} \geq 0 \quad \forall s, j$. Therefore, $\phi_j^m(s) \geq 0$ for all s and j . Thus, by applying Tonelli's theorem, it can be concluded that the interchange of the summation and integration is justified, allowing us to express the desired result as follows

$$f_{Y_m}(y) = \sum_{j=0}^{\infty} \frac{e^{-\lambda\lambda^j}}{j!} \frac{S_{pq}}{\sigma_{pq}\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-\frac{(s-\mu_{pq})^2}{2\sigma_{pq}^2}} ds. \quad (8.11)$$

Note here, both S_{pq} and μ_{pq} contain y and j . Now, for the integration part

$$\begin{aligned} \int_{-\infty}^{\infty} e^{-\left(\frac{s-\mu_{pq}}{\sqrt{2}\sigma_{pq}}\right)^2} ds &= \int_{-\infty}^{\infty} e^{-r^2} \sqrt{2}\sigma_{pq} dr \\ &= \sqrt{2}\sigma_{pq} \int_{-\infty}^{\infty} e^{-r^2} dr = \sqrt{2}\sigma_{pq}\sqrt{\pi} = \sqrt{2\pi}\sigma_{pq} \end{aligned} \quad (8.12)$$

where $r = \frac{s-\mu_{pq}}{\sqrt{2}\sigma_{pq}}$, $\sqrt{2}\sigma_{pq}r + \mu_{pq} = s$, $\sqrt{2}\sigma_{pq}dr = ds$ and $\int_{-\infty}^{\infty} e^{-r^2} dr = \sqrt{\pi}$. Finally, putting expression (8.12) in (8.11) one get,

$$\begin{aligned} f_{Y_m}(y) &= \sum_{j=0}^{\infty} \frac{e^{-\lambda}\lambda^j}{j!} \frac{S_{pq}}{\sigma_{pq}\sqrt{2\pi}} \sqrt{2\pi}\sigma_{pq} \\ &= \sum_{i=0}^{\infty} \frac{e^{-\lambda}\lambda^i}{i!} S_{fg} = \sum_{i=0}^{\infty} \frac{e^{-\lambda}\lambda^i}{i!} \frac{1}{\sqrt{2\pi(\sigma_p^2 + \sigma_q^2)}} e^{-\frac{1}{2(\sigma_p^2 + \sigma_q^2)}(\mu_p - \mu_q)^2} \\ &= \sum_{i=0}^{\infty} \frac{e^{-\lambda}\lambda^i}{i!} \frac{1}{\sqrt{2\pi(\sigma_X^2 + \sigma_{N_i^{(2)}}^2)}} e^{-\frac{(\sqrt{\tau}\mu_X - y + i + \mu_{N_m^{(2)}})^2}{2(\tau\sigma_X^2 + \sigma_{N_i^{(2)}}^2)}} \\ &= \sum_{j=0}^{\infty} \frac{e^{-\lambda}\lambda^j}{j!} \frac{1}{\sqrt{2\pi(\tau\sigma_{X_m}^2 + \sigma_{N_m^{(2)}}^2)}} e^{\left[-\frac{(y - j - \sqrt{\tau}\mu_{X_m} - \mu_{N_m^{(2)}})^2}{2(\tau\sigma_{X_m}^2 + \sigma_{N_m^{(2)}}^2)}\right]} \\ &= \sum_{j=0}^{\infty} v_j^{(Y_m)} \mathcal{N}\left(y, \mu_j^{(Y_m)}, \sigma_j^{(Y_m)^2}\right), \end{aligned} \quad (8.13)$$

where $v_j^{(Y_m)} = \frac{e^{-\lambda}\lambda^j}{j!}$, $\sum_{j=0}^{\infty} v_j^{(Y_m)} = 1$, $v_j^{(Y_m)} \geq 0 \quad \forall j \in \{0, 1, 2, \dots\}$ and $\mathcal{N}(y; \mu_j^{(Y_m)}, \sigma_j^{(Y_m)^2})$ is Gaussian density in dummy variable y , mean $\mu_j^{(Y_m)} = \sqrt{\tau}\mu_{X_m} + \mu_{N_m^{(2)}} + j$, and s.d. $\sigma_j^{(Y_m)} = \sqrt{(\tau\sigma_{X_m}^2 + \sigma_{N_m^{(2)}}^2)}$ with variance $\sigma_j^{(Y_m)^2}$.

Consider the p.d.f. of the received signal Y_m given by in (8.13), the approximation of $f_{Y_m}(y)$ is taken as

$$f_{Y_m}(y) = \sum_{j=0}^R v_j^{(Y_m)} \mathcal{N}\left(y; \mu_j^{(Y_m)}, \sigma_j^{(Y_m)^2}\right), \quad (8.14)$$

where $v_j^{(Y_m)} = \frac{e^{-\lambda}\lambda^j}{j!}$, $\sum_{i=0}^R v_i^{(Y_m)} \approx 1$ for large R , $\mu_j^{(Y_m)} = \sqrt{\tau}\mu_{X_m} + \mu_{N_m^{(2)}} + j$, and $\sigma_j^{(Y_m)} = \sqrt{\tau\sigma_{X_m}^2 + \sigma_{N_m^{(2)}}^2}$.

Therefore, for a fixed Gaussian quantum channel, the quantum received signal can be calculated as the convolution product of the Gaussian distributed transmitted signal and the quantum noise signal. Considering the

hybrid quantum noise and the Gaussian transmitted signal model as discussed above, the capacity of the quantum channel can be expressed as follows [23],

$$\begin{aligned}
C_m &= \sum_{j=0}^R \frac{e^{-\lambda} \lambda^j}{j!} \left(-\log_2 \left(\frac{e^{-\lambda} \lambda^j}{j!} \right) + \frac{1}{2} \log_2 \left(2\pi e (\tau \sigma_{X_m}^2 + \sigma_{N_m^{(2)}}^2) \right) \right. \\
&\quad \left. + \log_2 \left(\sum_{l=0}^R \frac{e^{-\lambda} \lambda^l}{l!} \mathcal{N} \left(\mu_{N_m^{(2)}} + i; \mu_{N_m^{(2)}} + l, 2\sigma_{N_m^{(2)}}^2 \right) \right) \right) \\
&= \sum_{j=0}^R \frac{e^{-\lambda} \lambda^j}{j!} \left(-\log_2 \left(\frac{e^{-\lambda} \lambda^j}{j!} \right) + \frac{1}{2} \log_2 \left(2\pi e (\tau \sigma_{X_m}^2 + \sigma_{N_m^{(2)}}^2) \right) \right. \\
&\quad \left. + \log_2 \left(\sum_{l=0}^R \frac{e^{-\lambda} \lambda^l}{l!} \frac{1}{\sqrt{2}\sigma_{N_m^{(2)}}\sqrt{2\pi}} e^{-\frac{1}{2} \left[\frac{j-l}{\sqrt{2}\sigma_{N_m^{(2)}}} \right]^2} \right) \right). \tag{8.15}
\end{aligned}$$

8.2.5 Feasible Zones and Geometric Considerations for Finite Regime SKR in CV-QKD using Satellite Quantum Channels

This section addresses the complexities of CV-QKD over SKR in satellite-based quantum communication systems. The analysis considers the geometric and physical constraints of free-space atmospheric channels between terrestrial ground stations and orbiting satellites.

Orbital Sectors and Communication Phases between Satellite and GS :

Fig. 8.1 illustrates the operational zones of a satellite during quantum communication with a ground station. The diagram is divided into several key regions [219]: 1. Zenith: The point directly overhead the ground station, where the satellite is in its closest position for communication. This is the optimal point for quantum communication due to minimal atmospheric interference and the shortest slant range. 2. Quantum Communication Zone: The central green sector represents the effective zone where quantum communication takes place. This area ensures the transmission of quantum states with sufficient efficiency and low noise levels. 3. Data Processing Zones: The orange sectors adjacent to the quantum communication zone indicate areas where data processing occurs. These zones represent transition regions where the satellite begins to move away from or approach the quantum communication zone. Atmospheric effects and longer slant ranges may reduce efficiency in this scenario. 4. No Tracing Zones: The red sectors near the horizon indicate zones where communication is not feasible due to significant atmospheric interference, beam divergence, and low SNR. These zones are outside the satellite's effective line-of-sight communication range. 5. Slant Angle (θ): The angle between the ground station's zenith and the

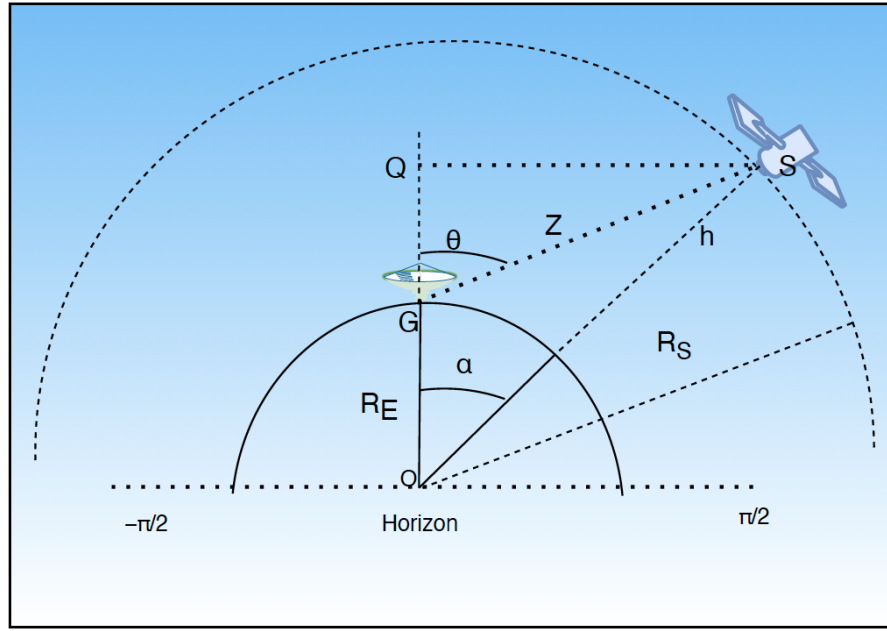


Figure 8.2: Geometric configuration of satellite-to-ground communication. S represents the satellite, G the ground station, and O the Earth's center. The satellite altitude is denoted by h , the Earth's radius by R_E , and the slant range by R_S . The zenith angle θ and the elevation angle α are measured relative to the ground station. The parameter Z represents the satellite's position projected relative to the zenith. This diagram illustrates the key parameters affecting satellite communication geometry.

satellite's position in the sky. This angle is a critical factor influencing the communication quality, with smaller angles (near the zenith) offering better transmission conditions. 6. Horizon: The boundary line where the satellite moves beyond the ground station's visible range, marking the limits of effective communication.

Depending on the effective quantum communication and quantum key exchange, the orbital trajectory is divided into three primary sectors based on zenith angles shown in Fig. 8.2: (I) Good Sector ($-1 \leq \theta \leq 1$): This region provides optimal transmissivity due to reduced atmospheric effects, making it ideal for active CV-QKD with high finite-size SKR. (II) Data Processing Sector ($1 < \theta < \pi/2$): This region facilitates post-processing tasks, such as reconciliation and error correction, essential for finite-size SKR optimization. (III) Encrypted Communication Sector ($-\pi/2 < \theta < -1$): This sector is reserved for encrypted key-based communications, relying on previously established quantum keys.

Geometric Architecture of Satellite-Ground Links :

In CV-QKD systems, finite-size effects play a crucial role in determining the achievable SKR due to limitations in quantum signal processing and transmission. Figure 8.2 illustrates the fundamental geometry, where the

ground station is near sea level ($h_0 \approx 0$) and the satellite orbits at an altitude $h > 100$ km. The zenith angle θ ranges from 0 (directly overhead) to $\pi/2$ (horizon). This geometric configuration introduces key challenges, including atmospheric losses and optical misalignment, both of which significantly impact the SKR. The orbital geometry determines the slant distance Z between the satellite and the ground station, which depends on the satellite's altitude h , zenith angle θ , satellite radius R_S , and Earth's radius R_E . The slant distance directly affects the quantum channel's transmissivity, a critical parameter in evaluating finite-size SKR. The essential geometric equations include the slant distance as a function of satellite altitude h and zenith angle θ ,

$$Z(h, \theta) = \sqrt{R_S^2 + R_G^2(\cos^2 \theta - 1) - R_G \cos \theta}, \quad (8.16)$$

where R_G denotes the distance of the ground station from the Earth's center, $R_G = R_E + h_0$ and $R_S = R_E + h$.

In this study, the ground station is considered to be at sea level ($h_0 = 0$), and the Earth's radius is approximated as $R_E = 6371$ km, reflecting its global average value for a spherical model. For satellite-to-ground communication, critical parameters such as slant distance, orbital characteristics, and temporal variations play a vital role in the analysis. The satellite altitude is determined as a function of the slant distance and zenith angle, expressed as follows, $h(Z, \theta)$, which measures the distance between the satellite and a ground station, is given by

$$h(Z, \theta) = \sqrt{R_G^2 + Z^2 + 2ZR_G \cos \theta} - R_E. \quad (8.17)$$

For satellites in circular orbits with a constant orbital radius R_S , specifically during zenith-crossing, the slant distance can be simplified and redefined as,

$$Z(R_S, \alpha) = \sqrt{R_G^2 + R_S^2 - 2R_GR_S \cos \alpha}, \quad (8.18)$$

with α representing the satellite's orbital angle.

The orbital period, T_S , which represents the time a satellite takes to complete one full orbit around Earth, is defined as, $T_S = 2\pi\sqrt{\frac{R_S^3}{GM_E}}$, where G is the gravitational constant and M_E is the Earth's mass. This formulation enables the orbital angle, α , to be expressed as, $\alpha = \frac{2\pi t}{T_S}$, where t denotes the elapsed time. Additionally, the orbital time, $t(\theta, h)$, specifies the time required for the satellite to reach a given zenith angle θ at a specific altitude h , and is given by

$$t(\theta, h) = \sqrt{\frac{(R_E + h)^3}{GM_E}} \arccos \left[\frac{R_G + z(h, \theta) \cos \theta}{R_E + h} \right]. \quad (8.19)$$

From (8.19), the equation for the total communication time given the satellite is expressed as,

$$t_{total} \approx 2 \frac{(R_E + h)^{3/2}}{\sqrt{GM_E}} \left(\theta_{\max} - \arcsin \left[\frac{R_E}{R_E + h} \sin \theta_{\max} \right] \right). \quad (8.20)$$

The total communication window t_{total} is determined by the satellite's orbital velocity and geometric constraints, with θ_{max} defining the maximum zenith angle. While suited for circular orbits, these calculations can adapt to arbitrary trajectories. This precision is vital for applications like quantum key distribution, satellite tracking, and ground station synchronization.

Optical Link Efficiency and Finite Size Effects:

Free-space CV-QKD operates using Gaussian optical modes, where beam divergence plays a critical role in determining transmission efficiency (η_g). The beam's spot size during propagation expands according to,

$$w_g(Z) = w_0 \sqrt{1 + \left(\frac{Z}{N_R} \right)^2}, \quad (8.21)$$

where $N_R = \pi w_0^2 / \lambda$ is the Rayleigh range, w_0 is the beam waist, and λ is the wavelength. The aperture efficiency η_g , which quantifies the fraction of the beam captured by the receiver, is expressed as,

$$\eta_g(Z) = 1 - e^{-\frac{2a_r^2}{w_g^2}}, \quad (8.22)$$

where a_r is the receiver aperture radius. The overall efficiency of the free-space channel is affected by atmospheric extinction, diffraction losses, and internal system losses. These factors, combined with the detector's non-unit quantum efficiency and optical imperfections, define the detector efficiency (η_{det}). For this setup, the fixed detector efficiency is assumed to be $\eta_{det} = 0.606$, accounting for losses from the generation of the Gaussian beam to its final detection at the receiver.

For free-space communication at a fixed altitude h , the attenuation of the signal can be effectively modeled using the Beer-Lambert equation, which is given by

$$\eta_{atm}(h) = e^{-\beta(h)Z}, \quad (8.23)$$

where $\beta(h)$ is the extinction factor. This is given by

$$\beta(h) = \beta_0 e^{-h/\tilde{h}}, \quad (8.24)$$

Here, h represents the altitude in meters, with $\tilde{h} = 6600$ m and the sea-level value of β_0 given as $5 \times 10^{-6} \text{ m}^{-1}$ for a wavelength of $\lambda = 800$ nm. To account for free-space optical communication at varying altitudes h , the given equation must be appropriately modified. Assuming the satellite is positioned directly at the zenith, its slant range Z is equal to its altitude h . Therefore, for satellites in this zenith position, one can approximate the transmittance with $\eta_{zen} = 0.94$.

For elevation angles within the good sector range ($-\pi/2$ to $\pi/2$), the atmospheric transmission efficiency, η_{atm} , is scaled as [23, 220, 221]

$$\eta_{atm} = \eta_{zen}^{sec(\theta)}, \quad (8.25)$$

The transmission efficiency at the zenith, denoted as η_{zen} , remains constant and is unaffected by differences between rural and urban aerosol models.

In satellite-to-ground communication systems, the satellite continuously tracks the ground station during its orbital pass by aligning its telescope with the station's position. This alignment is guided by a beacon laser emitted from the ground station. However, the finite speed of light introduces a delay that requires compensation through a point-ahead angle. This angle accounts for the time it takes for the light to travel, ensuring the beacon beam aligns correctly with the satellite's motion. The point-ahead angle is calculated using the satellite's orbital parameters and is applied as an offset to the beacon's angle of incidence. For example, a satellite orbiting at an altitude of 500 km may require a point-ahead angle of up to $53\mu\text{rad}$. Both the detection of the beacon and the application of the point-ahead mechanism are prone to errors. An accurate modeling and mitigation of system errors ensures precise tracking and reliable satellite-ground communication.

