EXPERIMENTAL ANALYSIS OF EINSTEIN-PODOLSKY-ROSEN STEERING FOR QUANTUM INFORMATION APPLICATIONS

Von der QUEST-Leibniz-Forschungsschule
der Gottfried Wilhelm Leibniz Universität Hannover
zur Erlangung des Grades

Doktor der Naturwissenschaften
- Dr. rer. nat. -

genehmigte Dissertation

von
DIPL.-PHYS. VITUS HÄNDCHEN

2016

Referent :	Prof. Dr. rer. nat. Roman Schnabel
	Institut für Laserphysik, Hamburg
Korreferent :	Prof. Dr. rer. nat. Reinhard F. Werner
	Institut für Theoretische Physik, Hannover
Tag der Promotion :	04.03.2016

ABSTRACT

The first description of quantum steering goes back to Schrödinger. In 1935 he named it a necessary and indispensable feature of quantum mechanics in response to Einstein's concerns about the completeness of quantum theory. In recent years investigations of the effect have experienced a revival, as it turned out that steering is a distinct subclass of entanglement. It is strictly stronger than genuine entanglement, meaning that all steerable states are entangled but not vice versa, and strictly weaker than the violation of Bell inequalities. Additionally, the violation of a steering inequality has an intrinsic asymmetry due to the directional construction. One party seemingly steers the other and their roles are in general not interchangeable. The first direct observation of this asymmetry is presented in this thesis. It was demonstrated that certain Gaussian quantum optical states show steering from one party to the other but not in the opposite direction. This is a profound result, as the experiment proves that the class of steerable states itself divides into distinct subclasses.

Furthermore, steering found major applications in quantum information. For example in the field of quantum key distribution (QKD) the non-classical correlations can be exploited to establish a secret, cryptographic key. Thereby, steering allows one-sided device independent security, since it violates a description with certain classical models. This thesis reports on the final results of the QKD project at the Leibniz University Hannover that aimed at the generation of a secure quantum key based on mutually entangled conjugate pairs of continuous variables. The protocol of a recent security proof was implemented in a table-top setup and nearly 100 MBit of usable key with composable and one-sided device independent security against coherent attacks were generated. The security analysis included finite size effects, and a newly developed hybrid reconciliation algorithm was used for efficient error correction. Furthermore, a loss study on the entanglement distribution showed that separation of the two detectors by a 5 km optical fibre would be possible. Therefore, the results of this work are a major step towards continuous variable QKD with state-of-the-art security in local area networks.

Key words: steering, squeezed light, quantum key distribution

KURZFASSUNG

Die erste Beschreibung von Quanten-Steering (z.dt. Quantenlenkung) geht auf Schrödinger zurück. Im Jahr 1935 nannte er es ein notwendiges und unverzichtbares Merkmal der Quantenmechanik in Antwort auf Einsteins Bedenken bezüglich der Vollständigkeit der Quantentheorie. In den letzten Jahren erlebten die Untersuchungen des Effekts einen Aufschwung, da es sich herausstellte, dass Steering eine ausgeprägte Unterklasse der Verschränkung darstellt. Es ist strikt stärker als originäre Verschränkung, d.h. alle Steering Zustände sind verschränkt aber nicht umgekehrt, und strinkt schwächer als die Verletzung Bellscher Ungleichungen. Zusätzlich hat die Verletzung einer Steering Ungleichung eine intrinsische Asymmetrie aufgrund der richtungsabhängigen Konstruktion. Eine Partei lenkt scheinbar die andere und ihre Rollen sind im Allgemeinen nicht vertauschbar. In dieser Arbeit wird die erste direkte Beobachtung dieser Asymmetrie präsentiert. Es wurde gezeigt, dass bestimmte Gaußsche Zustände in der Quantenoptik Steering von einer Partei zur anderen aufweisen, aber nicht in umgekehrter Richtung. Dies ist ein tiefgreifendes Resultat, da das Experiment beweist, dass sich die Klasse der Steering Zustände selbst in unterscheidbare Unterklassen aufteilt.

Darüber hinaus hat Steering wichtige Anwendungen in der Quanteninformation gefunden. Zum Beispiel können im Bereich der Quantenschlüsselverteilung (QKD) die nicht-klassischen Korrelationen ausgenutzt werden um einen geheimen, kryptographischen Schlüssel zu erzeugen. Dabei erlaubt Steering die einseitige Geräteunabhängigkeit der Sicherheit, da es die Beschreibung durch bestimmte klassische Modelle verletzt. In dieser Arbeit werden die finalen Ergebnisse des QKD Projekts an der Leibniz Universität Hannover vorgestellt, welches die Erzeugung eines sicheren Quantenschlüssels auf Basis gemeinsam verschränkter, konjugierter Paare kontinuierlicher Variablen zum Ziel hatte. Das Protokoll eines aktuellen Sicherheitsbeweises wurde in einem Tischaufbau umgesetzt und fast 100 MBit verwendbarer Schlüssel mit zusammensetzbarer und einseitig geräteunabhängiger Sicherheit gegen kohärente Angriffe wurden erzeugt. Die Sicherheitsanalyse schloss Effekte der endlichen Größe des Schlüssels mit ein und ein neu entwickelter, hybrider Abgleichalgorithmus wurde zur effizienten Fehlerkorrektur verwendet. Des Weiteren zeigte eine Verluststudie an der Verschränkungsverteilung, dass eine Separierung der beiden Detektoren durch 5 km Glasfaserkabel möglich wäre. Die Ergebnisse dieser Arbeit sind daher ein bedeutender Schritt für die Anwendung von QKD mit kontinuierlichen Variablen und modernster Sicherheit in lokalen Netzwerken.

Schlagworte: Quantenlenkung, gequetschtes Licht, Quantenschlüsselverteilung

CONTENTS

ABSTRACT iii

KURZFASSUNG v

LIST OF FIGURES x

LIST OF ACRONYMS xi

1 INTRODUCTION 1

2 QUANTUM OPTICS 5
- 2.1 Foundations of Quantum Mechanics 5
  - 2.1.1 Planck's Law and the Photo-Electric Effect 5
  - 2.1.2 Description and Interpretation of Quantum States 7
  - 2.1.3 Heisenberg's Uncertainty Principle 11
- 2.2 Quantization of the Electromagnetic Field 14
  - 2.2.1 The Classical Electromagnetic Field 14
  - 2.2.2 The Quantum-Mechanical Harmonic Oscillator 16
- 2.3 Hilbert Spaces for the Description of Light 18
  - 2.3.1 Number States 18
  - 2.3.2 Coherent States 21
  - 2.3.3 Squeezed States 24
- 2.4 The Quadrature Phase Space 30
  - 2.4.1 Quadrature Operators 30
  - 2.4.2 Statistical Moments and the Covariance Matrix 34
  - 2.4.3 Properties of the Covariance Matrix for Physical States 39

3 DETECTION OF OPTICAL QUANTUM STATES 43
- 3.1 Gaussian Optics 43
  - 3.1.1 Fundamental Solution of the Helmholtz Equation 43
  - 3.1.2 Higher Order Transversal Modes 44
  - 3.1.3 Implications for Experiments 45
- 3.2 Mixing of Different Modes 48
  - 3.2.1 The Classical Beam Splitter 48
  - 3.2.2 The Quantum Optical Beam Splitter 49
  - 3.2.3 Symplectic Beam Splitter Transformations 49
- 3.3 Balanced Homodyne Detection 50
  - 3.3.1 Description of the Fields at the Homodyne Beam Splitter 51
  - 3.3.2 Detection of Quadrature Amplitudes 52

- 3.4 Expectation Values and Variances of Homodyne Signals 54
  - 3.4.1 Measurement on the Vacuum State 54
  - 3.4.2 Measurement on the Squeezed Vacuum State 55
  - 3.4.3 Measurement on the Coherent State 58
- 3.5 Reconstruction of the Covariance Matrix 60

4 THE NOTION OF ENTANGLEMENT 63
- 4.1 The Einstein-Podolsky-Rosen Paradox 63
- 4.2 Classification of Entanglement 65
  - 4.2.1 Genuine Entanglement 65
  - 4.2.2 Violation of a Bell Inequality 66
  - 4.2.3 Einstein-Podolsky-Rosen Steering 68
- 4.3 Directionality of Gaussian Steering 70
- 4.4 Two-Mode Squeezed States and the EPR-Reid Criterion 73

5 DEMONSTRATION OF ONE-WAY EINSTEIN-PODOLSKY-ROSEN STEERING 81
- 5.1 Experimental Preliminaries 81
  - 5.1.1 Generation of Squeezed States 81
  - 5.1.2 Generation of Two-Mode Squeezed States 85
- 5.2 Demonstration of One-Way Steering 87
- 5.3 Connection to Other Entanglement Applications 89
  - 5.3.1 Tripartite and Multipartite Steering 89
  - 5.3.2 Entanglement Distribution by Separable States 91
  - 5.3.3 Data Reconciliation in Quantum Key Distribution 91

6 APPLICATION OF TWO-MODE SQUEEZED STATES FOR QKD 93
- 6.1 A Brief Introduction to QKD 93
  - 6.1.1 Classification of QKD Schemes 95
  - 6.1.2 The Continuous Variable QKD Project at the Leibniz University Hannover 97
- 6.2 CV-QKD with 1sDI Security Against Coherent Attacks 98
  - 6.2.1 The QKD Protocol 99
  - 6.2.2 Implementation of the Protocol 102
  - 6.2.3 Secret Key Distribution Results 108
- 6.3 Implementation of a 1 km Fiber Based Quantum Channel 111
  - 6.3.1 Concepts for a Remote Homodyne Detector 112
  - 6.3.2 Scheme for Dynamic Polarization Control 114
  - 6.3.3 Distribution of a Squeezed Field Through a 1 km Fiber 118
  - 6.3.4 Distribution of Entanglement Through a 1 km Fiber 121

7 CONCLUSION AND PROSPECT 125

A MATHEMATICAL AND COMPUTATIONAL DETAILS 129
- A.1 Influence of the Electronic Demodulation Phase on the Homodyne Signals 129
- A.2 Derivation of Analytic Functions for Gaussian Steering 130
- A.3 Mathematica Notebook to Investigate the DPC 131

BIBLIOGRAPHY 141

CURICULUM VITAE 157

LIST OF PUBLICATIONS 159

LIST OF FIGURES

Figure 2.1 Coherent state in the quadrature phase space 32
Figure 2.2 Squeezed state in the quadrature phase space 33
Figure 3.1 Intensity distribution of a Ψ_{12} Hermite-Gaussian mode 45
Figure 3.2 Intensity distribution of a Ψ_{22} Laguerre-Gaussian mode 46
Figure 3.3 Schematic of a generic mode matching setup 47
Figure 3.4 Schematic of a balanced homodyne detector 50
Figure 4.1 Implications of inseparability criteria 71
Figure 4.2 Gaussian one-way EPR steering visualized in phase space 72
Figure 4.3 Quadrature correlations of a two-mode squeezed state 77
Figure 5.1 Energy levels of parametric down-conversion 82
Figure 5.2 Schematic of a squeezed-light source 83
Figure 5.3 Measurement of squeezing for varying pump power 85
Figure 5.4 Schematic of the experimental setup for the generation of v-class entanglement 86
Figure 5.5 Comparison of the EPR-Reid criterion for s-class and v-class entanglement 87
Figure 5.6 Schematic of the experimental setup for the demonstration of one-way steering 88
Figure 5.7 Certification of one-way steering 90
Figure 6.1 Schematic of the squeezed-light source stabilization 103
Figure 6.2 Schematic of the entanglement phase lock 104
Figure 6.3 Schematic of the homodyne detection 105
Figure 6.4 Schematic of the QKD setup 106
Figure 6.5 Estimation of phase noise at Alice's detector 108
Figure 6.6 Secret key rate versus number of recorded samples 109
Figure 6.7 Secret key length versus transmission loss 110
Figure 6.8 Concept for a remote detector with copropagating local oscillator 112
Figure 6.9 Concept for a remote detector with local oscillator from a local laser 113
Figure 6.10 Schematic of the polarimeter 116
Figure 6.11 Noise measurement at the remote detector for different LO powers 119

Figure 6.12 Investigation of the linearity of the homodyne detector at low LO powers 120
Figure 6.13 Measurement of squeezing after 1 km of fiber for varying pump power 121
Figure 6.14 Measurement of s-class entanglement after 1 km of fiber 123

LIST OF ACRONYMS

1sDI	One-Sided Device Independent
AC	Alternating Current
AOM	Acousto-Optical Modulator
AR	Anti-Reflectivity
BCH	Baker-Campbell-Hausdorff (Theorem)
BHD	Balanced Homodyne Detection
CPU	Central Processing Unit
CV	Continuous Variables
cw	Continuous-Wave
DC	Direct Current
DPC	Dynamic Polarization Controller
DV	Discrete Variables
EDS	Entanglement Distribution by Separable States
EOM	Electro-Optical Modulator
EPR	Einstein-Podolsky-Rosen
fcEOM	Fiber-Coupled EOM
FSR	Free Spectral Range
GW	Gravitational Wave
HR	High Reflectivity
LDPC	Low Density Parity Check
LO	Local Oscillator

PBS	Polarizing Beam Splitter
PDH	Pound-Drever-Hall (Locking Technique)
PID	Proportional-Integral-Derivative (Controller)
PPKTP	Periodically Poled Potassium Titanyl Phosphate
PS	Phase Shifter
PZT	Piezo-Electric Transducer
QKD	Quantum Key Distribution
roc	Radius of Curvature
SSB	Single Sideband

1

INTRODUCTION

Quantum mechanics is one of the most successful physical theories. Established in the 1920s, it paved the way for many technological developments throughout the 20th century. At the root of many quantum effects is a phenomenon called *entanglement*. Roughly speaking it concerns correlations between two or more subsystems that are stronger than the statistical description of the measurements would allow. Where in the early days this *paradox* gave the leading developers of quantum theory quite a headache and lead to intense philosophical discussion, nowadays it is experimentally proven and accepted and seen as resource for quantum technologies.

On the one hand, entanglement finds applications in the field of quantum metrology, the measurement of observables at the quantum limit given by the Heisenberg Uncertainty Principle. Here, the sophisticated usage of entangled states can allow a higher precision in the determination of the desired observable than Heisenberg's uncertainty would allow. A famous example is the enhancement of the sensitivity of gravitational wave (GW) detectors with *squeezed* states of laser light (these are states with entangled upper and lower sidebands). Proposed already in 1981 [Cav81], it was successfully implemented in 2010 at GEO600, the km scale Michelson-type laser interferometer near Hannover/Germany [LSC11]. The sensitivity was significantly increased and squeezing became a key resource for all future upgrades and new developments of ground based GW detectors [Sna10, LSC13, Oel14]. Furthermore, many applications were developed in recent years, from the use of quadrature-entangled light as a veto channel for stray light signals in interferometers (quantum dense metrology) to the enhancement of the tracking of lipid granules in living yeast cells [Ste13, Tay13]. And with future technological developments, like efficient cryogenic cooling or low-loss optical components, the versatility of entanglement as a measurement enhancer will most likely even grow further.

On the other hand, the non-classical correlations cry out for an application in quantum information [Bra05]. The most prominent example might be the field of quantum key distribution (QKD), which aims at the establishment of secure communication based on quantum physical principles [vAs06]. Here, the application of entangled states initiated a series of new security proofs and protocols [Eke91, Urs07, Su09, Mad12, Fur12]. Thereby, not only the correlations can be used to generate a secure and symmetric key but the non-classicality of these correlations also allow the security to be independent of the implementation with macroscopic (hence classical) devices. Roughly speaking, an adversary trying to exploit implementation side channels would fail, as they could not forge the non-classical statistics. Furthermore, entanglement is also a key resource to solve problems arising from real world implementation of QKD, as it finds applications in quantum memories [Koz00, Jul04], quantum repeaters [Bri98, Dua01] or the super-activation of communication channels [Hor99, Smi11]. Related to these, but not restricted to QKD applications, are the areas of quantum teleportation [Ben93, Vai94, Bou97, Bra98], entanglement swapping [Tan99, Jia04] and distillation [Fiu07, Hag08, Don08]. And last but not least, the quantum computer relies on entanglement [Bri99]. This machine, its development currently making large progress, operates with only a few quanta well-shielded from the environment, which enables the formation of a multiply entangled state containing the computation. With its successful implementation it will open a whole new universe to computer science.

From the various and demanding applications of entangled states the field of *quantum engineering* emerged. The states do not only have to be generated and verified by an appropriate measurement, but they have to be producible on demand, they have to be controllable on fairly arbitrary time scales, and all processes necessary for their generation have to be thoroughly understood to allow the flawless implementation in connection with other technologies. Therefore, the generation and stable control of specific quantum states is not only of fundamental physical interest but also has implications for possible future applications and technologies.

In this thesis entanglement engineering was performed in two different but connected experiments. In the first one, the existence of a new class of entanglement, the *one-way steering*, could be experimentally demonstrated. Steering occurs in certain entangled states where a measurement on one subsystem seemingly steers the other subsystem (or in the multi-mode case several other subsystems) into a specific (pure) state. The one-way steerable states now show this effect only from one subsystem to the other but not vice versa, thereby demonstrating a new counterintuitive feature of entanglement. The effect was demonstrated with high statistical significance and in accordance with the theoretical description. In the second experiment, two-way steering was generated and applied for QKD with continuous variables in a table top experiment. The strong non-classical correlations enabled composable security against the most general coherent attacks. The security analysis also included effects emerging from the finite precision of the measurement statistics due to a finite number of measurement samples. Therefore, the system incorporated state-of-the-art quantum information theory and demonstrated the highest level of security that is currently possible with continuous variables. Furthermore, the presence of steering allowed the demonstration of *one-sided* device independent security. This means the security of the key distribution protocol is robust against implementation side channel attacks on the remote party, if we define the local party as the one that possesses the steering source. Additionally, a loss study on the system was conducted. The results suggest that a separation of the two parties by approximately 5 km standard optical fiber would be possible and with the inclusion of reverse reconciliation the range could be extended to 16 km. Thus, it demonstrates that entanglement based continuous variable QKD in local area networks is feasible. Finally, experimental investigations on the implementation of such a fiber link were made. The distribution of squeezed and entangled states through 1 km single mode fiber was successfully demonstrated. Nevertheless, the achieved level on non-classicality was not sufficient to employ it in the QKD protocol. The observed problems were studied in detail and found to be based on technical limitations that should be overcome by future developments.

STRUCTURE OF THIS THESIS

This thesis is divided into seven chapters: Following the introduction, Chapter 2 gives an overview of quantum mechanics and in particular of quantum optics. Chapter 3 is dedicated to the detection of continuous variable quantum systems with homodyne detection and explains what signals can be expected from the most important states used in this thesis. Chapter 4 provides a thorough description of entanglement and gives the theoretical background of one-way steering. Chapter 5 then introduces the key components of the experiments conducted in the framework of this thesis and presents the results of the one-way steering generation. In Chapter 6 the results of the QKD experiments are presented together with the required technical enhancements of the setup and the studies on the fiber transmission. All results are summarized in Chapter 7 together with future prospects of the findings.

2

QUANTUM OPTICS

2.1 FOUNDATIONS OF QUANTUM MECHANICS

2.1.1 *Planck's Law and the Photo-Electric Effect*

By the end of the 19th century an unsolved problem in physics was a consistent description of the so-called blackbody radiation. A blackbody can in good approximation be described by a tiny hole in a box that is blackened inside. On the one hand the walls then perfectly absorb any electromagnetic radiation contained in the box. On the other hand the walls will emit radiation depending on their absolute temperature. After giving the system enough time, the field in the cavity formed by the box will have reached thermal equilibrium. The theory of classical statistical mechanics demands that on the one hand the energy in each mode will follow the exponential Boltzmann distribution depending on the temperature. But on the other hand it follows from the equipartition theorem that in each mode the same amount of energy is contained. As no upper limit to the frequency of the modes is given this would result in an infinite amount of energy in the box, if summing over all modes, which is known as the *ultraviolet catastrophe*. Obviously this can not be true as the energy in the box should always be bounded.

The situation was resolved in 1900 in a publication by Max Planck [Pla00]. He suggested that the energy of the electromagnetic field in each mode was quantized, i.e. only discrete portions of energy could be absorbed or emitted at a time. The connection he proposed was simply linear, $E = \hbar\omega$, where ω is the angular frequency and $\hbar$ a fairly small but non-zero constant, which is the same for any mode and is nowadays known as the *quantum of action* or simply *Planck's constant*. The resulting distribution of energy over the frequencies of the modes showed the same behavior for low frequencies as the classical theory but predicted a rapid drop-off at high frequencies. By choosing the value for Planck's constant appropriately it was possible to actually match the theoretical spectral distribution of energy to the experimental observations. It can even be generalized to large scales and the spectrum of our sun can (up to some tiny quantum effects) perfectly be described by Planck's radiation formula if a surface temperature of about 5500 K is assumed.

While it seems that Planck himself thought the quantization was an effect of the atoms that form the walls of the box, in 1905 Albert Einstein gave the story a new twist and showed that the quantization was inherent to the electromagnetic field itself. By using Planck's quantization postulate he was able to explain the hitherto mysterious photoelectric effect [Ein05]. In this experiment, light was shone at a metal plate and the energy of the liberated electrons was investigated. With the classical theory of light one would have expected that the energy of the electrons increases if the intensity of the light was increased. But on the contrary it was observed that the energy of each electron stayed exactly the same no matter how much light was used and only the number of electrons that were liberated was changed. This becomes immediately reasonable if we assume the light to be quantized in what we nowadays call *photons*. Each photon has a certain probability of liberating an electron, thereby transmitting its energy. Some of the energy will be required to ionize the electron from its atom, the rest will be kinetic energy that can be experimentally measured. If now the intensity of the light is increased, more photons will hit the metal plate and the overall probability of electrons being liberated will increase. But each single electron still only absorbs the energy of one photon. The effect can be shown even more dramatically if monochromatic light is used. If the frequency of the light is small such that $\hbar\omega$ is smaller than the ionization energy for a single electron, no electrons will be liberated at all, no matter how intense the light is made.

Although from a classical point of view this was completely unintuitive and maybe even unreasonable, the seminal success in explaining these fundamental effects gave the theory of quantum mechanics its foundation and was soon accepted as the only possible way to describe the universe at the smallest scale. Nevertheless, it came with great controversy especially in its (philosophical) interpretation. To point this out let us have a look at what is called *wave-particle duality*. The findings by Planck and Einstein proposed that light actually consists of particles. This is in great contrast to the classical theory of light being a wave, as manifested in many interference experiments. Now one might think of conceiving such an experiment with no more than one photon at a time. Under the classical assumption of a particle the interference pattern (or whatever is observed with a classical wave) would have to vanish. But on the contrary the pattern still arises, it just takes quite a while as only one photon at a time hits the screen or the detector. Hence, one might say "each photon is interfering with itself", or even "light is simultaneously both, wave AND particle". The same is true with what is classically considered a particle, for example an electron. It will behave like a wave if we just look closely enough but still a single electron will always be detected as a single electron and never be "smeared" over the range of an interference pattern.

To solve this duality Erwin Schrödinger introduced the wave function to describe the evolution of a quantum system, although he might not have thought of it this way himself. This function ψ is a solution to the Schrödinger equation

$$\frac{d\psi}{dt} = \frac{1}{i\hbar}\hat{H}\psi, \tag{2.1}$$

where $\hat{H}$ is the Hamilton operator of the system (see next section). This equation has similarities to a classical wave equation which explains the wave character of its solutions. The particle aspect on the other hand arises from the interpretation of the wave function as a *probability amplitude* for the state of the system. This means the absolute square of ψ will describe the probability density for finding the system in any of its possible states, thereby, loosing all wave-like aspects contained in its complex argument. Hence, the wave function does not give an explicit description of the system of the form "at time t it will be at position x" but it contains all possible results of a measurement with its respective probabilities. By measuring a property of a quantum system one of these possibilities will be realized and only by repeating the experiment with many systems all prepared in the same way the probability distribution will be regained. This can be summarized in the statement that quantum mechanics is a statistical theory. It makes no predictions for the single measurement, since there is no way of predicting it.

2.1.2 *Description and Interpretation of Quantum States*

Before we can go into detailed descriptions of quantum optics we will revisit some fundamental mathematical definitions and propositions. We will just state the most relevant properties, a very good introduction including the mathematical subtleties can be found in [Hal13].

In classical analytic mechanics the state of a physical system is described by vectors on a phase space, for example (x, p) being the position and the momentum of a particle. In quantum mechanics the state is described by a unit vector $|\psi\rangle$ on a Hilbert space $\mathcal{H}$. The states are actually rays on $\mathcal{H}$, as $|\psi'\rangle = c|\psi\rangle$ for some $c \in \mathbb{C}$ represents the same physical state. Even the restriction to normalized vectors ($|c|^2 = 1$) leaves an infinite number of possible representations. Furthermore, the Hilbert space will normally be the space of square integrable functions on $\mathbb{R}$, $L^2(\mathbb{R})$. But in many cases it does not have to be specified, just the commutation relations of the observables of interest (see further down) will be given and $\mathcal{H}$ is assumed to be an irreducible representation of those relations.

The state vector $|\psi\rangle$ can be related to the previously mentioned wave function ψ by taking the inner product of it with an eigenstate of the desired variable of the wave function, and thus we will use them interchangeably. For example for the position we have

$$\psi(x) = \langle x|\psi\rangle.$$

Here, the brackets denote the sesquilinear inner product of the Hilbert space of the *ket* vector $|\psi\rangle$ and an adjoint *bra* vector $\langle\varphi|$,

$$\begin{aligned}\langle\varphi|\lambda\psi\rangle &= \lambda\langle\varphi|\psi\rangle,\\ \langle\lambda\varphi|\psi\rangle &= \lambda^*\langle\varphi|\psi\rangle.\end{aligned}$$

If a system can be fully described by a state $|\psi\rangle$ it is called a *pure* state. To investigate physical properties of such a state we define observables to be operators on the associated Hilbert space in analogy to functions on the classical phase space. These operators act on the states similar to matrices on vectors. For each operator $\hat{A}$ there is a unique adjoint operator $\hat{A}^\dagger$,

$$\langle\varphi|\hat{A}\psi\rangle = \langle\hat{A}^\dagger\varphi|\psi\rangle.$$

The expectation value of $\hat{A}$ with respect to the state $|\psi\rangle$ is given by

$$\mathrm{Exp}(\hat{A}) = \langle\psi|\hat{A}\psi\rangle =: \langle\hat{A}\rangle_\psi,$$

and similarly all higher moments of $\hat{A}$

$$\mathrm{Exp}(\hat{A}^n) = \langle\hat{A}^n\rangle_\psi.$$

As we will see in Section 2.4.2, these moments completely define the statistical properties of $|\psi\rangle$ under measurement of $\hat{A}$.

Now suppose $|\psi\rangle$ is an eigenvector of $\hat{A}$ (we will call this an eigenstate). Then we have

$$\hat{A}|\psi\rangle = \lambda|\psi\rangle,$$

with λ the corresponding eigenvalue. Hence, if $|\psi\rangle$ is normalized, that is $\langle\psi|\psi\rangle = 1$, we obtain for the expectation value

$$\begin{aligned}\langle\psi|\hat{A}\psi\rangle &= \lambda\langle\psi|\psi\rangle\\ &= \lambda.\end{aligned}$$

As this eigenvalue describes a physically measurable quantity, it should be real. Therefore, to represent a meaningful observable, $\hat{A}$ is required to be self-adjoint or *Hermitian* [Hal13],

$$\hat{A}^\dagger = \hat{A}.$$

Using the eigenvalue relation we can write an arbitrary vector $|\varphi\rangle$ in the eigenbasis $\{|\psi_k\rangle\}$ of an operator $\hat{A}$,

$$|\varphi\rangle = \sum_k a_k |\psi_k\rangle.$$

Note that the basis can, in principle, contain infinitely many elements, so the expansion can be an infinite series. The factors a_k are the probability amplitudes to find $|\varphi\rangle$ in the state $|\psi_k\rangle$, or in other terms, the probability to measure the classical observable A to be λ_k is

$$P(A = \lambda_k) = |a_k|^2.$$

A more general description of a quantum state is in terms of the density operator,

$$\begin{aligned} \hat{\rho}_\varphi &= \sum_k |a_k|^2 |\psi_k\rangle\langle\psi_k| \\ &= \sum_{k,l} |\psi_k\rangle \rho_{kl} \langle\psi_l|. \end{aligned}$$

Here ρ_{kl} is the density matrix with the probabilities $|a_k|^2$ on the diagonal. Hence, for consistency we have the requirement

$$\mathrm{tr}(\hat{\rho}) \overset{!}{=} 1.$$

Furthermore, it can be proven that $\mathrm{tr}(\hat{\rho}^2) \leqslant \mathrm{tr}(\hat{\rho})$ and that the density operator describes a pure state if and only if $\mathrm{tr}(\hat{\rho}^2) = 1$ [Nieoo]. With the density operator we can describe mixed states and rewrite the expectation value of the operator $\hat{A}$ as

$$\langle\hat{A}\rangle_\varphi = \mathrm{tr}(\hat{\rho}_\varphi \hat{A}).$$

We know from classical Hamilton mechanics that the Hamiltonian contains all physically relevant features to describe the evolution of a system. In analogy to this we define the Hamilton operator $\hat{H}$ to develop the evolution of quantum systems. As the Hamiltonian gives the energy of the system the eigenstates of the Hamilton operator are energy eigenstates, i.e. states with a definite energy,

$$\hat{H}|\psi\rangle = E_\psi |\psi\rangle.$$

This is also known as the time-independent Schrödinger equation. We will now give a rough idea of the time evolution of quantum systems. As we assume the state to have a wave-like behavior we will multiply it by a complex phase $\exp(-i\omega t)$. Furthermore, we have seen in the previous section that the energy is connected to the temporal frequency ω via $\hbar$. Therefore, if $|\psi_0\rangle$ is an energy eigen state it should evolve in time like

$$\psi(t) = e^{-i\omega t}\psi_0 = e^{-iEt/\hbar}\psi_0.$$

Note that we have decided to take the temporal exponent with a negative sign. We will, therefore, later choose the spatial exponent with a positive sign. This has the nice consequence that the solutions of our differential equations will move to the right in a standard coordinate system. Taking the time derivative of this equation we find

$$\frac{d\psi(t)}{dt} = \frac{E}{i\hbar}\psi(t),$$

and together with the time-independent Schrödinger equation and the conservation of energy we get

$$i\hbar\frac{d\psi(t)}{dt} = \hat{H}\psi(t).$$

This is the time-dependent Schrödinger equation, as we have seen it in the previous section in Equation (2.1). The statement is that all states of any quantum system have to evolve in time following this equation.

