Data Processing in Continuous-Variable Quantum Key Distribution Under Composable Finite-Size Security

Alexander George Mountogiannakis

Doctor of Philosophy

University of York

Computer Science

August 2023

Abstract

Continuous-variable quantum key distribution (CV-QKD) uses amplitude and phase modulation of light, in order to establish secure communications between two remote parties. The laws of quantum mechanics ensure the theoretical security of the protocol, in spite of the noise and losses of the communication channel. In practice, however, the resulting secret key rate depends not only on these two factors, but also on a series of data-processing steps, needed for transforming shared correlations into a final secret binary string.

In this work, we investigate the operation of three Gaussian-modulated coherent-state (GMCS) CV-QKD protocols: the homodyne detection, heterodyne detection and the continuous-variable measurement-device-independent (CV-MDI) protocol. We propose a comprehensive strategy covering their entire course, starting from the preparation and transmission of quantum states, until the extraction of a shared secret key. We also provide rigorous security proofs, considering optimal eavesdropper strategies and incorporating the composable framework under finite-size effects, which offers the highest level of security. In addition, we present results, where we explore the performance of different quantities of interest in the high signal-to-noise regime and identify intervals of parameters, where communications are regarded as secure. This is achieved under the assistance of our self-developed open-source Python library, which we use to simulate the stage of quantum communications and, afterwards, to process the resulting data via the stages of parameter estimation, information reconciliation and privacy amplification. Here, short-range communications are of particular interest. To enhance data processing in this high signal-to-noise ratio setting, we have combined an appropriate data preprocessing scheme with the use of high-rate, non-binary low-density parity-check (LDPC) codes. This allows us to examine the performance of short-range CV-QKD in practical implementations and optimize the parameters connected to the aforementioned steps.

Contents

Acknowledgements

First and foremost, I would like to thank my supervisor, Prof. Stefano Pirandola, for his guidance, eagerness and for the constant communication in every step of the PhD. His wisdom and experience were what sculpted this topic and brought the thesis where it is today.

In addition, the help from Dr. Panagiotis Papanastasiou has been invaluable. Panagiotis was ever-present, even when circumstances were dire. This thesis would have been impossible without him.

Declaration of Authorship

I, Alexander George Mountogiannakis , declare that the thesis titled *Data Processing in Continuous-Variable Quantum Key Distribution Under Composable Finite-Size Security* and the work presented in the thesis are both my own, and have been generated by me as the result of my own original research. I confirm that:

- this work was wholly done during my research degree at this University;
- this work has not previously been presented for a degree or other qualification at this University or elsewhere;
- where I have consulted the published work of others, this is always attributed;
- where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work;
- all sources are acknowledged as references;
- parts of this work have been published as:
  - A. G. Mountogiannakis, P. Papanastasiou, B. Braverman, and S. Pirandola, "Composably secure data processing for Gaussian-modulated continuous-variable quantum key distribution," *Phys. Rev. Research*, vol. 4, p. 013099, 2022.
  - A. G. Mountogiannakis, P. Papanastasiou, and S. Pirandola, "Data post-processing for the one-way heterodyne protocol under composable finite-size security," *Phys. Rev. A*, vol. 106, p. 042606, 2022.
  - P. Papanastasiou, A. G. Mountogiannakis, and S. Pirandola, "Composable security of CV-MDI-QKD with secret key rate and data processing," *Sci. Rep.*, vol. 13, p. 11636, 2023.

Preface

The world faces a growing threat from quantum computers, which will render current encryption methods obsolete. In response to this urgent need for security, quantum key distribution (QKD) has emerged as a promising solution. QKD offers an unbreakable cryptographic framework, that is immune to attacks from quantum computers. This is because the security is derived from the principles of quantum mechanics, instead of relying solely on mathematical complexity. As quantum computing advances, QKD is poised to play a vital role in ensuring secure communications in a post-quantum era, ushering the new age of quantum-safe cryptography.

Over the last twenty years, a new family of QKD protocols based on continuous-variable systems has arisen. Such protocols, named continuous-variable quantum key distribution protocols (CV-QKD), typically utilize Gaussian modulation and coherent states for the encoding of information. Security in CV-QKD has been proven in the asymptotic, finite-size effect and composable regime. Therefore, it has become an appealing competitor for securing future communications. As this field is relatively new, a great deal of research has yet to be carried out. The composable framework is particularly interesting, because it provides maximum security by considering all imperfections of a practical implementation. For this reason, it is the main focus of this work.

The first four literature chapters make an effort to briefly explain every notion, that will be subsequently used in the research part. This way, even complete beginners, who would like to take up the field of QKD, can begin their journey. Some basic knowledge of quantum mechanics, linear algebra, statistics and probabilities is still required to fully comprehend the content of the chapters. For the readers already acquainted with the topic, the data-processing part offers a thorough tour of all stages of CV-QKD, while the produced results determine its full potential, when higher security thresholds are considered. The proposed data processing techniques enable interested parties to adopt similar procedures in their work or to improve the current ones.

Because of the multidisciplinary nature of the subject, the dissertation contains an unprecedented number of distinct variables. Every effort has been made to meticulously differentiate all notations. In most cases, the notations follow mathematical conventions. For example, the matrices (but not the vectors) are represented by boldface, while

spaces, fields, sets and distributions are denoted by calligraphic letters. Furthermore, the quantum mechanical operators bear the hat ($\hat{\cdot}$) symbol and any estimators or guesses are presented the wide hat ($\widehat{\cdot}$). However, the large amount of variables also necessitates a handful of unusual methods for their definition, such as using the 'blackboard bold' style for statistical measures. All in all, special attention must be given to the notation of variables, when reading this work. It is important to note that up to the research part, all canonical commutation relations and their derivatives are presented in SI units. Beyond this point, units are given in terms of the shot noise.

List of Figures

List of Tables

Nomenclature

α	Phase-Space Cut-Off / Coherent State Eigenvalue
β	Reconciliation Efficiency
$\boldsymbol{x}$	Alice's Concatenated Variable
$\boldsymbol{y}$	Bob's Concatenated Variable
χ	Holevo Bound
Δ	Composable Framework Distance
δ	Lattice Step in Phase Space
Δ_{AEP}	Asymptotic Equipartition Property Distance
ℓ	Secret Key Length
η	Setup Efficiency
γ	CV-MDI Relay Output
$\hat{\mathsf{H}}$	Hamiltonian Operator
$\hat{\mathsf{n}}$	Photon Number Operator
$\hat{\rho}$	Density Operator
$\hat{a}$	Annihilation Operator
$\hat{D}$	Displacement Operator
$\hat{P}$	P-Quadrature Operator
$\hat{p}$	Momentum Operator
$\hat{Q}$	Q-Quadrature Operator
$\hat{r}$	Canonical Operators
$\hat{U}$	Phase-Shifting Operator

$\hat{x}$	Position Operator
$\hbar$	Reduced Planck Constant
κ	Field Mode
λ	Eigenvalue
$\mathbb{C}$	Covariance
$\mathbb{E}$	Expected Value
$\mathbb{V}$	Variance
$\mathbf{\Omega}$	Symplectic Matrix
$\mathbf{\Pi}$	Partial Measurement Matrix
$\mathbf{\Sigma}$	Covariance Matrix
$\mathbf{A}$	Alice's Mode Matrix
$\mathbf{B}$	Bob's Mode Matrix
$\mathbf{C}$	Correlation Matrix
$\mathbf{D}$	Circulant Matrix
$\mathbf{G}$	Eve's Correlation Matrix in CV-MDI
$\mathbf{H}$	Parity Check Matrix
$\mathbf{I}$	Identity Matrix
$\mathbf{O}$	Zero Matrix
$\mathbf{S}$	Symplectic Matrix
$\mathbf{T}$	Toeplitz Matrix
$\mathbf{U}$	Modified Toeplitz Matrix
$\mathbf{V}$	(Two-Mode) Gaussian State Covariance Matrix
$\mathbf{Z}$	Z Pauli Matrix
$\mathcal{A}$	Alphabet
$\mathcal{B}$	ε-ball
$\mathcal{C}$	Set of Complex Numbers
$\mathcal{F}$	Family of Two-Universal Hash Functions

$\mathcal{GF}$	Galois Field
$\mathcal{G}$	Gaussian (Normal) Distribution
$\mathcal{H}$	Hilbert Space
$\mathcal{N}$	Set of Natural Numbers
$\mathcal{P}$	Poisson Distribution
$\mathcal{R}$	Set of Real Numbers
$\mathcal{U}$	Uniform Distribution
$\mathcal{W}$	Wigner Quasiprobability Distribution
$\mathcal{X}$	Set of Possible Outcomes of X
$\mathcal{Y}$	Set of Possible Outcomes of Y
$\mathcal{Z}$	Set of Integers
$\mathscr{F}$	Fourier Transform
B	Magnetic Field
c	Speed of Light
E	Electric Field
e	Energy
f	Frequency
m	Mass
n	Photon
T	Kinetic Energy
t	Time
V	Potential Energy
μ	Signal Variance
ν	Dimension
ω	Thermal Noise
ϕ	Bidirectional Mapping
π	Pi Constant

ψ	Quantum System State Vector
ρ	Quantum State
Σ	Global Symplectic Invariant
σ	Standard Deviation
τ	Square-Root Transmissivity
det	Determinant
diag	Matrix diagonal
erf	Error Function
FER	Frame Error Rate
iter_{max}	Maximum Number of Error-Correcting Iterations
leak_{EC}	Information Leakage
SNR	Signal-to-Noise Ratio
tr	Trace
Θ	Composable Key Rate Penalty Term
θ	Angle
$\tilde{n}$	Privacy Amplification Input String Length
α	Alice's Outcome in CV-MDI
β	Bob's Outcome in CV-MDI
χ	Equivalent Noise
γ	CV-MDI Relay Output
ω	Angular Frequency
Υ	Final Secret Key
υ	CV-MDI Regression Coefficient
υ_{el}	Electronic Noise
ε	Epsilon Security
ε_{cor}	Correctness Error
ε_{ent}	Entropy Estimation Penalty

$\varepsilon_{\mathrm{PE}}$	Parameter Estimation Error
$\varepsilon_{\mathrm{sec}}$	Secrecy Parameter
ε_h	Hashing Parameter
ε_s	Smoothing Parameter
φ	Characteristic Function
ϱ	Reflectivity
ϑ	Fiber Attenuation
$\widehat{\mathbb{C}}$	Covariance Estimator
$\widehat{\Xi}$	Maximum-Likelihood Excess Noise Variance Estimator
$\widehat{\xi}$	Maximum-Likelihood Excess Noise Estimator
$\widehat{H}$	Entropy Estimator
$\widehat{T}$	Maximum-Likelihood Transmissivity Estimator
Ξ	Excess Noise Variance
ξ	Excess Noise
Ξ_M	Worst-Case Excess Noise Variance Estimator
ξ_M	Worst-Case Excess Noise Estimator
ζ	Quadrature Variable Coordinate
A	Alice's Mode
a	Alice's Mode
B	Bob's Mode
b	Bob's Mode
C	Channel Capacity
c	Correlation Mode
D	Trace Distance
d	Bottom Digits
E	Eve's Mode
e	Euler's Constant / Eve's Mode

F	Fidelity
f	Function
G	Bosonic Entropic Function
g	CV-MDI Correlation Parameter
H	Shannon Entropy
h	Hash Function
$H_{\min}$	Min-Entropy
$H_{\min}^{\varepsilon_s}$	Smooth Min-Entropy
I	Mutual Information
i	Imaginary Unit / Index
J	Discretization Interval Border Point
j	Secondary Index
K	Bob's Discretized Variable
k	Discretized Symbol
L	Channel Length
l	LDPC Number of Rows
M	Number of Parameter Estimation Runs
m	Parameter Estimation States Per Block
N	Number of States Per Block
n	Key Generation States Per Block
n_{bks}	Number of Blocks
O	Big O
P	Momentum Quadrature Component
p	Probability / Discretization Variable
p_{EC}	Error Correction Success Probability
Q	Position Quadrature Component
q	Most Important Bits

R	Composable Secret Key Rate
r	Canonical Operator Eigenvalues
R_M^{EC}	Finite-Size Secret Key Rate
R_{asy}	Asymptotic Secret Key Rate
R_{code}	Code Rate
R_M	Secret Key Rate After Parameter Estimation
S	Von Neumann Entropy
T	Channel Transmissivity
t	Length of Hash in Verification
T_M	Worst-Case Transmissivity Estimator
U	Unitary Transformation
u	Uniform Random Integer in Verification
V	Vacuum Noise
v	Symplectic Eigenvalue
W	Parameter Estimation Interval Set
w_{c}	LDPC Column Weight
w_{r}	LDPC Row Weight
X	Generic Variable / Alice's Normalized Variable
x	Generic Variable
Y	Generic Variable / Bob's Normalized Variable
y	Generic Variable
Z	Generic Variable
z	Gaussian Noise Variable

Chapter 1

Quantum Optics

Before delving into quantum key distribution, it is important to have an overview of the notions, that compose its physical foundation. Introduced in this chapter are terms, such as coherent states, quadratures, beam splitters and homodyne detection, which are paramount for the understanding of future sections.

1.1 Quantization of the Free Electromagnetic Field

During the 1860s, James Clerk Maxwell developed a unified theory for electricity and magnetism, formerly thought as separate forces. He achieved that by assembling four laws, which collectively constitute Maxwell's equations. These equations compose the foundations of every theory stated in classical electromagnetism and provide a comprehensive framework for understanding electromagnetic phenomena. The four laws are:

- **Gauss's Law**: Electric charges produce an electric field. The electric flux across a closed surface is proportional to the enclosed charge.
- **Gauss's Law for magnetism**: No single magnetic pole, or monopole, exists in electric charges. The magnetic field of a material always exists as a pair of attractive and repulsive poles, called a dipole. The magnetic flux across a closed surface is zero.
- **Faraday's Law**: Magnetic fields produce an electric field. Varying magnetic flux generates an electromotive force, resulting in the circulation of an electric field along a closed loop.
- **Ampère's Law**: Electric currents produce a magnetic field, whose direction depends on the direction of the current. Maxwell amended this law to add that time-varying electric fields also produce a magnetic field.

For an electric field E and a magnetic field B in free space, all charges and currents disappear, because their density is zero. As a result, Maxwell's equations in a vacuum are shaped in their differential form as follows:

$$\nabla \cdot \mathsf{E} = 0 \tag{1.1}$$

$$\nabla \cdot \mathsf{B} = 0 \tag{1.2}$$

$$\nabla \times \mathsf{E} = -\frac{1}{\mathsf{c}} \frac{\partial \mathsf{B}}{\partial \mathsf{t}} \tag{1.3}$$

$$\nabla \times \mathsf{B} = \frac{1}{\mathsf{c}} \frac{\partial \mathsf{E}}{\partial \mathsf{t}} \tag{1.4}$$

Here, c is the speed of light. The equations present a symmetry $(\mathsf{E}, \mathsf{B}) \rightarrow (\mathsf{B}, -\mathsf{E})$, which is known as electromagnetic duality.

There exist two theoretical descriptions for the electromagnetic field. The classical point of view depicts it as a smooth, continuous field, where propagation resembles a wavelike behavior. Quantum field theory portrays the field as quantized, meaning it consists of individual particles. Specifically, these particles are photons, which are bosons without mass, but with a well-defined energy, momentum and spin. Their carried energy is

$$\mathsf{e} = \hbar\omega \tag{1.5}$$

where ω symbolizes the angular frequency and $\hbar$ denotes the reduced Planck constant. The physical traits of the particle are embodied into a quantum state $|\psi\rangle$. If a trait can be measured, it is referred to as an observable. Every observable is associated with an operator, which is a linear map acting on a Hilbert space $\mathcal{H}$. The act of a certain measurement assigns the eigenvalues of an operator to the physical properties. A prominent example is that of the photon number operator $\hat{\mathsf{n}}$, which counts the total number of photons n in the field.

The total energy of a quantum system can be identified from the eigenvalues of the Hamiltonian operator. In the context of a quantum harmonic oscillator, the quantum-mechanical formulation of the Hamiltonian is

$$\hat{\mathsf{H}} = \mathsf{T}(\hat{p}) + \mathsf{V}(\hat{x}) = \frac{\hat{p}^2}{2\mathsf{m}} + \frac{1}{2}\mathsf{m}\omega^2\hat{x}^2 \tag{1.6}$$

where, in accordance with classical mechanics, the equalities consist of the kinetic energy T and the potential energy V. The two operators, $\hat{x}$ and $\hat{p}$, capture the position and momentum respectively and are canonical conjugate quantities. Finally, m is the mass. An energy eigenstate of a photon number operator $\hat{\mathsf{n}}$ is the eigenstate of the Hamiltonian. Given the Hamiltonian $\hat{\mathsf{H}}$ and a definite number of photons $\mathsf{n} \in \mathcal{N}$, the equality

$$\hat{\mathsf{H}} |\mathsf{n}\rangle = \lambda_{\mathsf{n}} |\mathsf{n}\rangle \tag{1.7}$$

holds. Because of the Hamiltonian being Hermitian, the energy is always a real number.

1.2 Ladder Operators

The quantum counterpart of the harmonic oscillator acts as an approximate solution to nearly every system with a minimum of potential energy. In order to obtain the eigenvalues and eigenfunction of the quantum harmonic oscillator, it is necessary to solve the time-independent Schrödinger equation

$$\mathsf{e}\psi(x) = -\frac{\hbar^2}{2\mathsf{m}}\frac{\partial^2\psi(x)}{\partial x^2} + \mathsf{V}(x)\psi(x) \tag{1.8}$$

Here, ψ is the state vector that describes the quantum system. After its solution, the eigenvalues for the quantum harmonic oscillator are determined by

$$\lambda_{\mathsf{n}} = \frac{2\mathsf{n}+1}{2}\hbar\omega \tag{1.9}$$

Apart from directly solving Eq. (1.8), there exists an alternative way to obtain the energy eigenvalues. This technique is commonly referred to as the ladder operator method. Combining Eq. (1.7) and Eq. (1.8) leads to the derivation of the following equation for a Hamiltonian operator:

$$\hat{\mathsf{H}} = -\frac{\hbar^2}{2\mathsf{m}}\frac{\partial^2}{\partial x^2} + \frac{1}{2}\mathsf{m}\omega^2 x^2 \tag{1.10}$$

Let an operator $\hat{a}$ and its adjoint $\hat{a}^\dagger$. By factorizing and processing Eq. (1.10), they can be defined on a Hilbert space $\mathcal{H}$ as

$$\hat{a} = \sqrt{\frac{\mathsf{m}\omega}{2\hbar}}(\hat{x} + \frac{i}{\mathsf{m}\omega}\hat{p}) \tag{1.11}$$

$$\hat{a}^\dagger = \sqrt{\frac{\mathsf{m}\omega}{2\hbar}}(\hat{x} - \frac{i}{\mathsf{m}\omega}\hat{p}) \tag{1.12}$$

The operator $\hat{a}^\dagger$ raises the eigenvalue of another operator and is consequently called a creation operator or raising operator. The operator $\hat{a}$ lowers it, and is therefore referred to as an annihilation operator or lowering operator. The operators are non-Hermitian. When the creation operator and the annihilation operator are applied to a state, a normalization factor must be present, as seen below:

$$\hat{a}^\dagger\,|\mathsf{n}\rangle = \sqrt{\mathsf{n}+1}\,|\mathsf{n}+1\rangle \tag{1.13}$$

$$\hat{a}\,|\mathsf{n}\rangle = \sqrt{\mathsf{n}}\,|\mathsf{n}-1\rangle \tag{1.14}$$

From the above set of relations, two more properties for the photon number operator $\hat{\mathsf{n}}$ can be extracted, which will prove important:

$$\hat{\mathsf{n}} = \hat{a}^\dagger\hat{a} \tag{1.15}$$

$$\hat{\mathsf{n}}\,|\mathsf{n}\rangle = \mathsf{n}\,|\mathsf{n}\rangle \tag{1.16}$$

From the canonical commutation relation, the following commutators can be derived:

$$[\hat{a}, \hat{a}^\dagger] = 1 \tag{1.17}$$

$$[\hat{\mathsf{n}}, \hat{a}^\dagger] = \hat{a}^\dagger \tag{1.18}$$

$$[\hat{\mathsf{n}}, \hat{a}] = -\hat{a} \tag{1.19}$$

Finally, the Hamiltonian can be rewritten in terms of the ladder operators as follows:

$$\hat{\mathsf{H}} = \hbar\omega(\hat{a}^\dagger\hat{a} + \frac{1}{2}) \tag{1.20}$$

The importance of the ladder operators is derived from their depiction of the state of the electromagnetic field by measuring quantities such as the amplitude and the intensity. This representation is mainly achieved in two ways, explained in the following section.

1.3 Fock States and Coherent States

The ladder operators of the quantum field provide the mathematical formulation for the description of the discrete states called photons. The eigenstates $|\mathsf{n}\rangle$ of a photon number operator $\hat{\mathsf{n}}$ are named Fock states or number states [Fock (1932)]. When the Hamiltonian of Eq. (1.20) acts on a Fock state, the result is

$$\hat{\mathsf{H}}_{\text{Fock}} |\mathsf{n}\rangle = \hbar\omega(\hat{a}^\dagger\hat{a} + \frac{1}{2}) |\mathsf{n}\rangle = \mathsf{e}_\mathsf{n} |\mathsf{n}\rangle \tag{1.21}$$

The Fock states form a countable orthonormal basis $\{|\mathsf{n}\rangle\}_{\mathsf{n}=0}^{\infty}$ for the Hilbert space $\mathcal{H}$, called the Fock basis. A Fock state $|\mathsf{n}\rangle$ is an eigenstate of the photon number operator $\hat{\mathsf{n}}$, as in Eq. (1.16). Simply put, when a light pulse is in the eigenstate $|\mathsf{n}\rangle$, it means that n photons are present in the pulse. If the eigenstate does not contain any photons, it is called a vacuum state. Naturally, the eigenvalue of a vacuum state $|0\rangle$ is zero. However, the lowest amount of energy for such a state is not zero, but is given instead by

$$\mathsf{e}_0 = \frac{1}{2}\hbar\omega \tag{1.22}$$

By iteratively applying the creation operator $\hat{a}^\dagger$ on the vacuum state, the Fock state $|\mathsf{n}\rangle$ can be generated as

$$|\mathsf{n}\rangle = \frac{(\hat{a}^\dagger)^\mathsf{n}}{\sqrt{\mathsf{n}!}} |0\rangle \tag{1.23}$$

The expected value of the photon number in a Fock state is equal to the number of photons in the state. Consequently, the variance of the states becomes zero:

$$\mathbb{E}(\mathsf{n}) = \langle\mathsf{n}| \hat{\mathsf{n}} |\mathsf{n}\rangle = \mathsf{n} \tag{1.24}$$

$$\mathbb{V}(\mathsf{n}) = 0 \tag{1.25}$$

The state of light generated by lasers is called a coherent state or Glauber state $|\alpha\rangle$ and is defined as an eigenstate of the annihilation operator $\hat{a}$ by the expression [Glauber (1963)]

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle \tag{1.26}$$

The eigenvalue $\alpha \in \mathcal{C}$ of $|\alpha\rangle$ represents the displacement of the state in phase space and it can be expressed in terms of its amplitude $|\alpha|$ and phase angle θ as

$$\alpha = |\alpha| e^{i\theta} \tag{1.27}$$

Coherent states can also be described using the Fock state basis $|\mathsf{n}\rangle$ as [Loudon (1983)]

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{\mathsf{n}=0}^{\infty} \frac{\alpha^{\mathsf{n}}}{\sqrt{\mathsf{n}!}} |\mathsf{n}\rangle \tag{1.28}$$

In the context of phase-space representation, coherent states offer a significant advantage over Fock states. The former have an indefinite number of photons but a well-defined phase, while the latter have a precisely measurable number of photons and exhibit a completely randomly distributed phase. This enables coherent states to depict continuous-variable signals.

The probability of detecting n photons in a coherent state is described by

$$p(\mathsf{n}) = |\langle \mathsf{n}|\alpha\rangle|^2 = e^{-|\alpha|^2} \frac{|\alpha|^{2\mathsf{n}}}{\mathsf{n}!} \tag{1.29}$$

with an expected value, specifically referred to as the mean photon number, given by

$$\bar{\mathsf{n}} = \mathbb{E}(\mathsf{n}) = \langle \alpha|\hat{\mathsf{n}}|\alpha\rangle = |\alpha|^2 \tag{1.30}$$

and a variance of also $|\alpha|^2$. Applying Eq. (1.30) to Eq. (1.29) produces the probability

$$p(\mathsf{n}) = \frac{\bar{\mathsf{n}}^{\mathsf{n}} e^{-\bar{\mathsf{n}}}}{\mathsf{n}!} \tag{1.31}$$

which noticeably follows a Poisson distribution.

Coherent states are said to be overcomplete, which is derived from the fact that a pair of coherent states $|\alpha_1\rangle$ and $|\alpha_2\rangle$ is non-orthogonal. The consequence of this property is that it is possible for any coherent state to be expanded in terms of all the other coherent states. Therefore, coherent states are not linearly independent.

Because of the canonicality between the position and momentum operators, coherent states are minimum uncertainty states for the conventional Heisenberg uncertainty relation. As a result, for a standard deviation σ, they obey the condition

$$\sigma_{\hat{x}} \sigma_{\hat{p}} = \frac{\hbar}{2} \tag{1.32}$$

which leads to the definition of the concept of quadratures in the next section.

1.4 Quadratures

Consider the electromagnetic field under its classical conceptualization. Herein, electromagnetic waves are continuous sinusoidal waves, whose characterization depends on their amplitude, their phase and their angular frequency. The field can be described by

$$\mathsf{E}(\mathsf{t}) = \mathsf{E}_0 \cos(\omega \mathsf{t} + \theta) = \mathsf{E}_0 \cos\theta \cos(\omega \mathsf{t}) - \mathsf{E}_0 \sin\theta \sin(\omega \mathsf{t}) \tag{1.33}$$

where E_0 is the amplitude of the field and θ its phase angle. The coefficients $\mathsf{E}_0 \cos\theta$ and $-\mathsf{E}_0 \sin\theta$ constitute the quadrature components of the field. Given the phasor representation of the same field and its complex amplitude a, provided by

$$a(\mathsf{t}) = ae^{-i\omega \mathsf{t}}, \quad a = \mathsf{E}_0 e^{-i\theta} \tag{1.34}$$

the phasor amplitude can be rewritten as the sum of the quadrature components as

$$a = \mathsf{E}_0 \cos\theta - i\mathsf{E}_0 \sin\theta \tag{1.35}$$

The same concept can be extended to the bosonic quantum field. Quadratures are dimensionless operators, which embody the real and imaginary parts of the amplitude. Broadly speaking, they correspond to the position and momentum operators of the quantum harmonic oscillator. The quadratures are described using the ladder operators[1]

$$\hat{Q} = \sqrt{\frac{\hbar}{2}}(\hat{a} + \hat{a}^\dagger) \tag{1.36}$$

$$\hat{P} = -i\sqrt{\frac{\hbar}{2}}(\hat{a} - \hat{a}^\dagger) \tag{1.37}$$

Hence, the annihilation operator, which corresponds to the complex eigenvalue α of the coherent state, along with its counterpart, the creation operator, whose action provides the complex conjugate of α, can be redefined as

$$\hat{a} = \frac{1}{\sqrt{2\hbar}}(\hat{Q} + i\hat{P}) \tag{1.38}$$

$$\hat{a}^\dagger = \frac{1}{\sqrt{2\hbar}}(\hat{Q} - i\hat{P}) \tag{1.39}$$

Because they satisfy the uncertainty relation of Eq. (1.32), $\hat{Q}$ and $\hat{P}$ are canonically conjugate. Therefore, they form a set of non-commuting operators, whose commutation relation in SI units is

$$[\hat{Q}, \hat{P}] = i\hbar \tag{1.40}$$

The quadrature states are the eigenstates of $\hat{Q}$ and $\hat{P}$, expressed as

$$\hat{Q}\,|Q\rangle = Q\,|Q\rangle \tag{1.41}$$

$$\hat{P}\,|P\rangle = P\,|P\rangle \tag{1.42}$$

[1] It is henceforth assumed that the mass $\mathsf{m} = 1$ and the angular frequency $\omega = 1$, unless otherwise specified.

1.5 Phase-Space Operators

Even though the phase has no physical meaning on its own, it plays a vital role in understanding the behavior of a wave in an electromagnetic field. Defining appropriate operators enables the movement of coherent states around the optical phase space. Two such operators are presented below.

The first is the phase-shifting operator, which enables movement around the phase space by rotating a coherent state by an angle θ. It is defined as

$$\hat{U}(\theta) = e^{-i\theta\hat{\mathfrak{n}}} \tag{1.43}$$

If the phase-shifting operator acts on a coherent state $|\alpha\rangle$, it transforms it as $\hat{U}(\theta)\,|\alpha\rangle$, resulting in a phase shift or rotation of θ as follows:

$$\hat{U}(\theta)\,|\alpha\rangle = \left|\alpha e^{-i\theta}\right\rangle \tag{1.44}$$

Another important operator is the displacement operator or Weyl operator $\hat{D}$, which converts a coherent state into another coherent state. It is given by

$$\hat{D}(\alpha) = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}} \tag{1.45}$$

where α, shown in Eq. (1.27), indicates the amount of displacement on the phase space and α^* is its complex conjugate. The displacement operator is a unitary map, such that

$$\hat{D}^\dagger(\alpha) = \hat{D}^{-1}(\alpha) = \hat{D}(-\alpha) \tag{1.46}$$

The most basic application of the displacement operator is the generation of a coherent state from a displaced vacuum state, expressed by the relation

$$|\alpha\rangle = \hat{D}(\alpha)\,|0\rangle \tag{1.47}$$

A pair of notable relations, which leads to Eq. (1.30), is [Barnett and Radmore (1997)]

$$\hat{D}^\dagger(\alpha)\hat{a}\hat{D}(\alpha) = \hat{a} + \alpha \tag{1.48}$$

$$\hat{D}^\dagger(\alpha)\hat{a}^\dagger\hat{D}(\alpha) = \hat{a}^\dagger + \alpha^* \tag{1.49}$$

In a future chapter, the significance of the displacement operator will be explored by examining its use in defining the characteristic function of a quantum state.

1.6 Multi-Mode Fields

All of the systems presented earlier appear in the single-mode electromagnetic field. In case a system in the quantized field is characterized by multiple canonical bosonic degrees of freedom, it must be described by multiple harmonic oscillators, which are referred to as the modes of the field. The system is then called a multi-mode system. This section contains a handful of important formulas, reformed for the multi-mode case.

Referring to the Hamiltonian of Eq. (1.20) for a single-mode system, the Hamiltonian of the multi-mode electromagnetic field is written as [Ferraro et al. (2005)]

$$\hat{\mathsf{H}} = \sum_{\kappa=1}^{\nu} \hbar\omega_\kappa (\hat{a}_\kappa^\dagger \hat{a}_\kappa + \frac{1}{2}) \tag{1.50}$$

where $\kappa = 1, \ldots, \nu$ symbolizes the field modes. In such a field, each operator $\hat{a}_\kappa$ and $\hat{a}_\kappa^\dagger$ operates on its own mode. Collectively, they satisfy the bosonic commutation relations

$$[\hat{a}_\kappa, \hat{a}_{\kappa'}^\dagger] = \delta_{\kappa\kappa'} \tag{1.51}$$

$$[\hat{a}_\kappa, \hat{a}_{\kappa'}] = [\hat{a}_\kappa^\dagger, \hat{a}_{\kappa'}^\dagger] = 0 \tag{1.52}$$

where δ denotes the Kronecker delta.

Multi-mode Fock states form a basis $\{|\mathsf{n}_1, \mathsf{n}_2, \ldots, \mathsf{n}_\nu\rangle\}_{\mathsf{n}=0}^{\infty}$ for the multi-mode Hilbert space $\mathcal{H}^{\otimes\nu}$. In multi-mode Fock space, the radiation field can be decomposed into distinct radiation modes, each characterized by its wave number vector and polarization. Here, the photon-number operator $\hat{\mathsf{n}}$ represents the sum of all such operators of each mode and is defined as the total number operator

$$\hat{\mathsf{n}}_{\text{tot}} = \sum_{\kappa=1}^{\nu} \hat{\mathsf{n}}_\kappa = \sum_{\kappa=1}^{\nu} \hat{a}_\kappa^\dagger \hat{a}_\kappa \tag{1.53}$$

Recalling Eq. (1.16), the multi-mode Fock state is an eigenvector of $\hat{\mathsf{n}}_{\text{tot}}$, whose eigenvalue is the overall count of particles distributed in all modes of the system, as displayed below:

$$\hat{\mathsf{n}}_{\text{tot}} |\mathsf{n}_\kappa\rangle = \sum_{\kappa=1}^{\nu} \mathsf{n}_\kappa |\mathsf{n}_\kappa\rangle \tag{1.54}$$

A multi-mode coherent state can be expressed as the tensor product of the individual states, i.e. $|\alpha_1, \alpha_2, ..., \alpha_\nu\rangle = |\alpha_1\rangle \otimes |\alpha_2\rangle \otimes ... \otimes |\alpha_\nu\rangle$. Then, $\vec{\alpha} = (\alpha_1, \alpha_2, ..., \alpha_\nu)$ is the vector of complex amplitudes, each representing a coherent state in its respective mode κ. A coherent state for a single mode κ is an eigenstate of the annihilation operator $\hat{a}_\kappa$:

$$\hat{a}_\kappa |\alpha_\kappa\rangle = \alpha_\kappa |\alpha_\kappa\rangle \tag{1.55}$$

Considering Eq. (1.28), every individual mode of a multi-mode coherent state is

$$|\alpha_\kappa\rangle = e^{-\frac{|\alpha_\kappa|^2}{2}} \sum_{\mathsf{n}_\kappa=0}^{\infty} \frac{\alpha^{\mathsf{n}_\kappa}}{\sqrt{\mathsf{n}_\kappa!}} |\mathsf{n}_\kappa\rangle \tag{1.56}$$

The quadrature phase operators of a multi-mode system for position and momentum, based on Eq. (1.36) and Eq. (1.37), are displayed below:

$$\hat{Q}_\kappa = \sqrt{\frac{\hbar}{2}}(\hat{a}_\kappa + \hat{a}_\kappa^\dagger) \tag{1.57}$$

$$\hat{P}_\kappa = -i\sqrt{\frac{\hbar}{2}}(\hat{a}_\kappa - \hat{a}_\kappa^\dagger) \tag{1.58}$$

The multi-mode displacement operator is given by

$$\hat{D}(\vec{\alpha}) = \exp\left[\sum_{\kappa=1}^{\nu}(\alpha_\kappa \hat{a}_\kappa^\dagger - \alpha_\kappa^* \hat{a}_\kappa)\right] \tag{1.59}$$

and the corresponding multi-mode coherent state generated by the displacement of the vacuum state for each κ is given by

$$|\alpha_1, \alpha_2, ..., \alpha_\nu\rangle = \bigotimes_{\kappa=1}^{\nu} \hat{D}(\alpha_\kappa)\,|0\rangle \tag{1.60}$$

1.7 Beam Splitter and Optical Detection

A beam splitter is an optical component, which allows part of an incident light beam to traverse it and reflects the remaining part. The device can also be employed to combine two light beams into a single signal. Some applications, which benefit significantly from the contribution of the beam splitter, are interferometry, quantum entangling and the performing of Bell measurements [Wang et al. (2007)].

A beam splitter can be characterized by its transmissivity T, which measures the amount of light that passes through, and its reflectivity $\mathscr{R}$, which quantifies the reflected amount of light. Given the angle of incidence $\theta \in [0, \frac{\pi}{2}]$, the pair is defined as

$$T = \cos^2\theta \tag{1.61}$$

$$\mathscr{R} = \sin^2\theta \tag{1.62}$$

The combination of the two equations implies that $T + \mathscr{R} = 1$. Note that this relation holds for a lossless beam splitter. In such a model, a photon must either be transmitted or reflected. In practice, some absorption and dissipation takes place, which means that $T + \mathscr{R} < 1$. A beam splitter is called balanced or 50/50, when one half of the incident light is transmitted and the other half is reflected; this requires an angle $\theta = \frac{\pi}{4}$, corresponding to equal transmissivity and reflectivity values of $T = \mathscr{R} = \frac{1}{2}$.

Through its two characteristics, the beam splitter transformation can be mathematically defined. Suppose two input modes, represented by the annihilation operators $\hat{a}_1^{\text{in}}$ and $\hat{a}_2^{\text{in}}$. The coupling between the modes yields two output modes $\hat{a}_1^{\text{out}}$ and $\hat{a}_2^{\text{out}}$ as follows:

$$\begin{bmatrix} \hat{a}_1^{\text{in}} \\ \hat{a}_2^{\text{in}} \end{bmatrix} \rightarrow \begin{bmatrix} \hat{a}_1^{\text{out}} \\ \hat{a}_2^{\text{out}} \end{bmatrix} = \begin{bmatrix} \tau & \varrho \\ -\varrho & \tau \end{bmatrix} \begin{bmatrix} \hat{a}_1^{\text{in}} \\ \hat{a}_2^{\text{in}} \end{bmatrix} \tag{1.63}$$

where τ and ϱ are the square roots of transmissivity T and reflectivity $\mathscr{R}$ respectively. The interference of two modes in a beam splitter can be described by a Gaussian unitary transformation U, which is given by

$$U(\theta) = e^{i\theta(\hat{a}_1^\dagger \hat{a}_2 - \hat{a}_1 \hat{a}_2^\dagger)} \tag{1.64}$$

This evolution preserves the Gaussian character of the state, inducing a symplectic transformation in the quantum phase space of the composite system. A symplectic transformation $\mathbf{S}$ is a linear transformation that preserves the symplectic structure of the phase space, maintaining its geometric and dynamical properties. In the context of the beam splitter, the symplectic transformation is parametrized by the transmissivity T and characterized by

$$\mathbf{S}_{\text{BS}}(T) = \begin{bmatrix} \sqrt{T}\mathbf{I} & \sqrt{1-T}\mathbf{I} \\ -\sqrt{1-T}\mathbf{I} & \sqrt{T}\mathbf{I} \end{bmatrix} \tag{1.65}$$

A prominent application of beam splitters can be found in optical detection systems. Contemporary photon detectors are unable to perfectly observe the nearly instantaneous oscillation of the wave of an electric field, in order to measure the phase of the field. Nevertheless, this can be achieved by two methods, labelled homodyne detection and heterodyne detection, under which the field quadratures are computed as a substitute [Li et al. (2015)]. A homodyne measurement estimates either $\hat{Q}$ or $\hat{P}$, while a heterodyne one measures both quadratures. Their main difference is that the light beams involved in the former process are in the same frequency, while the beams of the latter method typically involve multiple frequencies. However, there are ways to achieve heterodyne detection with beams in the same frequency, even though this is less common. The dissimilarity in frequency between the two fields is known as the intermediate frequency.

Homodyne and heterodyne detection are performed by interfering the weak input signal with a strong classical beam, called the local oscillator (LO). The LO acts as the phase reference for the system, in order to provide indirect access to the phase of the field. It is assumed to be in a coherent state $|\alpha_{\text{LO}}\rangle$ with a large photon number, in order to ensure a stable and consistent phase reference. The two beams are mixed using a balanced beam splitter. Both beam splitter outputs are detected with a pair of photodiodes and subtracted from each other.

In homodyne detection, the detected quadrature is dependent on the relative phase angle θ between the squeezed beam and the LO. A random selection of either $\theta = 0$ or $\theta = \frac{\pi}{2}$ ensures that the photon-number difference $\Delta\hat{\mathsf{n}}$ at the output ports of the beam splitter is directly related to only one of the two field quadratures, as shown by [Laudenbach et al. (2018)]

$$\Delta\hat{\mathsf{n}} = |\alpha_{\mathrm{LO}}|(\hat{Q}\cos\theta + \hat{P}\sin\theta) \tag{1.66}$$

where α_{LO} is described in Eq. (1.27). In heterodyne detection, the resulting interference generates an electrical signal at the intermediate frequency, which carries the amplitude and phase information of the original signal.

Chapter 2

Information Theory

Shannon's groundbreaking set of papers in 1948 changed the world forever by practically creating the discipline of information theory [Shannon (1948)]. The virtually unlimited potential of this field of study can spark an endless discussion around it. Nonetheless, only notions, which are necessary for the comprehension of this thesis, are explained in this chapter. The topic is reviewed from both a classical and a quantum standpoint.

2.1 Classical Information Theory

The section initially covers the foundational components of classical information theory, then proceeds to explain channel transmission and error correction and concludes with the more advanced concepts of the asymptotic equipartition property and the Slepian-Wolf bound.

2.1.1 Entropy

The most fundamental measure in information theory is the Shannon entropy. Entropy quantifies the amount of uncertainty involved in the value of a random variable or the outcome of a random process. By definition, it is a positive quantity. The most common unit of measurement of the entropy is the bit. Given a discrete random variable X, the entropy is computed by

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

where $\mathcal{X}$ is the set of all possible outcomes of X. For the special case, where X has only two possible outcomes and $p_X(x = 1)$, the formula reduces to the binary entropy as

$$H_2(X) = -p_X \log_2 p_X - (1 - p_X) \log_2 (1 - p_X) \tag{2.2}$$

When a set of variables is involved, the measure of uncertainty is referred to as the joint entropy. For two random discrete variables X and Y, the joint entropy is calculated as

$$H(X,Y) = -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log_2 p(x,y) \tag{2.3}$$

where $p(x,y)$ is the joint probability distribution, indicating the likelihood of x and y occurring simultaneously. Also, $\mathcal{Y}$ denotes the set of all possible outcomes for Y.

The conditional entropy indicates how much extra information on average needs to be provided to communicate Y, given that the other party knows X. The associated formula is

$$H(Y|X) = H(Y,X) - H(X) = -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log_2 \frac{p(x,y)}{p(x)} \tag{2.4}$$

In other words, the conditional entropy quantifies the remaining uncertainty about the source X, when Y is known. Zero conditional entropy means that Y is determined entirely by X.

The min-entropy of a discrete random variable provides a lower bound on the Shannon entropy, as $H_{\min}(X) \leq H(X)$ for any probability distribution of X. It quantifies the maximum predictability associated with X by highlighting the scenario, where a specific outcome is significantly more likely than any other. As such, it is used as the most conservative measure for the unpredictability of a random variable. It is expressed as

$$H_{\min}(X) = -\log_2 \max_{x\in\mathcal{X}} p(x) \tag{2.5}$$

In addition, the concept can be extended to circumstances, where side information is involved. Then, the quantity of interest becomes the conditional min-entropy, whose formula is given by [Tomamichel et al. (2011)]

$$H_{\min}(X|E) = -\log_2 p_{\text{guess}}(X|E) \leq H(X|E) \tag{2.6}$$

where p_{guess} signifies the guessing probability of X under an optimal strategy with access to E. The optimal strategy is to guess, for each value e of E, the X with the highest conditional probability $p_{X|E=e}$

$$p_{\text{guess}}(X|E) = \sum_{e} p_E(e)\max_{x} p_{X|E=e}(x) \tag{2.7}$$

In a distribution with min-entropy at least $H_{\min}$, all events take place with a probability of equal to or less than $2^{-H_{\min}}$. This property creates a necessary condition for a certain family of functions, called randomness extractors, to extract $H_{\min}$ random bits from a biased and correlated sequence. Such functions are able to produce a random, uniform and seemingly source-independent output. These attributes are extremely desirable in cryptography applications and particularly secret key distribution.

2.1.2 Mutual Information

Suppose two discrete random variables X and Y, which are sampled simultaneously. The quantity that measures the relationship between these variables is called mutual information. In other words, the mutual information $I(X:Y)$ stands for the obtainable number of information bits per symbol of a random variable X by knowing another random variable Y and vice versa. It is given by

$$I(X:Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = \sum_{y\in\mathcal{Y}}\sum_{x\in\mathcal{X}} p(x,y)\log_2\frac{p(x,y)}{p(x)p(y)} \quad (2.8)$$

A mutual information which equals zero implies that the two random variables are completely independent from each other.

Basic properties of the mutual information are listed below:

- **Non-negativity**: Mutual information is always zero or above zero.
- **Symmetry**: Mutual information is symmetric, i.e. $I(X:Y) = I(Y:X)$
- **Additivity**: Mutual information is additive for independent variables.

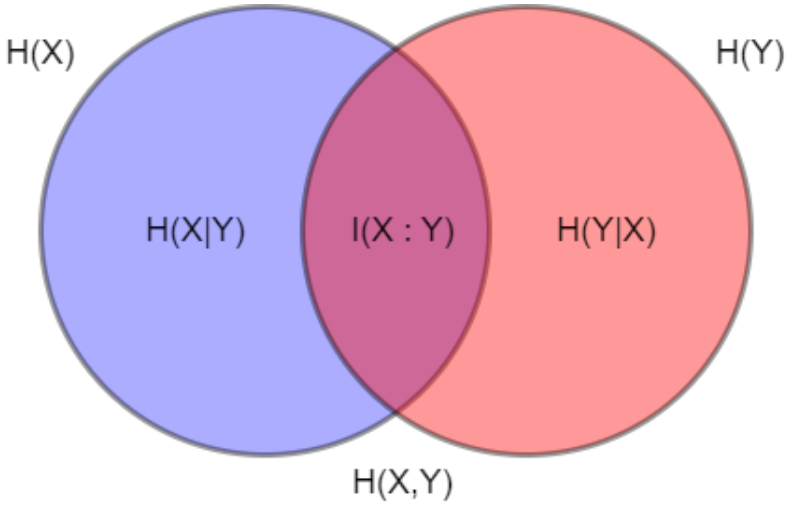

Figure 2.1: Venn diagram illustrating the relationships between different information measures, which are associated with correlated variables X and Y.

Through the mutual information, multiple theorems can be defined. One of them is the data processing inequality. In simple terms, it states that the information content of a signal cannot be increased via a local physical operation [Cover and Thomas (2001)]. Let three random variables X, Y, Z, where Y is a transformation of X and Z is a map originating from Y, thus forming a sequence of transformations $X \to Y \to Z$. The inequality is then signified by

$$X \to Y \to Z \Rightarrow I(X:Y) \geq I(X:Z) \quad (2.9)$$

2.1.3 Channels

A communication channel is a physical transmission medium, which imperfectly connects a transmitter and a receiver. A typical distinction is between wired channels, such as copper cables or optical fibers and wireless channels, such as Wi-Fi, Bluetooth and satellite links. A channel has an upper limit of transmittable information, called channel capacity and measured in bits per channel use. The channel capacity C is defined as the maximum rate, at which information can be transmitted reliably over a channel. In terms of the mutual information, it is given by [Cover and Thomas (2001)]

$$C = \max_{p_X} I(X : Y) \tag{2.10}$$

where X is the input variable and Y is the output variable.

In the context of information theory, a channel is regarded as a system, whose output depends probabilistically on its input. It represents a transformation, that maps input symbols to output symbols with certain error characteristics. Channels are studied as noiseless, which are ideal models and noisy, which corrupt the signal. Different models of noisy channels exist in theory, each serving a particular purpose. The most common examples are the binary symmetric channel (BSC), which may or may not invert a transmitted bit with a certain probability, and the additive white Gaussian noise channel (AWGN), which resembles actual noise sources. The wide use of the latter is also owed to its simplification of the mathematical analysis.

Shannon's seminal paper in 1948 resolved two core matters [Shannon (1948)]. The first was the compression rate of a transmitted message. This is dealt with by the source coding theorem, or noiseless coding theorem. The theorem states that data may be encoded in such a way, where the number of bits required to represent the data can be reduced, but without sacrificing essential information during the process. The measure of entropy was introduced here as the information content of the source on average.

The second was the reliability of the transmission over a noisy classical channel and it is described by the channel coding theorem. The channel capacity, also referred to as Shannon limit or Shannon capacity, was defined in this context, in order to quantify the maximum errorless transmission rate, when the link is subject to random errors. If the transmission rate R' of a channel is smaller than its capacity C, then particular codes, which detect and correct the errors, can be defined. The reverse is also true; if $R' > C$, the design of suitable codes, able to achieve errorless transmission, is infeasible. The results of Shannon's theorem paved the way for the invention of various error-correcting schemes, which enable reliable communication, regardless of the existence of noise.

2.1.4 Channel Coding

In practice, all channels are noisy. This means that information conveyed through them inevitably gets corrupted. The process of detecting and removing the errors, which arise during transmission, is known as error correction. A code is the scheme, that converts information to a state, suitable for transmission over a noisy channel. This process is called encoding, while the retrieval of the original message by the receiver is named decoding. The elements comprising the codes are known as codewords and are described by unique linear combinations of basis vectors composed by symbols, named letters, that belong in a finite field, called alphabet $\mathcal{A}$. The decoding process may involve calculating the syndrome of the codewords, which is a set of values providing information about the errors, in order to ensure accurate data recovery.

Named after its creator, the Hamming code is the first and one of the simplest examples of a linear block code [Hamming (1950)]. The term block implies that the encoding process takes place in blocks. Multiple classes of codes, such as convolutional codes or turbo codes, were devised over time. However, linear block codes remain highly relevant, because of their simple construction and very high efficiency. Every linear block code is represented by a matrix $\mathbf{H}$, called parity-check matrix. The corresponding parity-check matrix of the Hamming code is

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \tag{2.11}$$

Block codes often follow the $[n, \mathtt{k}, d_{\min}]$ notation, where every variable signifies:

- the number of columns n, also referred to as codeword length or block length,
- the number of information bits $\mathtt{k}$, also known as message length, and
- the distance $d_{\min}$, which is the minimum number of positions, in which any two distinct codewords differ.