The link efficiency due to pointing and tracking errors, denoted as η_{pt} , is expressed as

$$\eta_{pt} = \exp(-G_{tx}\theta_{pt}^2), \quad (8.26)$$

where G_{tx} represents the transmit antenna gain, and θ_{pt} is the angle accounting for the combined pointing and tracking errors of the satellite. The transmit antenna gain is defined by,

$$G_{tx} = \left(\frac{2\pi a_S}{w}\right)^2, \quad (8.27)$$

with a_S the clear transmitter aperture radius.

Pointing and tracking errors (θ_{pt}) play a crucial role in determining the efficiency of high-precision satellite communication systems. These errors directly affect the transmit antenna gain, which is also influenced by atmospheric beam spreading caused by turbulence. In a downlink scenario, the beam spread typically remains in the sub-microradian range, minimizing its impact on link efficiency. This allows calculations of pointing and tracking efficiency to focus primarily on the transmit antenna gain and the precision of the pointing and tracking mechanisms.

Temporal filtering further enhances efficiency by reducing dark counts, achieved by gating the detector within a defined time window (Δt), which is given by,

$$\eta_{\text{temporal}} = 1 - e^{-\frac{\Delta t}{t}}, \quad (8.28)$$

where, t represents the temporal width of the photon, and temporal filtering enhances spatial filtering by mitigating misalignment errors, thereby ensuring precise [SKR](#) calculations.

The total transmission efficiency, τ , incorporates multiple factors, including atmospheric transmissivity (η_{atm}) and pointing errors (η_{pt}). It is expressed as:

$$\tau = \eta_{\text{det}}\eta_g\eta_{\text{atm}}\eta_{pt}\eta_{\text{temporal}}, \quad (8.29)$$

where η_{det} is the detection efficiency, η_g accounts for geometric losses, and η_{temporal} reflects temporal filtering efficiency. Together, these factors significantly influence the finite-size [SKR](#).

8.2.6 The security analysis of collective attacks in the finite-key setting in Satellite-Based [CV-QKD](#)

In satellite-based [CV-QKD](#), [RR](#) is typically favoured over direct reconciliation because it is more robust against high levels of channel loss and noise. In [RR](#), the trusted receiver, usually positioned at the ground station, controls the key generation process. This approach offers greater resilience to the challenges of satellite-to-ground quantum communication, enabling a significantly improved asymptotic [SKR](#) [23].

In general, [CV-QKD](#) offers distinct advantages over [DV-QKD](#) for satellite communication. It is robust in high-loss environments, utilises coherent states with homodyne or heterodyne detection (eliminating the need for complex single-photon detectors), and integrates seamlessly with classical optical infrastructure. These features, combined with its tolerance to imperfections, make [CV-QKD](#) practical for large-scale satellite quantum communication networks [23, 51]. Finite-size [SKR](#) calculations must account for key factors, including beam wandering, turbulence, and transmission efficiency. Uplink transmissions face more turbulence-induced beam spreading, whereas downlink transmissions are influenced by thermal noise and atmospheric extinction. Effective [SKR](#) estimation incorporates transmission coefficients, detection efficiency, receiver aperture size, reconciliation efficiency, and hybrid noise effects, ensuring accurate protocol optimization under real-world conditions.

In practical implementations, finite-size effects impose limitations on the [SKR](#) due to statistical uncertainties in estimating channel parameters. For a block of M pulses, $M - k$ pulses are allocated for channel parameter estimation, while the remaining k pulses are utilized for key generation. Finite-size analysis for [CV-QKD](#) under collective attacks refines the [SKR](#) expression to account for these effects. The finite-key [SKR](#), denoted as K_{fin} , in the [RR](#) framework is expressed as,

$$\begin{aligned}
K_{fin} &= \frac{k}{M} (\beta I_{AB} - \chi_{BE} - \Delta(k)) \\
&= \frac{k}{M} [\beta I(a : b) - S_{\text{cPE}}(b : E) - \Delta(k)] \\
&= \frac{k}{M} \left[\beta \frac{1}{M} \sum_{m=1}^M \left[\sum_{j=0}^R \frac{e^{-\lambda} \lambda^j}{j!} \left(-\log_2 \left(\frac{e^{-\lambda} \lambda^j}{j!} \right) \right. \right. \right. \\
&\quad \left. \left. \left. + \frac{1}{2} \log_2 \left(2\pi e (\tau \sigma_{X_m}^2 + \sigma_{N_m^{(2)}}^2) \right) + \log_2 \left(\sum_{l=0}^R \frac{e^{-\lambda} \lambda^l}{l!} \frac{1}{2\sigma_{N_m^{(2)}} \sqrt{\pi}} e^{-\frac{1}{2} \left[\frac{j-l}{\sqrt{2}\sigma_{N_m^{(2)}}} \right]^2} \right) \right) \right] \right]
\end{aligned}$$

$$- \left[G\left(\frac{\lambda_1 - 1}{2}\right) + G\left(\frac{\lambda_2 - 1}{2}\right) - G\left(\frac{\lambda_3 - 1}{2}\right) - G\left(\frac{\lambda_4 - 1}{2}\right) \right] - \left[7 \cdot \sqrt{\log_2 \left(\frac{2/\bar{\epsilon}}{k} \right)} \right], \quad (8.30)$$

where

$$\beta I_{AB} = \beta \frac{1}{M} \sum_{m=1}^M C_m, \quad (8.31)$$

and C_m , defined by (8.15), applies for all $m = 1, 2, \dots, M$. Eve's accessible information is represented by χ_{BE} , while $\Delta(k)$ serves as a correction term that accounts for finite-size effects. Additionally, $S_{\epsilon_{\text{PE}}}(b : E)$ denotes Eve's conditional entropy regarding Bob's key, adjusted to incorporate parameter estimation inaccuracies, with a failure probability ϵ_{PE} , given by $S_{\epsilon_{\text{PE}}}(b : E) = \chi_{BE} = G\left(\frac{\lambda_1 - 1}{2}\right) + G\left(\frac{\lambda_2 - 1}{2}\right) - G\left(\frac{\lambda_3 - 1}{2}\right) - G\left(\frac{\lambda_4 - 1}{2}\right)$, where the symplectic eigenvalues $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ of the covariance matrix of Eve's system conditional on Bob's measurement outcome Y_B [23, 222]. The correction term $\Delta(k)$, which encapsulates finite-size effects, decreases as k increases, can be expressed as [23, 26, 222],

$$\Delta(k) = (2 \dim \mathcal{H}_X + 3) \sqrt{\frac{\log_2(2/\bar{\epsilon})}{n}} + \frac{2}{n} \log_2 \left(\frac{1}{\epsilon_{\text{PA}}} \right), \quad (8.32)$$

where $\dim \mathcal{H}_X = 2$ represents the dimensionality of the Hilbert space for the raw key variable X , while $\bar{\epsilon}$ and ϵ_{PA} are set to 10^{-10} to balance security with practical feasibility. The first term dictates the convergence speed of the smooth minimum entropy, while the second term accounts for the failure probability in private key amplification. These components underscore the significant impact of finite-size effects on the secret key rate, highlighting the need to optimize parameters such as k and M to achieve both security and efficiency.

The correction parameter $\Delta(k)$ is approximated as [23, 222],

$$\Delta(k) \approx 7 \cdot \sqrt{\log_2 \left(\frac{2}{\bar{\epsilon} \cdot k} \right)}, \quad (8.33)$$

where the smoothing parameter $\bar{\epsilon}$ is fixed at 10^{-10} . This adjustment incorporates finite-size effects, bridging the gap between theoretical models and practical implementations. The analysis reveals the trade-offs between security and performance, ensuring the framework's applicability to satellite-based CV-QKD systems. These considerations are crucial in addressing practical constraints, such as orbital mechanics, power limitations, and narrow data transfer windows, thereby making the results more relevant to real-world quantum communication scenarios.

For all bipartite quantum states ρ_{AB} with covariance matrix γ_{AB} , it has been proven that the secret key rate $K(\rho_{AB})$ satisfies the inequality $K(\rho_{AB}) \geq K(\rho_{G_{AB}})$. This establishes $K(\rho_{G_{AB}})$ as a lower bound on the secret key rate for any protocol, including non-Gaussian ones, under collective attacks (even non-Gaussian attacks). The key condition for this result

is that Alice and Bob compute the bound using the second-order moments of the quadratures. In the Gaussian CV setting, Eve's optimal attack is Gaussian, ensuring the bound is tight, such that $K(\rho_{AB}) = K(\rho_{G_{AB}})$.

The overall secure key rate K is expressed as a weighted sum of the key rates from individual segments [23, 220, 221],

$$K = \sum_i \max \left(0, \frac{k_i}{M} [\beta I_{AB} - \chi_{B_E} - \Delta(k_i)] \right), \quad (8.34)$$

where k_i is the number of raw key events in segment i , and M is the total number of segments. The term βI_{AB} represents the mutual information between Alice and Bob, χ_{B_E} denotes Eve's Holevo bound, and $\Delta(k_i)$ accounts for finite-size corrections. Only positive contributions to the key rate are included, ensuring that segments with insufficient key generation do not negatively impact the total rate.

For each segment, k_i corresponds to the raw key length, while the remaining $K_i - k_i$ data points are used for channel parameter estimation. The total number of data points across all segments satisfies $\sum_i K_i = M$. The relative weight of each segment, determined by k_i/M , reflects its contribution to the total secure key rate. More significant segments containing more data points have a proportionally greater influence on the overall key rate. This approach ensures an efficient and accurate calculation of the secure key rate, accommodating the finite-size effects and data segmentation during a satellite pass.

As discussed earlier, the finite-size secret key rate (K_{fin}) is influenced by key factors such as the transmissivity (τ), receiver telescope aperture (a_r), reconciliation efficiency (β), and the total number of signal samples (M). In Gaussian-modulated CV-QKD protocols, K_{fin} is calculated using the expression,

$$K_{fin} = \beta I(A : B) - \chi(B : E) - \Delta(M), \quad (8.35)$$

where $I(A : B)$ represents the mutual information shared between Alice (sender) and Bob (receiver), $\chi(B : E)$ denotes Eve's Holevo bound, and $\Delta(M)$ is a finite-size correction term that is inversely proportional to the block size M , with $M = 10^8$ in typical setups. The finite-size key rate achieves its maximum in the Good Sector, a region where atmospheric and optical losses are minimized, enabling optimal quantum communication performance.

8.3 Results and Numerical Analysis

This section presents an in-depth analysis of the finite-size SKR in free-space atmospheric satellite channels, emphasizing its dependence on the SNR. This chapter systematically investigates how key channel parameters—including reconciliation efficiency, receiver telescope aperture, transmission coefficient, beam waist, effective communication time, zenith angle,

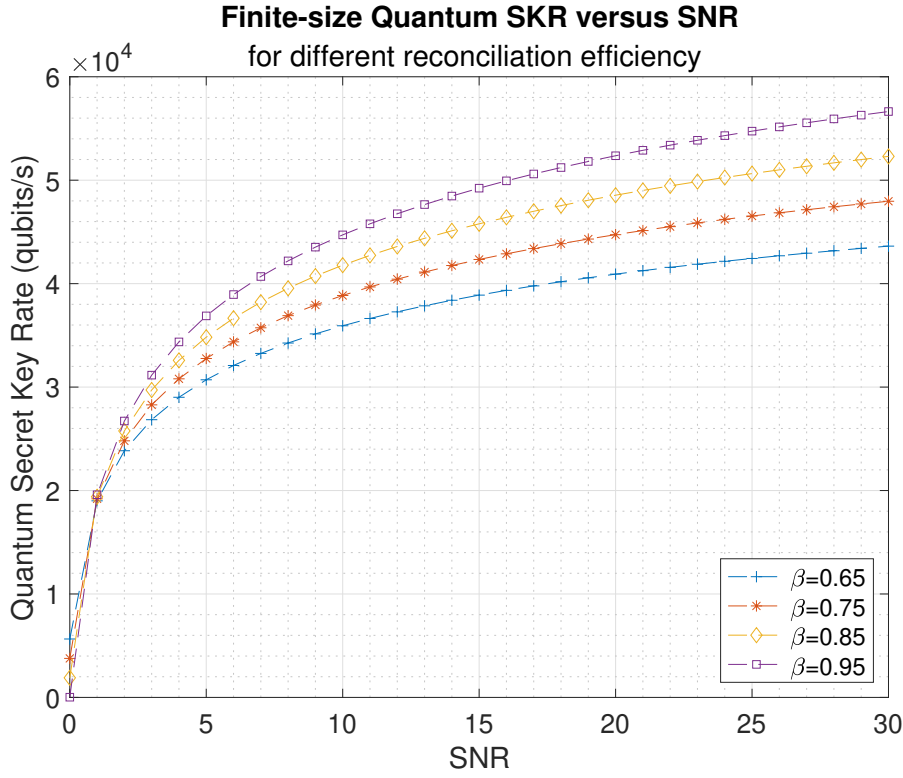


Figure 8.3: The relationship between the finite-size SKR and SNR for different values of reconciliation efficiency (β). The analysis explores how β influences the SKR in satellite quantum communication under varying SNR conditions.

and detection efficiency—affect the SKR in these quantum communication systems. These insights provide a comprehensive understanding of the intricate factors influencing the performance of QKD in satellite-based networks, shedding light on the challenges and opportunities in optimizing these cutting-edge technologies. For the finite-size regime, the block size M has been considered as 10^8 . Comparison with asymptotic size SKR can be available in [23]

Figure 8.3 illustrates the dependency of finite-size SKR on SNR and reconciliation efficiency (β). The results highlight the critical role of β in determining the fraction of mutual information between Alice and Bob that is securely retained after error correction. Higher β values enhance reconciliation efficiency, significantly improving SKR by minimizing information loss, even in low-SNR conditions. In contrast, lower β values lead to substantial information loss, limiting SKR regardless of channel quality. The analysis underscores the importance of optimizing β to ensure robust key generation in satellite-based quantum communication systems, especially in resource-constrained and dynamic environments. Advanced error correction protocols with high reconciliation efficiency are crucial for overcoming challenges such as finite block lengths and channel imperfections. As β approaches its maximum, the SKR remains resilient, demonstrating the value of efficient reconciliation strategies for maximizing secure key generation in

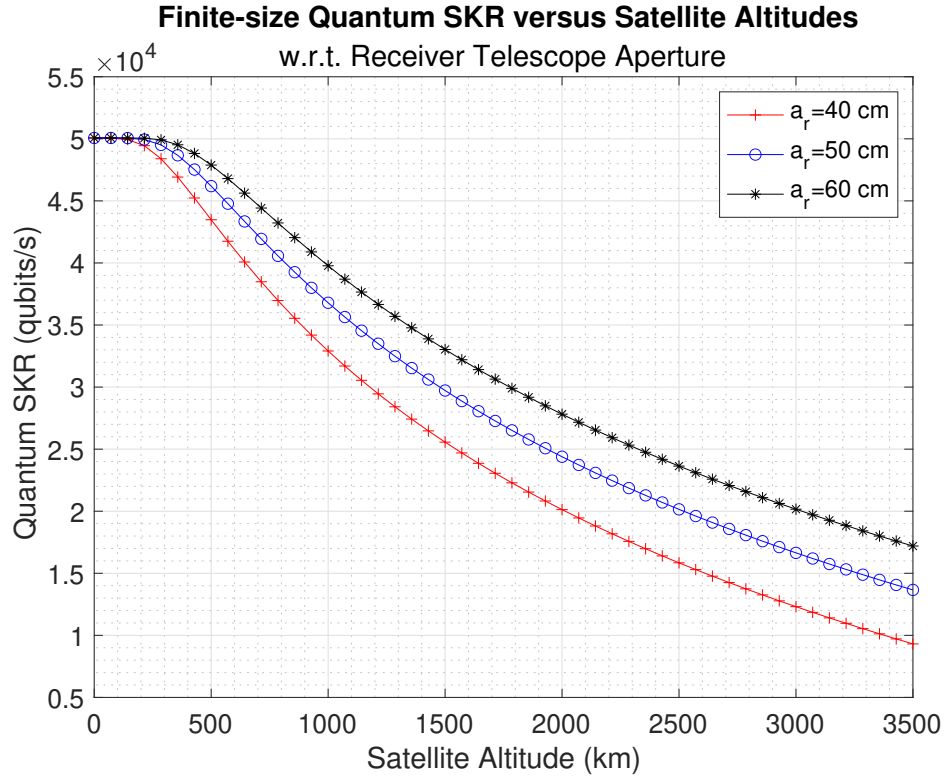


Figure 8.4: The relationship between the finite-size SKR and satellite altitude for varying receiver telescope apertures a_r . The analysis demonstrates the impact of aperture size on the SKR performance in satellite-based quantum communication systems.

practical satellite-based continuous-variable QKD systems.