With the Schrödinger equation we can have a look at the time evolution of expectation values. If we take the time derivative of $\langle\hat{A}\rangle_\psi$ we find

$$\begin{aligned}\frac{d}{dt}\langle\psi(t)|\hat{A}\psi(t)\rangle &= \left\langle \frac{d\psi(t)}{dt}\middle| \hat{A}\psi(t)\right\rangle + \left\langle \psi(t)\middle|\hat{A}\frac{d\psi(t)}{dt}\right\rangle \\ &= \left\langle \frac{\hat{H}\psi(t)}{i\hbar}\middle| \hat{A}\psi(t)\right\rangle + \left\langle \psi(t)\middle|\hat{A}\frac{\hat{H}\psi(t)}{i\hbar}\right\rangle \\ &= \frac{1}{i\hbar}\left\langle\psi(t)\left|\hat{A}\hat{H} - \hat{H}\hat{A}\right|\psi(t)\right\rangle \\ &= \frac{1}{i\hbar}\left\langle\psi(t)\left|[\hat{A},\hat{H}]\right|\psi(t)\right\rangle,\end{aligned}$$

where in the last line we have introduced the commutator of two operators,

$$[\hat{A},\hat{B}] = \hat{A}\hat{B} - \hat{B}\hat{A}.$$

In comparison to classical Hamilton mechanics the commutator can be seen, as taking the role of the Poisson bracket. It is interesting to note that the time derivative vanishes if the operator $\hat{A}$ commutes with the Hamilton operator. Slightly informally, we could say that things change in time (so something is happening at all) because some observables do NOT commute with the Hamilton operator.

The previous derivation of the time evolution is called the Schrödinger picture. It assumes that the time evolution takes place only in the quantum states and the operators are constant. An alternative way is to use the so-called Heisenberg picture. Let us replace the energy in the time evolution of the state by the Hamilton operator,

$$e^{-iEt/\hbar}\psi_0 = e^{-i\hat{H}t/\hbar}\psi_0.$$

That we may do so can be proven by the spectral theorem of operator algebra and also by the fact that the right hand side obviously is a solution of the Schrödinger equation (at least as long as $\hat{H}$ is well behaved enough). Now starting from the time dependent expectation value we find

$$\begin{aligned}\langle\psi(t)|\hat{A}\psi(t)\rangle &= \left\langle e^{-i\hat{H}t/\hbar}\psi_0\middle|\,\hat{A}\,\middle|e^{-i\hat{H}t/\hbar}\psi_0\right\rangle \\ &= \left\langle\psi_0\middle|e^{i\hat{H}t/\hbar}\hat{A}e^{-i\hat{H}t/\hbar}\middle|\psi_0\right\rangle \\ &= \langle\hat{A}(t)\rangle_{\psi_0},\end{aligned}$$

Hence, we have found the time dependence of an operator to be

$$\hat{A}(t) = e^{i\hat{H}t/\hbar}\hat{A}e^{-i\hat{H}t/\hbar},$$

Furthermore, we have defined a unitary time evolution operator,

$$\hat{U}(t) := e^{-i\hat{H}t/\hbar},$$

where unitarity means that $\hat{U}(t)\hat{U}^\dagger(t) = \mathbb{1}$. For the time derivative of the now time dependent operator $\hat{A}$ we find by a similar calculation as for the expectation value in the Schrödinger picture

$$\frac{d\hat{A}(t)}{dt} = \frac{1}{i\hbar}[\hat{A}(t), \hat{H}],$$

which is a very similar result. Note that the Hamilton operator will always commute with itself, hence, also in the Heisenberg picture it does not become time dependent. Thus, both pictures have proven to be possible descriptions of the time evolution of quantum states and we can make use of one or the other depending on which is more convenient in the respective case.

2.1.3 *Heisenberg's Uncertainty Principle*

Another consequence of the non-commutativity of certain operators is that the associated observables can not be simultaneously determined with arbitrary precision. The uncertainty of a measurement observable with respect to a quantum state is defined as the square root of the centralized second moment (see Section 2.4.2),

$$\Delta_\psi \hat{A} := \sqrt{\left\langle (\hat{A} - \langle \hat{A} \rangle_\psi)^2 \right\rangle_\psi}.$$

Let us define the operators $\hat{A}' := \hat{A} - \langle \psi | \hat{A} \psi \rangle$ and $\hat{B}' := \hat{B} - \langle \psi | \hat{B} \psi \rangle$. Now we take a look at the product of the squared uncertainties of the operators $\hat{A}$ and $\hat{B}$,

$$\begin{aligned}
\Delta^2_\psi \hat{A} \Delta^2_\psi \hat{B} &= \langle \psi | \hat{A}'^2 \psi \rangle \langle \psi | \hat{B}'^2 \psi \rangle \\
&= \langle \hat{A}' \psi | \hat{A}' \psi \rangle \langle \hat{B}' \psi | \hat{B}' \psi \rangle \\
&\geqslant |\langle \hat{A}' \psi | \hat{B}' \psi \rangle|^2 \\
&\geqslant |\mathrm{Im} \langle \hat{A}' \psi | \hat{B}' \psi \rangle|^2 \\
&= \frac{1}{4} |\langle \hat{A}' \psi | \hat{B}' \psi \rangle - \langle \hat{B}' \psi | \hat{A}' \psi \rangle|^2 \\
&= \frac{1}{4} |\langle [\hat{A}', \hat{B}'] \rangle_\psi|^2,
\end{aligned}$$

where in the second line we have used that $\hat{A}'$ and $\hat{B}'$ are Hermitian, in the third line we applied the Cauchy-Schwarz inequality, $|a|^2 |b|^2 \geqslant |ab|^2$, and in the fourth line we made use of the fact that the absolute value of a number is definitely larger than or equal to the absolute value of its imaginary part. The commutator of $\hat{A}'$ and $\hat{B}'$ in the last line can be evaluated to

$$\begin{aligned}
[\hat{A}', \hat{B}'] &= (\hat{A} - \langle \hat{A} \rangle_\psi)(\hat{B} - \langle \hat{B} \rangle_\psi) - (\hat{B} - \langle \hat{B} \rangle_\psi)(\hat{A} - \langle \hat{A} \rangle_\psi) \\
&= \hat{A}\hat{B} - \hat{A} \langle \hat{B} \rangle_\psi - \langle \hat{A} \rangle_\psi \hat{B} + \langle \hat{A} \rangle_\psi \langle \hat{B} \rangle_\psi \\
&\qquad - \hat{B}\hat{A} + \hat{B} \langle \hat{A} \rangle_\psi + \langle \hat{B} \rangle_\psi \hat{A} - \langle \hat{B} \rangle_\psi \langle \hat{A} \rangle_\psi \\
&= \hat{A}\hat{B} - \hat{B}\hat{A},
\end{aligned}$$

because the expectation values of Hermitian operators commute with all operators. Hence, it is identical to the commutator of $\hat{A}$ and $\hat{B}$ and by taking the square root the uncertainty product becomes

$$\Delta_\psi \hat{A} \Delta_\psi \hat{B} \geqslant \frac{1}{2} |\langle [\hat{A}, \hat{B}] \rangle_\psi|. \tag{2.2}$$

Note that Equation (2.2) only holds in general if ψ is not only an element of the domains of $\hat{A}$ and $\hat{B}$, but also that $\hat{A}\psi$ is an element of the domain of $\hat{B}$ and $\hat{B}\psi$ is an element of the domain of $\hat{A}$. Otherwise there are states which actually violate the relation [Hal13]. It can, nevertheless, be shown that the relation holds in general for canonically conjugate observables, hence, operators with a commutator of the form

$$[\hat{X}, \hat{P}] = i\hbar \mathbb{1},$$

In this case we end up with the Heisenberg Uncertainty Relation

$$\Delta_\psi \hat{X} \Delta_\psi \hat{P} \geqslant \frac{\hbar}{2}.$$

A more general way to define uncertainties is via the entropy of the states, as the standard deviation is only a very specific example for a measure of the spread of a distribution and, furthermore, also depends on the state in respect to which it is determined. Especially in the context of quantum information theory the entropic approach is useful, as the entropy can be seen as a measure of the information contained in a state. Thereby, the specific scenario under consideration has to be taken into account to define a meaningful entropic measure. In the very general case of a set of measurements $\{\hat{O}_i\}$ on a quantum state with density operator $\hat{\rho}$, an entropic uncertainty relation has the form

$$\frac{1}{N} \sum_{i=1}^{N} H(\hat{O}_i|\hat{\rho}) \geqslant c,$$

where c is a constant that solely depends on the measurement choice but not on the state $\hat{\rho}$. Thereby, $H(\hat{O}_i|\hat{\rho})$ is the entropy of the state under measurement of $\hat{O}_i$. It could for example be the (comparably simple) Shannon entropy,

$$H(\hat{O}_i|\hat{\rho}) = -\sum_{x} \operatorname{tr}(\hat{O}_i\hat{\rho}) \log_2 \operatorname{tr}(\hat{O}_i\hat{\rho}),$$

where x are the possible outcomes of the measurement. The uncertainty relation of important relevance for this thesis is based on smooth min- and max-entropies. For a pure state with density operator $\hat{\rho}_{ABC} \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ it reads

$$H^{\varepsilon}_{\min}(X|B) + H^{\varepsilon}_{\max}(Y|C) \geqslant -\log_2 c. \tag{2.3}$$

The min-entropy $H^{\varepsilon}_{\min}(X|B)$ can be seen as the logarithmic guessing probability of the outcome of a measurement $\hat{X}$ on subsystem A by performing the optimal measurement on subsystem B [Fur12Th] and, correspondingly, for a measurement $\hat{Y}$ and subsystem C. The constant c describes the overlap between the measurements $\hat{X}$ and $\hat{Y}$. The max-entropy is dual to the min-entropy [Ebe13Th],

$$H^{\varepsilon}_{\max}(\hat{\rho}_{AC}|C) = -H^{\varepsilon}_{\min}(\hat{\rho}_{AB}|B).$$

Here, $\hat{\rho}_{AB}$ and $\hat{\rho}_{AC}$ are the density operators of the (generally impure) corresponding subsystems. The term *smooth* refers to the fact that for the calculation of the entropies all states that are ε-close to the actual state are taken into account. This is nothing more but reasonable for real world implementations of quantum systems, as the precision of our statistics is always limited due to a finite number of measurements. We refrain from going further into detail, as the matter is mathematically quite complex and would go far beyond the scope of this chapter. A good introduction to entropic uncertainty relations can be found in [Weh10] and the references therein and an application of them to quantum information tasks is explained in [Fra12Th] and [Fur12Th].

2.2 QUANTIZATION OF THE ELECTROMAGNETIC FIELD

In classical physics the electromagnetic interaction is described by the four Maxwell equations, their solutions being electromagnetic waves. In quantum mechanics we find that this description is not sufficient. We will, therefore, in this section derive the quantum-mechanical theory of light and show some of its consequences.

2.2.1 *The Classical Electromagnetic Field*

The solutions of the Maxwell equations [Lou00] for the electric and the magnetic field in vacuum can be written as derivatives of a vector potential $\mathbf{A}$,

$$\mathbf{B} = \nabla \times \mathbf{A},$$

$$\mathbf{E} = -\frac{\partial \mathbf{A}}{\partial t}.$$

Here we have assumed the Coulomb gauge condition $\nabla \cdot \mathbf{A} = 0$, i.e. the vector potential is free of sources. Using these relations and replacing them in the fourth Maxwell equation we find [Lou00]

$$\nabla^2 \mathbf{A}(\mathbf{r}, t) = \frac{1}{c^2} \frac{\partial^2 \mathbf{A}(\mathbf{r}, t)}{\partial t^2}, \tag{2.4}$$

where c is the speed of light in vacuum. For now it is convenient to investigate the problem in a finite volume $V = L^3$ to get the Fourier expansion

$$\mathbf{A}(\mathbf{r}, t) = \sum_{\mathbf{k}} \sum_{\lambda} \mathbf{e}_{\mathbf{k}\lambda} A_{\mathbf{k}\lambda}(\mathbf{r}, t) + \text{h.c.},$$

where $\mathbf{e}_{\mathbf{k}\lambda}$ is a unit vector that has to be perpendicular to the wave vector $\mathbf{k}$ to fulfill the Coulomb gauge. Therefore, λ denotes the index for the two possible polarizations of the vector potential which is summed over by the second sum. The first sum is over $\mathbf{k}$ which is discretized due to the finite volume and its Cartesian components take the values

$$k_x = \frac{2\pi n_x}{L}, \qquad k_y = \frac{2\pi n_y}{L}, \qquad k_z = \frac{2\pi n_z}{L}, \qquad \{n_x, n_y, n_z\} \in \mathbb{Z}.$$

We now can solve the wave equation for the amplitude of each mode separately, as they are independent for different $\mathbf{k}$ and λ, by splitting the function in one part depending only on space and one part depending only on time, $A_{\mathbf{k}\lambda}(\mathbf{r},t) = u_{\mathbf{k}\lambda}(\mathbf{r})A_{\mathbf{k}\lambda}(t)$. We then find from Equation (2.4) that the spatial mode functions have to fulfill the Helmholtz equation

$$\left(\nabla^2 + k^2\right) u_{\mathbf{k}\lambda}(\mathbf{r}) = 0, \tag{2.5}$$

with $k^2 = \mathbf{k}\cdot\mathbf{k}$, whereas the time dependent parts have to fulfill the differential equation of the harmonic oscillator,

$$\left(\frac{\partial^2}{\partial t^2} + \omega_k^2\right) A_{\mathbf{k}\lambda}(t) = 0. \tag{2.6}$$

Here we have made use of the dispersion relation for the angular frequency

$$\omega_k = ck,$$

with $k = |\mathbf{k}|$.

Equation (2.6) is obviously solved by

$$A_{\mathbf{k}\lambda}(t) = A_{\mathbf{k}\lambda}e^{-i\omega_k t}.$$

The solutions of Equation (2.5) will be investigated in more detail in Section 3.1. For the moment let us assume the case of a plane wave, which is also a good approximation in many cases. Thus, we find

$$u_{\mathbf{k}\lambda}(\mathbf{r}) = e^{i\mathbf{k}\cdot\mathbf{r}},$$

and finally get the result for the vector potential,

$$\mathbf{A}(\mathbf{r},t) = \sum_{\mathbf{k}}\sum_{\lambda} \mathbf{e}_{\mathbf{k}\lambda}A_{\mathbf{k}\lambda}e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)} + \text{h.c.}$$

With this result we find the following expressions for the electric and the magnetic field,

$$\mathbf{E}(\mathbf{r},t) = i\sum_{\mathbf{k}}\sum_{\lambda} \omega_k \mathbf{e}_{\mathbf{k}\lambda}A_{\mathbf{k}\lambda}e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)} - \text{h.c.}, \tag{2.7}$$

$$\mathbf{B}(\mathbf{r},t) = i\sum_{\mathbf{k}}\sum_{\lambda} (\mathbf{k}\times\mathbf{e}_{\mathbf{k}\lambda})A_{\mathbf{k}\lambda}e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)} - \text{h.c.}$$

The total energy of the electromagnetic field is given by the classical Hamilton function

$$H(\mathbf{r},t) = \frac{1}{2}\int_V dx^3 \left[\varepsilon_0\mathbf{E}(\mathbf{r},t)\cdot\mathbf{E}(\mathbf{r},t) + \frac{1}{\mu_0}\mathbf{B}(\mathbf{r},t)\cdot\mathbf{B}(\mathbf{r},t)\right].$$

Here ε_0 is the electric permittivity and μ_0 is the magnetic permeability of the vacuum, which fulfill $\varepsilon_0\mu_0 = 1/c^2$. Using the fact that the spatial mode functions and the polarization vectors are orthonormal for different k and λ, we get

$$H = \varepsilon_0 V \sum_k \sum_\lambda \omega_k^2 \left[A_{k\lambda}A^*_{k\lambda} + A^*_{k\lambda}A_{k\lambda}\right]. \tag{2.8}$$

Anticipating the next section, we have not used the fact that the amplitude $A_{k\lambda}$ commutes with its complex conjugate for clarification, because this will no longer be the case when we replace them by operators in the next section.

2.2.2 *The Quantum-Mechanical Harmonic Oscillator*

So far our description was purely classical and the coefficients $A_{k\lambda}$ could be seen as the complex amplitudes of independent harmonic oscillators. We will now introduce the canonical quantization for each of these oscillators individually to get the quantum mechanical description of the electromagnetic field. The Hamilton function of the harmonic oscillator is therefor replaced by the Hamilton operator

$$\hat{H}_k = \frac{\omega_k^2 \hat{q}_k^2}{2} + \frac{\hat{p}_k^2}{2}. \tag{2.9}$$

Here $\hat{q}_k$ is the position operator and $\hat{p}_k = i\hbar\hat{\partial}_{q_k}$ is the momentum operator of mode k that obey the commutation relation

$$[\hat{q_k}, \hat{p_{k'}}] = i\hbar\delta_{kk'},$$

where $\delta_{kk'}$ denotes the Kronecker delta. Furthermore, we have set the mass of the oscillator to 1 and omitted the subscript λ, i.e. restrict ourselves to just one polarization for simplicity. By comparing Equations (2.9) and (2.8) we see that it is convenient to define amplitude operators,

$$\begin{aligned} \hat{a}_k &= \kappa\left(\omega\hat{q}_k + i\hat{p}_k\right), \\ \hat{a}_k^\dagger &= \kappa\left(\omega\hat{q}_k - i\hat{p}_k\right). \end{aligned} \tag{2.10}$$

As each set of two such operators describes an individual mode of the harmonic oscillator, we will also call them *mode operators*. With these we can express the Hamilton operator as,

$$\hat{H}_k = \frac{1}{4\kappa^2}\left(\hat{a}_k\hat{a}_k^\dagger + \hat{a}_k^\dagger\hat{a}_k\right). \tag{2.11}$$

The constant κ is so far undefined but we will fix this immediately by taking a look at the commutation relation of the mode operators,

$$\begin{aligned}
[\hat{a}_{\mathbf{k}}, \hat{a}_{\mathbf{k}'}] &= 0 = \left[\hat{a}^{\dagger}_{\mathbf{k}}, \hat{a}^{\dagger}_{\mathbf{k}'}\right], \\
\left[\hat{a}_{\mathbf{k}}, \hat{a}^{\dagger}_{\mathbf{k}'}\right] &= \hat{a}_{\mathbf{k}}\hat{a}^{\dagger}_{\mathbf{k}'} - \hat{a}^{\dagger}_{\mathbf{k}}\hat{a}_{\mathbf{k}'} \\
&= -2i\sqrt{\omega_{\mathbf{k}}\omega_{\mathbf{k}'}}\kappa^2 \left(\hat{q}_{\mathbf{k}}\hat{p}_{\mathbf{k}'} - \hat{p}_{\mathbf{k}}\hat{q}_{\mathbf{k}'}\right) \\
&= 2\omega_{\mathbf{k}}\hbar\kappa^2\delta_{\mathbf{k}\mathbf{k}'},
\end{aligned}$$

where in the last line we have used the fact that the frequency factor only contributes if $\mathbf{k} = \mathbf{k}'$. We want the commutator to equal unity which is then called the standard bosonic commutation relations. Therefore, we set $\kappa = (2\omega_{\mathbf{k}}\hbar)^{-1/2}$ to get the fully dimensionless mode operators and the Hamilton operator becomes

$$\hat{H}_{\mathbf{k}} = \frac{\hbar\omega_{\mathbf{k}}}{2}\left(\hat{a}_{\mathbf{k}}\hat{a}^{\dagger}_{\mathbf{k}} + \hat{a}^{\dagger}_{\mathbf{k}}\hat{a}_{\mathbf{k}}\right).$$

This definition of the mode operators becomes immediately natural if we take a look at the eigenstates of the Hamilton operator. These states will be energy eigenstates which relates them to the number of photons in mode $\mathbf{k}$. Therefore, we will denote them by $|n\rangle$ with $n \in \mathbb{N}$ and their energy by E_n,

$$\hat{H}|n\rangle = E_n|n\rangle, \tag{2.12}$$

where we will leave out the index $\mathbf{k}$ for simplicity. Now we will multiply this equation from the left by $\hat{a}^{\dagger}_{\mathbf{k}}$ to get

$$\begin{aligned}
& \tfrac{\hbar\omega}{2}\hat{a}^{\dagger}\left(\hat{a}\hat{a}^{\dagger} + \hat{a}^{\dagger}\hat{a}\right)|n\rangle &= E_n\hat{a}^{\dagger}|n\rangle \\
\Leftrightarrow\quad & \tfrac{\hbar\omega}{2}\left((\hat{a}\hat{a}^{\dagger} - 1)\hat{a}^{\dagger} + \hat{a}^{\dagger}(\hat{a}\hat{a}^{\dagger} - 1)\right)|n\rangle &= E_n\hat{a}^{\dagger}|n\rangle \\
\Leftrightarrow\quad & \tfrac{\hbar\omega}{2}\left(\hat{a}\hat{a}^{\dagger}\hat{a}^{\dagger} + \hat{a}^{\dagger}\hat{a}\hat{a}^{\dagger}\right)|n\rangle - \hbar\omega\hat{a}^{\dagger}|n\rangle &= E_n\hat{a}^{\dagger}|n\rangle \\
\Leftrightarrow\quad & \hat{H}\hat{a}^{\dagger}|n\rangle &= \left(E_n + \hbar\omega\right)\hat{a}^{\dagger}|n\rangle,
\end{aligned}$$

where we have made use of the commutation relation in the second line. The state $\hat{a}^{\dagger}|n\rangle$ is again an energy eigenstate whose energy is increased by $\hbar\omega$. A comparison with Section 2.1.1 shows that this corresponds to the energy of one photon with frequency ω. The corresponding calculation for $\hat{a}$ gives an energy that is decreased by the energy of one photon. This gives rise to the names *creation* and *annihilation operator* for the mode operators, as they act on the energy eigenstates by creating and annihilating a photon in the mode of frequency ω. Another common name is *ladder operators* as the application of $\hat{a}^{\dagger}$ and $\hat{a}$ acts like going one step up or down on the ladder of Harmonic Oscillator energy eigenstates.

Now that we have fixed the normalization and the energies turned out to be consistent with the quantization results postulated by Planck we can associate the classical amplitudes with the mode operators by comparing Equations (2.8) and (2.11),

$$A_k \to \sqrt{\frac{\hbar}{2\omega_k \varepsilon_0 V}}\hat{a}_k,$$
$$A_k^* \to \sqrt{\frac{\hbar}{2\omega_k \varepsilon_0 V}}\hat{a}_k^\dagger.$$

With these replacements we get the final result for the quantized electric and magnetic field,

$$\mathbf{E}(\mathbf{r},t) = i\sum_{\mathbf{k}} \mathbf{e}_{\mathbf{k}}\sqrt{\frac{\hbar\omega_k}{2\varepsilon_0 V}}\left(\hat{a}_{\mathbf{k}}e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)} - \hat{a}_{\mathbf{k}}^\dagger e^{-i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)}\right), \quad (2.13)$$

$$\mathbf{B}(\mathbf{r},t) = i\sum_{\mathbf{k}} (\mathbf{k}\times\mathbf{e}_{\mathbf{k}})\sqrt{\frac{\hbar}{2\omega_k \varepsilon_0 V}}\left(\hat{a}_{\mathbf{k}}e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)} - \hat{a}_{\mathbf{k}}^\dagger e^{-i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)}\right),$$

where we again are leaving out the sum over λ for simplicity.

2.3 HILBERT SPACES FOR THE DESCRIPTION OF LIGHT

We will now use our quantum mechanical description of the electromagnetic interaction to find sets of states that can act as a basis for the description of arbitrary states. The three sets that we are going to investigate in detail are the number states, the coherent states and the squeezed states. Particularly the squeezed states take a major role throughout this thesis but also the coherent states are of great importance for the generation and detection of the desired quantum states.

2.3.1 *Number States*

We have introduced the so-called number states already in the previous section as the eigenstates of the Harmonic Oscillator's Hamilton operator. They represent the number of photons in the field mode. To make them a meaningful basis for the quantum optical Harmonic Oscillator, we need a further definition, namely, that of the vacuum state,

$$\hat{a}|0\rangle = 0. \quad (2.14)$$

The existence of the state $|0\rangle$ and its property that it is destroyed by the annihilation operator is important, because otherwise states with negative eigenvalues and, therefore, negative energy could exist. The difference between 0 and $|0\rangle$ is that 0 is actually nothing, whereas $|0\rangle$ means there are no photons but there still is a vacuum field. The explicit position-dependent eigenfunction of $\hat{H}$ for the vacuum state is [Hal13]

$$\Psi(q) = \langle q|0\rangle = \sqrt{\frac{\pi\omega}{\hbar}} e^{-\frac{\omega}{2\hbar}q^2}, \tag{2.15}$$

where $|q\rangle$ is a position eigenstate, i.e. $\hat{q}|q\rangle = q|q\rangle$. With the property from Equation (2.14) it is easy to see that

$$\langle 0|\hat{H}|0\rangle = \frac{1}{2}\hbar\omega \neq 0.$$

We will comment on this so-called ground state energy in more detail further down. For the moment let us just accept that the energy of an empty mode is not vanishing.

We have also seen that the ladder operators increase and decrease the number of photons by one. One can furthermore show that the corresponding eigenfunction are given by

$$|n\rangle = \tilde{H}_n|0\rangle,$$

where $\tilde{H}_n$ are up to some normalizations the Hermite polynomials [Hal13]. From these we could calculate the eigen-energies but we can also deduce them already from Equation (2.12) and find

$$E_n = \hbar\omega(n + \frac{1}{2}).$$

As the Hamilton operator is proportional to $\hat{a}^\dagger\hat{a}$, it should give the number n when applied to a number state. To fulfill this we define the action of the ladder operators on the number states as

$$\hat{a}|n\rangle = \sqrt{n}|n-1\rangle, \qquad \hat{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle. \tag{2.16}$$

Using this and the vacuum state we can define the normalized number states as

$$|n\rangle = \frac{(\hat{a}^\dagger)^n}{\sqrt{n!}}|0\rangle. \tag{2.17}$$

These states are orthonormal to each other, i.e.

$$\langle n|m\rangle = \delta_{nm},$$

and form a complete set of basis vectors

$$\sum_n |n\rangle\langle n| = \mathbb{1}. \tag{2.18}$$

Hence, they form an orthonormal basis for our Hilbert space.

The number states are very useful to describe states that contain only a few photons. In this case they give an accurate description of experimental observations where only the number of photons is counted. In contrast, the description becomes inappropriate for experiments that should also show wavelike features. Let us take a look at the expectation value of the electric field operator from Equation (2.13),

$$\begin{aligned}\langle n|\mathbf{E}(\mathbf{r},t)|n\rangle &= i\mathbf{e}\sqrt{\frac{\hbar\omega}{2\varepsilon_0 V}}\left(\langle n|\hat{a}|n\rangle e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)} - \langle n|\hat{a}^\dagger|n\rangle e^{-i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)}\right)\\ &= 0,\end{aligned}$$

where we have used Equation (2.16) and orthogonality. This result does not meet our expectation of a wave evolving in space and time and we will need another set of states that give us a phase dependent expectation value to describe the various wavelike properties of light. We will introduce such states in the next section.

An intuitive understanding of the vanishing expectation value can be that the number states contain only information on the energy of a state but not on the phase. We can see this by taking a look at the variance of the field,

$$\begin{aligned}\langle n|\left(\mathbf{E}(\mathbf{r},t)\right)^2|n\rangle &= -\frac{\hbar\omega}{2\varepsilon_0 V}\Big(\langle n|\hat{a}^2|n\rangle e^{2i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)} - \langle n|\hat{a}\hat{a}^\dagger|n\rangle\\ &\qquad -\langle n|\hat{a}^\dagger\hat{a}|n\rangle + \langle n|\hat{a}^{\dagger 2}|n\rangle e^{-2i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)}\Big)\\ &= \frac{\hbar\omega}{2\varepsilon_0 V}(n+1+n)\\ &= \frac{1}{\varepsilon_0 V}E_n.\end{aligned}$$

The variance of the field contains two terms without a complex phase, that are exactly those which contribute.

Furthermore, we note that even for the vacuum state there is some non-vanishing uncertainty,

$$\langle 0|\left(\mathbf{E}(\mathbf{r},t)\right)^2|0\rangle = \frac{\hbar\omega}{2\varepsilon_0 V}.$$

This uncertainty of the field can not be circumvented and, although the expectation value is zero, we can not expect the field to be exactly zero but have to assume a Gaussian distribution concentrated around zero. Since this distribution has the smallest standard deviation for the vacuum, this is also called a minimum uncertainty state. We will see below that at least for some specific observables we can circumvent this uncertainty at the expense of increasing it for the conjugate observable. For the moment we have to accept that there is nothing less "noisy" than the vacuum. Finally, we also see that the variance is where the ground state energy ended up and that there is no problem with the vanishing expectation value in terms of energy conservation.