As $\mathtt{k}$ stands for the useful bits of information, $n - \mathtt{k}$ returns the quantity of redundant bits, which were added as an error-correction measure. The fraction, that measures the proportion of the useful bits against the parity ones, is known as the code rate R_{code}, demonstrated by

$$R_{\text{code}} = \frac{\mathtt{k}}{n} \tag{2.12}$$

Note that $0 \leq R_{\text{code}} \leq 1$, where the ideal $R_{\text{code}} = 1$ implies the lack of redundancy bits. The difference $1 - R_{\text{code}}$ indicates the ratio of redundant information used to reconcile errors. Considering the above, the Hamming code of Eq. (2.11) is a $[7, 4, 3]$ code with $R_{\text{code}} \approx 0.571$, as it has $n = 7$ columns, $\mathtt{k} = 4$ information bits on every row and a minimum distance of $d_{\min} = 3$.

A special category of linear block codes is the low-density parity-check (LDPC) code, whose parity-check matrix $\mathbf{H}$ has a low density of non-zero elements [Gallager (1962)]. LDPC codes are constructed using a sparse Tanner graph, which are bipartite graphs, specifically employed for code design. Two sets of nodes determine the design of the code: the check nodes, which represent the set of parity-check equations, and the variable nodes, which serve as the elements of the codewords. The number of edges of a node is referred to as its degree. A check node of degree $\mathtt{d}_\mathrm{c}$ is connected to $\mathtt{d}_\mathrm{c}$ variable nodes and a variable node of degree $\mathtt{d}_\mathrm{v}$ is connected to $\mathtt{d}_\mathrm{v}$ check nodes. A family of LDPC codes can be characterized by a pair of generating polynomials

$$\lambda(x) = \sum_{i=2}^{\mathtt{d}_{\mathrm{v}\max}} \Lambda_i x^{i-1} \quad 0 \leq \Lambda_i \leq 1 \tag{2.13}$$

$$\rho(x) = \sum_{j=2}^{\mathtt{d}_{\mathrm{c}\max}} \Pi_j x^{j-1} \quad 0 \leq \Pi_j \leq 1 \tag{2.14}$$

where Λ_i and Π_j indicate the normalized-to-1 proportion of edges connected to symbol and check nodes of degree i, respectively. The code rate of the family is then given by

$$R_\mathrm{code} = 1 - \frac{\sum_{j=2}^{\mathtt{d}_{\mathrm{c}\max}} \Pi_j / j}{\sum_{i=2}^{\mathtt{d}_{\mathrm{v}\max}} \Lambda_i / i} \tag{2.15}$$

Two important properties of the parity-check matrix are the number of non-zero elements of every column, or column weight, and the count of units in every row, or row weight. A code is classified as regular, when both the column and row weights are constant throughout the entire construction, or irregular, when the weights vary. The rate of a regular LDPC code can be fully characterized by either the number of rows and columns l and n or the row and column weights w_r and w_c of the matrix, as follows:

$$R_\mathrm{code} = 1 - \frac{l}{n} = 1 - \frac{w_\mathrm{c}}{w_\mathrm{r}} \tag{2.16}$$

High-quality LDPC codes with an adequately large block length have been shown to approach the Shannon limit [MacKay (1999)]. LDPC codes are typically combined with iterative belief propagation algorithms, such as the sum-product algorithm or the min-sum algorithm, decoded in time linear to their block length. It must be noted, that an LDPC code with a certain code rate is effective only in a particular range of error [Gallager (1962)]. Consequently, in order to be capable of reconciling in a wide range of error rates, a collection of codes is required.

A scenario often encountered in the study of coding concerns source coding with side information, where decoding occurs under the assistance of a separate but correlated source. For this subdivision of source coding problems, the achievable rate region is determined by the Slepian-Wolf bound or Slepian-Wolf limit [Slepian and Wolf (1973)].

A random sequence X can be sufficiently encoded, when the code rate $R_{\text{code}} > H(X)$. Suppose that X is correlated to a sequence Y, which is accessible by the decoder. If two sources $X, Y \sim p(X, Y)$ are encoded together, a rate of at least $H(X, Y)$ is necessary. If encoded separately, the intuitive assumption would be that the $R_{\text{code}} = H(X) + H(Y)$. Instead, $R_{\text{code}} = H(X, Y)$ is sufficient. Combined with Eq. (2.4), the bound states that

$$R_{\text{code}} \geq H(X, Y) = H(X) + H(Y|X) \leq H(X) + H(Y) \tag{2.17}$$

The Slepian-Wolf bound is invaluable in designing efficient code schemes that approach the theoretical bounds on achievable compression rates, enabling more effective error correction and data transmission in scenarios, where correlated sources are involved.

2.1.5 Asymptotic Equipartition Property

The notion of entropy gave birth to multiple new concepts, among which one of the most important is the asymptotic equipartition property (AEP). In simple terms, it suggests that a while a random process can generate a variety of results, the actual outcome originates from a subset of outcomes, known as the typical set [Cover and Thomas (2001)]. The term typical implies that the set consists of sequences, which occur neither extremely rarely nor excessively frequently; they represent what is expected within the given context. Such sets will have properties, that reflect the statistics of the underlying random variables. As a result, concentrating all focus on the typical set allows for reliably estimating the behavior of a random process. Calculating the sample entropy of a typical set, meaning the entropy calculated from a finite number of samples, returns a value very close to the true entropy. Given independent and i.i.d random variables $X_1, X_2, \ldots X_n$, where n tends to infinity, the AEP asserts that

$$\frac{1}{n} \log_2 \frac{1}{p(X_1, X_2, \ldots, X_n)} \xrightarrow{n \to \infty} H(X) \tag{2.18}$$

Here, $p(X_1, X_2, \ldots, X_n)$ stands for the probability of observing a specific sequence of outcomes and is approximated by

$$p(X_1, X_2, \ldots, X_n) \approx 2^{-nH(X)} \tag{2.19}$$

The formula indicates that, as the number of variables becomes extremely large, the joint distribution of the sequence becomes increasingly concentrated around the typical set. The probability of observing a sequence of outcomes outside the typical set, known as the atypical set, decreases exponentially. As the total probability of all typical sequences converges to 1, the size of typical set becomes approximately 2^{nH}.

The AEP is the information theoretic analog of the Law of Large Numbers, which states that, as the number of i.i.d. random variables approaches infinity, the average of these variables converges towards the expected value of the distribution. The importance of the AEP originates from its contribution to the proofs of source coding and channel capacity theorems. In future sections, the AEP will be applied in a cryptographic environment to quantify errors made by the inclusion of finite-size effects.

2.2 Quantum Information Theory

Quantum Information Theory expands the notions of its classical counterpart by encompassing the laws of quantum mechanics. This section briefly introduces the different states a quantum system can be in, then presents an easy way to describe them and, finally, explores quantum information-theoretic quantities, such as the von Neumann entropy and the Holevo bound.

2.2.1 State Description

In quantum mechanics, there exist multiple ways to describe a quantum state. The standard description is the state vector, denoted by $|\psi\rangle$, which is a column vector in a Hilbert space $\mathcal{H}$. Other terms for the notation are the Dirac notation, named after its inventor, and bra-ket notation, as the symbol used in the description is called a ket [Dirac (1950)]. The notation also includes the bra vector $\langle\psi|$, which represents the conjugate transpose of the ket vector. The bra is typically used in the calculation of the inner product between two vectors or the outer product of a state vector.

Quantum states can be distinguished based on several characteristics. One of the most usual distinctions is between a pure and a mixed state. A pure quantum state can be described by a single wave function. Simply put, the exact state a pure state is in is fully known. Contrarily, a mixed state is a mixture of the different pure states in the statistical ensemble. In this case, there is incomplete information about the state of the system and statistical averages must be performed, in order to describe the quantum observables. The process of transforming a mixed state into a pure state is called purification. An entity holding a purification implies having access to the underlying purified version of the state, which has been obtained by purifying the observed mixed state.

Composite or compound states refer to quantum states, that describe a multipartite quantum system. Such states are commonly categorized as either separable or entangled. Quantum states, which can be written as a convex combination of product states, are called separable states. The quantum state of the entire system can be expressed as a simple product of individual states for each subsystem. Changes in the behavior of one

subsystem do not affect any of the other subsystems. Given two subsystems, a pure state is separable, when it can be written in the form

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \tag{2.20}$$

If quantum states cannot be represented in this way, they are called entangled states. The subsystems of entangled states exhibit correlation, in the sense that the behavior of each system is intricately linked to the behavior of all other subsystems, regardless of the distance between them.

An alternate mathematical formulation for the states of a quantum system is given by a trace-class operator, called the density operator. The density operator $\hat{\rho}$ is a preferable choice when describing mixed states, whereas the state vector is better suited for pure states. The density operator of pure states is simply the outer product of a state vector $|\psi\rangle$, found by

$$\hat{\rho} = |\psi\rangle \langle\psi| \tag{2.21}$$

while the same operator requires a pure-state linear combination representation for mixed states, as follows:

$$\hat{\rho} = \sum_i p_i |\psi\rangle \langle\psi| \tag{2.22}$$

If there exist probabilities p_i and mixed states $\hat{\rho}_1^i$ and $\hat{\rho}_2^i$, such that the mixed state ρ can be written as a convex combination

$$\hat{\rho} = \sum_i p_i \hat{\rho}_1^i \otimes \hat{\rho}_2^i \tag{2.23}$$

then ρ is a separable state. This formula is also known as the convex decomposition of a mixed state.

The representation of the density operator is called a density matrix ρ. This is a square Hermitian matrix, whose size displays the dimension of the Hilbert space of the quantum system. The diagonal elements of ρ serve as the probabilities of finding the system in corresponding eigenstates, while the off-diagonal elements express the quantum correlations between the different states. The trace of the square of a density matrix indicates the purity of a state, which is the measure of how pure the state is. A system in a pure state has a purity of $\mathrm{tr}(\rho^2) = 1$, which is the maximum value the purity can take. The purity of a system in a mixed state satisfies the condition $\mathrm{tr}(\rho^2) < 1$. A purity of zero indicates a completely mixed state.

Some basic properties of density operators are presented below:

- **Idempotency**: A density operator describes a pure state, if $\hat{\rho} = \hat{\rho}^2$.
- **Hermiticity**: A density operator is Hermitian in the Hilbert space $\mathcal{H}$, because $\hat{\rho}^\dagger = \hat{\rho}$. As a result, its eigenvalues are real and its eigenvectors orthogonal.

- **Positive Semidefiniteness**: $\langle\psi|\,\hat{\rho}\,|\psi\rangle \geq 0$ for every $|\psi\rangle$, as $\hat{\rho}$ is Hermitian and all of its eigenvalues are non-negative: $\lambda_1, \lambda_2, \ldots, \lambda_\nu \geq 0$.
- **Normalization**: The trace of the density matrix always obeys $\mathrm{tr}(\hat{\rho}) = 1$. Because the sum of the eigenvalues is equal to the trace, this implies that the obtained set of eigenvalues λ_i can be interpreted as the probabilities p_i.

2.2.2 Von Neumann Entropy

Analogously to classical version, there exists a measure to quantify the uncertainty about the mixed state of a quantum system. For such a system that is described by a density matrix ρ, the von Neumann entropy or quantum entropy S is given by

$$S(\rho) = -\mathrm{tr}(\rho \ln \rho) \tag{2.24}$$

If and only if a quantum system is in a pure state, then the von Neumann entropy of the system is equal to zero. For mixed states, this amount is always positive.

Alternatively, when a quantum state is written in the form of Eq. (2.22), the von Neumann entropy of a mixed state can be reformed using the Schmidt decomposition to

$$S(\rho) = -\sum_i p_i \ln p_i \tag{2.25}$$

This form resembles the classical information theory entropy, as stated by Shannon.

Fundamental properties of the von Neumann entropy are displayed below:

- **Purity**: A pure state ρ has $S(\rho) = 0$.
- **Invariance**: The entropy remains the same under a unitary transformation, as in $S(U\rho U^{-1}) = S(\rho)$.
- **Maximum**: The maximum value of the entropy is given by a maximally mixed state and becomes equal to $S_{\max}(\rho) = \ln \nu$, ν being the Hilbert space dimension.
- **Concavity**: $S(\eta\rho_1 + (1-\eta)\rho_2) \geq \eta S(\rho_1) + (1-\eta)S(\rho_2)$, for $0 \leq \eta \leq 1$.
- **Subadditivity**: The entropy of a quantum composite system can be lower than the entropy of any of its parts, that is $S(\rho_{AB}) \leq S(\rho_A) + S(\rho_B)$.

Through the von Neumann entropy, other quantities can be extended to the quantum realm. One example is the conditional von Neumann entropy, determined as

$$S(A|B)_\rho = S(AB)_\rho - S(B)_\rho \tag{2.26}$$

Unlike the classical conditional entropy, it is possible for the conditional quantum entropy to be negative, even though the von Neumann entropy of single variable is never negative. The quantum mutual information is also defined as the measure of relationship between the subsystems of a state. Given a bipartite state ρ_{AB} on the state space $\mathcal{H}_A \otimes \mathcal{H}_B$, the quantum mutual information of two separable quantum systems A and B is defined as

$$I(A:B) = S(\rho_A) + S(\rho_B) - S(\rho_{AB}) \tag{2.27}$$

2.2.3 Holevo Bound

In 1973, Holevo proved that there is an upper bound on the obtainable amount of classical information from a quantum system [Holevo (1973)]. It is called Holevo bound and it dictates that it is impossible to extract more than one bit of classical information from a single qubit. At best, the obtainable bits are equal to the number of qubits, even though the qubits may hold a higher amount of classical information. This limit, otherwise known as Holevo information, is given by

$$\chi = S(\rho) - \sum_i p_i S(\rho_i) \tag{2.28}$$

where ρ_i is a mixed state drawn from an ensemble $\{\rho_1, \rho_2 \dots \rho_\nu\}$ with probability p_i. The Holevo bound quantifies the average reduction in the von Neumann entropy of an ensemble, when the preparation of the states is known.

Given two random variables X and Y, where the former is the source alphabet and the latter the outcome of a measurement or encoding process applied to X, their mutual information is always equal or less than the Holevo information:

$$I(X:Y) \leq \chi \tag{2.29}$$

This relationship ensures that the information obtained from measurement or encoding cannot exceed the total correlation between the source alphabet and the outcome of the process. Because the mutual information is always non-negative, evidently, the same applies for the Holevo bound.

The Holevo bound is also closely linked to the definition for the classical capacity a quantum channel. This capacity, provided by the Holevo-Schumacher-Westmoreland theorem, is the maximum achievable rate, at which information can be transmitted reliably over a quantum channel [Schumacher and Westmoreland (1997)]. The theorem states that if the transmitted states are encoded with an error-correcting code, the classical capacity of the channel is given by the maximum achievable mutual information between the input and output ensembles. The maximum mutual information is subject to the imposed bound.

The Holevo bound is a quantity of great interest from a quantum communications point of view, as it represents the upper limit on an eavesdropper's information. For two antagonizing entities, say an eavesdropper named Eve and a trusted party called Bob, the Holevo bound χ_{EB} is the difference of the von Neumann entropy of the accessible state of Eve and the conditional entropy of Eve and Bob of the eavesdropper's state, conditioned on Bob's measurement outcome. Mathematically, this is demonstrated by

$$\chi_{\mathrm{EB}} = S(E) - S(E|B) \tag{2.30}$$

In addition, if another trusted party named Alice shares with Bob a purification ρ_{AB}, which is also under the possession of Eve, the entropy of the system and the Holevo information are retained. This is owed to the invariance property of the von Neumann entropy.

2.2.4 Trace Distance and Fidelity

Different classical states are completely distinguishable. The same does not apply in quantum mechanics, where quantum state discrimination is one of the most important tasks in quantum information theory. Through density operators, various measures for the distinguishability between two quantum states can be defined. One of the most prominent metrics is known as trace distance and it is the quantum equivalent of the Kolmogorov distance between two classical probability distributions. The trace distance between two quantum states ρ_1 and ρ_2 is defined as

$$D(\rho_1, \rho_2) = \frac{1}{2}\mathrm{tr}(|\rho_1 - \rho_2|) \tag{2.31}$$

An alternative formulation is

$$D(\rho_1, \rho_2) = \frac{1}{2}\sum |\lambda_j| \tag{2.32}$$

where $\sum |\lambda_j|$ is the sum of the absolute values of the eigenvalues of the matrix $\rho_1 - \rho_2$. An important characteristic of the trace distance is its invariance under unitary maps.

Another similar concept is the quantum fidelity F, which represents a metric of the closeness between two quantum states ρ_1 and ρ_2 on the geometry of a finite-dimensional Hilbert space $\mathcal{H}$. The fidelity is given by

$$F(\rho_1, \rho_2) = \mathrm{tr}\left(\sqrt{\sqrt{\rho_1}\rho_2\sqrt{\rho_2}}\right)^2 \tag{2.33}$$

The fidelity is bounded by $0 \leq F(\rho_1, \rho_2) \leq 1$. It is equal to unit, if the states are identical, becomes smaller, as the difference between them grows, and turns into zero, if the states are orthogonal. The fidelity between a pure and a mixed state is given by

$$F(|\psi\rangle, \rho) = \sqrt{\langle\psi|\,\rho\,|\psi\rangle} \tag{2.34}$$

The following properties of the fidelity apply to both pure or mixed states: [Jozsa (1994)]

- **Symmetry**: $F(\rho_1, \rho_2) = F(\rho_2, \rho_1)$
- **Invariance**: Fidelity remains unchanged under unitary transformations on the state space, that is, $F(U\rho_1 U^\dagger, U\rho_2 U^\dagger) = F(\rho_1, \rho_2)$.

For two arbitrary density operators, the fidelity and the trace distance are linked by the Fuchs-van de Graaf inequalities as follows [Fuchs and van de Graaf (1999)]

$$1 - F(\rho_1, \rho_2) \leq D(\rho_1, \rho_2) \leq \sqrt{1 - F(\rho_1, \rho_2)^2} \tag{2.35}$$

The two distinguishability measures have diverse operational implications across various aspects of quantum communication, such as evaluating the quality of the transferred states. Regarding security, the proofs often rely on bounding the trace distance between quantum states. Smaller trace distances between states are generally indicative of higher security against eavesdropping attacks, when considering real and ideal states.

2.2.5 Smooth Min-Entropy

Smooth entropies serve as a means to quantify the trade-offs between different resources in information theory. The process of smoothing introduces a positive real parameter ε_s, called the smoothing parameter, which defines the maximum distance between an ideal state and an achievable state. When entropies are employed to characterize operational tasks, the choice of the smoothing parameter determines the level of precision in the analysis. Smaller smoothing parameters result in more conservative entropy estimates. This allows for the consideration of worst-case scenarios. Moreover, smoothing alleviates the influence of statistical fluctuations and improbable events. Finally, it establishes the quantum generalization of both the asymptotic equipartition property and the data processing inequality [Tomamichel et al. (2009)].

The aforementioned concept can now be integrated into the definition of the min entropy. Let ρ_{AB} be a bipartite state on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. The smooth conditional min-entropy was designed to quantify the maximum amount of uniformly distributed and independent randomness, that can be extracted from a correlated random variable. It is defined as the maximum value of the conditional min-entropy $H_{\min}(A|B)$, evaluated for all density operators $\tilde{\rho}$, that are ε_s-close to ρ [Tomamichel et al. (2011)]. It can be considered a strict generalization of the von Neumann entropy. Formally, the smooth min-entropy of A, conditioned on B, is defined as

$$H_{\min}^{\varepsilon_s}(A|B)_\rho = \max_{\tilde{\rho}_{AB} \in \mathcal{B}^{\varepsilon_s}(\rho_{AB})} H_{\min}(A|B)_{\tilde{\rho}} \tag{2.36}$$

where $\mathcal{B}$ stands for an ε_s-ball of states around a set $\mathfrak{S}$ of normalized states, as $\rho \in \mathfrak{S}(\mathcal{H})$.

The smooth min-entropy is given a direct operational meaning by the quantum leftover hash lemma, a fundamental cryptographic proposition. Roughly, the lemma states that a random choice from a secure family $\mathcal{F}$ of hash functions produces output, which is seemingly random and input-independent, even in the presence of partial knowledge about the input. It is an extension of the classical version, with the purpose of identifying whether and how much information Z can be obtained from a random variable X, that is uniform conditioned on some side information E. In this context, side information is interpreted as a potentially leaked sequence to an eavesdropper, who can utilize it to gain information on X. Then, on average over the choices of the hash function $h \sim \mathcal{F}$, the output Z resulting from $h(X)$ is Δ-close from uniform conditioned on E, with

$$\Delta = \frac{1}{2}\sqrt{2^{\ell - H_{\min}(X|E)}} \tag{2.37}$$

Here, ℓ symbolizes the maximum number of uniform random bits that can be extracted from Z. This quantity is upper bounded by $H_{\min}(X|E)$. In the smooth entropy framework, this bound takes the form $H_{\min}^{2\sqrt{\Delta}}(X|E)$ [Tomamichel et al. (2011)]. In applications related to cryptography, ℓ represents, in fact, the length of the final shared secret key.

Chapter 3

Continuous-Variable Systems

3.1 Definition

A quantum system is called a discrete-variable (DV) system, when it can be described by a finite-dimensional Hilbert space. A classic example of this case is the polarization of a single photon. A system described by observables with continuous eigenspectra on an infinite-dimensional Hilbert space is labelled a continuous-variable (CV) system [Weedbrook et al. (2012a)]. A generic continuous-variable system consists of multiple canonical bosonic modes $\kappa = 1, 2, \ldots, \nu$, which correspond to ν quantum harmonic oscillators. These modes are associated with a separable, tensor product Hilbert space

$$\mathcal{H}^{\otimes\nu} = \bigotimes_{\kappa=1}^{\nu} \mathcal{H}_\kappa \tag{3.1}$$

and an equal number ν of pairs of ladder operators $\{\hat{a}, \hat{a}^\dagger\}_{\kappa=1}^{\nu}$.

In continuous-variable systems, the observables are usually represented by operators, that act on the wave function or state vector of the system. Recalling the relations Eq. (1.57) and Eq. (1.58) from the description of multi-mode fields, the canonical operators can be arranged together in a vector of operators $\hat{r}$, as

$$\hat{r} = [\hat{Q}_1, \hat{P}_1, ..., \hat{Q}_\nu, \hat{P}_\nu]^T \tag{3.2}$$

These canonical commutation relations can then be condensed into the form

$$[\hat{r}_\kappa, \hat{r}_{\kappa'}] = i\hbar\mathbf{\Omega}_{\kappa\kappa'} \tag{3.3}$$

where $\kappa, \kappa' = 1, ..., 2\nu$ and the fixed $2\nu \times 2\nu$, invertible, skew-symmetric matrix $\mathbf{\Omega}$ is given by

$$\mathbf{\Omega} = \bigotimes_{\kappa=1}^{\nu} \omega, \quad \omega = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \tag{3.4}$$

The block matrix $\mathbf{\Omega}$ can find multiple uses in linear algebra. For example, a symplectic matrix $\mathbf{S}$ must obey the equality

$$\mathbf{\Omega} = \mathbf{S}^T \mathbf{\Omega} \mathbf{S} \tag{3.5}$$

To better capture states in phase space, the displacement operator can be redefined in terms of the column vector $\hat{r}$ as

$$\hat{D}(\zeta) = e^{i\zeta \mathbf{\Omega} \hat{r}} \tag{3.6}$$

where $\zeta = \{\zeta_Q, \zeta_P\} \in \mathcal{R}^{2\nu}$ acts as a coordinate, ranging over the conjugate phase space. The amount of displacement in phase space is then quantified by the displacement vector $\bar{r} \in \mathcal{R}^{2\nu}$, with $\mathcal{R}$ denoting the set of real numbers, as

$$\bar{r} := \langle \hat{r} \rangle = \mathrm{tr}(\rho \hat{r}) \tag{3.7}$$

3.2 Phase-Space Representation

The states of a continuous-variable system are the set of mode density operators $\hat{\rho}_\kappa$ on the infinite-dimensional Hilbert space $\mathcal{H}^{\otimes \nu}$. This implies that, by means of $\hat{\rho}$, the characterization of states can become exceptionally complicated, especially as the number of modes increases. For this reason, it is reasonable to seek alternative definitions for the field states. Phase-space representation makes an invaluable contribution to the provision of a complete description. This section presents two functions, which act on the phase space and contain all necessary information to completely describe a state.

The first function offering a complete description for a quantum state is the characteristic function. It a complex-valued function, which stands for the expectation value of the displacement operator of Eq. (3.6). With respect to an arbitrary quantum state and the displacement operator, the characteristic function is given by [Weedbrook et al. (2012a)]

$$\varphi(\zeta) = \mathrm{tr}\Big(\hat{\rho} \hat{D}(\zeta)\Big) \tag{3.8}$$

The density matrix is derivable from the characteristic function as [Wang et al. (2007)]

$$\rho = \frac{1}{(2\pi)^\nu} \int d^{2\nu} \zeta \varphi(\mathbf{\Omega}\zeta) \hat{D}^\dagger(\mathbf{\Omega}\zeta) \tag{3.9}$$

The $\hat{D}^\dagger(\mathbf{\Omega}\zeta)$ can also be replaced by $\hat{D}(-\mathbf{\Omega}\zeta)$, as per Eq. (1.46).

The second function, named the Wigner function, allows for the description of quantum systems without the need for a density operator or a wave function [Wigner (1932)]. It is the symplectic Fourier transform of the characteristic function, given by [Weedbrook et al. (2012a)]

$$\mathcal{W}(r) = \int_{\mathcal{R}^{2\nu}} \frac{d^{2\nu}\zeta}{(2\pi)^{2\nu}} e^{-ir^T \mathbf{\Omega} \zeta} \varphi(\zeta) \tag{3.10}$$

where $r \in \mathcal{R}^{2\nu}$ are the eigenvalues of the quadrature operators of $\hat{r}$.

This class of functions is particularly suitable as a phase-space distribution and is capable of providing a descriptive framework for understanding the behavior of quantum systems in continuous-variable settings, without the need of the density matrix. The Wigner function is also known as the Wigner quasiprobability distribution. This is owed to the fact that, while it may be normalized and bounded, it also is a real-valued function, which is unorthodox for probability distributions. This non-positivity property is indicative of the intrinsic quantum nature of the state.

3.3 Covariance Matrix

The covariance matrix (CM) is a mathematical tool, that characterizes the relationships between pairs of continuous variables, capturing both the correlations and uncertainties associated with them. Symbolized by $\mathbf{\Sigma}$, it is a real matrix with an even number of rows and columns $2\nu \times 2\nu$, which satisfies the uncertainty principle as [Simon et al. (1994)]

$$\mathbf{\Sigma} + i\mathbf{\Omega} \geq 0 \tag{3.11}$$

Here, $\mathbf{\Omega}$ is given by Eq. (3.5).

Some useful properties of the covariance matrix are presented below:

- **Symmetry**: The covariance matrix is symmetric, i.e. $\mathbf{\Sigma} = \mathbf{\Sigma}^T$, as $\mathbf{\Sigma}_{ij} = \mathbf{\Sigma}_{ji}$.
- **Hermiticity**: The covariance matrix is Hermitian, i.e. $\mathbf{\Sigma} = \mathbf{\Sigma}^\dagger$, because it is symmetric. The eigenvalues of the covariance matrix are also real.
- **Real Non-negative Diagonal**: All of the diagonal entries are real and non-negative, i.e. $\mathbf{\Sigma}_{ii} \in \mathcal{R}$, $\mathbf{\Sigma}_{ii} \geq 0$, $\forall i \in \{1, \ldots, 2\nu\}$, because they represent variances.
- **Positive Semidefiniteness**: The covariance matrix is positive semidefinite, as $\zeta^T \mathbf{\Sigma} \zeta \geq 0$, $\forall \zeta \in \mathcal{R}^{2\nu}$.
- **Non-negative Trace**: The trace of a covariance matrix is non-negative, because all diagonal entries are non-negative, i.e. $\mathrm{tr}(\mathbf{\Sigma}) = \sum_{i=1}^{2\nu} \mathbf{\Sigma}_{ii} \geq 0$.
- **Non-negative Determinant**: The determinant of such a matrix is non-negative, i.e. $\det(\mathbf{\Sigma}) = \prod_{i=1}^{2\nu} \lambda_i \geq 0$. If all variables are linearly independent, then $\det(\mathbf{\Sigma}) > 0$.

The elements of the covariance matrix represent the covariances $\mathbb{C}$ between specific pairs of variables. In the context of quantum mechanics, the diagonal entries of the matrix represent the variances of the quadrature operators as $\mathbb{V}_{ii} = \mathbb{V}(\hat{r}_i)$ and the off-diagonal elements serve as the mutual covariance functions of the two quadratures. Any arbitrary element of the matrix can be given by [Walls and Milburn (2008)]

$$\mathbf{\Sigma}_{ij} = \frac{1}{2}\langle \hat{r}_i \hat{r}_j + \hat{r}_j \hat{r}_i \rangle - \langle \hat{r}_i \rangle \langle \hat{r}_j \rangle \tag{3.12}$$

3.4 Gaussian States

A special class of continuous-variable states are the Gaussian states, whose characteristic function in multi-mode phase space is Gaussian. Their phase-space distribution function also follows a Gaussian form. All Gaussian states are minimum uncertainty states. A pure state is Gaussian if and only if its Wigner function is non-negative [Hudson (1974)].

Typically, Gaussian states are mathematically defined using characteristic functions. A possible representation is the following [Wang et al. (2007)]:

$$\varphi(\zeta) = \exp\left(-\frac{1}{4}\zeta^T \mathbf{\Sigma}\zeta + i\bar{r}^T\zeta\right) \tag{3.13}$$

Here, the displacement vector $\bar{r}$ and the covariance matrix $\mathbf{\Sigma} \in \mathcal{R}^{2\nu}$ act correspondingly to the first and second statistical moments of Gaussians. The first moment is given by Eq. (3.7) and the second one is given by Eq. (3.12). This means that Gaussian states can be fully described by the mean value and the variance of the operators of $\hat{r}$, displayed in Eq. (3.2).

The characteristic function of a Gaussian state is a Gaussian function, formulated as

$$\varphi(\zeta) = \exp\left[-\frac{1}{4}\zeta^T \mathbf{\Omega\Sigma\Omega}^T\zeta - i(\mathbf{\Omega}\bar{r})^T\zeta\right] \tag{3.14}$$

The same applies to the Wigner function of a Gaussian state. The result of Gaussian integration is [Wang et al. (2007)]

$$\mathcal{W}(\zeta) = \frac{1}{\pi^\nu\sqrt{\det(\mathbf{\Sigma})}}\exp\left[-(\zeta-\bar{r})^T\mathbf{\Sigma}^{-1}(\zeta-\bar{r})\right] \tag{3.15}$$

The study of the properties of Gaussian states is especially significant from a quantum optical perspective, because coherent states, squeezed states and thermal states are all subdivisions of Gaussian states. The characteristic function of a coherent state is given by [Wang et al. (2007)]

$$\varphi_\alpha(\zeta_Q,\zeta_P) = \exp\left[-\frac{1}{4}(\zeta_Q^2+\zeta_P^2) + \frac{i\zeta_Q(\alpha+\alpha^*)}{\sqrt{2}} + \frac{i\zeta_P(\alpha-\alpha^*)}{\sqrt{2}}\right] \tag{3.16}$$

Gaussian states, especially coherent states, are advantageous in practical scenarios and thus highly relevant in experimental studies, as they are easy to generate with current optical technologies. It must be noted, that Fock states are non-Gaussian states.

Covariance matrices represent a convenient solution, when it is required to understand the behavior of multi-mode Gaussian states. An important property of the covariance matrix $\mathbf{V}$ of a Gaussian state is its connection with diagonal matrices. According to Williamson's theorem, there exists a symplectic transformation for every positive-definite real matrix of even dimension, that diagonalizes such a matrix [Williamson (1936)].

Applying a symplectic map $\mathbf{S}$ to a κ-mode covariance matrix $\mathbf{V}$ returns the relation

$$\mathbf{V} = \mathbf{S}\mathbf{V}^{\oplus}\mathbf{S}^{T}, \quad \mathbf{V}^{\oplus} = \bigoplus_{\kappa=1}^{\nu} v_{\kappa}\mathbf{I} \tag{3.17}$$

The $\mathbf{S}$ matrix can be computed using [Pereira et al. (2021)]. The covariance matrix of the multi-mode Gaussian state can be written as [Ferraro et al. (2005)]

$$\mathbf{V} = \begin{bmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^{T} & \mathbf{B} \end{bmatrix} \tag{3.18}$$

The case of two bosonic modes is of particular interest. Two-mode Gaussian states can be represented by a 4×4 covariance matrix, where $\mathbf{A} = \mathbf{A}^{T}$, $\mathbf{B} = \mathbf{B}^{T}$ and $\mathbf{C}$ are 2×2 matrices, such that $\mathbf{A}, \mathbf{B}, \mathbf{C} \in \mathcal{R}$. Williamson's normal form is given by

$$\mathbf{V}^{\oplus} = (v_{-}\mathbf{I}) \oplus (v_{+}\mathbf{I}) \tag{3.19}$$

The eigenvalues v of the symplectic matrix are called symplectic eigenvalues. Through them, it is possible to determine the degree of squeezing, entanglement and purity of a Gaussian state. For the $v_{\pm}$ case of Eq. (3.19), they are given by

$$v_{\pm} = \sqrt{\frac{\Sigma \pm \sqrt{\Sigma^{2} - 4\det\mathbf{V}}}{2}} \tag{3.20}$$

where the determinant of $\mathbf{V}$ and Σ are global symplectic invariants. Σ is found by

$$\Sigma = \det\mathbf{A} + \det\mathbf{B} + 2\det\mathbf{C} \tag{3.21}$$

The uncertainty principle is then satisfied, when [Pirandola et al. (2009)]

- $\mathbf{V} > 0$,
- $\det\mathbf{V} \geq 1$ and
- $\Sigma \leq 1 + \det\mathbf{V}$.

Two-mode states of Eq. (3.18) can explicitly be described by a covariance matrix in the so-called standard form

$$\mathbf{V} = \begin{bmatrix} a\mathbf{I} & \mathbf{C} \\ \mathbf{C} & b\mathbf{I} \end{bmatrix}, \quad \mathbf{C} = \begin{bmatrix} c_{+} & 0 \\ 0 & c_{-} \end{bmatrix} \tag{3.22}$$

where $a, b, c_{+}, c_{-} \in \mathcal{R}$. This form holds true for any two-mode system up to Gaussian local operations and classical communication (LOCC). For the case of pure states, which satisfies $c_{+} = -c_{-}$ [Serafini et al. (2004)], the symplectic eigenvalues can be found using the matrix correlations

$$v_{\pm} = \frac{\sqrt{(a+b)^{2} - 4c^{2}} \pm (b-a)}{2} \tag{3.23}$$

One of the most useful bipartite Gaussian states, that can be utilized to demonstrate the calculations of a covariance matrix, is the two-mode squeezed vacuum (TMSV) state. Because of entanglement, the properties of one mode are inversely related to the properties of the other mode. When such a state has zero mean and variance μ, it is described by the covariance matrix

$$\mathbf{V}_{\mathrm{TMSV}}(\mu) = \begin{bmatrix} \mu\mathbf{I} & \sqrt{\mu^2-1}\mathbf{Z} \\ \sqrt{\mu^2-1}\mathbf{Z} & \mu\mathbf{I} \end{bmatrix} \tag{3.24}$$

where $\mathbf{Z}$ is the Pauli z-matrix. The TMSV state will prove instrumental in describing eavesdropper attacks.

The von Neumann entropy of a multi-mode Gaussian state is described in terms of the symplectic eigenvalues of its covariance matrix. The spectrum of the symplectic eigenvalues $\{v_1, \ldots, v_\nu\}$ can be instead calculated as the ordinary eigenvalues of the modulus of the matrix

$$\tilde{\mathbf{V}} = |i\mathbf{\Omega}\mathbf{V}| \tag{3.25}$$

Note that the matrix $\tilde{\mathbf{V}}$ is Hermitian and can be brought into a diagonal form by a unitary transformation. The von Neumann entropy is then calculated by

$$S(\rho) = \sum_{\kappa=1}^{\nu} G(v_\kappa) \tag{3.26}$$

where G stands for the bosonic entropic function

$$G(v) = \frac{v+1}{2}\log_2(\frac{v+1}{2}) - \frac{v-1}{2}\log_2(\frac{v-1}{2}) \tag{3.27}$$

A measurement on a single mode of a κ-mode Gaussian state will modify the Gaussian state of the remaining modes, depending on their correlations to the measured one. Consider the scenario, where a measurement is carried out on a mode B, while there exist $\kappa - 1$ other leftover modes A. The correlations between the modes A and B are captured by the matrix $\mathbf{C}$. The effect of this partial measurement of B on the remaining modes is determined by the chosen type of detection, i.e. homodyne or heterodyne, as

$$\mathbf{V}_{A|B}^{\mathrm{hom}} = \mathbf{A} - \mathbf{C}(\mathbf{\Pi}_{Q,P}\mathbf{B}\mathbf{\Pi}_{Q,P})^{-1}\mathbf{C}^T \tag{3.28}$$

$$\mathbf{V}_{A|B}^{\mathrm{het}} = \mathbf{A} - \mathbf{C}(\mathbf{B}+\mathbf{I})^{-1}\mathbf{C}^T \tag{3.29}$$

Here, the $^{-1}$ operation symbolizes the pseudo-inverse, because the result of $\mathbf{\Pi}\mathbf{B}\mathbf{\Pi}$ is singular [Weedbrook et al. (2012a)]. Considering the instance of homodyne detection, the measurements of the quadrature components Q and P are respectively given by $\mathbf{\Pi}_Q = \mathrm{diag}(1,0)$ and $\mathbf{\Pi}_P = \mathrm{diag}(0,1)$.

Chapter 4

Continuous-Variable Quantum Key Distribution

Having laid the groundwork by demonstrating necessary concepts, it is time to delve into the topic of quantum key distribution. The chapter starts with a brief historical note and continues by explaining sigificant notions and properties, which govern this unique type of key exchange. It also gives an initial description of the processes followed, presents potential attacks and addresses realistic effects and parameters, which can affect the quality and security of the communications.

4.1 Introduction

The objective of quantum key distribution (QKD) is to establish a random secret key between two authenticated parties over a potentially insecure quantum channel [Pirandola et al. (2020)]. The security of QKD is derived from two laws of quantum mechanics: the uncertainty principle and the no-cloning theorem [Wootters and Zurek (1982)]. The first QKD protocol was introduced by Bennett and Brassard in 1984 and was given the name BB84 accordingly [Bennett and Brassard (1984)]. In this version, single photons are successively transmitted through the channel and the information is encoded on the polarization of a photon, which is a property of discrete-variable systems. The BB84 protocol ushered in the period of discrete-variable quantum key distribution (DV-QKD), whose security has been since extensively studied [Scarani and Renner (2008), Scarani et al. (2009), Pirandola et al. (2020), Bunandar et al. (2020)].

Later on, a more modern family of protocols emerged, in which a continuous beam of light is emitted by the transmitter. The continuous nature of light gave birth to continuous-variable quantum key distribution (CV-QKD). Here, information is encoded by modulating the amplitude and phase of the electromagnetic wave in the position and

momentum quadratures of a bosonic mode. The first CV-QKD protocol was introduced in 1999 [Ralph (1999)]. Shortly after, two more related papers emerged in 2000 [Hillery (2000), Reid (2000)]. CV-QKD with Gaussian modulation was proposed for the first time in 2001 [Cerf et al. (2001)]. However, all of these models utilized discrete encoding of squeezed states of light. The first Gaussian-modulated CV-QKD protocol with coherent states was brought forward in 2002 [Grosshans and Grangier (2002)] and has become the de facto standard of CV-QKD. This work, named GG02 after its creators, adopted homodyne detection, as well as the direct reconciliation approach during the information reconciliation stage. Reverse reconciliation was first implemented in 2003 [Grosshans et al. (2003)], while heterodyne detection, initially called no-switching, was presented in 2004 [Weedbrook et al. (2004)]. Both protocols were adopted expeditiously by several works, which provided improved methods and performances [Van Assche et al. (2004), Lance et al. (2005), Sharma et al. (2006)]. All aforementioned protocols assume the participation of only one sender in the quantum transmission stage and are hence categorized as one-way protocols; the first two-way protocol, where transmission between the legitimate parties is bidirectional, was introduced in 2008 [Pirandola et al. (2008a)]. At the same time, the suitability of noisy coherent states, i.e. thermal states, was assessed by [Filip (2008)] and the security of such states was subsequently proven in realistic circumstances [Usenko and Filip (2010)]. This paved the way for extending CV-QKD to longer wavelengths, such as the microwave region, which is appropriate for short-range applications [Papanastasiou et al. (2018)].

Shortly after its conception, CV-QKD achieved secret key generation at the distance of 25km [Lodewyck et al. (2007)]. While the initial results were encouraging, the lack of reconciliation methods, specializing in low signal-to-noise conditions, limited research at longer distances. By combining the newfound multidimensional reconciliation technique [Leverrier et al. (2008)] with cutting-edge LDPC codes [Richardson and Urbanke (2002)], the secure distance was further extended to 120 km [Jouguet et al. (2011)] and 80 km [Jouguet et al. (2013)]. Nevertheless, the family of continuous-variable protocols is more robust in short-range applications, when compared to the family of discrete protocols. There has also been recent progress in free-space, microwave, Earth-to-satellite and chip-based QKD applications, both from a theoretical and experimental perspective [Hosseinidehaj and Malaney (2017), Günthner et al. (2017), Zhang et al. (2019), Zhang et al. (2021), Li et al. (2023)].

The most important advantages of CV-QKD over DV-QKD are presented below:

- **High Secure Key Rate**: Situationally higher secret key rates, especially when deployed in dense wavelength division multiplexing networks [Kumar et al. (2015)]. The performance of CV-QKD is close to the PLOB bound, which the fundamental limit of point-to-point quantum communications [Pirandola et al. (2017)].
- **Efficient and Cost-Effective Detection**: Efficient detection using homodyne receivers instead of single photon counters [Laudenbach et al. (2018)].

- **Compatibility**: Compatibility with existing telecommunications equipment, as the transceivers are similar to those in classical coherent high-speed communication systems [Orieux and Diamanti (2016), Kikuchi (2016)]. Deployment of dedicated dark fibres is not required [Laudenbach et al. (2018)].

This research is going to employ coherent states for state preparation. Coherent-state protocols are generally preferred over squeezed-state protocols, because of the technological challenges associated with generating squeezed light [Laudenbach et al. (2018)]. Among the Gaussian states, coherent ones are the easiest to produce in a laboratory; this paved the way for indoor and outdoor experimentation. Besides the foundational principles of state collapse upon measurement and the no-cloning theorem, which are integral to all QKD protocols, the provable security of coherent-state protocols stems from the non-orthogonality of coherent states.

The remainder of the thesis will focus exclusively on Gaussian-modulated coherent-state one-way protocols under fiber communications.

4.2 Secret Key Rate and Reconciliation

The most desirable attribute in quantum key distribution is the secret key rate, which is the length of securely shareable key per channel use [Watanabe et al. (2008)]. The security of any QKD protocol is guaranteed, when a rigorous security analysis certifies that the protocol produces a positive secret key rate. The simplest way to examine the behavior of a protocol is assuming the generation of an infinite number of signal states. In this case, the key rate is the outcome of three quantities:

- the **mutual information**, which represents the shared amount of information during the stage of information reconciliation,
- the **Holevo bound**, which is the upper estimate of the amount of information gained by the attacker through the interaction with the quantum channel and
- the **reconciliation efficiency**, which is the efficiency that an error-correcting code with a given code rate achieves, under a certain value of the mutual information.

The last quantity plays a crucial role during the information reconciliation stage, where the legitimate parties attempt to make their data similar by removing the corruption caused by noise and loss. In a CV-QKD protocol, there exist two ways to realize information reconciliation: either by direct reconciliation, where Bob corrects the errors in the key with respect to Alice's sequence, or reverse reconciliation, where Alice performs error correction with the assistance of the data in Bob's possession. Regardless of the

chosen method, the entity performing error correction receives the necessary data from the other legitimate entity via the authenticated classical channel. A direct reconciliation scheme is safe to implement only in short-distance CV-QKD protocols. This is owed to the fact that the protocol needs to be safe against a beam-splitting attack, where it has been shown that the upper bound for the transmission losses is 3dB. Considering that the standard loss in 1550nm optical fibers is 0.2dB/km, the typical length would be around 10km [Grosshans and Grangier (2002)]. Therefore, error-correction methods that utilize reverse reconciliation are considerably more widespread in existing literature.

Under both reconciliation types, the reconciliation efficiency β is measured by

$$\beta = \frac{R_{\text{code}} \log_2 |\mathcal{A}|}{I_{AB}}, \quad \beta \in [0, 1] \tag{4.1}$$

where R_{code} stands for the error-correction code rate, I_{AB} for the mutual information between Alice and Bob and $|\mathcal{A}|$ for the alphabet size of the code, which typically is an integer power of 2. The range of β is $0 \leqslant \beta \leqslant 1$, where the minimum value stands for a lack of extracted information and the maximum value indicates perfect reconciliation [Weedbrook et al. (2012a)]. Given knowledge of β, the secret key rate in the asymptotic limit R_{asy} under direct and reverse reconciliation is respectively calculated as

$$R_{\text{asy}}^{\text{DR}} = \beta I_{AB} - \chi_{AE} \tag{4.2}$$

$$R_{\text{asy}}^{\text{RR}} = \beta I_{AB} - \chi_{BE} \tag{4.3}$$

where χ is the Holevo bound between Eve and either Alice or Bob. The key rate is measured in either bits per channel use or bits per second. Evidently, to achieve the maximum possible key rate, the key rate coefficient needs to be maximized. One way to achieve this is by choosing an appropriate reconciliation scheme, based on the level of the channel noise and loss.

The asymptotic key rate is a primary quantity of interest, when the performance of a CV-QKD protocol is examined. However, the secret key rate, which truly defines and bounds the security of the protocol, depends not only on the noise and loss in the communication channel, but also on a series of data-processing steps, needed for transforming the shared correlations into a final string of secret bits. Such a quantity will be analyzed in detail in a later section.

4.3 Noise and Loss

The performance and security of a CV-QKD system is hindered by several limiting factors, most of which related to imperfect equipment and channel flaws. The imminent corruption of the outgoing signal results in the disassociation of the sequences of the transmitter and receiver. The most important sources of noise and loss, that are linked with CV-QKD protocols, are catalogued in this section.

- **Transmissivity**: Propagation of light requires a quantum channel, which conventionally is an optical fiber. Fibers are characterized by optical attenuation, which is the result of absorption, scattering and structural flaws. The attenuation of the fiber is determined by the wavelength. A fiber of length L and attenuation ϑ generates a channel of transmissivity T, which determines its loss. As the channel length increases, so does the loss; this causes the performance of the protocol to severely deteriorate at longer distances. Typically, channel losses are modelled using a beam splitter.

- **Coupling Losses**: The channel losses can originate not only from the fiber itself, but also from a faulty network setup. Misalignment between fibers happens, when their cores overlap or when there is a gap of nontrivial distance between them. The losses from such incidents are referred to as coupling losses. For the remainder of the thesis, the transmissivity and the coupling losses will be merged into the variable of the former.

- **Detection Efficiency**: The detection equipment on the receiver side has non-unit efficiency. Therefore, the imperfect detection adds a diminishing factor η to the transmission. Detection efficiency is considered a source of trusted noise, because it can be calibrated before the commencement of the protocol. As a result, the noise that originates from the detection is not attributed to the eavesdropper.

- **Electronic Noise**: The electronic noise υ_{el} is owed to disturbances, that occur in electronic components and circuits of the setup. Like the setup efficiency, this type of noise is regarded as trusted and is unrelated to the presence of an eavesdropper.

- **Vacuum Noise**: Also known as shot noise, the vacuum noise V is a fundamental noise, inherent in quantum systems and associated with the uncertainty principle. In shot-noise units (SNU), the variance of the vacuum noise is equal to 1.

- **Excess Noise**: The excess noise ξ encompasses various noise sources. One of the most common sources originates from Alice's state preparation and modulation and is called preparation noise. It can emanate from a noisy laser or an imperfect optical modulator. Other examples include Raman scattering, quantization and phase fluctuations. Assuming all excess noise sources are stochastically independent from one another, they can be summed up, due to the additivity property of their variances [Laudenbach et al. (2018)].

- **Thermal Noise**: Environmental thermal effects arise from interactions between a quantum system and its surroundings at non-zero temperatures. Such interactions include the thermal motion of particles, which leads to random fluctuations in the electromagnetic field [Meyers (2002)], or the emitted and absorbed thermal electromagnetic radiation between the system and the environment [Huang (1987)]. This type of noise is known as thermal noise ω and the decoherence induced by it can impact both the transmission and detection of quantum signals.

As in other signal-related topics, the measure of the signal power against the noise power is commonly given by the signal-to-noise-ratio (SNR). It is a crucial quantity, used to assess the quality of the exchanged signals. All of the aforementioned noise and loss sources directly affect the SNR. Therefore, maximizing the SNR can happen by minimizing the effects of these sources. The higher the SNR is, the better the chances of the communicating parties establishing a secret key.