Fig. 8.4 highlights the relationship between finite-size SKR and satellite altitude, with varying receiver telescope aperture (a_r) values while keeping other parameters constant. The receiver telescope aperture (a_r) is a crucial factor in shaping the quantum channel's performance, as larger apertures enhance photon collection efficiency and reduce channel losses, particularly at higher altitudes where slant ranges are longer. The analysis demonstrates that increasing a_r significantly improves the SKR, underscoring the sensitivity of QKD protocols to variations in aperture size. Larger apertures mitigate the effects of atmospheric turbulence and beam divergence, ensuring reliable photon detection and robust quantum communication. Conversely, smaller apertures limit photon collection, leading to reduced SKR and increased noise susceptibility. These findings emphasize the need to optimize receiver telescope aperture size for consistent and efficient system performance. Systems must account for potential constraints, such as physical limitations and atmospheric conditions, that may affect aperture optimization. By carefully designing receiver configurations to maximize a_r , satellite-based QKD systems can achieve higher SKR and maintain resilience across varying operational conditions and altitudes. This chapter demonstrates the critical role of a_r in ensuring the robustness and scalabil-

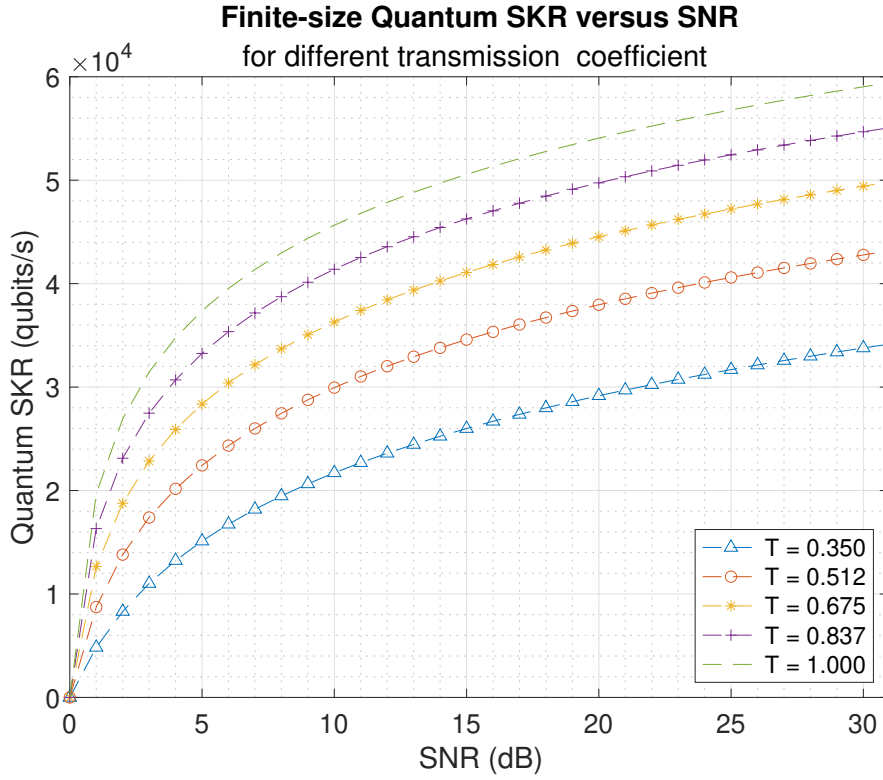


Figure 8.5: Variation of finite-size SKR with SNR for different transmission coefficients (T).

ity of quantum communication networks, highlighting its impact on secure key generation in practical free-space QKD implementations.

Fig. 8.5 illustrates the relationship between finite-size SKR and SNR for varying transmission coefficients (T), with all other parameters fixed. The transmission coefficient (T) is crucial in determining the performance of finite-regime quantum SKR, as it reflects the fraction of quantum states successfully transmitted through the channel. Higher T values directly enhance SKR by reducing losses and improving detection efficiency. The analysis highlights the sensitivity of SKR to T , which is influenced by factors such as atmospheric turbulence, weather conditions, and transmission distance in satellite-based QKD systems. Optimizing T is critical for robust SKR, particularly under finite-size constraints. Advanced techniques such as adaptive optics, optimized satellite trajectories, and enhanced error correction can mitigate channel losses and maximize T . The results emphasize the importance of maintaining high SNR and improving T to ensure reliable and high-performance quantum communication, even in dynamic environments.

Fig. 8.6 illustrates the variation of the finite-size quantum SKR as a function of satellite altitude for different beam waist values (w_0) measured in centimetres, while other parameters remain constant (Table 8.1). The beam waist, representing the optical beam's width at the receiver aperture, is a key factor influencing the efficiency of the communication chan-

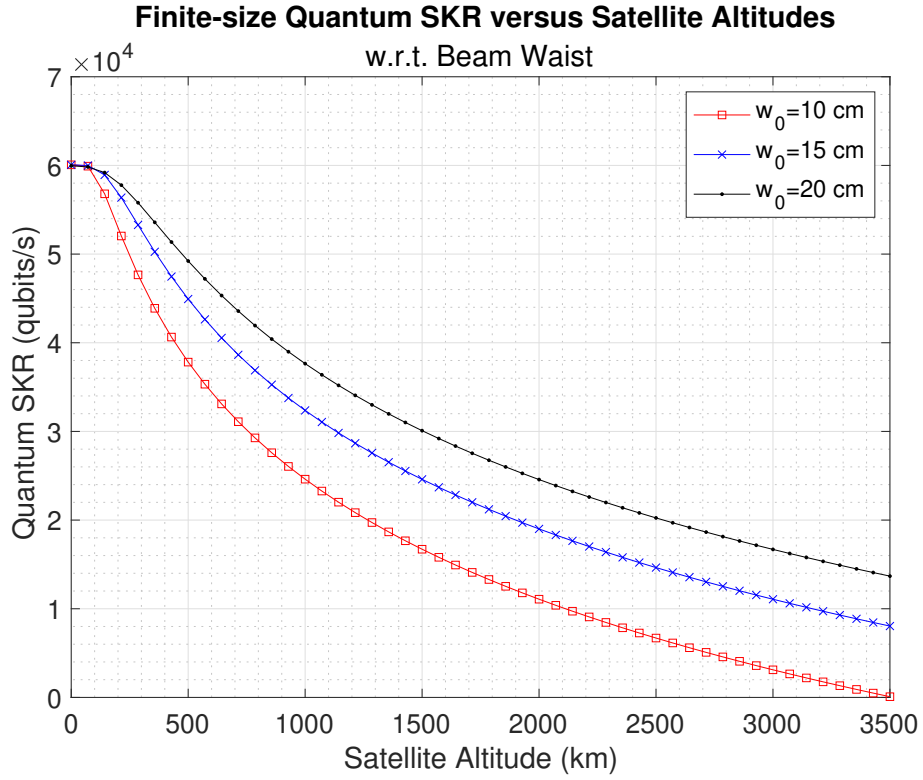


Figure 8.6: Variation of finite-size SKR with satellite altitude for different beam waist (w_0) values.

nel. The analysis reveals that changes in the beam waist have a significant impact on the SKR, underscoring its role as a critical design parameter for satellite-based quantum communication systems. As satellite altitude increases, the SKR decreases due to greater signal attenuation and losses over longer transmission distances. Larger beam waists (w_0) mitigate these losses by enhancing photon collection efficiency at the receiver, leading to improved SKR performance. However, excessively large beam waists may introduce optical aberrations or alignment challenges, necessitating careful optimization to balance signal collection and system stability. Conversely, narrower beam waists are more prone to diffraction losses, particularly at higher altitudes, further emphasizing the need for an optimal beam waist configuration. This analysis underscores the importance of beam waist optimization in maintaining robust and efficient performance in free-space optical quantum channels. The findings highlight that while the system is designed to handle typical beam waist levels encountered in atmospheric conditions, achieving optimal performance requires careful consideration of beam waist variations to effectively address altitude-induced losses.

Figure 8.7 explores the relationship between the finite-regime SKR and the adequate communication time, with the wavelength of the light source as a key variable. The adequate communication time is influenced by the zenith angle and satellite altitude, with a duration that is shorter than the satellite's total transit time. This limited window is crucial for secure quan-

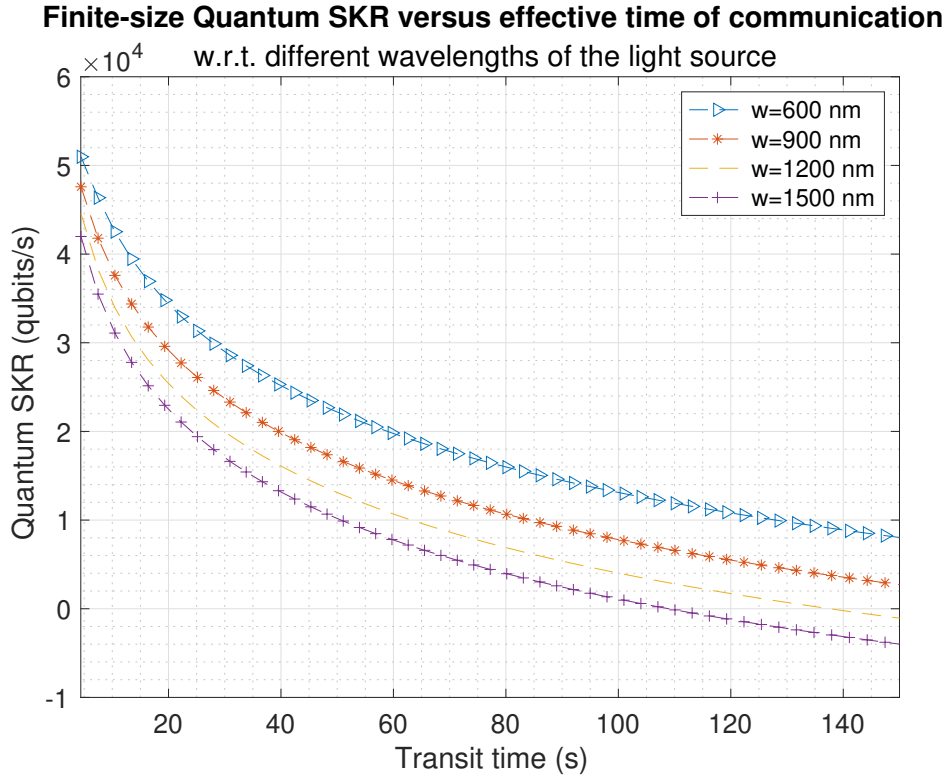


Figure 8.7: Dependence of finite-size SKR on effective communication time for different light source wavelengths.

tum communication. Wavelength significantly affects SKR due to the intrinsic quantum noise associated with photon emission. Longer wavelengths increase noise photons, reducing the SNR and compromising the fidelity of quantum states, which leads to lower SKR. Conversely, shorter wavelengths reduce noise, thereby enhancing SNR and improving SKR. However, shorter wavelengths face higher atmospheric attenuation, which necessitates careful design considerations. Adequate communication time also directly impacts SKR. Longer communication durations enable more data exchange, thereby improving parameter estimation and key generation. However, atmospheric conditions and environmental factors may limit this time, especially for shorter wavelengths. The findings emphasise the trade-off between minimizing noise and ensuring robust signal transmission through atmospheric channels. By optimizing the wavelength and effective communication time, it is possible to maximize SKR and enhance the reliability of satellite-based quantum communication systems. This analysis provides critical insights into balancing these factors to achieve efficient and secure quantum key distribution in free-space communication networks.

Figure 8.8 depicts the variation of finite-regime SKR as a function of the zenith angle, considering different SNR levels while keeping other parameters constant. The analysis focuses on the good sector (-1 rad to 1 rad), where SKR is most effective. The SKR peaks near the zenith, where the satellite's slant range is shortest, minimizing atmospheric attenuation

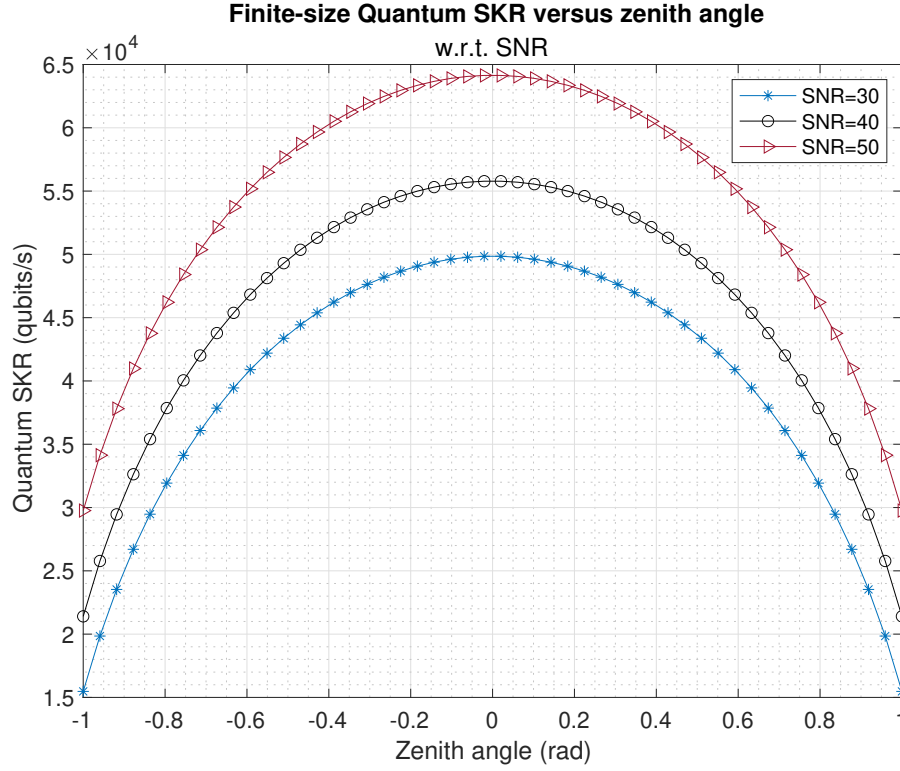


Figure 8.8: Variation of finite-regime SKR with respect to the zenith angle for different SNR values.

and enhancing signal quality. As the zenith angle increases toward the horizon, SKR decreases due to longer slant ranges, increased diffraction, scattering, and absorption. These effects are most pronounced at the horizon, where the satellite's elevation angle is minimal, and line-of-sight constraints are critical. Higher SNR values significantly improve SKR across the zenith angle range, demonstrating the importance of optimizing SNR for robust communication. This chapter highlights the need for adaptive strategies, such as enhanced error correction and optimized receiver configurations, to sustain communication near the horizon, where SKR is most vulnerable. This analysis emphasizes refining communication protocols to address atmospheric interference and geometric constraints, ensuring consistent and efficient quantum key distribution in satellite-based systems. Tailoring strategies for varying zenith angles is essential for maximizing the performance and reliability of quantum communication networks.

Fig. 8.9 illustrates the finite-regime quantum SKR as a function of detection efficiency (η_{det}) across varying satellite altitudes, with other parameters held constant (Table 8.1). Detection efficiency is shown to critically influence the SKR, as it determines the proportion of incoming quantum states successfully detected. The results demonstrate that high η_{det} ensures robust SKR performance, while significant reductions in η_{det} lead to diminished detection rates and lower SKR. Satellite altitude is highlighted as another key factor affecting communication parameters such as zenith angle, effec-

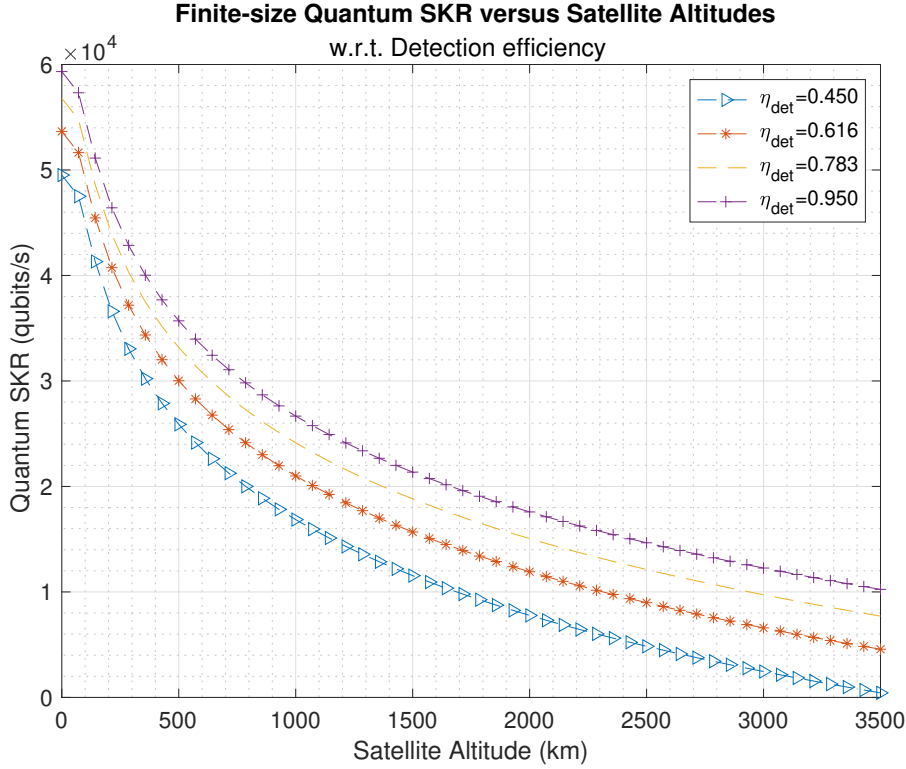


Figure 8.9: Impact of detection efficiency η_{det} on finite-regime SKR at different satellite altitudes.

tive communication time, and transit time. The analysis underscores the interdependence of detection efficiency, altitude, and geometric factors in shaping SKR, emphasizing the need for optimization. By comparing SKR across permissible altitudes, this chapter identifies reconciliation efficiency (β), transmission coefficient (T), and detection efficiency (η_{det}) as critical parameters for achieving reliable satellite-based quantum communication. These findings provide a foundation for designing efficient systems capable of secure and scalable quantum information transmission over global distances.