2.3.2 *Coherent States*

We want a set of states for which the electric field operator has non-vanishing expectation values. A natural approach is to demand them to be eigenstates of the annihilation operator,

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle, \tag{2.19}$$

where α is some complex number. Furthermore, we want these states to be normalized,

$$\langle\alpha|\alpha\rangle = 1. \tag{2.20}$$

With this it is easy to see that the expectation value of the electric field operator becomes

$$\langle\alpha|\mathbf{E}(\mathbf{r},t)|\alpha\rangle = i\mathbf{e}\sqrt{\frac{\hbar\omega}{2\varepsilon_0 V}}\left(\alpha e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)} - \alpha^* e^{-i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)}\right),$$

which is obviously a wave in space and time. A comparison with Equation (2.7) shows, that α takes the role of a complex amplitude. It is therefore sometimes also called the *coherent excitation*.

Calculating the variance of the field we find

$$\begin{aligned}\langle\alpha|\left(\mathbf{E}\;(\mathbf{r},t)\right)^2|\alpha\rangle - \langle\alpha|\mathbf{E}(\mathbf{r},t)|\alpha\rangle^2 =&\\ = -\frac{\hbar\omega}{2\varepsilon_0 V}&\left(\alpha^2 e^{2i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)} - (|\alpha|^2+1) - |\alpha|^2 + \alpha^{*2} e^{-2i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)}\right)\\ &+ \frac{\hbar\omega}{2\varepsilon_0 V}\left(\alpha e^{i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)} - \alpha^* e^{-i(\mathbf{k}\cdot\mathbf{r}-\omega_k t)}\right)^2\\ = \frac{\hbar\omega}{2\varepsilon_0 V},&\end{aligned}$$

where we have once more used the commutator of $\hat{a}$ and $\hat{a}^\dagger$. Hence, the coherent states have minimum uncertainty like the vacuum, independent of the magnitude and the phase of the excitation α. This makes them very useful to describe an almost classical wave like a laser beam and gives rise to the name *semi-classical* state.

To investigate the properties of $|\alpha\rangle$ in more detail, we are interested in the solution of Equation (2.19) in terms of the number states. We find a recursive solution by multiplying the equation with $\langle n-1|$ from the left. It follows

$$\langle n|\alpha\rangle = \frac{\alpha^n}{\sqrt{n!}}\langle 0|\alpha\rangle,$$

which gives a Poisson distribution in photon numbers [Wal94],

$$P(n) = |\langle n|\alpha\rangle|^2 = \frac{\alpha^{2n}}{n!}|\langle 0|\alpha\rangle|^2. \tag{2.21}$$

Now we can find the expansion of $|\alpha\rangle$ in terms of the number states,

$$\begin{aligned} |\alpha\rangle &= \sum_n |n\rangle\langle n|\alpha\rangle \\ &= \langle 0|\alpha\rangle \sum_n \frac{\alpha^n}{\sqrt{n!}}|n\rangle \\ &= \langle 0|\alpha\rangle \sum_n \frac{\left(\alpha\hat{a}^\dagger\right)^n}{n!}|0\rangle, \end{aligned} \tag{2.22}$$

where we have used Equation (2.18) in the first line and Equation (2.17) in the last line. Using the second line we can easily fix the value for $\langle 0|\alpha\rangle$ by using the normalization condition (2.20) and the orthogonality of the number states,

$$\begin{aligned} |\langle\alpha|\alpha\rangle|^2 &= |\langle 0|\alpha\rangle|^2 \sum_n \frac{|\alpha|^{2n}}{n!} \\ &= |\langle 0|\alpha\rangle|^2 e^{|\alpha|^2} \\ &\overset{!}{=} 1. \end{aligned}$$

From this we infer

$$\langle 0|\alpha\rangle = e^{-|\alpha|^2/2},$$

and find together with the last line from Equation (2.22)

$$|\alpha\rangle = e^{-|\alpha|^2/2} e^{\alpha\hat{a}^\dagger}|0\rangle.$$

We see that the two exponentials act like an operator creating a coherent state from the vacuum. But in the current state this operator is not unitary. To see this, we need the Baker-Campbell-Hausdorff theorem,

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

which holds for any operators $\hat{A}$ and $\hat{B}$ with c-numbered commutator ($[\hat{A},\hat{B}] \in \mathbb{C}$). Using this we see the non-unitarity of the operator,

$$\begin{aligned} e^{-|\alpha|^2/2} e^{\alpha\hat{a}^\dagger} e^{-|\alpha|^2/2} e^{\alpha^*\hat{a}} &= e^{-|\alpha|^2} e^{\alpha\hat{a}^\dagger + \alpha^*\hat{a}} e^{[\alpha\hat{a}^\dagger, \alpha^*\hat{a}]/2} \\ &= e^{-3|\alpha|^2/2} e^{\alpha\hat{a}^\dagger + \alpha^*\hat{a}} \\ &\neq 1. \end{aligned}$$

The solution to this is the introduction of an operator that acts as an identity on the vacuum state,

$$e^{f(\alpha)\hat{a}}|0\rangle = |0\rangle,$$

This is due the fact, that in the series expansion of the exponential only the first term contributes a one and all others vanish when applied to $|0\rangle$. Here, $f(\alpha)$ is an undefined function so far. We now can replace our vacuum state in equation (2.22) without changing anything

$$|\alpha\rangle = e^{-|\alpha|^2/2} e^{\alpha\hat{a}^\dagger} e^{f(\alpha)\hat{a}}|0\rangle,$$

and take another look at the unitarity of our new operator. By successive application of the BCH theorem, and keeping in mind that we have to change the order of the operators in the hermitian conjugate, we find

$$\begin{aligned}
&e^{-|\alpha|^2} e^{\alpha\hat{a}^\dagger} e^{f(\alpha)\hat{a}} e^{f^*(\alpha)\hat{a}^\dagger} e^{\alpha^*\hat{a}} = \\
&\quad = e^{-|\alpha|^2} e^{\alpha\hat{a}^\dagger + f(\alpha)\hat{a}} e^{[\alpha\hat{a}^\dagger, f(\alpha)\hat{a}]/2} \\
&\qquad\qquad \cdot e^{f^*(\alpha)\hat{a}^\dagger + \alpha^*\hat{a}} e^{[f^*(\alpha)\hat{a}^\dagger, \alpha^*\hat{a}]/2} \\
&\quad = e^{-|\alpha|^2 - \frac{1}{2}(\alpha f(\alpha) + f^*(\alpha)\alpha^*)} e^{\alpha\hat{a}^\dagger + f(\alpha)\hat{a} + f^*(\alpha)\hat{a}^\dagger + \alpha^*\hat{a}} \\
&\qquad\qquad \cdot e^{[\alpha\hat{a}^\dagger + f(\alpha)\hat{a}, f^*(\alpha)\hat{a}^\dagger + \alpha^*\hat{a}]/2} \\
&\quad = e^{-|\alpha|^2 - \frac{1}{2}(\alpha f(\alpha) + f^*(\alpha)\alpha^* + |\alpha|^2 - f(\alpha)f^*(\alpha))} e^{\alpha\hat{a}^\dagger + f(\alpha)\hat{a} + f^*(\alpha)\hat{a}^\dagger + \alpha^*\hat{a}} \\
&\quad \overset{!}{=} 1.
\end{aligned}$$

The only solution to this equation is to set

$$f(\alpha) = -\alpha^*.$$

Therefore, we end up with

$$\begin{aligned}
|\alpha\rangle &= e^{-|\alpha|^2/2} e^{\alpha\hat{a}^\dagger} e^{-\alpha^*\hat{a}}|0\rangle \\
&= e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}|0\rangle \\
&=: \hat{D}(\alpha)|0\rangle.
\end{aligned}$$

The operator $\hat{D}(\alpha)$ is called displacement operator, as it shifts the vacuum state by a complex amplitude α without changing its variance.

To check the set of coherent states for completeness we have to take the integral over α [Wal94]. The calculation is straightforward but a bit lengthy. Therefore, we will just give the result,

$$\int |\alpha\rangle\langle\alpha| d^2\alpha = \pi.$$

The factor π stems from the integration over the complex plain. Hence, it is actually correct that we do not get 1 as the result.

Taking a look at the orthogonality we calculate [Wal94]

$$\begin{aligned}|\langle\alpha'|\alpha\rangle|^2 &= |\exp[-\frac{1}{2}(|\alpha|^2+|\alpha'|^2)+\alpha\alpha'^*]|^2\\ &= \exp[-|\alpha-\alpha'|^2]\\ &\neq 0.\end{aligned}$$

Hence, two different coherent states are not orthogonal but only get close to orthogonality for $|\alpha-\alpha'| >> 1$. Therefore, they form an over-complete set and are not an actual basis for our Hilbert space. Nevertheless, we can use superpositions of them to represent other states, we just have to keep in mind that the representation might not be unambiguous due to the over-completeness.

2.3.3 *Squeezed States*

For the coherent states we have used the simplest approach and required them to be eigenstates of the annihilation operator. We can also make a more general consideration and investigate a linear combination of the annihilation and creation operator,

$$\begin{aligned}\hat{b} &= \mu\hat{a}+\nu\hat{a}^\dagger,\\ \hat{b}^\dagger &= \mu^*\hat{a}^\dagger+\nu^*\hat{a}.\end{aligned} \tag{2.23}$$

The commutation relation then reads

$$[\hat{b},\hat{b}^\dagger] = |\mu|^2[\hat{a},\hat{a}^\dagger]+|\nu|^2[\hat{a}^\dagger,\hat{a}] = |\mu|^2-|\nu|^2,$$

from which we deduce the requirement

$$|\mu|^2-|\nu|^2 = 1, \tag{2.24}$$

to have the standard bosonic commutator again.

Now we consider an eigenstate of this new mode operator,

$$\hat{b}|\beta_s\rangle = \beta|\beta_s\rangle, \tag{2.25}$$

where the subscript denotes, in foresight of the following results, that $|\beta_s\rangle$ is a *squeezed coherent state*.

To investigate the expectation value of the electric field we have to re-express $\hat{a}$ and $\hat{a}^\dagger$,

$$\begin{aligned}\hat{a} &= \mu^*\hat{b}-\nu\hat{b}^\dagger,\\ \hat{a}^\dagger &= \mu\hat{b}^\dagger-\nu^*\hat{b}.\end{aligned}$$

Inserting this in Equation (2.13) we find

$$
\begin{aligned}
\langle\beta_s|\mathbf{E}(\mathbf{r},t)|\beta_s\rangle = ie\sqrt{\frac{\hbar\omega}{2\varepsilon_0 V}}\langle\beta_s|\Big(\mu^*\hat{b}e^{i\chi} - \nu\hat{b}^\dagger e^{i\chi} \\
-\mu\hat{b}^\dagger e^{-i\chi} + \nu^*\hat{b}e^{-i\chi}\Big)|\beta_s\rangle \\
= ie\sqrt{\frac{\hbar\omega}{2\varepsilon_0 V}}\left((\mu^* e^{i\chi} + \nu^* e^{-i\chi})\beta - (\mu e^{-i\chi} + \nu e^{i\chi})\beta^*\right),
\end{aligned}
$$

with $\chi = \mathbf{k}\cdot\mathbf{r} - \omega_k t$, which gives again a wave in space and time. But now the amplitude and the phase do not only depend on β but also on the magnitude and relative phase of μ and ν. We regain the result for the coherent state by setting $\mu = 1$ and $\nu = 0$.

Analogously, the calculation for the variance yields

$$
\begin{aligned}
&\langle\beta_s|\mathbf{E}^2(\mathbf{r},t)|\beta_s\rangle - \langle\beta_s|\mathbf{E}(\mathbf{r},t)|\beta_s\rangle^2 = \\
&\quad = \frac{\hbar\omega}{2\varepsilon_0 V}\left[|\mu|^2 + |\nu|^2 + \mu^*\nu e^{2i\chi} + \mu\nu^* e^{-2i\chi}\right] \\
&\quad = \frac{\hbar\omega}{2\varepsilon_0 V}\left[|\mu|^2 + |\nu|^2 + (\mu^*\nu + \mu\nu^*)\cos(2\chi) + i(\mu^*\nu - \mu\nu^*)\sin(2\chi)\right].
\end{aligned}
$$

In order to get a more insightful result we now have to make an assumption on μ and ν that has to fulfill Equation (2.24). We can do so by setting

$$
\begin{aligned}
\mu = \cosh(r)\,,\ \nu = e^{i\varphi}\sinh(r) \\
r \in \mathbb{R}^+\,,\ \varphi \in [0, 2\pi),
\end{aligned}
\tag{2.26}
$$

which is unambiguous up to an overall phase. Then the variance reads

$$
\begin{aligned}
&\langle\beta_s|\mathbf{E}^2(\mathbf{r},t)|\beta_s\rangle - \langle\beta_s|\mathbf{E}(\mathbf{r},t)|\beta_s\rangle^2 = \\
&\quad = \frac{\hbar\omega}{2\varepsilon_0 V}\Big[\cosh^2(r) + \sinh^2(r) + \\
&\qquad\qquad 2\cosh(r)\sinh(r)\left(\cos(\varphi)\cos(2\chi) - \sin(\varphi)\sin(2\chi)\right)\Big] \\
&\quad = \frac{\hbar\omega}{2\varepsilon_0 V}\frac{1}{2}\left[\left(e^{2r} + e^{-2r}\right) + \left(e^{2r} - e^{-2r}\right)\cos(\varphi + 2\chi)\right] \\
&\quad = \frac{\hbar\omega}{2\varepsilon_0 V}\left[e^{2r}\cos^2(\varphi/2 + \chi) + e^{-2r}\sin^2(\varphi/2 + \chi)\right].
\end{aligned}
$$

Obviously the variance does not only depend on the parameters r and φ but also on the optical phase χ. We can find two distinct phase settings for which the variance gets minimal and maximal, respectively. For $\varphi/2 + \chi = n\pi, n \in \mathbb{N}$, we obtain

$$
\langle\beta_s|\mathbf{E}^2(\mathbf{r},t)|\beta_s\rangle - \langle\beta_s|\mathbf{E}(\mathbf{r},t)|\beta_s\rangle^2 = \frac{\hbar\omega}{2\varepsilon_0 V}e^{2r},
$$

whereas for $\varphi/2+\chi=(2n+1)\pi/2$ we obtain

$$\langle\beta_s|\mathbf{E}^2(\mathbf{r},t)|\beta_s\rangle-\langle\beta_s|\mathbf{E}(\mathbf{r},t)|\beta_s\rangle^2=\frac{\hbar\omega}{2\varepsilon_0 V}e^{-2r}.$$

Hence, the variance is periodically increased and decreased by a factor $\exp(2r)$ compared to the vacuum or a coherent state. This gives rise to the name *squeezed state*, and the parameter r is called the *squeezing factor*. Furthermore, the parameter φ defines at which optical phases the squeezing occurs and is therefore called *squeezing angle*.

The transformation in Equation (2.23) can be written with a unitary operator,

$$\hat{U}\hat{a}\hat{U}^\dagger=\hat{b}. \tag{2.27}$$

From equation (2.26) we also know

$$\hat{b}=\cosh(r)\hat{a}-e^{i\varphi}\sinh(r)\hat{a}^\dagger.$$

Now we can expand the hyperbolic functions in an exponential series,

$$\begin{aligned}\hat{b}&=\hat{a}\sum_n\frac{1}{(2n)!}r^{2n}+e^{i\varphi}\hat{a}^\dagger\sum_n\frac{1}{(2n+1)!}r^{2n+1}\\&=\hat{a}+\frac{1}{2}\hat{a}r^2+\frac{1}{24}\hat{a}r^4+\ldots+\hat{a}^\dagger re^{i\varphi}+\frac{1}{6}\hat{a}^\dagger r^3e^{i\varphi}+\frac{1}{120}\hat{a}^\dagger r^5e^{i\varphi}+\ldots\end{aligned}$$

Let $\zeta=re^{i\varphi}$. It follows,

$$\begin{aligned}\hat{b}&=\hat{a}+\hat{a}^\dagger\zeta+\frac{1}{2}\hat{a}|\zeta|^2+\frac{1}{6}\hat{a}^\dagger|\zeta|^2\zeta+\frac{1}{24}\hat{a}|\zeta|^4+\frac{1}{120}\hat{a}^\dagger|\zeta|^4\zeta+\ldots\\&=\hat{a}+\left[\hat{a},\frac{\zeta}{2}\hat{a}^{\dagger2}\right]+\frac{1}{2!}\left[\hat{a}^\dagger\zeta,-\frac{\zeta^*}{2}\hat{a}^2\right]+\frac{1}{3!}\left[\hat{a}|\zeta|^2,\frac{\zeta}{2}\hat{a}^{\dagger2}\right]+\ldots\\&=\hat{a}+\left[\hat{a},\frac{\zeta}{2}\hat{a}^{\dagger2}-\frac{\zeta^*}{2}\hat{a}^2\right]+\frac{1}{2!}\left[\left[\hat{a},\frac{\zeta}{2}\hat{a}^{\dagger2}-\frac{\zeta^*}{2}\hat{a}^2\right],\frac{\zeta}{2}\hat{a}^{\dagger2}-\frac{\zeta^*}{2}\hat{a}^2\right]+\ldots\\&=\sum_n\frac{1}{n!}\hat{a}_n,\end{aligned}$$

with the recursively defined operator sequence

$$\hat{a}_{n+1}:=\left[\hat{a}_n,\frac{\zeta}{2}\hat{a}^{\dagger2}-\frac{\zeta^*}{2}\hat{a}^2\right],\ \hat{a}_0=\hat{a}.$$

We make use of the following operator theorem [Lou00],

$$e^{-\hat{B}}\hat{A}e^{\hat{B}}=\hat{A}+[\hat{A},\hat{B}]+\frac{1}{2!}\left[[\hat{A},\hat{B}],\hat{B}\right]+\ldots\ ,$$

to find

$$\hat{b}=e^{-(\frac{\zeta}{2}\hat{a}^{\dagger2}-\frac{\zeta^*}{2}\hat{a}^2)}\hat{a}e^{\frac{\zeta}{2}\hat{a}^{\dagger2}-\frac{\zeta^*}{2}\hat{a}^2}.$$

Thus, we have found a unitary *squeezing operator*,

$$\hat{S}(\zeta) = \exp\left[\frac{\zeta^*}{2}\hat{a}^2 - \frac{\zeta}{2}\hat{a}^{\dagger 2}\right]. \tag{2.28}$$

From Equation (2.27) we can deduce

$$\begin{aligned} & \hat{b}\hat{U} = \hat{U}\hat{a} \\ \Leftrightarrow \quad & \hat{b}\hat{U}|\beta\rangle = \hat{U}\hat{a}|\beta\rangle \\ \Leftrightarrow \quad & \hat{b}\hat{U}|\beta\rangle = \beta\hat{U}|\beta\rangle, \end{aligned}$$

where $|\beta\rangle$ is a coherent state, and find by comparison with Equation (2.25) $\hat{U} = \hat{S}(\zeta)$ and

$$|\beta_s\rangle = \hat{S}(\zeta)|\beta\rangle. \tag{2.29}$$

Hence, the squeezed coherent states are generated from coherent states by application of the squeeze operator. As a special case we see that there is also a *squeezed vacuum state*,

$$|0_s\rangle = \hat{S}(\zeta)|0\rangle.$$

Starting from the eigenvalue Equation (2.25) we can make the same approach as for the coherent states from Equation (2.22) onward. Here we have to take the squeezed number states $|n_{sqz}\rangle = \hat{U}|n\rangle$ to make the calculation straight forward. We find an equivalent displacement relation

$$|\beta_s\rangle = \hat{D}_s(\beta)|0_s\rangle, \tag{2.30}$$

with the displacement operator

$$\hat{D}_s(\beta) = e^{\beta\hat{b}^\dagger - \beta^*\hat{b}} = e^{(\beta\mu^* - \beta^*\nu)\hat{a}^\dagger - (\beta^*\mu - \beta\nu^*)\hat{a}} = \hat{D}(\beta\mu^* - \beta^*\nu).$$

Taking the relation for the squeezed vacuum and associating $\alpha = \beta\mu^* - \beta^*\nu$ we get

$$|\beta_s\rangle = \hat{D}(\alpha)\hat{S}(\zeta)|0\rangle =: |\alpha, \zeta\rangle. \tag{2.31}$$

Hence, a squeezed coherent state $|\alpha, \zeta\rangle$ is generated from the vacuum by first squeezing it with ζ and then displacing it by a coherent excitation α. Alternatively we can derive from Equation (2.29) that the squeezed coherent state can be generated by first displacing the vacuum by β and then squeezing with ζ,

$$|\beta_s\rangle = \hat{S}(\zeta)\hat{D}(\beta)|0\rangle.$$

This state is the same as $|\alpha, \zeta\rangle$ if α and β are associated as above. It is also the original version of the squeezed states first derived under the name *two-photon coherent state* by H. P. Yuen in 1976 [Yue76]. As in this definition the squeezing operator changes the previously applied excitation β it is less intuitive and we will stick to the definition from Equation (2.31) which was published by C. Caves in 1981 [Cav81].

For the derivation of the displacement operator $\hat{D}_{\mathrm{sqz}}(\beta)$ in Equation (2.30) we have calculated scalar products with squeezed number states that do not represent photon numbers anymore. If we are interested in the actual photon number distribution we have to take the unsqueezed number states. This calculation is more involved and we will therefore just cite the results from [Yue76]. The basic idea of the proof is to take the scalar product of the squeezed coherent state with a coherent state and expand this in the number states,

$$\langle\alpha|\beta_s\rangle = \sum_n \langle\alpha|n\rangle\langle n|\beta_s\rangle. \tag{2.32}$$

Using

$$\langle\alpha|\beta_s\rangle = \frac{1}{\sqrt{\mu}}\exp\left[-\frac{|\alpha|^2}{2} - \frac{|\beta|^2}{2} - \frac{\nu\alpha^{*2} - \nu^*\beta^2 - 2\alpha^*\beta}{2\mu}\right]$$

and the identity

$$\exp\left[-t^2 + 2tz\right] = \sum_n \frac{H_n\left(z\right)}{n!}\cdot t^n, \tag{2.33}$$

where

$$t = \sqrt{\frac{\nu}{2\mu}}\alpha^*,$$
$$z = \frac{\beta}{\sqrt{2\mu\nu}} = \frac{\alpha + \alpha^*\nu/\mu}{\sqrt{2\nu/\mu}},$$

and $H_n(z)$ are the Hermite polynomials, we find by comparing the coefficients in Equation (2.32)

$$\langle n|\beta_s\rangle = \frac{1}{\sqrt{\mu\cdot n!}}\left(\frac{\nu}{2\mu}\right)^{\frac{n}{2}} H_n\left(\frac{\beta}{\sqrt{2\mu\nu}}\right) e^{-\frac{|\beta|^2}{2} + \frac{\nu^*\beta^2}{2\mu}}.$$

With the definitions for μ and ν from Equation (2.26) we get the photon number probability distribution

$$\begin{aligned} P(n) &= |\langle n|\beta_s\rangle|^2 \\ &= \frac{1}{\cosh(r)\cdot n!}\frac{\tanh^n(r)}{2^n}|H_n(z)|^2 e^{-|\alpha|^2 - \frac{\tanh(r)}{2}\left(\alpha^{*2}e^{i\varphi} + \alpha^2 e^{-i\varphi}\right)}, \end{aligned}$$

where

$$z = \frac{\alpha + \alpha^*\tanh(r)e^{i\varphi}}{\sqrt{2\tanh(r)e^{i\varphi}}}.$$

This is clearly not a Poissonian distribution. Depending on α, r and φ it can be either sub- or superpoissonian. Note that the argument of the Hermite polynomials diverges for zero squeezing. It is therefore not easy to see the reduction to the distribution of a coherent state. Equation (2.33) simply is not satisfied for $r = 0$. This means that we must make this substitution earlier, in Equation (2.32), and develop it from that point in order to find the distribution of a coherent state, as given in Equation (2.21). In contrast to that we can set α to zero without any issues. With the series expansion of the Hermite polynomials, we therefore obtain for a squeezed vacuum state's photon statistics

$$\begin{aligned} P(n) &= \frac{1}{\cosh(r) n!} \frac{\tanh^n(r)}{2^n} |H_n(0)|^2 \\ &= \frac{1}{\cosh(r) n!} \frac{\tanh^n(r)}{2^n} \left| (-1)^n \sum_{k_1 + 2k_2 = n} \frac{n!}{k_1! k_2!} (-1)^{k_1 + k_2} (0)^{k_1} \right|^2 . \end{aligned}$$

Here, the sum only gives a non-zero term for $k_1 = 0$, from which follows that n has to be even, i.e.

$$P(n) = \begin{cases} \frac{n!}{\cosh(r)((n/2)!)^2} \frac{\tanh^n(r)}{2^n} & , n \text{ even} \\ 0 & , n \text{ odd} \end{cases} .$$

We see that in a squeezed vacuum state only even photon numbers are excited. This is in perfect accordance with the application of the squeeze operator to the vacuum,

$$\hat{S}(\zeta)|0\rangle = \sum_n \frac{(\frac{\zeta^*}{2}\hat{a}^2 - \frac{\zeta}{2}\hat{a}^{\dagger 2})^n}{n!} |0\rangle,$$

where only even powers of $\hat{a}^\dagger$ can give a non-zero contribution. It is also the reason why the process of parametric down-conversion, in which *photon pairs* are created, yields a squeezed state, as we will show in Section 5.1.1.

Finally, we can show the completeness of the squeezed coherent states in the same way as for the coherent states, i.e.

$$\frac{1}{\pi} \int |\beta_s\rangle\langle\beta_s| d^2\beta = 1.$$

It is also obvious that the squeezed coherent states have the same orthogonality relation,

$$|\langle\beta_s|\beta_s'\rangle|^2 = |\langle\beta|\hat{U}^\dagger\hat{U}|\beta'\rangle|^2 = |\langle\beta|\beta'\rangle|^2 = \exp[-|\beta - \beta'|^2],$$

and are normalized,

$$\langle\beta_s|\beta_s\rangle = \langle\beta|\hat{U}^\dagger\hat{U}|\beta\rangle = 1.$$

Hence, the squeezed coherent states form a third basis for the description of our Hilbert space. They will especially be useful for the description of quadrature entangled states, as we will see in Section 4.

2.4 THE QUADRATURE PHASE SPACE

So far we have only investigated the properties of the electric field operator. This yields insight into the physical principles. But in an experimental implementation we will never resolve the optical frequency and, therefore, never directly observe the actual field. Furthermore, the annihilation and creation operators are not Hermitian and can not act as observables. Therefore, we will introduce a new set of Hermitian operators that span a phase space.

2.4.1 *Quadrature Operators*

Taking the electric field operator from Equation (2.13) we can split this into a real and an imaginary part,

$$\begin{aligned}\hat{E}(\mathbf{r},t) &= i\sqrt{\frac{\hbar\omega}{2\varepsilon_0 V}}\left[\hat{a}e^{i(\mathbf{k}\cdot\mathbf{r}-\omega t)} - \hat{a}^\dagger e^{-i(\mathbf{k}\cdot\mathbf{r}-\omega t)}\right]\\ &= \sqrt{\frac{\hbar\omega}{2\varepsilon_0 V}}\left[\hat{a}e^{i(\mathbf{k}\cdot\mathbf{r}-\omega t+\pi/2)} + \hat{a}^\dagger e^{-i(\mathbf{k}\cdot\mathbf{r}-\omega t+\pi/2)}\right]\\ &= \sqrt{\frac{\hbar\omega}{2\varepsilon_0 V}}\left[\hat{a}(\cos(\chi) - i\sin(\chi)) + \hat{a}^\dagger(\cos(\chi) + i\sin(\chi))\right]\\ &= \sqrt{\frac{\hbar\omega}{2\varepsilon_0 V}}\left[(\hat{a}^\dagger + \hat{a})\cos(\chi) + i(\hat{a}^\dagger - \hat{a})\sin(\chi)\right],\end{aligned}$$

with $\chi = \omega t - \mathbf{k}\cdot\mathbf{r} - \pi/2$. That way we have chosen the excitation to rotate with increasing time in a mathematically positive sense in the complex plane. The advantage of this splitting is that the cosine and the sine part of the electric field operator now are both Hermitian operators. We will define them as

$$\begin{aligned}\hat{X} &:= \left(\hat{a}^\dagger + \hat{a}\right) = \hat{X}^\dagger,\\ \hat{P} &:= i\left(\hat{a}^\dagger - \hat{a}\right) = \hat{P}^\dagger,\end{aligned} \tag{2.34}$$

from which follows the commutation relation

$$[\hat{X},\hat{P}] = 2i. \tag{2.35}$$

The names $\hat{X}$ and $\hat{P}$ are chosen in comparison with the definition of the mode operators from the position and the momentum operators of the Harmonic Oscillator in Equation (2.10). They can be seen as a dimensionless version of position and momentum and are called *quadrature operators* as they represent the quadrature components of the electric field. $\hat{X}$ is sometimes called the *amplitude quadrature* and $\hat{P}$ the *phase quadrature*. These names should not be confused with an amplitude and a phase operator but merely refer to amplitude and phase modulations of a wave that appear as sidebands in the according quadrature.

If we take a look at the expectation value and the variance of the quadrature operators with respect to a coherent state we get

$$\begin{aligned}
\langle\alpha|\hat{X}|\alpha\rangle &= \alpha^* + \alpha = 2\mathrm{Re}(\alpha), \\
\mathrm{Var}(\hat{X}) &= \alpha^{*2} + 2|\alpha|^2 + 1 + \alpha^2 - \alpha^{*2} - 2|\alpha|^2 - \alpha^2 = 1, \\
\langle\alpha|\hat{P}|\alpha\rangle &= i(\alpha^* - \alpha) = 2\mathrm{Im}(\alpha), \\
\mathrm{Var}(\hat{P}) &= -\alpha^{*2} + 2|\alpha|^2 + 1 - \alpha^2 + \alpha^{*2} - 2|\alpha|^2 + \alpha^2 = 1,
\end{aligned}$$

where we have used the bosonic commutation relation. Hence, the quadrature operators actually give the real and imaginary part of the coherent excitation up to a factor of two and their variance is normalized. This is due to our definition. An alternative way of defining the quadrature operators contains an additional factor of $1/2$. In that case the expectation values give directly the real and imaginary part, but the variance would be $1/4$. Both definitions are equivalent and the particular context will determine which is more convenient to use. As in this thesis in many cases variances will be compared with the vacuum variance, we will stick to the first definition giving a 1 for the latter.