4.4 Gaussian-Modulated Coherent-State Protocols

The scenario that is about to be presented is commonly referred to as a prepare-and-measure setup (P&M). Two legitimate parties are involved, namely Alice and Bob, whose aim is to establish a secret key by communicating over a potentially insecure quantum channel. Alice prepares quantum states, on which she encodes information, and transmits them through a public quantum channel. Bob receives the states and measures them. This process is repeated several times, until a key is deemed sufficient. Another party, Eve, is trying to intercept the quantum channel, in order to obtain information about the secret key. To ensure fidelity and security, Alice and Bob perform a series of postprocessing stages to compare and refine their results through a public classical authenticated channel. A summary is provided for every stage of the protocols.

4.4.1 State Preparation, Transmission and Measurement

Alice begins by employing amplitude and phase modulators to displace vacuum states, preparing a coherent-state sequence $|\alpha_1\rangle, \dots |\alpha_j\rangle, \dots, |\alpha_N\rangle$ of the form

$$|\alpha_j\rangle = |Q_j + iP_j\rangle \tag{4.4}$$

where $Q_j = |\alpha_j| \cos\theta$ and $P_j = |\alpha_j| \sin\theta$. The amount of displacement is determined by the quadrature components Q and P, which are drawn from two i.i.d. random variables $\mathcal{Q}$ and $\mathcal{P}$. These follow a zero-mean Gaussian distribution $\mathcal{G}$ with variance σ^2

$$\mathcal{Q} \sim \mathcal{P} \sim \mathcal{G}(0, \sigma^2) \tag{4.5}$$

With respect to the distributions in the above relation, the mean photon number of the state ensemble is

$$\bar{\mathsf{n}} := \langle \mathsf{n} \rangle = \langle \mathcal{Q}^2 \rangle + \langle \mathcal{P}^2 \rangle = 2\sigma^2 \tag{4.6}$$

After preparation, Alice transfers the signal states to Bob through a public insecure quantum channel, which is generally characterized by two parameters: the transmissivity T and the excess noise ξ. The signal inevitably gets corrupted during transmission.

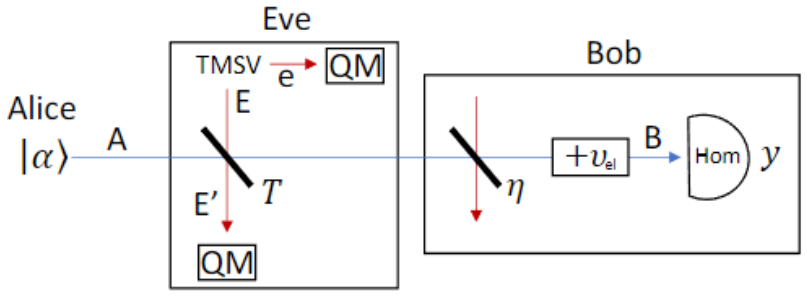

Figure 4.1: Structure of a CV-QKD protocol with (Gaussian-modulated) coherent states, considering a receiver that might have trusted levels of inefficiency and electronic noise. In the middle, the thermal-loss channel is induced by the collective Gaussian attack of Eve, who uses a beam splitter with transmissivity T and a TMSV state with variance ω. Eve stores her outputs in quantum memories, intending to measure them later. The optimal performance of the measurements is bounded by the Holevo bound. [Mountogiannakis et al. (2022a)]

When the signal reaches Bob, he uses homodyne or heterodyne detection to measure one or both of the quadratures. The approaches are described in Sec. 1.7. During the former method, Bob randomly selects with equal probability for every state only one of the Q and P quadratures. He then classically communicates to Alice the quadrature he measured, so that the other quadrature is discarded, along with its value. The process of reconciling the measurement bases is known as key sifting. In the latter detection method, Alice and Bob utilize both bases. Consequently, the sifting step is skipped.

4.4.2 Parameter Estimation

After the transmission of a series of states is complete, Alice and Bob will reveal and compare a random subset of their data. Through this comparison, they can estimate the values of channel parameters, which typically involve the transmissivity $\widehat{T}$ and the excess noise $\widehat{\xi}$ or its variance $\widehat{\Xi}$, under the maximum-likelihood estimation (MLE) method. Using these parameters and with the help of the covariance matrix, they are able to subsequently compute an approximation of their mutual information $\widehat{I}_{AB}$ and Eve's Holevo bound $\widehat{\chi}$. If $\widehat{\chi} > \beta\widehat{I}_{AB}$, the presence of an eavesdropper on the channel is strongly suspected and, consequently, the protocol is aborted. Otherwise, the protocol proceeds to the information reconciliation stage. The disclosed states used in the parameter estimation stage do not partake in the computation of the key rate and are discarded.

Depending on the desirable level of security, the parties may also compute lower bounds for the channel estimators, which are called worst-case estimators. [Leverrier et al. (2010), Ruppert et al. (2014)]. Via the worst-case estimators, an overestimation of the Holevo bound χ_M is identified, which leads to a more conservative approach.

It is worth mentioning, that there exist instances in literature, where the parameter estimation stage occurs after information reconciliation [Wang et al. (2019)]. Regardless, parameter estimation is far more widely implemented before error correction takes place.

4.4.3 Preprocessing

Preprocessing includes every task necessary to bring the resulting data from the quantum transmission in an appropriate form for information reconciliation. These tasks are executed in private, meaning that they are not associated with any information leakage to the eavesdropper. Generally, only the portion of the states, that have survived the parameter estimation stage, is affected by preprocessing. The methods followed depend on various factors, such as the chosen protocol or the signal-to-noise ratio.

In CV-QKD, it is requisite to convert a continuous variable into a discrete one, in order to further process it. Such a technique is referred to as discretization, digitization or quantization. There are various discretization schemes, which directly affect the error-correction performance and the key rate. Another typical process of this stage is the normalization of the data, where the sequences are normalized by a certain factor [Milisevic (2017), Zhou et al. (2019)].

4.4.4 Information Reconciliation

Having estimated the noise and loss parameters and having appropriately processed their sequences, Alice and Bob are now in a position, where they have all necessary components to start forming a secret key. As previously mentioned in Sec. 4.2, the crucial information reconciliation stage is where they correct the errors caused by the signal corruption, by means of either direct reconciliation or reverse reconciliation.

During the stage, they need to randomly announce part of the information through the public channel. It is assumed that Eve observes all classical communication processes. Therefore, the amount of leaked information leak_{EC} in the error correction process must be calculated. This amount quantifies part of Eve's knowledge on the key and will be eliminated in the final protocol stage.

Each reconciliation technique works best for a certain range of the SNR. For the low SNR regime, particularly suitable is the multidimensional reconciliation scheme, where a virtual binary-input additive white Gaussian noise (BIAWGN) channel is constructed through rotating the Gaussian variables of Alice and Bob [Leverrier et al. (2008), Jouguet et al. (2013), Wang et al. (2019), Zhang et al. (2020)]. For higher SNR values, the most commonly implemented scheme is slice reconciliation [Van Assche et al. (2004), Lodewyck et al. (2007), Jouguet et al. (2014), Wang et al. (2017), Wen et al. (2021)].

To decode the data, LDPC codes are massively more implemented than any other type of codes [Xu et al. (2022)]. The SNR is again a predominant factor, when determining the rate of the code. High losses generally require low code rates, while higher values of the SNR can manage error correction with higher rates. A family of LDPC codes, which can provide efficient error correction combined with high reconciliation efficiency even in the low SNR regime, are multi-edge type (MET) LDPC codes [Richardson and Urbanke (2002), Jouguet et al. (2011), Milicevic et al. (2018), Wang et al. (2019), Mani et al. (2021)]. Decoding is typically performed by an iterative belief propagation algorithm, such as the sum-product algorithm or the min-sum algorithm [Lodewyck et al. (2007), Milisevic (2017), Gümüs et al. (2021)]. These algorithms are highly effective, when they are coupled with LDPC codes.

After error correction, the blocks that were not decoded are discarded. The party that performed the correction hashes every successfully decoded block, using a hash function h, which is chosen uniformly at random from a family $\mathcal{F}$ of universal hash functions [Tsurumaru and Hayashi (2013)]. The resulting output is transmitted over the classical channel to the other party, who hashes their own corresponding blocks with the same hash function family. The digests are then compared, in order to verify their equality. There are three possible outcomes from this verification process:

- the digests are equal, which means that the corresponding decoded blocks proceed to next stage,
- the digests are unequal, which results in the blocks being discarded, or
- the digests collide.

A hash collision occurs when two different inputs are hashed with the same hash function and produce the same hash value. Therefore, Alice and Bob will be tricked into believing, that their original sequences were identical. The most suitable choice to minimize the chance of such an event is the class of universal hash functions, because they guarantee a minimal number of collisions. More specifically, for all possible transformations from $\mathcal{A}$ to $\mathcal{B}$, the probability of a collision is not larger than $\frac{1}{\mathcal{B}}$ [Carter and Wegman (1979)].

4.4.5 Privacy Amplification

After the verification stage, Alice and Bob concatenate their matching hash outputs into bit strings, which are identical with a very high probability. Nonetheless, Eve still has partial knowledge of the key. To eliminate Eve's knowledge, Alice and Bob proceed to the privacy amplification stage, where, again, a hash function from family of universal hash functions $h \sim \mathcal{F}$ is usually employed to compress to their shared strings. This way, they extract a random and secret key Υ, which can be used for secure communications. Privacy amplification is enabled by the leftover hash lemma, described in Sec. 2.2.5.

4.5 Measurement-Device-Independent Quantum Key Distribution

In addition to the Gaussian-modulated coherent-state protocols, another protocol is presented in this section. While not as widely reviewed in existing literature as the aforementioned, it exhibits its own distinct advantages, which can be useful under particular circumstances.

While the homodyne and heterodyne protocols demonstrably provide security, the equipment used in these cases is ideally considered to be absolutely trusted. In reality, they are still vulnerable to side-channel attacks. Potential side-channel attacks include the wavelength attack [Huang et al. (2013)], the local oscillator calibration attack [Ma et al. (2013)] and the detector saturator attack [Qin et al. (2016)]. All of these are associated with the adversary taking control over the preparation or detection mechanisms.

A more modern form of QKD, named measurement-device-independent (MDI) QKD, was introduced to mitigate these issues. It was first presented as a general concept in QKD [Braunstein and Pirandola (2012), Lo et al. (2012)], but was later reformulated especially for continuous-variable systems [Pirandola et al. (2015)]. It protects against side-channel attacks by providing an intermediate relay, which performs the detection and creates the secret correlations, instead of the parties. The relay is factored in the computations for the channel noise, which means it is regarded as untrusted, potentially controlled by the adversary. The detection outcomes are classically transmitted to the users, who follow these correlations to establish a secret key, independently of the device used for the measurements. The existence of an intermediate relay makes the MDI configuration the basis for constructing multi-user applications [Papanastasiou et al. (2018), Ottaviani et al. (2019), Papanastasiou et al. (2023), Appendix VII]. This setup can potentially be extended to QKD networks [Ghalaii et al. (2022)]. The CV-MDI protocol has also been implemented experimentally [Pirandola et al. (2015), Wang et al. (2018), Hajomer et al. (2023)].

4.6 Eavesdropping Attacks

The security of any QKD protocol hinges significantly on the potential technological capabilities under the possession of the eavesdropper. With regard to these capabilities, the possible eavesdropping attacks an adversary can perform on a CV-QKD system can be categorized into three groups: individual attacks, collective attacks and coherent attacks. For every type of attack, the security of the system should be examined for both realistic block sizes and at the asymptotic limit. The attacks, as well as references for their security analysis, are listed below.

- **Individual attack**: In an individual attack scenario, Eve executes an i.i.d. attack, which involves preparing a set of individual and identical quantum systems, every one of which interacts individually with one signal pulse in the quantum channel. The state transmitted from Alice to Bob can then be treated as an i.i.d. state, such as $\rho_{A^N B^N} = \tilde{\rho}_{AB}^{\otimes N}$, where N signifies the number of transmitted signals. Assuming she possesses a quantum memory, she stores the output ensemble there. After the end of the sifting step, she performs an individual measurement on all states, independently from one another. The first proof for individual attacks against coherent-state protocols was introduced by [Grosshans and Cerf (2004)].

- **Collective attack**: Similarly to the individual attack, Eve initiates an i.i.d. attack with separable states. However, in a collective attack, a collective measurement is performed on the stored states. This measurement takes place only after the classical postprocessing phase. The maximum amount of information extracted from a collective attack is determined by the Holevo bound.

  Regarding GMCS CV-QKD protocols, it has been proven that the optimal class of collective attacks are Gaussian attacks, where the operation of the eavesdropper corresponds to a Gaussian map [Leverrier and Grangier (2010), Pirandola et al. (2020)]. The security of CV-QKD against collective Gaussian attacks was shown independently by [Navascués et al. (2006)] and by [Garcia-Patrón and Cerf (2006)]. Collective Gaussian attacks have also been fully characterized by [Pirandola et al. (2008b)]. The security against such attacks has also been extended to the finite-size effects regime [Leverrier et al. (2010)]. Security analyses against general collective attacks have been realized in the composable security framework for the homodyne and heterodyne protocols [Leverrier (2015), Pirandola (2021a), Pirandola (2022)], as well as for the CV-MDI protocol [Papanastasiou et al. (2017)]. The most notable representation of a collective Gaussian attack is the entangling cloner attack, which is discussed in the next section.

- **Coherent attack**: As individual and collective attacks somewhat restrict Eve's ability, a QKD protocol is considered unconditionally secure, when it is secure under coherent attacks. This is because such attacks do not limit the ability of eavesdroppers, thereby being the most general attacks. In a coherent attack, Eve prepares an optimal global ancillary state, whose modes interact with the signal pulses in the channel, employing all possible unitary transformations and measurements. The results are then stored in the quantum memory. Likewise to a collective attack, the collective measurement is performed after postprocessing. The first security analysis for coherent attacks was presented by [Garcia-Patrón and Cerf (2006)]. Soon after, [Renner and Cirac (2009)] provided a proof for asymptotic-limit coherent attacks by reducing them to collective attacks under certain circumstances. It was later shown that even finite-size coherent-attack security, specifically for the heterodyne protocol, is provided by simply establishing security against collective Gaussian attacks [Leverrier (2017)].

4.7 The Entangling Cloner Attack

The entangling cloner attack is the modelization of a collective Gaussian attack. In such an attack, Eve uses an entangling cloner to create two copies of Alice's quantum state. In reverse reconciliation, she keeps one for herself and sends the other one to Bob [Grosshans et al. (2003)]. This way, she avoids adding extra noise on the data. The analysis of the attack ultimately leads to the derivation of the Holevo bound between Bob and Eve, which is essential in calculating the key rate. The representation of the attack primarily from [Laudenbach et al. (2018)] and secondarily from [Weedbrook et al. (2012b)] is closely followed in this section.

Consider the mutual state ρ_{AB} of Alice and Bob. This is a TMSV state with zero mean and variance μ, described by the covariance matrix $\mathbf{V}_{AB}$ of Eq. (3.24). Similarly, Eve also generates a TMSV state for her modes E_1 and E_2 with zero mean and variance ω, whose covariance matrix is given by

$$\mathbf{V}_{E_1E_2} = \begin{bmatrix} \omega\mathbf{I} & \sqrt{\omega^2-1}\mathbf{Z} \\ \sqrt{\omega^2-1}\mathbf{Z} & \omega\mathbf{I} \end{bmatrix} \tag{4.7}$$

The direct sum of the covariance matrices of the two EPR states is calculated, creating the covariance matrix of the total state

$$\mathbf{V}_{ABE_1E_2} = \mathbf{V}_{AB} \oplus \mathbf{V}_{E_1E_2} = \begin{bmatrix} \mu\mathbf{I} & \sqrt{\mu^2-1}\mathbf{Z} & 0 & 0 \\ \sqrt{\mu^2-1}\mathbf{Z} & \mu\mathbf{I} & 0 & 0 \\ 0 & 0 & \omega\mathbf{I} & \sqrt{\omega^2-1}\mathbf{Z} \\ 0 & 0 & \sqrt{\omega^2-1}\mathbf{Z} & \omega\mathbf{I} \end{bmatrix} \tag{4.8}$$

Eve replaces the quantum channel with a noiseless channel, i.e. $\omega = 1$, making it a pure-loss channel. The new channel is modelled by a beam splitter with transmissivity $T \in [0,1]$ and excess noise given by

$$\xi = \frac{1-T}{T}(\omega - 1) \tag{4.9}$$

The beam splitter mixes Bob's mode B with one of Eve's modes E_1. Eve keeps one of the outputs to herself and passes the other one to Bob. The beam splitter operator from Eq. (1.65) acts on the modes B and E_1 of the state above. It is represented by

$$\mathbf{S}_{ABE_1E_2} = \mathbf{I}_A \oplus \mathbf{S}_{BE_1} \oplus \mathbf{I}_{E_2} = \begin{bmatrix} \mathbf{I} & 0 & 0 & 0 \\ 0 & \sqrt{T}\mathbf{I} & \sqrt{1-T}\mathbf{I} & 0 \\ 0 & -\sqrt{1-T}\mathbf{I} & \sqrt{T}\mathbf{I} & 0 \\ 0 & 0 & 0 & \mathbf{I} \end{bmatrix} \tag{4.10}$$

The beam splitter operator can enact a symplectic transformation on the total state of Eq. (4.8), producing [Laudenbach et al. (2018)]

$$\mathbf{V}'_{ABE_1E_2} = \mathbf{S}_{ABE_1E_2}\mathbf{V}_{ABE_1E_2}\mathbf{S}^T_{ABE_1E_2} = \begin{bmatrix} \mu\mathbf{I} & \sqrt{T(\mu^2-1)}\mathbf{Z} & -\sqrt{1-T}\sqrt{(\mu^2-1)}\mathbf{Z} & 0 \\ \sqrt{T(\mu^2-1)}\mathbf{Z} & (T\mu+[1-T]\omega)\mathbf{I} & \sqrt{T(1-T)}(\omega-\mu)\mathbf{I} & \sqrt{1-T}\sqrt{(\omega^2-1)}\mathbf{Z} \\ -\sqrt{1-T}\sqrt{(\mu^2-1)}\mathbf{Z} & \sqrt{T(1-T)}(\omega-\mu)\mathbf{I} & ([1-T]\mu+T\omega)\mathbf{I} & \sqrt{T(\omega^2-1)}\mathbf{Z} \\ 0 & \sqrt{1-T}\sqrt{(\omega^2-1)}\mathbf{Z} & \sqrt{T(\omega^2-1)}\mathbf{Z} & \omega\mathbf{I} \end{bmatrix} \tag{4.11}$$

Reduction of the above matrix to include only Alice's and Bob's mode yields

$$\mathbf{V}'_{AB} = \begin{bmatrix} \mu\mathbf{I} & \sqrt{T(\mu^2-1)}\mathbf{Z} \\ \sqrt{T(\mu^2-1)}\mathbf{Z} & (T\mu+[1-T]\omega)\mathbf{I} \end{bmatrix} \tag{4.12}$$

In case Eve chooses the variance of her TMSV state to be ω, rewriting Eq. (4.9) to solve for ω returns the covariance matrix

$$\mathbf{V}'_{AB} = \begin{bmatrix} \mu\mathbf{I} & \sqrt{T(\mu^2-1)}\mathbf{Z} \\ \sqrt{T(\mu^2-1)}\mathbf{Z} & [T(\mu-1)+1+\xi]\mathbf{I} \end{bmatrix} \tag{4.13}$$

which portrays the transmission through a lossy channel under excess noise without Eve's interception. To obtain Eve's information, the symplectic eigenvalues of the covariance matrix under modes E_1 and E_2 are required. Removing Alice's and Bob's modes from Eq. (4.11), the matrix is given by

$$\mathbf{V}'_{E_1E_2} = \begin{bmatrix} ([1-T]\mu+T\omega)\mathbf{I} & \sqrt{T(\omega^2-1)}\mathbf{Z} \\ \sqrt{T(\omega^2-1)}\mathbf{Z} & \omega\mathbf{I} \end{bmatrix} \tag{4.14}$$

This matrix describes a two-mode state, which obeys the structure of Eq. (3.22). This means that its symplectic eigenvalues v_+ and v_-, which are used to compute the entropy S_E, can be conveniently calculated using the formula of Eq. (3.23).

Suppose the case of homodyne detection. To calculate the conditional von Neumann entropy between Bob and Eve $S_{E|B}$, the symplectic eigenvalues of Eve's covariance matrix upon Bob's measurement are first required to be known. By eliminating only Alice's quadratures from Eq. (4.11), the covariance matrix of Bob and Eve becomes

$$\mathbf{V}'_{BE_1E_2} = \begin{bmatrix} [\omega(1-T)+\mu T]\mathbf{I} & (\omega-\mu)\sqrt{T(1-T)}\mathbf{I} & \sqrt{(1-T)(\omega^2-1)}\sigma_z \\ (\omega-\mu)\sqrt{T(1-T)}\mathbf{I} & [\mu(1-T)+\omega T]\mathbf{I} & \sqrt{T(\omega^2-1)}\sigma_z \\ \sqrt{(1-T)(\omega^2-1)}\sigma_z & \sqrt{T(\omega^2-1)}\sigma_z & \omega\mathbf{I} \end{bmatrix} \tag{4.15}$$

When Bob's mode undergoes a homodyne measurement, Eve's system $E = E_1E_2$ is altered, according to Eq. (3.28):

$$\mathbf{V}_{E|B}^{\text{hom}} = \mathbf{V}'_{E_1E_2} - \mathbf{C}_{E|B}(\mathbf{\Pi B \Pi})^{-1}\mathbf{C}_{E|B}^T = \mathbf{V}'_{E_1E_2} - \frac{1}{\mu_B}\mathbf{C}_{E|B}\mathbf{\Pi}\mathbf{C}_{E|B}^T \tag{4.16}$$

Eve's covariance matrix $\mathbf{V}'_{E_1E_2}$ is displayed in Eq. (4.14), while Eq. (4.13) returns

$$\mu_B = (1-T)\omega + T\mu \tag{4.17}$$

As three modes participate in this transformation, the 4×2 matrix $\mathbf{C}_{E|B}$ of the partial measurement, which describes the quantum correlations between Eve's modes and Bob's mode, is defined as [Weedbrook et al. (2012b)]

$$\mathbf{C}_{E|B} = \begin{bmatrix} -\sqrt{T-(1-T)}(\mu-\omega)\mathbf{I} \\ \sqrt{(1-T)(\omega^2-1)}\mathbf{Z} \end{bmatrix} \tag{4.18}$$

Finally, $\mathbf{\Pi}$ is taken here as $\text{diag}(1,0)$. After a series of cumbersome computations, the result of Eq. (4.16) resembles a matrix of the form of Eq. (3.18), whose submatrices $\mathbf{A}$, $\mathbf{B}$ and $\mathbf{C}$ are given by

$$\mathbf{A} = \begin{bmatrix} \dfrac{\mu\omega}{T(\mu-\omega)+\omega} & 0 \\ 0 & (1-T)\mu + T\omega \end{bmatrix} \tag{4.19}$$

$$\mathbf{B} = \begin{bmatrix} \dfrac{1-T+T\omega\mu}{T\mu+\omega-T\omega} & 0 \\ 0 & \omega \end{bmatrix} \tag{4.20}$$

$$\mathbf{C} = \begin{bmatrix} \dfrac{\sqrt{T(\omega^2-1)}\mu}{T\mu+\omega-T\omega} & 0 \\ 0 & -\sqrt{T(\omega^2-1)} \end{bmatrix} \tag{4.21}$$

All in all, the final matrix is shaped as

$$\mathbf{V}_{E|B}^{\text{hom}} = \begin{bmatrix} \dfrac{\mu\omega}{T(\mu-\omega)+\omega} & 0 & \dfrac{\sqrt{T(\omega^2-1)}\mu}{T\mu+\omega-T\omega} & 0 \\ 0 & (1-T)\mu+T\omega & 0 & -\sqrt{T(\omega^2-1)} \\ \dfrac{\sqrt{T(\omega^2-1)}\mu}{T\mu+\omega-T\omega} & 0 & \dfrac{1-T+T\omega\mu}{T\mu+\omega-T\omega} & 0 \\ 0 & -\sqrt{T(\omega^2-1)} & 0 & \omega \end{bmatrix} \tag{4.22}$$

The set of symplectic eigenvalues $v_\pm$ of the resulting conditional covariance matrix can be obtained by either using Eq. (3.20) or by identifying the ordinary eigenvalues of the matrix, found in Eq. (3.25). The calculation of the conditional von Neumann entropy based on Bob's measurement $S_{E|B}$ can now take place. Combining this term with Eve's entropy S_E gives the Holevo information χ_{BE}, as shown in Eq. (2.30). Note that the derivation for the heterodyne protocol follows the formula of Eq. (3.29).

4.7.1 Purification Attack

As there is no knowledge of Eve's attack plan, the worst-case scenario is assumed. In this, Eve possesses a purification of Alice's and Bob's quantum state ρ_{AB}. The total pure state ρ_{ABE} is then characterized by Eq. (2.21). By removing Eve's subspace, a mixed state ρ_{AB}, whose von Neumann entropy is given by Eq. (2.25), is produced. This assumption implies the entropy of Eve is equal to the entropy between Alice and Bob

$$S_E = S_{AB} = -\sum_i \lambda_i \ln \lambda_i \tag{4.23}$$

As a result, the calculation of the Holevo bound between Bob and Eve can be simplified by completely disregarding Eve's activity, using the following formula [Pirandola (2014)]:

$$\chi_{BE} = S_E - S_{E|B} = S_{AB} - S_{A|B} \tag{4.24}$$

The von Neumann entropy S_{AB} can be calculated by Eq. (3.26), using the symplectic eigenvalues v_1 and v_2 from matrix Eq. (4.13). The calculation of the conditional entropy $S_{A|B}$ depends on the type of detection utilized by Bob. Assuming homodyne detection, the formula is given by Eq. (3.28). Let Eq. (4.13) take the form of Eq. (3.22). For $\mathbf{A} = a\mathbf{I}$, $\mu_B = b$ and $\mathbf{C} = c\sigma_z$ [Laudenbach et al. (2018)], the result is

$$\mathbf{V}_{A|B} = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} - \frac{1}{b}\begin{bmatrix} c^2 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a - \dfrac{c^2}{b} & 0 \\ 0 & a \end{bmatrix} \tag{4.25}$$

The symplectic eigenvalues can be calculated as ordinary eigenvalues, as demonstrated by Eq. (3.25)

$$\tilde{\mathbf{V}}_{A|B} = i\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} a - \dfrac{c^2}{b} & 0 \\ 0 & a \end{bmatrix} = \begin{bmatrix} 0 & ia \\ i(-a + \dfrac{c^2}{b}) & 0 \end{bmatrix} \tag{4.26}$$

Computation of the eigenvalue $\tilde{v}$ can be achieved under typical eigenvalue solving of a matrix

$$\det\left(\tilde{v}\mathbf{I} - \tilde{\mathbf{V}}_{A|B}\right) = 0 \Leftrightarrow \det\left(\begin{bmatrix} \tilde{v} & -ia \\ -i(-a + \dfrac{c^2}{b}) & \tilde{v} \end{bmatrix}\right) = 0 \Leftrightarrow \tilde{v}^2 + a(-a + \frac{c^2}{b}) = 0 \tag{4.27}$$

Ultimately, the eigenvalue $\tilde{v}$ is given by

$$\tilde{v} = \sqrt{a(a - \frac{c^2}{b})} \tag{4.28}$$

4.8 Finite-Size Effects

The above sections provided a foundational overview of the different stages of CV-QKD protocols and some of the challenges associated with them. In practice, from all of the data-processing procedures arise imperfections, which must be accounted for, to accurately estimate the security of the protocol.

So far, the protocols have been examined in the asymptotic limit, which assumes the generation of an infinite number of states. In practice, this number is always finite. The selected number of states depends on multiple factors, such as the noise and loss of the communication channel or the desired key rate. Usually, the total amount of generated points ranges anywhere from 10^7 to 10^{12}. However, the execution of error correction is required to be completed in a timely fashion. As a result, this large sequence may be broken into n_{bks} smaller sequences, called frames or blocks. Generally, each block contains $N = 10^5$ to $N = 10^7$ points [Milisevic (2017), Zhang et al. (2020), Supplementary Material].

In a practical implementation, a subset n of the total states N proceeds to the error-correction stage, while another portion m needs to be sacrificed, in order to estimate the channel parameters $\widehat{T}$ and $\widehat{\Xi}$. Consequently, as only the surviving states n should participate in the true key rate of the protocol, a diminishing factor of $\frac{n}{N}$ should be added in the calculation. In addition, there might be significant deviation between the estimated and actual values. For this reason, it is common that Alice and Bob also calculate worst-case scenarios T_m and Ξ_m, which they use to compute an overestimation of Eve's Holevo bound χ_m. The key rate integrating these features is informally referred to as the parameter-estimation based rate [Pirandola (2021a)] and is calculated by

$$R_M = \frac{n}{N}\left(\beta I_{XY}|_{\widehat{T},\widehat{\Xi}} - \chi|_{T_m,\Xi_m}\right) \quad [1] \tag{4.29}$$

Another concept, which is infeasible in reality, is perfect reconciliation. Reconciliation is affected by multiple factors, such as the channel conditions, the preprocessing scheme, the error-correction algorithm, the design quality, the code rate and the length of the chosen LDPC code and, finally, the specified correctness error ε_{cor}, which is described in the next section. The factor of the LDPC block length n points to one of the reasons why long block sizes are preferred, as LDPC codes have been shown to exhibit superior decoding performance at such block sizes [Luby et al. (2001)]. During the error correction stage, there is a probability that the decoding process may fail for certain frames. The rate of failure is measured by the frame error rate FER, while p_{EC} denotes the metric for the probability of successful reconciliation, which includes both error correction and verification. In addition, because the reconciliation process cannot be perfect, its underlying quantity β, which captures the effectiveness of the code to operate as close as possible to the Shannon limit at a particular SNR, can also never be perfect.

[1] The symbol | denotes the evaluation of a function with respect to a specific set of parameters.

The quantities β and p_{EC} are inherently connected. Reducing the desired efficiency may yield higher error correction performances, while a higher efficiency may have an adverse effect on the success of decoding. Given that some of the key generation states will be discarded, if not correctly decoded, a finite-size effect key rate can be defined by

$$R_M^{\mathrm{EC}} = \frac{np_{\mathrm{EC}}}{N}\left(\beta I_{XY}|_{\widehat{T},\widehat{\Xi}} - \chi|_{T_m,\Xi_m}\right) \tag{4.30}$$

where $\beta < 1$. Maximizing the secret key rate requires that the error-correcting code must be able to achieve both a high error-correction success rate, ideally 1, and high reconciliation efficiency, ideally as close to 1 as possible. In any case, achieving $p_{\mathrm{EC}} > 0$ is mandatory for the protocol to continue. Otherwise, the implication is that no sequences have been correctly decoded, which means that a secret key cannot be formed.

Finally, another subtle practical effect, which may potentially affect the key rate and whose importance is not often stressed enough, is the speed, at which error correction is performed. In this setting, the speed is determined by

- the maximum number of error-correcting iterations $\mathrm{iter}_{\max}$,
- the capabilities of the hardware,
- the design of the decoder,
- or some or all of the above combined.

As already mentioned, the computationally complex sum-product algorithm is typically employed by Alice for the decoding of blocks, in the reverse reconciliation scenario. If decoding, and by extension key generation, is not quick enough, then the two parties would have to resort to a lower value for β. Such a compromise would require fewer $\mathrm{iter}_{\max}$ rounds, which comes with an increased decoding speed and, potentially, a higher p_{EC}, but would detrimentally affect the key rate. To clarify, a CV-QKD protocol with slow error correction will be unsafe in longer distances. For this reason, decoding in CV-QKD, especially at long distances, is almost exclusively performed with graphics processing units (GPUs), because the sum-product algorithm is highly parallelizable by design [Milisevic (2017)]. As GPUs possess a superior number of cores compared to central processing units (CPUs), far more processes can be simultaneously executed. All in all, there is an implicit connection between β, p_{EC} and the speed of error correction. Identifying the optimal trade-off, which maximizes the performance of the protocol, can pose a considerable challenge.

4.9 Composable Framework

While the security analysis benefits significantly from the inclusion of finite-size effects, it is still incomplete. To ensure the security of the protocol, the notion of composability must be introduced in the context of CV-QKD. The definition of security in a quantum cryptographic setting from [Renner (2005)] stands out as the most robust and rigorous in the field. A QKD protocol is said to be ε-secure, if

$$D(\rho_{ABE}, \sigma_{AB} \otimes \rho_E) \leq \varepsilon \tag{4.31}$$

Here, D signifies the trace distance of Eq. (2.32), ρ_{ABE} is the final joint state of Alice, Bob and Eve and $\sigma_{AB} \otimes \rho_E$ is the ideal secret key state. The parameter ε indicates the probability of Alice and Bob generating a shared key, which is not identical to an ideal key. Conversely, the key is ideal with a probability of $1 - \varepsilon$ and, therefore, it is completely disassociated from Eve.

Composability implies defining an ideal protocol, which is perfectly secure by design. The ideal version is then compared to the practical version. The ideal and practical versions should be virtually indistinguishable, with Renner's definition serving as the benchmark for their comparison. A protocol under the composable framework takes into account the worst possible outcome for a variety of tasks.

Security proofs, that incorporate composability, have been demonstrated for various CV-QKD protocols [Leverrier (2015), Leverrier (2017), Pirandola (2021a), Pirandola (2021b), Papanastasiou and Pirandola (2021), Pirandola (2022)]. These proofs are based on probabilities, called epsilon parameters or ε-parameters, which are related to various errors or inaccuracies from processes, that take place during the protocol. In this thesis, five ε-parameters, each introducing a certain penalty, are identified and discussed:

- **Parameter estimation error** $\varepsilon_{\mathrm{PE}}$, which is the probability that the estimated channel parameters do not belong in the marked out confidence region, laid out by the worst-case scenario estimators.
- **Entropy estimation error** $\varepsilon_{\mathrm{ent}}$, which is associated with the impact of finite samples on the entropy estimation of key generation sequences. When estimating the entropy of a sequence, the probabilities of each symbol appearing become more reliable, as the sample size converges towards infinity. Nonetheless, for smaller samples, the probabilities may not accurately represent the actual underlying distribution. Instead, the observed frequencies are used as estimates for the probabilities. Therefore, the estimator should be smaller than or equal to the true value for the entropy. To ensure security, a penalty, related to the probability of the estimated entropy being larger than the actual one, is introduced.

- **Correctness error** ε_{cor}, which represents the collision probability of a family of universal hash functions $\mathcal{F}$, which is used during the verification stage. The correctness error is an inherent property of the family of a hash function h, as it is imposed by the specific design and properties of the chosen family. It determines the length in bits of the hash digests as

$$t = \lceil -\log_2 \varepsilon_{\text{cor}} \rceil \tag{4.32}$$

  It is evident that a smaller value for the correctness error will result in a smaller length for the verification hash output length and, thus, a weaker verification. Successively, this will negatively affect the success probability of error correction.

- **Smoothing parameter** ε_s, discussed in Sec 2.2.5, which quantifies the error probability of particular information-theoretic tasks, such as failing to accurately determine the probability distribution of the key.

- **Hashing parameter** ε_h, which is a direct result of the leftover hash lemma and indicates the collision error of the universal hash function used during the privacy amplification stage.

In analyses of experimental implementations, additional ε-parameters have emerged, such as the probability of faulty calibration of the transmitter or the receiver, as well as the probability that the quantum random number generator has induced errors during discretization [Lupo (2020), Jain et al. (2022)].

The smoothing and hashing parameters constitute another ε-parameter, the secrecy parameter

$$\varepsilon_{\text{sec}} = \varepsilon_h + \varepsilon_s \tag{4.33}$$

which characterizes the privacy amplification stage. It stands for the probability of failing to prevent Eve from obtaining information about the key. In composable terms, it bounds the distance between the actual final key and an ideal key, that is, a key about which Eve possesses zero knowledge.

The ε-parameters contribute in the shaping of extra terms, which, in turn, will define a new key rate. The first term the relation of the secret key rate with finite-size effects takes into consideration the fact that the Holevo information function is not working correctly in a finite-size effects regime. Thus, there is an extra term that accounts for this correction, which is dependent on the number of signals used for key extraction. This term is approximated by Δ_{AEP}, which quantifies the error committed bounding the smooth-min entropy, using the AEP [Tomamichel (2012)]. Another term, denoted by Θ, is introduced to satisfy the bound originated from the leftover hash lemma [Pirandola et al. (2020), Appendix G]. The mathematical formulation of these notions is variable and depends on various factors, including the adopted preprocessing methods and the considered ε-parameters.

Taking all the above into consideration, the secret key rate should not only depend on the noise and losses of the communication channel, but also on a series of data-processing steps, required for transforming shared correlations into a final string of secret bits. The secret key rate encompassing both the composable framework and finite-size effects is called composable key rate and is defined as [Pirandola (2021a), Pirandola (2022)]

$$R = R_M^{\mathrm{EC}} - \frac{p_{\mathrm{EC}}\sqrt{n}}{N}\Delta_{\mathrm{AEP}} + \frac{p_{\mathrm{EC}}}{N}\Theta \tag{4.34}$$

A protocol that is ε-secure always produces a positive composable key rate and vice versa. In other words, ε-security implies that, despite the presence of an eavesdropper, Alice's and Bob's final keys Υ_X and Υ_Y are identical, uniformly distributed, and completely disassociated from the eavesdropper, except with probability ε. Through a positive composable key rate, the amount of compression, that must be applied to construct the final key Υ can be quantified. The secret key length ℓ is generally determined by the total amount of generated states times the composable key rate.

Chapter 5

Data Processing in Gaussian-Modulated Coherent-State CV-QKD

The research part of the thesis fully describes the entire operation of three protocols, namely the GMCS protocols under homodyne and heterodyne detection, as well as the CV-MDI protocol. The course of action of the protocols, from state preparation to secret key generation, will be carefully explained and guided step by step. In order to provide an accurate depiction of a realistic implementation, the description will incorporate the composable security framework under finite-size effects. Except when explicitly stated within the text, differentiation between the protocols will be communicated either by using different subsections or by means of piecewise functions. In the rest of the cases, the three protocols follow the same course.

The focus of this thesis is the realization of the protocols under short-distance communications. Therefore, the resulting SNR will receive values which are considered relatively high. As a result, the amount of mutual information between Alice and Bob will also be high. In order to be able to maintain a high value for the reconciliation efficiency, which is a crucial requirement to achieve a positive composable key rate, the preprocessing and error correction stages have been adapted to an appropriate scheme for such conditions.

5.1 Protocol Description

Here, the quantum communication stage of the three protocols will be presented. This includes the preparation, transmission and detection of the coherent states. Moreover, the method of the eavesdropping attack is captured. Finally, the fundamental quantities characterizing the protocol are also defined in this section.

5.1.1 Homodyne and Heterodyne Protocol Description

Alice begins by preparing a bosonic mode A in a coherent state $|\alpha\rangle$, whose amplitude is Gaussian-modulated. In other words, it is appropriate to provide the description[1]

$$\alpha = \frac{Q + iP}{2} \tag{5.1}$$

Besides, $x = \{Q, P\}$ is the mean value of the generic quadrature operator $\hat{x} = \{\hat{Q}, \hat{P}\}$, which is randomly chosen according to a zero-mean Gaussian distribution $\mathcal{G}(0, \sigma_x^2)$, whose probability density function is given by

$$p_{\mathcal{G}}(x) = \frac{1}{\sqrt{2\pi}\sigma_x} \exp\left(\frac{-x^2}{2\sigma_x^2}\right) \tag{5.2}$$

Here, $\sigma_x^2 \geq 0$ stands for the modulation variance, while μ is the total signal variance, which is given by the sum of the modulation variance and the vacuum noise as

$$\mu = \sigma_x^2 + V \tag{5.3}$$

The notation adopted here for $\hbar = 2$ is

$$[\hat{Q}, \hat{P}] = 2i \tag{5.4}$$

which originates from [(Weedbrook et al., 2012a, Sec. II)] and follows the representation in SNU, as the vacuum state has noise variance $V = 1$. Note that

$$Q = 2\,\mathrm{Re}\,\alpha \tag{5.5}$$

$$P = 2\,\mathrm{Im}\,\alpha \tag{5.6}$$

The coherent states travel to Bob through an optical fiber with length L and attenuation ϑ. This is simulated by a thermal-loss channel with transmissivity

$$T = 10^{-\frac{\vartheta L}{10}} \tag{5.7}$$

and thermal noise

$$\omega = 2\bar{\mathsf{n}} + 1 \tag{5.8}$$

where $\bar{\mathsf{n}}$ is the thermal number associated with an environmental mode E [Ottaviani et al. (2016)]. The process can equivalently be represented by a beam splitter with transmissivity T mixing Alice's mode A with mode E, which is in a thermal state with $\bar{\mathsf{n}}$ mean photons. Through purification, the environmental thermal state can be converted into in a TMSV $\mathbf{V}_{eE}$, with modes e and E, zero mean and CM

$$\mathbf{V}_{eE}(\omega) = \begin{bmatrix} \omega\mathbf{I} & \sqrt{\omega^2 - 1}\mathbf{Z} \\ \sqrt{\omega^2 - 1}\mathbf{Z} & \omega\mathbf{I} \end{bmatrix} \tag{5.9}$$

[1] Recall that Eq.

Here, $\mathbf{I} = \mathrm{diag}(1,1)$ and $\mathbf{Z} = \mathrm{diag}(1,-1)$. This dilation based on a beam splitter and a TMSV state is the entangling cloner attack, which represents a realistic collective Gaussian attack, that is optimal against GMCS CV-QKD protocols. This class of attacks has been thoroughly described in Sec. 4.7.

At the other end of the channel, Bob measures the incoming states by mixing the arriving mode B with a vacuum mode, using a balanced beam splitter. The states enter his detector, which is characterized by setup efficiency η and electronic noise υ_{el}. In the homodyne scenario, the detector is randomly switched between the two quadratures. Under heterodyne detection, a homodyne measurement is applied to each beam splitter output, targeting a different conjugate quadrature. Each measurement introduces a vacuum noise term V, leading to the notation

$$V^* = \begin{cases} 1 & \text{Homodyne} \\ 2 & \text{Heterodyne} \end{cases} \tag{5.10}$$

With $\hat{y}$ being the generic quadrature of Bob's mode B, the outcome y of the detector is described by the input-output formula

$$y = \sqrt{T\eta}x + z \tag{5.11}$$

where z is a Gaussian noise variable with zero mean and variance

$$\sigma_z^2 = \upsilon_{\mathrm{el}} + \Xi + V^* \tag{5.12}$$

Here, Ξ is excess noise variance of the channel, defined by

$$\Xi = \eta T \xi \tag{5.13}$$

where ξ represents the actual excess noise, expressed by Eq. (4.9).

It is important to make two considerations. The first concerns the management of Bob's detector, accounting for the possible presence of trusted levels of quantum efficiency and electronic noise. In the worst-case scenario, these levels can be set equal to zero. It can then be assumed, that these contributions are implicitly part of the channel transmissivity and excess noise. In other words, a possible map is $T\eta \to T$ in Eq. (5.11), while υ_{el} can become a part of ξ in Eq. (5.12), so that $\xi \to \xi + \upsilon_{\mathrm{el}}/T$ in Eq. (4.9).

The second point is that Alice and Bob might not be able to control or mitigate other imperfections in their setups, such as the modulation noise or the phase noise. These imperfections are automatically included in the channel noise and loss via the general relations of Eq. (5.11) and Eq. (5.12). Furthermore, the extra noise contributions can be considered to be Gaussian in the worst-case scenario, resorting to the optimality of Gaussian attacks against GMCS CV-QKD protocols.

So far, the description of the protocol can be condensed in the depiction of Fig. 4.1. Assuming this general scenario, the mutual information between Alice and Bob can be computed by the following steps. From Eq. (5.11), the variance of y is equal to

$$\sigma_y^2 = T\eta\sigma_x^2 + \sigma_z^2 = T\eta(\mu - 1 + \xi) + V^* + \upsilon_{\text{el}} \tag{5.14}$$

while the conditional variance is given by

$$\sigma_{y|x}^2 = \sigma_y^2(\mu = 1) = \eta T\xi + V^* + \upsilon_{\text{el}} \tag{5.15}$$

The mutual information associated with the variables x and y is given by the difference between the differential entropy $H(y)$ of y and the conditional entropy $H(y|x)$ as

$$I(x:y) = H(x) - H(y|x) = \frac{V^*}{2}\log_2\left(\frac{\sigma_y^2}{\sigma_{y|x}^2}\right) = \frac{V^*}{2}\log_2(1 + \text{SNR}) \tag{5.16}$$

The doubling of the mutual information in the heterodyne case is owed to the two independent quadratures having the same variance. Note that the mutual information stays the same, whether the type of reconciliation is direct or reverse. The mutual information also contains the SNR term, which is written as

$$\text{SNR} = \frac{\mu - 1}{\chi} \tag{5.17}$$

where the quantity

$$\chi = \xi + \frac{V^* + \upsilon_{\text{el}}}{T\eta} \tag{5.18}$$

is known as the equivalent noise. The joint Gaussian distribution of the two variables x and y has zero mean and CM

$$\mathbf{\Sigma}_{xy} = \begin{bmatrix} \sigma_x^2 & \rho\sigma_x\sigma_y \\ \rho\sigma_x\sigma_y & \sigma_y^2 \end{bmatrix} \tag{5.19}$$

where

$$\rho = \frac{\mathbb{E}(xy)}{\sigma_x\sigma_y} \tag{5.20}$$

is a correlation parameter and $\mathbb{E}$ stands for the expected value. From the classical formula [Cover and Thomas (2001)]

$$I(x:y) = -\frac{V^*}{2}\log_2(1 - \rho^2) \tag{5.21}$$

it is evident that the correlation can be expressed in terms of the SNR as

$$\rho = \sqrt{\frac{\text{SNR}}{1 + \text{SNR}}} \tag{5.22}$$

It is important to stress that, in order to asymptotically achieve the maximum number of shared bits $I(x:y)$ per channel use in reverse reconciliation, Bob needs to send $H(y|x)$ bits through the public channel, according to Slepian-Wolf coding. In practice, Alice and Bob will perform a suboptimal procedure of reconciliation, revealing more information $\text{leak}_{\text{EC}} \geq H(y|x)$. To account for this, it is assumed that only a portion $\beta I(x:y)$ of the mutual information can be achieved using the reconciliation parameter $\beta \in [0,1)$.

Remark 1. From a data processing perspective, Alice generates Nn_{bks} signal states, leading to a total of $2Nn_{\text{bks}}$ samples. This means there are Nn_{bks} samples for each quadrature. During the key sifting step of the homodyne protocol, Bob randomly switches between the Q and P quadratures, keeping only one and discarding the other. His selections are transferred to Alice, who discards her quadratures correspondingly. Here, one generated signal state corresponds to one measurement. In the end, the two parties possess Nn_{bks} samples each, meaning every block $1, 2, \ldots, n_{\text{bks}}$ holds N samples. In the heterodyne version, Alice encodes $2Nn_{\text{bks}}$ samples $[x]_i$, $i = 1, \ldots, 2N$, of the generic variable $x \sim \mathcal{G}(0, \mu - 1)$ on the two conjugate quadratures of Nn_{bks} signal states. Then, she groups them in instances $[\mathbf{x}]_j = ([Q_x]_j, [P_x]_j) = ([x]_{2j-1}, [x]_{2j})$ for $j = 1 \ldots N$ and encodes them in n_{bks} blocks of coherent states $|\alpha_j\rangle$, where $\alpha_j = ([x]_{2j-1} + \mathrm{i}[x]_{2j})/2$. Bob's instances become $[\mathbf{y}]_j = ([Q_y]_j, [P_y]_j) = ([y]_{2j-1}, [y]_{2j})$ for the jth state encoding Alice's instances $[\mathbf{x}]_j$. To clarify, odd-indexed samples are encoded in the Q-quadrature, while even-indexed ones are in the P-quadrature of the Nn_{bks} states. The result is the concatenation of Q and P, leading to $2Nn_{\text{bks}}$ samples for each party. In practice, this is only virtually theorized. An analysis of this concept can be found in Appendix C.

5.1.2 CV-MDI Protocol Description

Alice and Bob prepare coherent states $|\alpha_A\rangle$ and $|\alpha_B\rangle$ with amplitudes

$$\alpha_A = \frac{Q_A + iP_A}{2} \tag{5.23}$$

$$\alpha_B = \frac{Q_B + iP_B}{2} \tag{5.24}$$

carried by modes A and B respectively. In particular, they encode the real vectorial variables $\boldsymbol{\alpha} = (Q_A, P_A)$ and $\boldsymbol{\beta} = (Q_B, P_B)$, which follow the Gaussian distributions

$$\mathcal{G}(\boldsymbol{\alpha}) = \frac{e^{[-\frac{1}{2}(Q_A^2+P_A^2)^2/\sigma_A^2]}}{2\pi\sigma_A^2} \qquad \mathcal{G}(\boldsymbol{\beta}) = \frac{e^{[-\frac{1}{2}(Q_B^2+P_B^2)^2/\sigma_B^2]}}{2\pi\sigma_B^2} \tag{5.25}$$

The two bosonic modes travel to an intermediate relay, where a Bell measurement is applied to the incoming modes. The output of the relay is

$$\gamma = \frac{Q_R + \mathrm{i}P_R}{2} \tag{5.26}$$

The notation $\boldsymbol{\gamma} = (Q_R, P_R)$ is also adopted here.