8.4 Conclusion

This chapter has successfully introduced a comprehensive framework for analyzing finite-regime QKD in satellite-based quantum communication, focusing on a hybrid quantum channel model that captures the fading characteristics of free-space links and satellite orbital dynamics. Central to this research is the exploration of finite key size effects, a critical factor in practical implementations where limited data samples influence parameter estimation and security. This chapter bridges theoretical advancements with practical system requirements by addressing these effects alongside composable security under collective attacks, enabling secure communication over

long distances. Essential parameters such as reconciliation efficiency, transmission coefficient, detection efficiency, receiver telescope aperture, beam waist, and adequate communication time are systematically analyzed, revealing their pivotal role in shaping the SKR and ensuring system robustness. The findings highlight trade-offs, such as balancing longer communication windows with increased noise at higher altitudes, emphasizing the importance of finite key size analysis in operational scenarios that diverge from idealized, asymptotic assumptions. This chapter also introduced a hybrid noise framework that integrates quantum Poissonian noise and classical AWGN, providing a realistic evaluation of free-space quantum channels. This approach addresses atmospheric turbulence, signal attenuation, and background noise, offering actionable strategies to mitigate their impact on SKR. This research underscores the superiority of satellite-based quantum communication over traditional networks by demonstrating the feasibility of finite-regime QKD in uplink and downlink configurations. Emphasising finite key size effects and key parameter optimization sets the stage for scalable, reliable, and secure global quantum communication networks, bringing it closer to realizing a secure quantum internet.

Chapter 9

Conclusion

QIP fundamentally relies on the capacity and reliability of quantum channels to enable secure and efficient communication, cryptography, and computation. This work presents a novel HQN model that integrates quantum Poisson noise with classical AWGN, providing a refined framework for estimating quantum channel capacity. By characterizing this hybrid noise using GMM, the study advances statistical modeling techniques to better represent practical quantum communication channels. A key insight from this research is that entropy-based mutual information analysis reveals that Gaussian input distributions achieve the highest capacity-to-signal-to-noise ratio compared to non-Gaussian inputs, reaffirming the centrality of Gaussian signaling in optimizing quantum communication.

A significant contribution of this research is the development of a comprehensive mathematical framework for modeling HQN. By analyzing the p.d.f. of hybrid noise, this study demonstrates that a finite number of mixture components can accurately approximate the noise distribution, a crucial result for practical quantum channel analysis. Furthermore, the research establishes a vital link between the Poisson noise parameter and the number of mixture components in the hybrid noise model, offering new insights into optimizing quantum channels for enhanced performance and resilience against noise.

This research also makes a significant contribution to entropy-based quantum information analysis by establishing a rigorous framework for quantifying hybrid quantum noise using various entropy measures. The study enhances our understanding of quantum channel capacity by deriving entropy-based expressions for mutual information. It provides deeper insights into entropy-driven noise effects in quantum communication networks. The study successfully derives closed-form expressions for channel capacities under both Gaussian and non-Gaussian input distributions, demonstrating the superiority of Gaussian signaling in achieving optimal data rates across varying signal-to-noise ratios.

Beyond theoretical modeling, this research integrates machine learning techniques to enhance quantum noise modeling and optimize communication systems. The study refines hybrid quantum noise models by employing

Gaussian mixture models and the EM algorithm, improving the estimation of quantum channel capacity. The results demonstrate that reducing the number of Gaussian clusters while preserving the essential noise characteristics enhances the accuracy of channel capacity prediction. This ML-based approach significantly advances quantum noise clustering, optimizing noise mitigation strategies for satellite-based QKD.

A significant contribution of this research lies in applying hybrid quantum noise models to satellite-based quantum communication. The study develops a free-space quantum channel model that integrates hybrid quantum noise, providing a realistic evaluation of quantum SKRs in asymptotic and finite regimes. Critical system parameters—including reconciliation efficiency, transmission coefficient, detection efficiency, receiver telescope aperture, beam waist, and adequate communication time—are systematically analyzed to optimize SKR performance. The findings reveal key trade-offs among satellite altitude, communication windows, noise levels, and synchronization, underscoring the need for effective noise mitigation strategies. Additionally, this study demonstrates that CV Gaussian quantum channels are vulnerable to both quantum and classical noise under collective attacks in a RR setting, offering a more realistic security assessment of QKD. The research further extends its analysis to finite-regime QKD, incorporating satellite orbit dynamics and atmospheric fading effects to optimize secure quantum communication in real-world scenarios.

This work lays a strong foundation for integrating statistical modeling, machine learning, and quantum signal processing to enhance the performance of quantum communication systems. By bridging existing quantum noise models with hybrid quantum noise-based QKD challenges, the findings make a significant contribution to the development of secure and efficient satellite-based quantum networks. The hybrid quantum noise model proposed in this research lays the groundwork for more realistic, accurate, and scalable quantum communication strategies, thereby enhancing the security and efficiency of global quantum networks. Moving forward, this research framework can be extended to more complex multi-hop satellite-based quantum communication architectures, adaptive noise modeling techniques, and the integration of quantum machine learning for dynamic optimization of quantum networks. Ultimately, these advancements will drive the next generation of robust and secure quantum communication infrastructures, accelerating the transition from theoretical models to practical, large-scale quantum networks.

9.1 Future Works:

The findings of this research open several other promising avenues for further exploration, such as in the regime of quantum key distribution. A key direction involves extending the hybrid quantum noise model to complex quantum network architectures, such as multi-hop satellite-based quantum communication networks. Investigating how hybrid noise propagates through

interconnected quantum channels will provide deeper insights into error mitigation, capacity optimization, and the resilience of large-scale quantum communication infrastructures. Future research should explore adaptive noise modeling techniques to mitigate entropy-driven quantum decoherence, enhancing the stability and reliability of real-world quantum networks. Developing dynamic error-correction frameworks and machine-learning-based noise prediction models will be crucial for optimizing the performance of quantum communication. Additionally, investigating the interplay between different quantum entropy measures in practical settings can refine security protocols for large-scale quantum networks. These advancements will contribute to the robustness and scalability of next-generation quantum communication systems. Additionally, the development of adaptive noise models that dynamically adjust based on real-time quantum channel conditions will enhance system robustness under diverse environmental and operational constraints.

Another critical area is the advancement of machine learning techniques for quantum channel estimation and noise modeling. Future work will explore deep learning-based clustering methods and complex clustering techniques to enhance the adaptability of the hybrid quantum noise model. Expanding beyond the current bivariate assumption, future studies will generalize the model to multi-dimensional quantum noise datasets. This will improve noise characterization in more complex quantum communication scenarios, optimizing error correction and security protocols. Additionally, integrating advanced clustering techniques will refine entropy-based quantum channel capacity estimation for real-world applications. Deep learning approaches, particularly variational autoencoders and reinforcement learning-based methods, could improve noise clustering accuracy and optimize resource allocation in quantum communication networks. Future research could also integrate quantum machine learning techniques to develop efficient and scalable quantum error correction protocols tailored for hybrid quantum noise models.

From a security standpoint, investigating the implications of hybrid noise on quantum cryptographic protocols beyond QKD—such as quantum secure direct communication and quantum-enhanced classical cryptographic schemes—will be crucial. Developing security analysis frameworks that incorporate hybrid noise effects will strengthen the resilience of quantum communication systems against sophisticated eavesdropping strategies and adversarial attacks.

Another promising avenue is the study of hybrid noise models in various quantum computing paradigms, including continuous-variable quantum computing and fault-tolerant quantum error correction. Understanding how hybrid quantum noise influences quantum computational processes will be essential for designing noise-resilient quantum algorithms and optimizing fault-tolerant quantum circuits.

Furthermore, experimental validation of hybrid quantum noise models in real-world satellite-based quantum communication testbeds will be a crucial

step toward the practical implementation of these models. Collaborations with space agencies and quantum research institutions could facilitate large-scale testing of these models within operational quantum satellite networks.

Ultimately, this research lays a strong foundation for hybrid quantum noise modeling, with future developments poised to enhance the feasibility, security, and efficiency of quantum communication networks. By bridging theoretical advancements with real-world applications, ongoing research in this area will play a pivotal role in advancing quantum information science and technology.

Appendix A

Qubits Model

Approximating the qubit by a single variable function:

- **Assumption related to joint quantum noise effects:**

Classical communication theory finds that the bits will remain within a specific region of the actual position [20] due to a specific range of noise power, which is practically observed. Although the bit may travel beyond this region, in that case, the noise power would be extremely high, which is not usually observed in practice. The quantum noise can generally be observed when the classical noise has been suppressed. We are simultaneously considering the classical and quantum noise. Considering the above noise power theory is a straightforward choice, as the classical noise is integrated with the quantum system, and its effects should be reflected in the calculations. In connection with control theory, we can infer that within a specific (practical) range of the joint noise power, the qubit will not move far beyond its actual position due to the joint noise effect. This works for both the pure state and the mixed state qubits.

- **Representation of a qubit :**

Case I: *A pure state qubit can be represented by a point (θ, ϕ) on the Bloch sphere:*

A qubit on the Bloch sphere can be viewed as a pure-state qubit. It can be represented by a vector (θ, ϕ) on the surface of the sphere, and it can be represented by a bivariate function $\zeta(\theta, \phi)$, it is clear from the notation that ζ is bivariate function, whose arguments are θ and ϕ , which we call variables x_1 and x_2 respectively. Let us consider the pure-state qubit, and we will discuss how its position is affected by the noise power. Since the pure qubit is lying on the surface of the Bloch sphere, the qubit can be represented as a vector (θ, ϕ) of

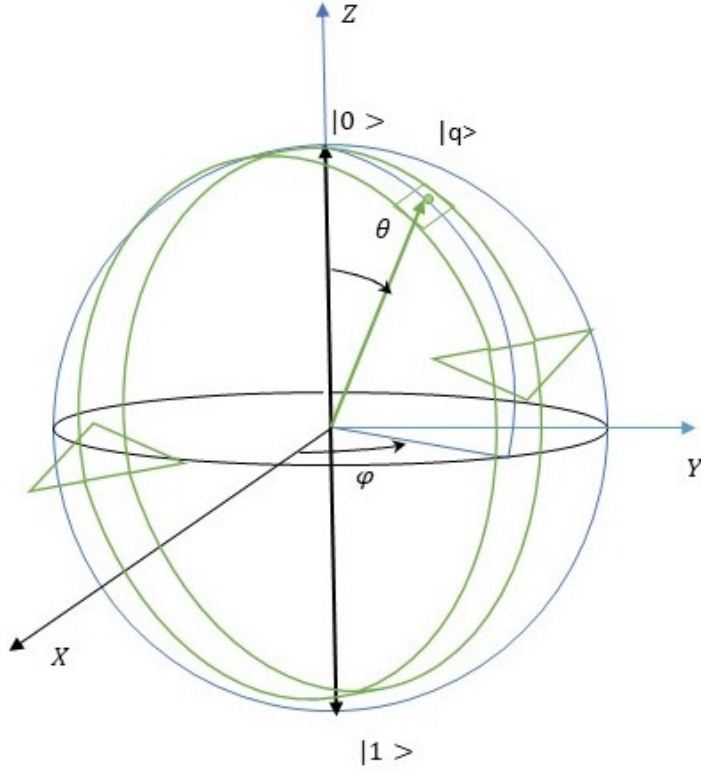


Figure A.1: Case I: Representation of a pure state qubit on the Bloch sphere.

dimension 2. We assume that within a certain noise power the qubit will remain within a complete strip along the surface of the Bloch sphere. In particular, we consider a circular path along the surface of the sphere, which will be the path of the qubit if the qubit is rotated by varying θ while keeping ϕ constant. Now consider a strip along the surface of the sphere that contains the path circle of the qubit in the middle, then the distance from the qubit on the circle to the edges of the strip will be δ on each side. Hence, the breath of the strip will be 2δ shown in Fig. A.1. We consider that if the qubit experiences a certain (practically feasible) range of noise power, then the position of the qubit will not end up far beyond the indicated region (the strip). Mathematically, we considered $(\theta, \phi) \mapsto (\tilde{\theta}, \phi \pm \delta)$ where $\tilde{\theta} \in [0, 2\pi]$. To reduce the computational complexity of the problem, we infer that δ will be so small that the second variable ϕ can be considered constant with respect to θ .

Case II: A mixed qubit can be represented by a point (θ, ϕ, r) inside the Bloch sphere :

A qubit inside the Bloch sphere can be viewed as a mixed-state qubit. It can be represented by a vector (θ, ϕ, r) inside the sphere, and it can be represented by a multivariate function $\tilde{\zeta}(\theta, \phi, r)$, whose arguments are θ , ϕ and r , which we call variables x_1 , x_2 and x_3 respectively. Let us consider the mixed state qubit, and we will discuss its position

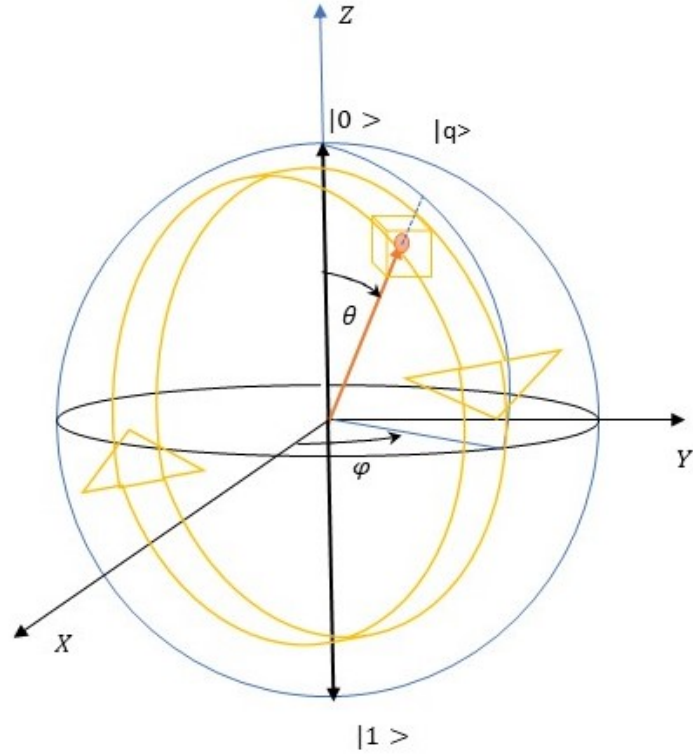


Figure A.2: Case II: Representation of a mixed state qubit inside the Bloch sphere.

affected by the noise power. When we are dealing with the qubit that lies inside the Bloch sphere, the mixed state qubit can be represented as a vector (θ, ϕ, r) , where r is the distance of the qubit from the center of the sphere. In connection to classical communication theory, we assumed that within a certain (feasible) range of noise power, the qubit would remain within a torus/tunnel-like object (whose cross-section is square) inside the Bloch sphere. Consider a circular path inside the sphere, which will be the path of the qubit if one rotates the qubit by varying θ while keeping ϕ and r constant. Now consider a torus/tunnel-like object (whose cross-section is square) inside the sphere that contains the path circle of the qubit in the middle; the distance from the qubit on the circle to the sides of the tunnel will be δ on each side of the cube. Therefore, the area of the cross-sectional region (which is a square) will be $2\delta \times 2\delta$ shown in Fig. A.2. We consider that if the qubit experiences a certain (practically feasible) range for the noise power, then the position of the qubit will not go far beyond the indicated region (the torus /tunnel). Mathematically, we considered $(\theta, \phi, r) \mapsto (\tilde{\theta}, \phi \pm \delta_1, r \pm \delta_2)$ where $\tilde{\theta} \in [0, 2\pi]$. To reduce the complexity, we can infer that the cuboid region can be approximated by the cube region discussed above. Hence, we have, $(\theta, \phi, r) \mapsto (\tilde{\theta}, \phi \pm \delta, r \pm \delta)$ where $\tilde{\theta} \in [0, 2\pi]$. We expect that δ will be so small that the second and third variables ϕ and r can be

considered constant with respect to the first variable θ . Therefore, we have $(\theta, \phi, r) \mapsto (\tilde{\theta}, \phi, r)$ where $\tilde{\theta} \in [0, 2\pi]$.

- In summary, this approximation can be done by varying any of the variables θ and ϕ at a time, considering the other variables as constant with respect to the said variable. In our case, we varied θ , considering the remaining variables as constant.

Appendix B

Quantum Collision Entropy of Hybrid Quantum Noise Approximated as Differential entropy

For well-separated components ($i \neq j$), the integral I in 5.33 is exponentially tiny, meaning the dominant terms arise from the self-overlap terms ($i = j$)

$$I \approx \sum_{i=1}^R w_i^2 \frac{1}{(2\pi)^{d/2} |\Sigma_i|^{1/2}}. \quad (\text{B.1})$$

Thus, the collision entropy of the hybrid quantum noise simplifies to

$$H_2(Z) \approx -\log \sum_{i=1}^R w_i^2 \frac{1}{(2\pi)^{d/2} |\Sigma_i|^{1/2}}. \quad (\text{B.2})$$

The differential entropy of hybrid quantum noise is given by (5.6). For well-separated components $\mathcal{N}(z|\mu_j, \Sigma_j)$ of the hybrid noise, the dominant contribution to $f_Z(z) \log f_Z(z)$ comes from within each Gaussian component

$$h(Z) \approx \sum_{i=1}^R w_i h(\mathcal{N}_i) - \sum_{i=1}^R w_i \log w_i. \quad (\text{B.3})$$

where $H(\cdot)$ is the differential entropy function. The detailed explanation of this approximation is shown in the Appendix. Since for a Gaussian $H(\mathcal{N}_i) = \frac{d}{2} \log(2\pi e) + \frac{1}{2} \log |\Sigma_i|$, [223] we obtain

$$\begin{aligned} H(\mathbf{Z}) &\approx \sum_{i=1}^R w_i \left(\frac{d}{2} \log(2\pi e) + \frac{1}{2} \log |\Sigma_i| \right) - \sum_{i=1}^R w_i \log w_i \\ &\approx \frac{d}{2} \log(2\pi e) + H(\mathbf{w}), \end{aligned} \quad (\text{B.4})$$

where $H(\mathbf{w}) = -\sum_{i=1}^R w_i \log w_i$ is the discrete Shannon entropy of the mixture weights, $\sum_{i=1}^R w_i = 1$ and $\Sigma_i = \mathbf{I}_d$.