We can visualize the electric field of a coherent state in the complex plane spanned by $\hat{X}$ and $\hat{P}$ (see Figure 2.1). The coherent excitation is a phasor from the origin to the point 2α. The angle between the vector and the $\hat{X}$-axis is the initial phase θ, $\alpha = |\alpha|e^{i\theta}$. With increasing time this vector will rotate counterclockwise with the optical frequency ω. The projection to the $\hat{X}$-axis then gives a cosine wave shifted by θ in phase. These visualizations of the optical phase give rise to the name *quadrature phase space* for the described complex plane. For most of the remainder of this thesis we will deal with this phase space and functions defined on it.

Furthermore, the picture does not only show the wave behavior, but also the quantum noise we have found in the previous section can be visualized. The tip of the vector is uncertain and has a distribution around the mean value. This is stated by the variance being non-zero. We can indicate this by adding a circle with radius 1 around the tip. The border of this circle is thereby not a limit for the distribution but gives the distance at which the probability has dropped to $1/e$. The

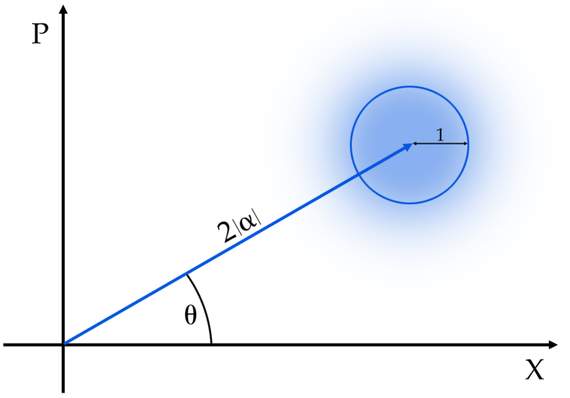


Figure 2.1: Coherent state in the quadrature phase space. A coherent state can be visualized as a phasor in the complex plane spanned by the quadratures X and P. The length α and the angle θ define the amplitude and the phase of the appertaining electromagnetic wave. Additionally, the vacuum uncertainty of the state can by depicted by a circle around the tip of the phasor.

actual distribution is spread about the whole space. In the projection to the quadratures this distribution gives some noise with standard deviation $\sigma = 1$ on the wave.

Having this picture in mind it is now easy to see what happens if we replace the coherent state with a squeezed one (see Figure 2.2). The wave behavior obviously stays the same but the noise on it depends on the optical phase and changes periodically. For example, if we set $\theta = 0$ and $\varphi = 0$ the noise is squeezed by e^{-2r} each time the coherent excitation is coaligned with the $\hat{X}$-axis, so it is squeezed in the amplitude quadrature. At the same moment it is anti-squeezed by e^{2r} in the phase quadrature. Setting $\varphi = \pi/2$ we get exactly the converse. This could already define the names *amplitude* and *phase squeezing* but there is an even better explanation. Given that the *squeezing ellipse* is rotating with the coherent excitation in phase space, we see that for $\varphi = 0$ at any time the uncertainty of the length of the vector (the amplitude) is reduced, whereas it is increased in the angle (the phase). For $\varphi = \pi/2$ it is obviously the other way around.

The setting of $\theta = 0$ is of course a very strong restriction which can not hold in general. Nevertheless, the calculations prove to be universal if we define a rotated quadrature phase space. If $|\alpha'\rangle$ is shifted in phase by some arbitrary θ in respect to $|\alpha\rangle$ we see by using the eigenvalue equation of the coherent states

$$\begin{aligned} & |\alpha'\rangle = |\alpha e^{i\theta}\rangle \\ \Leftrightarrow\quad & \hat{a}|\alpha'\rangle = e^{i\theta}\hat{a}|\alpha\rangle \\ \Leftrightarrow\quad & \hat{a}e^{-i\theta}|\alpha'\rangle = \alpha|\alpha\rangle. \end{aligned}$$

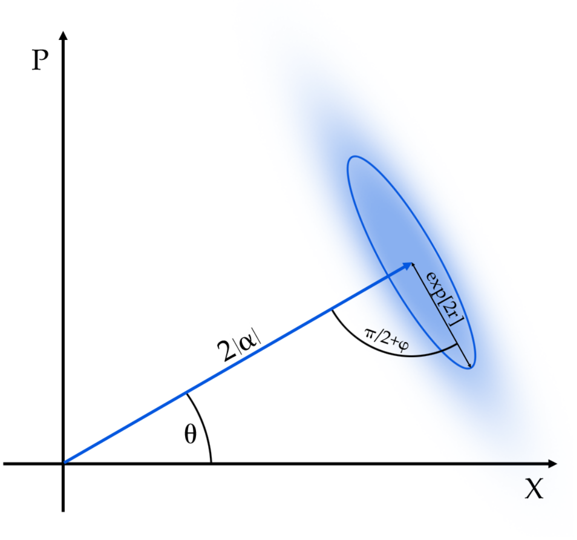


Figure 2.2: Squeezed state in the quadrature phase space. A squeezed coherent state can be visualized in the same way as a coherent state in Figure 2.1. Here, the vacuum noise at the tip of the phasor is squeezed by a factor exp[2r]. The direction of the squeezing is determined by the angle φ.

Hence, we have to rotate the mode operator by $-\theta$ to regain the result α. Re-expressing the mode operators with the quadrature operators we find

$$\begin{aligned}\hat{a}e^{-i\theta} &= \frac{1}{2}\left(\hat{X}+i\hat{P}\right)e^{-i\theta} = \frac{1}{2}\left(\hat{X}\cos\theta+\hat{P}\sin\theta+i\hat{P}\cos\theta-i\hat{X}\sin\theta\right)\\ \hat{a}^{\dagger}e^{i\theta} &= \frac{1}{2}\left(\hat{X}-i\hat{P}\right)e^{i\theta} = \frac{1}{2}\left(\hat{X}\cos\theta+\hat{P}\sin\theta-i\hat{P}\cos\theta+i\hat{X}\sin\theta\right),\end{aligned}$$

and taking the sum and the difference of the two equations (compare Equation (2.34)),

$$\begin{aligned}\hat{X}_{\theta} &:= \hat{a}^{\dagger}e^{i\theta}+\hat{a}e^{-i\theta} = \hat{X}\cos\theta+\hat{P}\sin\theta\\ \hat{P}_{\theta} &:= i\left(\hat{a}^{\dagger}e^{i\theta}-\hat{a}e^{-i\theta}\right) = \hat{P}\cos\theta-\hat{X}\sin\theta,\end{aligned} \tag{2.36}$$

which is equivalent to

$$\begin{pmatrix}\hat{X}_{\theta}\\ \hat{P}_{\theta}\end{pmatrix} = \begin{pmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{pmatrix}\begin{pmatrix}\hat{X}\\ \hat{P}\end{pmatrix}.$$

The phase space spanned by $\hat{X}_{\theta}$ and $\hat{P}_{\theta}$ has the same properties and may by used for an equivalent description. Depending on the field under investigation we may use the standard phase space or the rotated one wherever it seems more useful.

2.4.2 *Statistical Moments and the Covariance Matrix*

We have to deal a bit with statistics to understand how we can describe the uncertainty features of quantum states in the quadrature phase space. We will just give a brief overview to derive the basic description needed for this thesis. A good introduction to the statistical description of stochastic processes can for example be found in [Mid96] and [Jac03]. The statements derived in this section will be used throughout this thesis for the description of quantum states and measurement results.

PROBABILITY MEASURES AND DENSITIES Assume we have some random variable X. Then measuring X will give some random value x according to some *distribution function*. An infinite repetition of the measurement of identically prepared states should thereby reproduce the distribution. Thus, the distribution can be defined as [Mid96]

$$D(x) = P(X \leqslant x),$$

where $P(X \leqslant x)$ is the *probability measure* to find a value smaller than x when measuring X. Obviously the following hold:

$$\begin{aligned} D(x) &\geqslant 0 \ \forall x, \\ D(x) &\leqslant 1 \ \forall x, \\ D(-\infty) &= 0, \\ D(\infty) &= 1. \end{aligned}$$

Accordingly, the probability to find X between a and b is

$$P(a < X \leqslant b) = D(b) - D(a).$$

Taking this to the infinite limit we construct the *probability density* as the first derivative of the distribution, if it exists,

$$\lim_{h \to 0} \frac{D(x+h) - D(x)}{h} = \frac{dD(x)}{dx} =: w(x).$$

Conversely we find

$$D(x) = \int_{-\infty}^{x} w(x')dx'.$$

Together with the properties of the distribution we get

$$\begin{aligned} w(x) &\geqslant 1 \ \forall x, \\ \int_{-\infty}^{\infty} w(x)dx &= 1, \\ w(x)dx &= P(x < X \leqslant x + dx). \end{aligned}$$

The integration over the whole space giving 1 is a necessary and sufficient condition for $w(x)$ to be a probability density and completely defines the probability measure of X [Jac03]. The quantity $w(x)dx$ is also called the *probability element* and represents the probability to find X in an infinitely small element dx [Mid96].

CHARACTERISTIC FUNCTION AND STATISTICAL MOMENTS An insightful way to investigate the statistical properties of a random variable X is to define the *characteristic function*

$$F(u) = \int e^{iux} w(x) dx,$$

which is the (non-unitary) Fourier transform of the probability density. Consequently, we have

$$w(x) = \int e^{-iux} F(u) du.$$

Expanding the exponential in the definition of the characteristic function we find

$$\begin{aligned} F(u) &= \int \sum_n \frac{(iux)^n}{n!} w(x) dx \\ &= \sum_n \frac{(iu)^n}{n!} \int x^n w(x) dx, \end{aligned}$$

where we can interchange the integral and the sum due to the uniform convergence of the series. With the definition

$$\mu_n := \int x^n w(x) dx$$

we get a Taylor series in the complex argument iu,

$$F(u) = \sum_n \mu_n \frac{(iu)^n}{n!}. \tag{2.37}$$

The coefficients μ_n are called the *statistical moments* of X. By taking the definition of the Taylor series for $F(u)$ and comparing it to Equation (2.37) we see

$$\mu_n = (-i)^n \frac{d^n}{du^n} F(u) \Big|_{u=0}.$$

Hence, the nth statistical moment of X is proportional to the nth derivative of its characteristic function.

The moments are of special interest as they characterize the statistics of the random variable. In particular we have the first moment being the *expectation value* (or *mean*)

$$\langle X\rangle = \int x w(x) \mathrm{d}x,$$

and the second moment being the *mean square*

$$\langle X^2\rangle = \int x^2 w(x) \mathrm{d}x.$$

In case the mean vanishes (as, for example, in all vacuum states) the mean square is identical to the *variance*,

$$\mathrm{Var}(X) := \langle (X - \langle X\rangle)^2\rangle = \langle X^2\rangle - \langle X\rangle^2 = \langle X^2\rangle. \tag{2.38}$$

For all other instances we can define the so-called *central moments*,

$$\mu'_n := \int (x - \langle X\rangle)^n w(x) \mathrm{d}x.$$

Furthermore, the third moment is known as the *skewness*, characterizing whether the density is "leaning" to the right (positive skew) or the left (negative skew), and the fourth moment is known as the *kurtosis*, characterizing the curvature of the density, i.e. whether it is "slim and tall with long tails" (high kurtosis) or "broad, low and compact" (low kurtosis). Also the higher moments can be of interest in a specific random process.

CONDITIONAL DENSITIES AND COVARIANCES We can generalize the statements we have made so far to a n-dimensional space, i.e. to a vector of random variables $\mathbf{X} = (X_1, ..., X_n)$. Then we define the distribution function [Jac03, Mid96]

$$D(\mathbf{x}) = P\left(\prod_i (X_i \leqslant x_i)\right) = \int_{-\infty}^{x_1} ... \int_{-\infty}^{x_n} w(\mathbf{x}')\mathrm{d}x'_1 ... \mathrm{d}x'_n.$$

This distribution function can be difficult to interpret in higher dimensions, but the probability density (if it exists) is actually straightforwardly extended from the one-dimensional case. We will restrict ourselves to two dimensions to keep the calculations clear, but all of them immediately apply to the general case of n dimensions.

The 2-dimensional density can be reduced to the previous one-dimensional case, the so-called *marginal distributions*, via

$$w_{X_1}(x_1) = \int_{-\infty}^{\infty} w(\mathbf{x}')\mathrm{d}x'_2,$$
$$w_{X_2}(x_2) = \int_{-\infty}^{\infty} w(\mathbf{x}')\mathrm{d}x'_1,$$

from which it is easy to see

$$\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} w(\mathbf{x}')\mathrm{d}x_1'\mathrm{d}x_2' = 1.$$

Again it can be shown that $w(\mathbf{x})$ is a probability density if and only if this equation holds [Jac03].

Of special interest is the question of whether X_1 and X_2 are statistically independent. If and only if they are, it holds [Jac03]

$$w(\mathbf{x}) = w(x_1)w(x_2).$$

Hence, the overall density factorizes into the marginal distributions.

Furthermore, we can (especially if X_1 and X_2 are not independent) define the *conditional density*

$$w_{X_2|X_1}(x_2) := w_{X_1=x_1}(x_2) = \frac{w(\mathbf{x})}{w(x_1)}, \tag{2.39}$$

which is the probability density of X_2 given $X_1 = x_1$. We see immediately that $w_{X_2|X_1}(x_2) = w_{X_2}(x_2)$ if and only if X_1 and X_2 are independent. This definition of the conditional density should be handled with care, as for a continuous distribution the probability of finding X_1 at exactly x_1 is zero. It should, therefore, be understood as a fraction of probability elements representing the probability of finding X_1 between x_1 and $x_1 + \mathrm{d}x_1$,

$$w_{X_1=x_1}(x_2)\mathrm{d}x_2 = \frac{P(x_1 < X_1 \leqslant x_1 + \mathrm{d}x_1, x_2 < X_2 \leqslant x_2 + \mathrm{d}x_2)}{P(x_1 < X_1 \leqslant x_1 + \mathrm{d}x_1)}.$$

We define the covariance of two random variables as

$$\mathrm{Cov}(X_1, X_2) := \langle X_1X_2\rangle - \langle X_1\rangle\langle X_2\rangle,$$

which is a measure of how X_1 and X_2 "co-vary" around their respective expectation value. If they are correlated this will result in a positive covariance, whereas if they are anti-correlated it will be negative. We say X_1 and X_2 are uncorrelated if the covariance vanishes. With the definition of the statistical moments it is easy to see that X_1 and X_2 are uncorrelated if they are independent [Jac03]. The converse is not true: if they are uncorrelated we can only say that they are *linearly independent*, stating that they are independent up to their first joint moment, but might not be for higher moments. A comparison with Equation (2.38) also shows

$$\mathrm{Cov}(X, X) = \mathrm{Var}(X).$$

Extending this to n dimensions, we can define the *covariance matrix* γ with entries

$$\gamma_{ij} := \mathrm{Cov}(X_i, X_j).$$

In the special case of pairwise uncorrelated X_i this matrix takes a diagonal form where the ith diagonal element is the variance of X_i. More generally we can say: Assume $\mathbf{Y} \oplus \mathbf{Z} = \mathbf{X} \in \mathbb{R}^n$, with $\mathbf{Y} \in \mathbb{R}^k$ and $\mathbf{Z} \in \mathbb{R}^l$, $\mathbb{R}^k \cup \mathbb{R}^l = \mathbb{R}^n$, $\mathbb{R}^k \cap \mathbb{R}^l = \{0\}$. Then $\mathbf{Y}$ and $\mathbf{Z}$ are uncorrelated if and only if

$$\gamma_X = \gamma_Y \oplus \gamma_Z.$$

The covariance matrix takes a block form with the upper left block containing the intrinsic covariances of $\mathbf{Y}$ and the lower right block those of $\mathbf{Z}$ [Jac03].

THE NORMAL DISTRIBUTION We will now specialize the above results to the most important probability density that we will deal with in this thesis, namely the *normal distribution*. As it goes back to Carl Friedrich Gauß it is often also called *Gaussian distribution* or simply *Gaussian*. It is defined by

$$w_N(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-\mu)^2}{2\sigma^2}}, \tag{2.40}$$

with $\sigma = \sqrt{\mathrm{Var}(X)}$ the standard deviation and $\mu = \langle X \rangle$ the expectation value. This function is of course a density and not a distribution. So the statement "X is Gaussian" is a bit sloppy and actually means "X follows a normal distribution and has a Gaussian probability density". We will use these terms synonymously, as the meaning should always be clear from the context.

The importance of this function is due to the fact that the most important state we will deal with, the ground state of the Harmonic Oscillator, has a Gaussian probability density (compare Equation (2.15)),

$$|\langle x|0\rangle|^2 \propto e^{-x^2}, \tag{2.41}$$

Thus, the statistics of our measurements will always converge to a normal distribution if we take enough data points.

The characteristic function appertaining to the Gaussian distribution is given by

$$F(u) = e^{iu\mu - \frac{\sigma^2 u^2}{2}}.$$

Generalizing this to n dimensions, we find that the random variables $\mathbf{X}$ are Gaussian if and only if the characteristic function takes the form [Jac03]

$$F(\mathbf{u}) = e^{i\mathbf{u}^T\cdot\boldsymbol{\mu}-\frac{1}{2}\mathbf{u}^T\cdot\gamma\cdot\mathbf{u}},$$

where $\boldsymbol{\mu}$ is the n-dimensional vector of means and γ is the covariance matrix from above. If and only if all X_i in $\mathbf{X}$ are independent, γ is diagonal and $F(\mathbf{u})$ factors,

$$F(\mathbf{u}) = \prod_i F(u_i).$$

Even more generally it can be proven [Jac03] that if $\mathbf{Y}$ and $\mathbf{Z}$ are Gaussian and, if they are independent, then $\mathbf{X} = \mathbf{Y} \oplus \mathbf{Z}$ is Gaussian and we have

$$F_X(\mathbf{u}_X) = F_Y(\mathbf{u}_Y)F_Z(\mathbf{u}_Z),$$

and the covariance matrix takes block form, hence, $\text{Cov}(\mathbf{Y},\mathbf{Z}) = 0$ and $\mathbf{Y}$ and $\mathbf{Z}$ are uncorrelated. This is of course a reproduction of the previous result for general distributions, but in addition to this it can be proven that in the case of Gaussian random variables $\mathbf{Y}$ and $\mathbf{Z}$ are independent if and only if they are uncorrelated. This is a very strong statement, as it implies that independence and uncorrelatedness are equivalent for Gaussian random variables. Furthermore, any vector $\mathbf{X}$ of Gaussian random variables can be reduced to a vector $\mathbf{Y}$ with pairwise independent Y_j, where the number of Y_j is strictly less than the number of X_i [Jac03].

Finally, these results can be used to prove that a Gaussian $\mathbf{X}$ has a density on $\mathbb{R}^n$ if and only if the covariance matrix is non-degenerate, i.e. $\det\gamma \neq 0$ and it is found to be [Jac03]

$$w_N(\mathbf{x}) = \frac{1}{2\sqrt{\pi^n \det\gamma}} e^{-\frac{1}{2}(\mathbf{x}-\boldsymbol{\mu})^T\cdot\gamma^{-1}\cdot(\mathbf{x}-\boldsymbol{\mu})}. \tag{2.42}$$

This summarizes our findings that for any set of Gaussian random variables, all statistical properties are described by the first and second moment, $\boldsymbol{\mu}$ and γ. Therefore, in the experiments we can check the measurement data for Gaussianity to make use of these profound results.

2.4.3 *Properties of the Covariance Matrix for Physical States*

The fact that a Gaussian distribution is fully described by its covariance matrix makes it reasonable to summarize some of its properties. Throughout this thesis we will deal with states that have n modes, each described by a pair of quadrature operators. Therefore, the covariance matrix will be a $2n \times 2n$-matrix and we will use a pairwise ordering of the operators in a vector $\xi = (\hat{X}_1, \hat{P}_1, ..., \hat{X}_n, \hat{P}_n)$. Then the function $w_N(\xi)$ from Equation (2.42) becomes the Wigner function [Wig32] that describes the phase space probability density of the quantum state with covariance matrix γ. Note that we may interpret the Wigner function as probability density only for Gaussian states. With this ordering of the quadrature operators we find a condition for the physicality of the state [Krü06Th],

$$\gamma + i\sigma \geqslant 0. \tag{2.43}$$

Here, σ is the symplectic form

$$\sigma := \bigoplus_{i=1}^{n} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

The relation for the covariance matrix has to be understood as an eigenvalue condition stating that all eigenvalues of the matrix $\gamma + i\sigma$ are positive semidefinite. It is actually a generalized version of the Heisenberg Uncertainty Relation which becomes clear from the following argument. Suppose γ is diagonal, so it has the eigenvalues $\gamma_1, ..., \gamma_{2n}$. Then the relation requires that the eigenvalues $\gamma_i \pm 1$ of $\gamma + i\sigma$ are larger than 0, which means that the eigenvalues of gamma have to be larger than 1. By definition of the covariance matrix we then find

$$\begin{aligned} \gamma_{2i-1}\gamma_{2i} &= \left(\langle \hat{X}_i^2 \rangle - \langle \hat{X}_i \rangle^2\right)\left(\langle \hat{P}_i^2 \rangle - \langle \hat{P}_i \rangle^2\right) \\ &\geqslant 1, \end{aligned}$$

which is equivalent to (compare Equations (2.2) and (2.35))

$$\Delta^2 \hat{X} \Delta^2 \hat{P} \geqslant \frac{1}{4} |\langle [\hat{X}, \hat{P}] \rangle_\psi|^2.$$

It can furthermore be shown that any covariance matrix can be diagonalized which makes the argument hold in general [Krü06Th].

On the other hand, if in Equation (2.43) equality holds γ describes a minimum uncertainty state and its eigenvalues are 1. Now we can make use of the Parseval theorem to connect the density operator of a quantum state to the characteristic function [Krü06Th]

$$\mathrm{tr}(\hat{\rho}_\psi \hat{\rho}_\varphi) = \frac{1}{(2\pi)^n} \int d\mathbf{u} F_\psi^*(\mathbf{u}) F_\varphi(\mathbf{u})$$

to find

$$\mathrm{tr}(\hat{\rho}^2) = \frac{1}{(2\pi)^n} \int d\mathbf{u} |F(\mathbf{u})|^2.$$

For a Gaussian state the integrand on the right hand side evaluates to

$$|F^*(\mathbf{u})|^2 = e^{-\mathbf{u}^T \gamma \mathbf{u}},$$

hence, if all eigenvalues of γ are 1 the integral yields $(2\pi)^n$ and we have shown that a minimum uncertainty Gaussian state is also a pure state. If we now multiply the physicality condition by $i\sigma$ we find

$$i\sigma\gamma + \mathbb{1} = 0,$$

where we have used $\sigma^2 = -\mathbb{1}$. And by taking the square we get a condition for Gaussian states to be pure,

$$(\sigma\gamma)^2 = -\mathbb{1}.$$

We would like to make a final comment on symplectic transformation and symplectic invariants. A symplectic transformation S is a basis change of the phase space that keeps the scalar product invariant. The scalar product for two n-mode vectors ξ and ζ is defined via the symplectic form,

$$\langle \xi, \zeta \rangle = \xi^T \sigma \zeta.$$

A symplectic transformation will now act on the vectors like

$$\begin{aligned} \xi^T \sigma \zeta &\overset{!}{=} (S \cdot \xi)^T \sigma (S \cdot \zeta) \\ &= \xi^T \cdot S^T \sigma S \cdot \zeta, \end{aligned}$$

from which follows that it must not change the symplectic form,

$$S^T \sigma S = \sigma.$$

As σ is connected to the physicality condition in Equation (2.43), this means that physical states are transformed into physical states under symplectic transformations. We will make use of this in the theoretical description of the beam splitter in Section 3.2.3. Also many other optical implementations can be described by symplectic transformations in an elegant way, for example the generation of squeezing from the vacuum [Ebe13Th]. Furthermore, the symplectic invariants are of special interest. These are quantities that are independent of the phase space under consideration, as they do not change under symplectic transformation. For example for a two-mode covariance matrix γ we find these four invariants [Bu010]:

$$\begin{aligned} I_1 &= \det A, \\ I_2 &= \det B, \\ I_3 &= \det C, \\ I_4 &= \det \gamma. \end{aligned} \tag{2.44}$$

Here, we have defined the covariance matrix in block form consisting of four 2×2-matrices,

$$\gamma = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix}.$$

This block form as well as the symplectic invariants will be very useful to describe entangled states with two modes (see Chapters 4 and 5). The blocks A and B can be seen as the local descriptions of the two modes whereas the block C contains the information about any correlations between the modes.

3

DETECTION OF OPTICAL QUANTUM STATES

Following the epistemological foundations of modern natural science, the theoretical description of a process must precisely define and predict the observation of an experiment and the experiment must precisely implement the description to test nature under controlled circumstances and to prove or disprove the theory [Kan98]. In quantum mechanics we establish a theory that describes the processes of elementary particles and single quanta. Therefore, a meaningful experiment that tests quantum theory has to operate at the level of a single or very few quanta in a specific single (or sufficiently singularized) mode. The mode is here the space-time element in which the interaction we are interested in takes place, and we do not want this interaction to be disturbed by any other modes because that would render our measurement result useless to test the theory. In this chapter we will explain how we can make sure to detect a single mode with a sensitivity that allows a resolution at the level of the quantum of action $\hbar$.

3.1 GAUSSIAN OPTICS

3.1.1 *Fundamental Solution of the Helmholtz Equation*

In Section 2.2.1 we have found that the spatial modes of the electromagnetic field obey the Helmholtz Equation (2.5). For the derivation of the fundamental quantum optical principles it was sufficient to solve this with a plane wave. But such a wave is unrealistic in experimental circumstances, as it would imply infinite extension perpendicular to the propagation direction. We will now assume the light to propagate in a beam in z-direction, i.e. to have a small extent in the x-y-plane. This allows us to restrict the optical wave to the propagation direction, $u_{\mathbf{k}}(\mathbf{r}) = \Psi(x, y, z) \exp(ikz)$, and to paraxially approximate the Helmholtz equation,

$$\frac{\partial^2 \Psi}{\partial x^2} + \frac{\partial^2 \Psi}{\partial y^2} + 2ik\frac{\partial \Psi}{\partial z} = 0. \qquad (3.1)$$

We have, hereby, made the assumption that Ψ changes so slowly with z that we can neglect the second derivative. The fundamental solution to this equation is [Kog66]

$$\Psi_{00}(x, y, z) = \frac{w_0}{w} \exp\left[i\Phi - (x^2 + y^2)\left(\frac{1}{w^2} + \frac{ik}{2R}\right)\right].$$

Here w is the beam radius, R is the radius of curvature of the wave front and Φ is the Gouy phase and all are functions of z given by

$$\begin{aligned} w(z) &= w_0\sqrt{1+\left(\frac{2z}{kw_0^2}\right)^2}, \\ R(z) &= z\left[1+\left(\frac{kw_0^2}{2z}\right)^2\right], \\ \Phi(z) &= \arctan\frac{2z}{kw_0^2}. \end{aligned}$$

The constant w_0 describes the minimum beam radius at position $z = 0$ and is called the *waist*. This is also one of the three points where the wave front is flat. The other two are at $z = \pm\infty$ where the wave front approaches that of a spherical wave with infinite radius. The Gouy phase at these two points is $\Phi = \pm\pi/2$, hence, the beam collects an extra phase of π as it travels from the negative infinity through the waist to the positive infinity.

Taking a look at the intensity we find

$$I_{00} \propto |\Psi_{00}|^2 = \left(\frac{w_0}{w}\right)^2 \exp\left[-\frac{2(x^2+y^2)}{w^2}\right].$$

The exponential describes a Gaussian intensity profile with respect to the distance from the z-axis, that has a standard deviation of $w/2$. As w grows with increasing absolute value of z the beam profile gets broader. For $|z| >> 1$, it approaches a beam with fixed opening angle $\theta = \arctan(2/kw_0)$, hence, it only depends on the waist size and the optical frequency. This far-field relation explains why a big beam diameter is necessary to achieve a very small waist and why an actual point focus can never be achieved. The factor w_0/w takes into account that the overall intensity should be the same at any point and decreases the maximum of the Gaussian distribution for increasing absolute value of z.

3.1.2 *Higher Order Transversal Modes*

The function Ψ_{00} is only the fundamental solution of the differential equation (3.1). It can in general be multiplied by some functions that only depend on x and y, thereby gaining a whole set of possible transversal modes. There are two principle ways to do this, one in Cartesian coordinates and one in cylindrical coordinates. The first one delivers solutions of the form [Kog66]

$$\begin{aligned} \Psi_{mn}(x,y,z) &= H_m\left(\frac{\sqrt{2}x}{w}\right) H_n\left(\frac{\sqrt{2}y}{w}\right) \Psi_{00}(x,y,z), \\ \Phi(m,n,z) &= (m+n+1)\Phi(z), \end{aligned}$$

where H_m are the Hermite polynomials and $m, n \in \mathbb{N}$. For this reason these modes are called *Hermite-Gaussian*. They show a rectilinear pattern in the intensity profile, where m gives the number of intensity minima in the x-direction, and n in the y-direction. An exemplary Ψ_{12} Hermite-Gaussian mode is displayed in Figure 3.1.

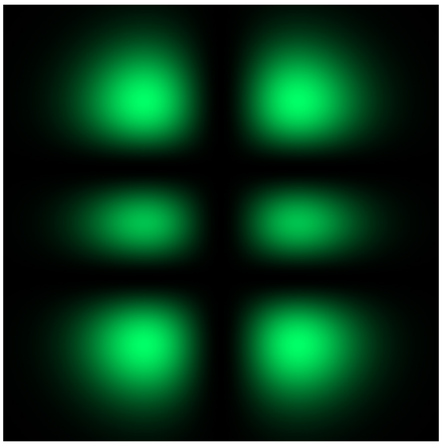


Figure 3.1: Intensity distribution of a Ψ_{12} Hermite-Gaussian mode. The intensity shows 1 minimum in x-direction and 2 minima in y-direction.