Eve interacts with the roaming modes via a two-mode attack, which is depicted in Fig. 5.1. The first mode E_1 is mixed with mode A through a beam splitter with transmissivity T_A. Similarly, mode E_2 with mode B are interfered using a beam splitter with transmissivity T_B. The two links are characterized by thermal noise, which is defined in terms of their respective transmissivity and excess noise as

$$\omega_A = \frac{T_A \xi_A}{1 - T_A} + 1 \tag{5.27}$$

$$\omega_B = \frac{T_B \xi_B}{1 - T_B} + 1 \tag{5.28}$$

The covariance matrix of Eve's modes is given by

$$\mathbf{V}_{E_1 E_2} = \begin{bmatrix} \omega_A \mathbf{I} & \mathbf{G} \\ \mathbf{G} & \omega_B \mathbf{I} \end{bmatrix}, \quad \mathbf{G} = \begin{bmatrix} g & 0 \\ 0 & g' \end{bmatrix} \tag{5.29}$$

where g and g' are correlation parameters, whose bona fide conditions are provided in [Pirandola et al. (2015)]. Given the correlation parameter description, the most powerful attacks are executed, when $g < 0$ and $g' > 0$. These are collective two-mode Gaussian attacks and represent the entangling cloner attack counterpart of a channel comprised of two links [Pirandola et al. (2008b), Papanastasiou et al. (2021)]. Taking into consideration this area of values, it is evident that as $|g|$ and $|g'|$ become larger, the modes become more quickly and more strongly correlated. Then, $g_{\max} = \max\{|g|, |g'|\}$ can be chosen, assuming the worst-case scenario attack with

$$\mathbf{G}_{\max} = \begin{bmatrix} -g_{\max} & 0 \\ 0 & g_{\max} \end{bmatrix} \tag{5.30}$$

In such a case, the quadratures can be treated equivalently, as they follow the same probability distribution.

The outputs Q_R and P_R are dependent on the variables Q_A, P_A and Q_B, P_B respectively, according to the following equations:

$$Q_R = \tau_B Q_B - \tau_A Q_A + Q_z \tag{5.31}$$

$$P_R = \tau_B P_B + \tau_A P_A + P_z \tag{5.32}$$

where τ_A and τ_B are rescaling parameters, connected to the overall attenuation via

$$\tau_A = \sqrt{\frac{\eta T_A}{2}} \tag{5.33}$$

$$\tau_B = \sqrt{\frac{\eta T_B}{2}} \tag{5.34}$$

Here, η is the calibrated detection efficiency.

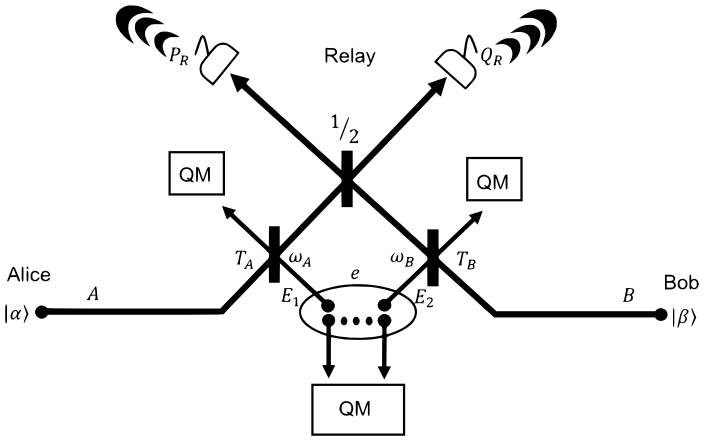

Figure 5.1: Representation of the quantum communications stage in CV-MDI. Alice and Bob send coherent states $|\alpha\rangle$ and $|\beta\rangle$ with modes A and B to the intermediate relay. Eve's modes E_1 and E_2 interact with the roaming modes via beam splitters with transmissivities T_A and T_B respectively. Eve's two-mode attack is characterized by thermal noise parameters ω_1 and ω_2, as in Eq. (5.29). Eve's modes are stored in a quantum memory, awaiting the communication between the parties for an optimal measurement [Papanastasiou et al. (2023)].

The noise variables Q_z and P_z have variance σ_z^2, such that

$$\sigma_z^2 = \upsilon_{\text{el}} + \Xi + 1 \tag{5.35}$$

where υ_{el} denotes the electronic noise of the detectors and Ξ the excess noise variance, provided by the formula

$$\Xi = \frac{\eta}{2}\left[(1-T_A)(\omega_A - 1) + (1-T_B)(\omega_B - 1)\right] + \eta g_{\max}\sqrt{(1-T_A)(1-T_B)} \tag{5.36}$$

with

$$g_{\max} = \max\{\sqrt{(\omega_A - 1)(\omega_B + 1)}, \sqrt{(\omega_B - 1)(\omega_A + 1)}\} \tag{5.37}$$

5.2 Asymptotic Key Rate Calculation

This section describes how to calculate the achievable secret key rate for infinite uses of the quantum communication channel between Alice and Bob. For the homodyne and heterodyne protocols, the mutual information has already been calculated. Putting the efficiency aside, the only missing parameter for the calculation of the asymptotic rate of Eq. (4.3), assuming reverse reconciliation, is the Holevo information between Eve and Bob. The CV-MDI protocol still requires the computation of both the mutual information and the Holevo bound. In line with the definition of a collective Gaussian attack, it is assumed that after a Gaussian interaction with the signal modes, Eve stores her modes in a quantum memory and measures them optimally, after all communications between Alice and Bob conclude.

5.2.1 Homodyne Protocol Asymptotic Rate Calculation

The description follows the entanglement-based representation of the protocol. Herein, Alice's input ensemble of coherent states is generated on mode A by heterodyning mode A' of a TMSV $\mathbf{V}_{A'A}$ with variance μ. Note that this representation is not strictly necessary in this analysis, as it may be carried out equivalently using a P&M scheme. However, it is adopted for the sake of completeness, so as to give the total state with all the correlations between Alice, Bob and Eve.

The output modes A' and B shared by the parties will be in a zero-mean Gaussian state $\rho_{A'B}$ with CM

$$\mathbf{V}_{A'B} = \begin{bmatrix} \mu\mathbf{I} & \xi\mathbf{Z} \\ \xi\mathbf{Z} & \upsilon\mathbf{I} \end{bmatrix} \tag{5.38}$$

where the constituents are given by

$$\xi = \sqrt{T\eta(\mu^2 - 1)} \tag{5.39}$$

$$\upsilon = T\eta(\mu + \xi) + 1 - T\eta + v_{\text{el}} \tag{5.40}$$

Then, the global output state $\rho_{A'BeE'}$ of Alice, Bob and Eve is a zero-mean Gaussian state, whose CM is given by

$$\mathbf{V}_{A'BeE'} = \begin{bmatrix} \mu\mathbf{I} & \xi\mathbf{Z} & \mathbf{O} & \zeta\mathbf{Z} \\ \xi\mathbf{Z} & \upsilon\mathbf{I} & \pi\mathbf{Z} & \theta\mathbf{I} \\ \mathbf{O} & \pi\mathbf{Z} & \omega\mathbf{I} & \psi\mathbf{Z} \\ \zeta\mathbf{Z} & \theta\mathbf{I} & \psi\mathbf{Z} & \phi\mathbf{I} \end{bmatrix} \tag{5.41}$$

where $\mathbf{O}$ is the 2×2 zero matrix and the rest of the variables are [Pirandola (2022)]

$$\zeta = -\sqrt{(1-T)(\mu^2 - 1)} \tag{5.42}$$

$$\theta = \sqrt{\eta T(1-T)}(\omega - \mu) \tag{5.43}$$

$$\pi = \sqrt{\eta(1-T)(\omega^2 - 1)} \tag{5.44}$$

$$\psi = \sqrt{T(\omega^2 - 1)} \tag{5.45}$$

$$\phi = T\omega + (1-T)\mu \tag{5.46}$$

To compute the Holevo bound, the von Neumann entropies $S(\rho_{eE'})$ and $S(\rho_{eE'|y})$ need to be derived. These can be computed from the symplectic spectra of the reduced CM $\mathbf{V}_{eE'}$ and the conditional CM $\mathbf{V}_{eE'|y}$. Given the partial homodyne detection formula of Eq. (3.28), with the correlation matrix written as

$$\mathbf{C} = \begin{bmatrix} \pi\mathbf{Z} & \theta\mathbf{I} \end{bmatrix} \tag{5.47}$$

the pseudo-inverse operation can be used to compute

$$\mathbf{V}_{eE'|y} = \mathbf{V}_{eE'} - \mathbf{C}^T[\mathbf{\Pi}(\upsilon\mathbf{I})\mathbf{\Pi}]^{-1}\mathbf{C} \tag{5.48}$$

$$= \mathbf{V}_{eE'} - \upsilon^{-1}\mathbf{C}^T\mathbf{\Pi}\mathbf{C} \tag{5.49}$$

$$= \begin{bmatrix} \omega\mathbf{I} & \psi\mathbf{Z} \\ \psi\mathbf{Z} & \phi\mathbf{I} \end{bmatrix} - \upsilon^{-1}\begin{bmatrix} \pi^2\mathbf{\Pi} & \pi\theta\mathbf{\Pi} \\ \pi\theta\mathbf{\Pi} & \theta^2\mathbf{\Pi} \end{bmatrix} \tag{5.50}$$

Since both $\mathbf{V}_{eE'}$ and $\mathbf{V}_{eE'|y}$ are two-mode CMs, it is straightforward to compute their symplectic spectra, denoted as $\{v_\pm\}$ and $\{\tilde{v}_\pm\}$, using Eq. (3.23). Their general analytical expressions are too cumbersome to be presented here, unless the limit $\mu \gg 1$ is taken. In this instance, the convergence of the spectra is shown by $v_+ \to (1-T)\mu$ and $v_- \to \omega$.

Finally, Eq. (4.24) of the Holevo bound can be rewritten as

$$\chi(E:y) = S(\rho_{eE'}) - S(\rho_{eE'|y}) = G(v_+) + G(v_-) - G(\tilde{v}_+) - G(\tilde{v}_-) \tag{5.51}$$

where G is the bosonic entropic function, given by Eq. (3.27). It is important to stress that, for any processing $y \to y'$ done by Bob, the inequality $\chi(E:y') \leq \chi(E:y)$ stands. Therefore, the right-side value can always be taken as an upper bound for the actual eavesdropping performance.

All components for the calculation of the asymptotic key rate are now in place. Following Eq. (4.3), which concerns the reverse reconciliation scenario, the key rate is given by

$$R_{\text{asy}} = \beta I(x:y) - \chi(E:y) \tag{5.52}$$

Supposing that η and v_{el} are known and the parties have preliminary estimates of T and ξ, Alice can compute an optimal value μ^{opt} for the signal variance μ for a target β. This can be achieved by testing the asymptotic for a given interval of values for $\mu > 1$. Then, $\mu = \mu^{\text{opt}}$, when the maximum asymptotic key rate is returned.

5.2.2 Heterodyne Protocol Asymptotic Rate Calculation

Remark 2. Following Remark 1, the complementary notations $\mathbf{x}$ and $\mathbf{y}$ will henceforth refer to the concatenated quadratures. The mutual information of Eq. (5.16) will be denoted as $I(\mathbf{x}:\mathbf{y}) = 2I(x:y) = \log_2(1+\text{SNR})$ for the heterodyne case.

Alice and Bob are able to quantify the maximum possible amount of leaked information using the Holevo bound. This is computed from the von Neumann entropies $S(\rho_{E'e})$ and $S(\rho_{E'e|\mathbf{y}})$, which are in turn calculated from the joint CM of Bob and Eve, given by

$$\mathbf{V}_{BeE'} = \begin{bmatrix} \upsilon\mathbf{I} & \pi\mathbf{Z} & \theta\mathbf{I} \\ \pi\mathbf{Z} & \omega\mathbf{I} & \psi\mathbf{Z} \\ \theta\mathbf{I} & \psi\mathbf{Z} & \phi\mathbf{I} \end{bmatrix} \tag{5.53}$$

Here, υ is found in Eq. (5.40), θ in Eq. (5.43), π in Eq. (5.44), ψ in Eq. (5.45) and ϕ in Eq. (5.46).

By tracing out mode B from Eq. (5.53), the CM $\mathbf{V}_{eE'}$ is obtained. Then, by setting $\mathbf{C}$ as shown in Eq. (5.47) and modifying the formula for the heterodyne measurement of Eq. (3.29), Eve's conditional CM is obtained as

$$\mathbf{V}_{eE'|\boldsymbol{y}} = \mathbf{V}_{eE'} - (\upsilon+1)^{-1}\mathbf{C}^T\mathbf{C}\begin{bmatrix}\omega\mathbf{I} & \psi\mathbf{Z}\\ \psi\mathbf{Z} & \phi\mathbf{I}\end{bmatrix} - (\upsilon+1)^{-1}\begin{bmatrix}\pi^2\mathbf{I} & \pi\theta\mathbf{Z}\\ \pi\theta\mathbf{Z} & \theta^2\mathbf{I}\end{bmatrix} \tag{5.54}$$

Then, the Holevo information can be identified identically to the homodyne protocol by

$$\chi(E:\mathbf{y}) = S(\rho_{E'e}) - S(\rho_{E'e|\mathbf{y}}) = G(v_+) + G(v_-) - G(\tilde{v}_+) - G(\tilde{v}_-) \tag{5.55}$$

The entropic function G has been defined in Eq. (3.27) and $\{v_\pm\}$, $\{\tilde{v}_\pm\}$ are the symplectic spectra of $\mathbf{V}_{eE'}$ and $\mathbf{V}_{eE'|\mathbf{y}}$ respectively. They can be derived from either Eq. (3.23) or Eq. (3.25). Finally, similarly to Eq. (5.52), the asymptotic secret key rate is given by

$$R_{\text{asy}} = \beta I(\mathbf{x}:\mathbf{y}) - \chi(E:\mathbf{y}) \tag{5.56}$$

5.2.3 CV-MDI Asymptotic Rate Calculation

In the entanglement-based representation of CV-MDI, additional modes a and b are introduced, corresponding to modes A and B of the TMSV states, which have variances

$$\mu_A = \sigma_A^2 + 1 \tag{5.57}$$

$$\mu_B = \sigma_B^2 + 1 \tag{5.58}$$

Then, the encoding process is simulated by a heterodyne measurement on modes a and b, with corresponding measurement outcomes $\tilde{\alpha}$ and $\tilde{\beta}$. The total state CM is given by the direct sum of the subsystems as

$$\mathbf{V}_{aABbE_1E_2} = \mathbf{V}_{aA} \oplus \mathbf{V}_{Bb} \oplus \mathbf{V}_{E_1E_2} \tag{5.59}$$

with $\mathbf{V}_{aA}(\mu_A)$ and $\mathbf{V}_{Bb}(\mu_B)$ being CMs of a TMSV state. The attack corresponds to applying a beam splitter with transmissivity T_A between the modes A and E_1 and a beam splitter of transmissivity T_B between modes B and E_2. The beam splitter symplectic operation $\mathbf{S}$ with transmissivity T is given by Eq. (1.65).

Afterwards, Alice's and Bob's output modes A' and B' travel from each beam splitter to the relay, where they are mixed by a balanced beam splitter. Conjugate homodyne measurements are applied to the output modes, with outcomes grouped in the variable γ. Supposing a CM with the general form of Eq. (3.18), a homodyne measurement applied to mode B with outcome x_B will yield the CM, as shown in Eq. (3.28).

In this description, the CM after the relay measurements is shaped as

$$\mathbf{V}_{ab|\gamma} = \begin{bmatrix} \zeta\mathbf{I} & \psi\mathbf{Z} \\ \psi\mathbf{Z} & \theta\mathbf{I} \end{bmatrix} \tag{5.60}$$

where

$$\zeta = 1 + \sigma_A^2 - \frac{\tau_A^2\sigma_A^2(\sigma_A^2+2)}{\tau_B^2\sigma_B^2 + \tau_A^2\sigma_A^2 + \sigma_z^2} \tag{5.61}$$

$$\theta = 1 + \sigma_B^2 - \frac{\tau_B^2\sigma_B^2(\sigma_B^2+2)}{\tau_B^2\sigma_B^2 + \tau_A^2\sigma_A^2 + \sigma_z^2} \tag{5.62}$$

$$\psi = \frac{\tau_A\tau_B\sqrt{\sigma_A^2(\sigma_A^2+2)\sigma_B^2(\sigma_B^2+2)}}{\tau_B^2\sigma_B^2 + \tau_A^2\sigma_A^2 + \sigma_z^2} \tag{5.63}$$

According to Eq. (3.29), Bob performs a heterodyne measurement on mode b with outcome $\tilde{\beta}$, whose conditional CM is given by

$$\mathbf{V}_{a|\tilde{\beta}\gamma} = \left(\zeta - \frac{\psi^2}{\theta+1}\right)\mathbf{I} \tag{5.64}$$

From the matrices

$$\mathbf{V}_{a|\gamma} = \zeta\mathbf{I} \tag{5.65}$$

and $\mathbf{V}_{a|\tilde{\beta}\gamma}$, the mutual information between outcomes $\tilde{\alpha}$ and $\tilde{\beta}$ can be computed as

$$I(\tilde{\alpha}:\tilde{\beta}|\gamma) = \frac{1}{2}\log_2\frac{\det\mathbf{V}_{a|\gamma} + \operatorname{tr}\mathbf{V}_{a|\gamma} + 1}{\det\mathbf{V}_{a|\gamma\tilde{\beta}} + \operatorname{tr}\mathbf{V}_{a|\gamma\tilde{\beta}} + 1} \tag{5.66}$$

From the CM in Eq. (5.60), Eve's Holevo information may also be found by

$$\chi(E:\tilde{\beta}|\gamma) = S(E|\gamma) - S(E|\tilde{\beta}\gamma) \tag{5.67}$$

$$= \int p(\gamma)S(\rho_{E|\gamma})\,\mathrm{d}^2\gamma - \int p(\tilde{\beta},\gamma)S(\rho_{E|\tilde{\beta}\gamma})\,\mathrm{d}^2\gamma\,\mathrm{d}^2\tilde{\beta} \tag{5.68}$$

$$= S(\rho_{ab|\gamma}) - S(\rho_{a|\tilde{\beta}\gamma}) \tag{5.69}$$

which is expressed in terms of conditional von Neumann entropies. Then, assuming that Eve's systems $E = E_1'E_2'e$ purify the whole output state, the von Neumann entropy of the state $\rho_{E|\tilde{\beta}\gamma}$ equals that of $\rho_{ab|\tilde{\beta}\gamma}$. A similar equivalence holds between $\rho_{E|\tilde{\beta}\gamma}$ and $\rho_{a|\tilde{\beta}\gamma}$. These entropies can be expressed in terms of the symplectic eigenspectrum $\{v_\pm\}$ of the CM $\mathbf{V}_{ab|\gamma}$ and the symplectic eigenvalue $\tilde{\nu}$ of $\mathbf{V}_{a|\tilde{\beta}\gamma}$, so that

$$\chi(E:\tilde{\beta}|\gamma) = S(\rho_{ab|\gamma}) - S(\rho_{a|\tilde{\beta}\gamma}) = G(v_+) + G(v_-) - G(\tilde{v}) \tag{5.70}$$

The eigenvalues can be calculated from Eq. (3.25) and the bosonic entropic function G is given by Eq. (3.27).

In terms of mutual information, the measurement variables $\tilde{\alpha}$ and $\tilde{\beta}$ in the entanglement-based scheme are equivalent to the rescaled P&M variables α and β. The conditioning on γ is equivalent to a displacement on the variables α and β. Considering these aspects in addition with Remark 2, the key extraction variables $\boldsymbol{x} = (Q_x, P_x)$ and $\boldsymbol{y} = (Q_y, P_y)$ need to be suitably constructed. In fact, the parties use the following relations:

$$Q_x = Q_A - \upsilon_{Q_x} Q_R \tag{5.71}$$

$$P_x = P_A - \upsilon_{P_x} P_R \tag{5.72}$$

$$Q_y = Q_B - \upsilon_{Q_y} Q_R \tag{5.73}$$

$$P_y = P_B - \upsilon_{P_y} P_R \tag{5.74}$$

An optimal option for the various υ-parameters is adopted by considering a minimal correlation between the new variables x and y and the relay outputs. This assumption implies that Eve has the least possible level of knowledge about x and y by knowing γ. Therefore, it is imposed that

$$\langle Q_y Q_R \rangle = \langle Q_x Q_R \rangle = 0 \tag{5.75}$$

$$\langle P_y P_R \rangle = \langle P_x P_R \rangle = 0 \tag{5.76}$$

in order to obtain the formulas for the υ-parameters, as follows:

$$\upsilon_{Q_x} = \frac{\langle Q_A Q_R \rangle}{\langle Q_R^2 \rangle} = \frac{-\tau_A \sigma_A^2}{\tau_B^2 \sigma_B^2 + \tau_A^2 \sigma_A^2 + \sigma_z^2} \tag{5.77}$$

$$\upsilon_{P_x} = \frac{\langle P_A P_R \rangle}{\langle P_R^2 \rangle} = -\upsilon_{Q_x} \tag{5.78}$$

$$\upsilon_{Q_y} = \frac{\langle Q_B Q_R \rangle}{\langle Q_R^2 \rangle} = \frac{\tau_B \sigma_B^2}{\tau_B^2 \sigma_B^2 + \tau_A^2 \sigma_A^2 + \sigma_z^2} \tag{5.79}$$

$$\upsilon_{P_y} = \frac{\langle P_B P_R \rangle}{\langle P_R^2 \rangle} = \upsilon_{Q_y} \tag{5.80}$$

These are the regression coefficients. Given a bipartition of a multivariate Gaussian distribution $\{\boldsymbol{x}_1, \boldsymbol{x}_2\}$ with CM $\boldsymbol{\Sigma}$, the regression coefficients are given by the matrix $\boldsymbol{\Sigma}_{12}\boldsymbol{\Sigma}_{22}^{-1}$. One may write that $\boldsymbol{y} = \boldsymbol{x}_1 | \boldsymbol{x}_2 = \boldsymbol{x}_1 - \boldsymbol{\Sigma}_{12}\boldsymbol{\Sigma}_{22}^{-1}\boldsymbol{x}_2$.

With the assistance of Appendix F, the mutual information can be computed as

$$I(\boldsymbol{x} : \boldsymbol{y}) = I(\alpha : \beta | \gamma) = I(\tilde{\alpha} : \tilde{\beta} | \gamma) \tag{5.81}$$

The quantum mutual information between Eve's system $E = E_1' E_2' e$ and Bob's key extraction variable $\boldsymbol{y}$, given that Eve has access to the variable γ, is determined by [(Renner, 2013, Lemma 7.4.4)]

$$I(E\gamma : \boldsymbol{y}) = \cancelto{0}{I(\boldsymbol{y} : \gamma)} + I(E : \boldsymbol{y} | \gamma) = \chi(E : \boldsymbol{y} | \gamma) \tag{5.82}$$

This quantity is equal to the Holevo information $\chi(E:\boldsymbol{y}|\gamma)$, because $\boldsymbol{y}$ is a classical variable. In particular, given γ, there is a function $\boldsymbol{y}=f(\beta)$ determined by the relations in Eq. (5.73) and Eq. (5.74), such that $\beta=f^{-1}(\boldsymbol{y})$. This allows for the application of the data processing inequality in both directions, with respect to $\boldsymbol{y}$ and β, yielding

$$\chi(E:\boldsymbol{y}|\gamma)=\chi(E:\beta|\gamma) \tag{5.83}$$

At this point, the asymptotic key rate can be defined as

$$R_{\text{asy}}=\beta I(\boldsymbol{x}:\boldsymbol{y})-\chi(E:\boldsymbol{y}|\gamma) \tag{5.84}$$

$$=\beta I(\alpha:\beta|\gamma)-\chi(E:\beta|\gamma) \tag{5.85}$$

which is calculated starting from the CM in Eq. (5.60), as in [Pirandola et al. (2015)].

As in the case of the homodyne and heterodyne protocols, the optimal variances μ_A^{opt} and μ_B^{opt} can also be computed here. Note that, given that the optimization has to take place over two variables, the speed may be considerably slow, depending on the desired interval of variance values.

5.3 Parameter Estimation

In a practical implementation, the parties use the quantum channel a finite number of times. One of the consequences of the finite-size scenario is that the parties do not possess perfect knowledge of the channel parameters T and ξ. Consequently, once the quantum communications are over, Alice and Bob enter the parameter estimation stage. In the homodyne and heterodyne protocols, they declare m random instances $\{x_i\}$ and $\{y_i\}$ of their local variables x and y. In CV-MDI, they announce m instances $\{q_{A_i}\}$, $\{p_{A_i}\}$ and $\{q_{B_i}\}$, $\{p_{B_i}\}$ of their local variables, while also making use of the relative relay output instances $\{q_{R_i}\}$ and $\{p_{R_i}\}$ in their disposal. From these instances, they build the MLEs $\widehat{T}$ of the transmissivity T and $\widehat{\Xi}$ of the excess noise variance Ξ. They achieve this by also exploiting their knowledge of the trusted levels of the detector and setup efficiency η and electronic noise υ_{el}.

It must be noted, that the assumption for the channel is that it is stable over a long time, as it typically is in ground-based fiber implementations. If the channel varies instead over a timescale, then parameter estimation has to be performed independently for each block. The consequence of this would be a different key rate for each block and the final rate would then be given by an average. This is a condition that may occur in free-space quantum communications [Pirandola (2021a)].

5.3.1 Parameter Estimation in Homodyne and Heterodyne Protocols

Following the standard channel estimation method from [Ruppert et al. (2014)],

$$\widehat{T} = \frac{1}{\eta\sigma_x^4}\left(\widehat{\mathbb{C}}_{xy}\right)^2 \tag{5.86}$$

where $\widehat{\mathbb{C}}_{xy}$ is the estimator for the covariance between x and y, computed by

$$\widehat{\mathbb{C}}_{xy} = \frac{1}{m}\sum_{i=1}^{m} x_i y_i \tag{5.87}$$

while the actual covariance is given by

$$\mathbb{C}_{xy} = \sqrt{\eta T}\sigma_x^2 \tag{5.88}$$

This covariance is normally distributed with the following mean and variance:

$$\mathbb{E}(\widehat{\mathbb{C}}_{xy}) = \sqrt{\eta T}\sigma_x^2 = \mathbb{C}_{xy} \tag{5.89}$$

$$\mathbb{V}(\widehat{\mathbb{C}}_{xy}) = \frac{1}{m}\left(2\eta T\left(\sigma_x^2\right)^2 + \sigma_x^2\sigma_z^2\right) = \mathbb{V}_{\mathbb{C}_{xy}} \tag{5.90}$$

Then, $\widehat{T}$ can be expressed as a scaled noncentral chi-squared variable by

$$\widehat{T} = \frac{\mathbb{V}_{\mathbb{C}_{xy}}}{\eta\left(\sigma_x^2\right)^2}\left(\frac{\widehat{\mathbb{C}}_{xy}}{\sqrt{\mathbb{V}_{\mathbb{C}_{xy}}}}\right)^2 \tag{5.91}$$

since $\widehat{\mathbb{C}}_{xy}/\sqrt{\mathbb{V}_{\mathbb{C}_{xy}}}$ follows a standard normal distribution. The mean and variance of $\widehat{T}$ are given by the associated noncentral chi-squared parameters $\kappa = 1$ and $\lambda_{\text{chi}} = \frac{\mathbb{C}_{xy}^2}{\mathbb{V}_{\mathbb{C}_{xy}}}$ as

$$\mathbb{E}(\widehat{T}) = \frac{\mathbb{V}_{\mathbb{C}_{xy}}}{\eta\left(\sigma_x^2\right)^2}\left(1 + \frac{\mathbb{C}_{xy}^2}{\mathbb{V}_{\mathbb{C}_{xy}}}\right) \tag{5.92}$$

$$\mathbb{V}(\widehat{T}) = \frac{2\mathbb{V}_{\mathbb{C}_{xy}}^2}{\eta^2\left(\sigma_x^2\right)^4}\left(1 + 2\frac{\mathbb{C}_{xy}^2}{V_{\mathbb{C}_{xy}}}\right) \tag{5.93}$$

Using Eq. (5.89) and Eq. (5.90) and keeping only the significant terms with respect to $1/m$, the mean and variance become

$$\mathbb{E}(\widehat{T}) = T \tag{5.94}$$

$$\mathbb{V}(\widehat{T}) := \sigma_{\widehat{T}}^2 = \frac{4}{m}T^2\left(2 + \frac{\sigma_z^2}{\eta T\sigma_x^2}\right) \tag{5.95}$$

The estimator for the noise variance σ_z^2 is given by

$$\widehat{\sigma_z^2} = \frac{1}{m}\sum_{i=1}^{m}\left(y_i - \sqrt{\eta\widehat{T}}x_i\right)^2 \tag{5.96}$$

Assuming $\widehat{T} \approx T$ and rescaling the term inside the brackets by $1/\sigma_z$, a standard normal distribution for the variable z_i/σ_z is shaped, with

$$z_i = y_i - \sqrt{\eta T} x_i \tag{5.97}$$

Therefore, the estimated noise variance can be rewritten as

$$\widehat{\sigma_z^2} = \frac{\sigma_z^2}{m} \sum_{i=1}^{m} \left(\frac{z_i}{\sigma_z} \right)^2 \tag{5.98}$$

It can be observed, that this is a scaled chi-squared variable. From the associated chi-squared parameter $\kappa = m$, the following mean and variance can be identified:

$$\mathbb{E}(\widehat{\sigma_z^2}) = \sigma_z^2 \tag{5.99}$$

$$\mathbb{V}(\widehat{\sigma_z^2}) = \frac{2\left(\sigma_z^2\right)^2}{m} \tag{5.100}$$

Then, from the formula of Eq. (5.12), the following relations arise:

$$\widehat{\Xi} = \widehat{\sigma_z^2} - \upsilon_{\mathrm{el}} - V^* \tag{5.101}$$

$$\mathbb{E}(\widehat{\Xi}) = \Xi \tag{5.102}$$

$$\mathbb{V}(\widehat{\Xi}) := \sigma_{\Xi}^2 = \frac{2\left(\sigma_z^2\right)^2}{m} \tag{5.103}$$

For a sufficiently large m and up to an error probability $\varepsilon_{\mathrm{PE}}$, the channel parameters fall in the intervals

$$T \in [\widehat{T} - W\sigma_{\widehat{T}}, \widehat{T} + W\sigma_{\widehat{T}}] \tag{5.104}$$

$$\Xi \in [\widehat{\Xi} - W\sigma_{\widehat{\Xi}}, \widehat{\Xi} + W\sigma_{\widehat{\Xi}}] \tag{5.105}$$

where $\sigma_{\widehat{T}}$, $\sigma_{\widehat{\Xi}}$ are given by the Eq. (5.95) and Eq. (5.103) respectively. The actual values of T and σ_z^2 are replaced by their corresponding estimators. Note that W is expressed in terms of $\varepsilon_{\mathrm{PE}}$ via the inverse error function as

$$W = \sqrt{2}\,\mathrm{erf}^{-1}(1 - \varepsilon_{\mathrm{PE}}) \tag{5.106}$$

The worst-case estimators are given by

$$T_m = \widehat{T} - W\sigma_{\widehat{T}} \tag{5.107}$$

$$\Xi_m = \widehat{\Xi} + W\sigma_{\widehat{\Xi}} \tag{5.108}$$

Up to an error probability $\varepsilon_{\mathrm{PE}}$, these values present a lower bound for the transmissivity $T \geq T_m$ and an upper bound for the excess noise variance $\Xi \leq \Xi_m$. The derivation of T_m, as well as an alternative derivation method, are thoroughly detailed in Appendix E.

The overall failure probability is

$$2\varepsilon_{\mathrm{PE}}(1-\varepsilon_{\mathrm{PE}})+\varepsilon_{\mathrm{PE}}^2 \leq 2\varepsilon_{\mathrm{PE}} \tag{5.109}$$

In the next step, Alice and Bob compute an overestimation of Eve's Holevo bound in terms of T_m and Ξ_m, so that they may write the rate after parameter estimation as

$$R_m = \begin{cases} \beta I(x:y) - \chi(E:y)|_{T_m,\Xi_m} & \text{Homodyne} \\ \beta I(\boldsymbol{x}:\boldsymbol{y}) - \chi(E:\boldsymbol{y})|_{T_m,\Xi_m} & \text{Heterodyne} \end{cases} \tag{5.110}$$

Accounting for the number of signals sacrificed for PE, the effective rate in terms of bits per channel use must align with the rate in Eq. (4.29) by the rescaling $R_m \to \frac{n}{N}R_m$, where

$$n = N - m \tag{5.111}$$

is the number of key generation instances.

Remark 3. In the heterodyne protocol, under the assumption of concatenating the quadratures, one could that hypothesize that the instances n represent measurements, i.e. to every n corresponds either a Q-measurement or a P-measurement. In a data processing environment, as the session under the heterodyne protocol would have double the total states, the amount of both sacrificed and key generation points would also be doubled. In this case, a handful of subsequent notations for n and m would have to be replaced by $2n$ and $2m$ respectively. From a data processing perspective, this would be a more appropriate notation, as it pinpoints where the doubling of the states should take place. However, any occurrence of n, m or any of their derivative quantities, always pertains to signal states in a secret key rate formula. To avoid confusion, the adopted notation for the aforementioned measures throughout the parameter estimation section concerns signal states and is thus the same for the homodyne and heterodyne protocols.

Note that, from the estimators $\widehat{T}$ and $\widehat{\Xi}$, the parties may compute an estimator for the SNR using the formula

$$\widehat{\mathrm{SNR}} = \frac{(\mu-1)\eta\widehat{T}}{\upsilon_{\mathrm{el}} + \widehat{\Xi} + V^*} \tag{5.112}$$

By extension, the estimated SNR is used to calculate the estimated mutual information:

$$I(x:y)|^{\mathrm{hom}}_{\widehat{T},\widehat{\Xi}} = \frac{1}{2}\log_2\left(1+\widehat{\mathrm{SNR}}\right) \qquad I(\boldsymbol{x}:\boldsymbol{y})|^{\mathrm{het}}_{\widehat{T},\widehat{\Xi}} = \log_2\left(1+\widehat{\mathrm{SNR}}\right) \tag{5.113}$$

Therefore, in a more practical implementation, the rate in Eq. (5.110) is replaced by

$$R_m = \begin{cases} \frac{n}{N}\left(\beta I\,(x:y)|_{\widehat{T},\widehat{\Xi}} - \chi(E:y)|_{T_m,\Xi_m}\right) & \text{Homodyne} \\ \frac{n}{N}\left(\beta I\,(\boldsymbol{x}:\boldsymbol{y})|_{\widehat{T},\widehat{\Xi}} - \chi(E:\boldsymbol{y})|_{T_m,\Xi_m}\right) & \text{Heterodyne} \end{cases} \tag{5.114}$$

In practice, the data generated for a CV-QKD protocol are sliced in $n_{\text{bks}} \gg 1$ blocks. Assuming the channel remains sufficiently stable over time, the statistics, which include the estimators and the worst-case values, can be computed over

$$M = mn_{\text{bks}} \gg m \tag{5.115}$$

random instances. This way, all the estimators, i.e, $\widehat{T}$, $\widehat{\Xi}$, T_m, and Ξ_m, are computed over M points. Making the replacement $R_m \to R_M$ in Eq. (5.114), the rate is reshaped under the worst-case estimators T_M and Ξ_M as

$$R_M = \begin{cases} \frac{n}{N}\left(\beta I\left(x:y\right)|_{\widehat{T},\widehat{\Xi}} - \chi(E:y)|_{T_M,\Xi_M}\right) & \text{Homodyne} \\ \frac{n}{N}\left(\beta I\left(\boldsymbol{x}:\boldsymbol{y}\right)|_{\widehat{T},\widehat{\Xi}} - \chi(E:\boldsymbol{y})|_{T_M,\Xi_M}\right) & \text{Heterodyne} \end{cases} \tag{5.116}$$

This also means that an average of

$$m = \frac{M}{n_{\text{bks}}} \tag{5.117}$$

points are revealed for parameter estimation from each block and an average number of

$$n = N - \frac{M}{n_{\text{bks}}} \tag{5.118}$$

key generation points from each block are left to be processed during the error correction step. If N is adequately large, the variations around the averages can be regarded as negligible, meaning that m and n are assumed to be the actual values for each block.

5.3.2 Parameter Estimation in the CV-MDI Protocol

For CV-MDI, the adopted PE method is derived from [Papanastasiou et al. (2017)]. An alternative way is described in Appendix E.3, based on extra simplifying assumptions. Based on m samples $[Q_A]_i$,$[Q_B]_i$, $[Q_R]_i$, for $i = 1, \ldots, m$, the parties calculate the MLEs

$$\mathbb{C}(Q_A, Q_R) = \langle Q_A Q_R \rangle = -\tau_A \sigma_A^2 \tag{5.119}$$

$$\mathbb{C}(Q_B, Q_R) = \langle Q_B Q_R \rangle = \tau_B \sigma_B^2 \tag{5.120}$$

of the covariances. These estimators are given by

$$\widehat{C}_{Q_A Q_R} = \frac{1}{m}\sum_{i=1}^{m}[Q_A]_i[Q_R]_i \tag{5.121}$$

$$\widehat{C}_{Q_B Q_R} = \frac{1}{m}\sum_{i=1}^{m}[Q_B]_i[Q_R]_i \tag{5.122}$$

$$\widehat{C}_{P_A P_R} = \frac{1}{m}\sum_{i=1}^{m}[P_A]_i[P_R]_i \tag{5.123}$$

$$\widehat{C}_{P_B P_R} = \frac{1}{m}\sum_{i=1}^{m}[P_B]_i[P_R]_i \tag{5.124}$$

From these, they define estimators for T_A and T_B as

$$\widehat{T}_A = \frac{2}{\eta(\sigma_A^2)^2}\min\{|\widehat{C}_{Q_AQ_R}|^2, |\widehat{C}_{P_AP_R}|^2\} \tag{5.125}$$

$$\widehat{T}_B = \frac{2}{\eta(\sigma_B^2)^2}\min\{|\widehat{C}_{Q_BQ_R}|^2, |\widehat{C}_{P_BP_R}|^2\} \tag{5.126}$$

and an estimator for σ_z^2 as

$$\begin{aligned}\widehat{\sigma}_z^2 = \max\Bigg\{&\frac{1}{m}\sum_{i=1}^{m}\left([Q_R]_i + \widehat{\tau}_A[Q_A]_i - \widehat{\tau}_B[Q_B]_i\right)^2, \\ &\frac{1}{m}\sum_{i=1}^{m}\left([P_R]_i - \widehat{\tau}_A[P_A]_i - \widehat{\tau}_B[P_B]_i\right)^2\Bigg\}\end{aligned} \tag{5.127}$$

with

$$\widehat{\tau}_A = \sqrt{\frac{\eta\widehat{T}_A}{2}} \tag{5.128}$$

$$\widehat{\tau}_B = \sqrt{\frac{\eta\widehat{T}_B}{2}} \tag{5.129}$$

They obtain the associated variances, whose derivation is analyzed in Appendix E.2, as

$$\sigma^2_{\widehat{T}_A} \simeq \frac{4\widehat{T}_A}{m}\left[\widehat{T}_A + \frac{\widehat{T}_B}{2}\frac{\sigma_B^2}{\sigma_A^2}\right]\left(2 + \frac{2\widehat{\sigma}_z^2/\eta}{\widehat{T}_A\sigma_A^2 + \frac{\widehat{T}_B}{2}\sigma_B^2}\right) \tag{5.130}$$

$$\sigma^2_{\widehat{T}_B} \simeq \frac{4\widehat{T}_B}{m}\left[\widehat{T}_B + \frac{\widehat{T}_A}{2}\frac{\sigma_A^2}{\sigma_B^2}\right]\left(2 + \frac{2\widehat{\sigma}_z^2/\eta}{\widehat{T}_B\sigma_B^2 + \frac{\widehat{T}_A}{2}\sigma_A^2}\right) \tag{5.131}$$

Based on $\widehat{\sigma}_z^2$, they find an estimator for Ξ, given by

$$\widehat{\Xi} = \widehat{\sigma}_z^2 - \upsilon_{\mathrm{el}} - 1 \tag{5.132}$$

with variance, which is again examined in Appendix E.2, equal to

$$\sigma^2_{\widehat{\Xi}} := \mathbb{V}_z \simeq \frac{2(\widehat{\sigma}_z^2)^2}{m} \tag{5.133}$$

Finally, given the PE error $\varepsilon_{\mathrm{PE}}$, the worst-case scenario values can be derived by

$$T_{M_A} = \widehat{T}_A - W\sigma_{\widehat{T}_A} \tag{5.134}$$

$$T_{M_B} = \widehat{T}_B - W\sigma_{\widehat{T}_B} \tag{5.135}$$

$$\Xi_M = \widehat{\Xi} + W\sigma_{\widehat{\Xi}} \tag{5.136}$$

where W is given in Eq. (5.106).

Using the aforementioned values, the parties can compute a secret key rate under an overestimated Holevo information as

$$R_m = \beta I(\boldsymbol{x} : \boldsymbol{y})|_{\widehat{T}_A,\widehat{T}_B,\widehat{\Xi}} - \chi(E : \boldsymbol{y}|\gamma)|_{\widetilde{T}_A,\widetilde{T}_B,\widetilde{\Xi}} \tag{5.137}$$

Note here that Remark 3 fully applies in the case of CV-MDI as well. Repeating the relations for the sake of completeness, the sacrificed instances per block are obtained by

$$m = N - n \tag{5.138}$$

where N is the number of signals sent through the channel and n is the number of signals devoted to secret key extraction for each block. In a practical situation, where the transmission can be assumed stable over a large number of blocks n_{bks}, m signals can be used on average from each block, in order to estimate the channel parameters. Therefore, during the parameter estimation stage, the parties sacrifice a total of

$$M = mn_{\text{bks}} \tag{5.139}$$

states and the corresponding rate is determined by

$$R_m \to R_M = \Big[\beta I(\boldsymbol{x} : \boldsymbol{y})|_{\widehat{T}_A,\widehat{T}_B,\widehat{\Xi}} - \chi(E : \boldsymbol{y}|\gamma)|_{T_{M_A},T_{M_B},\Xi_M}\Big]_{m=M} \tag{5.140}$$

The mutual information and the correlation between the two Gaussian variables x and y are connected by Eq. (F.2) as follows:

$$I(\boldsymbol{x} : \boldsymbol{y}) = \log_2(1 + \text{SNR}) = \log_2\left[(1 - \rho^2_{\boldsymbol{xy}})^{-1}\right] \tag{5.141}$$

The estimator for the correlation between the variables can be derived by setting the MLEs of the transmissivities and noise into the mutual information as

$$\widehat{\rho}_{\boldsymbol{xy}} = \sqrt{1 - 2^{-I(\boldsymbol{x}:\boldsymbol{y})}} \tag{5.142}$$

To prepare for the data processing stages, Alice and Bob apply the transformations of Eq. (5.71) - Eq. (5.74), based on the quantities in Eq. (5.77) - Eq. (5.80), calculated via the MLEs. Following Remark 1, the parties combine their data from the Q and P quadratures into a single variable. In particular, they apply the following mapping:

$$[x]_{2i-1} = [Q_x]_i \tag{5.143}$$
$$[x]_{2i} = [P_x]_i \tag{5.144}$$
$$[y]_{2i-1} = [Q_y]_i \tag{5.145}$$
$$[y]_{2i} = [P_y]_i \tag{5.146}$$

in order to obtain $2n$ samples from each block. This implies that the principles of Appendix C are then applied to CV-MDI as well.

5.4 Preprocessing

After obtaining estimates of the channel parameters, the parties proceed to the key extraction process. Having sacrificed a total of M states during parameter estimation, they will now attempt to form correlated sequences using their remaining pairs of key generation states. From this stage onwards, the three protocols follow a similar path; any differences between them lie mostly in the formulas.

Remark 4. Because of the assumed quadrature concatenation in the heterodyne and CV-MDI protocols, the processing of data in numerous steps requires double the amount of key generation points. To avoid repetition by constantly differentiating between the protocols, the count of key generation instances for a single block will onward be denoted, where necessary, by

$$n^* = \begin{cases} n & \text{Homodyne} \\ 2n & \text{Heterodyne \& CV-MDI} \end{cases} \tag{5.147}$$

Note that in equations describing key rates, the notation strictly refers to signal states and is therefore n.

5.4.1 Normalization

In each block of size N, Alice and Bob have n pairs $\{x_i, y_i\}$ of their variables x and y, that are related by Eq. (5.11). This yields a total of

$$n_{\text{tot}} = n_{\text{bks}} n^* \tag{5.148}$$

instances, which can be used for key generation.

It is assumed here that the variables x and y have a zero mean value. Alternatively, the parties subtract the mean value $\bar{x}$ and $\bar{y}$ of x and y respectively from their instances to create updated centered variables $x \leftarrow x - \bar{x}$ and $y \leftarrow y - \bar{y}$. As a first step, Alice and Bob concatenate the n samples from each block, in order to estimate the variance of their sequences as

$$\widehat{\sigma_x^2} = \frac{1}{n_{\text{tot}}} \sum_{k=1}^{n_{\text{tot}}} [x]_k^2 \tag{5.149}$$

$$\widehat{\sigma_y^2} = \frac{1}{n_{\text{tot}}} \sum_{i=1}^{n_{\text{tot}}} [y]_k^2 \tag{5.150}$$

Then, using the standard deviations

$$\widehat{\sigma_x} = \sqrt{\widehat{\sigma_x^2}} \tag{5.151}$$

$$\widehat{\sigma_y} = \sqrt{\widehat{\sigma_y^2}} \tag{5.152}$$

they create the normalized samples $[x]_i \to [X]_i$ and $[y]_i \to [Y]_i$, as seen below:

$$X = \frac{x}{\widehat{\sigma_x}} \tag{5.153}$$

$$Y = \frac{y}{\widehat{\sigma_y}} \tag{5.154}$$

Variables X and Y follow a standard normal bivariate distribution with correlation ρ, given by

$$\rho_{XY} = \mathbb{E}(XY) \tag{5.155}$$

In a practical scenario, neither party can access the other's variables. Recalling that the correlation parameter is connected to the SNR by Eq. (5.22), an estimator $\widehat{\rho}_{XY}$ for the correlation can be measured using the estimated SNR, which is approximated by Eq. (5.112). The variables X and Y now also have the following CM:

$$\mathbf{\Sigma}_{XY} = \begin{bmatrix} 1 & \rho_{XY} \\ \rho_{XY} & 1 \end{bmatrix} \tag{5.156}$$

5.4.2 Discretization

Bob discretizes his normalized variable Y in a p-ary variable K, with generic value $k \in \{0, \ldots, 2^p - 1\}$ being an element of a Galois field $\mathcal{GF}(2^p)$. Information on this class of finite fields can be found in Appendix B.1. This is achieved by partitioning the real space $\mathcal{R}$ into intervals or bins. The approach of [Furrer et al. (2012)] is followed here, wherein the security proof requires that the range $[-\alpha, \alpha)$ is divided into constant-size intervals of size $\delta > 0$. Bob sets the cut-off parameter α, such that $|Y| \geq \alpha$ occurs with negligible probability. This is approximately true for $\alpha \geq 3$. The outcomes that fall under $(-\infty, -\alpha]$ and $[\alpha, \infty)$ are allocated to their respective neighboring intervals in $[-\alpha, \alpha)$. Then, the border points of the bins $[J_k^-, J_k^+)$ are defined as [Pacher et al. (2016)]

$$J_k^- = \begin{cases} -\infty & \text{if } k = 0 \\ -\alpha + k\delta & \text{if } k > 0 \end{cases} \tag{5.157}$$

$$J_k^+ = \begin{cases} -\alpha + (k+1)\delta & \text{if } k < 2^p - 1 \\ \infty & \text{if } k = 2^p - 1 \end{cases} \tag{5.158}$$

where the one-dimensional lattice step δ is given by

$$\delta = \frac{\alpha}{2^{p-1}} \tag{5.159}$$

Finally, for any value of $Y \in [J_k^-, J_k^+)$, Bob takes K equal to k. Thus, for n^* points, the normalized string Y^{n^*} is transformed into a string of discrete values K^{n^*}. Note that this discretization technique is very basic. The performance of the protocol could potentially improve by employing bins of different sizes, based on the estimated SNR.

5.4.3 Splitting

Bob sets an integer value for $q < p$ and computes the number of bottom bits d as

$$d = p - q \tag{5.160}$$

Then, he splits his discretized variable in two parts $K = (\overline{K}, \underline{K})$, where the top variable $\overline{K}$ is q-ary and the bottom variable $\underline{K}$ is d-ary. Their values are defined by splitting the generic value k in the following two parts

$$\overline{k} = \frac{k - (k \bmod 2^d)}{2^d} \tag{5.161}$$

$$\underline{k} = k \bmod 2^d \tag{5.162}$$

Combining the two parts yields

$$k = \overline{k} 2^d + \underline{k} \tag{5.163}$$

With the top variable $\overline{K}$, Bob creates 2^q super bins, each containing 2^d bins, associated with the bottom variable $\underline{K}$. This process is clearly illustrated in Fig. 5.2.