Since $\sum w_i^2$ is related to the effective number of components (denoted as R_{eff}) [18, 22], we approximate $\sum_{i=1}^R w_i^2 \approx \frac{1}{R_{\text{eff}}}$. Thus

$$H_2(\mathbf{Z}) \approx \frac{d}{2} \log(2\pi). \quad (\text{B.5})$$

A detailed overview of this approximation is given in the Appendix. Similarly,

$$H(\mathbf{Z}) \approx \frac{d}{2} \log(2\pi e) + H(\mathbf{w}) \approx \frac{d}{2} \log(2\pi e) + \log R_{\text{eff}}. \quad (\text{B.6})$$

Using the approximation $H(\mathbf{w}) \approx \log R_{\text{eff}}$, as $\sum_i w_i \log w_i \leq \log(\sum_i w_i^2) = -\log R_{\text{eff}}$. Now comparing (B.5) with (B.6), the difference

$$H(\mathbf{Z}) - H_2(\mathbf{Z}) \approx \log_2 R_{\text{eff}} + \frac{d}{2} \log_2 e. \quad (\text{B.7})$$

For large R_{eff} , this shows that Hence,

$$H(\mathbf{Z}) \approx H_2(\mathbf{Z}) + \log_2 R_{\text{eff}}. \quad (\text{B.8})$$

For a single Gaussian, $H_2(Z)$ and $h(Z)$ differ by a constant. For a well-separated GMM, $H_2(Z) \approx h(Z) + \log R_{\text{eff}}$. The difference accounts for the number of effective components R_{eff} in the mixture. As $R \rightarrow \infty$ with well-separated clusters, the entropies become asymptotically equivalent to a small correction term. This technique is useful in approximate entropy estimation for high-dimensional GMMs, especially in statistical learning, signal processing, and quantum information theory.

Hence, differential entropy is typically preferred over collision entropy in quantum communication due to its sensitivity to system changes and disturbances within the system. Differential entropy yields higher values than collision entropy, measuring a broader range of statistical uncertainty. In addition, it considers the maximized disturbance to the quantum system and a superior selection of measures when considering information loss, noise, or decoherence in continuous-variable quantum systems.

Appendix C

Proof of Lemma 1 and 2

APPENDIX

C.0.1 Proof of Lemma 1

The aim is to compute an expression for $\boldsymbol{\mu}_k^{(z)}$ as a function of responsibility γ ; this can be done by setting a partial derivative of log-likelihood w.r.t. $\boldsymbol{\mu}_k^{(z)}$ as zero, given by

$$\begin{aligned} \frac{\partial}{\partial \boldsymbol{\mu}_k^{(z)}} \ln f_Z(\mathbf{z}; w, \boldsymbol{\mu}^{(z)}, \boldsymbol{\Sigma}^{(z)}) = 0 &\implies \frac{\partial}{\partial \boldsymbol{\mu}_k^{(z)}} \sum_{n=1}^N \ln f_Z(\mathbf{z}_n; w, \boldsymbol{\mu}^{(z)}, \boldsymbol{\Sigma}^{(z)}) = 0 \\ &\implies \sum_{n=1}^N \frac{\frac{e^{-\lambda} \lambda^k}{k!} \frac{\partial}{\partial \boldsymbol{\mu}_k^{(z)}} \{\mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)})\}}{\sum_{k=1}^K \frac{e^{-\lambda} \lambda^k}{k!} \mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)})} = 0 \quad (\text{C.1}) \end{aligned}$$

To evaluate the density derivative of $\mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)})$ w.r.t. $\boldsymbol{\mu}_k^{(z)}$ given by,

$$\begin{aligned} \frac{\partial}{\partial \boldsymbol{\mu}_k^{(z)}} \mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)}) &= \frac{\partial}{\partial \boldsymbol{\mu}_k^{(z)}} \left\{ \frac{1}{(2\pi)^{D/2} |\boldsymbol{\Sigma}_k^{(z)}|^{1/2}} e^{-\frac{1}{2}(\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)})^T \boldsymbol{\Sigma}_k^{(z)-1} (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)})} \right\} \\ &= \frac{1}{(2\pi)^{D/2} |\boldsymbol{\Sigma}_k^{(z)}|^{1/2}} \frac{\partial}{\partial \boldsymbol{\mu}_k^{(z)}} e^{-\frac{1}{2}(\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)})^T \boldsymbol{\Sigma}_k^{(z)-1} (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)})} \\ &= \frac{1}{(2\pi)^{D/2} |\boldsymbol{\Sigma}_k^{(z)}|^{1/2}} e^{-\frac{1}{2}(\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)})^T \boldsymbol{\Sigma}_k^{(z)-1} (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)})} \\ &\quad \frac{\partial}{\partial \boldsymbol{\mu}_k^{(z)}} \left\{ -\frac{1}{2}(\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)})^T \boldsymbol{\Sigma}_k^{(z)-1} (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)}) \right\} \\ &= -\frac{1}{2} \mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)}) \frac{\partial}{\partial \boldsymbol{\mu}_k^{(z)}} \left\{ (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)})^T \boldsymbol{\Sigma}_k^{(z)-1} (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)}) \right\} \\ &= \mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)}) (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)})^T \boldsymbol{\Sigma}_k^{(z)-1} \end{aligned} \quad (\text{C.2})$$

Moreover, the density derivative $(\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)})^T \boldsymbol{\Sigma}_k^{(z)-1} (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)})$ w.r.t. $\boldsymbol{\mu}_k^{(z)}$ is given by

$$\frac{\partial}{\partial \boldsymbol{\mu}_k^{(z)}} \left\{ (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)})^T \boldsymbol{\Sigma}_k^{(z)-1} (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)}) \right\} = -2(\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)})^T \boldsymbol{\Sigma}_k^{(z)-1} \quad (\text{C.3})$$

This can simply done by using the matrix rule, $\frac{\partial}{\partial x} \{x^T A x\} = x^T A^T + x^T A$, and setting $x = \mathbf{z}_n - \boldsymbol{\mu}_k^{(z)}$, $A := \boldsymbol{\Sigma}_k^{(z)-1}$ and also note $\boldsymbol{\Sigma}_k^{(z)}$ is symmetric.

Therefore, the ultimate equation for calculating the expression of $\boldsymbol{\mu}_k^{(z)}$ as a function of the responsibility γ is derived as follows

$$\sum_{n=1}^N \left[\frac{\frac{e^{-\lambda} \lambda^k}{k!} \mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)})}{\sum_{j=1}^K \frac{e^{-\lambda} \lambda^j}{j!} \mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_j, \boldsymbol{\Sigma}_j)} (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)})^T \{\boldsymbol{\Sigma}_k^{(z)}\}^{-1} \right] = 0 \quad (\text{C.4})$$

since each $\gamma(t_{n,k})$ being a probability is a scalar, therefore $\gamma(t_{n,k})^T = \gamma(t_{n,k})$ gives

$$\boldsymbol{\mu}_k^{(z)} = \frac{\sum_{n=1}^N \gamma(t_{n,k}) \mathbf{z}_n}{\sum_{n=1}^N \gamma(t_{n,k})}. \quad (\text{C.5})$$

C.0.2 Proof of Lemma 2

To compute an expression for $\boldsymbol{\Sigma}_k^{(z)}$ as a function of responsibility γ , let us set the partial derivative of log-likelihood w.r.t. $\boldsymbol{\Sigma}_k^{(z)}$ by setting zero, given by $\frac{\partial}{\partial \boldsymbol{\Sigma}_k^{(z)}} \log f_{\mathbf{Z}}(\mathbf{z}; w, \boldsymbol{\mu}, \boldsymbol{\Sigma}) = 0$. Before compute an expression for $\boldsymbol{\Sigma}_k^{(z)}$, it is necessary to simplify the partial derivative log-likelihood w.r.t. $\boldsymbol{\Sigma}_k^{(z)}$ given by

$$\begin{aligned} & \frac{\partial}{\partial \boldsymbol{\Sigma}_k^{(z)}} \ln f_{\mathbf{Z}}(\mathbf{z}; w, \boldsymbol{\mu}, \boldsymbol{\Sigma}) \\ &= \frac{\partial}{\partial \boldsymbol{\Sigma}_k^{(z)}} \sum_{n=1}^N \ln \sum_{k=1}^K \frac{e^{-\lambda} \lambda^k}{k!} \mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)}) = \sum_{n=1}^N \frac{\frac{\partial}{\partial \boldsymbol{\Sigma}_k^{(z)}} \left(\frac{e^{-\lambda} \lambda^k}{k!} \mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)}) \right)}{\sum_{k=1}^K \frac{e^{-\lambda} \lambda^k}{k!} \mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)})}, \end{aligned} \quad (\text{C.6})$$

as $\frac{\partial}{\partial \boldsymbol{\Sigma}_k^{(z)}} \frac{e^{-\lambda} \lambda^j}{j!} \mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_j, \boldsymbol{\Sigma}_j) = 0 \forall j \neq k \in 1, \dots, N$.

To compute the part, $\frac{\partial}{\partial \boldsymbol{\Sigma}_k^{(z)}} \frac{e^{-\lambda} \lambda^k}{k!} \mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)})$ we will approach through the partial derivative of the logarithm of $\frac{e^{-\lambda} \lambda^k}{k!} \mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)})$ w.r.t. $\boldsymbol{\Sigma}_k^{(z)}$, given by $\frac{\partial}{\partial \boldsymbol{\Sigma}_k^{(z)}} \ln \left(\frac{e^{-\lambda} \lambda^k}{k!} \mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)}) \right)$.

This method simplifies the differentiation process by taking advantage of the logarithm's properties to break down the product and exponential

components within the function. Note that

$$\begin{aligned} & \frac{\partial}{\partial \Sigma_k^{(z)}} \frac{e^{-\lambda} \lambda^k}{k!} \mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_k^{(z)}, \Sigma_k^{(z)}) \\ &= \frac{e^{-\lambda} \lambda^k}{k!} \mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_k^{(z)}, \Sigma_k^{(z)}) \frac{\partial}{\partial \Sigma_k^{(z)}} \ln \left(\frac{e^{-\lambda} \lambda^k}{k!} \mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_k^{(z)}, \Sigma_k^{(z)}) \right), \quad (\text{C.7}) \end{aligned}$$

plugging all together gives the partial derivative of log-likelihood w.r.t. $\Sigma_k^{(z)}$ as,

$$\frac{\partial}{\partial \Sigma_k^{(z)}} \ln f_{\mathbf{Z}}(\mathbf{z}; w, \boldsymbol{\mu}, \boldsymbol{\Sigma}) = \sum_{n=1}^N \gamma(t_{n,k}) \frac{\partial}{\partial \Sigma_k^{(z)}} \ln \left(\frac{e^{-\lambda} \lambda^k}{k!} \mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_k^{(z)}, \Sigma_k^{(z)}) \right). \quad (\text{C.8})$$

Note here that

$$\begin{aligned} & \frac{\partial}{\partial \Sigma_k^{(z)}} \ln \left(\frac{e^{-\lambda} \lambda^k}{k!} \mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_k^{(z)}, \Sigma_k^{(z)}) \right) \\ &= \frac{\partial}{\partial \Sigma_k^{(z)}} \ln \left(\frac{e^{-\lambda} \lambda^k}{k!} \right) + \frac{\partial}{\partial \Sigma_k^{(z)}} \ln \left(\frac{1}{(2\pi)^{D/2} |\Sigma_k^{(z)}|^{1/2}} \right) \\ & \quad + \frac{\partial}{\partial \Sigma_k^{(z)}} \left\{ -\frac{1}{2} (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)})^T \Sigma_k^{(z)-1} (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)}) \right\} \quad (\text{C.9}) \end{aligned}$$

For the first part, $\ln \left(\frac{e^{-\lambda} \lambda^k}{k!} \right)$ is constant w.r.t. $\Sigma_k^{(z)}$, hence $\frac{\partial}{\partial \Sigma_k^{(z)}} \left\{ \ln \frac{e^{-\lambda} \lambda^k}{k!} \right\} = 0$. For the second part,

$$\begin{aligned} & \frac{\partial}{\partial \Sigma_k^{(z)}} \left\{ \ln \left(\frac{1}{(2\pi)^{D/2} |\Sigma_k^{(z)}|^{1/2}} \right) \right\} \\ &= \frac{\partial}{\partial \Sigma_k^{(z)}} \left\{ \ln((2\pi)^{-D/2} |\Sigma_k^{(z)}|^{-1/2}) \right\} \\ &= \frac{\partial}{\partial \Sigma_k^{(z)}} \left\{ -\frac{D}{2} \ln(2\pi) - \frac{1}{2} \ln |\Sigma_k^{(z)}| \right\} = -\frac{1}{2} \frac{\partial}{\partial \Sigma_k^{(z)}} \ln |\Sigma_k^{(z)}| \\ &= -\frac{1}{2} \frac{1}{|\Sigma_k^{(z)}|} \frac{\partial}{\partial \Sigma_k^{(z)}} |\Sigma_k^{(z)}| = -\frac{1}{2} \frac{1}{|\Sigma_k^{(z)}|} |\Sigma_k^{(z)}| (\Sigma_k^{(z)-1})^T = -\frac{1}{2} \Sigma_k^{(z)-1} \end{aligned} \quad (\text{C.10})$$

This can be computed using the matrix rule $\frac{\partial}{\partial \mathbf{A}} |\mathbf{A}| = |\mathbf{A}| (\mathbf{A}^{-1})^T$; and note $\Sigma_k^{(z)}$ is symmetric.

For the third part, the partial derivative of $\frac{1}{2} (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)})^T \Sigma_k^{(z)-1} (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)})$ w.r.t. $\Sigma_k^{(z)}$, can be computed using the matrix rule $\frac{\partial}{\partial \mathbf{A}} (\mathbf{b}^T \mathbf{A}^{-1} \mathbf{b}) =$

$-\mathbf{A}^{-1}\mathbf{b}\mathbf{b}^T\mathbf{A}^{-1}$, considering, $\mathbf{b} = \mathbf{z}_n - \boldsymbol{\mu}_k^{(z)}$; $\mathbf{A} = \boldsymbol{\Sigma}_k^{(z)}$, which is given by

$$\begin{aligned} \frac{\partial}{\partial \boldsymbol{\Sigma}_k^{(z)}} \left\{ -\frac{1}{2}(\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)})^T \boldsymbol{\Sigma}_k^{(z)-1} (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)}) \right\} &= -\frac{1}{2} \frac{\partial}{\partial \boldsymbol{\Sigma}_k^{(z)}} \left\{ (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)})^T \boldsymbol{\Sigma}_k^{(z)-1} (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)}) \right\} \\ &= -\frac{1}{2} \left\{ -\boldsymbol{\Sigma}_k^{(z)-1} (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)}) (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)})^T \boldsymbol{\Sigma}_k^{(z)-1} \right\} \\ &= \frac{1}{2} \boldsymbol{\Sigma}_k^{(z)-1} (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)}) (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)})^T \boldsymbol{\Sigma}_k^{(z)-1}. \quad (\text{C.11}) \end{aligned}$$

Therefore, we have

$$\begin{aligned} \frac{\partial}{\partial \boldsymbol{\Sigma}_k^{(z)}} \ln \left(\frac{e^{-\lambda} \lambda^k}{k!} \mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)}) \right) \\ = \frac{\partial}{\partial \boldsymbol{\Sigma}_k^{(z)}} \left\{ \ln \left(\frac{1}{(2\pi)^{D/2} |\boldsymbol{\Sigma}_k^{(z)}|^{1/2}} \right) \right\} + \frac{\partial}{\partial \boldsymbol{\Sigma}_k^{(z)}} \left\{ -\frac{1}{2} (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)})^T \boldsymbol{\Sigma}_k^{(z)-1} (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)}) \right\} \\ = -\frac{1}{2} \boldsymbol{\Sigma}_k^{(z)-1} + \frac{1}{2} \boldsymbol{\Sigma}_k^{(z)-1} (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)}) (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)})^T \boldsymbol{\Sigma}_k^{(z)-1}. \quad (\text{C.12}) \end{aligned}$$

Hence, the final expression of the partial derivative of log-likelihood w.r.t. $\boldsymbol{\Sigma}_k^{(z)}$ by

$$\begin{aligned} \frac{\partial}{\partial \boldsymbol{\Sigma}_k^{(z)}} \ln f_{\mathbf{Z}}(\mathbf{z}; w, \boldsymbol{\mu}, \boldsymbol{\Sigma}) \\ = \sum_{n=1}^N \gamma(t_{n,k}) \left\{ -\frac{1}{2} \boldsymbol{\Sigma}_k^{(z)-1} + \frac{1}{2} \boldsymbol{\Sigma}_k^{(z)-1} (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)}) (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)})^T \boldsymbol{\Sigma}_k^{(z)-1} \right\}. \quad (\text{C.13}) \end{aligned}$$