The second possibility gives modes with radial symmetry. The solutions are of the form [Kog66]

$$\begin{aligned}\Psi_{pl}(r, \varphi, z) &= \left(\frac{\sqrt{2}r}{w}\right)^{l} L_p^l\left(\frac{2r^2}{w^2}\right) e^{il\varphi}\Psi_{00}(r, \varphi, z),\\ \Phi(p, l, z) &= (2p + l + 1)\Phi(z),\end{aligned}$$

where $r^2 = x^2 + y^2$, $\varphi = \arctan[y/x]$ and L_p^l are the generalized Laguerre polynomials with $p, l \in \mathbb{N}$. Thus, these modes are referred to as *Laguerre-Gaussian*. The intensity profile shows p minima in the radial direction and $2l$ minima on the circle around the beam axis. An exemplary Ψ_{22} Laguerre-Gaussian mode is displayed in Figure 3.2.

3.1.3 *Implications for Experiments*

The difference of the Gouy phase from the fundamental mode is the reason why in a cavity different transversal modes have different resonance frequencies, as they will normally collect a different phase in one round trip. Therefore, when scanning the length of a cavity a spectrum becomes visible where each peak belongs to a different transversal mode. Thereby, both sets of modes occur. The Hermite-Gaussian modes stem from a tilt-shift of the incident beam with respect to the fundamental eigenmode of the cavity, whereas the Laguerre-Gaussian modes stem from an offset of the waist size and the waist position in beam direction. This can be used to adjust

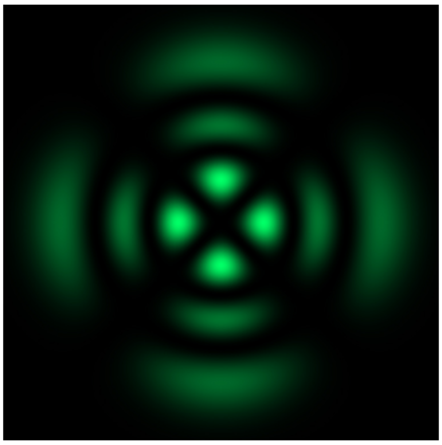


Figure 3.2: Intensity distribution of a Ψ_{22} Laguerre-Gaussian mode. The intensity shows 2 minimum in radial direction and 4 minima on the full circle.

a beam to a cavity. In Figure 3.3 a generic optical configuration of a three mirror ring cavity is shown. By sending the incident beam to two mirrors, each tiltable around the x- and the y-axis, the beam direction and position can be adjusted. Positioning an appropriate set of lenses in the path, the waist size and position can be matched to the eigenmode of the cavity. The beam is then said to be *mode matched*. The adjustment of the tilt-shift is normally quite intuitive and can be done by simply observing the mode spectrum while scanning the length of the cavity, and iteratively adjusting the mirrors until all higher Hermite-Gaussian modes are minimized. On the other hand, the correct combination and position of lenses can be difficult to find, since in many cases only a specific combination of a concave and a convex lens leads to the desired waist. Therefore, for almost all mode matchings in this thesis the Java script *JamMT* by N. Latzka was used to numerically calculate an initial mode matching [Lat10]. Starting from this result, an iterative fine positioning of the lenses was performed similar to the adjustment of the mirrors. With this procedure mode matchings close to 100% were achieved in all cases, which means almost all light was in the Ψ_{00} mode of the respective cavity.

The question arises why one would actually care about the transversal modes. As both sets of solutions form a complete and orthogonal set, the scalar product of two different modes, which in this case has integral form, would yield 0. Note that the mode functions already contain appropriate weighting functions to make the Hermite and the Laguerre polynomials orthogonal. Therefore, when superimposing two different modes no interference should occur. Especially in the case of homodyne detection (see Section 3.3), the local oscillator in Ψ_{00} mode will select the Ψ_{00} mode of the signal and all other modes will not be detected. Hence, the signal could have an arbitrary beam shape. Now this is only a quarter of the story. First of

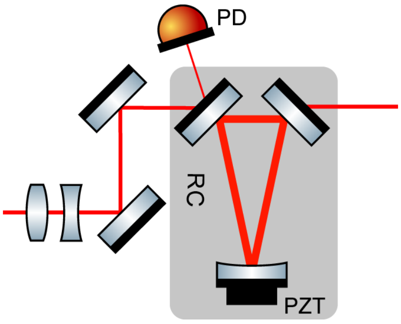


Figure 3.3: Schematic of a generic mode matching setup. The beam can be adjusted to the fundamental eigenmode of the three mirror ring cavity (RC) via a system of lenses and mirrors. The mode matching can be observed by scanning the length of the cavity with the piezo-mounted rear mirror (PZT). Due to the different Gouy phases of the different modes, a spectrum becomes visible at the photo diode (PD).

all, the scalar product only vanishes in the infinite integration. But an actual photo diode has a small diameter, and one can certainly not assume that the whole x-y-plane is detected. Surely the spot size on the photo diode of a beam in Ψ_{00} mode can be made small such that a high detection efficiency is achieved. But this is not necessarily true for higher order transversal mode. Secondly, the orthogonality is only fulfilled if the superimposed modes have the same beam radius. But the best way to define the beam radius is by having a defined waist in a cavity somewhere along the beam axis. This gives rise to the application of an *analyzing* ring cavity. This is a cavity like in Figure 3.3 with good non-degeneracy properties that is reached via a flip mirror after the superposition of two beams at a beam splitter. If both beams have perfect mode matching to the analyzing cavity they are also mode matched at the beam splitter. Thirdly, it turns out that the best way to generate continuous-wave squeezed light is in a cavity. And to achieve a high efficiency, all beams required in this process have to be perfectly mode matched to this cavity. So throughout this thesis good mode matchings were required, be it for the efficiency of quantum processes or the contrast at a superposition or the optical detection efficiency. Therefore, all auxiliary beams like the local oscillator or the pump for the squeezed light sources were sent through a so-called *mode cleaner cavity*. This resonator is structurally identical to the analyzing cavity but in addition to the scanning ability it has a Pound-Drever-Hall lock [Bla01] to stabilize it to the fundamental cavity eigenmode. That way all higher order transversal modes were reflected at the cavity and it was made sure that in the experiment the beams are as close as possible to a Ψ_{00} mode.

3.2 MIXING OF DIFFERENT MODES

3.2.1 *The Classical Beam Splitter*

The key ingredient for any interference experiment is the beam splitter, an optical device with two inputs and two outputs that, due to a non-zero transmissivity for the inputs, enables a superposition of different modes. The classical beam splitter can be described by a matrix relation [Lou00],

$$\begin{pmatrix} E_3 \\ E_4 \end{pmatrix} = \begin{pmatrix} r_1 & t_2 \\ t_1 & r_2 \end{pmatrix} \begin{pmatrix} E_1 \\ E_2 \end{pmatrix}.$$

Here we have assumed all electric fields to be of the same polarization and monochromatic frequency. The reflection and transmission amplitudes r and t are in general complex but energy conservation gives some constraints. The fact that

$$|E_1|^2 + |E_2|^2 = |E_3|^2 + |E_4|^2$$

is required, delivers [Lou00]

$$\begin{aligned} |r_1|^2 + |t_1|^2 &= |r_2|^2 + |t_2|^2 = 1, \\ r_1 t_2^* + r_2^* t_1 &= 0. \end{aligned}$$

Investigating the magnitudes and arguments separately we find

$$\begin{aligned} |r_1| = |r_2| =: r, \qquad |t_1| = |t_2| =: t, \\ \arg(r_1) + \arg(r_2) - \arg(t_1) - \arg(t_2) = \pm\pi. \end{aligned}$$

The first line states that the beam splitter has to be symmetric to fulfill energy conservation. The second line leaves some arbitrariness. For example, we can choose to set $\arg(r_2) = \pi$ and all others to zero. This means that only at the reflection of one port a phase flip of π occurs. In general, many other conventions are possible but the chosen one has the advantage that the beam splitter matrix becomes completely real,

$$\begin{pmatrix} E_3 \\ E_4 \end{pmatrix} = \begin{pmatrix} r & t \\ t & -r \end{pmatrix} \begin{pmatrix} E_1 \\ E_2 \end{pmatrix}.$$

With this it becomes most obvious that the real parameters r and t are reflection and transmission amplitudes. For example, for a 50:50 beam splitter which mixes the two input fields equally we have $r = t = 1/\sqrt{2}$.

3.2.2 *The Quantum Optical Beam Splitter*

To get a description within quantum optics we have to replace the electric fields by the mode operators according to Equation (2.13). The rest stays basically the same and we find

$$\begin{pmatrix} \hat{a}_3 \\ \hat{a}_4 \end{pmatrix} = \begin{pmatrix} r & t \\ t & -r \end{pmatrix} \begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \end{pmatrix}.$$

The same holds for the adjoint operators, note that the beam splitter matrix is unitary. Using this relation it can be shown that the output mode operators fulfill the same bosonic commutation relation as the input mode operators. Hence, we do not have to change anything in our description. The only real difference from the classical beam splitter happens, if one input port is left open. In the classical picture the corresponding field would simply be zero and not contribute at all. In contrast to this, the mode operators do have a non-vanishing action on the vacuum state which we have to assume, if no input field is present. Therefore, at least the vacuum will always contribute to the output states.

This fact enables us to describe optical loss with the beam splitter. If a quantum optical state experiences some loss we can think of this as some part of it vanishing (into the thermal bath of the universe) and being replaced by a corresponding amount of vacuum. Hence, we can use a beam splitter with one input port open whose reflectivity amplitude is the square root of the optical loss we want to model,

$$\begin{pmatrix} \hat{a}_{\text{out}} \\ \hat{a}_{\text{lost}} \end{pmatrix} = \begin{pmatrix} \sqrt{1-\eta} & \sqrt{\eta} \\ \sqrt{\eta} & -\sqrt{1-\eta} \end{pmatrix} \begin{pmatrix} \hat{a}_{\text{vac}} \\ \hat{a}_{\text{in}} \end{pmatrix}.$$

Here η is the optical detection efficiency. The mode $\hat{a}_{\text{lost}}$ is lost, which is why it is called optical loss. We only can keep the mode $\hat{a}_{\text{out}} = \sqrt{\eta}\hat{a}_{\text{in}} + \sqrt{1-\eta}\hat{a}_{\text{vac}}$ and the difference between a beam splitter and optical loss is that in the latter case we have just one output mode.

3.2.3 *Symplectic Beam Splitter Transformations*

We can generalize the beam splitter relation to the description of Gaussian state by the covariance matrix and define a unitary, symplectic beam splitter operator (see Section 2.4.3) acting on the quadrature phase space with N modes,

$$\left(U_{BS}^{k,l}(t)\right)_{i,j} = \begin{cases} r\delta_{i,j} + t(\delta_{2k-i,2l-j} - \delta_{2l-i,2k-j}) & i,j \in M \\ \delta_{i,j} & i,j \in [1,2N]\backslash M \end{cases}. \tag{3.2}$$

Here, $\delta_{i,j}$ is the Kronecker delta and $r = \sqrt{1-|t|^2}$ as previously. The domain $M = \{2k-1, 2k, 2l-1, 2l\}$ are the indices of the four quadratures describing the two modes k and l that get mixed by the beam splitter. For all other modes the operator acts as an identity. The application to the covariance matrix then reads

$$\gamma_{\text{mix}(k,l)} = U_{BS}^{k,l}(t)\gamma U_{BS}^{k,l}(t)^T. \tag{3.3}$$

Note that $U_{BS}^T = U_{BS}^\dagger$, due to the convention of non-imaginary entries in the matrix.

The application to optical loss is straightforward by replacing t with the square root of the detection efficiency and by expanding the covariance matrix with an individual vacuum mode for each mode that a loss should by applied to. Hence, for each mode that suffers from optical loss the dimension of the covariance matrix has to be increased by 2 and is then embedded in the Hilbert space $\mathcal{H}_{\text{loss}} = \mathcal{H} \oplus \mathcal{H}_{\text{vac}}$.

3.3 BALANCED HOMODYNE DETECTION

The detection of quadrature amplitudes is normally realized by balanced homodyne detection (BHD). As shown in Fig. 3.4, the signal is superimposed at a balanced beam splitter with a strong field, called the local oscillator (LO). The two outputs are measured by PIN photo diodes and the photocurrents are subtracted and filtered appropriately. We will now show that this leads to the desired measurement of arbitrary quadrature amplitudes.

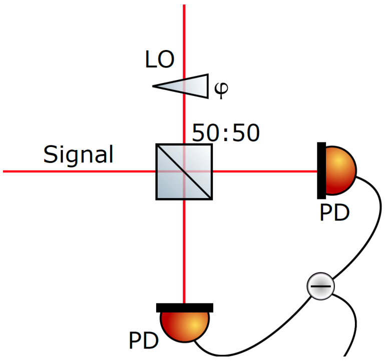


Figure 3.4: Schematic of a balanced homodyne detector. The signal is superimposed at a 50:50 beam splitter with a strong local oscillator (LO). The two outputs are detected by PIN photo diodes (PD) and the resulting photo currents are subtracted. The detected quadrature can by changed by the relative phase φ.

3.3.1 *Description of the Fields at the Homodyne Beam Splitter*

Let as assume the LO to be strong enough so we can fairly approximate it by a classical field,

$$E_{LO}(t) = |\alpha| e^{i\omega_0 t + \theta},$$

with a so far arbitrary phase θ. Here we neglect any additional noise accompanying the LO which might also be present at other frequencies. We can do so because these amplitudes will be amplified by the coherent excitation at the second beam splitter input port, which is assumed to be negligibly small compared to α. A rule of thumb is that a ratio of about 30 is sufficient for this assumption, and in experiments often even ratios of several orders of magnitude are realized.

Now let us consider the second beam splitter port. Here, we can not restrict the description to the single frequency ω, as at least a vacuum state at all possible frequencies has to be taken into account. In the general Fourier expansion of the electromagnetic field

$$E_{sig}(t) = \sum_k \left[\sqrt{\frac{\hbar\omega_k}{2\varepsilon_0 V}} \hat{a}_k e^{-i\omega_k t} + \text{h.c.} \right]$$

we have quantized the field in a finite volume $V = AL$ and the spacing between different frequencies is $\Delta\omega = 2\pi c/L$. Here we have left out the spatial mode functions as we will select one specific spatial mode in the detection by the overlap with the spatial mode of the LO. This will define the finite cross sectional area A of our quantization volume.

As we assume the second beam splitter port to be in general completely open, we have to let the length L of the quantization volume go to infinity. The discrete sum will thereby change to a continuous integral [Lou00],

$$\sum_k \to \frac{1}{\Delta\omega} \int d\omega.$$

Furthermore, the mode operators from Section 2.2.2 change as

$$\hat{a}_k \to \sqrt{\Delta\omega}\, \hat{a}(\omega), \qquad \hat{a}_k^\dagger \to \sqrt{\Delta\omega}\, \hat{a}^\dagger(\omega),$$

with the new commutation relation

$$\left[\hat{a}(\omega), \hat{a}^\dagger(\omega') \right] = \delta(\omega - \omega'),$$

where δ denotes the Dirac delta distribution. Hence, the modes for different frequencies are orthonormal to each other.

With these replacements we find the continuous expansion of the field

$$\begin{aligned} E_{sig}(t) &= \int_0^\infty d\omega \sqrt{\frac{\hbar\omega}{4\pi\varepsilon_0 cA}} \left[\hat{a}(\omega) e^{-i\omega t} + \text{h.c.}\right] \\ &= \int_{-\omega_0}^{\infty} d\Omega \sqrt{\frac{\hbar(\omega_0+\Omega)}{4\pi\varepsilon_0 cA}} \left[\hat{a}(\omega_0+\Omega) e^{-i\omega_0 t} e^{-i\Omega t} + \text{h.c.}\right], \end{aligned}$$

where in the second step we have changed the integration variable to sideband frequencies of the LO, $\Omega = \omega - \omega_0$.

3.3.2 *Detection of Quadrature Amplitudes*

The detected photocurrents in the two output ports are proportional to the intensities of the superimposed fields,

$$i_1 \propto \left| \frac{1}{\sqrt{2}} (E_{LO} + E_{sig}) \right|^2 \quad , \quad i_2 \propto \left| \frac{1}{\sqrt{2}} (E_{LO} - E_{sig}) \right|^2 ,$$

which gives, after some algebra

$$\begin{aligned} i_{1,2} = \frac{\mathcal{C}'}{2} \Big[|\alpha|^2 \pm |\alpha| \int_{-\omega_0}^{\infty} d\Omega \sqrt{\frac{\hbar(\omega_0+\Omega)}{4\pi\varepsilon_0 cA}} \\ \cdot \left(\hat{a}_\Omega e^{-i\Omega t} (e^{-2i\omega_0 t} e^{-i\theta} + e^{i\theta}) + \text{h.c.} \right) \Big], \end{aligned}$$

The $+$ refers to i_1, the $-$ refers to i_2, $\hat{a}_\Omega = \hat{a}(\omega_0 + \Omega)$ and $\mathcal{C}'$ is some constant depending on the electronics. Furthermore, we have omitted all terms that are just quadratic in $\hat{a}$ and do not contain an α, as these are negligible compared to the coherent amplitude α. We see that there are terms oscillating at the doubled frequency of the LO. As these are not directly observable optical frequencies, but are averaged over to yield 0, we can also omit all terms of the form $e^{2i\omega_0}$.

Now we take the difference of the two currents,

$$\begin{aligned} i_{\text{dif}} &= i_1 - i_2 \\ &= \mathcal{C}'|\alpha| \int_{-\omega_0}^{\infty} d\Omega \sqrt{\frac{\hbar(\omega_0+\Omega)}{4\pi\varepsilon_0 cA}} \left(\hat{a}_\Omega e^{-i\Omega t} e^{i\theta} + \text{h.c.} \right), \end{aligned}$$

and, thereby, double the amplitude and remove the constant term from the LO.

As we are interested in the signal amplitude at a specific sideband frequency Ω_0, we will demodulate this photo current difference with an electronic oscillator. The mathematical equivalent of this operation is the multiplication of the signal with a cosine,

$$\begin{aligned}\hat{X}_{\Omega_0,\theta}(t) &:= \cos(\Omega_0 t)\cdot i_{dif}\\ &= \frac{\mathcal{C}'|\alpha|}{2}\int\limits_{-\omega_0}^{\infty} d\Omega\sqrt{\frac{\hbar(\omega_0+\Omega)}{4\pi\varepsilon_0 cA}}\left(\hat{a}_\Omega e^{-i(\Omega-\Omega_0)t}e^{i\theta}+\text{h.c.}\right)\\ &\quad+\frac{\mathcal{C}'|\alpha|}{2}\int\limits_{-\omega_0}^{\infty} d\Omega\sqrt{\frac{\hbar(\omega_0+\Omega)}{4\pi\varepsilon_0 cA}}\left(\hat{a}_\Omega e^{-i(\Omega+\Omega_0)t}e^{i\theta}+\text{h.c.}\right).\end{aligned} \tag{3.4}$$

Now we restrict our observation to a certain range of resolution bandwidth Ω_R, which is usually done by some electronic filters,

$$\begin{aligned}\hat{X}_{\Omega_0,\theta}(t) = &\frac{\mathcal{C}'|\alpha|}{2}\int\limits_{\Omega_0-\Omega_R/2}^{\Omega_0+\Omega_R/2} d\Omega\sqrt{\frac{\hbar(\omega_0+\Omega)}{4\pi\varepsilon_0 cA}}\left(\hat{a}_\Omega e^{-i(\Omega-\Omega_0)t}e^{i\theta}+\text{h.c.}\right)\\ +&\frac{\mathcal{C}'|\alpha|}{2}\int\limits_{-\Omega_0-\Omega_R/2}^{-\Omega_0+\Omega_R/2} d\Omega\sqrt{\frac{\hbar(\omega_0+\Omega)}{4\pi\varepsilon_0 cA}}\left(\hat{a}_\Omega e^{-i(\Omega+\Omega_0)t}e^{i\theta}+\text{h.c.}\right).\end{aligned}$$

In the second integral we change the integration direction by swapping the upper and lower bound and change the integration variable $\Omega \to -\Omega$. As both operations give a minus sign, the overall sign does not change,

$$\begin{aligned}\hat{X}_{\Omega_0,\theta}(t) = \mathcal{C}'\sqrt{\frac{|\alpha|^2\hbar\omega_0}{16\pi\varepsilon_0 cA}}\int\limits_{\Omega_-}^{\Omega_+} d\Omega\,\Big[&\left(\hat{a}_\Omega e^{-i(\Omega-\Omega_0)t}e^{i\theta}+\text{h.c.}\right)\\ &+\left(\hat{a}_{-\Omega} e^{-i(-\Omega+\Omega_0)t}e^{i\theta}+\text{h.c.}\right)\Big],\end{aligned}$$

with $\Omega_\pm = \Omega_0 \pm \Omega_R/2$. Here we have used the scaled narrow band approximation $\Omega << \omega$ to get the square root factor out of the integral. Comparing the two integrands to the definition of a rotated quadrature in Equation (2.36) we see immediately

$$\begin{aligned}\hat{X}_{\Omega_0,\theta}(t) &= \mathcal{C}\int\limits_{\Omega_-}^{\Omega_+} d\Omega\left(\hat{X}_{\theta-\chi}(\Omega)+\hat{X}_{\theta+\chi}(-\Omega)\right),\\ \mathcal{C} &= \mathcal{C}'\sqrt{\frac{|\alpha|^2\hbar\omega_0}{16\pi\varepsilon_0 cA}},\end{aligned} \tag{3.5}$$

with $\chi = (\Omega - \Omega_0)t$. So the detected amplitude is proportional to the sum of the quadrature amplitudes of the upper and lower sideband. Note, that the quadrature angle for frequencies $\Omega \neq \Omega_0$ is time dependent and opposite for the two sidebands. Hence, here we take the sum of quadratures rotating against each other in time. But actually this does not make any difference in the measured variances as a calculation in the Appendix A.1 shows. Apart from this we can for simplicity make the assumption that the detected frequencies follow a δ-distribution at Ω_0 which gives

$$\hat{X}_{\Omega_0,\theta}(t) = \mathcal{C}\left(\hat{X}_\theta(\Omega_0) + \hat{X}_\theta(-\Omega_0)\right). \tag{3.6}$$

We can think of the actual distribution as an infinite sum over such δ-distributions, each with an appropriate $\mathbb{R}$-valued coefficient.

3.4 EXPECTATION VALUES AND VARIANCES OF HOMODYNE SIGNALS

The result of the previous section was that the homodyne signals are proportional to the quadrature amplitude at a selectable quadrature angle and sideband frequency. We are now interested in the expectation values and variances of these signals for the states that were used in the framework of this thesis.

3.4.1 *Measurement on the Vacuum State*

We take a look at the time series of the operator $\hat{X}_{\Omega_0,\theta}(t)$ from Equation (3.5). This will of course depend on the input state at the second beam splitter port, and a natural starting point is to assume a vacuum state. So we are interested in the magnitudes

$$\langle 0|\hat{X}_{\Omega_0,\theta}(t)|0\rangle$$

and

$$\mathrm{Var}_{\mathrm{vac}}(\hat{X}_{\Omega_0,\theta}(t)) = \langle 0|\left(\hat{X}_{\Omega_0,\theta}(t)\right)^2|0\rangle - \langle 0|\hat{X}_{\Omega_0,\theta}(t)|0\rangle^2.$$

Remembering that the quadrature operators are the sum of the mode operator and its hermitian conjugate, and that these are orthonormal for different frequencies, it is easy to see that the expectation value vanishes immediately as expected.

For the variance we have to take the square of the integral, which in general is not equal to the integral over the square. But as we know that modes of different frequencies commute, we can neglect all cross terms and actually restrict to the integral over the square. Nevertheless, the calculation gets a bit lengthy, but with the same arguments as for the expectation value, and using $\hat{a}|0\rangle = 0$, we find that only two terms contribute in the case of a vacuum state,

$$\begin{aligned}\mathrm{Var}_{\mathrm{vac}}(\hat{X}_{\Omega_0,\theta}(t)) &= \langle 0|\mathcal{C}^2 \int_{\Omega_-}^{\Omega_+} d\Omega \left(\hat{a}_{\Omega}\hat{a}^{\dagger}_{\Omega} + \hat{a}_{-\Omega}\hat{a}^{\dagger}_{-\Omega}\right)|0\rangle \\ &= 2\mathcal{C}^2 \int_{\Omega_-}^{\Omega_+} d\Omega \\ &= 2\mathcal{C}^2\Omega_R.\end{aligned}$$

Here we see that the detected vacuum noise level is proportional to the resolution bandwidth. Note that we have taken the simple case of a rectangular distribution in frequency. The actual distribution of the filter might be a different function of Ω, nevertheless, there will be proportionality between bandwidth and noise level. This is intuitively reasonable, as in a broader distribution more frequency modes contribute to the noise. Hence, if we want to compare the variance of some other state to that of the vacuum, we have to make sure that we take the same resolution bandwidth.

3.4.2 *Measurement on the Squeezed Vacuum State*

Now we would like to investigate the result of such a measurement if we take a squeezed vacuum as signal input. As we have seen in Section 2.3.3, there are states that exhibit a squeezed noise compared to the vacuum in one quadrature. Where in the previous description we considered the idealized case of a degenerate parametric amplifier, we now want to look at the actual situation in the experiment. In this case the down-conversion (see Section 5.1.1) is non-degenerate, and there are photon pairs created with frequencies $\omega + \Omega$ and $\omega - \Omega$, where for energy conservation ω is half the pump frequency. Hence, we get the squeezing operator

$$\hat{S}(\zeta) = \exp\left[\zeta^* \hat{a}_{+\Omega}\hat{a}_{-\Omega} - \zeta\hat{a}^{\dagger}_{+\Omega}\hat{a}^{\dagger}_{-\Omega}\right],$$

with $\hat{a}_{\pm\Omega}$ as above and $\zeta = re^{i\varphi}$. Note that r in general can be a function of Ω, hence, the squeezing factor can be frequency dependent. Furthermore, φ can also be a function of Ω, which leads to a frequency dependent squeezed quadrature. For simplicity, and as we will later on only use squeezing at one sideband frequency, we will assume both of them to be constant.

Using the identity

$$\hat{S}^{\dagger}(\zeta)\hat{a}_{\pm\Omega}\hat{S}(\zeta) = \hat{a}_{\pm\Omega}\cosh(r) - \hat{a}^{\dagger}_{\mp\Omega}e^{i\varphi}\sinh(r)$$

we find the following expectation values [Wal94]

$$\begin{aligned}
\langle \hat{a}_{\pm\Omega} \rangle_{\mathrm{sqz}} &= \langle 0|\hat{S}(\zeta)^\dagger \hat{a}_{\pm\Omega} \hat{S}(\zeta)|0\rangle = 0,\\
\langle \hat{a}_{\pm\Omega}\,\hat{a}_{\pm\Omega} \rangle_{\mathrm{sqz}} &= 0,\\
\langle \hat{a}_{\pm\Omega}\,\hat{a}_{\mp\Omega} \rangle_{\mathrm{sqz}} &= -e^{i\varphi}\sinh(r)\cosh(r),\\
\langle \hat{a}^\dagger_{\pm\Omega}\,\hat{a}_{\pm\Omega} \rangle_{\mathrm{sqz}} &= \sinh^2(r).
\end{aligned}$$

With these on hand we can calculate the expectation values for the sideband quadratures $\hat{X}_{\theta\mp\chi}(\pm\Omega)$,

$$\begin{aligned}
\langle \hat{X}_{\theta\mp\chi}(\pm\Omega) \rangle_{\mathrm{sqz}} &= \langle 0| \left(\hat{X}_{\theta\mp\chi}(\pm\Omega)\cosh(r) - \hat{X}_{-\theta\pm\chi-\varphi}(\mp\Omega)\sinh(r)\right)|0\rangle\\
&= 0,
\end{aligned}$$

$$\begin{aligned}
\langle \hat{X}^2_{\theta\mp\chi}(\pm\Omega) \rangle_{\mathrm{sqz}} &= \langle 0|\hat{S}^\dagger \hat{X}_{\theta\mp\chi}(\pm\Omega)\hat{S}\hat{S}^\dagger \hat{X}_{\theta\mp\chi}(\pm\Omega)\hat{S}|0\rangle\\
&= \langle 0| \left(\hat{X}_{\theta\mp\chi}(\pm\Omega)\cosh(r) - \hat{X}_{-\theta\pm\chi-\varphi}(\mp\Omega)\sinh(r)\right)^2|0\rangle\\
&= \cosh^2(r) + \sinh^2(r),
\end{aligned}$$

$$\begin{aligned}
&\langle \hat{X}_{\theta\mp\chi}(\pm\Omega)\hat{X}_{\theta\pm\chi}(\mp\Omega) \rangle_{\mathrm{sqz}} =\\
&\quad= \langle 0| \left(\hat{X}_{\theta\mp\chi}(\pm\Omega)\cosh(r) - \hat{X}_{-\theta\pm\chi-\varphi}(\mp\Omega)\sinh(r)\right)\\
&\qquad \left(\hat{X}_{\theta\pm\chi}(\mp\Omega)\cosh(r) - \hat{X}_{-\theta\mp\chi-\varphi}(\pm\Omega)\sinh(r)\right)|0\rangle\\
&\quad= -2\cos(2\theta+\varphi)\cosh(r)\sinh(r),
\end{aligned}$$

This makes it easy to see the expectation value and the variance of the measured amplitude $\hat{X}_{\Omega_0,\theta}(t)$,

$$\begin{aligned}
\langle \hat{X}_{\Omega_0,\theta} \rangle_{\mathrm{sqz}} &= \mathcal{C}\int_{\Omega_-}^{\Omega_+} d\Omega \left\langle \left(\hat{X}_{\theta-\chi}(\Omega) + \hat{X}_{\theta+\chi}(-\Omega)\right)\right\rangle\\
&= 0,
\end{aligned}$$

$$\begin{aligned}
\mathrm{Var}(\hat{X}_{\Omega_0,\theta}) &= \mathcal{C}^2 \int_{\Omega_-}^{\Omega_+} d\Omega \left\langle \left(\hat{X}_{\theta-\chi}(\Omega) + \hat{X}_{\theta+\chi}(-\Omega)\right)^2\right\rangle \qquad (3.7)\\
&= \mathcal{C}^2 \int_{\Omega_-}^{\Omega_+} d\Omega \Big[2\cosh^2(r) + 2\sinh^2(r)\\
&\qquad -4\cos(2\theta+\varphi)\cosh(r)\sinh(r)]\\
&= 2\mathcal{C}^2\Omega_R\left[\cosh(2r) - 2\cos(2\theta+\varphi)\sinh(2r)\right].
\end{aligned}$$

As expected for a vacuum state, the mean vanishes. Furthermore, we see that there are two distinct settings of interest for the angle θ for which the variance becomes extremal. By differentiating for θ and setting the result to 0 we find the corresponding quadrature angles $2\theta + \varphi = \pi/2 \mp \pi/2$ where the cosine becomes ± 1. The difference between the two solutions for θ is exactly $\pi/2$, hence, the two extremal quadratures are orthogonal. Their variances are

$$\begin{aligned}\mathrm{Var}(\hat{X}_{\Omega_0,-\varphi/2}(t)) &= 2\mathcal{C}^2\Omega_R e^{-2r},\\ \mathrm{Var}(\hat{X}_{\Omega_0,\pi/2-\varphi/2}(t)) &= 2\mathcal{C}^2\Omega_R e^{+2r}.\end{aligned}$$

Note that the vacuum noise is $2\mathcal{C}^2\Omega_R$, thus, the noise in one quadrature is squeezed by a factor e^{-2r} whereas in the other it is anti-squeezed by a factor e^{+2r}.