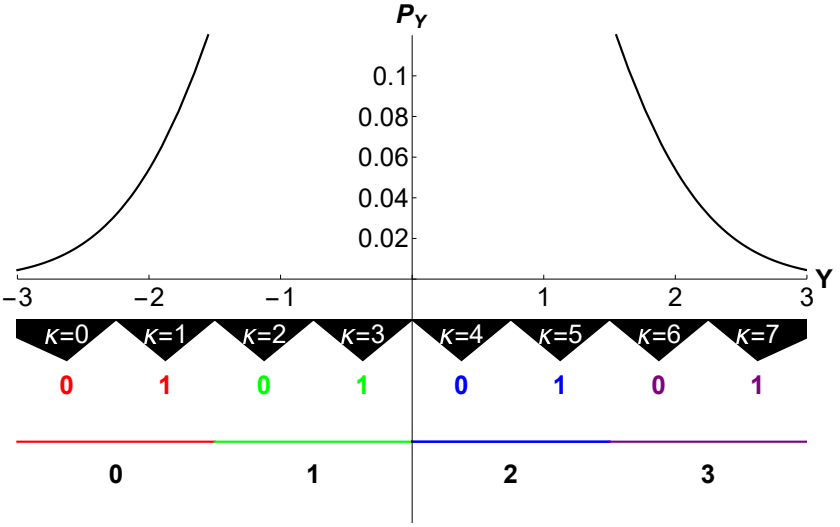

Figure 5.2: Discretization and splitting with $\alpha = 3$, $p = 3$ and $q = 2$. The variable Y follows a normal distribution $\mathcal{Y}$, so that the probability of $|Y| > 3$ is assumed to be negligible. Variable Y and the bins defined in Eq. (5.157) and Eq. (5.158) identify a discrete variable K with values $k = 0, \ldots, 7$ (black triangles). During the splitting stage, each bin can be described by two numbers: $\overline{k} = 0 \ldots, 3$ associated with $q = 2$, and $\underline{k} = 0, 1$ associated with $d = p - q = 1$. It can be observed, that 2^d bins belong to each super bin $\overline{k}$ (colored intervals).

Repeating this for n^* points provides a string of values $\overline{K}^{n^*}$ for the super bins and another string for the relative bin-positions $\underline{K}^{n^*}$. The most significant string $\overline{K}^{n^*}$ is locally processed by an LDPC code, while the least significant string $\underline{K}^{n^*}$ serves as the side information, which is revealed through the public channel to assist in the decoding.

5.5 Syndrome Calculation

In a practical scenario, before communications commence, Alice and Bob already share a multitude of LDPC matrices for the decoding process. Depending on the block length and the code rate obtained from the data, they opt for a suitable matrix. In this setting, it is assumed that the parties do not share any matrices beforehand. For the construction of the parity-check matrix, the code rate needs to be known. The following steps will handle the computation of the code rate, the creation of the LDPC code and, ultimately, the calculation of the syndrome.

As a consequence of the classical data processing inequality, Alice and Bob's mutual information may decrease with every preprocessing step, as suggested by

$$I(x:y) \geq I(X:Y) \geq I(X:K) = H(K) - H(K|X) \geq H(K) - \text{leak}_{\text{EC}} \tag{5.164}$$

The same principle applies for the heterodyne and CV-MDI protocols, where $I(x:y) \to I(\boldsymbol{x}:\boldsymbol{y})$. An analysis about the single-quadrature variable K for the heterodyne and CV-MDI protocols can be found in Appendix C.2. Here, $\text{leak}_{\text{EC}} \geq H(K|X)$ comes from the Slepian-Wolf bound and $H(K)$ is the Shannon entropy of K, which, under channel stability conditions, is computed over the entire record of Bob's key generation points. A maximum-likelihood entropy estimator $\widehat{H}(K)$ is empirically calculated by

$$\widehat{H}(K) = -\sum_{k=0}^{2^p-1} \mathsf{f}_k \log_2 \mathsf{f}_k \tag{5.165}$$

where

$$\mathsf{f}_k = \frac{n_k}{n_{\text{tot}}} \tag{5.166}$$

stands for the frequency of a symbol k, that is, the ratio of the appearance times of k over the entire amount of key generation states. Performing an estimation of the entropy is associated with a penalty, as follows [Antos and Kontoyiannis (2001)]:

$$H(K) \geq \widehat{H}(K) - \delta_{\text{ent}} \tag{5.167}$$

with

$$\delta_{\text{ent}} = \log_2(n_{\text{tot}}) \sqrt{\frac{2\ln(2/\varepsilon_{\text{ent}})}{n_{\text{tot}}}} \tag{5.168}$$

It is worth noting that the base of the first log is 2, while the base of the second one is e. This bound is valid up to an error probability ε_{ent}, described in Sec. 4.9.

In Eq. (5.164), the leakage leak_{EC} is upper-bounded by the equivalent number of bits per use, that are broadcast after the application of the LDPC matrix in each block, as

$$\text{leak}_{\text{EC}} \leq d + \frac{lq}{n} \tag{5.169}$$

Here, l stands for the matrix rows. Evidently, d should be as small as possible, in order to minimize the leakage, yet not negligible, so that the reconciliation scheme can succeed.

Combining the expressions of Eq. (5.164), Eq. (5.167) and Eq. (5.169) results in

$$I(x:y) \geq \beta I(x:y) = \widehat{H}(K) - \delta_{\text{ent}} + R_{\text{code}} q - p \tag{5.170}$$

Correspondingly, $I(x:y) \to I(\boldsymbol{x}:\boldsymbol{y})$ for the heterodyne and CV-MDI cases. It must be noted, that in a practical implementation Alice and Bob do not have access to $I(x:y)$, but rather $I(x:y)|_{\widehat{T},\widehat{\Xi}}$ from Eq. (5.113). Considering this modification in Eq. (5.170) and reordering the equation, the practical reconciliation efficiency of the protocol is

$$\beta = \begin{cases} \dfrac{\widehat{H}(K) - \delta_{\text{ent}} + R_{\text{code}} q - p}{I(x:y)|_{\widehat{T},\widehat{\Xi}}} & \text{Homodyne} \\ 2\dfrac{\widehat{H}(K) - \delta_{\text{ent}} + R_{\text{code}} q - p}{I(x:y)|_{\widehat{T},\widehat{\Xi}}} & \text{Heterodyne \& CV-MDI} \end{cases} \tag{5.171}$$

where the term 2 in the second case accounts for the presence of both quadratures. If β is defined in terms of $\widehat{\text{SNR}}$ instead of $I(x:y)|_{\widehat{T},\widehat{\Xi}}$, the two equations are identical. Subsequently, the code rate for all cases can be identified under the same relation through $\widehat{\text{SNR}}$. From Eq. (5.113) and Eq. (5.171), the LDPC code must be chosen to have rate

$$R_{\text{code}} \simeq \frac{\frac{\beta}{2}\log_2\left(1 + \widehat{\text{SNR}}\right) + p - \widehat{H}(K) + \delta_{\text{ent}}}{q} \tag{5.172}$$

The estimator for the SNR is given in Eq. (5.112). Besides the already known $\beta \leq 1$ and $R_{\text{code}} \leq 1$, two more restrictions have to be enforced: $\alpha \geq 3$ and $q < p$. Once R_{code} is established, the sparse parity-check matrix $\mathbf{H}$ of the LDPC code can be constructed.

Alice and Bob may now share a regular $l \times n^*$ low-density parity-check matrix $\mathbf{H}$. The column weight can be given to the matrix as input. Then, Eq. (2.16) can be rearranged to solve for the row weight w_{r}, as

$$w_{\text{r}} = \frac{1 - R_{\text{code}}}{w_{\text{c}}} = \frac{l}{n^* w_{\text{c}}} \tag{5.173}$$

Using the guidelines from [(MacKay and Neal, 1996, Construction 1A)], the matrix must:

- have a weight per row w_{r} as uniform as possible
- have a weight per column w_{c} as uniform as possible
- have columns, whose inner product is 1

After construction, the non-zero elements of the matrix are replaced by random q-ary entries from $\mathcal{GF}(2^q)$. This replacement can take place in a completely random manner [(Tomlinson et al., 2017, Chapter 12.1.3)].

The matrix is then applied to the top string $\overline{K}^{n^*}$ to derive the l-long syndrome

$$K_{\text{syn}}^{l} = \mathbf{H}\overline{K}^{n^*} \tag{5.174}$$

where the matrix-vector product is defined in $\mathcal{GF}(2^q)$. The syndrome is sent to Alice together with the direct communication of the bottom string $\underline{K}^{n^*}$ through the public classical channel, meaning the bottom sequence is publicly revealed. The maximum length of the data sent by Bob for reconciliation per channel use is $p - R_{\text{code}}q$ bits.

5.6 Decoding

From the knowledge of the syndrome K_{syn}^{l}, Bob's bottom string $\underline{K}^{n^*}$ and her local string X^{n^*}, Alice decodes her guess $\widehat{K}^{n^*}$ of Bob's top string $\overline{K}^{n^*}$. This is done via a non-binary sum-product algorithm, where Alice updates a suitable likelihood function during every iteration [Davey and MacKay (1998)]. Before the algorithm starts, the initial value of the likelihood function originates from the a priori probabilities [Pacher et al. (2016)]

$$p(\overline{K}|X,\underline{K}) = \frac{p(\overline{K},\underline{K}|X)}{\sum_{\overline{K}} p(\overline{K},\underline{K}|X)} \tag{5.175}$$

where

$$p(\overline{K},\underline{K}|X) = P(K|X) = \frac{1}{2}\text{erf}\left(\frac{J_k^+ - X\widehat{\rho}}{\sqrt{2(1-\widehat{\rho}^2)}}\right) - \frac{1}{2}\text{erf}\left(\frac{J_k^- - X\widehat{\rho}}{\sqrt{2(1-\widehat{\rho}^2)}}\right) \tag{5.176}$$

is the conditional probability of K, given Alice's variable X, and erf is the error function. The interval border points J_k^- and J_k^+ are given in Eq. (5.157) and (5.158) respectively.

During every iteration iter $\leq$ iter$_{\text{max}}$, Alice finds the argument, that maximizes the likelihood function. If the syndrome of this argument is equal to K_{syn}^{l}, then the argument forms her guess $\widehat{K}^{n^*}$ of Bob's top string $\overline{K}^{n^*}$. However, if the syndromes are not equal within the maximum number of iterations iter$_{\text{max}}$, the block is discarded. The adaptation of the sum-product algorithm implemented for this step is detailed in Appendix A.

The possibility of failure during syndrome decoding reduces the total number of input blocks from n_{bks} to

$$n_{\text{bks}}^{\text{syn}} = p_{\text{syn}} n_{\text{bks}} \tag{5.177}$$

where p_{syn} is the probability of successful decoding within the fixed iter$_{\text{max}}$ iterations. If the syndrome of $\widehat{K}^{n^*}$ is equal to K_{syn}^{l}, then Alice's guess $\widehat{K}^{n^*}$ of Bob's top string $\overline{K}^{n^*}$ is promoted to the next verification step. If syndrome decoding fails for iter$_{\text{max}}$ iterations, the block is discarded and the probability $1 - p_{\text{syn}}$ of this event is registered.

5.7 Verification

The final step of the information reconciliation stage involves the verification of the $n_{\text{bks}}^{\text{syn}}$ decoded blocks. The parties possess two n^*-long q-ary strings with identical syndromes, i.e., Bob's top string $\overline{K}^{n^*}$ and Alice's guess $\widehat{K}^{n^*}$, for each of these blocks. The parties convert their strings into a binary representation, $\overline{K}_{\text{bin}}^{n^*}$ and $\widehat{K}_{\text{bin}}^{n^*}$, so that each of them is qn^* bit long. Alice and Bob employ universal hashing to compute t-bit long hashes of their converted binary strings according to [Thorup (2015)]. The length t is determined from Eq. (4.32) and is completely dependent on the correctness error ε_{cor}. For the chosen family $\mathcal{F}$ of this class of universal hash functions, the correctness error is set to $\varepsilon_{\text{cor}} = 2^{-32}$, returning a hash output length of $t = 32$ bits.

For every block, each pair of promoted strings $\overline{K}^{n^*}$ and $\widehat{K}^{n^*}$ is converted to a binary representation $\overline{K}_{\text{bin}}^{n^*}$ and $\widehat{K}_{\text{bin}}^{n^*}$. The binary strings are segmented into J-bit strings, which are then converted into J-ary numbers to form the strings $\overline{K}_J^{n'}$ and $\widehat{K}_J^{n'}$. Here, n' must be an integer. If this is not the case, the strings $\overline{K}_{\text{bin}}^{n^*}$ and $\widehat{K}_{\text{bin}}^{n^*}$ are padded with σj zeros, so that n' becomes an integer, as follows:

$$n' = \begin{cases} \dfrac{nq}{J} & \text{if } \dfrac{nq}{J} \in \mathcal{Z} \\ \dfrac{(n+\sigma)j}{J} & \text{if } \dfrac{nq}{J} \notin \mathcal{Z} \end{cases}, \; J > j \tag{5.178}$$

Bob then derives independent uniform random integers $u_i = 1, \ldots, 2^{J^*} - 1 \sim \mathcal{U}$ for $i = 1, \ldots, n'$, where u_i is odd, an integer $u_{\text{ext}} = 0, \ldots, 2^{J^*} - 1$ and $J^* \leq J + t - 1$, with $\varepsilon_{\text{cor}} \leq 2^{-t}$ being the target collision probability. After Bob communicates his choice of families to Alice, they both hash each of the J-ary numbers and combine the results, according to the function

$$h\left(x'\right) = \left(\sum_{i=1}^{n'} u_i x_i\right) + u_{\text{ext}} \tag{5.179}$$

where $x' = \overline{K}_Q^{n'}$ for Bob and $x' = \widehat{K}_J^{n'}$ for Alice. Here, summation and multiplication are modulo 2^{J^*}. In practice, this is done by discarding the overflow, which is the number of bits over J^* of $h(x')$. Finally, they keep only the first t bits, in order to form the hashes.

Eventually, Bob discloses his hash output to Alice, who compares it with hers. If the outputs are identical, the verification stage is deemed successful. The original strings $\overline{K}_{\text{bin}}^{n^*}$ and $\widehat{K}_{\text{bin}}^{n^*}$ are also identical, up to a small error probability $2^{-t} \leq \varepsilon_{\text{cor}}$. In a successful case, the associated bottom string $\underline{K}^{n^*}$ held by both parties is also converted into a binary form $\underline{K}_{\text{bin}}^{n^*}$ and appended to the respective strings, forming the sequences

$$S_B = \overline{K}_{\text{bin}}^{n^*} \underline{K}_{\text{bin}}^{n^*} \simeq S_A = \widehat{K}_{\text{bin}}^{n^*} \underline{K}_{\text{bin}}^{n^*} \tag{5.180}$$

Every sequence S_A and S_B progresses to the final stage with a bit length of

$$\tilde{n} = pn^* \tag{5.181}$$

By contrast, if the hashes are different, the two strings are discarded, together with the public bottom string. Therefore, associated with the hash verification test, there is a probability of success, denoted by p_{ver}, which is implicitly connected with ε_{cor}. In fact, a smaller ε_{cor} implies the need for a larger hash verification length, meaning that the probability of spotting an uncorrected error in the strings also becomes larger. This may potentially lead to a reduction of the verification success probability p_{ver}. Combining the possible failures in syndrome decoding and hash verification, the total probability of success for error correction is given by

$$p_{\text{EC}} = p_{\text{syn}} p_{\text{ver}} = 1 - \text{FER} \tag{5.182}$$

where FER stands for frame error rate.

5.8 Composable Key Rate Calculation

After error correction, Alice and Bob are left with $p_{\text{EC}} n_{\text{bks}}$ successfully corrected binary strings, each of them being represented by Eq. (5.180) and containing $\tilde{n}$ bits. The next step is to calculate the composable key rate R, which will indicate the possibility of creating a shared secret key. If $R \leq 0$, the protocol is aborted, as communication is not considered secure. Otherwise, the protocol proceeds to the privacy amplification stage. Initially, the key rate under all accounted finite-size effects has to be determined. These include the sacrificed states, the estimated channel parameters and the error correction success rate. Following Eq. (4.30), the finite-size effects key rate is calculated as

$$R_M^{\text{EC}} = \begin{cases} \dfrac{np_{\text{EC}}}{N}\left(\beta I(x:y)|_{\widehat{T},\widehat{\Xi}} - \chi(E:y)|_{T_M,\Xi_M}\right) & \text{Homodyne} \\ \dfrac{np_{\text{EC}}}{N}\left(\beta I(\boldsymbol{x}:\boldsymbol{y})|_{\widehat{T},\widehat{\Xi}} - \chi(E:\boldsymbol{y})|_{T_M,\Xi_M}\right) & \text{Heterodyne} \\ \dfrac{np_{\text{EC}}}{N}\left(\beta I(\boldsymbol{x}:\boldsymbol{y})|_{\widehat{T}_A,\widehat{T}_B,\widehat{\Xi}} - \chi(E:\beta|\gamma)|_{T_{M_A},T_{M_B},\Xi_M}\right) & \text{CV-MDI} \end{cases} \tag{5.183}$$

In case $R_M^{\text{EC}} \leq 0$, Alice and Bob abort the protocol without further consideration.

The composable secret key rate is presented in Eq. (4.34). Here, the term Δ_{AEP} is given by [Pirandola (2021a), Pirandola (2022)]

$$\Delta_{\text{AEP}} = \begin{cases} 4\log_2\left(2^{p/2}+2\right)\sqrt{\log_2\left(\frac{18}{p_{\text{EC}}^2\varepsilon_{\text{s}}^4}\right)} & \text{Homodyne} \\ 4\log_2\left(2^{p}+2\right)\sqrt{\log_2\left(\frac{18}{p_{\text{EC}}^2\varepsilon_{\text{s}}^4}\right)} & \text{Heterodyne \& CV-MDI} \end{cases} \tag{5.184}$$

and the Θ term is defined as follows:

$$\Theta = \log_2[p_{\text{EC}}(1 - \frac{\varepsilon_s^2}{3})] + 2\log_2\sqrt{2}\varepsilon_h \tag{5.185}$$

Note that in the heterodyne and CV-MDI protocols, the discretization bits p in Δ_{AEP} provide a total dimension of 2^{2p} per symbol. This effect is a consequence of the virtual concatenation, described in detail in Appendix C.1.

After error correction, Alice Bob and Eve share a classical-classical-quantum (CCQ) state $\tilde{\rho}^n$, which, following Eq. (4.31), is given by

$$p_{\text{EC}} D(\tilde{\rho}^n, \rho_{\text{id}}) \leq \varepsilon = \varepsilon_{\text{sec}} + \varepsilon_{\text{cor}} \tag{5.186}$$

where ε is the epsilon security of the protocol, D is the trace distance and ρ_{id} is the output of an ideal protocol, where Eve is completely decoupled from Bob, with Alice's and Bob's keys being exactly the same [Pirandola (2021a)].

The CCQ state $\tilde{\rho}^n$ can be rewritten as a worst-case scenario state $\tilde{\rho}^n_{\text{wc}}$, when considering the estimation of the channel parameters of Eq. (5.107) and Eq. (5.108) and the entropy estimation of Eq.(5.167) in the calculation of the key rate. However, there is still a small probability ε'_{PE}, which involves a different state ρ_{bad} overstepping the bounds associated with the worst-case estimators. On average, the state becomes

$$\rho_{\text{PE}} = (1 - \varepsilon'_{\text{PE}})\tilde{\rho}^n_{\text{wc}} + \varepsilon'_{\text{PE}}\rho_{\text{bad}} \tag{5.187}$$

Because of the composable distance of Eq. (5.186) and the implication of the previous equation, $D(\tilde{\rho}^n_{\text{wc}}, \rho_{\text{PE}}) \leq \varepsilon'_{\text{PE}}$, the triangle inequality provides

$$p_{\text{EC}} D(\rho_{\text{PE}}, \rho_{\text{id}}) \leq \varepsilon + p_{\text{EC}}\varepsilon'_{\text{PE}} \tag{5.188}$$

This means meaning that the imperfect parameter estimation adds an extra term $p_{\text{EC}}\varepsilon'_{\text{PE}}$ to the epsilon security of the protocol. In other words, the protocol is secure up to redefining $\varepsilon \to \varepsilon + p_{\text{EC}}\varepsilon'_{\text{PE}}$. Note that

$$\varepsilon'_{\text{PE}} = (1 - 2\varepsilon_{\text{PE}})\varepsilon_{\text{ent}} + (1 - \varepsilon_{\text{ent}})2\varepsilon_{\text{PE}} + 2\varepsilon_{\text{PE}}\varepsilon_{\text{ent}} \simeq 2\varepsilon_{\text{PE}} + \varepsilon_{\text{ent}} \tag{5.189}$$

which returns the overall epsilon security ε of the protocol as

$$\varepsilon = \varepsilon_{\text{sec}} + \varepsilon_{\text{cor}} + p_{\text{EC}}\varepsilon'_{\text{PE}} \simeq \begin{cases} \varepsilon_{\text{s}} + \varepsilon_{\text{h}} + \varepsilon_{\text{cor}} + p_{\text{EC}}(2\varepsilon_{\text{PE}} + \varepsilon_{\text{ent}}) \\ \quad \text{Homodyne \& Heterodyne} \\ \varepsilon_{\text{s}} + \varepsilon_{\text{h}} + \varepsilon_{\text{cor}} + p_{\text{EC}}(3\varepsilon_{\text{PE}} + \varepsilon_{\text{ent}}) \\ \quad \text{CV-MDI} \end{cases} \tag{5.190}$$

The term p_{EC} becomes a factor of ε'_{PE} due to the fact that error correction occurs after parameter estimation. In addition, the factor before ε_{PE} is derived from the number of the different estimated channel parameters. In the homodyne and heterodyne protocols, these are the transmissivity and the excess noise. In CV-MDI, the transmissivities of both links, as well as the excess noise, are approximated.

5.8.1 Theoretical Composable Key Rate

The practical secret key rate in Eq. (4.34) can be compared with a corresponding rate, which is based on theoretical assumptions rather than observed outcomes of the parameters. This rate will henceforth be termed the theoretical rate. It is found by [Mountogiannakis et al. (2022a), Mountogiannakis et al. (2022b), Papanastasiou et al. (2023)]

$$R_{\text{theo}} = \tilde{R}_M^{\text{EC}} - \frac{\tilde{p}_{\text{EC}}\sqrt{n}}{N}\tilde{\Delta}_{\text{AEP}} + \frac{\tilde{p}_{\text{EC}}}{N}\tilde{\Theta} \tag{5.191}$$

where $\tilde{p}_{\text{EC}}$ is guessed, with $\tilde{\Delta}_{\text{AEP}}$ and $\tilde{\Theta}$ being computed on that guess. The theoretical finite-size key rate is determined by the formula

$$\tilde{R}_M^{\text{EC}} = \begin{cases} \frac{n\tilde{p}_{\text{EC}}}{N}\left(\tilde{\beta}I(x:y)|_{T,\Xi} - \chi(E:y)|_{T_M^*,\Xi_M^*}\right) & \text{Homodyne} \\ \frac{n\tilde{p}_{\text{EC}}}{N}\left(\tilde{\beta}I(\boldsymbol{x}:\boldsymbol{y})|_{T,\Xi} - \chi(E:\boldsymbol{y})|_{T_M^*,\Xi_M^*}\right) & \text{Heterodyne} \\ \frac{n\tilde{p}_{\text{EC}}}{N}\left(\tilde{\beta}I(\boldsymbol{x}:\boldsymbol{y})|_{T_A,T_B,\Xi} - \chi(E:\beta|\gamma)|_{T_{M_A}^*,T_{M_B}^*,\Xi_M^*}\right) & \text{CV-MDI} \end{cases} \tag{5.192}$$

where $\tilde{\beta}$ is also guessed. The estimators are approximated by their mean values, so that

$$\widehat{T} \to \mathbb{E}(\widehat{T}) \simeq T \tag{5.193}$$

$$\widehat{\Xi} \to \mathbb{E}(\widehat{\Xi}) \simeq \Xi \tag{5.194}$$

and the formulas for the worst-case scenario estimators become

$$T_M^* = T - W\sigma_T \tag{5.195}$$

$$\Xi_M^* = \Xi + W\sigma_\Xi \tag{5.196}$$

with W depending on ε_{PE}, as in Eq. (5.106). The standard deviations σ_T and σ_Ξ can be calculated by taking the square root of the variances found in Eq. (5.95) and Eq. (5.103) respectively. For CV-MDI, $T_{M_A}^*$ and $T_{M_B}^*$ can be calculated in similar fashion. The variance of the transmissivities can be obtained from Eq. (5.130) and Eq. (5.131), while the variance associated with the excess noise is shown in Eq. (5.133).

The theoretical rate R_{theo} is a valuable tool, when trying to immediately determine the security and performance of a protocol under certain parameters. The estimation of this rate is based on computationally trivial calculations, because the state generation and postprocessing steps are completely skipped. Running the entire protocol using the same parameters should yield similar results, with some level of deviation from the theoretical rate. This level may be determined by the number of generated samples used for the simulation. As more results are generated from simulations, their average value tends to converge towards the theoretical rate.

5.9 Privacy Amplification

In the final stage, the aim of Alice and Bob is to eliminate any trace of Eve's knowledge on all of the obtained binary strings $S_A \simeq S_B$ and form a final secret key Υ of length ℓ. For this purpose, they adopt the following block-by-block privacy amplification approach. First, they quantify the amount of compression to be applied through the composable rate. The secret key must have a bit length of

$$\ell = NR \tag{5.197}$$

while every $\tilde{n}$-bit sequence S_A and S_B is transformed into a shorter sequence of length

$$\ell' = \lceil \frac{\ell}{p_{\mathrm{EC}} n_{\mathrm{bks}}} \rceil \tag{5.198}$$

For each of their respective sequences S_A and S_B, Alice and Bob utilize an extractor function $h : \{0,1\}^{\tilde{n}} \to \{0,1\}^{\ell'}$, randomly chosen from a family $\mathcal{F}$ of two-universal hash functions. The most suitable function for this task is the application of the Toeplitz matrix $\mathbf{T}$. Applying the Toeplitz matrix to every S_A and S_B produces binary sequences

$$\Upsilon'_A = \mathbf{T}_{\ell',\tilde{n}} S_{\mathrm{A}} \simeq \Upsilon'_B = \mathbf{T}_{\ell',\tilde{n}} S_{\mathrm{B}} \tag{5.199}$$

The secret key Υ is then constructed by concatenating the results Υ' of all the blocks into a long binary string, whose length will be ℓ.

The time complexity of the dot product between a Toeplitz matrix $\mathbf{T}$ and a binary sequence is $O(\tilde{n}^2)$. When dealing with extremely long sequences, as in this case, such a complexity can become prohibitive. However, it is possible to reduce it to $O(\tilde{n} \ln \tilde{n})$ by utilizing a class of matrices, called circulant matrices, in conjunction with the Fast Fourier Transform (FFT). A circulant matrix $\mathbf{D}$ is a special case of the Toeplitz matrix, where every row of the matrix is a right cyclic shift of the row above it [Gray (2006)]. The circulant matrix is always square and can be completely defined by its first row $\mathbf{D}_0$. The steps are the following [(Nie et al., 2015, Supplemental Material)]:

- The Toeplitz matrix is reformed into a circulant matrix by merging its first row and column together. Since the first row has dimensions $\tilde{n} \times \ell'$, where $\tilde{n}$ is the privacy amplification block length and ℓ' is the resulting length, the length of the first column becomes $\tilde{n} + \ell' - 1$.
- The long binary sequence S is extended, as $\ell' - 1$ zeros are padded to its end. The length of the new sequence S' is now equal to the length of $\mathbf{D}_0$.
- To efficiently calculate the key, an optimized multiplication is carried out as

$$\widetilde{\Upsilon}' = \mathscr{F}^{-1}[\mathscr{F}(S') * \mathscr{F}(\mathbf{D}_0)] \tag{5.200}$$

Here, $\mathscr{F}$ represents the FFT and $\mathscr{F}^{-1}$ stands for the inverse FFT. Because of the convolution theorem, the $*$ operator signifies the Hadamard product and therefore elementwise multiplication can be performed.

- As the format of the secret key is required to be binary, the result of the inverse FFT $\widetilde{\Upsilon}'$ is taken modulo 2.
- From the bit sequence $\widetilde{\Upsilon}'$ of length $\tilde{n}+\ell'-1$, the first ℓ' bits are kept to form Υ'.

This technique requires the generation of a random seed $s \in \{0,1\}^{\tilde{n}+\ell'}$, which implies that the size of family $\mathcal{F}$ of Toeplitz matrix hashing is

$$|\mathcal{F}_{\mathbf{T}}| = 2^{\tilde{n}+\ell'} \tag{5.201}$$

Later on, an improved strategy emerged, whose advantage is that it requires the length of the seed to be only $\tilde{n}$-bit long [Hayashi (2011)]. This method employs a modified Toeplitz matrix $\mathbf{U}$, which is formed by concatenating the identity matrix $\mathbf{I}$ with the original Toeplitz matrix $\mathbf{T}$. Then, the size of the family of hash functions under the modified Toeplitz matrix becomes

$$|\mathcal{F}_{\mathbf{U}}| = 2^{\tilde{n}} \tag{5.202}$$

The method is as follows [Tang et al. (2019)]:

- A random seed $s \in \{0,1\}^{\tilde{n}}$ is generated and split into two strings: a string with length $\tilde{n}-\ell'$ for the first row of the Toeplitz matrix $\mathbf{T}$ and a string of length ℓ' for its first column. The first element of the row and the column is the same.
- An identity matrix $\mathbf{I}$ of size $\ell' \times \ell'$ is concatenated with the Toeplitz matrix $\mathbf{T}$ of size $\ell' \times \tilde{n}-\ell'$, forming the modified Toeplitz matrix $\mathbf{U}(\mathbf{I}|\mathbf{T})$.
- From the given input sequence S, the first ℓ' elements will be multiplied by $\mathbf{I}$, while the remaining $\tilde{n}-\ell'$ bits will be multiplied by $\mathbf{T}$. The sequence Υ' will be formed by the following relation:

$$\Upsilon' = \mathbf{U}S = \mathbf{I}S^{\ell'} \oplus \mathbf{T}S^{\tilde{n}-\ell'} \tag{5.203}$$

- The dot product of $\mathbf{I}$ and of the first ℓ' bits of S is easily calculated. The outcome is a scalar of ℓ' bits.
- The product $\mathbf{T}S^{\tilde{n}-\ell'}$ can be efficiently calculated by precisely following the steps from the aforementioned original Toeplitz matrix strategy, starting from the optimized multiplication step and onward.
- Finally, the direct sum of the two resulting components, which is here equivalent to the XOR operation, is computed to return Υ'.

Chapter 6

Results

After articulating the entire course of action, the outcome of the data processing for every examined protocol will be demonstrated. First, a thorough description of the rationale, that was used to obtain the results, will be provided. Then, the results are documented in different sections, according to the corresponding protocol. Except for the plots, potential advantages, disadvantages and trade-offs of parameters are discussed.

6.1 Methodology

The objective is to detect ranges for a combination of parameters, where the composable key rate becomes positive and, thus, communications are considered secure up to an error ε. The investigation revolves around short-range implementations of CV-QKD, over distances of around 5 km in standard optical fiber. The rest of the noise variables are generally adjusted, so that the SNR values spans from around 5 to 12. Identifying composably secure domains has proven tricky, even at this high asymptotic rate regime.

In all protocols, three factors have been deemed essential in achieving a positive rate R. The first is a sufficient combination of generated states $n_{\text{bks}}N$. Adopting a sufficiently large amount of total instances can provide both adequate sacrificed instances M and key generation instances n_{tot}. The former not only leads to more accurate channel estimators $\widehat{T}$ and $\widehat{\xi}$ by examining more statistical samples, but also minimizes the penalty from the calculation of the variances, which are used in the worst-case scenario estimators T_M and ξ_M. The latter leads to improved reconciliation efficiency values. The connection between β and n_{tot} is provided by the presence of the entropy penalty term δ_{ent} in Eq. (5.171), which becomes smaller, as the number of key extraction states increases. However, there is another penalty that has to be addressed, namely the finite-size penalty of the Δ_{AEP} term in the composable key rate formula of Eq. (4.34). Regardless of the number of blocks, a block size N of the order of at least 10^5 is an absolutely necessary requirement for the composable rate to be positive.

Last, but not least, comes the value of the reconciliation efficiency. In the given setting, β is given as an input to the algorithm. In order to achieve $R > 0$, values for β must generally be over 85%. In most instances, the parameters were adjusted to maintain a good balance between a high reconciliation efficiency and a good error-correcting performance p_{EC}. Note that the reconciliation efficiency is partially determined by the code rate, as shown by Eq. (5.171), and the code rate slightly varies from one simulation to another, depending on the generated data and estimated parameters. However, the regular LDPC matrices are designed under a fixed code rate. To the best of efforts, the protocol variables are always adjusted to almost match the LDPC code rate. Nonetheless, it is impossible to be extremely accurate in this regard. In order to be exact, a proposed solution is to give an estimate for the reconciliation efficiency $\widehat{\beta}$, which is then rescaled, so that the adjusted rate from the data perfectly matches the LDPC matrix R_{code}. In such a scenario, a different $\widehat{\beta}$ must be reported at the end of every simulation. The approach followed to derive the results involves providing an average value for β, gathered over a large sample of different generated data. Therefore, there is a trivial error between the reported β and the actual one, which should be below the order of 10^{-4}. This method was preferred over others for the reason that it is easier for the reader to comprehend the results by having a single point of reference for a variable. In most of the plots, β occupies the top axis, offering insightful information.

The results were obtained by executing simulations using a Python library, especially developed for this purpose. The library is open-source and accessible via the URLs:

- Homodyne Protocol: https://github.com/softquanta/homCVQKD
- Heterodyne Protocol: https://github.com/softquanta/hetCVQKD
- CV-MDI Protocol: https://github.com/softquanta/CVMDIQKD

A high-level overview of the modus operandi of the simulations is found in Appendix G. Particularly, Alg. 2 describes the homodyne protocol, Alg. 3 outlines the heterodyne protocol and, finally, Alg. 4 reports the CV-MDI procedure. The input parameters received by the simulations are listed in Table 6.1. These are almost the same between the protocols. A discrepancy between the GMCS protocols and the CV-MDI protocol is that in the former, the transmissivity T is expressed in terms of the channel length and attenuation, while in the latter, the two link transmissivities T_A and T_B are directly given as an input. Similarly, the excess noise ξ_A and ξ_B of both links has to be provided as an input in CV-MDI. The column weight of the non-binary LDPC matrices has been chosen as $w_{\text{c}} = 2$. Such ultra-sparse matrices have the potential to exhibit enhanced iterative decoding performance [Venkiah et al. (2008), Steiner et al. (2017)]. Concerning the desired level of security, the ε-parameters are initialized throughout all simulations with $\varepsilon_{\text{s}} = \varepsilon_{\text{h}} = \varepsilon_{\text{cor}} = \varepsilon_{\text{PE}} = \varepsilon_{\text{ent}} = 2^{-32} \simeq 2.3 \times 10^{-10}$, so that $\varepsilon \lesssim 4 \times 10^{-9}$ for any p_{EC}. The most important output variables of the simulations are catalogued in Table 6.2.

The amount of the most important bits remains constant and equal to $q = 4$ throughout all simulations, as this value allows for a combination of a reasonable key rate and error-correction speed. The precomputed matrices for the instance of $\mathcal{GF}(2^4)$ can be found in Appendix B.2. Under the current version of the sum-product algorithm and given the large block sizes plus the fact, that the simulations were executed using a CPU, it is computationally infeasible to achieve decoding with higher values for q in a reasonable time frame. Doing so would require decoding algorithms with an emphasis on decreasing the computational complexity or the implementation of the decoder in another processing unit, such as a GPU or an FPGA. Details on the complexity of the sum-product algorithm are provided in Appendix H.

Parameter	Description
L	Channel length (km)
ϑ	Attenuation rate (dB/km)
ξ	Excess noise
η	Detector/Setup efficiency
υ_{el}	Electronic noise
n_{bks}	Number of blocks
N	Block size
M	Number of PE runs
p	Discretization bits
q	Most significant (top) bits
α	Phase-space cut-off
$\text{iter}_{\max}$	Max number of EC iterations
$\varepsilon_{\text{PE, s, h, corr, ent}}$	Epsilon parameters
μ	Total signal variance
β	Reconciliation efficiency

Table 6.1: The main input parameters of the simulations.

Parameter	Description
μ^{opt}	Optimal signal variance
R_{asy}	Asymptotic key rate
$\widehat{T}$, $\widehat{\Xi}$, T_M, Ξ_M	Channel estimators
$\widehat{\text{SNR}}$	Estimated SNR
$\widehat{\rho}$	Estimated correlation
$\widehat{H}(K)$	Key entropy estimator
R_{code}	Code rate
p_{EC}	EC success probability
fnd_{rnd}	EC syndrome matching round
ℓ	Final key length
ε	ε-security
R	Composable key rate
Υ	Final key

Table 6.2: The main output parameters from the simulations.

6.2 Homodyne Protocol Simulations

The parameters chosen for the simulations of the homodyne protocol are displayed in Table 6.3. The first objective is to identify a sample block size, where the key rate becomes positive and which can be used to obtain useful results in the next simulations. Fig. 6.1 depicts the behavior of R, as the block size N increases. Recall that an increasing N is beneficial for reasons stated in the second paragraph of Sec. 6.1. Here, Alice's signal variance μ is adjusted for the setup to achieve a target high value of SNR $= 12$. It can be observed, that the key rate grows faster as the block size increases and the growth steadily slows down. Meanwhile, all of the simulations attained a very high error correction success rate. The numerical values of the rate can be considered to be high, since a key rate of 10^{-1} bits/use corresponds to 500 kbits/sec with a relatively slow clock of 5 MHz. Fig. 6.2 implies that equally high rates can be achieved even with fewer total states Nn_{bks}, when a large block size, e.g. $N = 250000$, is fixed and the number of blocks n_{bks} varies instead. Note that endpoint of both figures, which is determined by $N = 250000$ and $n_{\text{bks}} = 100$, represents the same simulations. As a result, having an adequately large block size is much more advantageous in obtaining a positive R than having more blocks of smaller sizes [Mountogiannakis et al. (2022a)].

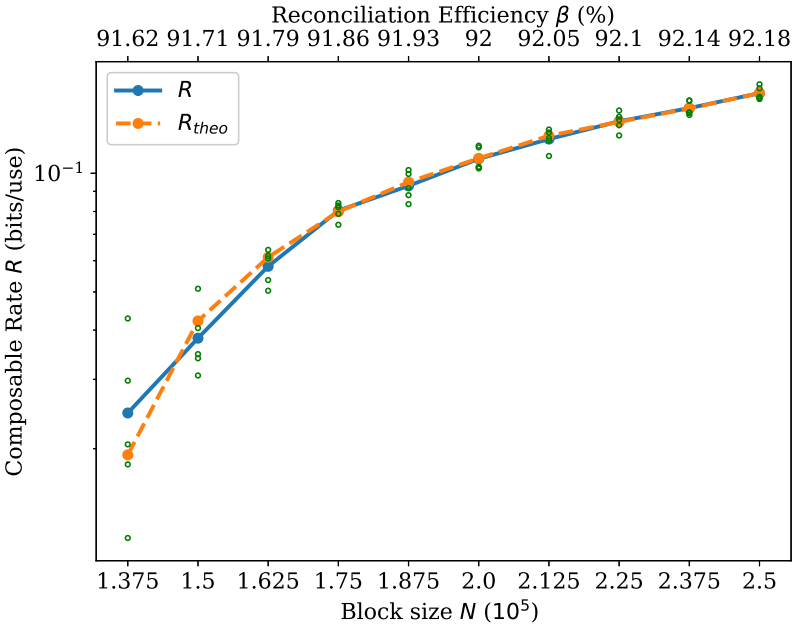

Figure 6.1: Composable secret key rate R (bits/use) versus the block size N for SNR $= 12$. The rate of Eq. (4.34) from five simulations (green points) and their average (blue line) is compared with the theoretical rate of Eq. (5.191) (orange line). The theoretical guesses for $\tilde{\beta}$ and $\tilde{p}_{\text{EC}}$ are chosen compatibly with the simulations. For every simulation, $\tilde{p}_{\text{EC}} = p_{\text{EC}}$ has been set. All simulations have achieved $p_{\text{EC}} \geq 0.95$. The step of N is 12500. The values of the reconciliation efficiency β are shown on the top axis and are chosen, so as to produce $R_{\text{code}} \approx 0.875$. See Table 6.3 for the list of input parameters used in the simulations.

Parameter	Value (Fig. 6.1)	Value (Fig. 6.2)	Value (Fig. 6.3)
L	5	5	variable
ϑ	0.2	0.2	0.2
ξ	0.01	0.01	0.01
η	0.8	0.8	0.8
υ_{el}	0.1	0.1	0.1
n_{bks}	100	variable	100
N	variable	2.5×10^5	2×10^5
M	$0.1 n_{\text{bks}} N$	$0.1 n_{\text{bks}} N$	$0.1 n_{\text{bks}} N$
p	7	7	7
q	4	4	4
α	7	7	7
$\text{iter}_{\max}$	100	100	150
ε-params	2^{-32}	2^{-32}	2^{-32}
μ	≈ 21.89	≈ 21.89	20
Parameter	**Value (Fig. 6.4)**	**Value (Fig. 6.5)**	**Value (Fig. 6.6 & Fig. 6.7)**
L	4	5	5
ϑ	0.2	0.2	0.2
ξ	variable	0.01	0.01
η	0.85	0.8	0.8
υ_{el}	0.05	0.1	0.1
n_{bks}	100	100	100
N	2.5×10^5	2×10^5	2.5×10^5
M	$0.1 n_{\text{bks}} N$	$0.1 n_{\text{bks}} N$	$0.1 n_{\text{bks}} N$
p	7	7	variable
q	4	4	4
α	7	7	7
$\text{iter}_{\max}$	200	150	150
$\varepsilon_{\text{-params}}$	2^{-32}	2^{-32}	2^{-32}
μ	25	variable	variable

Table 6.3: The input parameters for the homodyne protocol simulations.

In Fig. 6.3, the behavior of the composable secret key rate versus the distance L, expressed in km of standard optical fiber, is studied. Here, the blocks used are of size $N = 2 \times 10^5$, while the reconciliation efficiency β takes values from 90.25% to 92.17%. As seen in the plot, high rates of around 0.5 bits/use can be achieved at very short distances ($L = 1$ km), while a distance of $L = 7$ km can yield a rate of about 0.004 bits/use.

In Fig. 6.4, the robustness of the protocol, with respect to the amount of untrusted excess noise in the quantum communication channel, is analyzed. Note that this parameter may also include any other imperfection coming from the experimental setup. As portrayed, positive key rates are achievable for relatively high values of the excess noise ($\xi = 0.08$). The sharper decline of the key rate at the higher excess noise points ($\xi = 0.07$ and $\xi = 0.08$) is partially owed to the deterioration of the error correction success probability.

SNR	$\beta_{p=7}$	$\beta_{p=8}$	$\beta_{p=9}$	R_{code}	w_{r}
6	0.8588			0.75	8
7	0.8788	0.8775		0.777	9
8	0.8868	0.8865	0.8864	0.8	10
9_{a}	0.89	0.8897	0.8896	0.818	11
9_{b}	0.9265	0.9262	0.9261	0.833	12
10	0.9194	0.9190	0.9189	0.846	13
11_{a}	0.9116	0.9113	0.9113	0.857	14
11_{b}		0.9327	0.9326	0.866	15
12	0.9218	0.9215	0.9214	0.875	16

Table 6.4: The chosen reconciliation efficiency β for each SNR of Fig. 6.6 and Fig. 6.7, together with its respective code rate R_{code} and the row weight w_r of the LDPC code. The cases 'a' and 'b' refer respectively to the solid and dashed lines of Fig. 6.6 and Fig. 6.7. A missing value for the reconciliation efficiency implies that a simulation under the specified values will most likely return a negative composable key rate. The column weight w_{c} remains constant and equal to 2 for all simulations.

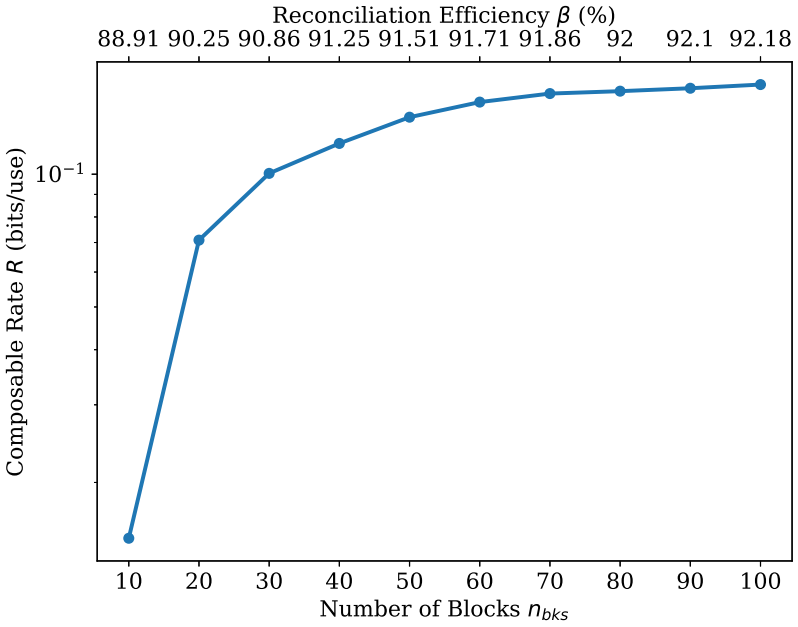

Figure 6.2: Composable secret key rate R (bits/use) versus the number of blocks n_{bks} for SNR = 12. The step of n_{bks} is 10. The individual block size is fixed and equal to $N = 2.5 \times 10^5$. Every point represents the average value of R, which is obtained after 5 simulations. All simulations have achieved $p_{\text{EC}} \geq 0.95$. The values of the reconciliation efficiency β are shown on the top axis and are chosen so as to produce $R_{\text{code}} \approx 0.875$. See Table 6.3 for the list of input parameters used in the simulations.

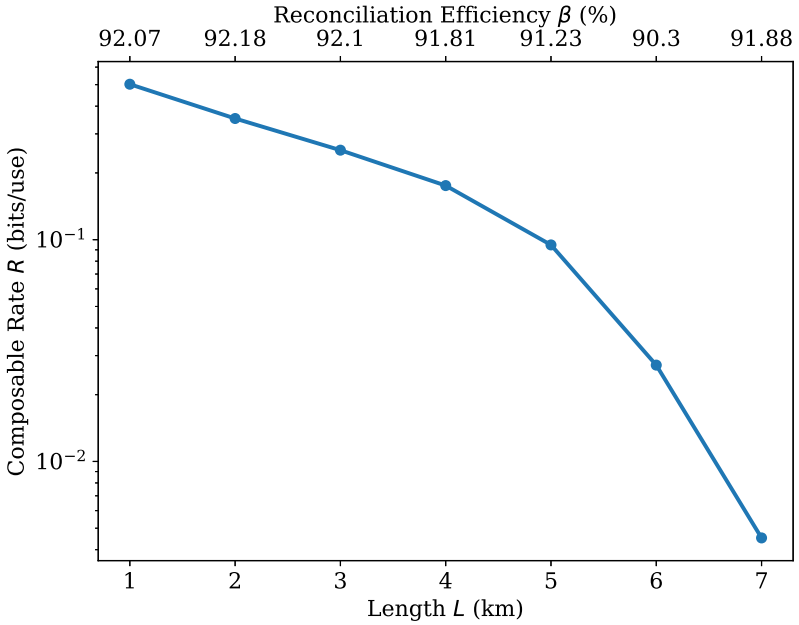

Figure 6.3: Composable secret key rate R (bits/use) versus the channel length L (km). Here, $N = 2 \times 10^5$ is used. Every point represents the average value of R, which is obtained after 5 simulations. All simulations have achieved $p_{\text{EC}} \geq 0.95$. The values of the reconciliation efficiency β are shown on the top axis. Other parameters are taken as in Table 6.3.

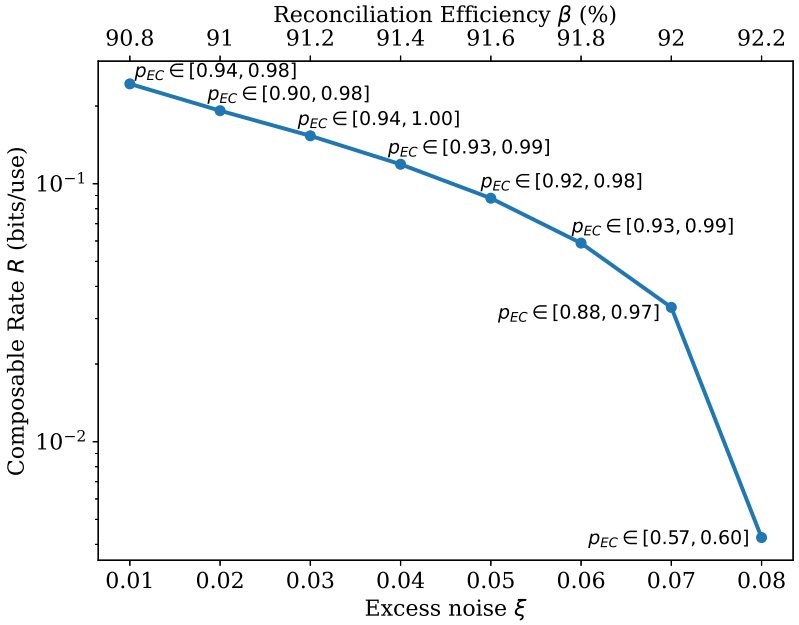

Figure 6.4: Composable secret key rate R (bits/use) versus the excess noise ξ. Every point represents the average value of R, which is obtained after 5 simulations. The interval displayed next to each point displays the minimum and maximum values achieved for p_{EC}. The values of the reconciliation efficiency β are shown on the top axis and are chosen so as to produce $R_{\text{code}} \approx 0.913$. Other parameters are taken as in Table 6.3.