Finally, maximizing log-likelihood w.r.t. $\boldsymbol{\Sigma}_k^{(z)}$ by setting the derivative zero gives the expression for $\boldsymbol{\Sigma}_k^{(z)}$ depending on the responsibility γ as,

$$\begin{aligned} \frac{\partial}{\partial \boldsymbol{\Sigma}_k^{(z)}} \log f_{\mathbf{Z}}(\mathbf{z}; w, \boldsymbol{\mu}, \boldsymbol{\Sigma}) &= 0 \\ \Rightarrow \sum_{n=1}^N \frac{1}{\sum_{k=1}^K \frac{e^{-\lambda} \lambda^k}{k!} \mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)})} \frac{\partial}{\partial \boldsymbol{\Sigma}_k^{(z)}} \frac{e^{-\lambda} \lambda^k}{k!} \mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)}) &= 0 \\ \Rightarrow \sum_{n=1}^N \frac{1}{\sum_{k=1}^K \frac{e^{-\lambda} \lambda^k}{k!} \mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)})} \\ \frac{e^{-\lambda} \lambda^k}{k!} \mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)}) \frac{\partial}{\partial \boldsymbol{\Sigma}_k^{(z)}} \ln \left(\frac{e^{-\lambda} \lambda^k}{k!} \mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)}) \right) &= 0 \\ \Rightarrow \frac{1}{2} \sum_{n=1}^N \frac{\frac{e^{-\lambda} \lambda^k}{k!} \mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)})}{\sum_{k=1}^K \frac{e^{-\lambda} \lambda^k}{k!} \mathcal{N}(\mathbf{z}_n; \boldsymbol{\mu}_k^{(z)}, \boldsymbol{\Sigma}_k^{(z)})} \\ \left[\{\boldsymbol{\Sigma}_k^{(z)}\}^{-1} - \{\boldsymbol{\Sigma}_k^{(z)}\}^{-1} (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)}) (\mathbf{z}_n - \boldsymbol{\mu}_k^{(z)})^T \{\boldsymbol{\Sigma}_k^{(z)}\}^{-1} \right] &= 0 \end{aligned}$$

$$\begin{aligned}
&\Rightarrow \sum_{n=1}^N \gamma(t_{n,k}) \{\Sigma_k^{(z)}\}^{-1} \left[(\mathbf{z}_n - \mu_k^{(z)}) (\mathbf{z}_n - \mu_k^{(z)})^T \{\Sigma_k^{(z)}\}^{-1} - 1 \right] = 0 \\
&\Rightarrow \sum_{n=1}^N \gamma(t_{n,k}) \left[(\mathbf{z}_n - \mu_k^{(z)}) (\mathbf{z}_n - \mu_k^{(z)})^T \{\Sigma_k^{(z)}\}^{-1} - 1 \right] = 0 \\
&\Rightarrow \left\{ \sum_{n=1}^N \gamma(t_{n,k}) (\mathbf{z}_n - \mu_k^{(z)}) (\mathbf{z}_n - \mu_k^{(z)})^T \{\Sigma_k^{(z)}\}^{-1} \right\} = \sum_{n=1}^N \gamma(t_{n,k})
\end{aligned} \tag{C.14}$$

$$\Sigma_k^{(z)} = \frac{\sum_{n=1}^N \gamma(t_{n,k}) (\mathbf{z}_n - \mu_k^{(z)}) (\mathbf{z}_n - \mu_k^{(z)})^T}{\sum_{i=1}^N \gamma(t_{n,k})}. \tag{C.15}$$

C.0.3 The conditional density $f_Z(\mathbf{z}|t_k = 0)$ given that $\mathbf{z}$ does not belong to the k -th Gaussian component

To simplify the calculation for $f_Z(\mathbf{z}|t_k = 0)$, let's break down the steps in a more straightforward way. The GMM for the noise $\mathbf{Z}$ is given by (6.4). The conditional density when a data point belongs to the k -th Gaussian component is given in Section III(A). The joint probability is computed in (6.5). The conditional density the density of $\mathbf{z}$ given that it does not belong to the k -th Gaussian component is given by $f_Z(\mathbf{z}|t_k = 0)$. It can be calculated by considering all components except the k -th

$$f_Z(\mathbf{z}|t_k = 0) = \frac{f_Z(\mathbf{z}) - f_Z(\mathbf{z}, t_k = 1)}{1 - f_Z(t_k = 1)}. \tag{C.16}$$

Using the expressions for $f_Z(\mathbf{z})$ and $f_Z(\mathbf{z}, t_k = 1)$,

$$f_Z(\mathbf{z}|t_k = 0) = \frac{\sum_{i=0}^K \frac{e^{-\lambda} \lambda^i}{i!} N(\mathbf{z}; \mu_i^{(z)}, \Sigma_i^{(z)}) - \frac{e^{-\lambda} \lambda^k}{k!} N(\mathbf{z}; \mu_k^{(z)}, \Sigma_k^{(z)})}{1 - \frac{e^{-\lambda} \lambda^k}{k!}}. \tag{C.17}$$

The numerator simplifies to $\sum_{\substack{i=0 \\ i \neq k}}^K \frac{e^{-\lambda} \lambda^i}{i!} N(\mathbf{z}; \mu_i^{(z)}, \Sigma_i^{(z)})$, and the denominator becomes $1 - \frac{e^{-\lambda} \lambda^k}{k!}$, that is $\sum_{\substack{i=0 \\ i \neq k}}^K \frac{e^{-\lambda} \lambda^i}{i!}$. Therefore, the simplified expression for $f_Z(\mathbf{z}|t_k = 0)$ is

$$f_Z(\mathbf{z}|t_k = 0) = \left[\sum_{\substack{i=0 \\ i \neq k}}^K \frac{e^{-\lambda} \lambda^i}{i!} N(\mathbf{z}; \mu_i^{(z)}, \Sigma_i^{(z)}) \right] / \left[\sum_{\substack{i=0 \\ i \neq k}}^K \frac{e^{-\lambda} \lambda^i}{i!} \right]. \tag{C.18}$$

This formula provides the p.d.f. for $\mathbf{z}$ given that it does not belong to the k -th component, expressed as a weighted sum of all other Gaussian components.

Bibliography

- [1] Ivan B Djordjevic. *Quantum Communication, Quantum Networks, and Quantum Sensing*. Academic Press, 2022.
- [2] Mark M Wilde. *Quantum information theory*. Cambridge university press, 2013.
- [3] Sandor Imre and Laszlo Gyongyosi. *Advanced quantum communications: an engineering approach*. John Wiley & Sons, 2012.
- [4] Nadasadat Hosseinidehaj, Zunaira Babar, Robert Malaney, Soon Xin Ng, and Lajos Hanzo. Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook. *IEEE Communications Surveys & Tutorials*, 21(1):881–919, 2019.
- [5] Laszlo Gyongyosi and Sandor Imre. Resource prioritization and balancing for the quantum internet. *Scientific Reports*, 10(22390), 2020.
- [6] Sandor Imre and Ferenc Balazs. *Quantum Computing and Communications: An Engineering Approach*. John Wiley & Sons, 2005.
- [7] Ivan B. Djordjevic. *Physical-Layer Security and Quantum Key Distribution*. Springer, 2019. ISBN 978-3-030-27564-8, 978-3-030-27567-9, 978-3-030-27565-5. doi: 10.1007/978-3-030-27565-5.
- [8] Laszlo Gyongyosi and Sandor Imre. Entanglement concentration service for the quantum internet. *Quantum Information Processing*, 19: 1–28, 2020.
- [9] Ivan B. Djordjevic and Vijay Nafria. Entanglement assisted radars operated over strong atmospheric turbulence channels. In *2024 24th International Conference on Transparent Optical Networks (ICTON)*, pages 1–6, 2024. doi: 10.1109/ICTON62926.2024.10647723.
- [10] N.J. Cerf, G. Leuchs, and E.S. Polzik. “*Quantum Information with Continuous Variables of Atoms and Light*”. Imperial College Press, London, United Kingdom, 2007. ISBN 9781860947605.
- [11] Anthony Mark Fox. *Quantum optics: an introduction*, volume 15. Oxford University Press, 2006.

- [12] Laszlo Gyongyosi and Sandor Imre. Routing space exploration for scalable routing in the quantum internet. *Scientific reports*, 10(1):11874, 2020.
- [13] Laszlo Gyongyosi and Sandor Imre. Optimizing high-efficiency quantum memory with quantum machine learning for near-term quantum devices. *Scientific Reports*, 10:135, 2020. doi: 10.1038/s41598-019-56689-0.
- [14] Laszlo Gyongyosi and Sandor Imre. Theory of quantum gravity information processing. *Quantum Engineering*, 1(4):e23, 2019.
- [15] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical computer science*, 560:7–11, 2014.
- [16] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of modern physics*, 74(1):145, 2002.
- [17] H Jeff Kimble. The quantum internet. *Nature*, 453(7198):1023–1030, 2008.
- [18] Mouli Chakraborty, Anshu Mukherjee, Ioannis Krikidis, Avishek Nag, and Subhash Chandra. An unsupervised machine learning to optimize hybrid quantum noise clusters for gaussian quantum channel. *IEEE Transactions on Green Communications and Networking*, pages 1–1, 2025. doi: 10.1109/TGCN.2025.3587144.
- [19] Stefano Pirandola, B Roy Bardhan, Tobias Gehring, Christian Weedbrook, and Seth Lloyd. Advances in photonic quantum sensing. *Nature Photonics*, 12(12):724–733, 2018.
- [20] S. S. Haykin. *Communication systems*. Wiley, New York, 2001.
- [21] Mouli Chakraborty, Anshu Mukherjee, Avishek Nag, and Subhash Chandra. Hybrid quantum noise model to compute Gaussian quantum channel capacity. *IEEE Access*, 12:14671–14689, 2024.
- [22] Mouli Chakraborty, Anshu Mukherjee, Ioannis Krikidis, Avishek Nag, and Subhash Chandra. Hybrid quantum noise approximation and pattern analysis on parameterized component distributions. In *2024 IEEE Middle East Conference on Communications and Networking (MECOM)*, pages 251–256, 2024. doi: 10.1109/MECOM61498.2024.10881051.
- [23] Mouli Chakraborty, Anshu Mukherjee, Ioannis Krikidis, Avishek Nag, and Subhash Chandra. A hybrid noise approach to modeling of free-space satellite quantum communication channel for continuous-variable qkd. *IEEE Transactions on Green Communications and Networking*, 9(3):1311–1325, 2025. doi: 10.1109/TGCN.2024.3525297.

- [24] Mouli Chakraborty, Anshu Mukherjee, Avishek Nag, and Subhash Chandra. A hybrid noise model for satellite quantum communication channels: Continuous-variable QKD in the finite-size regime, 2024. URL <https://arxiv.org/abs/2404.0>.
- [25] Imre Gyongyosi and Sandor Imre. Low-dimensional reconciliation for continuous-variable quantum key distribution. *Applied Sciences*, 8(1): 87, 2018. doi: 10.3390/app8010087.
- [26] Daniele Dequal, Luis Trigo Vidarte, Victor Roman Rodriguez, Giuseppe Vallone, Paolo Villoresi, Anthony Leverrier, and Eleni Diamanti. Feasibility of satellite-to-ground continuous-variable quantum key distribution. *npj Quantum Information*, 7(1):3, 2021.
- [27] Laszlo Gyongyosi and Sandor Imre. Secret key rates of free-space optical continuous-variable quantum key distribution. *International Journal of Communication Systems*, 32(18):e4152, 2019.
- [28] Stefano Pirandola. Satellite quantum communications: Fundamental bounds and practical security. *Phys. Rev. Res.*, 3:023130, May 2021.
- [29] Masanori Ohya and Dénes Petz. *Quantum entropy and its use*. Springer Science & Business Media, 2004.
- [30] Christopher M Bishop. *Pattern Recognition and Machine Learning by Christopher M. Bishop*. Springer Science+ Business Media, LLC, 2006.
- [31] Jelena Mackeprang, Durga B Rao Dasari, and Jörg Wrachtrup. A reinforcement learning approach for quantum state engineering. *Quantum Machine Intelligence*, 2:1–14, 2020.
- [32] Yannic Rath, Aldo Glielmo, and George H Booth. A bayesian inference framework for compression and prediction of quantum states. *The Journal of chemical physics*, 153(12), 2020.
- [33] Eva Patel and Dharmender Singh Kushwaha. Clustering cloud workloads: K-means vs Gaussian mixture model. *Procedia computer science*, 171:158–167, 2020.
- [34] Laszlo Gyongyosi and Sandor Imre. Gaussian quadrature inference for multicarrier continuous-variable quantum key distribution. *Quantum studies: mathematics and foundations*, 6(4):397–430, 2019.
- [35] Christopher Erven, B Heim, E Meyer-Scott, JP Bourgoïn, R Laflamme, G Weihs, and T Jennewein. Studying free-space transmission statistics and improving free-space quantum key distribution in the turbulent atmosphere. *New Journal of Physics*, 14(12):123018, 2012.

- [36] Masoud Ghalaii and Stefano Pirandola. Quantum communications in a moderate-to-strong turbulent space. *Communications Physics*, 5(1): 38, 2022.
- [37] D Yu Vasylyev, AA Semenov, and W Vogel. Toward global quantum communication: beam wandering preserves nonclassicality. *Physical review letters*, 108(22):220501, 2012.
- [38] Wenyuan Wang, Feihu Xu, and Hoi-Kwong Lo. Prefixed-threshold real-time selection method in free-space quantum key distribution. *Physical Review A*, 97(3):032337, 2018.
- [39] Stefano Pirandola. Satellite quantum communications: Fundamental bounds and practical security. *Physical Review Research*, 3(2):023130, 2021.
- [40] S. Wehner et al. Quantum internet: A vision for the road ahead. *Science*, 362(6412), 2018. doi: 10.1126/science.aam9288.
- [41] Jessica Illiano, Marcello Caleffi, Antonio Manzalini, and Angela Sara Cacciapuoti. Quantum internet protocol stack: A comprehensive survey. *Computer Networks*, 213:109092, 2022. ISSN 1389-1286. doi: <https://doi.org/10.1016/j.comnet.2022.109092>. URL <https://www.sciencedirect.com/science/article/pii/S1389128622002250>.
- [42] Sara Santos, Francisco A. Monteiro, Bruno C. Coutinho, and Yasser Omar. Shortest path finding in quantum networks with quasi-linear complexity. *IEEE Access*, 11:7180–7194, 2023. doi: 10.1109/ACCESS.2023.3237997.
- [43] Jiancheng An, Hongbin Li, Derrick Wing Kwan Ng, and Chau Yuen. Fundamental detection probability vs. achievable rate tradeoff in integrated sensing and communication systems. *IEEE Transactions on Wireless Communications*, 22(12):9835–9853, 2023.
- [44] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, 2014.
- [45] Valerio Scarani et al. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81:1301–1350, 2009. doi: 10.1103/RevModPhys.81.1301.
- [46] Artur K. Ekert. Quantum cryptography based on Bell’s theorem. *Physical Review Letters*, 67:661–663, 1991. doi: 10.1103/PhysRevLett.67.661.
- [47] Thomas Jennewein et al. Quantum cryptography with entangled photons. *Physical Review Letters*, 84:4729–4732, 2000. doi: 10.1103/PhysRevLett.84.4729.

- [48] H. J. Briegel et al. Quantum repeaters: the role of imperfect local operations in quantum communication. *Physical Review Letters*, 81: 5932–5935, 1998. doi: 10.1103/PhysRevLett.81.5932.
- [49] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein. Advances in quantum teleportation. *Nature Photonics*, 9(10): 641–652, 2015.
- [50] Michael A. Nielsen and Isaac L. Chuang. “*Quantum Computation and Quantum Information: 10th Anniversary Edition*”. Cambridge University Press, 2010. doi: 10.1017/CBO9780511976667.
- [51] László Gyöngyösi, Laszlo Bacsardi, and Sandor Imre. A survey on quantum key distribution. *Infocommunications journal*, 11(2):14–21, 2019.
- [52] Salonik Resch and Ulya R. Karpuzcu. Benchmarking quantum computers and the impact of quantum noise. *ACM Comput. Surv.*, 54(7), jul 2021. ISSN 0360-0300.
- [53] S. Castelletto, I. P. Degiovanni, and M. L. Rastello. Quantum and classical noise in practical quantum-cryptography systems based on polarization-entangled photons. *Physical Review A*, 67(2), feb 2003.
- [54] H. Paul. Photon antibunching. *Rev. Mod. Phys.*, 54:1061, 1982.
- [55] M. J. Kirton et al. Advances in solid state photomultipliers. *Laser and Photon. Rev.*, 12:1700208, 2018.
- [56] C. C. Gerry et al. Quantum optical state comparison amplifier. *Phys. Rev. A*, 66:033812, 2002.
- [57] F. W. Strauch. Relativistic quantum walks. *Phys. Rev. A*, 73:054302, 2006.
- [58] M. O. Scully et al. *Quantum optics*. Cambridge University Press, 1997.
- [59] L. G. C. Rego et al. 1/f noise in phonon transport. *Phys. Rev. Lett.*, 81:232, 1998.
- [60] G. P. Agrawal et al. Modeling of quantum-dot semiconductor lasers. *IEEE J. Quantum Electron.*, 39:1383, 2003.
- [61] A. Issac et al. Correlated photon pair generation in AlGaAs nanowaveguides via spontaneous FWM. *Phys. Rev. B*, 87:035313, 2013.
- [62] J. B. Johnson. Thermal agitation of electricity in conductors. *Phys. Rev.*, 32:97, 1928.