This result is in perfect accordance with the previous one in Section 2.3.3. But in contrast to the idealized situation of squeezing at DC (0 Hz sideband frequency) we now have understood where squeezed variances at non-zero sideband frequencies stem from. It can actually be understood as an entanglement of the upper and lower sideband. If we would measure the amplitudes $\hat{X}_\theta(\pm\Omega)$ independently, both would have zero expectation value and the same variance of

$$\mathrm{Var}(\hat{X}_\theta(\pm\Omega)) = \mathcal{C}^2\Omega_R\cosh(2r).$$

This variance is independent of the quadrature angle θ as well as of the squeezing angle φ and increases monotonically with increasing squeezing factor r. Note that for $r = 0$ the variance is a factor of 2 smaller than the vacuum noise because we measured just one of the two sidebands. But as we have seen, the variance is squeezed, if we take the sum of the two sideband quadrature amplitudes for a certain θ. Hence, for this quadrature the amplitudes of the two sidebands are anti-correlated, and the strength of the correlation is determined by the squeezing factor. For the orthogonal quadrature we would also see an equivalently squeezed variance if we could measure the difference of the upper and lower sideband quadrature amplitudes. This can be seen in Equation (3.7), where in this case the sign of the cosine would change. Hence, in this quadrature the amplitudes are correlated correspondingly. This is an entanglement of the upper and lower sideband in their quadrature amplitudes and it has been demonstrated in [Sam07] by splitting the two sideband and sending them to different homodyne detectors. To measure the difference of the phase quadratures amplitudes and prove this entanglement with just one homodyne detector, the only possibility would be to introduce a phase flip of π between the two sidebands already before the homodyne beam splitter. While this would in general be possible, in the case of the homodyne detection this would, apart from an irrelevant overall phase, just result in swapping the squeezed and the anti-squeezed quadratures. We are left with also measuring the sum of the correlated quadratures which of course results in anti-squeezed noise. Note that due to the entanglement of the two sidebands the anti-squeezed variance is not just the sum of the two independent variances but a bit smaller, where the deviation vanishes for $r \to \infty$.

3.4.3 *Measurement on the Coherent State*

So far we have only investigated scalar products in the basis sets of the number states and the squeezed states. Now let as consider the third possible basis of our Hilbert space spanned by the coherent states. First of all we will have a look at a single coherent excitation at, say, $+\Omega_0$. Such a state is called a single sideband (SSB) for obvious reasons and we assume it to have an infinitely narrow bandwidth. Remembering that a coherent state is an eigenstate of the annihilation operator, $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$, we see immediately that the expectation value can no longer vanish in general,

$$\begin{aligned}\langle \hat{X}_{\Omega_0,\theta}(t)\rangle_{SSB} &= \mathcal{C}\langle \alpha_{\Omega_0}| \int\limits_{\Omega_-}^{\Omega_+} d\Omega \left(\hat{X}_{\theta-\chi}(\Omega) + \hat{X}_{\theta+\chi}(-\Omega)\right) |\alpha_{\Omega_0}\rangle \\ &= \mathcal{C} \int\limits_{\Omega_-}^{\Omega_+} d\Omega \langle \alpha_{\Omega_0}| \hat{a}_\Omega e^{i(\theta-\chi)} + \text{h.c.} |\alpha_{\Omega_0}\rangle \\ &= \mathcal{C}\Omega_R \left(\alpha_{\Omega_0} e^{i\theta} + \alpha^*_{\Omega_0} e^{-i\theta}\right) \\ &= 2\mathcal{C}\Omega_R |\alpha_{\Omega_0}| \cos(\theta - \arg(\alpha_{\Omega_0})),\end{aligned}$$

where in the second line we have used the fact that only the quadrature amplitude of the upper sideband contributes, in the third line that only a single frequency contributes and in the fourth line that $\alpha_{\Omega_0} = |\alpha_{\Omega_0}| \exp(-i \arg(\alpha_{\Omega_0}))$. Assuming the phase $\arg(\alpha_{\Omega_0})$ to be constant, we see that the expectation value only depends on the phase θ of the LO in a sinusoidal way. This behavior enables us to use the detected quadrature amplitude as an error signal for the LO phase (see Section 6.2.2). Note that we have chosen the coherent excitation to be exactly at the demodulation frequency Ω_0. If we would have chosen it to be at a different frequency (but within the detected bandwidth) the signal would furthermore oscillate with the difference frequency in time.

When calculating the variance of $\hat{X}_{\Omega_0,\theta}(t)$ we have to take into account that the lower sideband without coherent excitation does not contribute to the expectation value but it will contribute a vacuum uncertainty to the variance. With this in mind, we find that the variance is actually equal to that of pure vacuum, as we would expect for a coherent state.

Note that we can set the sideband frequency to 0 without any issues. The SSB then describes a coherent excitation at DC. This happens for example with the control field that is used for the squeezed light generation and that co-propagates with the squeezed vacuum. It is easy to see that the incident of this beam on the signal port of the homodyne detector results in a cosine signal only depending on the relative phase of the LO. The control field defines the amplitude quadrature in the direction of α_0, i.e. $\arg(\alpha_0) = 0$ by definition. Therefore, the resulting signal can only be used to stabilize the homodyne detector to the phase quadrature ($\theta = \pm\pi/2$), where the cosine crosses zero. Since there is no sideband frequency, there is no demodulation phase that could shift this crossing to other quadrature angles. Nevertheless, this technique was used for the experiments in Chapter 5 as a phase quadrature lock.

Now let us consider two coherent excitations placed symmetrically around the LO frequency ω_0. For simplicity we will again assume them to be exactly at the demodulation frequency with infinitely small bandwidth. Then we find

$$\begin{aligned}\langle \hat{X}_{\Omega_0,\theta}(t)\rangle_{\mathrm{mod}} &= \mathcal{C}\langle \alpha_{\Omega_0}, \alpha_{-\Omega_0}| \\ &\qquad \int_{\Omega_-}^{\Omega_+} d\Omega \left[\hat{X}_{\theta-\chi-\beta}(\Omega) + \hat{X}_{\theta+\chi+\beta}(-\Omega)\right] |\alpha_{\Omega_0}, \alpha_{-\Omega_0}\rangle \\ &= \mathcal{C}\Omega_R \Big[\alpha_{\Omega_0} e^{i(\theta-\beta)} + \alpha^*_{\Omega_0} e^{-i(\theta-\beta)} \\ &\qquad + \alpha_{-\Omega_0} e^{i(\theta+\beta)} + \alpha^*_{-\Omega_0} e^{-i(\theta+\beta)}\Big] \\ &= 2\mathcal{C}\Omega_R \left[|\alpha_{\Omega_0}| \cos(\theta - \beta - \arg(\alpha_{\Omega_0}))\right. \\ &\qquad \left. + |\alpha_{-\Omega_0}| \cos(\theta + \beta - \arg(\alpha_{-\Omega_0}))\right].\end{aligned}$$

where we also have taken the demodulation phase β from Appendix A.1 into account. Let us assume the two excitations to have the same amplitude, $|\alpha_{\Omega_0}| = |\alpha_{-\Omega_0}|$. Then

$$\begin{aligned}\langle \hat{X}_{\Omega_0,\theta}(t)\rangle_{\mathrm{mod}} = 2\mathcal{C}\Omega_R |\alpha_{\Omega_0}| \cos\left(\theta - \frac{\arg(\alpha_{\Omega_0}) + \arg(\alpha_{-\Omega_0})}{2}\right) \\ \cdot \cos\left(\beta + \frac{\arg(\alpha_{\Omega_0}) - \arg(\alpha_{-\Omega_0})}{2}\right).\end{aligned}$$

Again we get a signal that is sinusoidally dependent on θ but now the amplitude of it is a function of the demodulation phase and the phase relation between the two sidebands. Hence, for optimal signal amplitude β has to be adapted with respect to this phase relation. Furthermore, for the phase relation between the sidebands there are two distinct possibilities, $\arg(\alpha_{\Omega_0}) - \arg(\alpha_{-\Omega_0}) = 0$ and $\arg(\alpha_{\Omega_0}) - \arg(\alpha_{-\Omega_0}) = \pi$. With the first relation we get an amplitude modulation and with the second one a phase modulation of the signal input of the homodyne detector. If we also set $\arg(\alpha_{\Omega_0}) = 0$ or $\arg(\alpha_{\Omega_0}) = \pi$ the signal becomes equivalent to an amplitude modulation or a phase modulation of the LO. This was used for the experiments in Chapter 5 to complement the previously mentioned phase quadrature lock based on the DC control field with an amplitude quadrature lock based on the phase modulation on the control field. This modulation was initially used to stabilize the squeezed-light source to resonance with a PDH technique [Bla01]. But it also delivered a sine signal at the homodyne detector for the quadrature angle θ,

$$\begin{aligned}\langle \hat{X}_{\Omega_0,\theta}(t)\rangle_{\mathrm{mod}} &\propto \cos\left(\theta \pm \frac{\pi}{2}\right)\cdot\cos\left(\beta + \frac{\pi}{2}\right)\\ &\propto \pm\sin(\theta)\cdot\sin(\beta)\,.\end{aligned}$$

Therefore, it could be used as a second feedback for the phase of the LO, since the sine vanishes precisely for the angles of the amplitude quadrature. A switching between these two locks allowed to select the detected quadrature.

3.5 RECONSTRUCTION OF THE COVARIANCE MATRIX

With the detection of arbitrary quadrature angles and amplitudes we can now reconstruct the covariance matrix of the signal input at the homodyne detector. This is of special interest in the case of multimode Gaussian states for which the covariance matrix describes all statistical properties. The following protocol for reconstruction is described in [DGu10Th] for two modes A and B. An extension to n modes is straightforward.

RECONSTRUCTION PROTOCOL

I A and B simultaneously measure the amplitude quadrature. This allows to calculate $\langle \hat{X}_A \hat{X}_B\rangle$ as well as $\langle \hat{X}_A^2\rangle$ and $\langle \hat{X}_B^2\rangle$ from a series of such measurements.

II A and B simultaneously measure the phase quadrature. This allows to calculate $\langle \hat{P}_A \hat{P}_B\rangle$ as well as $\langle \hat{P}_A^2\rangle$ and $\langle \hat{P}_B^2\rangle$.

III A measures the amplitude quadrature and B simultaneously the phase quadrature. This allows to calculate $\langle \hat{X}_A \hat{P}_B\rangle$.

IV A measures the phase quadrature and B simultaneously the amplitude quadrature. This allows to calculate $\langle \hat{P}_A \hat{X}_B\rangle$.

V Both A and B measure a linear combination of amplitude and phase quadrature, for example at 45°. Via the connection [Sam12]

$$\langle \hat{X}_{\pi/4}^2\rangle = \frac{1}{2}\left(\langle \hat{X}^2\rangle + \langle \hat{X}\hat{P} + \hat{P}\hat{X}\rangle + \langle \hat{P}^2\rangle\right)$$

this allows to calculate $\langle \hat{X}_A \hat{P}_A\rangle$ and $\langle \hat{X}_B \hat{P}_B\rangle$.

With the calculated values the covariance matrix is fully reconstructed and allows to investigate the properties of the state based on γ. Note that the fifth step is not mandatory in all circumstances. As long as $\hat{X}$ and $\hat{P}$ are measured perfectly orthogonal to each other, the covariance for the two operators of the same mode vanish identically anyway for all vacuum states. Therefore, in the application of this protocol in Chapter 5 a partial tomography was performed and step V was omitted. Note furthermore that the reconstruction of the covariance matrix is not allowed in quantum key distribution (QKD) protocols with security against arbitrary attacks, as these do not allow to assume the Gaussianity of the distributed state. Therefore, the reconstruction was not performed in Chapter 6.

4

THE NOTION OF ENTANGLEMENT

4.1 THE EINSTEIN-PODOLSKY-ROSEN PARADOX

In a seminal publication in 1935 A. Einstein, B. Podolsky and N. Rosen (EPR) considered the question of whether the quantum mechanical description of reality could be complete or whether some underlying process explains the statistics by hitherto *hidden variables* [Ein35]. As we have seen in Section 2.1.3 canonically conjugate variables have to fulfill the Heisenberg uncertainty relation, hence, no simultaneous exact description of the appertaining observables is possible. Now EPR invented a sophisticated *gedanken* experiment accompanied by a philosophical argumentation to show that under certain circumstances the relation is violated and an exact description might be hidden under the quantum noise.

Suppose two quantum particles that interacted at a certain point in space and time, are sent to two observers, Alice and Bob, without further interaction. Then we cannot describe the states of the two subsystems individually after the interaction [Ein35] which is what E. Schrödinger named *entanglement* in response to EPR's paper [Srö35]. Such an individual or *local* description only becomes possible if a measurement is performed that reduces the wave functions, i.e. projects the whole system onto a specific (pure) state corresponding to the outcome of the measurement. Then the state can be written as a superposition of all outcomes weighted with their probability,

$$|\Psi\rangle = \sum_n c_n |\psi_n\rangle_A \otimes |u_n\rangle_B .$$

Here $|\psi_n\rangle_A$ is a basis of the eigenstates of an operator $\hat{O}_1$ applied to Alice's subsystem, while $|u_n\rangle_B$ is a corresponding normalized (not necessarily orthogonal) set of states at Bob's subsystem [Cac09]. But Alice is not restricted to measuring $\hat{O}_1$ and the state can also be written as

$$|\Psi\rangle = \sum_s c'_s |\varphi_s\rangle_A \otimes |\nu_s\rangle_B ,$$

for $|\varphi_s\rangle_A$ being a basis of eigenstates of an operator $\hat{O}_2$ and corresponding $|\nu_s\rangle_B$. This means that, depending on which measurement Alice performs, the state is reduced to one of the $|\psi_j\rangle_A \otimes |u_j\rangle_B$ states or one of the $|\varphi_k\rangle_A \otimes |\nu_k\rangle_B$ states.

Now EPR assumed $\hat{O}_1 = \hat{x}$ and $\hat{O}_2 = \hat{p}$, the position and the momentum operator. The canonical conjugation of the operators guarantees that Bob's set of states for every possible outcome x on Alice's side is different from those for every possible outcome p at Alice [Cac09]. This is because non-commuting operators do not have an orthonormal basis of simultaneous eigenvectors [Hal13]. Thus, depending on the measurement on Alice's subsystem the state at Bob's side has different wave functions.

Furthermore, EPR made the following argument. A physical quantity is considered to be an element of reality if it can be predicted with certainty. A physical theory is considered to be complete if it contains all elements of reality. Additionally, they implied but did not explicitly state, as it probably seemed just natural to them, that a description of physical quantities is local if the quantities are not changed by some remote operation via superluminal signaling. Now if Alice performs a measurement on her subsystem then, due to locality, there is no way Bob's subsystem can know which measurement was performed. Therefore, as Alice chooses her measurement at random, both states Bob would obtain must have been elements of reality beforehand, of which one gives a precise value for the position and the other a precise value for the momentum. On the other hand the local quantum mechanical descriptions of Alice and Bob always obey the uncertainty relation for position and momentum. Thus, it contradicts a simultaneous reality of both states because they are not predictable with certainty. Therefore, EPR concluded that the quantum mechanical description can not be considered complete.

The effect of the projection on different states of Bob's subsystem was later named *steering* by E. Schrödinger [Srö35]. He believed in the completeness of quantum mechanics but neither could he find a flaw in EPR's argumentation. This is why he named the phenomenon a *paradox* [Srö35]. Moreover he examined the process of entanglement (see Section 4.2.1) showing that the steering effect is caused by the disentanglement by measurement (see Section 4.2.3). Although the entanglement present in the system described by EPR could have been explained by local hidden variables, carrying the "true" information about the measurement outcomes, Schrödinger rejected this possibility (maybe by intuition [Cac09]) and named steering "a necessary and indispensable feature" [Srö36] of quantum mechanics.

Nowadays the steering effect has been demonstrated in a variety of experiments [Ou92, Zha00, Sil01, Sor02, Bow03a, Lau05, Tak06, Kel08, DAu09, Sau10, Hag11, Ebe11, Hän12, Smi12, Wit12, Ebe13b]. Most of these experiments used continuous variable two-mode squeezed states and certified the presence of steering through a violation of the EPR-Reid criterion. This inequality was developed by M. Reid to adapt the original argumentation by EPR for position and momentum to the field quadratures of an electromagnetic wave as their quantum optical counter parts [Rei89]. Its applicability to quantum optical experiments made it one of the most important criteria to certify the presence of entanglement. In more recent publications by H. Wiseman and co-workers it was shown that any steering criterion can by derived from fundamental Heisenberg uncertainty-like constraints on the statistical description of the measurement results [Wis07, Cac09]. In this context the EPR-Reid criterion is a special case which gives a tight bound for the variables Reid had under consideration in her original publication.

In this chapter we will give an introduction to the theoretical description of entanglement based on references [Wis07] and [Cac09]. We will then give a thorough examination of EPR steering in the Gaussian regime and show that the directionality of this class of entanglement leads to the existence of one-way steering.

4.2 CLASSIFICATION OF ENTANGLEMENT

4.2.1 *Genuine Entanglement*

A state with density operator $\hat{\rho}$ on a Hilbert space $\mathcal{H} = \mathcal{H}^{(A)} \otimes \mathcal{H}^{(B)}$ is called *separable* if the density operator can be written as a convex combination

$$\hat{\rho} = \sum_{\lambda} p_{\lambda} \hat{\rho}_{\lambda}^{(A)} \otimes \hat{\rho}_{\lambda}^{(B)}.$$

The probabilities p_{λ} for the preparation of state λ have to sum up to unity and the density operators $\hat{\rho}_{\lambda}^{(A,B)}$ describe the state of the subsystem on the respective Hilbert subspace. If it can not be separated like this the state is called *entangled*.

We can rewrite this condition in terms of a probability description for the measurement outcomes [Cac09]. The probability to find the state $\hat{\rho}_{\lambda}^{(A)}$ in $|x\rangle$ when measuring X is given by the expectation value of a projector $\Pi_X^x = |x\rangle\langle x|$, where $|x\rangle$ is an eigen state of $\hat{X}$ with eigenvalue x,

$$P_Q(x|X, \lambda) = \mathrm{tr}\left(\Pi_X^x \hat{\rho}_{\lambda}^{(A)}\right),$$

and similar for y and $\hat{\rho}_{\lambda}^{(B)}$. Here the subscript Q denotes a probability that conforms with quantum mechanics, as it was derived from a density operator. In particular, it obeys the uncertainty relation. With this the probability to find x and y when measuring X and Y on the respective subsystem becomes

$$\begin{aligned}P(x,y|X,Y) &= \mathrm{tr}\left((\Pi_X^x \otimes \Pi_Y^y)\sum_\lambda p_\lambda \hat{\rho}_\lambda^{(A)} \otimes \hat{\rho}_\lambda^{(B)}\right)\\ &= \sum_\lambda p_\lambda \mathrm{tr}\left(\Pi_X^x \hat{\rho}_\lambda^{(A)} \otimes \Pi_Y^y \hat{\rho}_\lambda^{(B)}\right)\\ &= \sum_\lambda p_\lambda \mathrm{tr}\left(\Pi_X^x \hat{\rho}_\lambda^{(A)}\right) \mathrm{tr}\left(\Pi_Y^y \hat{\rho}_\lambda^{(B)}\right)\\ &= \sum_\lambda p_\lambda P_Q(x|X,\lambda) P_Q(y|Y,\lambda).\end{aligned}$$

We see that λ takes the role of a hidden variable that explains any correlations between the measurements. A state is called entangled exactly if we cannot find such a description of the occurring probabilities that can be determined by a statistical analysis of repeated measurements on identically prepared states. An *entanglement criterion* is any constraint that can be derived from this probability description. For example the Duan criterion [Dua00]

$$\mathrm{Var}(a\hat{X}_A - \frac{1}{a}\hat{X}_B) + \mathrm{Var}(a\hat{P}_A + \frac{1}{a}\hat{P}_B) \geqslant 2\left(a^2 + \frac{1}{a^2}\right), \qquad a \in \mathbb{R}^+ \quad (4.1)$$

is a necessary and sufficient condition for two-mode states to be entangled in their field quadratures, if it is violated.

4.2.2 *Violation of a Bell Inequality*

We can relax the condition for the local probabilities to be derivable from a density operator and try to describe the occurring probabilities for the measurement results with any distribution,

$$P(x,y|X,Y) = \sum_\lambda p_\lambda P(x|X,\lambda) P(y|Y,\lambda).$$

This is a purely classical description, i.e. we try to explain the correlations that are observed with a classical model. In this case λ is an actual hidden variable. It contains all information that predetermines the measurement results which would be hidden in a quantum mechanical description. Hence, this is what EPR assumed to be underlying the entanglement they described, as they stated that quantum mechanics is incomplete. For example a two-mode squeezed state that violates the criterion (4.1) and, therefore, is not describable by a quantum model, is describable by a classical model, at least as far as quadrature measurements are concerned. This is because the Wigner function of such a state is positive semi-definite and can be seen as probability distribution in phase space, therefore acting as a classical model.

Any state whose correlations cannot be explained by a classical model violates at least one so-called Bell inequality. These inequalities were introduced by John Bell in 1964 to clarify the discussion on the EPR argument [Bel64]. He showed that for any classically correlated system certain bounds on the probabilities for joint measurement results can be found. For example the probability that a sock survives a washing at 0°C but not at 45°C plus the probability that a sock survives a washing at 45°C but not at 90°C is not less than the probability that a sock survives a washing at 0°C but not at 90°C [Bel81]. This is obvious as all socks from the third group are at least in the first or the second group. With a similar idea inequalities for quantum systems can be constructed, for example for Stern-Gerlach measurements on entangled electron spins under different angles [Bel81] or, similarly, projections of entangled photon pairs onto orthogonal polarizations. To date such inequalities have been violated in a variety of experiments [Asp81, Tit98, Wei10] which proves that there cannot be any classical description underlying that explains the correlations. Of course these experiments are subject to many subtleties as, for example, one has to make sure that the observers/measurement devices are space like separated and the random choice of the measurement is made after the state was generated. But very recently the first violation of a Bell inequality without any loopholes was demonstrated [Hen15] which finally rules out the possibility of hidden variables explaining quantum mechanics.

Bell also concluded the following possibilities for the nature of reality [Bel81]:

I Following EPR, quantum mechanics may be in-complete and there should be an underlying description for specific experimental situations that would make the theory complete. But since the Bell inequality can convincingly be violated in experiments, we know that at least for these situations there cannot be such a description. Note that quantum theory can very well reproduce all experimental data and predict the occurring correlations which we will call the *empiricality* of the theory. Hence, abandoning the Einsteinian point of view, we could very well say: of course quantum mechanical description of reality is complete.

II There may be causal influences going faster than light. But this would violate the theory of special relativity which has been experimentally verified many times and is also very successful in connection to other physical theories. Therefore, it is reasonable to assume what we will call the *local causality* of the theory, i.e. the fact that we can describe a system without knowing anything about remote (and maybe entangled) systems and operations on those.

III Following N. Bohr, quantum mechanics may be non-realistic, i.e. there is “no reality below some classical, macroscopic level” [Bel81]. But this obviously contradicts what we will call the *classicality* of the theory, i.e. the existence of a list of properties containing all information on a system or subsystem.

The three premises *empiricality*, *local causality* and *classicality* were contrasted in [Duh10] (note that they are not equivalent to the possibilities I-III), and it was shown that they cannot be fulfilled simultaneously in a fundamental physical theory. Since the *empiricality* and the *local causality* have hitherto never been contradicted, we are left with abandoning the *classicality*. Therefore, the personal opinion of the author is that we should go with possibility III, without claiming completeness of the discussion. This does not mean that there is no reality at all but that a quantum state has no reality in the classical sense before we measured it to be a certain state. The different states of quantum systems described in the wave function are nothing more but possibilities. Especially, they do *not* have simultaneous reality.

4.2.3 *Einstein-Podolsky-Rosen Steering*

The third class of entanglement we will describe is sort of intermediate between the previous two. Instead of describing both local systems with classical distribution we can do this for just one of the two parties,

$$P(x, y|X, Y) = \sum_{\lambda} p_{\lambda} P(x|X, \lambda) P_{Q}(y|Y, \lambda). \tag{4.2}$$

This could for example refer to a situation where Bob on his end “trusts” quantum mechanics, i.e. he knows that the quantum mechanical description is complete and he also knows that he is performing a correct measurement and not “cheating” in any way. On the other hand he does not know whether Alice is actually honest and prepares a correct quantum state or whether she is trying to generate the entanglement-like correlations by some classical process. Therefore, we describe Alice’s probability classically and Bob’s probability quantum mechanically [Cac09].

The joint probability of x and y given that X and Y are measured can again be written as the expectation value of a projector Π_{Y}^{y} defined as before,

$$P(x, y|X, Y) = \operatorname{tr}\left(\Pi_{Y}^{y} \hat{\rho}_{\lambda|X}^{(B)}\right).$$

Here

$$\hat{\rho}^{(B)}_{\lambda|X} = \sum_{\lambda} P(x|X,\lambda) p_{\lambda} \hat{\rho}^{(B)}_{\lambda} \tag{4.3}$$

is the reduced state Bob receives if Alice obtained x by measuring X. As we allow Alice's probabilities to be classically described, Equation (4.3) means that Bob's state can be locally decomposed into some quantum states defined by λ,

$$\hat{\rho}^{(B)} = \sum_{\lambda} p_{\lambda} \hat{\rho}^{(B)}_{\lambda}.$$

In comparison to the hidden variable model we have seen previously, this can be called a *hidden state* model describing the probabilities of Bob's measurement results [Wis07]. If and only if a state does not allow such a decomposition is it called a steerable state [Cac09]. In that case it seems like Alice's measurement steered Bob's subsystem into a specific state that is defined more precisely than a quantum mechanical decomposition would allow. We will explain this in more detail for the specific case of two-mode squeezed states in the next section.

Any constraint that can be derived from Equation (4.2) is called a steering inequality. For example we can take a look at the conditional probability of Bob finding y given Alice has found x (compare Equation (2.39) and Reference [Cac09])

$$\begin{aligned} P(x|y) &= \sum_{\lambda} \frac{p_{\lambda} P(x|\lambda)}{P(x)} P_Q(y|\lambda) \\ &= \sum_{\lambda} P(\lambda|x) P_Q(y|\lambda), \end{aligned}$$

where we have left out the measurement settings for simplicity. Now suppose Bob's observables have a non-vanishing commutator, i.e. his results must fulfill the Heisenberg uncertainty relation. Then, by a similar calculation as in Section 2.1.3, we can find a lower bound on the conditional uncertainties [Cac09],

$$\Delta_{\text{cond}} y_1 \Delta_{\text{cond}} y_2 \geqslant \frac{1}{2} \sum_{\lambda} p_{\lambda} |\langle [\hat{Y}_1, \hat{Y}_2] \rangle_{\lambda}|,$$

where

$$\Delta^2_{\text{cond}} y = \sum_{x} P(x) \Delta^2(y|x)$$

is the variance of the conditional distribution. If we now replace $\hat{Y}_1$ and $\hat{Y}_2$ by the quadrature operators we find the uncertainty relation

$$\begin{aligned}\Delta_{\text{cond}} X^{(B)} \Delta_{\text{cond}} P^{(B)} &\geqslant \frac{1}{2} \sum_{\lambda} p_{\lambda} \cdot 2 \\ &= 1.\end{aligned}$$

Note that the expectation value is independent of Alice's measurement choice and, therefore, independent of λ. By taking the square of this equation we write this in the more common way in terms of the conditional variances,

$$\mathrm{Var}_{B|A}(X)\mathrm{Var}_{B|A}(P) \geqslant 1. \tag{4.4}$$

Here the subscript of the variances explicitly states that Bob conditions on Alice. This means $\mathrm{Var}_{B|A}(X)$ is the variance of Bob's measurement result $X^{(B)}$ given that Alice's result was $X^{(A)}$. This inequality is the EPR-Reid criterion as we will show in Section 4.4. If it is violated the state shows steering from Alice to Bob.

Obviously the conditional variances can be defined vice versa which would interchange the roles ob Alice and Bob. If the similar constrain obtained for this situation is violated the state also shows steering from Bob to Alice. But the question arises whether there are states that show steering only in one direction [Wis07]. We will, therefore, investigate this situation now in more detail for Gaussian states.