Fig. 6.5, Fig. 6.6 and Fig. 6.7 explore different quantities of interest, such as the frame error rate FER, the rate and the EC rounds respectively. The quantities are measured as a function of the SNR and for various choices of the number p of discretization bits. The parameters used in the simulations are given in Table 6.3, where μ is variable and adapted to attain the desired SNR. In particular, in Fig 6.6 and Fig. 6.7, the reconciliation efficiency β, shown in Table 6.4, is chosen according to the following rationale: (i) because a regular LDPC code only achieves a specific value of R_{code}, β is chosen so that the R_{code} from Eq. (5.172) matches the R_{code} of a regular LDPC code with high numerical accuracy; (ii) β is high enough so that a positive key rate can be achieved for various values of p for the same SNR; and (iii) β is low enough, so that a limited number of EC rounds exceeds the iteration limit $\text{iter}_{\max}$. If β is too high, this limit is exceeded and FER increases or can even be equal to 1. In this case, none of the blocks are correctly decoded.

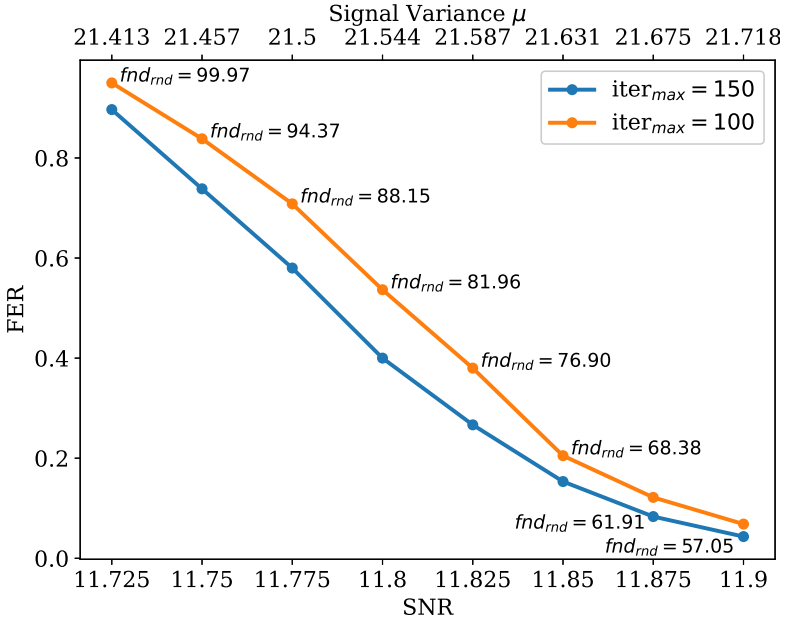

Figure 6.5: FER versus SNR for $p = 7$. The FER is compared for the same simulations, when the maximum number of EC iterations is $\text{iter}_{\max} = 150$ (blue line) and when $\text{iter}_{\max} = 100$ (orange line). Every point represents the average value of FER, which is obtained after 6 simulations. The step of the SNR is 0.025. It is observed, that a slight increase of μ causes the FER to decline rapidly. The values of the reconciliation efficiency β are chosen so as to produce $R_{\text{code}} \approx 0.875$. The signal variance μ that was used to achieve the respective SNR is displayed on the top axis with an accuracy of 3 decimal digits. The average number of iterations fnd_{rnd} needed to decode and verify a block is displayed for every point next to their respective points. The other parameters are constant and listed in Table 6.3.

Fig. 6.5 shows the FER for different values of the SNR. As seen, the FER is higher for lower SNRs and quickly declines, even with a small increase of the SNR. Note that every simulation, which was executed to produce the particular data, returned a positive

key rate (the highest FER attained was FER = 0.95 for SNR = 11.725). This result suggests that, when N is adequately large, a positive R can be achieved even with a minimal number of correctly decoded and verified blocks. The plot also shows the FER for the same simulations, if the maximum iteration limit had instead been $\text{iter}_{\max} = 100$. In the case of SNR = 11.725, if $\text{iter}_{\max} = 100$ had been set, a positive R would not have been realized for some simulations.

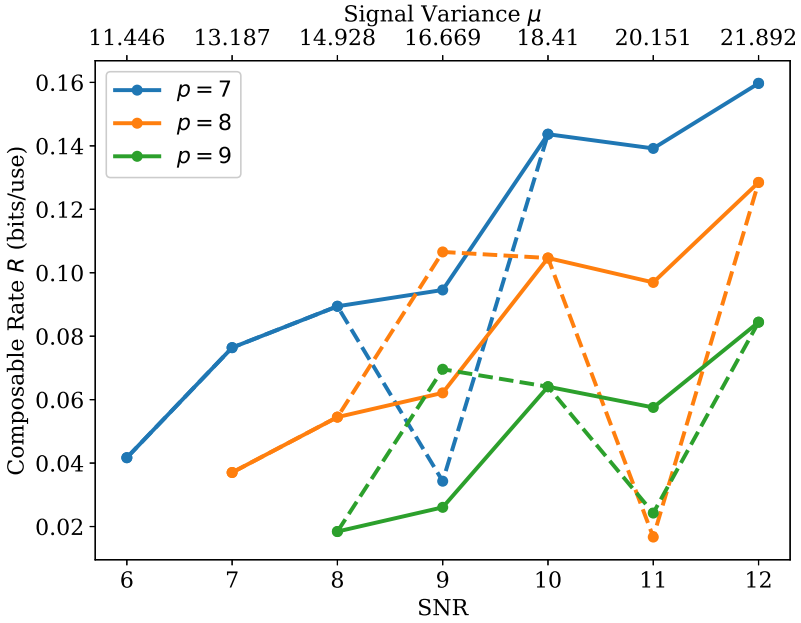

Figure 6.6: Composable secret key rate R versus SNR for discretization bits $p = 7$, $p = 8$ and $p = 9$. For each value of the SNR, the chosen reconciliation efficiency β is shown in Table 6.6. For SNR = 9 and SNR = 11, the solid lines follow the values of the entries 'a' of Table 6.6, while the dashed lines describe the 'b' cases. It is observed that, for lower values of p (at a fixed $q = 4$), higher rates for the corresponding SNR are obtained. The signal variance μ, that was used to achieve the respective SNR, is displayed on the top axis with an accuracy of 3 decimal digits. Other parameters are chosen as in Table 6.3.

Fig. 6.6 shows the composable key rate R versus the SNR for different discretization values p, while keeping the value of q constant and equal to 4. As observed, for fixed values of SNR and β, the lower the p is, the higher the rate R is. For every SNR and β, there is a maximum value for p able to achieve a positive R. For example, for SNR = 6 and $\beta \approx 0.8588$ ($R_{\text{code}} \approx 0.75$) a positive R is impossible to achieve with $p \geq 8$. For SNR = 7 and $\beta \approx 0.8775$ ($R_{\text{code}} \approx 0.777$), a positive R is infeasible with $p \geq 9$. The composable key rate improvement is owed to the fact that a smaller amount of bits d are declared publicly, when a smaller p is chosen. Meanwhile, the protocol maintains a good EC performance thanks to a sufficiently large number of EC iterations. On the other hand, by increasing p for a fixed q, the number of the public d-bits, which assist the LDPC decoding via the sum-product algorithm, is increased as well. This means that the EC step is successfully terminated in fewer rounds.

In Fig. 6.7, the average number of EC rounds fnd_{rnd} required to decode a block versus the SNR is plotted for different values of p. For a larger value of p, fewer decoding rounds are needed. This does not only make the decoding faster, but, depending on the specified $\text{iter}_{\max}$, it also gives the algorithm the ability to achieve a lower FER. Thus, a higher p can potentially achieve a better p_{EC}, while a smaller p may return a better R, assuming that $\text{iter}_{\max}$ is large enough. Therefore, at any fixed SNR and $\text{iter}_{\max}$, one could suitably optimize the protocol over the number of discretization bits p.

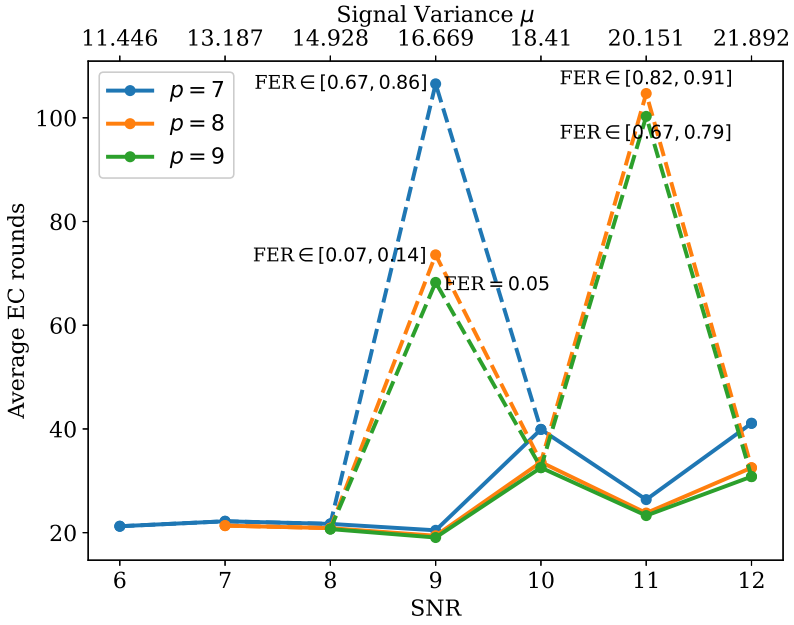

Figure 6.7: Average EC rounds fnd_{rnd} needed to decode a frame versus the SNR for discretization bits $p = 7$, $p = 8$ and $p = 9$. A round is registered only if the frame passes the verification step. The chosen reconciliation efficiency β for each value of the SNR is shown in Table 6.6. For SNR $= 9$ and SNR $= 11$ specifically, the solid lines respectively follow the values of the entry 9_{a} and 11_{a} of Table 6.6, while the dashed lines describe the 9_{b} and 11_{b} cases. For the 'b' cases, the FER is reported next to the respective values. The signal variance μ that was used to achieve the respective SNR is displayed on the top axis with an accuracy of 3 decimal digits. Other parameters are chosen as in Table 6.3.

6.3 Heterodyne Protocol Simulations

The next protocol under examination involves heterodyne measurements. Here, there is a key difference in the choice of input parameters. Since the Q and P quadratures are concatenated, the blocks are generally larger, compared to the homodyne ones. For this reason, the number of blocks has been cut in half in most simulations, i.e. $n_{\text{bks}} = 50$, so that the error correction is completed in a more timely fashion. Again, the SNR of interest is relatively high, taking values from almost 6 to 10. The variables used in the heterodyne simulations are listed in Table 6.5 [Mountogiannakis et al. (2022b)].

First, a demonstration of sample parameters, that achieve a positive rate R is required. The behavior of the rate, according to changes in the block size N and number of blocks n_{bks}, is shown in Fig. 6.8 and Fig. 6.9 respectively. Alice's signal variance μ is tuned, so as to produce a rather high signal-to-noise ratio of SNR $= 10$. It is observed in Fig. 6.8, that a block size of at least 2×10^5 is needed for $R > 0$. Additionally, Fig. 6.9 shows that it is generally possible to yield higher key rates with fewer total states, if an adequately large N is specified. The final point of both plots represents the same set of executed simulations. This set, using a block of $N = 3 \times 10^5$ states and $n_{\text{bks}} = 50$, attains on average a relatively high key rate $R \approx 0.24$.

Symbol	Value (Fig. 6.8)	Value (Fig. 6.9)	Value (Fig. 6.10)
L	3	3	variable
A	0.2	0.2	0.2
ξ	0.01	0.01	0.01
η	0.85	0.85	0.8
υ_{el}	0.1	0.1	0.1
n_{bks}	50	variable	50
N	variable	3×10^5	3.6×10^5
M	$0.1 n_{\text{bks}} N$	$0.1 n_{\text{bks}} N$	$0.1 n_{\text{bks}} N$
p	7	7	6
q	4	4	4
α	7	7	7
$\text{iter}_{\max}$	100	100	150
$\varepsilon_{\text{PE, s, h, corr}}$	2^{-32}	2^{-32}	2^{-32}
μ	≈ 29.46	≈ 29.46	20
Symbol	Value (Fig. 6.11)	Value (Fig. 6.12)	
L	4	5	
A	0.2	0.2	
ξ	variable	0.01	
η	0.85	0.85	
υ_{el}	0.05	0.1	
n_{bks}	50	50	
N	4.5×10^5	4×10^5	
M	$0.1 n_{\text{bks}} N$	$0.1 n_{\text{bks}} N$	
p	6	variable	
q	4	4	
α	7	7	
$\text{iter}_{\max}$	100	150	
$\varepsilon_{\text{PE, s, h, corr}}$	2^{-32}	2^{-32}	
μ	25	variable	

Table 6.5: The input parameters for the heterodyne protocol simulations.

Fig. 6.10 portrays the composable rate R versus distance L, expressed in km of standard optical fiber. Here, the SNR varies from 5.732 to 6.887. For this simulation, the discretization bits value was set to $p = 6$, in order to reach farther distances. A higher value for p would severely limit the protocol's ability to achieve a positive R at distances larger than 3 km.

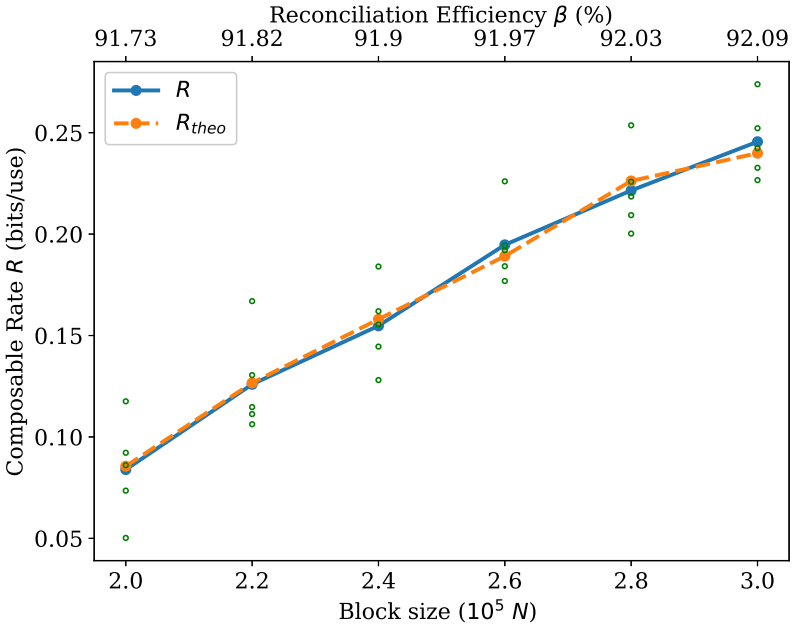

Figure 6.8: Composable secret key rate R (bits/use) versus the block size N for SNR $= 10$. The rate of Eq. (4.34) from five simulations (green points) and their average (blue solid line) is compared with the theoretical rate R_{theo} from Eq. (5.191) (orange dashed line). The theoretical guesses for $\tilde{\beta}$ and $\tilde{p}_{\text{EC}}$ are chosen compatibly with the simulations. For every simulation, $\tilde{p}_{\text{EC}} = p_{\text{EC}}$ has been set. All simulations have achieved $p_{\text{EC}} \geq 0.9$. The step of N is 20000. The values of the reconciliation efficiency β are shown on the top axis and are chosen so as to produce $R_{\text{code}} \approx 0.846$. See Table 6.5 for the list of input parameters used in the simulations.

Fig. 6.11 presents an estimate of the maximum tolerable excess noise ξ. The SNR of this setting is slightly above 8. While the decrease of the SNR is fairly small as the excess noise increases, the composable rate declines rapidly. In addition, the reconciliation efficiencies used here are in the range of 88.23% - 88.71%. Such values provide efficient error correction in terms of speed and performance, but are not ideal for attaining a positive rate. Larger values for the reconciliation efficiency would be detrimental to the efficiency of decoding. All in all, a larger block of size $N = 450000$ was utilized, in order to achieve a positive rate at $\xi = 0.05$, given the specified environment.

Fig. 6.12 describes the behavior of the key rate against different SNR values, when the noise terms are fixed and the modulation variance is variable. If the same code rate is used, lower values of p return higher rates for the corresponding SNR, considering a fixed $q = 4$. It is possible for a higher p value to yield a better composable rate than a smaller p, in case a larger code rate, and therefore a larger reconciliation efficiency, is employed. An example is given by cases 'a' and 'b' of SNR $= 9$, whose code rates and reconciliation efficiencies are shown in Table 6.6. A combination of $p = 8$ and $\beta = 0.9301$ beats the combination of $p = 7$ and $\beta = 0.894$ in terms of the composable rate by a fairly large margin.

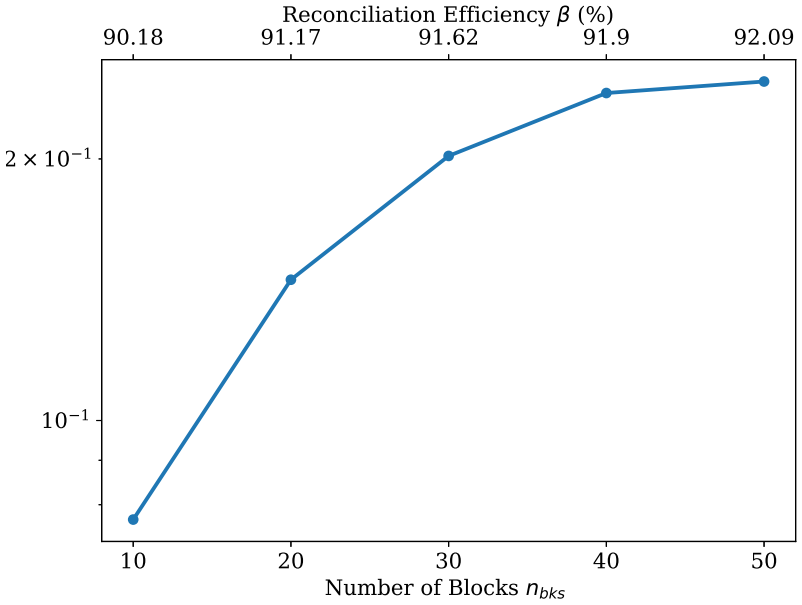

Figure 6.9: Composable secret key rate R (bits/use) versus the number of blocks n_{bks} for SNR $= 10$. The step of n_{bks} is 10. The individual block size is fixed and equal to $N = 3 \times 10^5$. Every point represents the average value of R, which is obtained after 5 simulations. All simulations have achieved $p_{\text{EC}} \geq 0.9$. The values of the reconciliation efficiency β are shown on the top axis and are chosen so as to produce $R_{\text{code}} \approx 0.846$. See Table 6.5 for the list of input parameters used in the simulations.

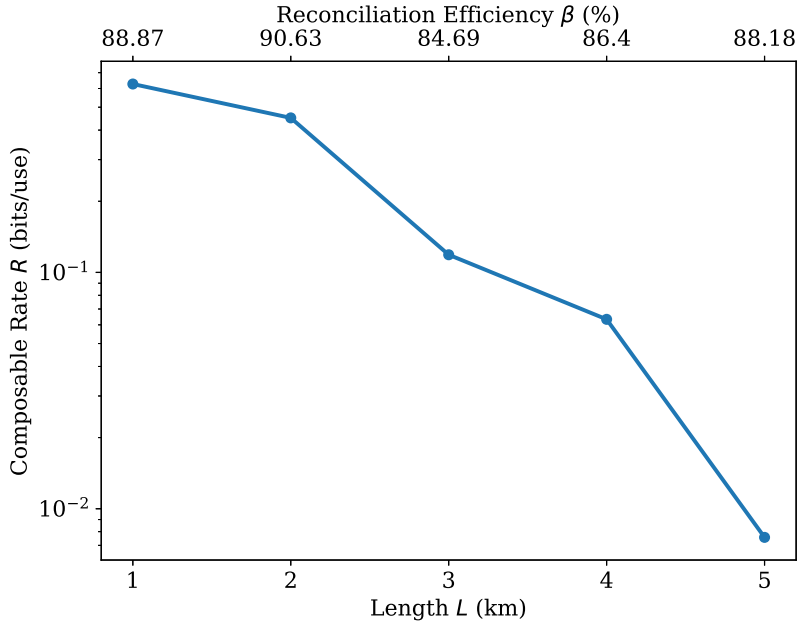

Figure 6.10: Composable secret key rate R (bits/use) versus the channel length L (km). Here, $N = 3.6 \times 10^5$ is used. Every point represents the average value of R, which is obtained after 5 simulations. All simulations have achieved $p_{\text{EC}} \geq 0.9$. The values of the reconciliation efficiency β are shown on the top axis. Other parameters are taken as in Table 6.5.

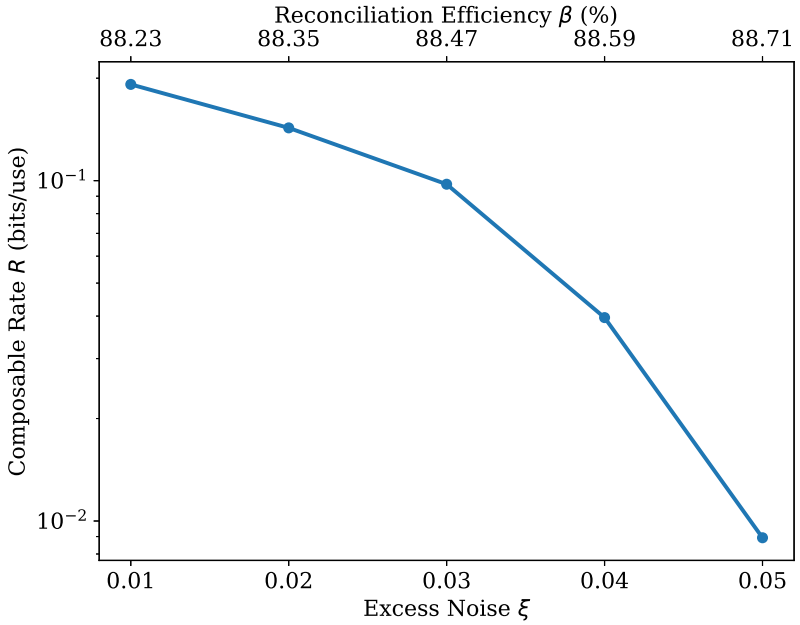

Figure 6.11: Composable secret key rate R (bits/use) versus the excess noise ξ. Every point represents the average value of R, which is obtained after 5 simulations. Here, $N = 4.5 \times 10^5$ and $n_{\text{bks}} = 50$ are used. The values of the reconciliation efficiency β for the heterodyne protocol simulations are chosen so as to produce $R_{\text{code}} \approx 0.8$. Other parameters are taken as in Table 6.5.

SNR	$\beta_{p=6}$	$\beta_{p=7}$	$\beta_{p=8}$	R_{code}	d_c
6	0.8651			0.75	8
7	0.8836			0.777	9
8	0.8924	0.8910		0.8	10
9_{a}	0.8953	0.8940		0.818	11
9_{b}			0.9301	0.833	12
10	0.9244	0.9231	0.9229	0.846	13

Table 6.6: The chosen reconciliation efficiency β for each SNR of Fig. 6.12, together with its respective code rate R_{code} and the row weight d_c of the LDPC code. A missing value for the reconciliation efficiency implies that the returned composable key rate will most likely be negative under the specified values. The column weight d_v remains constant and equal to 2 for all simulations.

However, there is a trade-off. While the rate produced by the former combination is higher, the error correction stage requires plenty more iteration rounds, making the procedure more computationally expensive. It must be noted that, for certain code rates, a minimum value for p is required. Such an occasion is the 'b' case of SNR = 9, where error correction can only be achieved for $p = 8$, given a constant q. Smaller values for p would not be able to achieve error correction and, consequently, a positive rate. This is owed to the fact, that the number of bottom bits d, which constitute the side information, is not sufficient.

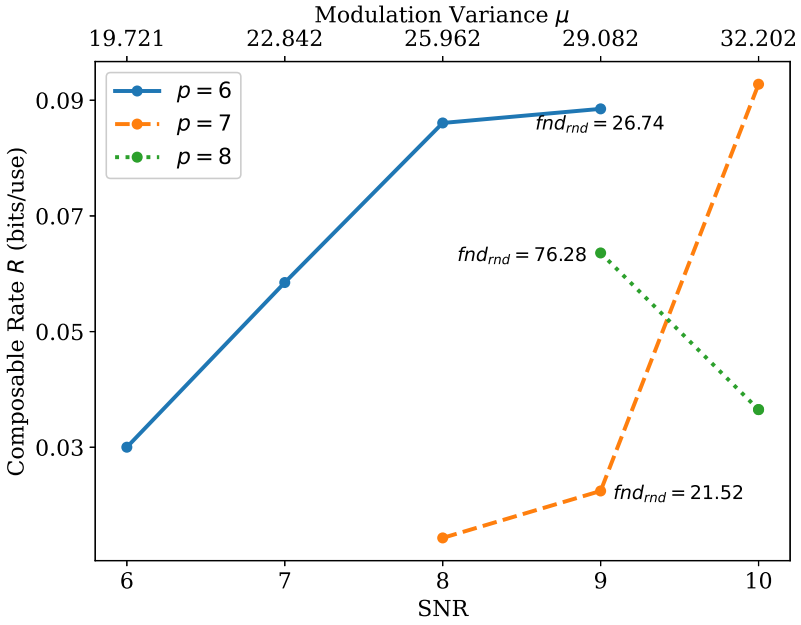

Figure 6.12: Composable secret key rate R versus SNR for discretization bits $p = 6$ (blue solid line), $p = 7$ (orange dashed line) and $p = 8$ (green dotted line). The chosen reconciliation efficiency β for each value of the SNR is shown in Table 6.6. Every point represents the average value of R, which is obtained after 5 simulations. For SNR $= 9$, the average number of iterations fnd_{rnd} needed to decode and verify a block is displayed for every point next to their respective points. The signal variance μ that was used to achieve the respective SNR is displayed on the top axis with an accuracy of 3 decimal digits. Other parameters are chosen as in Table 6.5.

6.4 CV-MDI Protocol Simulations

The parameters used to execute the simulations are listed in Table 6.7. CV-MDI is a situational protocol, whose performance has been shown to be inferior in comparison to the other two GMCS protocols. Therefore, it is tougher to find a signal variance range, for which the composable rate R becomes positive. To achieve this, the asymptotic rate R_{asy} was maximized using a modulation variance optimization function. The provided μ_A^{opt} and μ_B^{opt} enabled the identification of an interval for the variances, which achieves a positive R [Papanastasiou et al. (2023)]. To begin with, the symmetric version of the protocol is examined, which means that the signal variance and the channel parameters will be the same between Alice and Bob, i.e. $\mu_A = \mu_B$, $T_A = T_B$ and $\xi_A = \xi_B$. Table 6.8 shows that $R > 0$ can be achieved, when $45 \leq \mu_A, \mu_B \leq 50$. Under these conditions, the SNR spans from approximately 10 to 11.89. As presented in the table, the choice of the reconciliation efficiency is important, when trying to maximize the value of R. It is important to note that the neither the asymptotic nor the composable rate will further grow, as the signal variances increase. This means that, at some point, the rates saturate and eventually become negative again.

Parameter	Value (Fig. 6.13)	Value (Fig. 6.14)	Value (Fig. 6.15)	Value (Table 6.8)
T_A	0.98	0.98	variable	0.96
T_B	0.98	0.98	0.985	0.985
ξ_A	0.005	variable	0.006	variable
ξ_B	0.005	variable	0.004	0.004
η	0.98	0.98	0.98	0.98
v_{el}	0.01	0.01	0.01	0.01
n_{bks}	100	100	100	100
N	5×10^5	5×10^5	5.88×10^5	5.88×10^5
M	$0.1 n_{\text{bks}} N$	$0.1 n_{\text{bks}} N$	$0.15 n_{\text{bks}} N$	$0.15 n_{\text{bks}} N$
p	6	6	7	7
q	4	4	4	4
α	7	7	7	7
iter_{max}	200	200	100	100
ε-params	2^{-32}	2^{-32}	2^{-32}	2^{-32}
μ_A	variable	46	60	60
μ_B	variable	46	50	50

Table 6.7: The input parameters for the CV-MDI protocol simulations.

Knowing the variables, for which the composable rate becomes positive, the maximum tolerable excess noise in the system can now be identified. For this purpose, $\mu_A = \mu_B = 46$ is chosen, in order to produce a high rate, which tolerates more excess noise. Simultaneously the EC procedure will be faster, when compared to that of $\mu_A = \mu_B = 49$. Therefore, in Fig. 6.13, the symmetric case of the protocol is considered again, with $\mu_A = \mu_B = 46$ and with the excess noise being variable. As observed from the plot, ξ can take values up to 0.008, before the protocol is deemed unsafe for key extraction.

Next, the asymmetric version of the protocol is investigated. In this scenario, the channel parameters, as well as the signal variances, may be different between Alice and Bob. Here, two cases are examined: Fig. 6.14 shows the behavior of Alice's transmissivity against the composable key rate and Fig. 6.15 displays the maximum tolerable values for Alice's excess noise. Regarding the former case, it is possible for Alice's channel to reach transmissivity values of about $T_A = 0.94$, which translates to a fiber length of 1.34km. The latter case shows that it is feasible to achieve a positive R under relatively high values for the excess noise, which can be extended to $\xi_A = 0.01$. To ensure a positive composable rate under harsher noise settings, it is possible to employ a larger LDPC matrix with a block length very close to the order of 10^6 and $R_{\text{code}} = 0.875$ for the task. Because of the minimization of the entropy penalty, a larger LDPC block size leads to higher values for the reconciliation efficiency, when all other values remain the same.

μ_A, μ_B	β	R_{code}	SNR	R
45	90%	0.833	10.019	0.00452259
46	92.15%	0.846	10.252	0.06346475
47	91.35%	0.846	10.485	0.04397952
48	90.62%	0.846	10.718	0.01369927
49	92.35%	0.857	10.951	0.06547397
50	91.64%	0.857	11.189	0.04992091

Table 6.8: Composable secret key rate R (bits/use) versus Alice's and Bob's signal variances μ_A and μ_B. The rightmost column displays the average value for R, which is obtained after 5 simulations. Here, $N = 5 \times 10^5$ and $n_{\text{bks}} = 100$ are used. All simulations have achieved $p_{\text{EC}} \geq 0.95$. Parameters not listed here are taken as in Table 6.7.

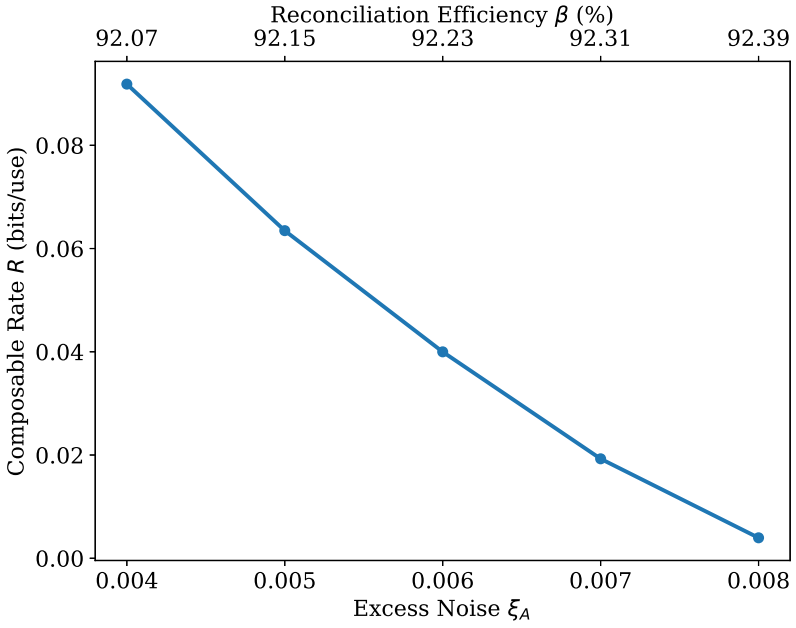

Figure 6.13: Composable secret key rate R (bits/use) versus Alice's and Bob's excess noise values $\xi = \xi_A = \xi_B$. Here, $N = 5 \times 10^5$ and $n_{\text{bks}} = 100$ are used. Every point represents the average value of R, which is obtained after 5 simulations. All simulations have achieved $p_{\text{EC}} \geq 0.95$. The signal variances used by Alice and Bob are constant and equal ($\mu_A = \mu_B = 46$). The values of the reconciliation efficiency β are shown on the top axis. Other parameters are taken as in Table 6.7.

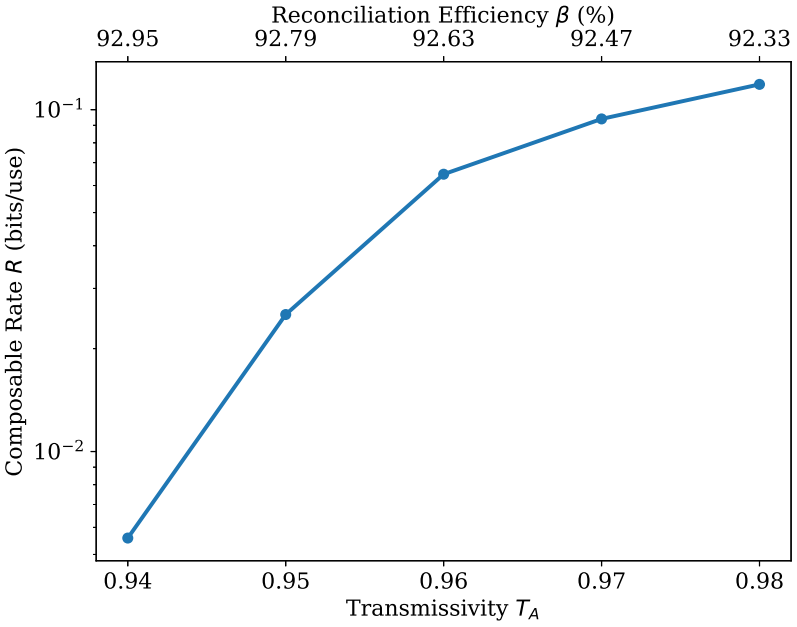

Figure 6.14: Composable secret key rate R (bits/use) versus Alice's transmissivity T_A. Here, $N = 5.88 \times 10^5$ and $n_{\text{bks}} = 100$ are used. Every point represents the average value of R, which is obtained after 5 simulations. All simulations have achieved $p_{\text{EC}} \geq 0.95$. The signal variances used by Alice and Bob are constant ($\mu_A = 60$, $\mu_B = 50$). The values of the reconciliation efficiency β are shown on the top axis. Other parameters are taken as in Table 6.7.

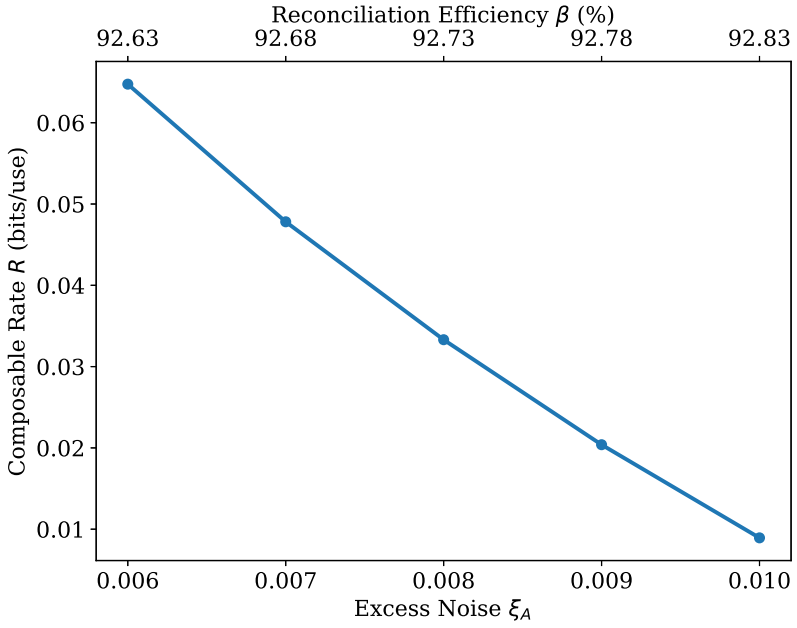

Figure 6.15: Composable secret key rate (bits/use) versus Alice's excess noise value ξ_A. Here, $N = 5.88 \times 10^5$ and $n_{\text{bks}} = 100$ are used. Every point represents the average value of R, which is obtained after 5 simulations. All simulations have achieved $p_{\text{EC}} \geq 0.95$. The signal variances used by Alice and Bob are constant ($\mu_A = 60$, $\mu_B = 50$). The values of the reconciliation efficiency β are shown on the top axis. Other parameters are taken as in Table 6.7.

Chapter 7

Conclusion

In this thesis, the exposition of three GMCS CV-QKD protocols, namely the homodyne, the heterodyne and the CV-MDI protocols, is achieved. This description is accompanied by a security analysis under the composable finite-size framework. The protocols have been designed to preferably operate in a high signal-to-noise ratio environment. As a result, they have been integrated with a suitable preprocessing scheme and non-binary sum-product decoding. The protocols were modelled using a Python-based library, which receives input parameters for a certain protocol, simulates the stages of quantum state preparation, transmission and measurement and performs every postprocessing step. Ultimately, it creates a shared secret key, assuming a positive composable key rate.

Numerical results were produced, which assessed the behavior and performance of the protocols against a variety of parameters. These parameters are related to noise measures, such as the channel length, excess noise and signal-to-noise ratio and finite-size effects, such as the block size, the number of blocks or the maximum number of error-correcting iterations. The results enabled the identification of secure domains and maximum tolerable noise conditions. Moreover, a variety of useful outcomes was extracted, which relates to the advantages of preferring some variables over others, as well as the compromises, which have to be made, when adjusting inherently connected parameters.

7.1 Importance of Research

CV-QKD protocols have been relatively slower in achieving comparable levels of security to their DV-QKD counterparts, especially in terms of demonstrating composability and robustness against finite-size effects. The work presented in this thesis attempts to bridge this gap between CV-QKD and DV-QKD by presenting a complete solution. It provides an invaluable contribution to existing literature by proving the security of a practical implementation, up to a small error.

What is more, the striking majority of CV-QKD research naturally revolves around extending the maximum transmission length and improving long-range implementations, meaning there is a shortage of quality results for short-range communications. Especially when considering the composable framework in an analysis, the collective contribution of the ε-parameters can have a detrimental effect on the practical rate of a protocol, even in the high signal-to-noise ratio regime. The results of this work, which were obtained following a lucid methodology, are the outcome of a multitude of parameters. These have received realistic values, which would govern a practical CV-QKD implementation. Authors can directly adopt them in their research or use them to test an experimental application, knowing that they represent a secure communications domain, even in an optimal attack scenario.

Last, but not least, the source code of the protocols is openly available. The software can be readily exploited by any parties, who are interested in the expansion of the protocols, the generation of correlated sequences or the production of numerical results.

7.2 Outlook

There is a lot of potential in the field of CV-QKD and, by extension, in this specific project. The work presented in this thesis is inaugural, in terms of a full description of a protocol, based on the composable finite-size framework and accompanied by a proposed data-processing strategy and a variety of numerical results.

From a more generic perspective, there are numerous features, that future studies can incorporate. To begin with, more CV-QKD protocols can be integrated by following the course of action of this dissertation. Potential ideas include the postselection protocol [Silberhorn et al. (2002)], the CV-MDI protocol with postselection [Wilkinson et al. (2020)] or any adaptation from the family of discrete-modulated CV-QKD protocols [Leverrier and Grangier (2009), Papanastasiou and Pirandola (2021)]. Furthermore, numerical results for the low signal-to-noise ratio regime can be explored, encompassed by the composable framework under finite-size effects. Finally, a step in a different direction would be to include two-way protocols [Pirandola et al. (2008a)] and even multi-party QKD protocols [Fletcher and Pirandola (2022)].

With respect to the current work, an interesting idea would be to adopt a modern version of the slice reconciliation technique [Ai and Malaney (2022)]. The data processing and, if needed, the security proof should be adapted to this scheme and a direct comparison between the two works can be performed by the means of numerical results. Additionally, especially when considering experimental implementations, more imperfections from the various procedures may be identified, leading to the inclusion of more composable terms [Jain et al. (2022)]. Finally, one may wonder why the construction of the LDPC matrix in this work is a regular one, when in existing literature other types of optimized irregular

codes [Xu et al. (2022)] have been shown to achieve better error-correcting performance. The reason for this is versatility; it is essential for the requirements of this work that there is a fast, on-demand production of LDPC codes, which vary greatly in block lengths and code rates. As a result, another suggestion would be to employ LDPC codes, which have been shown to exhibit superior performance, when compared to random regular constructions. Potential benefits of this would be yielding better error-correction success rates and faster convergence to a correct decoding guess, which, in turn, may improve the values of the reconciliation efficiency. Under both benefits, the key rate increases, strengthening the performance of the protocol.

As far as the software is concerned, the biggest challenge would be to increase the speed of error correction. An initial step would be to reduce the complexity by employing the FFT-based non-binary sum product algorithm [Barnault and Declercq (2003)]. In case the speed would still not be satisfactory, the project could be upgraded to include decoding on FPGA-based [Spagnol et al. (2007)] or GPU-based [Andrade et al. (2013)] systems. The improvement of the error correction process would allow for the use of larger block sizes, increasing the key rates and the tolerance to noise. In addition, it would pave the way for the complete optimization of the protocol parameters. The current implementation accounts for optimization either empirically, e.g. identification of the optimal p for a certain set of variables from the results, or algorithmically, e.g. the optimal modulation variance μ^{opt}. However, limitations have been imposed on other parameters, such as the number of the most important bits q. Higher values for q would signficantly expand the capability of the software to produce better results.

Appendix A

The Non-Binary Sum-Product Algorithm

A.1 Likelihood Function Updating

Assume a device, whose output is described by the variable X, which is parametrized by ϑ. The random variable X takes values x according to a family $\mathcal{X}$ of probability distributions. Given the sampled data string X_i, for $i = 1, \ldots, n$ from this distribution, one can build a string of data X^n and define the likelihood $\mathbb{L}$ of the parameter ϑ, describing the associated probability distribution as

$$\mathbb{L}(\vartheta|X^n) = p(X^n|\vartheta) = \prod_{i=1}^{n} p(X_i|\vartheta) \tag{A.1}$$

where $p(X^n|\vartheta)$ is the conditional probability for a specific X^n to be the result of the device, given that its distribution $\mathbb{P}(X;\vartheta)$ is described by ϑ and the outcome of the device is i.i.d. Intuitively, a good guess $\widehat{\vartheta}$ of the parameter ϑ would be the argument ϑ^* of the maximization of the likelihood function over ϑ. Using Bayes' rule, the conditional probability $p(X^n|\vartheta)$ can be written as

$$p(X^n|\vartheta) = \frac{p(X^n)}{p(\vartheta)} p(\vartheta|X^n) \tag{A.2}$$

It can be observed, that $p(X^n)$ is not dependent on ϑ and $p(\vartheta)$ is considered uniform and, thus, independent of ϑ. Therefore, $p(\vartheta|X^n)$ can be maximized instead. For simplification purposes, the previous probability will be expressed as a function, which is dependent only on the parameter ϑ, as

$$f(\vartheta) = p(\vartheta|X^n) \tag{A.3}$$

Consider the case, where the distribution $p_{\mathcal{X}}(X|\vec{\vartheta})$ is described by a vector of parameters $\vec{\vartheta} = (\vartheta_1, \ldots, \vartheta_n)$. Respectively, the probability

$$f(\vec{\vartheta}) = f(\vartheta_1, \ldots, \vartheta_n) \tag{A.4}$$

can be defined, along with its marginals

$$f(\vartheta_i) = \sum_{k \neq i} f(\vartheta_1, \ldots, \vartheta_k, \ldots, \vartheta_n) \tag{A.5}$$

Suppose that there exist certain constraints, that $\vec{\vartheta}$ should satisfy. These are summarized by a system of l linear equations as

$$\mathbf{H}\vec{\vartheta} = \vec{\epsilon} \tag{A.6}$$

where $\mathbf{H}$ is an $l \times n$ LDPC matrix. In particular, there are l equations that the ϑ_i should satisfy in the form of

$$\sum_i \mathbf{H}_{ji}\vartheta_i = \epsilon_j, \quad j = 1, \ldots, l \tag{A.7}$$

For instance, when $\vec{\epsilon} = (3, 1, 2)$, the matrix in Table A.1 gives the following three equations, which are only valid in $\mathcal{GF}(4)$:

$$3\vartheta_3 + \vartheta_5 = 3 \tag{A.8}$$

$$2\vartheta_1 + \vartheta_4 = 1 \tag{A.9}$$

$$\vartheta_2 + 2\vartheta_4 + 3\vartheta_5 = 2 \tag{A.10}$$

Then, one needs to pass from the probability distribution of Eq. (A.4) to $\widetilde{f}(\vec{\vartheta})$, in order to calculate its marginals

$$\widetilde{f}(\vartheta_i) = f(\vartheta_i|\mathbf{H}\vec{\vartheta} = \vec{\epsilon}) \tag{A.11}$$

A.2 Sum-Product Algorithm

The sum-product algorithm follows the same path as the analysis of the previous section, in order to efficiently calculate the marginals of Eq. (A.11) as

$$\widetilde{f}(\overline{K}_i) = f(\overline{K}_i|\mathbf{H}\overline{K}^n = K_{\text{syn}}^l) \tag{A.12}$$

for $\vartheta_i = \overline{K}_i$, $\vec{\vartheta} = \overline{K}^n$, $\vec{\epsilon} = K_{\text{syn}}^l$, and the a priori marginal probabilities of Eq. (5.175) as

$$f(\overline{K}_i = \overline{k}) = P(\overline{k}|X_i\underline{K}_i) \tag{A.13}$$

To do so, it associates a Tanner graph to the matrix $\mathbf{H}$ and assumes a signal exchange between its nodes. More specifically, the graph consists of two kinds of nodes: n variable nodes, symbolizing the parameters $\overline{K}_i$, and l check nodes, corresponding to the linear equations described by Eq. (5.174). Then, for each variable i participating in the jth equation, there is an edge connecting the relevant nodes. An example of such a Tanner graph is presented in Fig. A.1(a). The graph is based on the matrix $\mathbf{H}$ of Table A.1. The signal sent from the variable node i to a factor node j is denoted as $\mathsf{q}_{ji\overline{k}}$ and it stands for the probability, that the variable $\overline{K}_i = \overline{k}$ and all the linear equations are true, apart from equation j. The signal sent from the check node j to the variable node i is labelled as $\mathsf{r}_{ji\overline{k}}$ and represents the probability that equation j will be satisfied, given that $\overline{K}_i = \overline{k}$. Based on these definitions, the marginals of Eq. (A.12) are determined by

$$\widetilde{f}(\overline{K}_i = \overline{k}) = \mathsf{q}_{ji\overline{k}}\mathsf{r}_{ji\overline{k}} \tag{A.14}$$

for any equation j, where the variable i partakes.

In particular, in every iteration, the algorithm updates $\mathsf{r}_{ji\overline{k}}$ through the signals of the neighbor variable nodes, apart from the signal from node i. This is called the horizontal step of the algorithm. The updating follows a certain rule: given a vector $\overline{K}^n$, whose ith element is equal to $\overline{K}_i = \overline{k}$, the result is

$$\mathsf{r}_{ji\overline{k}} = \sum_{\{i\}} p[K_{\mathrm{syn}_j}|\overline{K}^n] \prod_{k\in\mathcal{M}(j)\setminus i} \mathsf{q}_{jk\overline{K}_k} \tag{A.15}$$

where $p[K_{\mathrm{syn}_j}|\overline{K}^n]$ takes the value 1, if the check j is satisfied from $\overline{K}^n$, or 0 if it is not. Note that the values of $\mathsf{q}_{jk\overline{K}_k}$ are initially updated with the a priori probabilities during the initialization step, as in line 5 of Algorithm 1, and that $\mathcal{M}(j)$ is the set of neighbors of the jth check node. An example of such an update is depicted in Fig. A.1(b).

The algorithm takes advantage of the fact that

$$\mathsf{r}_{ji\overline{k}} = p\left[\mu_{j(i-1)} + \nu_{j(i+1)} = K_{\mathrm{syn}_j} - \mathbf{H}_{ji}\overline{K}_i\right] \tag{A.16}$$

where

$$\mu_{jk} = \sum_{i:i\leq k} \mathbf{H}_{ji}\overline{K}_i \tag{A.17}$$

$$\nu_{jk} = \sum_{i:i\geq k} \mathbf{H}_{ji}\overline{K}_i \tag{A.18}$$

are partial sums with different direction, running over the jth check. Specifically, Eq. (A.16) can be further simplified into a sum of a product of probabilities from the previous partial sums, taking specific values by satisfying the jth check, as stated in line 10 of Algorithm 1. Afterwards, the algorithm updates $\mathsf{q}_{ji\overline{k}}$ through the signals coming from the neighbor check nodes, excluding node j, as illustrated in the example of Fig. A.1(c).