- [63] W. Schottky. Über spontane stromschwankungen in verschiedenen elektrizitätsleitern. *Ann. Phys.*, 362:541, 1918.
- [64] D. B. Leeson. A simple model of feedback oscillator noise spectrum. *Proc. IEEE*, 54:329, 1966.
- [65] R. F. Voss. 1/f (flicker) noise: A brief review. In *33rd Annual Symposium on Frequency Control*, 1979.
- [66] S. Donati. *Photodetectors*. Prentice Hall, 1999.
- [67] J. Bardeen et al. Currents due to drift and diffusion of electrons and holes in germanium. *Phys. Rev.*, 71:717, 1947.
- [68] F. N. Hooge. 1/f noise is no surface effect. *Phys. Lett. A*, 29:139, 1969.
- [69] M. J. Buckingham. *Noise in Electronic Devices and Systems*. Horwood, 1983.
- [70] Hyang-Tag Lim, Jong-Chan Lee, Kang-Hee Hong, and Yoon-Ho Kim. Avoiding entanglement sudden death using single-qubit quantum measurement reversal. *Optics express*, 22 16:19055–68, 2014. URL <https://api.semanticscholar.org/CorpusID:19420592>.
- [71] K. C. Lee, M. R. Sprague, B. J. Sussman, J. Nunn, N. K. Langford, X.-M. Jin, T. Champion, P. Michelberger, K. F. Reim, D. England, D. Jaksch, and I. A. Walmsley. Entangling macroscopic diamonds at room temperature. *Science*, 334(6060):1253–1256, 2011.
- [72] Haijun Kang, Dongmei Han, Na Wang, Yang Liu, Shuhong Hao, and Xiaolong Su. Experimental demonstration of robustness of gaussian quantum coherence, 2021.
- [73] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd. Gaussian quantum information. *Rev. Mod. Phys.*, 84:621, May 2012.
- [74] John Preskill. Lecture notes for physics 219: Quantum computation. *Caltech Lecture Notes*, 7, 1999.
- [75] D. Aharonov, A. Kitaev, and J. Preskill. Fault-tolerant quantum computation with long-range correlated noise. *Physical Review Letters*, 81 (11):2190, 1998. doi: 10.1103/PhysRevLett.81.2190.
- [76] D. A. Lidar and K. B. Whaley. Decoherence-free subspaces and subsystems. In *Irreversible Quantum Dynamics*, pages 83–120. Springer, 2003. doi: 10.1007/978-3-662-10349-5-5.

- [77] Charles H. Bennett and Stephen J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Physical Review Letters*, 69:2881–2884, 1992. doi: 10.1103/PhysRevLett.69.2881.
- [78] D. Gottesman. *Stabilizer codes and quantum error correction*. PhD thesis, California Institute of Technology, 1997.
- [79] J. Preskill. Quantum information and computation, 2000. Lecture notes available online: <http://www.theory.caltech.edu/people/preskill/ph229/>.
- [80] P. W. Shor. Scheme for reducing decoherence in quantum computer memory. *Physical Review A*, 52(4):R2493–R2496, 1995. doi: 10.1103/PhysRevA.52.R2493.
- [81] D. Gottesman. An introduction to quantum error correction and fault-tolerant quantum computation. *Proceedings of Symposia in Applied Mathematics*, 68:13–58, 2010.
- [82] Daryus Chandra, Zeynep B. Kaykac Egilmez, Yifeng Xiong, Soon Xin Ng, Robert G. Maunder, and Lajos Hanzo. Universal decoding of quantum stabilizer codes via classical guesswork. *IEEE Access*, 11: 19059–19072, 2023. doi: 10.1109/ACCESS.2023.3247966.
- [83] Diogo Cruz, Francisco A. Monteiro, and Bruno C. Coutinho. Quantum error correction via noise guessing decoding. *IEEE Access*, 11:119446–119461, 2023. doi: 10.1109/ACCESS.2023.3327214.
- [84] Zunaira Babar, Daryus Chandra, Hung Viet Nguyen, Panagiotis Botsinis, Dimitrios Alanis, Soon Xin Ng, and Lajos Hanzo. Duality of quantum and classical error correction codes: Design principles and examples. *IEEE Communications Surveys & Tutorials*, 21(1): 970–1010, 2019. doi: 10.1109/COMST.2018.2861361.
- [85] M. C. Kuzyk and S. J. van Enk. Mimicking decoherence in classical noise. *Physical Review A*, 99(6), 2019. doi: 10.1103/PhysRevA.99.062101.
- [86] P. A. Knott. A search for quantum decoherence effects in heavy ion recoil events. *European Physical Journal C*, 76(1), 2016. doi: 10.1140/epjc/s10052-015-3864-0.
- [87] J. E. Hoffman et al. Decoherence, quantum fluctuations, and quantum noise. In *AIP Conference Proceedings*, volume 1362, 2011. doi: 10.1063/1.3627288.
- [88] N. Kumar et al. Matching classical and quantum noise for arbitrary noise spectrum. *Physical Review A*, 91(1), 2015. doi: 10.1103/PhysRevA.91.013825.

- [89] H. Cramér. *Mathematical Methods of Statistics*. Princeton University Press, 1946.
- [90] C. M. Caves. Quantum-mechanical noise in an interferometer. *Phys. Rev. D*, 23:1693, 1981.
- [91] V. Giovannetti et al. Classical capacity of the quantum bosonic channel with memory. *Phys. Rev. A*, 70:032315, 2004.
- [92] K. Jacobs and D. A. Steck. A straightforward introduction to continuous quantum measurement. *Contemp. Phys.*, 47:279, 2006.
- [93] M. Howard et al. Quantum dynamical simulation of many-body decoherence. *New J. Phys.*, 8:33, 2006.
- [94] A. Ishizaki and G. R. Fleming. Unified treatment of quantum coherent and incoherent hopping dynamics in electronic energy transfer: Reduced hierarchy equation approach. *J. Chem. Phys.*, 130:234111, 2009.
- [95] N. Gisin and I. C. Percival. The quantum-state diffusion model applied to open systems. *J. Phys. A: Math. Gen.*, 25:5677, 1992.
- [96] O. P. Saira et al. Environmentally induced decay of quantum correlations due to localization. *Phys. Rev. A*, 82:030102, 2010.
- [97] Sebastian Ecker, Johannes Pseiner, Jorge Piris, and Martin Bohmann. Advances in entanglement-based qkd for space applications. In *International Conference on Space Optics—ICSO 2022*, volume 12777, pages 925–945. SPIE, 2023.
- [98] Yuchen Guo and Shuo Yang. Noise effects on purity and quantum entanglement in terms of physical implementability. *npj Quantum Information*, 9(1):11, 2023.
- [99] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. 2010. This book provides a comprehensive introduction to quantum computing and communication, including discussions on decoherence and error correction.
- [100] Yanqiang Guo, Haifeng Li, Yingqi Wang, Xiangyu Meng, Tong Zhao, and Xiaomin Guo. Chaos with gaussian invariant distribution by quantum-noise random phase feedback. *Optics Express*, 31(19):31522–31532, 2023.
- [101] Vladyslav C. Usenko, Antonio Acín, Romain Alléaume, Ulrik L. Andersen, Eleni Diamanti, Tobias Gehring, Adnan A. E. Hajomer, Florian Kanitschar, Christoph Pacher, Stefano Pirandola, and Valerio Pruneri. Continuous-variable quantum communication, 2025. URL <https://arxiv.org/abs/2501.12801>.

- [102] Laszlo Gyongyosi and Sandor Imre. Superactivation of quantum channels is limited by the quantum relative entropy function, 2012. URL <https://arxiv.org/abs/1206.5691>.
- [103] Laszlo Bacsardi. On the way to quantum-based satellite communication. *IEEE Communications Magazine*, 51(8):50–55, 2013.
- [104] Michael A. Nielsen. Optical quantum computation using cluster states. *Phys. Rev. Lett.*, 93:040503, Jul 2004. doi: 10.1103/PhysRevLett.93.040503.
- [105] Pieter Kok, William J Munro, Kae Nemoto, Timothy C Ralph, Jonathan P Dowling, and Gerard J Milburn. Linear optical quantum computing with photonic qubits. *Reviews of modern physics*, 79(1):135–174, 2007.
- [106] Nathan K Langford. *Encoding, manipulating and measuring quantum information in optics*. PhD thesis, Citeseer, 2007.
- [107] J. Eisert and M. Plenio. Introduction to the basics of entanglement theory in continuous-variable systems. *International Journal of Quantum Information*, 1(04):479–506, 2003.
- [108] Richard Cleve and Harry Buhrman. Substituting quantum entanglement for communication. *Physical Review A*, 56:1201–1204, 1997. doi: 10.1103/PhysRevA.56.1201.
- [109] Alexander CB Greenwood, Larry TH Wu, Eric Y Zhu, Brian T Kirby, and Li Qian. Machine learning derived entanglement witnesses. *Physical Review Applied*, 19(3):034058, 2023.
- [110] Shahnawaz Ahmed, Carlos Sánchez Muñoz, Franco Nori, and Anton Frisk Kockum. Quantum state tomography with conditional generative adversarial networks. *Physical Review Letters*, 127:140502, 2021. doi: 10.1103/PhysRevLett.127.140502.
- [111] Xiaodie Lin, Zhenyu Chen, and Zhaohui Wei. Quantifying quantum entanglement via a hybrid quantum-classical machine learning framework. *Physical Review A*, 107:062409, 2023.
- [112] Juan Carrasquilla, Giacomo Torlai, Roger G Melko, et al. Reconstructing quantum states with generative models. *Nature Machine Intelligence*, 1:155–161, 2019. doi: 10.1038/s42256-019-0028-1.
- [113] Giacomo Torlai and Roger G. Melko. Neural decoder for topological codes. *Physical Review Letters*, 119(3):030501, 2018. doi: 10.1103/PhysRevLett.119.030501.
- [114] Giacomo Torlai, Christopher J. Wood, Atithi Acharya, et al. Quantum process tomography with unsupervised learning and tensor networks. *Nature Communications*, 14, 2023. doi: 10.1038/s41467-023-35800-2.

- [115] Mhlambululi Mafu. Advances in artificial intelligence and machine learning for quantum communication applications. *IET Quantum Communication*, 2024.
- [116] Haoran Liao, Derek S Wang, Iskandar Sitdikov, Ciro Salcedo, Alireza Seif, and Zlatko K Minev. Machine learning for practical quantum error mitigation. *arXiv preprint arXiv:2309.17368*, 2023.
- [117] Trung Q Duong, James Adu Ansere, Bhaskara Narottama, Vishal Sharma, Octavia A Dobre, and Hyundong Shin. Quantum-inspired machine learning for 6g: fundamentals, security, resource allocations, challenges, and future research directions. *IEEE Open Journal of Vehicular Technology*, 3:375–387, 2022.
- [118] Giuseppe Vallone, Davide Bacco, Daniele Dequal, Simone Gaiarin, Vincenza Luceri, Giuseppe Bianco, and Paolo Villoresi. Experimental satellite quantum communications. *Physical Review Letters*, 115(4):040502, 2015.
- [119] Julius Wallnöfer, Alexey A Melnikov, Wolfgang Dür, and Hans J Briegel. Machine learning for long-distance quantum communication. *PRX quantum*, 1(1):010301, 2020.
- [120] Christoph Simon. Towards a global quantum network. *Nature Photonics*, 11(11):678–680, 2017.
- [121] Sheng-Kai Liao, Wen-Qi Cai, Johannes Handsteiner, Bo Liu, Juan Yin, Liang Zhang, Dominik Rauch, Matthias Fink, Ji-Gang Ren, Wei-Yue Liu, et al. Satellite-relayed intercontinental quantum network. *Physical review letters*, 120(3):030501, 2018.
- [122] Ivan B Djordjevic. On global quantum communication networking. *Entropy*, 22(8):831, 2020.
- [123] Yaseera Ismail, Ilya Sinayskiy, and Francesco Petruccione. Integrating machine learning techniques in quantum communication to characterize the quantum channel. *JOSA B*, 36(3):B116–B121, 2019.
- [124] Sotirios P Chatzis, Dimitrios Korkinof, and Yiannis Demiris. A quantum-statistical approach toward robot learning by demonstration. *IEEE Transactions on Robotics*, 28(6):1371–1381, 2012.
- [125] Geoffrey J McLachlan and Thriyambakam Krishnan. *The EM algorithm and extensions*. John Wiley & Sons, 2007.
- [126] Kevin P Murphy. *Machine learning: a probabilistic perspective*. MIT press, 2012.
- [127] Ivan Djordjevic. *Quantum information processing and quantum error correction: an engineering approach*. Academic press, 2012.

- [128] V. Maz'ya and G. Schmidt. On approximate approximations using Gaussian kernels. *IMA J. Numer. Anal.*, 16:13–29, 1996.
- [129] D. Reynolds. Gaussian mixture models. In *Encyclopedia of Biometrics*. Springer, Boston, MA, 2015.
- [130] M. F. Huber, T. Bailey, H. Durrant-Whyte, and U. D. Hanebeck. On entropy approximation for Gaussian mixture random vectors. In *2008 IEEE International Conference on Multisensor Fusion and Integration for Intelligent Systems*, pages 181–188, Seoul, Korea (South), 2008. doi: 10.1109/MFI.2008.4648062.
- [131] Alexander I Lvovsky and Michael G Raymer. Continuous-variable optical quantum-state tomography. *Reviews of modern physics*, 81(1):299, 2009.
- [132] Jacob Biamonte, Peter Wittek, Nicola Pancotti, Patrick Rebentrost, Nathan Wiebe, and Seth Lloyd. Quantum machine learning. *Nature*, 549(7671):195–202, 2017.
- [133] Zdeněk Hradil, Jaroslav Řeháček, Jaromír Fiurášek, and Miroslav Ježek. 3 maximum-likelihood methods in quantum mechanics. *Quantum state estimation*, pages 59–112, 2004.
- [134] Vedran Dunjko and Hans J. Briegel. Machine learning & artificial intelligence in the quantum domain: a review of recent progress. *Reports on Progress in Physics*, 81(7):074001, 2018. doi: 10.1088/1361-6633/aab406.
- [135] Robert Bedington, Juan Miguel Arrazola, and Alexander Ling. Progress in satellite quantum key distribution. *npj Quantum Information*, 3(1):30, 2017.
- [136] Sumeet Khatri, Anthony J Brady, Renée A Desporte, Manon P Bart, and Jonathan P Dowling. Spooky action at a global distance: analysis of space-based entanglement distribution for the quantum internet. *npj Quantum Information*, 7(1):4, 2021.
- [137] Simon Fossier, Eleni Diamanti, Thierry Debuisschert, Rosa Tualle-Brouri, and Philippe Grangier. Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers. *Journal of Physics B: Atomic, Molecular and Optical Physics*, 42(11):114014, 2009.
- [138] Yang Li, Wen-Qi Cai, Ji-Gang Ren, Chao-Ze Wang, Meng Yang, Liang Zhang, Hui-Ying Wu, Liang Chang, Jin-Cai Wu, Biao Jin, Hua-Jian Xue, Xue-Jiao Li, Hui Liu, Guang-Wen Yu, Xue-Ying Tao, Ting Chen, Chong-Fei Liu, Wen-Bin Luo, Jie Zhou, Hai-Lin Yong, Yu-Huai Li, Feng-Zhi Li, Cong Jiang, Hao-Ze Chen, Chao Wu, Xin-Hai Tong, Si-Jiang Xie, Fei Zhou, Wei-Yue Liu, Nai-Le Liu, Li Li, Feihu

- Xu, Yuan Cao, Juan Yin, Rong Shu, Xiang-Bin Wang, Qiang Zhang, Jian-Yu Wang, Sheng-Kai Liao, Cheng-Zhi Peng, and Jian-Wei Pan. Microsatellite-based real-time quantum key distribution, 2024. URL <https://arxiv.org/abs/2408.10994>.
- [139] Alessio Serafini. *Quantum continuous variables: a primer of theoretical methods*. CRC press, 2017.
 - [140] Jérôme Lodewyck, Matthieu Bloch, Raúl García-Patrón, Simon Fossier, Evgueni Karpov, Eleni Diamanti, Thierry Debuisschert, Nicolas J Cerf, Rosa Tualle-Brouri, Steven W McLaughlin, et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Physical Review A*, 76(4):042305, 2007.
 - [141] Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, Liang Zhang, Yang Li, Ji-Gang Ren, Juan Yin, Qi Shen, Yuan Cao, Zheng-Ping Li, et al. Satellite-to-ground quantum key distribution. *Nature*, 549(7670):43–47, 2017.
 - [142] L Moli-Sanchez, A Rodriguez-Alonso, and Gonzalo Seco-Granados. Performance analysis of quantum cryptography protocols in optical earth-satellite and intersatellite links. *IEEE Journal on Selected Areas in Communications*, 27(9):1582–1590, 2009.
 - [143] Jasminder S Sidhu, Thomas Brougham, Duncan McArthur, Roberto G Pousa, and Daniel KL Oi. Finite key effects in satellite quantum key distribution. *npj Quantum Information*, 8(1):18, 2022.
 - [144] Najme Ahmadi, Sven Schwertfeger, Philipp Werner, Lukas Wiese, Joseph Lester, Elisa Da Ros, Josefine Krause, Sebastian Ritter, Mostafa Abasifard, Chanaprom Cholsuk, et al. Quick 3⁺-design of a satellite-based quantum light source for quantum communication and extended physical theory tests in space. *Advanced Quantum Technologies*, 7(4):2300343, 2024.
 - [145] Thang V Nguyen, Hoa T Le, Hien TT Pham, Vuong Mai, and Ngoc T Dang. Enhancing design and performance analysis of satellite entanglement-based cv-qkd/fso systems. *IEEE Access*, 2023.
 - [146] Richard J Hughes, William T Buttler, Paul G Kwiat, SK Lamoreuax, GL Morgan, Jane E Nordholt, and Charles G Peterson. Quantum cryptography for secure satellite communications. In *2000 IEEE Aerospace Conference. Proceedings (Cat. No. 00TH8484)*, volume 1, pages 191–200. IEEE, 2000.
 - [147] JD Barry and GS Mecherle. Beam pointing error as a significant design parameter for satellite-borne, free-space optical communication systems. *Optical Engineering*, 24(6):1049–1054, 1985.