4.3 DIRECTIONALITY OF GAUSSIAN STEERING

In the following we will present the description of Gaussian steering that was developed in this thesis and published in [Hän12]. As we have seen in Section 4.2, steering is strictly stronger than entanglement and strictly weaker than the violation of a Bell inequality, i.e. steering does not imply the violation of any Bell inequality, while the violation of at least one Bell inequality immediately implies steering in both directions [Wer89] as shown in Fig. 4.1. In contrast to entanglement and Bell tests, Alice and Bob have certain roles in the steering scenario which are not interchangeable. This intrinsic asymmetry raises the question [Wis07] whether there are physical states certifying steering only in one direction for arbitrary observables. This *one-way* steering would lead to the peculiar situation that two experimenters measuring the same observables on their subsystems would describe the same shared state in qualitatively different ways. For the Gaussian regime, i.e. for Gaussian state preparation and Gaussian measurements, we can answer this question positively. In a pioneering paper by H.-A. Bachor and co-workers, two-way steering with an asymmetry in the steering strengths was observed [Wag08]. Their theoretical analysis proposes a possible extension of their setup towards observing one-way steering. And in a theoretical work, an intra-cavity nonlinear coupler was proposed to generate Gaussian one-way steering [Mil10]. We will now show that the generation of one-way steering in the Gaussian regime is possible with two-mode squeezed states.

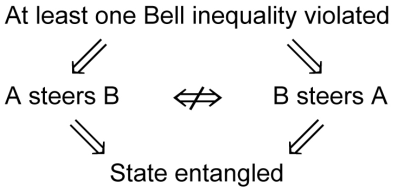


Figure 4.1: Implications of inseparability criteria. A violation of at least one Bell inequality implies steering in both directions. If steering is only present in one direction, no Bell inequality can be violated. But any certification of steering implies that the state is entangled. The converse implications are not true: Entangled states are not necessarily steerable states and steering does not imply the violation of a Bell inequality. A similar figure was published in [Fra12Th].

To analyze the steering scenario, we start with the bipartite situation in which Alice sends quantum states to Bob. If Bob locally observes a mixed state, this can be decomposed into convex combinations of purer states. These decompositions can be seen as more precise descriptions of his system. Indeed, any information that Alice has about the state will give a decomposition into conditional states which are purer than Bob's mixed state. This can be seen in the upper panels of Fig. 4.2 for the case of a Gaussian system and quadrature measurements. Two exemplary measurement results X_1 and P_1 which Alice obtains on her system are depicted by the green and blue line. The related conditional states on Bob's side are shown by the accordingly colored ellipses. These are states of the form in Equation (4.3), i.e. the reduced state that Bob receives after Alice obtained X_1 and P_1, respectively. Note that we can describe them as squeezed coherent states (see Section 2.3.3) with a reduced purity due to optical loss. For all measurement results Alice can obtain, these ellipses will have the same shape and just their position in phase space will be different. So Alice's X- and P-results give two different decompositions of Bob's system.

The argument by EPR and Schrödinger is now, that measurements on Alice's side should not influence Bob's system. So the decomposition of Bob's state should be independent of Alice's choice of observable. This implies that the conditional decompositions, which depend on Alice's choice, should have a common finer-grained decomposition, which does not depend on Alice's choice. Such a refinement should show an X-uncertainty that is at most as large as the one of Bob's X-conditional state (green arrow). At the same time, it should show a P-uncertainty that is at most as large as the one of Bob's

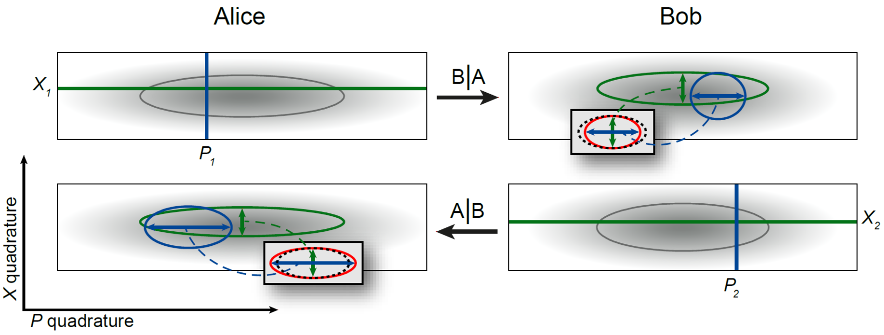


Figure 4.2: Gaussian one-way EPR steering visualized in phase space. The local Wigner functions of a bipartite quantum state are represented by the gray ellipses as well as by the background clouds. In the upper panels steering from Alice to Bob is shown. Two exemplary measurement results X_1 and P_1 are depicted by the green and blue line. The appertaining conditional states at Bob's system are depicted by the accordingly colored ellipses, with their uncertainties in the respective quadratures given by the arrows. Any hypothetical common refinement, depicted by the red ellipse in the inset, may not exceed these uncertainties. Otherwise, it would violate the Heisenberg Uncertainty Relation, shown in black. In the lower panels a non-steering situation from Bob to Alice is shown. In this case a common refinement is possible, i.e. the uncertainty relation is not violated.

P-conditional state (blue arrow). We have depicted this hypothetical state in the inset as a red ellipse. But this state would clearly violate the Heisenberg uncertainty relation, depicted by the black dotted ellipse, and is therefore forbidden within quantum mechanics.

The absence of a common refinement leads to the conclusion that Alice's choice of observable somehow changes the states of Bob's system, which Schrödinger called steering. More formally, we define a bipartite state to be steerable with respect to Alice's observables, if the resulting conditional state decompositions of Bob's state do not allow a common refinement. We say that the state is steerable from Alice to Bob, if there are some observables for which it is steerable. This description of steering is close to Schrödinger's original presentation and is equivalent to the definition based on the existence of certain classical models as given in Section 4.2.3.

The converse scenario is shown in the lower panels of Fig. 4.2 for the same quantum state as in the upper panels. The two measurement results obtained by Bob give related conditional states on Alice's side and permit two different decompositions. But this time these conditional decompositions do have a common refinement that does not violate the uncertainty relation. So, in terms of Schrödinger, Bob's measurements do not steer Alice's system, as an underlying description with pure states is possible. Therefore, the state analyzed in Fig. 4.2 shows one-way steering. In Section 5.2 we will show that such a state can actually be experimentally generated. The criteria to certify one-way steering are given in Equation (4.7) and (4.8) and will be derived in the following.

4.4 TWO-MODE SQUEEZED STATES AND THE EPR-REID CRITERION

Since we consider the Gaussian regime, our vivid description of steering is equivalent to the desciption by Reid [Rei89]. Her definition is based on Heisenberg Uncertainty Relations for conditional measurements of the amplitude and phase quadrature X and P of light fields which give a constraint for a state to show steering, as shown in Section 4.2.3. Reid originally formulated steering as an information theoretical task for Alice to infer Bobs measurement result based on her own result. As for the vacuum states under consideration the expectation values vanish, a good estimation for Alice is to multiply her X value by some real factor g and her P value by some factor h. With this we can define the inferred variances

$$\begin{aligned} \mathrm{Var}_{\mathrm{inf}}(X_B) &:= \mathrm{Var}(X_B + g \cdot X_A), \\ \mathrm{Var}_{\mathrm{inf}}(P_B) &:= \mathrm{Var}(P_B + h \cdot P_A). \end{aligned} \tag{4.5}$$

By choosing the factor g and h appropriately Alice can minimize these variances. Now Reid showed that steering from Alice to Bob is present if the product of these optimally inferred variances violates the uncertainty relation for X_B and P_B, i.e. the EPR-Reid criterion that has to be violated reads

$$\mathrm{Var}_{\mathrm{inf,min}}(X_B) \cdot \mathrm{Var}_{\mathrm{inf,min}}(P_B) \geqslant 1.$$

A violation of this inequality is exactly what is shown in the upper inset of Fig. 4.2 where the red ellipse is smaller than the black. Conversely, Bob can try to infer Alice's measurement result which give a similar criterion

$$\mathrm{Var}_{\mathrm{inf,min}}(X_A) \cdot \mathrm{Var}_{\mathrm{inf,min}}(P_A) \geqslant 1.$$

If this is violated steering from Bob to Alice is certified.

Now Wiseman and co-workers showed that the inferred variances have a lower bound given by the conditional variances [Wis07, Cac09]. Hence, the conditioning of Bob's measurements on Alice's gives the minimal variance for the inference Alice performs and vice versa. With this we end up precisely with the multiplicative steering condition from Equation (4.4). Although in general the conditional variances might not be accessible in an experiment for the case of two-mode squeezed states we can explicitly give them in terms of the covariance matrix, as the latter fully describes the state.

A two-mode squeezed state is generally produced by superimposing two orthogonally squeezed states at a 50:50 beam splitter. Assuming identical squeezing factors for both input states and a perfect alignment of the squeezing angles with the amplitude and the phase quadrature, respectively, the covariance matrix of such a state reads

$$\gamma = \begin{pmatrix} \cosh 2r & 0 & \sinh 2r & 0 \\ 0 & \cosh 2r & 0 & -\sinh 2r \\ \sinh 2r & 0 & \cosh 2r & 0 \\ 0 & -\sinh 2r & 0 & \cosh 2r \end{pmatrix}. \tag{4.6}$$

Let us for a moment forget about the actual values of the entries and just observe that the matrix contains a lot of zeros. Therefore, its inverse is easy to determine,

$$\gamma^{-1} = \begin{pmatrix} \frac{\langle \hat{X}_A^2 \rangle}{\lambda_1} & 0 & -\frac{\langle \hat{X}_A \hat{X}_B \rangle}{\lambda_1} & 0 \\ 0 & \frac{\langle \hat{P}_A^2 \rangle}{\lambda_2} & 0 & -\frac{\langle \hat{P}_A \hat{P}_B \rangle}{\lambda_2} \\ -\frac{\langle \hat{X}_A \hat{X}_B \rangle}{\lambda_1} & 0 & \frac{\langle \hat{X}_B^2 \rangle}{\lambda_1} & 0 \\ 0 & -\frac{\langle \hat{P}_A \hat{P}_B \rangle}{\lambda_2} & 0 & \frac{\langle \hat{P}_B^2 \rangle}{\lambda_2} \end{pmatrix},$$

with

$$\lambda_1 = \langle \hat{X}_A^2 \rangle \langle \hat{X}_B^2 \rangle - \langle \hat{X}_A \hat{X}_B \rangle^2,$$
$$\lambda_2 = \langle \hat{P}_A^2 \rangle \langle \hat{P}_B^2 \rangle - \langle \hat{P}_A \hat{P}_B \rangle^2.$$

From this we can calculate the probability density of the state. For simplicity we will restrict to the amplitude quadratures, the calculation for the phase quadratures goes analogously. We can do so, because the X- and P-measurements are uncorrelated and the description can be split up. The Gaussian distribution we find is

$$w(X_A, X_B) = \frac{1}{2\pi\sqrt{\lambda_1}} \exp\left[\frac{1}{2\lambda_1}\left(\langle \hat{X}_B^2 \rangle X_A^2 - 2\langle \hat{X}_A \hat{X}_B \rangle X_A X_B + \langle \hat{X}_A^2 \rangle X_B^2\right)\right]$$

To get the conditional density $w_{B|A}(X_B)$ we have to divide this by the marginal distribution for Alice (compare Section 2.4.2),

$$w_A(X_A) = \int_{-\infty}^{\infty} w(X_A, X_B) dX_B = \frac{1}{\sqrt{2\pi\langle \hat{X}_A^2 \rangle}} \exp\left[-\frac{X_A^2}{2\langle \hat{X}_A^2 \rangle}\right].$$

With this we find

$$\begin{aligned} w_{B|A}(X_B) &= \frac{w(X_A, X_B)}{w_A(X_A)} \\ &= \frac{1}{\sqrt{2\pi\frac{\lambda_1}{\langle \hat{X}_A^2 \rangle}}} \exp\left[-\frac{\langle \hat{X}_A^2 \rangle}{2\lambda_1}\left(-\frac{\langle \hat{X}_A \hat{X}_B \rangle}{\langle \hat{X}_A^2 \rangle} X_A + X_B\right)^2\right]. \end{aligned}$$

By comparing the conditional density with the definition of a Gaussian distribution in Equation (2.40) we see that the mean and the standard deviation are

$$\mu = \frac{\langle \hat{X}_A \hat{X}_B \rangle}{\langle \hat{X}_A^2 \rangle} X_A,$$
$$\sigma = \sqrt{\frac{\lambda_1}{\langle \hat{X}_A^2 \rangle}} = \sqrt{\langle \hat{X}_B^2 \rangle - \frac{\langle \hat{X}_A \hat{X}_B \rangle^2}{\langle \hat{X}_A^2 \rangle}}.$$

Taking the square of the standard deviation and turning back to our previous notation we get the conditional variance (the variance of the conditional density) for Bob's amplitude measurements,

$$\mathrm{Var}_{B|A}(X_B) = \mathrm{Var}(X_B) - \frac{(\mathrm{Cov}(X_A, X_B))^2}{\mathrm{Var}(X_A)}$$

Correspondingly for $\hat{P}_B$ we get

$$w_{B|A}(P_B) = \frac{1}{\sqrt{2\pi \frac{\lambda_2}{\langle \hat{P}_A^2 \rangle}}} \exp\left[-\frac{\langle \hat{P}_A^2 \rangle}{2\lambda_2} \left(-\frac{\langle \hat{P}_A \hat{P}_B \rangle}{\langle \hat{P}_A^2 \rangle} P_A + P_B \right)^2 \right],$$

and

$$\mathrm{Var}_{B|A}(P_B) = \mathrm{Var}(P_B) - \frac{(\mathrm{Cov}(P_A, P_B))^2}{\mathrm{Var}(P_A)}.$$

Furthermore, the conversely conditioned variances are simply given by interchanging all A and B in the equations.

To find the optimally inferred variances from Equation (4.5) we can differentiate them by g and h, respectively, and find that they are minimized precisely by the conditional variances. The conditional variance product can be given in an even simpler fashion, namely in terms of the symplectic invariants of the covariance matrix (compare Equations (2.44)). The criterion that has to be violated to certify steerability from Alice to Bob then reads [Fra12Th]

$$\mathrm{Var}_{B|A}(X_B) \cdot \mathrm{Var}_{B|A}(P_B) = \frac{I_4}{I_1} \geqslant 1, \tag{4.7}$$

and correspondingly for steerability from Bob to Alice

$$\mathrm{Var}_{A|B}(X_A) \cdot \mathrm{Var}_{A|B}(P_A) = \frac{I_4}{I_2} \geqslant 1. \tag{4.8}$$

Since the symplectic invariants are the determinants and sub-determinants of the covariance matrix and as these are inversely connected to the purity of the described system or subsystem, we can interpret the violation of these criteria as the statement that the subsystem of Alice and Bob, respectively, is less pure than the complete state.

Finally, we can plug in the values from the covariance matrix in Equation (4.6) and find

$$\begin{aligned}\mathrm{Var}_{B|A}(X_B)\cdot\mathrm{Var}_{B|A}(P_B) &= \left(\cosh 2r - \frac{\sinh^2 2r}{\cosh 2r}\right)^2\\ &= \frac{1}{\cosh^2 2r}\\ &= \mathrm{Var}_{A|B}(X_A)\cdot\mathrm{Var}_{A|B}(P_A)\end{aligned}$$

Hence, a perfect two mode squeezed state shows steering with equal strength in both directions for any non-zero squeezing.

Now we can go away from the idealized experimental scenario and change the parameters. For example in the experiment we will normally not have identical squeezing from both sources, so we have to introduce a second, independent squeezing factor. These two squeezing factors can be very different and the state will still show two-way steering. In fact we can even go to the extreme case and set one squeezing factor to 0, as we will do in the experiments in Chapter 5. Furthermore, the detection efficiencies of Alice and Bob will never be 1. Therefore, our analysis should include individual optical loss for both modes. Note that optical loss before the superposition at the beam splitter acts as symmetric loss on both modes, i.e. we do not have to model it individually but just include it in both detection efficiencies. A general derivation of the covariance matrix as well as of the left-hand sides of the EPR-Reid criteria is given in Appendix A.2, here we will just give some results for specific scenarios. A detailed description of the construction of covariance matrices can be found in [Duh15Th].

An exemplary covariance matrix under experimental conditions could look like

$$\gamma = \begin{pmatrix} 21.84 & 0 & 21.65 & 0\\ 0 & 25.51 & 0 & -25.92\\ 21.65 & 0 & 21.66 & 0\\ 0 & -25.92 & 0 & 26.54 \end{pmatrix}. \tag{4.9}$$

The experimental parameters are approximately squeezing factors of 2.02 and 1.93, respectively, an optical loss of 9.5% for Alice and 8% for Bob and a beam splitter reflectivity of 0.506. This matrix can be reconstructed from measurements on a two-mode squeezed state following the protocol in Section 3.5. A summary of such measurements is shown as an example in the phase space plots in Figure 4.3. The four plots depict the correlation block of the covariance matrix. The correlation in the X-quadrature and the anti-correlation in the P-quadrature are clearly visible in the upper left and the lower right, respectively. Roughly speaking the value of the covariance is determined by the difference of the semi-major and the semi-minor axis of the ellipses. For comparison a vacuum state is shown in black. The two plots in the upper right and lower left do not show any correlation, as the distribution is symmetric in all quadratures. They just show parametrically amplified vacuum noise. All distribution are Gaussian, as we would expect in comparison with Equation (2.41).

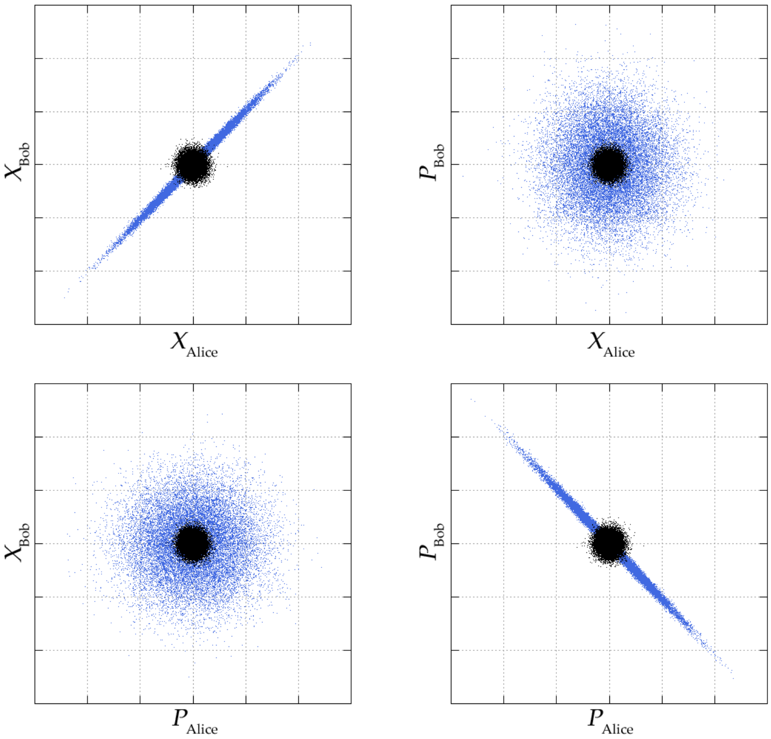


Figure 4.3: Quadrature correlations of a two-mode squeezed state. The correlations in the X-quadrature and the anti-correlation in the P-quadrature are visible in the two plots in the upper left and the lower right. The other two plots show the uncorrelatedness of the orthogonal quadratures. A vacuum state is shown in black as reference.

If we calculate the Reid criteria from this covariance matrix, we find

$$\frac{I_4}{I_1} = 0.0448 \ll 1,$$
$$\frac{I_4}{I_2} = 0.0434 \ll 1,$$

and see that the state significantly shows steering in both directions. We also see that the criterion values are slightly different for Alice and Bob. A detailed investigation shows that this is due to the slightly asymmetric optical loss.

To see the direct connection between a one-sided optical loss and the steerability for the two parties, let as go back to a setting of equal squeezing factors and a perfect 50:50 beam splitter. Furthermore, we assume Alice to have 100% detection efficiency and just introduce a variable loss ε on Bob's side. Then the covariance matrix reads

$$\gamma = \begin{pmatrix} c & 0 & \sqrt{1-\varepsilon}s & 0 \\ 0 & c & 0 & -\sqrt{1-\varepsilon}s \\ \sqrt{1-\varepsilon}s & 0 & (1-\varepsilon)c+\varepsilon & 0 \\ 0 & -\sqrt{1-\varepsilon}s & 0 & (1-\varepsilon)c+\varepsilon \end{pmatrix},$$

with

$$c = \cosh 2r,$$
$$s = \sinh 2r.$$

We see that the optical loss on Bob's mode will only change I_4 and I_2 but not I_1. Therefore, the left hand sides of the two steering criteria develop differently for increasing loss,

$$\frac{I_4}{I_1} = \frac{1 + 4\varepsilon \sinh^2 r + 4\varepsilon^2 \sinh^4 r}{\cosh^2 2r},$$
$$\frac{I_4}{I_2} = \frac{1 + 4\varepsilon \sinh^2 r + 4\varepsilon^2 \sinh^4 r}{\cosh^2 2r - 4\varepsilon \sinh^2 r \cosh 2r + 4\varepsilon^2 \sinh^4 r}.$$

The interesting question is now at which optical loss the criteria are no longer violated. By solving the inequalities for ε we find

$$\varepsilon \geqslant \frac{\cosh 2r - 1}{2\sinh^2 r} = 1$$

as the threshold for no steering from Alice to Bob. Hence, Alice will only lose her steerability when the loss on Bob's mode approaches unity and he obtains a pure vacuum. On the other hand, the threshold for no steering from Bob to Alice is found to be

$$\varepsilon \geqslant \frac{\sinh^2 2r}{4\sinh^2 r(1+\cosh 2r)} = \frac{1}{2}.$$

We see that only 50% optical loss on Bob's mode is required till he loses his steerability. Therefore, for $\varepsilon \in [0.5, 1)$ the state shows steering from Alice to Bob but no steering from Bob to Alice. This is precisely what we call a one-way steerable state. Note that the thresholds for ε are completely independent of the squeezing factors as long as $r > 0$. For $r \to 0$ the equations for the thresholds are no longer defined but obviously in this case no threshold can be defined, as there is anyway no steering.

In conclusion we have seen that two-mode squeezed states show EPR steering and that we can verify this by a violation of the Reid criteria. Thereby, the squeezing factor determines the strength of the violation but not whether the criteria are violated at all (except for the trivial case of $r = 0$). Furthermore, we have found that asymmetric optical loss will result in asymmetric violations of the criteria for the different directions. We can find settings where actually one criterion is violated while the other is not. In the next chapter we will present an experimental implementation of these findings and show that Gaussian one-way steering can be observed by homodyne measurements on specifically designed two-mode squeezed states.

5

DEMONSTRATION OF ONE-WAY EINSTEIN-PODOLSKY-ROSEN STEERING

In Chapter 4 we have seen that certain Gaussian states show the effect of one-way steering. In this chapter we will present an experimental realization of these states. To this end two-mode squeezed states were generated which generally are two-way steerable states as long as the detection efficiencies of both parties are sufficiently high. Therefore, one of the entangled modes (say Bob's mode) had to be decohered via a Gaussian channel, thereby lowering Bob's effective detection efficiency of the original entanglement, to generate the specific state depicted in Figure 4.2. The amount of decoherence had to be controllable, as it had to be large enough to forbid steering from Bob to Alice but small enough to still allow steering from Alice to Bob. The presence of steering was verified by the EPR-Reid criteria from Equations (4.7) and (4.8) and matched the theoretical results.

5.1 EXPERIMENTAL PRELIMINARIES

Before going into the details of the experiments we have to summarize some of the experimental techniques used for the implementation. As all experiments in this thesis required continuous-wave (cw) non-classical states carrying continuous variable (CV) entanglement the generation of squeezing and two-mode squeezing was a crucial part common to all experiments.

5.1.1 *Generation of Squeezed States*

Squeezed states are normally generated by parametric down-conversion in a second order non-linear medium ($\chi^{(2)} \neq 0$). The medium is pumped with a strong light field at the second harmonic frequency. A schematic of the process is shown in Figure (5.1). It can be understood as one photon of the pump frequency ω_p exciting the parametric oscillator. This can spontaneously relax by emitting two photons of the fundamental frequency $\omega = \omega_p/2$. More precisely the two photons do not necessarily have to be at the exact fundamental frequency but can have an offset to an upper and lower sideband, where energy conservation requires $\omega_+ + \omega_- = \omega_p$. As we have seen in section 3.4 these two photons are entangled in the frequency domain and yield exactly a squeezed state at the respective sideband frequency. The strength of the squeezing (i.e. the noise reduction below vacuum) depends on the power in the pump field. We will see a direct connection in Equation (5.1).

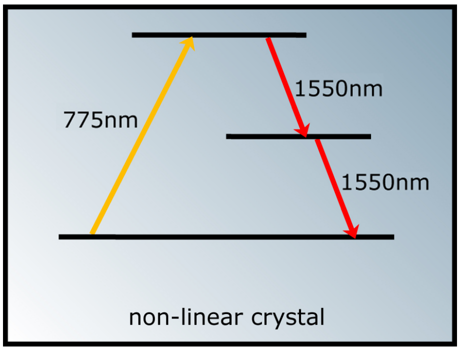


Figure 5.1: Energy levels of parametric down-conversion. The photons of the pump field (775 nm) excite the parametric oscillator in the non-linear crystal. In the relaxation a spontaneous emission of two photons of the fundamental frequency (1550 nm) can happen. This output field is then squeezed due to the correlations between the two photons.

We can describe the process of non-degenerate parametric down conversion by the interaction Hamiltonian [Ger08],

$$H_{\text{int}} = i\hbar\chi^{(2)}\left(\hat{a}_+\hat{a}_-\hat{b}^\dagger - \hat{a}_+^\dagger\hat{a}_-^\dagger\hat{b}\right).$$

Here $\hat{a}_\pm$ are the mode operators of the upper and lower sideband and $\hat{b}$ of the pump field. Now we can assume that the pump is a strong coherent excitation such that its depletion by the process is negligible. Then we can approximate $\hat{b}$ by a complex number β. Using this and the definition of the unitary time evolution from Section 2.1.2, we find

$$\begin{aligned}\hat{U}_{\text{int}}(t) &= \exp\left[-i\hat{H}_{\text{int}}t/\hbar\right]\\ &= \exp\left[\beta^*\chi^{(2)}t\hat{a}_+\hat{a}_- - \beta\chi^{(2)}t\hat{a}_+^\dagger\hat{a}_-^\dagger\right],\end{aligned}$$

where we have exploited the previously defined frequency relations. By associating $\zeta = 2\beta\chi^{(2)}t$ we see that $\hat{U}_{\text{int}}$ becomes the squeezing operator from Equation 2.28. Thereby, we have shown that parametric down conversion produces squeezing. Recalling $\zeta = re^{i\varphi}$ we furthermore see that the amplitude of the pump field $|\beta|$ together with the non-linearity $\chi^{(2)}$ and the interaction time t defines the squeezing factor r, and that the argument of β (i.e. the relative phase of the pump field) defines the squeezing angle φ. Hence, by choosing β the squeezing parameters of the generated state can be controlled.

So far we just have a non-linear medium emitting a squeezed state at a random sideband frequency. To achieve squeezing in a specific spatial and temporal mode we have to put the medium in a cavity. A schematic of the resonators used in this thesis is shown in Figure (5.2). The cavity is formed on the one end by the curved end face of the medium, in this case crystalline periodically-poled potassium titanyl phosphate (PPKTP). The spherical polishing has a radius of curvature (roc) of 12.5 mm and a high reflectivity (HR) coating for 775 nm as well as 1550 nm with a transmission below 300 ppm. The other end of the cavity is formed by an external mirror mounted on a piezo-electric transducer (PZT) to actuate the length of the cavity. This mirror is meniscus shaped with an inner roc of 25 mm and 90% reflectivity coating for 1550 nm. For 775 nm it is anti-reflection (AR) coated, so the pump field just takes one round trip in the cavity without getting enhanced. The mirror reflectivities together with the crystal length and the air gap between crystal and coupling mirror define the properties of the resonator for the fundamental frequency, yielding approximately 60 MHz linewidth and a free spectral range (FSR) of about 3.8 GHz. To minimize the intra-cavity damping the second end face of the crystal is AR coated for both wavelengths. Furthermore, it is plane, so that the waist of the intra-cavity field should be in close proximity to it to avoid diffraction of the mode shape. The waist size and position of the cavity can be tuned by the air gap between crystal and meniscus. Stable configurations are found approximately between 21 mm and 25 mm. Fine tuning of the air gap in the sub tenth millimeter regime can dramatically enhance the conversion efficiency. One reason is that by lengthening the cavity the waist gets smaller and a higher power density in the non-linear medium is achieved. The other reason is mode degeneracy of the Ψ_{00} mode and higher order transversal modes, that can counteract the desired process. Finding a good spot without any degeneracies is actually a matter of luck, as a full mode-spectral description of the cavity is hardly possible. In this experiment a good air gap was found slightly below 24 mm yielding a waist of 48.5 μm just inside the crystal at the plane end face.

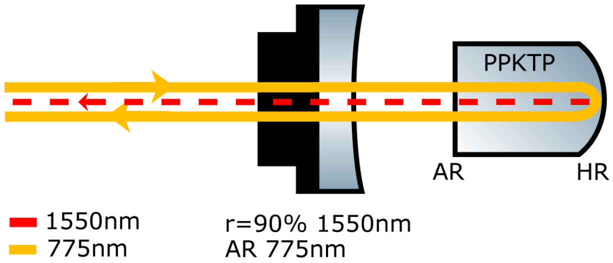


Figure 5.2: Schematic of a squeezed-light source. A strong pump field (775 nm) is coupled into the non-linear crystal (PPKTP). Inside the crystal a squeezed state (1550 nm) is generated. The rear side of the crystal is curved and high reflective (HR) coated while the plane side is anti-reflection (AR) coated for both wavelengths each. The meniscus shaped coupling mirror that closes the resonator has a reflectivity of 90% for the fundamental wavelength. It is AR coated for the pump field such that it just takes one round trip through the crystal.