The rule to do so is given in line 12 of the pseudocode (vertical step). Finally, in the tentative decoding step, the algorithm takes the product of $\mathsf{q}_{ji\overline{k}}$ and $\mathsf{r}_{ji\overline{k}}$ and then calculates and maximizes the marginal of Eq. (A.14) over $\overline{k}$. The arguments $\widehat{K}_i$ of this maximization of every marginal create a good guess $\widehat{K}^n$ for $\overline{K}^n$. In the next iteration, the algorithm follows the same steps, using the preceding $\mathsf{q}_{ij\overline{k}}$ to make all the updates.

A.3 Non-Binary Sum-Product Algorithm Pseudocode

Algorithm 1 Non-Binary Sum-Product Algorithm

Input: $p(\overline{K}_i|X_i\underline{K}_i), K^l_{\text{syn}}$, **Output:** $\widehat{K}^n, \text{fnd}, \text{fnd}_{\text{rnd}}$

1: **Step 1:** Initialization
2: $\vec{\epsilon} \leftarrow K^l_{\text{syn}}$
3: $j, i \leftarrow j, i : \mathbf{H}_{ji} \neq 0$ (Tanner graph creation)
4: $f_i^{\overline{k}} \leftarrow p(\overline{K}_i = \overline{k}|X_i, \underline{K}_i)$
5: $\mathsf{q}_{ji\overline{k}} \leftarrow f_i^{\overline{k}}$
6: **for** iter $= 1, 2, \ldots \text{iter}_{\max}$ **do**
7: **Step 2:** Horizontal Step
8: $\mu_{ji} \leftarrow \sum_{l \leq i} \mathbf{H}_{jm}\widehat{K}_l$
9: $\nu_{ji} \leftarrow \sum_{l \geq i} \mathbf{H}_{jm}\widehat{K}_l$
10: $\mathsf{r}_{ji\overline{k}} \leftarrow \sum_{s,t:s+t=\epsilon_j-\mathbf{H}_{ji}\overline{k}} p\left[\mu_{j(i-1)} = s\right] p\left[\nu_{j(i+1)} = t\right]$
11: **Step 3:** Vertical Step
12: $\mathsf{q}_{ji}^{\overline{k}} \leftarrow \varphi_{ji} f_i^{\overline{k}} \prod_{l \setminus j} \mathsf{r}_{mi\overline{k}}$, $\varphi_{ji} : \sum_{\overline{k}=0}^{2^{\mathsf{q}}-1} \mathsf{q}_{ji\overline{k}} = 1$
13: **Step 4:** Tentative Decoding
14: $\widehat{K}_i \leftarrow \arg\max_{\overline{k}} f_{i\overline{k}} \prod_j \mathsf{r}_{ji\overline{k}}$
15: **if** $\mathbf{H}\widehat{K}^n = \vec{\epsilon}$ **then**
16: **return** $\widehat{K}^n, \text{fnd}_{\text{rnd}}, \text{fnd} \leftarrow$ True
17: **end if**
18: **if** iter $= \text{iter}_{\max}$ **then**
19: **return** fnd $\leftarrow$ False
20: **end if**
21: **end for**

$$\mathbf{H} = \begin{bmatrix} 0 & 0 & 3 & 0 & 1 \\ 2 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 2 & 3 \end{bmatrix}$$

Table A.1: An example for a $l \times n$ parity check matrix with values in $\mathcal{GF}(2^2)$ for $l = 3$ checks (check nodes) and $n = 5$ transmitted signals (variable nodes). For this matrix, the assumptions of a regular code explained in Sec. 5.5 are not valid and it is used only as a toy model for the convenience of the description for the sum-product algorithm.

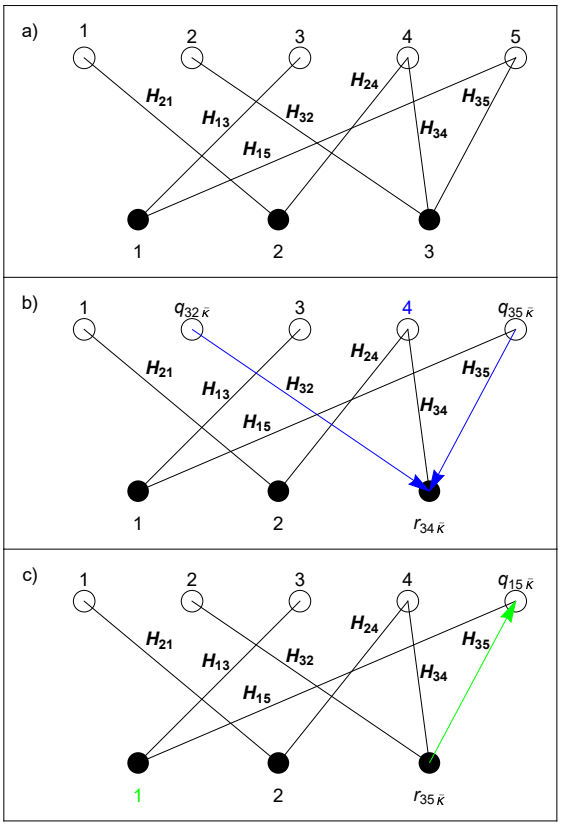

Figure A.1: a) Tanner graph of the parity-check matrix of Table A.1. The variable nodes (white disks) are connected with the check nodes (black disks), when $\mathbf{H}_{ji} \neq 0$.
b) One instance of the horizontal step (Step 2) of Algorithm 1. Here, the signal probability $\mathsf{r}_{34\overline{k}}$ is updated for all the $\overline{k} \in \mathcal{GF}(2^2)$ from the contribution (blue arrows) of the rest of the neighbour variable nodes of check node 3, excluding the variable node 4 (node in blue). This update will be repeated in the same step for all the variable nodes, i.e., $\mathsf{r}_{32\overline{k}}$ and $\mathsf{r}_{35\overline{k}}$ will be calculated as well. The same procedure will be followed for syndrome nodes 1 and 2, before the algorithm passes to the horizontal step. This description provides the conceptual steps to derive the desirable result. Practically, the algorithm follows a more complex path, as, for example, it calculates probabilities of partial sums.
c) An instance of the horizontal step (Step 3) of Algorithm 1. Here, $\mathsf{q}_{15\overline{k}}$ is updated $\forall \overline{k} \in \mathcal{GF}(2^2)$. It is updated only from the contribution of syndrome node 3 (green arrow), while node 1 (node in green) is not participating. This update will happen for all the syndrome nodes, as $\mathsf{q}_{35\overline{k}}$ will be calculated as well. It will be repeated for all variable nodes, before the tentative decoding (Step 4) is going to start [Mountogiannakis et al. (2022a)].

Appendix B

Galois Fields

B.1 Definition of Galois Fields

A Galois field is a field with finite number of elements. A common way to construct it is to take the modulo of the division of the integers over a prime number p. Consider, that for any field a positive integer i exists, such that $\mathsf{i} \cdot \mathsf{s} = 0$, $\forall \mathsf{s} \in \mathcal{R}$. Then, the least such positive integer is termed the characteristic of the field [Fraleigh (1982)]. In the case of Galois fields, the characteristic of the field is p. The order of a field is determined by the number of its elements. In this case, the cardinality of the alphabet $\mathcal{A}$ is the number of the symbols in the alphabet, given by

$$|\mathcal{A}| = \mathsf{p}^q \tag{B.1}$$

with $q \in \mathcal{N}^+$. All the Galois fields with the same number of elements are isomorphic and can be identified by $\mathcal{GF}(|\mathcal{A}|)$.

A special case is the order $|\mathcal{A}| = 2^q$. In a field with such an order, each element is associated with a binary polynomial of degree no more than $q - 1$. In other words, the elements can be described as q-bit strings, where each bit of the string corresponds to the coefficient of the polynomial at the same position. For example, the element 5 of $\mathcal{GF}(2^3)$ can be rewritten as $101 \rightarrow x^2 + 1$. Using this mapping, the operations of addition and multiplication can be defined in the field. For example, the sum of 5 and 6 is computed as follows:

$$101 + 110 \rightarrow (x^2 + 1) + (x^2 + x) = \underbrace{\overbrace{(1+1)}^{0} x^2 + x + 1}_{011 \rightarrow 3} \tag{B.2}$$

As the field is finite, addition can be performed using a precomputed matrix. For instance, the addition matrix $\mathbf{N}$, which includes all outcomes for $\mathcal{GF}(2^3)$, is

$$\mathbf{N}_3 = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 0 & 3 & 2 & 5 & 4 & 7 & 6 \\ 2 & 3 & 0 & 1 & 6 & 7 & 4 & 5 \\ 3 & 2 & 1 & 0 & 7 & 6 & 5 & 4 \\ 4 & 5 & 6 & 7 & 0 & 1 & 2 & 3 \\ 5 & 4 & 7 & 6 & 1 & 0 & 3 & 2 \\ 6 & 7 & 4 & 5 & 2 & 3 & 0 & 1 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \end{bmatrix} \tag{B.3}$$

Subtraction between two elements of $\mathcal{GF}(2^q)$ gives the same result as addition, making the two operations equivalent. Multiplication is more complicated, especially when the result is a polynomial with a degree larger then $q-1$. For instance, in $\mathcal{GF}(2^3)$, 7×6 is calculated as

$$\begin{aligned} 111 \times 110 \rightarrow (x^2+x+1) \times (x^2+x) \\ = x^4+x^3+x^3+x^2+x^2+x = x^4+x \end{aligned} \tag{B.4}$$

Because this is a degree 4 polynomial, this result needs to be taken modulo an irreducible polynomial of degree 3, e.g., x^3-x+1. A polynomial is irreducible in a Galois field, when it does not have a solution in that field. Thus,

$$(x^4+x \bmod x^3-x+1) = x^2 \rightarrow 100 \rightarrow 4 \tag{B.5}$$

where the operation can be made by adopting a long division with exclusive OR (XOR) [Mullen and Panario (2013)]. Instead of this cumbersome process, multiplication can be performed by using a precomputed matrix, likewise to addition. For instance, in $\mathcal{GF}(2^3)$, the results are specified by the following matrix:

$$\mathbf{M}_3 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 2 & 4 & 6 & 3 & 1 & 7 & 5 \\ 0 & 3 & 6 & 5 & 7 & 4 & 1 & 2 \\ 0 & 4 & 3 & 7 & 6 & 2 & 5 & 1 \\ 0 & 5 & 1 & 4 & 2 & 7 & 3 & 6 \\ 0 & 6 & 7 & 1 & 5 & 3 & 2 & 4 \\ 0 & 7 & 5 & 2 & 1 & 6 & 4 & 3 \end{bmatrix} \tag{B.6}$$

As it can be noticed from the matrices of Eq. (B.3) and Eq. (B.6), the Galois field is closed and commutative under both addition and multiplication operations. In addition, the field is always associative and distributive.

B.2 $\mathcal{GF}(2^4)$ Precomputed Matrices

For the convenience of the reader, the addition and multiplication matrices of $\mathcal{GF}(2^4)$ used for the syndrome calculation and the non-binary sum-product algorithm decoding are hereby presented.

$$\mathbf{N}_4 = \begin{bmatrix}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\
1 & 0 & 3 & 2 & 5 & 4 & 7 & 6 & 9 & 8 & 11 & 10 & 13 & 12 & 15 & 14 \\
2 & 3 & 0 & 1 & 6 & 7 & 4 & 5 & 10 & 11 & 8 & 9 & 14 & 15 & 12 & 13 \\
3 & 2 & 1 & 0 & 7 & 6 & 5 & 4 & 11 & 10 & 9 & 8 & 15 & 14 & 13 & 12 \\
4 & 5 & 6 & 7 & 0 & 1 & 2 & 3 & 12 & 13 & 14 & 15 & 8 & 9 & 10 & 11 \\
5 & 4 & 7 & 6 & 1 & 0 & 3 & 2 & 13 & 12 & 15 & 14 & 9 & 8 & 11 & 10 \\
6 & 7 & 4 & 5 & 2 & 3 & 0 & 1 & 14 & 15 & 12 & 13 & 10 & 11 & 8 & 9 \\
7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 & 15 & 14 & 13 & 12 & 11 & 10 & 9 & 8 \\
8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\
9 & 8 & 11 & 10 & 13 & 12 & 15 & 14 & 1 & 0 & 3 & 2 & 5 & 4 & 7 & 6 \\
10 & 11 & 8 & 9 & 14 & 15 & 12 & 13 & 2 & 3 & 0 & 1 & 6 & 7 & 4 & 5 \\
11 & 10 & 9 & 8 & 15 & 14 & 13 & 12 & 3 & 2 & 1 & 0 & 7 & 6 & 5 & 4 \\
12 & 13 & 14 & 15 & 8 & 9 & 10 & 11 & 4 & 5 & 6 & 7 & 0 & 1 & 2 & 3 \\
13 & 12 & 15 & 14 & 9 & 8 & 11 & 10 & 5 & 4 & 7 & 6 & 1 & 0 & 3 & 2 \\
14 & 15 & 12 & 13 & 10 & 11 & 8 & 9 & 6 & 7 & 4 & 5 & 2 & 3 & 0 & 1 \\
15 & 14 & 13 & 12 & 11 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0
\end{bmatrix} \tag{B.7}$$

$$\mathbf{M}_4 = \begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\
0 & 2 & 4 & 6 & 8 & 10 & 12 & 14 & 3 & 1 & 7 & 5 & 11 & 9 & 15 & 13 \\
0 & 3 & 6 & 5 & 12 & 15 & 10 & 9 & 11 & 8 & 13 & 14 & 7 & 4 & 1 & 2 \\
0 & 4 & 8 & 12 & 3 & 7 & 11 & 15 & 6 & 2 & 14 & 10 & 5 & 1 & 13 & 9 \\
0 & 5 & 10 & 15 & 7 & 2 & 13 & 8 & 14 & 11 & 4 & 1 & 9 & 12 & 3 & 6 \\
0 & 6 & 12 & 10 & 11 & 13 & 7 & 1 & 5 & 3 & 9 & 15 & 14 & 8 & 2 & 4 \\
0 & 7 & 14 & 9 & 15 & 8 & 1 & 6 & 13 & 10 & 3 & 4 & 2 & 5 & 12 & 11 \\
0 & 8 & 3 & 11 & 6 & 14 & 5 & 13 & 12 & 4 & 15 & 7 & 10 & 2 & 9 & 1 \\
0 & 9 & 1 & 8 & 2 & 11 & 3 & 10 & 4 & 13 & 5 & 12 & 6 & 15 & 7 & 14 \\
0 & 10 & 7 & 13 & 14 & 4 & 9 & 3 & 15 & 5 & 8 & 2 & 1 & 11 & 6 & 12 \\
0 & 11 & 5 & 14 & 10 & 1 & 15 & 4 & 7 & 12 & 2 & 9 & 13 & 6 & 8 & 3 \\
0 & 12 & 11 & 7 & 5 & 9 & 14 & 2 & 10 & 6 & 1 & 13 & 15 & 3 & 4 & 8 \\
0 & 13 & 9 & 4 & 1 & 12 & 8 & 5 & 2 & 15 & 11 & 6 & 3 & 14 & 10 & 7 \\
0 & 14 & 15 & 1 & 13 & 3 & 2 & 12 & 9 & 7 & 6 & 8 & 4 & 10 & 11 & 5 \\
0 & 15 & 13 & 2 & 9 & 6 & 4 & 11 & 1 & 14 & 12 & 3 & 8 & 7 & 5 & 10
\end{bmatrix} \tag{B.8}$$

Appendix C

Virtual Concatenation of the Conjugate Quadrature Variables

C.1 Secret Key Derivation

The current appendix is a review and direct adaptation of the theory developed in [(Pirandola, 2021a, Appendix G)]. Suppose that the measurement variables of Bob are $\boldsymbol{y} = (Q_y, P_y)$. He maps these variables to $\boldsymbol{l} = (Q_{\mathsf{l}}, P_{\mathsf{l}})$[1]. Then, the output classical-quantum state (CQ) of Alice, Bob and Eve, after the collective attack will be given by a state in a tensor product form $\rho^{\otimes n}$, where the single copy state will be represented by

$$\rho = \sum_{\boldsymbol{k},\boldsymbol{l}} p(\boldsymbol{k},\boldsymbol{l}) |\boldsymbol{k}\rangle_{\mathsf{R}_A}\langle\boldsymbol{k}| \otimes |\boldsymbol{l}\rangle_{\mathsf{R}_B}\langle\boldsymbol{l}| \otimes \rho_E(\boldsymbol{k},\boldsymbol{l}) \tag{C.1}$$

where R_A and R_B are Alice's and Bob's classical raw-key registers, $\boldsymbol{k} = (Q_{\mathsf{k}}, P_{\mathsf{k}})$ is the corresponding discretized version of Alice's encoding variable and $p(\boldsymbol{k},\boldsymbol{l})$ is the joint probability of the discretized variables.

The tensor product state can be then written as

$$\begin{aligned}\rho^{\otimes n} &= \sum_{\boldsymbol{k}^n,\boldsymbol{l}^n} p(\boldsymbol{k}^n,\boldsymbol{l}^n) \boldsymbol{k}^n\rangle_{\mathsf{R}_A^n}\langle\boldsymbol{k}^n| \otimes |\boldsymbol{l}^n\rangle_{\mathsf{R}_B^n}\langle\boldsymbol{l}^n| \otimes \rho_E^{\otimes n}(\boldsymbol{k}^n,\boldsymbol{l}^n) \\ &= \sum_{\mathsf{k}^{2n},\mathsf{l}^{2n}} p(\mathsf{k}^{2n},\mathsf{l}^{2n}) |\mathsf{k}^{2n}\rangle_{\mathsf{R}_A^n}\langle\mathsf{k}^{2n}| \otimes |\mathsf{l}^{2n}\rangle_{\mathsf{R}_B^n}\langle\mathsf{l}^{2n}| \otimes \rho_E^{\otimes n}(\mathsf{k}^{2n},\mathsf{l}^{2n})\end{aligned} \tag{C.2}$$

The sequence $\boldsymbol{l}^n$ is replaced by l^{2n}, so that each element $[\mathsf{l}]_{2j-1}$ corresponds to the element $[Q_{\mathsf{l}}]_j$ and each element $[\mathsf{l}]_{2j}$ to the element $[P_{\mathsf{l}}]_j$ for $j = 1 \dots n$.

[1] This variable is denoted as K in the main text.

In the reverse reconciliation setting, Alice guesses Bob's sequence I^{2n} with $\tilde{\mathsf{I}}^{2n}$, using her corresponding sequence k^{2n} and $\mathrm{leak}_{\mathrm{EC}}$ bits of information from Bob. The parties publicly compare the two hashes, each of length t as shown in Eq. (4.32), derived from $\tilde{\mathsf{k}}^{2n}$ and I^{2n} respectively. If they are equal, the parties continue with the protocol with probability p_{EC}; otherwise they abort.

This procedure is associated with a residual failure probability $\varepsilon_{\mathrm{cor}}$, which bounds the probability of the two sequences being different, even if their hashes coincide, as

$$p_{\mathrm{EC}}\mathrm{Prob}(\tilde{\mathsf{I}}^{2n} \neq \mathsf{I}^{2n}) \leq p_{\mathrm{EC}} 2^{-\lceil 1-\log_2 \varepsilon_{\mathrm{cor}} \rceil} \leq \varepsilon_{\mathrm{cor}} \tag{C.3}$$

In turn, EC can be simulated by a projection $\Pi_{\mathfrak{S}}$ of Alice's and Bob's classical registers R_A^n and R_B^n onto a "good" set $\mathfrak{S}$ of sequences. With success probability

$$p_{\mathrm{EC}} = \mathrm{tr}(\Pi_{\mathfrak{S}} \rho^{\otimes n}) \tag{C.4}$$

this quantum operation generates a CQ state

$$\tilde{\rho}^n = \frac{\Pi_{\mathfrak{S}} \rho^{\otimes n} \Pi_{\mathfrak{S}}}{p_{\mathrm{EC}}} \tag{C.5}$$

which is restricted to those sequences $\{\mathsf{k}^{2n}, \mathsf{I}^{2n}\}$ that can be corrected, i.e., mapped to a successful pair $\{\tilde{\mathsf{I}}^{2n}, \mathsf{I}^{2n}\}$.

The parties continue with the PA step with probability p_{EC} and apply a two-universal hash function over $\tilde{\rho}^n$, which outputs the PA state $\bar{\rho}^n$ approximating the ideal state ρ_{id}

$$p_{\mathrm{EC}} D(\bar{\rho}^n, \rho_{\mathrm{id}}) \leq \varepsilon_{\mathrm{sec}} \tag{C.6}$$

In fact, Alice and Bob perform EC and PA over the state $\rho^{\otimes n}$, in order to approximate the ℓ-bit ideal CQ state

$$\rho_{\mathrm{id}} = 2^{-s_n} \sum_{z=0}^{2^{s_n}-1} |z\rangle_{\mathsf{R}_A^n} \langle z| \otimes |z\rangle_{\mathsf{R}_B^n} \langle z| \otimes \rho_{E^n} \tag{C.7}$$

with Alice's and Bob's classical registers entirely decoupled from Eve and containing the same completely random sequence z with length ℓ. Using the triangle inequality from [(Portmann and Renner, 2014, Theorem 4.1)], the bound

$$p_{\mathrm{EC}} D(\tilde{\rho}^n, \rho_{\mathrm{id}}) \leq \varepsilon = \varepsilon_{\mathrm{cor}} + \varepsilon_{\mathrm{sec}} \tag{C.8}$$

is formed. The state $\bar{\rho}^n$ will contain ℓ bits of shared uniform randomness, satisfying the direct leftover hash bound as

$$\ell \geq H_{\min}^{\varepsilon_{\mathrm{s}}}(\mathsf{I}^{2n}|E^n)_{\tilde{\rho}^n} + 2\log_2 \sqrt{2}\varepsilon_{\mathrm{h}} - \mathrm{leak}_{\mathrm{EC}} \tag{C.9}$$

Here, $H_{\min}^{\varepsilon_s}(\mathsf{I}^{2n}|E^n)_{\tilde{\rho}^n}$ is the smooth min-entropy of Bob's sequence I^{2n} conditioned on Eve's system E^n after EC, and the smoothing ε_s and hashing ε_h parameters satisfy Eq. (4.33). The inequality explicitly accounts for the bits, that are leaked to Eve during EC. In fact, it can be rewritten as

$$s_n \geq H_{\min}^{\varepsilon_s}(\mathsf{I}^{2n}|E^n\mathsf{R})_{\tilde{\rho}^n} + 2\log_2\sqrt{2}\varepsilon_h \tag{C.10}$$

where R is a register of dimension $2^{\text{leak}_{\text{EC}}}$, while E^n are the systems used by Eve during the quantum communication. Then, the chain rule for the smooth-min entropy leads to

$$H_{\min}^{\varepsilon_s}(\mathsf{I}^{2n}|E^n\mathsf{R})_{\tilde{\rho}^n} \geq H_{\min}^{\varepsilon_s}(\mathsf{I}^{2n}|E^n)_{\tilde{\rho}^n} - \log_2 2^{\text{leak}_{\text{EC}}} \tag{C.11}$$

As seen earlier in the proposed EC procedure, Bob sends to Alice at most $p - R_{\text{code}}q$ bits for each of the quadratures in a signal state. This allows for the bounding of the leakage term by

$$\text{leak}_{\text{EC}} \leq 2n(p - R_{\text{code}}q) \tag{C.12}$$

The previous result is connected with the smooth min-entropy of $\rho^{\otimes n}$, which will later enable the AEP approximation. It is shown, that [(Pirandola et al., 2020, Appendix G2)]

$$H_{\min}^{\varepsilon_s}(\mathsf{I}^{2n}|E^n)_{\tilde{\rho}^n} \geq H_{\min}^{p_{\text{EC}}\varepsilon_s^2/3}(\mathsf{I}^{2n}|E^n)_{\rho^{\otimes n}} + \log_2(1 - \frac{\varepsilon_s^2}{3}) \tag{C.13}$$

It is theorized, that the parties concatenate their discretized values corresponding to the two quadrature variables of a single channel use, according to the bidirectional mapping

$$\phi = Q_{\mathsf{I}}2^p + P_{\mathsf{I}} \tag{C.14}$$

In that sense, instead of labeling the classical states as in Eq. (C.1) by using the combination of two labels, each described by p bits, only one label of $2p$ bits is used. Therefore, there is a classical mapping from a state $\rho^{\otimes n} = \rho_{\mathsf{I}^{2n}}^{\otimes n}$, described by the sequence I^{2n}, to the state $\rho_{l^n}^{\otimes n} \leftarrow \rho_{\mathsf{I}^{2n}}^{\otimes n}$, described by the sequence l^n. Applying Appendix D to Eq. (C.13), the following relation for the smooth min-entropy of the two states is obtained:

$$H_{\min}^{p_{\text{EC}}\varepsilon_s^2/3}(\mathsf{I}^{2n}|E^n)_{\rho_{\mathsf{I}^{2n}}^{\otimes n}} \geq H_{\min}^{p_{\text{EC}}\varepsilon_s^2/3}(\phi^n|E^n)_{\rho_{\phi^n}^{\otimes n}} \tag{C.15}$$

Then, from the AEP theorem, one obtains

$$H_{\min}^{p_{\text{EC}}\varepsilon_s^2/3}(\phi^n|E^n)_{\rho_{\phi^n}^{\otimes n}} \geq nH(\phi|E)_\rho - \sqrt{n}\Delta_{\text{AEP}}(p_{\text{EC}}\frac{\varepsilon_s^2}{3}, |\mathcal{L}|) \tag{C.16}$$

where $H(\phi|E)_\rho$ is the conditional von Neumann entropy computed over the single-copy state ρ, after applying the mapping of Eq. (C.14), and

$$\Delta_{\text{AEP}}(\varepsilon_s, |\mathcal{L}|) = 4\log_2(\sqrt{|\mathcal{L}|} + 2)\sqrt{\log_2\left(\frac{2}{\varepsilon_s^2}\right)} \tag{C.17}$$

with $|\mathcal{L}|$ being the cardinality of the discretized variable ϕ, given by

$$|\mathcal{L}| = 2^{2p} \tag{C.18}$$

By combining Eq. (C.9), Eq. (C.13) and Eq. (C.16), the following lower bound can be defined:

$$\ell \geq nH(\phi|E)_\rho - \sqrt{n}\Delta_{\text{AEP}}(p_{\text{EC}}\frac{\varepsilon_{\text{s}}^2}{3}, 2^{2p}) + \log_2(1 - \frac{\varepsilon_{\text{s}}^2}{3}) + 2\log_2\sqrt{2}\varepsilon_{\text{h}} - \text{leak}_{\text{EC}} \tag{C.19}$$

Note that the formula for the conditional entropy is

$$H(\phi|E)_\rho = H(\phi) - \chi(\phi : E)_\rho \tag{C.20}$$

where $H(l)$ is the Shannon entropy of ϕ and $\chi(E : \phi)_\rho$ is Eve's Holevo bound with respect to ϕ. By means of the data processing inequality, the Holevo bound relations become

$$\chi(E : \phi)_\rho \leq \chi(E : Q_y, P_y) = \chi(E : \boldsymbol{y}) \tag{C.21}$$

where the latter term is calculated using Eq. (5.67). Therefore,

$$H(\phi|E)_\rho \geq H(\phi) - \chi(E : \boldsymbol{y}) \tag{C.22}$$

Furthermore, the following replacement can also be made:

$$H(\phi) - n^{-1}\text{leak}_{\text{EC}} = \beta I(\boldsymbol{x} : \boldsymbol{y}) \tag{C.23}$$

Here, $I(\boldsymbol{x} : \boldsymbol{y})$ is calculated as shown in Remark 2 for the heterodyne protocol. For the CV-MDI case, it is found in Eq. (5.81). The reconciliation efficiency β is computed as

$$\beta = \frac{H(\phi) - n^{-1}\text{leak}_{\text{EC}}}{I(\boldsymbol{x} : \boldsymbol{y})} \tag{C.24}$$

Replacing Eq. (C.23) and (C.22) in (C.19), the result is

$$\ell \geq nR_{\text{asy}} - \sqrt{n}\Delta_{\text{AEP}}(p_{\text{EC}}\frac{\varepsilon_{\text{s}}^2}{3}, 2p) + \log_2(1 - \frac{\varepsilon_{\text{s}}^2}{3}) + 2\log_2\sqrt{2}\varepsilon_{\text{h}} \tag{C.25}$$

where the asymptotic secret key rate of Eq. (5.52) is integrated. After a successful PE stage, the parties compute R_{asy} over a state $\tilde{\rho}_{\text{wc}}^n$, instead of $\tilde{\rho}^n$. This is calculated with respect to the worst-case parameters, given in Eq. (5.107) and (5.108), along with the worst-case scenario entropy in Eq. (5.167). Consequently, Eq. (C.8) is replaced by the following relation:

$$p_{\text{EC}}D(\tilde{\rho}_{\text{wc}}^n, \rho_{\text{id}}) \leq \varepsilon_{\text{cor}} + \varepsilon_{\text{h}} + \varepsilon_{\text{s}} \tag{C.26}$$

However, there is still the probability that the actual state is a bad state $\tilde{\rho}^n_{\text{bad}}$ with probability $\tilde{\varepsilon}_{\text{PE}} = 2\varepsilon_{\text{PE}} + \varepsilon_{\text{ent}}$. On average, this is given by

$$\rho_{\text{PE}} = (1 - \tilde{\varepsilon}_{\text{PE}})\tilde{\rho}^n_{wc} + \tilde{\varepsilon}_{\text{PE}}\tilde{\rho}^n_{\text{bad}} \tag{C.27}$$

whose distance from the assumed worst-case state is

$$p_{\text{EC}} D(\rho_{\text{PE}}, \tilde{\rho}^n_{wc}) \leq p_{\text{EC}}\tilde{\varepsilon}_{\text{PE}} \tag{C.28}$$

By using Eq. (C.26) and Eq. (C.28), together with the triangle inequality, the result is

$$p_{\text{EC}} D(\rho_{\text{PE}}, \rho_{\text{id}}) \leq \varepsilon_{\text{cor}} + \varepsilon_{\text{h}} + \varepsilon_{\text{s}} + p_{\text{EC}}(2\varepsilon_{\text{PE}} + \varepsilon_{\text{ent}}) \tag{C.29}$$

Then, the secret key length can be bounded by

$$\ell \geq nR_M - \sqrt{n}\Delta_{\text{AEP}}(p_{\text{EC}}\frac{\varepsilon_{\text{s}}^2}{3}, 2p) + \log_2(1 - \frac{\varepsilon_{\text{s}}^2}{3}) + 2\log_2\sqrt{2}\varepsilon_{\text{h}} \tag{C.30}$$

where R_M has been taken from Eq. (5.116). The analysis of the EC process allows the connection of R_M with the practical rate R_M^{EC} through the parameter $\widehat{\beta}$ in Eq. (5.171). By replacing the latter in the previous secret key bound and multiplying by the successful probability of a block p_{EC} over the number of signals per block N, the composable secret key rate of Eq. (4.34) is obtained.

Note that, although the concatenation of the quadratures may not be applied in practice, theoretically, it has to be considered for the calculation of the discretization parameter $|\mathcal{L}|$, which is included in the correction term Δ_{AEP}. In fact, considering the proposed EC procedure, $|\mathcal{L}|$ takes the value $2p$ instead of p, when compared with the homodyne case. In turn, this affects the compression needed to extract a secret key with length ℓ.

C.2 Entropic Bounding

Suppose the reverse reconciliation scenario, where Alice estimates Bob's sequence, which is described by the continuous variable $\boldsymbol{y}$. Alice holds a variable $\boldsymbol{x}$, which is correlated with $\boldsymbol{y}$ via the quantum channel. Following Remark 2, the boldface notation for $\boldsymbol{x}$ and $\boldsymbol{y}$ implies the inclusion of both quadratures. Considering Bob's entropy is $H(\boldsymbol{y})$, he needs to send $H(\boldsymbol{y}|\boldsymbol{x})$ bits of information through a public channel, for Alice's accessible information to become equal to the mutual information, as

$$I(\boldsymbol{x} : \boldsymbol{y}) = 2I(x : y) = H(\boldsymbol{y}) - H(\boldsymbol{y}|\boldsymbol{x}) \tag{C.31}$$

As can be extracted from Eq. (C.23), the relation bounding the $H(\boldsymbol{y}|\boldsymbol{x})$ public bits is

$$\frac{\text{leak}_{\text{EC}}}{n} \geq H(\boldsymbol{y}|\boldsymbol{x}) \tag{C.32}$$

Assume the variable I[2] to be the discretized version of Y, which stands for Bob's variable after normalization. After the classical processing, the expression

$$H(\boldsymbol{y}) = H(Q_y, P_y) = 2H(y) \geq 2H(Y) \tag{C.33}$$

$$\geq 2H(\mathsf{I}) = H(Q_\mathsf{I}) + H(P_\mathsf{I}) = H(Q_\mathsf{I}, P_\mathsf{I}) = H(\phi) \tag{C.34}$$

holds, where the variables Q_I and P_I correspond to samples with odd and even indexes respectively and ϕ is the bidirectional mapping, given in Eq. (C.14).

Note that Eq. (C.33) is valid, because Q_y and P_y are independent. The same is true for Q_I and P_I, as they comprise different samples of an i.i.d. variable. Suppose a comparison of the differential entropy H of between two Gaussian variables: the first is y with variance σ_y^2 and the second is Y with unit variance, because of the normalization. In this context, the differential entropy is dependent only on the variances of the two variables [(Cover and Thomas, 2001, Th. 17.2.3)]. Passing from Eq. (C.33) to Eq. (C.34) can be achieved under the joint entropy of Y and ϕ. Note that for a function f applied on a random variable X, the following relation is true:

$$H(X, f(X)) = H(X) + \underbrace{H(f(X)|X)}_{=0} = H(f(X)) + H(X|f(X)) \tag{C.35}$$

The uncertainty for $f(X)$ given X is vanishing, leading to the inequality

$$H(X) \geq H(f(X)) \tag{C.36}$$

It can then be observed, that ϕ is a deterministic outcome of Y, while the opposite is not true. The last equation in Eq. (C.34) holds, because the mapping in Eq. (C.14) is bidirectional [Cicalese et al. (2017)]. The parties can then estimate $H(\phi)$ through $H(\mathsf{I})$.

[2] This variable is denoted as K in the main text.

Appendix D

Classical Data Mapping and Smooth Min-Entropy

Suppose a bidirectional mapping $X \leftrightarrow Z = f(X)$, where X is a discrete random variable, taking values x in the alphabet $\mathcal{X}$ with probability p_X. Then, Z takes values $z = f(x) \in \mathcal{Z}$ with probability p_Z. In fact, the probability function can absorb the action of f, such that

$$p_Z(z) = p_Z(f(x)) = p_X(x) \tag{D.1}$$

Therefore, the probabilities for the letters in $\mathcal{Y}$ are the same for the corresponding letter in $\mathcal{X}$.

The current investigation revolves around what is the effect on $H_{\min}^{\varepsilon}$ of such a mapping, when it is applied to the classical system of the CQ state

$$\rho_{XE} = \sum_x p_X(x)|x\rangle_X\langle x| \otimes \rho_E(x) \tag{D.2}$$

To do so, the proof of [(Tomamichel, 2016, Prop. 6.20)] is adapted for the state ρ_E, instead of ρ_{AB}. Thus the isometry $U : U_X \otimes \mathbf{I}_E$ is applied, with $U_X : |x\rangle \mapsto |x\rangle_{X'}|f(x)\rangle_Z$ being the Stinespring dilation of f [Stinespring (1955)] and $\mathbf{I}_E$ the identity. As a result, the following state is returned:

$$\tau_{X'ZE} = U\rho_{XE}U^{\dagger} \tag{D.3}$$

According to the invariance of the smooth min-entropy under isometries [(Tomamichel, 2016, Corollary 6.11)], the following relation is obtained:

$$H_{\min}^{\varepsilon}(X|E)_{\rho} = H_{\min}^{\varepsilon}(X'Z|E)_{\tau} \tag{D.4}$$

Furthermore, using [(Tomamichel, 2016, Lemma 6.17)] can lead to the bound

$$H_{\min}^{\varepsilon}(X'Z|E)_{\tau} \geq H_{\min}^{\varepsilon}(Z|E)_{\tau} \tag{D.5}$$

for

$$\tau_{ZE} = \sum_{x} p_X(x)|f(x)\rangle_Z\langle f(x)| \otimes \rho_E(x) \tag{D.6}$$

Finally, from Eq. (D.4) and Eq. (D.6), the bound becomes

$$H_{\min}^{\varepsilon}(X|E)_{\rho} \geq H_{\min}^{\varepsilon}(Z|E)_{\tau} \tag{D.7}$$

Note that, in the same way, Eq. (D.7) can be extended to the case of two classical systems X and Y, considering a Stinespring dilation $U_{XY} = U_X U_Y$ with $U_X : |x\rangle \mapsto |x\rangle_{X'}|f(x)\rangle_Z$ and $U_Y : |y\rangle \mapsto |y\rangle_{Y'}|f(y)\rangle_{Z'}$. Combining then Eq. (D.4) and (D.6) for the state

$$\rho_{XYE} = \sum_{xy} p_{XY}(xy)|x\rangle_X\langle x| \otimes |y\rangle_Y\langle y| \otimes \rho_E(x,y)$$

the inequality

$$H_{\min}^{\varepsilon}(XY|E)_{\rho} \geq H_{\min}^{\varepsilon}(ZZ'|E)_{\tau} \tag{D.8}$$

holds, where

$$\tau_{ZZ'E} = \sum_{xy} p_{XY}(x,y)|f(x)\rangle_Z\langle f(x)| \otimes |f(y)\rangle_{Z'}\langle f(y)| \otimes \rho_E(x,y)$$

Appendix E

Channel Parameter Estimation

E.1 Alternative Formulas for Parameter Estimation

The estimator for the square-root transmissivity

$$\tau = \sqrt{\eta T} \tag{E.1}$$

can be defined as

$$\widehat{\tau} = \frac{\sum_{i=1}^{m} x_i y_i}{\sum_{i=1}^{m} x_i^2} \simeq \frac{1}{m\sigma_x^2} \sum_{i=1}^{m} x_i y_i \tag{E.2}$$

Its variance is given by

$$\mathbb{V}(\widehat{\tau}) = \frac{\mathbb{V}\left(\sum_{i=1}^{m} x_i y_i\right)}{m^2(\sigma_x^2)^2} = \frac{\mathbb{V}(xy)}{m(\sigma_x^2)^2} = \frac{2}{m}\tau^2 + \frac{\sigma_z^2}{m\sigma_x^2} = \sigma_\tau^2 \tag{E.3}$$

Thus, the worst-case estimator for the transmissivity $T = \tau^2$ will be given by

$$\begin{aligned} T_m &= \frac{(\tau - W\sigma_\tau)^2}{\eta} = \frac{\left(\sqrt{\eta T} - W\sqrt{\frac{2}{m}\eta T + \frac{\sigma_z^2}{m\sigma_x^2}}\right)^2}{\eta} \\ &= \frac{\eta T - 2W\sqrt{\eta T}\sqrt{\frac{2}{m}\eta T + \frac{\sigma_z^2}{m\sigma_x^2}}}{\eta} + O(\frac{1}{m}) \simeq T\left(1 - 2W\sqrt{\frac{1}{m}}\sqrt{2 + \frac{\sigma_z^2}{\eta T \sigma_x^2}}\right) \end{aligned} \tag{E.4}$$

This expression is condensed in the main text, as shown by Eq. (5.107).

One may derive a less stringent estimator by assuming the approximation

$$\sum_{i=1}^{m} x_i^2 \simeq m\sigma_x^2 \tag{E.5}$$

meaning that a sample of size m from the data is sufficient to reproduce the theoretical variance σ_x^2. In such a case, one may write

$$\begin{aligned}\widehat{\tau} \simeq \frac{1}{m\sigma_x^2}\sum_{i=1}^{m} x_i(\tau x_i + z_i) =& \frac{1}{m\sigma_x^2}\left(\tau\sum_{i=1}^{m} x_i^2 + \sum_{i=1}^{m} x_i z_i\right) \\ \simeq& \frac{1}{m\sigma_x^2}\left(\tau m\sigma_x^2 + \sum_{i=1}^{m} x_i z_i\right) = \tau + \frac{\sum_{i=1}^{m} x_i z_i}{m\sigma_x^2}\end{aligned} \tag{E.6}$$

Therefore, the variance is now given by

$$\mathbb{V}(\widehat{\tau}) = \frac{\mathbb{V}\left(\sum_{i=1}^{m} x_i z_i\right)}{m^2(\sigma_x^2)^2} = \frac{\mathbb{V}\left(xz\right)}{m(\sigma_x^2)^2} = \frac{\sigma_z^2}{m\sigma_x^2} = (\sigma_\tau')^2 \tag{E.7}$$

yielding the worst-case parameter

$$T_m' = \frac{(\tau - W\sigma_\tau')^2}{\eta} \simeq T\left(1 - 2W\sqrt{\frac{1}{m}}\sqrt{\frac{\sigma_z^2}{\eta T\sigma_x^2}}\right) \tag{E.8}$$

Comparing the two methods, the relation in Eq. (E.4) returns a more pessimistic value for the worst-case transmissivity. This is owed to an extra term equal to 2 appearing in the square root term $\sqrt{2 + \sigma_z^2/\eta T\sigma_x^2}$, which is absent in Eq. (E.8). The analysis and the results in the main text consider the most conservative option, corresponding to the estimator in Eq. (E.4).

E.2 Calculation of MLE Variances in CV-MDI

The variance of the quantity of Eq. (5.121) is [Papanastasiou et al. (2017)]

$$\mathbb{V}(\widehat{C}_{Q_AQ_R}) = \frac{1}{m^2}\sum_{i=1}^{m}\mathbb{V}([Q_A]_i[Q_R]_i) = \frac{1}{m}\left(\tau_B^2\langle Q_B^2Q_A^2\rangle + 2\tau_A^2\langle Q_A^2\rangle^2 + \langle Q_z^2Q_A^2\rangle\right) \tag{E.9}$$

Replacing with Eq. (5.31) and Eq. (5.32), the variance becomes

$$\mathbb{V}(\widehat{C}_{Q_AQ_R}) = \frac{\frac{(\sigma_A^2)^2}{m}\left(\tau_A^2 + \frac{\tau_B^2}{2}\frac{\sigma_B^2}{\sigma_A^2}\right)}{\left(2 + \frac{\sigma_z^2}{\tau_A^2\sigma_A^2 + \frac{\tau_B^2}{2}\sigma_B^2}\right)^{-1}} = \mathbb{V}_{Q_AQ_R} \tag{E.10}$$

The variances from Eq. (5.122), Eq. (5.123) and Eq. (5.124) are calculated similarly.

Considering Eq. (5.125), in case $|\widehat{C}_{Q_AQ_R}| < |\widehat{C}_{P_AP_R}|$, Alice's channel transmissivity estimator is shaped as

$$\widehat{T}_A = \frac{2\mathbb{V}_{Q_AQ_R}}{\eta(\sigma_A^2)^2}\left(\frac{\widehat{C}_{Q_AQ_R}}{\sqrt{\mathbb{V}_{Q_AQ_R}}}\right)^2 \tag{E.11}$$

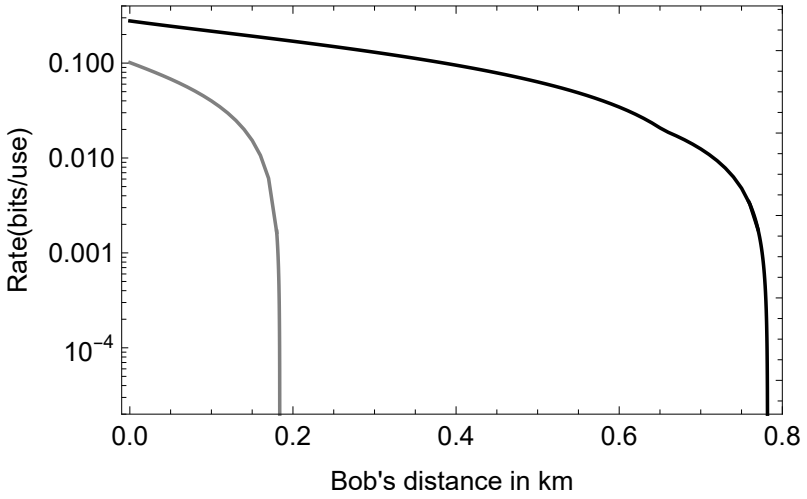

Figure E.1: Theoretical composable secret key rate R_{theo} (bits/use) versus Bob's channel length (km). Here, the formula of Eq. (5.191) is used to generate the results (black solid line), assuming $\tilde{\beta} = 0.9188$ and $\tilde{p}_{\text{EC}} = 0.95$. In addition, $p = 6$ and $N = 5.175 \times 10^5$ have been set. The remaining parameters have been taken from Table 6.7 for the simulations of Fig. 6.14. The theoretical composable rate is compared with the rate from [Lupo et al. (2018)] for the same parameters (gray line).

The variable $\left(\frac{\widehat{C}_{Q_A Q_R}}{\sqrt{\mathbb{V}_{Q_A Q_R}}}\right)^2$ is a chi-squared distributed variable with variance

$$\mathbb{V} = 2\left[1 + 2\left(\frac{C_{Q_A Q_R}}{\sqrt{\mathbb{V}_{Q_A Q_R}}}\right)^2\right] \tag{E.12}$$

such that

$$\mathbb{V}(\widehat{T}_A) = \frac{16\mathbb{V}_{Q_A Q_R} C^2_{Q_A Q_R}}{\eta^2 (\sigma_A^2)^4} + O\left(\frac{1}{m^2}\right) \tag{E.13}$$

Otherwise, $\widehat{T}_A$ is expressed by P_A and P_R and a similar relation for $\mathbb{V}(\widehat{T}_A)$ is returned. Eq. (5.130) is then obtained, after making all the appropriate replacements. Eq. (5.131) for $\widehat{T}_B$ is computed in the same way.

Based on Eq. (5.127) and given that

$$\frac{1}{m}\sum_{i=1}^{m}\left([q_R]_i + \widehat{\tau}_A[q_A]_i - \widehat{\tau}_B[q_B]_i\right)^2 > \frac{1}{m}\sum_{i=1}^{m}\left([p_R]_i - \widehat{\tau}_A[p_A]_i - \widehat{\tau}_B[p_B]_i\right)^2 \tag{E.14}$$

the outcome is

$$\begin{aligned}
\mathbb{V}(\widehat{\sigma}_z^2) &= \mathbb{V}\left[\frac{1}{m}\sum_{i=1}^{m}\left([q_R]_i + \widehat{\tau}_A[q_A]_i - \widehat{\tau}_B[q_B]_i\right)^2\right] \\
&\simeq \mathbb{V}\left[\frac{\sigma_z^2}{m}\sum_{i=1}^{m}\left(\frac{[q_R]_i + \tau_A[q_A]_i - \tau_B[q_B]_i}{\sqrt{\sigma_z^2}}\right)^2\right] \\
&= \frac{(\sigma_z^2)^2}{m^2} 2m = \frac{2}{m}(\sigma_z^2)^2
\end{aligned} \tag{E.15}$$

It is hypothesized, that the estimators $\widehat{\tau}_A$ and $\widehat{\tau}_B$ have negligible variances and can be replaced with their true values, so that any uncertainty for σ_z^2 stems purely from the data. It is then observed, that the sum in the same equation can be considered to be a chi-squared distributed variable with variance equal to $2m$. Finally, Eq. (5.132) is obtained by solving Eq. (5.35) with respect to the excess noise variance Ξ. Eq. (E.15) with σ_z^2 is then used, replaced by its estimator. Similar calculations hold for the other direction of the inequality in Eq. (E.14).