- [148] Dirk Giggenbach and Amita Shrestha. Atmospheric absorption and scattering impact on optical satellite-ground links. *International Journal of Satellite Communications and Networking*, 40(2):157–176, 2022.
- [149] Aleksandr Khmelev, Alexey Duplinsky, Ruslan Bakhshaliev, Egor Ivchenko, Liubov Pismeniuk, Vladimir Mayboroda, Ivan Nesterov, Arkadiy Chernov, Anton Trushechkin, Evgeniy Kiktenko, et al. Eurasian-scale experimental satellite-based quantum key distribution with detector efficiency mismatch analysis. *Optics Express*, 32(7):11964–11978, 2024.
- [150] JP Bourgoin, Evan Meyer-Scott, Brendon L Higgins, B Helou, Chris Erven, Hannes Huebel, B Kumar, D Hudson, Ian D’Souza, Ralph Girard, et al. A comprehensive design and performance analysis of low earth orbit satellite quantum communication. *New Journal of Physics*, 15(2):023006, 2013.
- [151] Gunes Karabulut Kurt, Mohammad G Khoshkholgh, Safwan Alfatani, Ahmed Ibrahim, Tasneem SJ Darwish, Md Sahabul Alam, Halim Yanikomeroglu, and Abbas Yongacoglu. A vision and framework for the high altitude platform station (haps) networks of the future. *IEEE Communications Surveys & Tutorials*, 23(2):729–779, 2021.
- [152] Nilesh Maharjan, Nikesh Devkota, and Byung Wook Kim. Atmospheric effects on satellite-ground free space uplink and downlink optical transmissions. *Applied Sciences*, 12(21):10944, 2022.
- [153] Nedasadat Hosseinidehaj and Robert Malaney. Quantum key distribution over combined atmospheric fading channels. In *2015 IEEE International Conference on Communications (ICC)*, pages 7413–7419. IEEE, 2015.
- [154] LC Andrews, RL Phillips, and PT Yu. Optical scintillations and fade statistics for a satellite-communication system. *applied optics*, 34(33):7742–7751, 1995.
- [155] Mario Mastriani and Sundaraja Sitharama Iyengar. Satellite quantum repeaters for a quantum internet. *Quantum Engineering*, 2(4):e55, 2020.
- [156] Mark Dmytryszyn, Matthew Crook, and Timothy Sands. Lasers for satellite uplinks and downlinks. *Sci*, 3(1):4, 2021.
- [157] Xueying Zhang, Yichen Zhang, Yijia Zhao, Xiangyu Wang, Song Yu, and Hong Guo. Finite-size analysis of continuous-variable measurement-device-independent quantum key distribution. *Physical Review A*, 96(4):042334, 2017.

- [158] Agoston Schranz, Eszter Udvary, Balazs Matolcsy, Laszlo Bacsardi, and Andras Nagy. A portable ambient optical noise measurement station. In *2023 23rd International Conference on Transparent Optical Networks (ICTON)*, pages 1–6, 2023.
- [159] András Mihály and László Bacsárdi. Effects of selected noises on the quantum memory satellite based quantum repeaters. *Infocommunications Journal*, 13(2):19–24, 2021.
- [160] Junsang Oh, Jeongsik Cho, and June-Koo Kevin Rhee. Continuous-variable quantum key distribution with time-division dual-quadrature homodyne detection. *Optics Express*, 31(19):30669–30681, 2023.
- [161] Ivan B. Djordjevic. Hybrid cv-dv quantum communications and quantum networks. *IEEE Access*, 10:23284–23292, 2022. doi: 10.1109/ACCESS.2022.3154468.
- [162] Marcos Curty, Feihu Xu, Wei Cui, Charles Ci Wen Lim, Kiyoshi Tamaki, and Hoi-Kwong Lo. Finite-key analysis for measurement-device-independent quantum key distribution. *Nature communications*, 5(1):3732, 2014.
- [163] Tanvirul Islam, Jasminder S Sidhu, Brendon L Higgins, Thomas Brougham, Tom Vergoossen, Daniel KL Oi, Thomas Jennewein, and Alexander Ling. Finite-resource performance of small-satellite-based quantum-key-distribution missions. *PRX Quantum*, 5(3):030101, 2024.
- [164] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications. *Nature communications*, 8(1):15043, 2017.
- [165] Dongkuan Xu and Yingjie Tian. A comprehensive survey of clustering algorithms. *Annals of data science*, 2(2):165–193, 2015.
- [166] Rui Xu and D. Wunsch. Survey of clustering algorithms. *IEEE Transactions on Neural Networks*, 16(3):645–678, 2005. doi: 10.1109/TNN.2005.845141.
- [167] Weiming Wei, Chunming Tang, and Yucheng Chen. Efficient privacy-preserving k-means clustering from secret-sharing-based secure three-party computation. *Entropy*, 24(8):1145, 2022.
- [168] Nicolò Bonaldi, Martina Rossi, Daniele Mattioli, Michele Grapulin, Blanca Silva Fernández, Davide Caputo, Marco Magagnini, Arianna Osti, and Fabio Veronese. Boost clustering with gaussian boson sampling: a quantum-classical hybrid approach. *Quantum Machine Intelligence*, 6(2):65, 2024.

- [169] Yanni Ou, Emilio Hugues-Salas, Foteini Ntavou, Rui Wang, Yu Bi, SY Yan, George Kanellos, Reza Nejabati, and Dimitra Simeonidou. Field-trial of machine learning-assisted quantum key distribution (qkd) networking with sdn. In *2018 European Conference on Optical Communication (ECOC)*, pages 1–3. IEEE, 2018.
- [170] Yuan Cao, Yongli Zhao, Rui Lin, Xiaosong Yu, Jie Zhang, and Jiajia Chen. Multi-tenant secret-key assignment over quantum key distribution networks. *Opt. Express*, 27(3):2544–2561, Feb 2019. doi: 10.1364/OE.27.002544. URL <https://opg.optica.org/oe/abstract.cfm?URI=oe-27-3-2544>.
- [171] Yuan Cao, Yongli Zhao, Jun Li, Rui Lin, Jie Zhang, and Jiajia Chen. Reinforcement learning based multi-tenant secret-key assignment for quantum key distribution networks. In *2019 Optical Fiber Communications Conference and Exhibition (OFC)*, pages 1–3. IEEE, 2019.
- [172] Purva Sharma, Shubham Gupta, Vimal Bhatia, and Shashi Prakash. Deep reinforcement learning-based routing and resource assignment in quantum key distribution-secured optical networks. *IET Quantum Communication*, 4(3):136–145, 2023.
- [173] Ben Buchler, Jesse Everett, Young-Wook Cho, Aaron Tranter, Harry Slatyer, Michael Hush, Karun Paul, Pierre Vernaz-Gris, Anthony Leung, Daniel Higginbottom, et al. Stopped and stationary light with cold atomic ensembles and machine learning. In *CLEO: QELS_Fundamental Science*, pages FM1G–5. Optica Publishing Group, 2018.
- [174] Sumeet Khatri. Policies for elementary links in a quantum network. *Quantum*, 5:537, 2021.
- [175] Juan Yin, Ji-Gang Ren, He Lu, Yuan Cao, Hai-Lin Yong, Yu-Ping Wu, Chang Liu, Sheng-Kai Liao, Fei Zhou, Yan Jiang, et al. Quantum teleportation and entanglement distribution over 100-kilometre free-space channels. *Nature*, 488(7410):185–188, 2012.
- [176] Simon D Reiß and Peter van Loock. Deep reinforcement learning for key distribution based on quantum repeaters. *Physical Review A*, 108(1):012406, 2023.
- [177] Ye Dong, Xiaojun Chen, Liyan Shen, and Dakui Wang. Privacy-preserving distributed machine learning based on secret sharing. In *Information and Communications Security: 21st International Conference, ICICS 2019, Beijing, China, December 15–17, 2019, Revised Selected Papers 21*, pages 684–702. Springer, 2020.
- [178] Weiming Wei, Chunming Tang, and Yucheng Chen. Efficient privacy-preserving k-means clustering from secret-sharing-based secure three-party computation. *Entropy*, 24(8):1145, 2022.

- [179] Sirui Lu, Shilin Huang, Keren Li, Jun Li, Jianxin Chen, Dawei Lu, Zhengfeng Ji, Yi Shen, Duanlu Zhou, and Bei Zeng. Separability-entanglement classifier via machine learning. *Physical Review A*, 98(1):012315, 2018.
- [180] Yiwei Chen, Yu Pan, Guofeng Zhang, and Shuming Cheng. Detecting quantum entanglement with unsupervised learning. *Quantum Science and Technology*, 7(1):015005, 2021.
- [181] Naema Asif, Uman Khalid, Awais Khan, Trung Q Duong, and Hyundong Shin. Entanglement detection with artificial neural networks. *Scientific Reports*, 13(1):1562, 2023.
- [182] Julius Walln fer, Alexey A Melnikov, Wolfgang D r, and Hans J Briegel. Machine learning for long-distance quantum communication. *PRX quantum*, 1(1):010301, 2020.
- [183] Hui Zhang, Lingxiao Wan, Tobias Haug, Wai-Keong Mok, Stefano Paesani, Yuzhi Shi, Hong Cai, Lip Ket Chin, Muhammad Faeyz Karim, Limin Xiao, et al. Resource-efficient high-dimensional subspace teleportation with a quantum autoencoder. *Science advances*, 8(40):eabn9783, 2022.
- [184] Jiaye Xu, Yun Mao, Yuxin Chen, Xiaowen Xu, and Ying Guo. Machine learning assisted prediction for free-space continuous variable quantum teleportation. *IEEE Photonics Journal*, 14(4):1–7, 2022.
- [185] Fr d ric Grosshans and Philippe Grangier. Reverse reconciliation protocols for quantum cryptography with continuous variables. e-print. *arXiv preprint quant-ph/0204127*, pages 1–0204127.
- [186] R. J. Glauber. *Phys. Rev.*, 121:2766, 1963.
- [187] P. Giorda and M. Allegra. Gaussian states in quantum information: a survey. *EJTP*, 10:165–178, 2013. URL <https://ejtp.com/articles/ejtpv10i29p165.pdf>.
- [188] C. Weedbrook et al. Gaussian quantum information. *Rev. Mod. Phys.*, 84:621, 2012. doi: 10.1103/RevModPhys.84.621.
- [189] Y. Miwa et al. Exploring a new regime for processing optical qubits: squeezing and unsqueezing single photons. *Phys. Rev. Lett.*, 113:013601, 2014. doi: 10.1103/PhysRevLett.113.013601.
- [190] T. Eberle et al. Quantum enhancement of the zero-area Sagnac interferometer topology for gravitational wave detection. *Phys. Rev. Lett.*, 104:251102, 2010. doi: 10.1103/PhysRevLett.104.251102.
- [191] S. L. Braunstein and P. van Loock. Quantum information with continuous variables. *Rev. Mod. Phys.*, 77:513, 2005. doi: 10.1103/RevModPhys.77.513.

- [192] U. L. Andersen et al. 30 years of squeezed light generation. *Phys. Scripta*, 91:053001, 2016. doi: 10.1088/0031-8949/91/5/053001.
- [193] B. Demoen, P. Vanheuverzwijn, and A. Verbeure. Completely positive maps on ccr-algebra. *Letters in Mathematical Physics*, 2(2):161–166, 1977.
- [194] A. S. Holevo, M. Sohma, and O. Hirota. Capacity of quantum Gaussian channels. *Physical Review A*, 59(3):1820, 1999.
- [195] A. S. Holevo and R. F. Werner. Evaluating capacities of bosonic Gaussian channels. *Physical Review A*, 63(3):032312, 2001.
- [196] J. Eisert and M. B. Plenio. Conditions for the local manipulation of Gaussian states. *Physical Review Letters*, 89(9):097901, 2002.
- [197] G. Lindblad. Cloning the quantum oscillator. *Journal of Physics A: Mathematical and General*, 33(28):5059, 2000.
- [198] Jens Eisert and Michael M Wolf. Gaussian quantum channels. *arXiv preprint quant-ph/0505151*, 2005.
- [199] Steven Weinberg. “*The quantum theory of fields*”, volume 2. Cambridge University Press, Cambridge, United Kingdom, 1995.
- [200] Alexander S Holevo. “*Statistical structure of quantum theory*”, volume 67. Springer Science & Business Media, Springer Berlin, Heidelberg, Germany, 2003.
- [201] Umut Orguner. Notes on differential entropy calculation using particles. Technical report, Linköping University Electronic Press, 2008.
- [202] Glenn F Knoll. *Radiation detection and measurement*. John Wiley & Sons, 2010.
- [203] Zihao Li, Xiaolin Zhou, Chengrui Wan, Gang Du, and Yuequan Wang. A poisson shot noise limited mmse precoding for photon-counting mimo systems with reinforcement learning. *Applied Sciences*, 13(19):10855, 2023.
- [204] Ying Chen, Xiaolin Zhou, Jian Wang, Zhichao Dong, and Yongkang Chen. On weighted sum rate of multi-user photon-counting multiple-input multiple-output visible light communication systems under poisson shot noise. *Applied Sciences*, 14(4):1423, 2024.
- [205] Douglas A Reynolds et al. Gaussian mixture models. *Encyclopedia of biometrics*, 741(659-663), 2009.
- [206] Stefania Castelletto, Ivo P Degiovanni, and MARIA LUISA Rastello. Quantum and classical noise in practical quantum-cryptography systems based on polarization-entangled photons. *Physical Review A*, 67(2):022305, 2003.

- [207] H. Paul. Photon antibunching. *Rev. Mod. Phys.*, 54:1061, 1982.
- [208] D Renker and E Lorenz. Advances in solid state photon detectors. *Journal of Instrumentation*, 4(04):P04004, 2009.
- [209] Electra Eleftheriadou, Stephen M Barnett, and John Jeffers. Quantum optical state comparison amplifier. *Physical Review Letters*, 111(21):213601, 2013.
- [210] Li Liu, Yukun Wang, Emilien Lavie, Chao Wang, Arno Ricou, Fen Zhuo Guo, and Charles Ci Wen Lim. Practical quantum key distribution with non-phase-randomized coherent states. *Physical Review Applied*, 12:024048, 2019.
- [211] Arthur P Dempster, Nan M Laird, and Donald B Rubin. Maximum likelihood from incomplete data via the EM algorithm. *Journal of the Royal Statistical Society: Series B (methodological)*, 39(1):1–22, 1977.
- [212] CF Jeff Wu. On the convergence properties of the EM algorithm. *The Annals of statistics*, pages 95–103, 1983.
- [213] Rafael Coimbra Pinto and Paulo Martins Engel. A fast incremental gaussian mixture model. *PLOS ONE*, 10(10):1–12, 10 2015. doi: 10.1371/journal.pone.0139931. URL <https://doi.org/10.1371/journal.pone.0139931>.
- [214] Amos Lapidoth and Shlomo Shamai. Fading channels: how perfect need "perfect side information" be? *IEEE Transactions on Information Theory*, 48(5):1118–1134, 2002.
- [215] Vladlen Galetsky and Manfred Niehus. Leo small satellite qkd downlink performance: Quantsat-pt case study. *arXiv preprint arXiv:2209.10293*, 2022.
- [216] V Marulanda Acosta, Daniele Dequal, Matteo Schiavon, Aurélie Montmerle-Bonnefois, Caroline B Lim, Jean-Marc Conan, and Eleni Diamanti. Analysis of satellite-to-ground quantum key distribution with adaptive optics. *New Journal of Physics*, 26(2):023039, 2024.
- [217] Nguyen Thanh Son and Tatjana Stykel. Symplectic eigenvalues of positive-semidefinite matrices and the trace minimization theorem. *arXiv preprint arXiv:2208.05291*, 2022.
- [218] Jasmininder S Sidhu, Thomas Brougham, Duncan McArthur, Roberto G Pousa, and Daniel KL Oi. Finite key performance of satellite quantum key distribution under practical constraints. *Communications Physics*, 6(1):210, 2023.
- [219] Kyungjoo Noh, Stefano Pirandola, and Liang Jiang. Enhanced energy-constrained quantum communication over bosonic Gaussian channels. *Nature communications*, 11(1):457, 2020.

- [220] Ivan Derkach and Vladyslav Usenko. Applicability of continuous-variable quantum key distribution over satellite links. In *International Conference on Space Optics—ICSO 2022*, volume 12777, pages 1089–1103. SPIE, 2023.
- [221] Ivan Derkach and Vladyslav C Usenko. Applicability of squeezed- and coherent-state continuous-variable quantum key distribution over satellite links. *Entropy*, 23(1):55, 2020.
- [222] Giuseppe Vallone, Davide Bacco, Daniele Dequal, Simone Gaiarin, Vincenza Luceri, Giuseppe Bianco, and Paolo Villoresi. Experimental satellite quantum communications. *Physical Review Letters*, 115(4):040502, 2015.
- [223] Dah-Jing Jwo, Ta-Shun Cho, and Amita Biswal. Geometric insights into the multivariate Gaussian distribution and its entropy and mutual information. *Entropy*, 25(8):1177, 2023.