E.3 Simplifying Assumptions for CV-MDI

Alice and Bob declare m instances $\{q_{Ai}\}$, $\{p_{Ai}\}$ and $\{q_{Bi}\}$, $\{p_{Bi}\}$ for $i = 1, \ldots, m$ of their local variables. Using the relative relay output instances $\{q_{Ri}\}$, $\{p_{Ri}\}$, they estimate τ_A, τ_B, σ_z^2 and $\sigma_{z'}^2$. In particular, according to the multiple linear regression model [MIT Open Courseware (2006)], the following MLEs are obtained:

$$\widehat{\tau}_{A_q} = -\frac{\sum_{i=1}^m q_{Ai} q_{Ri}}{\sum_{i=1}^m q_{Ai}^2} \tag{E.16}$$

$$\widehat{\tau}_{A_p} = \frac{\sum_{i=1}^m p_{Ai} p_{Ri}}{\sum_{i=1}^m p_{Ai}^2} \tag{E.17}$$

$$\widehat{\tau}_{B_q} = \frac{\sum_{i=1}^m q_{Bi} q_{Ri}}{\sum_{i=1}^m q_{Bi}^2} \tag{E.18}$$

$$\widehat{\tau}_{B_p} = \frac{\sum_{i=1}^m p_{Bi} p_{Ri}}{\sum_{i=1}^m p_{Bi}^2} \tag{E.19}$$

$$\widehat{\sigma}_z^2 = \frac{1}{m} \sum_{i=1}^m (q_{Ri} - \widehat{\tau_B} q_{Bi} - \widehat{\tau_A} q_{Ai})^2 \tag{E.20}$$

$$\widehat{\sigma}_{z'}^2 = \frac{1}{m} \sum_{i=1}^m (p_{Ri} - \widehat{\tau}_B p_{Bi} - \widehat{\tau}_A p_{Ai})^2 \tag{E.21}$$

This is true for the MLEs for τ_A and τ_B, because the modulation of Alice's mode takes place independently from Bob. Then, from the theory of linear multiple regression, this is true for τ_{Aq}, τ_{Bq} and the MLE for σ_z^2. The same reasoning holds for $\widehat{\tau_{Ap}}$, $\widehat{\tau_{Bp}}$ and $\sigma_{z'}^2$. The previous MLEs are distributed according to

$$\widehat{\tau}_{A_q} \sim \mathcal{G}(\tau_A, \frac{\widehat{\sigma_z^2}}{m\sigma_x^2}) \tag{E.22}$$

$$\widehat{\tau}_{B_q} \sim \mathcal{G}(\tau_B, \frac{\widehat{\sigma_z^2}}{m\sigma_x^2}) \tag{E.23}$$

$$\widehat{\tau}_{A_p} \sim \mathcal{G}(\tau_A, \frac{\widehat{\sigma}_{z'}^2}{m\sigma_x^2}) \tag{E.24}$$

$$\widehat{\tau}_{B_p} \sim \mathcal{G}(\tau_B, \frac{\widehat{\sigma}_{z'}^2}{m\sigma_x^2}) \tag{E.25}$$

$$\frac{m\widehat{\sigma}_z^2}{\sigma_z^2} \sim \chi^2(m-2) \tag{E.26}$$

$$\frac{m\widehat{\sigma}_{z'}^2}{\sigma_{z'}^2} \sim \chi^2(m-2) \tag{E.27}$$

It must be noted, that $\widehat{\tau}_{A_q}$ and $\widehat{\tau}_{A_p}$ can be calculated by Alice without the exchange of variables. Their value can then be communicated to Bob. For this reason, Alice can manipulate all her data to estimate τ_A. The same is true for Bob, with respect to τ_B. In fact, both of them can combine the two estimators from the conjugate quadratures into a single one through a linear optimization, based on the estimators

$$\widehat{\tau}_A = \kappa\widehat{\tau}_{A_q} + (1-\kappa)\widehat{\tau}_{A_p} \tag{E.28}$$

$$\widehat{\tau}_B = \kappa\widehat{\tau}_{B_q} + (1-\kappa)\widehat{\tau}_{B_p} \tag{E.29}$$

with

$$\kappa = \frac{\mathbb{V}(\widehat{\tau}_{A_p})}{\mathbb{V}(\widehat{\tau}_{A_q}) + \mathbb{V}(\widehat{\tau_{A_p}})} = \frac{\mathbb{V}(\widehat{\tau}_{B_p})}{\mathbb{V}(\widehat{\tau}_{B_q}) + \mathbb{V}(\widehat{\tau}_{B_p})} = \frac{\widehat{\sigma}^2_{z'}}{\widehat{\sigma}^2_z + \widehat{\sigma}^2_{z'}} \tag{E.30}$$

These new estimators have variance $\kappa\frac{\widehat{\sigma}^2_z}{N\sigma^2_x}$. Therefore, one obtains

$$\widehat{T}_A = \frac{2\widehat{\tau}^2_A}{\eta} \tag{E.31}$$

$$\widehat{T}_B = \frac{2\widehat{\tau}^2_B}{\eta} \tag{E.32}$$

$$\widehat{\Xi} = \widehat{\sigma}_z - v_{\mathrm{el}} - 1 \tag{E.33}$$

$$\widehat{\Xi}' = \widehat{\sigma}_{z'} - v_{\mathrm{el}} - 1 \tag{E.34}$$

For large m, the distribution $\chi^2(m-2)$ can be regarded as Gaussian with variance $2m$. Next, based on the previous considerations, the parties derive confidence intervals as

$$\tau_A, \tau_B \in [\widehat{\tau}_{A,B} - W_\tau, \widehat{\tau}_{A,B} - W_\tau] \tag{E.35}$$

$$\sigma^2_{z,z'} \in [\widehat{\sigma}^2_{z,z'} - W_{z,z'}, \widehat{\sigma}^2_{z,z'} + W_{z,z'}] \tag{E.36}$$

with

$$W_\tau = W\sqrt{\kappa\frac{\widehat{\sigma}^2_z}{N\sigma^2_x}} \tag{E.37}$$

$$W_{z,z'} = W\widehat{\sigma}^2_{z,z'}\sqrt{\frac{2}{m}} \tag{E.38}$$

Finally, Alice and Bob calculate worst-case scenario values for the parameters T_A, T_B, Ξ and Ξ' using the following formulas:

$$T_{Am} = 2\frac{(\widehat{\tau}_A - \Delta_\tau)^2}{\eta} \tag{E.39}$$

$$T_{Bm} = 2\frac{(\widehat{\tau}_B - \Delta_\tau)^2}{\eta} \tag{E.40}$$

$$\Xi_m = \widehat{\Xi} + \Delta_z \tag{E.41}$$

$$\Xi'_m = \widehat{\Xi}' + \Delta_{z'} \tag{E.42}$$

Appendix F

Equivalent Mutual Information

The CM of Alice's and Bob's key extraction variables x and y is given by

$$\mathbf{\Sigma}_{xy} = \begin{bmatrix} \sigma_x^2\mathbf{I} & \sigma_{xy}\mathbf{Z} \\ \sigma_{xy}\mathbf{Z} & \sigma_y^2\mathbf{I} \end{bmatrix} = \begin{bmatrix} \left(\sigma_A^2 - \frac{\tau_A^2(\sigma_A^2)^2}{\tau_A^2\sigma_A^2+\tau_B^2\sigma_B^2+\sigma_z^2}\right)\mathbf{I} & \frac{\tau_A\tau_B\sigma_A^2\sigma_B^2}{\tau_A^2\sigma_A^2+\tau_B^2\sigma_B^2+\sigma_z^2}\mathbf{Z} \\ \frac{\tau_A\tau_B\sigma_A^2\sigma_B^2}{\tau_A^2\sigma_A^2+\tau_B^2\sigma_B^2+\sigma_z^2}\mathbf{Z} & \left(\sigma_B^2 - \frac{\tau_B^2(\sigma_B^2)^2}{\tau_A^2\sigma_A^2+\tau_B^2\sigma_B^2+\sigma_z^2}\right)\mathbf{I} \end{bmatrix} \tag{F.1}$$

Taking into account Eq. (5.141) and considering the independence of the quadratures, the formula for the mutual information for bivariate normal distributions from [Cover and Thomas (2001)] can be applied, as follows:

$$I(\boldsymbol{x}:\boldsymbol{y}) = \left[\frac{1}{2}\log_2\left(\frac{1}{1-(\rho_{\boldsymbol{xy}}^Q)^2}\right)\right] + \left[\frac{1}{2}\log_2\left(\frac{1}{1-(\rho_{\boldsymbol{xy}}^P)^2}\right)\right] = \log_2\left(\frac{1}{1-\rho_{\boldsymbol{xy}}^2}\right) \tag{F.2}$$

where

$$\rho_{\boldsymbol{xy}} = \rho_{\boldsymbol{xy}}^Q = -\rho_{\boldsymbol{xy}}^P = \frac{\sigma_{xy}}{\sqrt{\sigma_x^2}\sqrt{\sigma_y^2}} = \tau_A\tau_B\sqrt{\frac{\sigma_A^2\sigma_B^2}{(\tau_A^2\sigma_A^2+\sigma_z^2)(\tau_B^2\sigma_B^2+\sigma_z^2)}} \tag{F.3}$$

It can then be verified that this is equivalent to Eq. (5.66).

Appendix G

Procedural Pseudocode

The following algorithms provide a high-level overview of the steps followed during the simulations for each protocol. It must be noted, that the assignment of the constant parameters, i.e. q, w_{c}, $\varepsilon_{\mathrm{PE}}$, $\varepsilon_{\mathrm{ent}}$, $\varepsilon_{\mathrm{cor}}$, ε_s, ε_h, is shown explicitly to reflect the path of the executed simulations of Chapter 6. In practice, these parameters can be initialized with any value.

Algorithm 2 Homodyne Protocol

$L, A, \eta, \xi, v_{\mathrm{el}}, n_{\mathrm{bks}}, N, M, \beta, \mathrm{iter}_{\max}, p, \alpha \leftarrow$ Input_Definition()
$\varepsilon_{\mathrm{PE}}, \varepsilon_{\mathrm{ent}}, \varepsilon_{\mathrm{cor}}\varepsilon_s, \varepsilon_h \leftarrow 2^{-32}$
$w_{\mathrm{c}} \leftarrow 2$
$q \leftarrow 4$
Validity_Checks()
$T, \sigma_z^2, \Xi, m, n, t, \mathrm{GF}, \delta, d \leftarrow$ Dependent_Values()
if is_mu_optimal **then**
    $\mu^{\mathrm{opt}} \leftarrow$ Optimal_Signal_Variance()
else
    $\mu \leftarrow$ user_input
end if
for blk $= 1, \ldots n_{\mathrm{bks}}$ **do**
    x[blk] $\leftarrow$ State_Preparation()
    y[blk] $\leftarrow$ State_Transmission()
    y[blk] $\leftarrow$ State_Measurement()
    x[blk] $\leftarrow$ Key_Sifting()
end for
R_{asy}, $I(x:y)|_{T,\Xi}$, $\chi(E:y)|_{T,\Xi} \leftarrow$ Rate_Calculation()
$\{i_u, x_{i_u}\}_{u=1}^{M}, \{i_u, y_{i_u}\}_{u=1}^{M} \leftarrow$Sacrificed_States_Selection()
$\widehat{T}, \widehat{\Xi}, T_M, \Xi_M \leftarrow$ Parameter_Estimation()
R_M, $I(x:y)|_{\widehat{T},\widehat{\Xi}}$, $\chi(E:y)|_{T_M,\Xi_M} \leftarrow$ Rate_After_PE_Calculation()
if $I(x:y)|_{\widehat{T},\widehat{\Xi}} \leq \chi(E:y)|_{T_M,\Xi_M}$ **then**
    Abort_Protocol()
end if
$X, Y \leftarrow$ Normalization()
for blk $= 1, \ldots n_{\mathrm{bks}}$ **do**
    K[blk] $\leftarrow$ Discretization()
    $\overline{K}$[blk], $\underline{K}$[blk] $\leftarrow$ Splitting()
    $p_{\overline{K}|X,\underline{K}}$[blk] $\leftarrow$ A_Priori_Probabilities_Calculation()
end for
$\widehat{H}$(K),$R_{\mathrm{code}} \leftarrow$ Code_Rate_Calculation()
$\mathbf{H} \leftarrow$ LDPC_Code_Generation()
$\widehat{\mathrm{SNR}}, \widehat{\rho} \leftarrow$ Correlation()
for blk $= 1, \ldots n_{\mathrm{bks}}$ **do**
    $\overline{K}^{l}_{\mathrm{sd}}$[blk] $\leftarrow$ Bob_Syndrome_Calculation()
    $\widehat{K}^{n}$[blk], fnd, $\mathrm{rnd}_{\mathrm{fnd}} \leftarrow$ Non_Binary_Decoding()
    $\widehat{K}^{n}_{\mathrm{bin}}$[blk], $\overline{K}^{n}_{\mathrm{bin}}$[blk], $\underline{K}^{n}_{\mathrm{bin}}$[blk] $\leftarrow$ Bin_Conversion()
    hash_verified[blk] $\leftarrow$ Verification()
    if is_hash_verified[blk] **then**
        S_A[blk] $\leftarrow$ Concatenate($\widehat{K}^{n}_{\mathrm{bin}}$[blk], $\underline{K}^{n}_{\mathrm{bin}}$[blk])
        S_B[blk] $\leftarrow$ Concatenate($\overline{K}^{n}_{\mathrm{bin}}$[blk], $\underline{K}^{n}_{\mathrm{bin}}$[blk])
    end if
end for
$p_{\mathrm{EC}}, \mathrm{FER} \leftarrow$ Frame_Error_Rate_Calculation()
$R_M^{\mathrm{EC}} \leftarrow$ Finite_Size_Rate_Calculation()
$R, r, \tilde{n}, \varepsilon \leftarrow$ Composable_Rate_Calculation()
if $R > 0$ **then**
    for blk $= 1, \ldots p_{\mathrm{EC}} n_{\mathrm{bks}}$ **do**
        $\Upsilon' \leftarrow$ Privacy_Amplification(S_A)
    end for
    $\Upsilon \leftarrow$ Concatenate(Υ')
end if

Algorithm 3 Heterodyne Protocol

$L, A, \eta, \xi, v_{\mathrm{el}}, n_{\mathrm{bks}}, N, M, \beta, \mathrm{iter}_{\max}, p, q, \alpha \leftarrow$ Input_Definition()
$\varepsilon_{\mathrm{PE}}, \varepsilon_{\mathrm{ent}}, \varepsilon_{\mathrm{cor}}\varepsilon_s, \varepsilon_h \leftarrow 2^{-32}$
$w_{\mathrm{c}} \leftarrow 2$
$q \leftarrow 4$
Validity_Checks()
$T, \sigma_z^2, \Xi, m, n, t, \mathrm{GF}, \delta, d \leftarrow$ Dependent_Values()
if is_mu_optimal **then**
    $\mu^{\mathrm{opt}} \leftarrow$ Optimal_Signal_Variance()
else
    $\mu \leftarrow$ user_input
end if
for blk $= 1, \ldots n_{\mathrm{bks}}$ **do**
    x[blk] $\leftarrow$ State_Preparation()
    y[blk] $\leftarrow$ State_Transmission()
    x[blk], y[blk] $\leftarrow$ Quadrature_Concatenation()
end for
R_{asy}, $I(x:y)|_{T,\Xi}$, $\chi(E:y)|_{T,\Xi} \leftarrow$ Rate_Calculation()
$\{i_u, x_{i_u}\}_{u=1}^{M}, \{i_u, y_{i_u}\}_{u=1}^{M} \leftarrow$Sacrificed_States_Selection()
$\widehat{T}, \widehat{\Xi}, T_M, \Xi_M \leftarrow$ Parameter_Estimation()
R_M, $I(x:y)|_{\widehat{T},\widehat{\Xi}}$, $\chi(E:y)|_{T_M,\Xi_M} \leftarrow$ Rate_After_PE_Calculation()
if $I(x:y)|_{\widehat{T},\widehat{\Xi}} \leq \chi(E:y)|_{T_M,\Xi_M}$ **then**
    Abort_Protocol()
end if
$X, Y \leftarrow$ Quadrature_Concatenation()
$X, Y \leftarrow$ Normalization()
for blk $= 1, \ldots n_{\mathrm{bks}}$ **do**
    K[blk] $\leftarrow$ Discretization()
    $\overline{K}$[blk], $\underline{K}$[blk] $\leftarrow$ Splitting()
    $p_{\overline{K}|X,\underline{K}}$[blk] $\leftarrow$ A_Priori_Probabilities_Calculation()
end for
$\widehat{H}$(K),$R_{\mathrm{code}} \leftarrow$ Code_Rate_Calculation()
$\widehat{\mathrm{SNR}}, \widehat{\rho} \leftarrow$ Correlation()
$\mathbf{H} \leftarrow$ LDPC_Code_Generation()
for blk $= 1, \ldots n_{\mathrm{bks}}$ **do**
    $\overline{K}_{\mathrm{sd}}^{l}$[blk] $\leftarrow$ Bob_Syndrome_Calculation()
    $\widehat{K}^{2n}$[blk], fnd, $\mathrm{rnd}_{\mathrm{fnd}} \leftarrow$ Non_Binary_Decoding()
    $\widehat{K}_{\mathrm{bin}}^{2n}$[blk], $\overline{K}_{\mathrm{bin}}^{2n}$[blk], $\underline{K}_{\mathrm{bin}}^{2n}$[blk] $\leftarrow$ Bin_Conversion()
    hash_verified[blk] $\leftarrow$ Verification()
    if is_hash_verified[blk] **then**
        $\widehat{S}$[blk] $\leftarrow$ Concatenate($\widehat{K}_{\mathrm{bin}}^{2n}$[blk], $\underline{K}_{\mathrm{bin}}^{2n}$[blk])
        S[blk] $\leftarrow$ Concatenate($\overline{K}_{\mathrm{bin}}^{2n}$[blk], $\underline{K}_{\mathrm{bin}}^{2n}$[blk])
    end if
end for
$p_{\mathrm{EC}}, \mathrm{FER} \leftarrow$ Frame_Error_Rate_Calculation()
$R_M^{\mathrm{EC}} \leftarrow$ Finite_Size_Rate_Calculation()
$R, r, \tilde{n}, \varepsilon \leftarrow$ Composable_Rate_Calculation()
if $R > 0$ **then**
    for blk $= 1, \ldots p_{\mathrm{EC}} n_{\mathrm{bks}}$ **do**
        $\Upsilon' \leftarrow$ Privacy_Amplification(S_A)
    end for
    $\Upsilon \leftarrow$ Concatenate(Υ')
end if

Algorithm 4 CV-MDI Protocol

$T_A, T_B, \eta, \xi_A, \xi_B, v_{\text{el}}, n_{\text{bks}}, N, M, \beta, \text{iter}_{\max}, p, \alpha \leftarrow$ Input_Definition()
$\varepsilon_{\text{PE}}, \varepsilon_{\text{ent}}, \varepsilon_{\text{cor}}\varepsilon_s, \varepsilon_h \leftarrow 2^{-32}$
$w_{\text{c}} \leftarrow 2$
$q \leftarrow 4$
Validity_Checks()
$T, \sigma_z^2, m, n, t, \text{GF}, \delta, d \leftarrow$ Dependent_Values()
if is_mu_optimal **then**
    $\mu_A^{\text{opt}}, \mu_B^{\text{opt}} \leftarrow$ Optimal_Signal_Variance()
else
    $\mu_A, \mu_B \leftarrow$ user_input
end if
$\Xi, g, g' \leftarrow$ Correlation_Parameters()
for blk $= 1, \ldots n_{\text{bks}}$ **do**
    x[blk] $\leftarrow$ State_Preparation()
    y[blk] $\leftarrow$ State_Transmission()
end for
R_{asy}, $I(x:y)|_{T,\Xi}$, $\chi(E:y)|_{T,\Xi} \leftarrow$ Rate_Calculation()
$\{i_u, x_{i_u}\}_{u=1}^{M}, \{i_u, y_{i_u}\}_{u=1}^{M} \leftarrow$Sacrificed_States_Selection()
$\widehat{T}, \widehat{\Xi}, T_M, \Xi_M \leftarrow$ Parameter_Estimation()
R_M, $I(x:y)|_{\widehat{T},\widehat{\Xi}}$, $\chi(E:y)|_{T_M,\Xi_M} \leftarrow$ Rate_After_PE_Calculation()
if $I(x:y)|_{\widehat{T},\widehat{\Xi}} \leq \chi(E:y)|_{T_M,\Xi_M}$ **then**
    Abort_Protocol()
end if
$Q_X, P_X, Q_Y, P_Y \leftarrow$ Key_Extraction_Variable_Formation()
$X, Y \leftarrow$ Quadrature_Concatenation()
$X, Y \leftarrow$ Normalization()
for blk $= 1, \ldots n_{\text{bks}}$ **do**
    K[blk] $\leftarrow$ Discretization()
    $\overline{K}$[blk], $\underline{K}$[blk] $\leftarrow$ Splitting()
    $p_{\overline{K}|X,\underline{K}}$[blk] $\leftarrow$ A_Priori_Probabilities_Calculation()
end for
$\widehat{H}(\text{K})$,$R_{\text{code}} \leftarrow$ Code_Rate_Calculation()
$\widehat{\text{SNR}}, \widehat{\rho} \leftarrow$ Correlation()
$\mathbf{H} \leftarrow$ LDPC_Code_Generation()
for blk $= 1, \ldots n_{\text{bks}}$ **do**
    $\overline{K}_{\text{sd}}^{l}$[blk] $\leftarrow$ Bob_Syndrome_Calculation()
    $\widehat{K}^{2n}$[blk], fnd, $\text{rnd}_{\text{fnd}} \leftarrow$ Non_Binary_Decoding()
    $\widehat{K}_{\text{bin}}^{2n}$[blk], $\overline{K}_{\text{bin}}^{2n}$[blk], $\underline{K}_{\text{bin}}^{2n}$[blk] $\leftarrow$ Bin_Conversion()
    hash_verified[blk] $\leftarrow$ Verification()
    if is_hash_verified[blk] **then**
        $\widehat{S}$[blk] $\leftarrow$ Concatenate($\widehat{K}_{\text{bin}}^{2n}$[blk], $\underline{K}_{\text{bin}}^{2n}$[blk])
        S[blk] $\leftarrow$ Concatenate($\overline{K}_{\text{bin}}^{2n}$[blk], $\underline{K}_{\text{bin}}^{2n}$[blk])
    end if
end for
$p_{\text{EC}}, \text{FER} \leftarrow$ Frame_Error_Rate_Calculation()
$R_M^{\text{EC}} \leftarrow$ Finite_Size_Rate_Calculation()
$R, r, \tilde{n}, \varepsilon \leftarrow$ Composable_Rate_Calculation()
if $R > 0$ **then**
    for blk $= 1, \ldots p_{\text{EC}} n_{\text{bks}}$ **do**
        $\Upsilon' \leftarrow$ Privacy_Amplification(S_A)
    end for
    $\Upsilon \leftarrow$ Concatenate(Υ')
end if

Appendix H

Software Performance and Requirements

It can be anticipated, that the simulation and postprocessing of an entire CV-QKD protocol can be demanding, in terms of computational resources. To provide algorithmic speedups, various techniques were used, which include, but are not limited to

- the usage of the Numba library,
- the parallelization of most processes,
- the use of dictionary structures, whose lookup time complexity is $O(1)$ and
- precomputed tables for the Galois field computations. These exact tables are located in Appendix B.2.

The simulations were executed on the Interactive Research Linux Service of the University of York, whose specifications are noted in Table H.1. Despite employing a powerful workstation for the tasks, the software is able to run on a conventional computer as well. However, the speed will be significantly diminished. The workstation is recommended to have any modern processor, at least 16GB of RAM and a Python version of 3.7 and above.

CPU Model	Intel Xeon E5-2680 v4
CPU Clock Speed	2.60 GHz
Number of Cores	56
RAM	512GB
OS	Ubuntu 20.04
Python Version	3.8

Table H.1: The specifications of the system, on which the simulations were executed.

Benchmarks, which illustrate the performance of the software, in terms of speed and memory consumption, are presented in [(Mountogiannakis et al., 2022a, Appendix E)]. They are not included in this work, because they do not reflect the current status of the software. Since the documentation of these benchmarks, the software has been significantly improved in both performance areas. Note that the error correction stage still accounts for the overwhelming majority of the entire runtime.

An advantage of the sum-product algorithm is that it is highly parallelizable by design. Therefore, possessing more processing cores is beneficial in terms of speed. Consequently, projects with the sum-product algorithm are often carried out in GPUs [Milisevic (2017)] because of their superior number of cores compared to CPUs. To provide massive compatibility, the software is written to target solely CPUs. Future versions of the software may process the error correction stage on a GPU level. In addition, the non-binary sum-product method used in this paper is anachronistic, in terms of speed. The complexity of the implemented version is $\mathbf{n}w_c q^2$ per iteration [Davey and MacKay (1998)]. There exists a newer method, which moves the burdensome computations of the horizontal step to the frequency domain by utilizing the FFT [Barnault and Declercq (2003), Safarnejad and Sadeghi (2012)]. The complexity of the process can then be significantly reduced [Hong and Sun (2011)]. Future improvements on the algorithm could potentially include this method as well.

References

A. G. Mountogiannakis, P. Papanastasiou, B. Braverman, and S. Pirandola, "Composably secure data processing for Gaussian-modulated continuous-variable quantum key distribution," *Phys. Rev. Research*, vol. 4, p. 013099, 2022.

P. Papanastasiou, A. G. Mountogiannakis, and S. Pirandola, "Composable security of CV-MDI-QKD with secret key rate and data processing," *Sci. Rep.*, vol. 13, p. 11636, 2023.

C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, "Continuous-variable measurement-device independent quantum key distribution: Composable security against coherent attacks," *Phys. Rev. A*, vol. 97, p. 052327, 2018.

V. Fock, "Konfigurationsraum und zweite Quantelung," *Z. Phys.*, vol. 75, pp. 622–647, 1932.

R. J. Glauber, "The Quantum Theory of Optical Coherence," *Phys. Rev.*, vol. 130, pp. 2529–2539, 1963.

R. Loudon, *The Quantum Theory of Light.* Oxford: Clarendon Press, 1983.

S. M. Barnett and P. M. Radmore, *Methods in Theoretical Quantum Optics.* New York: Oxford University Press, 1997.

A. Ferraro, S. Olivares, and M. G. A. Paris, "Gaussian states in quantum information," *Napoli Series on Physics and Astrophysics*, 2005.

X.-B. Wang, T. Hiroshima, A. Tomita, and M. Hayashi, "Quantum information with Gaussian states," *Phys. Rep.*, vol. 448, pp. 1–111, 2007.

W. Li, Z. Meng, X. Yu, and J. Zhang, "Experimental study of balanced optical homodyne and heterodyne detection by controlling sideband modulation," *Sci. China: Phys. Mech. Astron.*, vol. 58, p. 104201, 2015.

F. Laudenbach, C. Pacher, Chi-Hang, F. Fund, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, "Continuous-Variable Quantum Key Distribution with Gaussian Modulation - The Theory of Practical Implementations," *Adv. Quantum Technol.*, vol. 1, p. 1800011, 2018.

C. E. Shannon, "A Mathematical Theory of Communication," *Bell Syst. Tech. J.*, vol. 27, pp. 379–423, 1948.

M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, "Leftover Hashing Against Quantum Side Information," *IEEE Trans. Inf. Theory*, vol. 57, pp. 5524–5535, 2011.

T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Hoboken, New Jersey: Wiley-Interscience, 2001.

R. W. Hamming, "Error Detecting and Error Correcting Codes," *Bell Syst. Tech. J.*, vol. 29, pp. 147–160, 1950.

R. G. Gallager, "Low-density parity-check codes," *IEEE Trans. Inf. Theory*, vol. 8, pp. 21–28, 1962.

D. J. C. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inf. Theory*, vol. 45, pp. 399–431, 1999.

D. Slepian and J. K. Wolf, "Noiseless Coding of Correlated Information Sources," *IEEE Trans. Inf. Theory*, vol. 19, pp. 471–480, 1973.

P. A. M. Dirac, "Generalized Hamiltonian dynamics," *Can. J. Math.*, vol. 2, pp. 129–148, 1950.

A. S. Holevo, "Some estimates for the amount of information transmittable by a quantum communications channel," *Problemy Peredachi Informatsii*, vol. 9, pp. 3–11, 1973.

B. Schumacher and M. D. Westmoreland, "Sending classical information via noisy quantum channels," *Phys. Rev. A*, vol. 56, pp. 131–138, 1997.

R. Jozsa, "Fidelity for Mixed Quantum States," *J. Mod. Opt.*, vol. 41, pp. 2315–2323, 1994.

C. A. Fuchs and J. van de Graaf, "Cryptographic distinguishability measures for quantum-mechanical states," *IEEE Trans. Inf. Theory*, vol. 45, pp. 1216–1227, 1999.

M. Tomamichel, R. Colbeck, and R. Renner, "A Fully Quantum Asymptotic Equipartition Property," *IEEE Trans. Inf. Theory*, vol. 55, pp. 5840–5847, 2009.

C. Weedbrook, S. Pirandola, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian Quantum Information," *Rev. Mod. Phys.*, vol. 84, pp. 621–669, 2012.

E. Wigner, "On the Quantum Correction For Thermodynamic Equilibrium," *Phys. Rev.*, vol. 40, pp. 749–759, 1932.

R. Simon, N. Mukunda, and B. Dutta, "Quantum-noise matrix for multimode systems: U(n) invariance, squeezing, and normal forms," *Phys. Rev. A*, vol. 49, pp. 1567–1583, 1994.

D. F. Walls and G. J. Milburn, *Quantum Optics*, 2nd ed. Springer, 2008.

R. L. Hudson, "When is the wigner quasi-probability density non-negative?" *Rep. Math. Phys.*, vol. 6, pp. 249–252, 1974.

J. Williamson, "On the Algebraic Problem Concerning the Normal Forms of Linear Dynamical Systems," *Am. J. Math.*, vol. 58, pp. 141–163, 1936.

J. L. Pereira, L. Banchi, and S. Pirandola, "Symplectic decomposition from submatrix determinants," *Proc. R. Soc. A.*, vol. 477, p. 20210513, 2021.

S. Pirandola, A. Serafini, and S. Lloyd, "Correlation matrices of two-mode bosonic systems," *Phys. Rev. A*, vol. 79, p. 052327, 2009.

A. Serafini, F. Illuminati, M. G. A. Paris, and S. D. Siena, "Entanglement and purity of two-mode Gaussian states in noisy channels," *Phys. Rev. A*, vol. 69, p. 022318, 2004.

S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," *Adv. Opt. Photon*, vol. 12, pp. 1012–1236, 2020.

W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, pp. 802–803, 1982.

C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of International Conference on Computers, Systems and Signal Processing*, Bangalore, India, December 1984, pp. 175–179.

V. Scarani and R. Renner, "Quantum Cryptography with Finite Resources: Unconditional Security Bound for Discrete-Variable Protocols with One-Way Post-processing," *Phys. Rev. Lett.*, vol. 100, p. 200501, 2008.

V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, "The Security of Practical Quantum Key Distribution," *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, 2009.

D. Bunandar, L. C. G. Govia, H. Krovi, and D. Englund, "Numerical finite-key analysis of quantum key distribution," *npj Quantum Inf.*, vol. 6, p. 104, 2020.

T. C. Ralph, "Continuous variable quantum cryptography," *Phys. Rev. A*, vol. 61, p. 010303, 1999.

M. Hillery, "Quantum cryptography with squeezed states," *Physical Review A*, vol. 61, p. 022309, 2000.

M. D. Reid, "Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations," *Phys. Rev. A*, vol. 62, p. 062308, 2000.

N. J. Cerf, M. Levy, and G. Van Assche, "Quantum distribution of Gaussian keys using squeezed states," *Phys. Rev. A*, vol. 63, p. 052311, 2001.

F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, vol. 88, p. 057902, 2002.

F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using gaussian-modulated coherent states," *Nature*, vol. 421, pp. 238–241, 2003.

C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, "Quantum Cryptography Without Switching," *Phys. Rev. Lett.*, vol. 93, p. 170504, 2004.

G. Van Assche, J. Cardinal, and N. J. Cerf, "Reconciliation of a Quantum-Distributed Gaussian Key," *IEEE Trans. Inf. Theory*, vol. 50, pp. 394–400, 2004.

A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, "No-Switching Quantum Key Distribution Using Broadband Modulated Coherent Light," *Phys. Rev. Lett.*, vol. 95, p. 180503, 2005.

V. Sharma, A. M. Lance, T. Symul, C. Weedbrook, T. C. Ralph, and P. K. Lam, "A complete quantum cryptographic system using a continuous wave laser," in *Photonics: Design, Technology, and Packaging II*, vol. 6038, 2006, p. 603803.

S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, "Continuous Variable Quantum Cryptography using Two-Way Quantum Communication," *Nat. Phys.*, vol. 4, pp. 726–730, 2008.

R. Filip, "Continuous-variable quantum key distribution with noisy coherent states," *Phys. Rev. A*, vol. 77, p. 022310, 2008.

V. C. Usenko and R. Filip, "Feasibility of continuous-variable quantum key distribution with noisy coherent states," *Phys. Rev. A*, vol. 81, p. 022318, 2010.

P. Papanastasiou, C. Weedbrook, and S. Pirandola, "Continuous-variable quantum key distribution in fast fading channels," *Phys. Rev. A*, vol. 97, p. 032311, 2018.

J. Lodewyck, M. Bloch, R. Garcia-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, "Quantum key distribution over 25 km with an all-fiber continuous-variable system," *Phys. Rev. A*, vol. 76, p. 042305, 2007.

A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, "Multidimensional reconciliation for a continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 77, p. 042325, 2008.

T. Richardson and R. L. Urbanke, "Multi-edge type LDPC codes," in *Workshop honoring Prof. Bob McEliece on his 60th birthday*, Pasadena, California, 2002.

P. Jouguet, S. Kunz-Jacques, and A. Leverrier, "Long-distance continuous-variable quantum key distribution with a Gaussian modulation," *Phys. Rev. A*, vol. 84, p. 062317, 2011.

P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of continuous-variable quantum key distribution over 80 km of standard telecom fiber," in *CLEO: 2013*, 2013.

N. Hosseinidehaj and R. Malaney, "CV-MDI Quantum Key Distribution via Satellite," *Quantum Inf. Comput.*, vol. 17, pp. 361–379, 2017.

K. Günthner, I. Khan, D. Elser, B. Stiller, Ö. Bayraktar, D. T. Christian R. Müller, Karen Saucke, F. Heine, S. Seel, P. Greulich, H. Zech, B. Gütlich, S. Philipp-May, C. Marquardt, and G. Leuchs, "Quantum-limited measurements of optical signals from a geostationary satellite," *Optica*, vol. 4, pp. 611–616, 2017.

G. Zhang, J. Y. Haw, H. Cai, F. Xu, S. M. Assad, J. F. Fitzsimons, X. Zhou, Y. Zhang, S. Yu, J. Wu, W. Ser, L. C. Kwek, and A. Q. Liu, "An integrated silicon photonic chip platform for continuous-variable quantum key distribution," *Nat. Photonics*, vol. 13, pp. 839–842, 2019.

M. Zhang, P. Foshat, S. P. Khanjari, M. Imran, M. Weides, and K. Delfanazari, "Quantum Key Distribution on microwave band for superconducting quantum computing," in *35th International Symposium on Superconductivity (ISS2022)*, Nagoya, Japan, November 2021, pp. 1–6.

L. Li, T. Wang, X. Li, P. Huang, Y. Guo, L. Lu, L. Zhou, and G. Zeng, "Continuous-variable quantum key distribution with on-chip light sources," *Photonics Res.*, vol. 11, pp. 504–516, 2023.

R. Kumar, H. Qin, and R. Alléaume, "Coexistence of continuous variable QKD with intense DWDM classical channels," *New J. Phys.*, vol. 17, p. 043027, 2015.

S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nature Communications*, vol. 8, p. 15043, 2017.

A. Orieux and E. Diamanti, "Recent advances on integrated quantum communications," *J. Opt.*, vol. 18, p. 083002, 2016.

K. Kikuchi, "Fundamentals of coherent optical fiber communications," *J. Light. Technol.*, vol. 34, pp. 157–179, 2016.

S. Watanabe, R. Matsumoto, and T. Uyematsu, "Tomography increases key rates of quantum-key-distribution protocols," *Phys. Rev. A*, vol. 78, p. 042316, 2008.

R. A. Meyers, *Encyclopedia of Physical Science and Technology*, 3rd ed. Academic Press, 2002.

K. Huang, *Statistical Mechanics*. John Wiley & Sons, 1987.

A. Leverrier, F. Grosshans, and P. Grangier, "Finite-size analysis of a continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 81, p. 062343, 2010.

L. Ruppert, V. C. Usenko, and R. Filip, "Long-distance continuous-variable quantum key distribution with efficient channel estimation," *Phys. Rev. A*, vol. 90, p. 062310, 2014.

X. Wang, Y. Zhang, S. Yu, and H. Guo, "High Efficiency Postprocessing for Continuous-variable Quantum Key Distribution: Using All Raw Keys for Parameter Estimation and Key Extraction," *Quantum Inf. Process.*, vol. 18, p. 264, 2019.

M. Milisevic, "Low-Density Parity-Check Decoder Architectures for Integrated Circuits and Quantum Cryptography," Ph.D. dissertation, University of Toronto, November 2017.

C. Zhou, X. Wang, Y. Zhang, Z. Zhang, S. Yu, and H. Guo, "Continuous-Variable Quantum Key Distribution with Rateless Reconciliation Protocol," *Phys. Rev. Appl.*, vol. 12, p. 054013, 2019.

Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, "Long Distance Continuous-Variable Quantum Key Distribution over 202.81 km of Fiber," *Phys. Rev. Lett.*, vol. 125, p. 010502, 2020.

P. Jouguet, D. Elkouss, and S. Kunz-Jacques, "High Bit Rate Continuous-Variable Quantum Key Distribution," *Phys. Rev. A*, vol. 90, p. 042329, 2014.

X. Wang, Y. Zhang, S. Yu, B. Xu, Z. Li, and H. Guo, "Efficient rate-adaptive reconciliation for continuous-variable quantum key distribution," *Quantum Inf. Comput.*, vol. 17, pp. 1123–1134, 2017.

X. Wen, Q. Li, H. Mao, X. Wen, and N. Chen, "An Improved Slice Reconciliation Protocol for Continuous-Variable Quantum Key Distribution," *Entropy*, vol. 23, p. 1317, 2021.

J. Xu, Z. Zheng, and K. Tian, "Low-Density Parity-Check Codes: Research Status and Development Direction," *J. Inf. Secur.*, vol. 13, pp. 257–271, 2022.

M. Milicevic, C. Feng, L. M. Zhang, and P. G. Gulak, "Quasi-cyclic multi-edge LDPC codes for long-distance quantum cryptography," *npj Quantum Inf.*, vol. 4, p. 21, 2018.

H. Mani, T. Gehring, P. Grabenweger, C. Pacher, , and U. L. Andersen, "Multiedge-type low-density parity-check codes for continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 103, p. 062419, 2021.

K. Gümüs, T. A. Eriksson, M. Takeoka, M. Fujiwara, M. Sasaki, L. Schmalen, and A. Alvarado, "A novel error correction protocol for continuous variable quantum key distribution," *Sci. Rep.*, vol. 10, p. 10465, 2021.

T. Tsurumaru and M. Hayashi, "Dual universality of hash functions and its applications to quantum cryptography," *IEEE Trans. Inf. Theory*, vol. 59, pp. 4700–4717, 2013.

J. L. Carter and M. N. Wegman, "Universal Classes of Hash Functions," *J. Comput. Syst. Sci.*, vol. 18, pp. 143–154, 1979.

J.-Z. Huang, C. Weedbrook, Z.-Q. Yin, S. Wang, H.-W. Li, W. Chen, G.-C. Guo, and Z.-F. Han, "Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack," *Phys. Rev. A*, vol. 87, p. 062329, 2013.

X.-C. Ma, S.-H. Sun, M.-S. Jiang, and L.-M. Liang, "Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems," *Phys. Rev. A*, vol. 88, p. 022339, 2013.

H. Qin, R. Kumar, and R. Alléaume, "Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 94, p. 012325, 2016.

S. L. Braunstein and S. Pirandola, "Side-Channel-Free Quantum Key Distribution," *Phys. Rev. Lett.*, vol. 108, p. 130502, 2012.

H.-K. Lo, M. Curty, and B. Qi, "Measurement-Device-Independent Quantum Key Distribution," *Phys. Rev. Lett.*, vol. 108, p. 130503, 2012.

S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, "High-rate measurement-device-independent quantum cryptography," *Nat. Photon*, vol. 9, pp. 397–402, 2015.

C. Ottaviani, C. Lupo, R. Laurenza, and S. Pirandola, "Modular network for high-rate quantum conferencing," *Commun. Phys.*, vol. 2, p. 118, 2019.

M. Ghalaii, P. Papanastasiou, and S. Pirandola, "Composable end-to-end security of Gaussian quantum networks with untrusted nodes," 2022, https://arxiv.org/pdf/2203.11969v3.pdf.

T. Wang, P. Huang, Y. Zhou, W. Liu, H. Ma, S. Wang, and G. Zeng, "High key rate continuous-variable quantum key distribution with a real local oscillator," *Opt. Express*, vol. 26, pp. 2794–2806, 2018.

A. A. Hajomer, U. L. Andersen, and T. Gehring, "Real-world data encryption with continuous-variable measurement device-independent quantum key distribution," 2023, https://arxiv.org/pdf/2303.01611.pdf.

F. Grosshans and N. J. Cerf, "Continuous-Variable Quantum Cryptography is Secure against Non-Gaussian Attacks," *Phys. Rev. Lett.*, vol. 92, p. 047905, 2004.

A. Leverrier and P. Grangier, "Simple proof that Gaussian attacks are optimal among collective attacks against continuous-variable quantum key distribution with a Gaussian modulation," *Phys. Rev. A*, vol. 81, p. 062314, 2010.

M. Navascués, F. Grosshans, and A. Acin, "Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography," *Phys. Rev. Lett.*, vol. 97, p. 190502, 2006.

R. Garcia-Patrón and N. J. Cerf, "Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution," *Phys. Rev. Lett.*, vol. 97, p. 190503, 2006.

S. Pirandola, S. L. Braunstein, and S. Lloyd, "Characterization of collective Gaussian attacks and security of coherent-state," *Phys. Rev. Lett.*, vol. 101, p. 200504, 2008.

A. Leverrier, "Composable security proof for continuous-variable quantum key distribution with coherent states," *Phys. Rev. Lett.*, vol. 114, p. 070501, 2015.

S. Pirandola, "Limits and Security of Free-Space Quantum Communications," *Phys. Rev. Research*, vol. 3, p. 013279, 2021.

——, "Composable security for continuous variable quantum key distribution: Trust levels and practical key rates in wired and wireless networks," *Phys. Rev. Research*, vol. 3, p. 043014, 2022.

P. Papanastasiou, C. Ottaviani, and S. Pirandola, "Finite-size analysis of measurement-device-independent quantum cryptography with continuous variables," *Phys. Rev. A*, vol. 96, p. 042332, 2017.

R. Renner and J. I. Cirac, "de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography," *Phys. Rev. Lett.*, vol. 102, p. 110504, 2009.

A. Leverrier, "Security of Continuous-Variable Quantum Key Distribution via a Gaussian de Finetti Reduction," *Phys. Rev. Lett.*, vol. 118, p. 200501, 2017.

C. Weedbrook, S. Pirandola, and T. C. Ralph, "Continuous-Variable Quantum Key Distribution using Thermal States," *Phys. Rev. A*, vol. 86, p. 022318, 2012.

S. Pirandola, "Quantum discord as a resource for quantum cryptography," *Sci. Rep.*, vol. 4, p. 6956, 2014.

M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman, "Improved Low-Density Parity-Check Codes Using Irregular Graphs," *IEEE Trans. Inf. Theory*, vol. 47, pp. 585–598, 2001.

R. Renner, "Security of Quantum Key Distribution," Ph.D. dissertation, ETH, September 2005.

S. Pirandola, "Satellite quantum communications: Fundamental bounds and practical security," *Phys. Rev. Research*, vol. 3, p. 023130, 2021.

P. Papanastasiou and S. Pirandola, "Continuous-variable quantum cryptography with discrete alphabets: Composable security under collective Gaussian attacks," *Phys. Rev. Research*, vol. 3, p. 013047, 2021.

C. Lupo, "Towards practical security of continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 102, p. 022623, 2020.

N. Jain, H.-M. Chin, H. Mani, C. Lupo, D. S. Nikolic, A. Kordts, S. Pirandola, T. B. Pedersen, M. Kolb, B. Ömer, C. Pacher, T. Gehring, and U. L. Andersen, "Practical continuous-variable quantum key distribution with composable security," *Nat. Commun.*, vol. 13, p. 4740, 2022.

M. Tomamichel, "A Framework for Non-Asymptotic Quantum Information Theory," Ph.D. dissertation, ETH, March 2012.

C. Ottaviani, R. Laurenza, T. P. W. Cope, G. Spedalieri, S. L. Braunstein, and S. Pirandola, "Secret key capacity of the thermal-loss channel: Improving the lower bound," in *Proc. SPIE Quantum Inf. Sci. Technol. II*, vol. 9996, 2016, p. 999609.

P. Papanastasiou, C. Ottaviani, and S. Pirandola, "Security of continuous-variable quantum key distribution against canonical attacks," in *2021 International Conference on Computer Communications and Networks (ICCCN)*, 2021, pp. 1–6.

R. Renner, "Quantum Information Theory," https://edu.itp.phys.ethz.ch/hs15/QIT/renner_lecture_notes12.pdf, 2013.

F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, "Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security against Coherent Attacks," *Phys. Rev. Lett.*, vol. 109, p. 100502, 2012.

C. Pacher, J. Martinez-Mateo, J. Duhme, T. Gehring, and F. Furrer, "Information Reconciliation for Continuous-Variable Quantum Key Distribution using Non-Binary Low-Density Parity-Check Codes," 2016, https://arxiv.org/pdf/1602.09140.pdf.

A. Antos and I. Kontoyiannis, "Convergence properties of functional estimates for discrete distributions," *Random Struct. Algorithms*, vol. 19, pp. 163–193, 2001.

D. J. C. MacKay and R. M. Neal, "Near Shannon limit performance of low density parity check codes," *Electron. Lett.*, vol. 32, pp. 1645–1646, 1996.

M. Tomlinson, C. J. Tjhai, M. A. Ambroze, M. Ahmed, and M. Jibril, *Error-Correction Coding and Decoding*. Cham, Switzerland: Springer, 2017.

M. C. Davey and D. MacKay, "Low-density Parity Check Codes over GF(q)," *IEEE Commun. Lett.*, vol. 2, pp. 165–167, 1998.

M. Thorup, "High Speed Hashing for Integers and String," 2015, https://arxiv.org/pdf/1504.06804v9.pdf.

A. G. Mountogiannakis, P. Papanastasiou, and S. Pirandola, "Data postprocessing for the one-way heterodyne protocol under composable finite-size security," *Phys. Rev. A*, vol. 106, p. 042606, 2022.

R. M. Gray, "Toeplitz and Circulant Matrices: A Review," *Found. Trends Commun. Inf. Theory*, vol. 2, pp. 155–239, 2006.

Y.-Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J.-W. Pan, "68 Gbps quantum random number generation by measuring laser phase fluctuations," *Rev. Sci. Instrum.*, vol. 86, p. 063105, 2015.

M. Hayashi, "Exponential Decreasing Rate of Leaked Information in Universal Random Privacy Amplification," *IEEE Trans. Inf. Theory*, vol. 57, pp. 3989–4001, 2011.

B.-Y. Tang, B. Liu, Y.-P. Zhai, C.-Q. Wu, and W.-R. Yu, "High-speed and Large-scale Privacy Amplification Scheme for Quantum Key Distribution," *Sci. Rep*, vol. 9, p. 15733, 2019.

A. Venkiah, D. Declercq, and C. Poulliat, "Design of Cages with a Randomized Progressive Edge-Growth Algorithm," *IEEE Commun. Lett.*, vol. 12, pp. 301–303, 2008.

F. Steiner, G. Liva, and G. Boecherer, "Ultra-Sparse Non-Binary LDPC Codes for Probabilistic Amplitude Shaping," in *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, Singapore, December 2017, pp. 1–5.

C. Silberhorn, N. Korolkova, and G. Leuchs, "Quantum Key Distribution with Bright Entangled Beams," *Phys. Rev. Lett.*, vol. 88, p. 167902, 2002.

K. N. Wilkinson, P. Papanastasiou, C. Ottaviani, T. Gehring, and S. Pirandola, "Long-distance continuous-variable measurement-device-independent quantum key distribution with postselection," *Phys. Rev. Research*, vol. 2, p. 033424, 2020.

A. Leverrier and P. Grangier, "Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation," *Phys. Rev. Lett.*, vol. 102, p. 180504, 2009.

A. I. Fletcher and S. Pirandola, "Continuous variable measurement device independent quantum conferencing with postselection," *Sci. Rep.*, vol. 12, p. 17329, 2022.

X. Ai and R. Malaney, "Optimised Multithreaded CV-QKD Reconciliation for Global Quantum Networks," *IEEE Trans. Commun.*, vol. 70, pp. 6122–6132, 2022.

L. Barnault and D. Declercq, "Fast Decoding Algorithm for LDPC over GF(2q)," in *Proceedings 2003 IEEE Information Theory Workshop*, 2003, pp. 70–73.

C. Spagnol, W. Marnane, and E. Popovici, "FPGA Implementations of LDPC over GF(2m) Decoders," in *2007 IEEE Workshop on Signal Processing Systems*, 2007, pp. 273–278.

J. Andrade, G. Falcao, V. Silva, and K. Kasai, "FFT-SPA non-binary LDPC decoding on GPU," in *2013 IEEE International Conference on Acoustics, Speech and Signal Processing*, 2013, pp. 5099–5103.

J. B. Fraleigh, *A First Course in Abstract Algebra*, 7th ed. Boston: Addison-Wesley, 1982.

G. L. Mullen and D. Panario, *Handbook of Finite Fields*. New York: CRC Press, 2013.

C. Portmann and R. Renner, "Cryptographic security of quantum key distribution," 2014, https://arxiv.org/pdf/1409.3525.pdf.

F. Cicalese, L. Gargano, and U. Vaccaro, "Bounds on the Entropy of a Function of a Random Variable and their Applications," 2017, https://arxiv.org/pdf/1712.07906.pdf.

M. Tomamichel, *Quantum Information processing with finite resources*. Sydney, Australia: Springer, 2016.

W. F. Stinespring, "Positive Functions on C*-Algebras," *Proc. Am. Math. Soc.*, vol. 6, pp. 211–216, 1955.

MIT Open Courseware, "Statistics For Applications," https://ocw.mit.edu/courses/18-443-statistics-for-applications-fall-2006/resources/section15/, 2006.

L. Safarnejad and M.-R. Sadeghi, "FFT Based Sum-Product Algorithm for Decoding LDPC Lattices," *IEEE Commun. Lett.*, vol. 16, pp. 1504–1507, 2012.

H. Hong and Z. Sun, "An Improved Decoding Algorithm of Non binary LDPC Code," in *2011 International Conference of Information Technology, Computer Engineering and Management Sciences*, vol. 3, Nanjing, China, September 2011, pp. 104–107.