In the case of the described squeezed light source the achieved reduction of the variance compared to the vacuum can be described by the following formula [Tkn07] ,

$$\mathrm{Var}_{\mathrm{asqz,sqz}} = 1 \pm \eta\gamma \frac{4\sqrt{P/P_{th}}}{(1-\sqrt{P/P_{th}})^2 + 4K(\Omega)^2}. \tag{5.1}$$

Here, η is the detection efficiency of the setup and $\gamma = T/(T+L)$ is the escape efficiency of the cavity, with T the transmissivity of the coupling mirror and L the intra-cavity loss. $K(\Omega) = 2\pi\Omega/\kappa$ is the normalized sideband frequency at which we measure, where $\kappa = c(T+L)/l$ is the cavity decay rate with c the speed of light in vacuum and l the optical cavity round trip length. Note that the speed of light varies between the air gap and the crystal. Therefore, the crystal length has to be multiplied by its index of refraction before calculating l. The most important thing is the dependence on the pump power P. This power has to be normalized by the so-called threshold power P_{th}. This is the light power at which the medium starts to lase for itself, i.e. the conversion from the pump to the fundamental field gets strong enough that a coherent state at the fundamental frequency emerges and induced emission starts. The threshold is, therefore, strongly dependent on the medium parameters, the intra-cavity loss and the mode matching. For the squeezed light source used for the experiments in this chapter a threshold power of 440 mW was achieved.

Finally, the conversion efficiency is also tuned by the phase matching of the fundamental and the second harmonic frequency. As these normally experience a different index of refraction they tend to get out of phase, thereby decreasing the desired conversion effect. In bulk media as for example Mg doped LiNbO3 the birefringence can be used to find a temperature where the effect cancels out over the length of the crystal. In this thesis PPKTP was used, where the periodic poling changes the sign of the second order non-linearity every time the phase shift has reached π. That way an effective phase matching of 67% can optimally be achieved. The disadvantage of a limited optimal phase matching is compensated by a higher non-linearity of KTP compared to LiNbO3, yielding a 2.5 times higher effective non-linearity. Furthermore, the phase matching is less sensitive to temperature fluctuation, making it easier to keep the crystal at the right working point. In this work an optimal phase matching was achieved at about 60°C. At this optimal working point a squeezing of 10 dB below shot noise was measured. A series of squeezing measurements for varying pump power is shown in Figure 5.3 together with the function from Equation (5.1) with the following parameters: $l = 66.6\,\mathrm{mm}$, $T = 0.1$, $L = 0.056$, $\Omega = 5\,\mathrm{MHz}$ and $\eta\gamma = 0.91$.

The pump field for the squeezed light source was produced by second harmonic generation (SHG). This process can be seen as an inversion of the down-conversion. More specifically, it is parametric

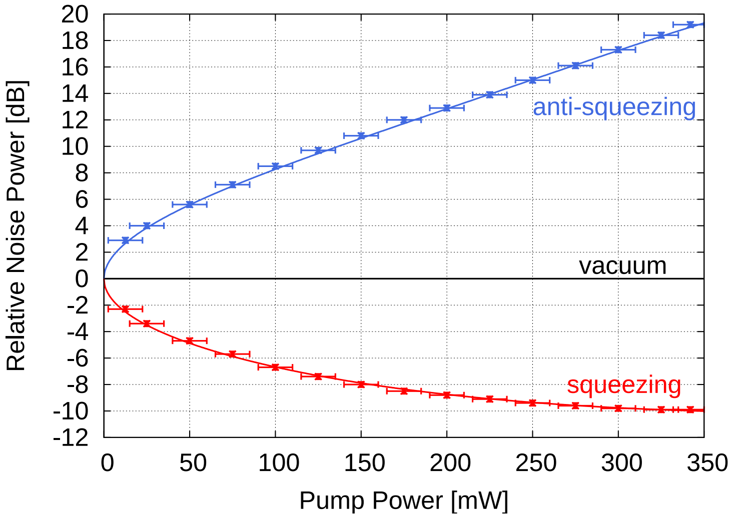


Figure 5.3: Measurement of squeezing for varying pump power. The pump power was varied from 12.5 mW to 342 mW and each time the squeezed and anti-squeezed noise was measured and normalized to the vacuum noise level. The theoretical curve is the function from Equation (5.1), the parameters are given in the text.

up-conversion above threshold. Therefore, the setup for SHG is identical to the squeezed-light source and the cavity has the same parameters. The only difference is that it is pumped with a strong coherent field at the fundamental frequency. By tuning the temperature to accurate phase matching of the periodic poling a maximum conversion efficiency of 84% could be achieved at the maximum pump power of 570 mW of 1550 nm light.

5.1.2 *Generation of Two-Mode Squeezed States*

The easiest way to generate cw two-mode squeezing is so-called *v-class entanglement*. By superimposing a squeezed state with a vacuum at a 50:50 beam splitter, i.e. blocking the second input port of the beam splitter, two entangled output modes are generated [DGu10Th]. A schematic of this experimental setup is shown in Figure 5.4. The advantage of this method is, apart from needing less resources, that no mode matching at the beam splitter has to be found, since the vacuum is matching in any possible mode. This comes with the drawback of a limitation in the achievable non-classicality. For example for an amplitude-squeezed state the correlations in the phase quadrature of the two output fields are at most as good as twice the vacuum noise. On the other hand, in the amplitude quadrature the correlations are only limited by the input squeezing and can in principle be infinitely strong. Now depending on the entanglement criterion under investigation, different situations can arise in comparison to a setup using two squeezed-light sources, also known as *s-class entanglement*. For

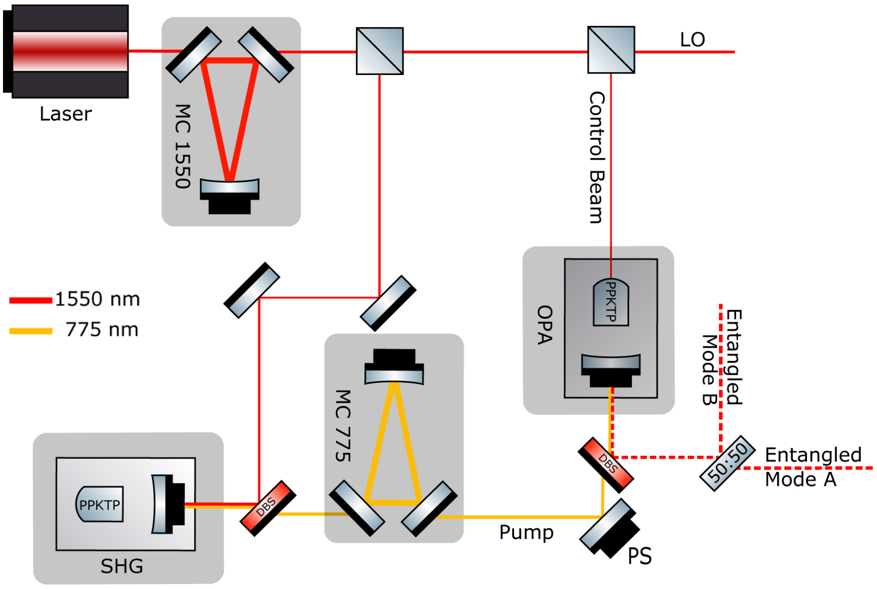


Figure 5.4: Schematic of the experimental setup for the generation of v-class entanglement. The 1550 nm laser field is mode filters in a ring cavity (MC 1550). Most of the power is then coupled into the second harmonic generation (SHG), the rest is used for the control beam and the local oscillator (LO). The frequency doubled field is separated from the fundamental field at a dichroic beam splitter (DBS) and also mode filtered (MC 775). Via a phase shifter (PS) and another DBS it is coupled into the optical parametric amplifier (OPA) where a squeezed state is generated in the crystal (PPKTP). The squeezed field is superimposed with vacuum at a 50:50 beam splitter. The two output modes are then entangled.

the Duan criterion there will be entanglement, no matter how much loss is present in the measurement. But the criterion value will always be limited to -3 dB compared to the vacuum which rules out the application for quantum teleportation protocols [Fus98, Bow03b]. For the EPR-Reid criterion (see Section (4.4)) on the other hand the criterion value is not limited at all and can approach zero for infinite squeezing. But it is strongly dependent on the optical loss and for an overall detection efficiency smaller than $2/3$ no EPR violation is possible for v-class states. A summary of these statements is plotted in Figure 5.5.

The strongest possible entanglement for v-class states is, therefore, the EPR-Reid violation. The remarkable result is that for 0 optical loss no fundamental limit to the entanglement strength is present. This makes them useful to demonstrate fundamental quantum optical properties due to their lower resource requirement. In the presented setup a significant violation could be demonstrated with $0.39 \pm 0.01 < 1$ [Ebe11]. Furthermore, even an applicability to quantum key distribution could theoretically be shown, although the achievable key rates are significantly smaller than for s-class entanglement [Ebe13a, Ebe13Th]. In this thesis we used the v-class states to demonstrate the

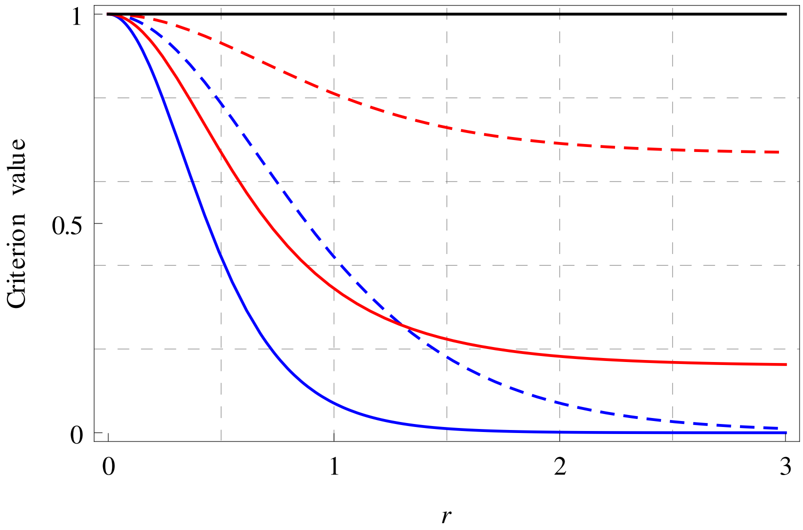


Figure 5.5: Comparison of the EPR-Reid criterion for s-class and v-class entanglement. The EPR-Reid criterion from Equation (4.7) is plotted versus the squeezing factor. The violation of a s-class entangled state (full) is always stronger than for a v-class state (dashed). The violation strength also depends on the optical loss. With no loss (blue) it is more significant than with 20% symmetric loss for both modes (red). We also see that this loss has a significantly stronger influence on the v-class state and limits the achievable criterion value to about 0.65 instead of 0.18 for the s-class state.

one-way steering effect (see Sections 4.3 and 4.4 for a theoretical introduction).

5.2 DEMONSTRATION OF ONE-WAY STEERING

The experimental setup for the generation of one-way steering states was developed in this thesis and published in [Hän12]. A schematic of the setup is shown in Fig. 5.6. The 10.2 dB squeezed state at 1550 nm was generated by type I parametric down conversion in a half-monolithic cavity. After the superposition with vacuum on a first balanced beam splitter, output mode B was sent through a half-wave plate and a polarizing beam splitter. This setup allowed the preparation of mode B with an adjustable contribution of a second vacuum mode. The measurements at A and B were performed by balanced homodyne detection. Both detectors could independently choose the measured quadrature by adjusting the phase of their local oscillators. The signals of the homodyne detectors were simultaneously recorded with a data acquisition system consisting of a mixer and an anti-aliasing filter for each channel and a data acquisition card in a laboratory computer. The mixers demodulated the signals at 8.3 MHz sideband frequency. The data acquisition card recorded the resulting values as a time series on the hard drive of the computer. It had a data depth of 16 Bit and maximum sampling rate of 500 kHz, since the two signals had to share one analogue-to-digital converter with 1 MHz sampling rate. Following the Nyquist theorem [Nyq28], no signals at frequencies above half the discretization frequency may be detected to avoid aliasing. Therefore, from the data depth it was calculated that signals above 250 kHz had to be suppressed by 84 dB. This was realized by two identical ninth order Bessel lowpass filters at 35 kHz as anti-aliasing filters for the two channels.

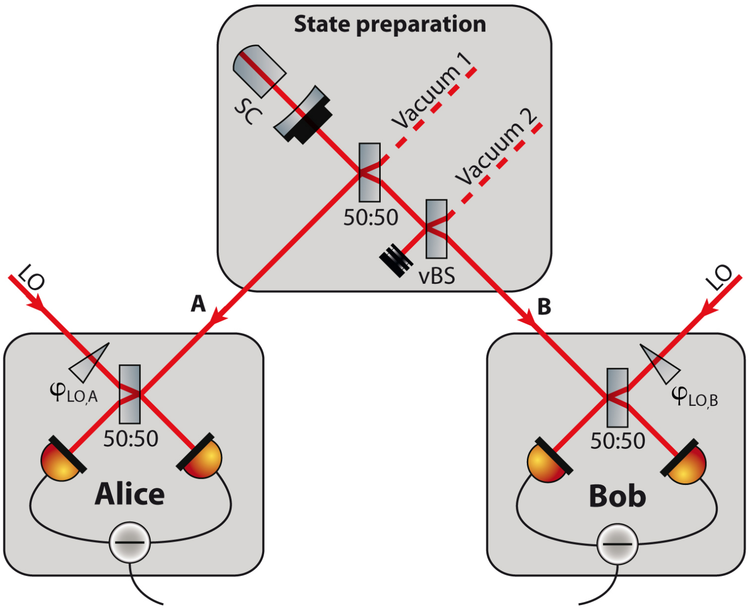


Figure 5.6: Schematic of the experimental setup for the demonstration of one-way steering. A squeezed-light field at 1550 nm, produced by a squeezing cavity (SC), is superimposed at a balanced beam splitter with a vacuum mode. A variable beam splitter (vBS) is implemented in one output mode to change the contribution of a second vacuum mode. Measurements are performed by balanced homodyne detection where the measured quadrature is chosen by the phase φ_{LO} of the local oscillator (LO).

The setup can mathematically be described by taking the initial covariance matrix of a squeezed state and successively applying the symplectic beam splitter formalism from Equation (3.3) for the entanglement beam splitter, the detection efficiencies of Alice and Bob and the contribution of the second vacuum mode. A full derivation of the analytic description can be found in Appendix A.2. Here, we will just give the result for a v-class entangled state with 16.3 dB initial pure squeezing and detection efficiencies of $\eta_A = 0.884$ and $\eta_B = 0.937$ for Alice and Bob, respectively. With these values the conditional variance product from the left hand side of Equation (4.7), which certifies steering from Alice to Bob if smaller than one, reads

$$\frac{I_4}{I_1} = 0.391 + 1.419\varepsilon - 0.81\varepsilon^2, \tag{5.2}$$

where ε is the contribution of the second vacuum mode, i.e. the reflectivity of the second beam splitter. Note, that we have to replace Bob's optical loss by $1 - \eta_B + \varepsilon\eta_B$ to correctly model the influence of the second beam splitter. The function for the converse steering direction from Equation (4.8) is given by

$$\frac{I_4}{I_2} = \frac{4.34 + 15.76\varepsilon - 8.99\varepsilon^2}{11.20 - 1.21\varepsilon - 8.99\varepsilon^2}. \tag{5.3}$$

Figure 5.7 shows the result of this experiment. The conditional variance products from inequalities (4.7) and (4.8) for Alice's ability to steer Bob (lower line, red crosses) and Bob's ability to steer Alice (upper line, blue crosses) are plotted against the contribution of the second vacuum mode. For values between 0% and 95% a partial tomographic measurement was performed to reconstruct the relevant entries of the covariance matrix (see Section 3.5). The uncertainties of the contributed vacuum result from the adjustment accuracy of the half-wave plate. In order to determine the means and standard deviations of the conditional variance products a bootstrapping method was used [DGu11]. One million data points were randomly chosen out of the set of $5 \cdot 10^6$. This was repeated 10^4 times. From these the two conditional variance products were calculated for each data set. A histogram of these values for 50% vacuum contribution is shown in the small boxes in Fig. 5.7. This is the setting where the observed one-way steering effect becomes most obvious. For Alice (left box) the mean of 0.908 is 31 standard deviations below 1 whereas for Bob (right box) the mean of 1.206 is 53 standard deviations above 1. Furthermore, the Gaussianity of the states was verified using a Q-Q-plot method as in [DGu11] to make sure that the covariance matrix is an exhaustive description of the state (compare Section 2.4.2).

The two solid lines in Fig. 5.7 are the theory curves from Equation (5.2) and (5.3), respectively. For a vacuum contribution smaller than 39%, both Alice and Bob can steer the respective remote subsystem, whereas for a contribution larger than 70% neither of them can. These values arise from the overall optical loss in the setup and would for a perfectly lossless experiment be 50% and 100%, respectively. One-way steering is observed precisely between these two values in the white region in Fig. 5.7.

5.3 CONNECTION TO OTHER ENTANGLEMENT APPLICATIONS

5.3.1 *Tripartite and Multipartite Steering*

While for the presented experiment one of the output modes of the variable beam splitter was dumped, a tripartite situation arises when instead a third party, Charlie, receives this mode. For symmetry reasons Alice would then also be able to steer Charlie, in fact, simulta-

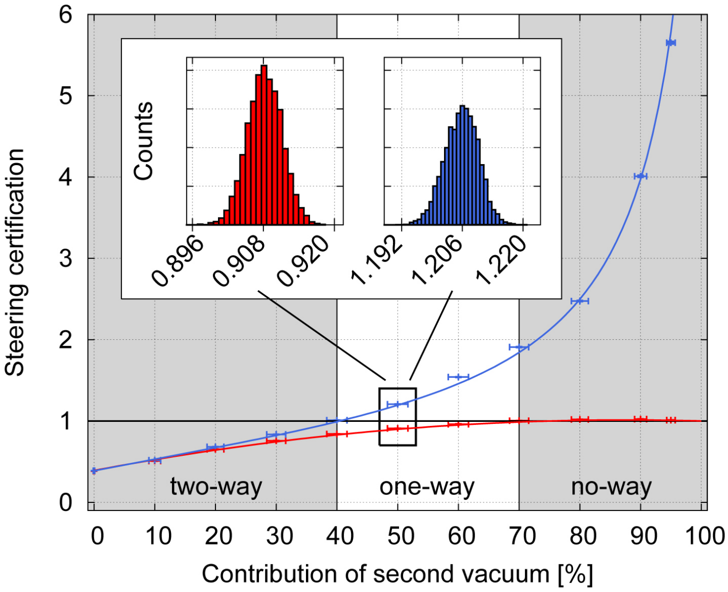


Figure 5.7: Certification of one-way steering. Shown are measurement results of the conditional variance products according to the criteria (4.7) and (4.8) versus an increasing contribution of the second vacuum mode in mode B. One-way steering is observed if the value for one steering direction is below unity, whereas the value for the other steering direction is above the unity benchmark. This is fulfilled in the white region and most significantly at a vacuum contribution of 50%, as shown by the measurement histograms.

neously to Bob. We can further say, that neither Bob can steer Charlie nor conversely since the input of the second beam splitter already has a vacuum mode contribution of 50% due to the first beam splitter. Steering in the presence of just one squeezed mode is only possible for vacuum contributions less than 33% [Ebe11].

The situation can become arbitrarily complex by introducing more beam splitters, hence, generating more entangled modes. Consider a four-partite scenario with Alice, Bob, Charlie and Domenica. Now steering can not only be investigated for each individual combination but also for composite parties. For example we could summarize the measurements of Alice and Bob by adding them with an appropriate scaling factor and try to steer the measurements of Charlie or Domenica or even the composite of Charlie and Domenica. Depending on the respective optical detection efficiency there will arise many different situations showing all possible combinations of two-way, one-way and "no-way" steering. In a recent publication an eight-partite network was realized [Arm15] with variable beam splitters dividing the modes (which is equivalent to the situation of adding optical loss [Wag14]). The steering properties were mapped for the space of reflectivities and could be shown to be in accordance with the theoretical description. To simplify, we can understand these results in the following way: Whether a party (or a composite of parties) can or cannot steer another party depends on the amount of the initial squeezed state the respective parties obtain after a network of beam splitters. If the amount is to small the steering inequality can not be violated.

5.3.2 *Entanglement Distribution by Separable States*

The question of whether entanglement can be distributed between two parties by only sending separable modes from one to the other was answered positively in [Vol13]. As we have seen before, a two-mode squeezed state can not be dis-entangled (i.e. made separable) just by adding optical loss. Therefore, to the initial v-class state in the experiment thermal noise was added in both quadratures. After distributing these separable auxiliary modes to the receiving party the noise could be removed in a simple beam splitter operation and entanglement was regained if the phase relation between the auxiliaries was chosen correctly. In this thesis we have only investigated the influence of optical loss to steering states but the application of thermal noise is straightforward. And a detailed analysis showed that to make the protocol work the initial entangled state must not show two-way steering [Fra12Th]. It can at most be a one-way steerable state from the sender to the receiver. The reason is that a state showing steering from the receiver to the sender can never be dis-entangled by adding Gaussian noise. Hence, the border between one-way and two-way steering also is a boundary for the applicability of the EDS protocol.

5.3.3 *Data Reconciliation in Quantum Key Distribution*

There is a heuristic connection of one-way steering to the reconciliation procedure in quantum key distribution (QKD) protocols (see Chapter 6). In this classical post-processing step the communicating parties exchange data to correct for errors in their bit strings. Now there are in priciple two possibilities: Either Alice gives information on her measurement results to Bob (*direct reconciliation*) or Bob gives information to Alice (*reverse reconciliation*). In each case the receiving party will rescale its data according to the occuring variances. Only if the resulting average distance between the data strings is smaller than a predefined threshold, a positive key rate is achieved (see Section 6.2.1). Therefore, the algorithm is similar to the calculation of the inferred variances in the EPR-Reid criterion in Section 4.4 and the scaling factors correspond to parameters g and h. This is then a weaker version of the EPR-Reid criterion based on conditional variances and successful direct reconciliation would correspond to steering from Bob to Alice, while successful reverse reconciliation would correspond to steering from Alice to Bob.

Now in a perfect setup the direct reconciliation will only succeed up to 50% transmission loss, whereas the key rate for reverse reconciliation only drops to zero in the limit of 100% loss [Gro02]. These boundaries coincide precisely with the boundaries for one-way and two-way steering in an otherwise perfectly loss-free setup. This coincidence is of course not a proof but it just gives a hint that there might be a connection. The link between steering and QKD scenarios is subject to ongoing theoretical investigations. We will make further comments on this topic in the discussion of the QKD results in Section 6.2.3.

6

APPLICATION OF TWO-MODE SQUEEZED STATES FOR QUANTUM KEY DISTRIBUTION

6.1 A BRIEF INTRODUCTION TO QKD

The development of the computer and efficient communication protocols using radio frequencies laid the foundation for our modern information society. Where the original inventions were designed to fulfill very specific tasks, their universal applicability became obvious very soon. The 21st century will be the age of information, accessible and publishable by anyone, anywhere and anytime, which will most likely fundamentally change our way of living and thinking. Apart from economical, sociological and ethical challenges, the networking of our world demands the everyday application of cryptography to keep sensitive information secret during communication. A security breach of data transfers can lead to serious threats to individuals as well as to companies or even whole societies. And the risk will become even higher when our machines will start exchanging data based on their logical (and at a certain point maybe even intelligent) programming without any human control. This will render us completely helpless to control what information is exposed to eavesdropping threats.

These circumstances gave the field of cryptography a significant boost throughout the last decades. A variety of encryption protocols were developed, based on fundamental mathematical research and exploiting the fact that even computers fail at solving problems with high complexity in a reasonable time. In the current day we can assume protocols like RSA or AES [Riv78, Dea02] in their latest versions to be secure against cryptoanalytic attacks. To the best knowledge of the author all security breaches that were reported in the last years (be it by hackers or by intelligence agencies) were caused by flaws or back doors in the implementation or by incorrect use of the techniques and protocols.

Nevertheless, the fact that our communication security is based on computational hardness to break the encryption is a severe drawback, as this will not be save in the future. The processing speed of CPUs increases every year and the development of the quantum computer will open a door to algorithms that can overcome the complexity of classical computational problems. On the one hand, this will reduce the amount of required time to break encryptions so significantly that we can not assume our current cryptography to be secure anymore. On the other hand, it will also give the possibility to retroactively gain access to encrypted messages, a severe threat to all current informations that are not outdated in a few years.

A solution to this problem could be to use the one-time pad encryption that is mathematically provable absolutely secure [Ver26]. This protocol uses a symmetric key for encryption with the following properties: It is as long as the message; It is independent and identically distributed over the key alphabet (i.e. it is truly random); It is only known to the two communicating parties; It is used only once. The security of this protocol is obvious. A truly random key that contains no repetitions generates a cipher text with a uniform and truly random distribution of symbols. Such a text cannot be attacked in a meaningful cryptoanalytic way. However, the drawback of the one-time pad protocol is, apart from the technical problem of generating true randomness, the absolutely secure (i.e. secret and correct) distribution of the key to the communicating parties. For this reason the one-time pad never gained significance in cryptography and is nowadays only used in circumstances where the demand of secrecy justifies the effort of using pre-distributed code books.

This is where quantum key distribution (QKD) comes into play. The distribution of the one-time pad key can be made secure based on quantum physical principles [Gis02, Sca00] like the *no-cloning* theorem for quantum states [Die82, Woo82]. This also overcomes the problem of retroactive access even if a specific QKD protocol should be compromised by future technologies (see for example References [Lyd10] and [Jor15] for successful attacks on single photon based systems). As any quantum state is altered or annihilated during the required measurement process for the key generation, a security breach of a specific protocol would not compromise the keys that were generated with it previously. The resource for the key would simply no longer be accessible and only the protocol would be outdated.

The idea of state-of-the-art quantum key distribution is based on the fact that two non-commuting observables cannot be measured with arbitrary precision simultaneously, which manifests itself in the Heisenberg Uncertainty Principle. Suppose now two parties, Alice and Bob, each have a measurement device that can measure two such observables and that allows for each individual measurement an independent random choice of which observable is measured. Furthermore, suppose a (two-mode) quantum state is distributed to the two parties that exhibits some sort of correlation if both measure the same observable. Then Alice and Bob can generate a shared secret by performing a series of such randomly chosen measurements and afterwards excluding all results where they measured different observables (on average 50%) by communicating their measurement choices but not their results. By comparing a random subset of their measurement results they can verify not only the correctness but also the secrecy of their protocol. Assuming the measured quantum state has to obey quantum mechanics, they can calculate the amount of information that dissipated to the universe (and thereby to a hypothetical and omnipotent eavesdropper) by comparing it to an entropic uncertainty relation based on a mathematical proof. Depending on the result of these calculations they can either exclude the respective amount of information or, if too much information might have been revealed to the universe, abort the protocol and start all over. If the protocol is not aborted they can perform classical post-processing of the data and establish a completely random, secret and symmetric key. This can be used in further cryptographic protocols and ensures absolute security based on quantum physical principles and mathematical proofs.

6.1.1 *Classification of QKD Schemes*

Since the first protocol for QKD by C. Bennet and G. Brassard in 1984 [Ben84] many different systems were proposed and realized using a variety of quantum observables and channels and numerous mathematical security proofs. These systems can be classified by their technical implementation as well as by the security they achieve.

The technical implementations of QKD systems can by divided into four main classes. The first distinction concerns the observables, whether the measured variables have a discrete or a continuous spectrum. Where for the first class a mapping to discrete bits (0s and 1s) is obviously directly delivered by the measurement result, for the second class an artificial discretization step is required after the measurements were performed. This has crucial influence on the error reconciliation in the classical post-processing. In general this part of the protocol is more demanding for continuous variables. Due to the continuous distribution, there will always be a finite probability of a strong mismatch between the measurement results of the two parties. The second distinction concerns the source of the quantum states, whether the states are generated by one party and sent to the other party for measurement (a *prepare-and-measure* scheme) [Ben84, Jou13a, Dia15] or whether an entanglement source provides them for both parties for measurement (an *entanglement-based* scheme) [Eke91, Ben92, Aci07, Fur12, Geh15]. The first class of implementations has the advantage that the preparing party does not have to measure anything but actually generates the raw key and keeps it for post processing. This comes with the drawback that a source of true randomness is required. True randomness is fairly difficult to prove [Ebe13Th]. The second class provides the required randomness directly out of the source. For example two-mode squeezed states consist of parametrically amplified vacuum fluctuation that are truly random by their quantum nature. The disadvantage is that entanglement generation is in general experimentally more challenging than the generation of specific states with classical modulators. Furthermore, entangled states are more sensitive to transmission loss which can drastically reduce the achievable key rates in real world applications.

The classification of the security actually is a classification of the assumptions that are made on a potential eavesdropper Eve. The common assumption for all classes is that Eve has access to all classical communication between Alice and Bob, that she can measure anything that dissipates from the quantum channel to the environment with 100% efficiency and that she has unlimited computational power. Furthermore specific assumptions on the attack power are made. In the simplest case of *individual attacks* it is assumed that Eve can not store the distributed quantum states and has to attack each signal individually. This simplifies the security analysis as the information Eve can access can be described directly on the density operator of a single distributed quantum state. A more sophisticated class are the *collective attacks* [Cer01, Lod07, Wee12]. In this case Eve has a quantum memory and can store all distributed signals. This enables here to wait for Alice and Bob to perform the protocol, to listen to their classical communication and to use this additional information to collectively attack all signals in an appropriate way which increases her success probability. Finally there is the class of the most general *coherent attacks* where we make no assumptions at all that would restrict Eve's power of attack [Ren09, Fur12, Lev13]. There is no actual description of what a coherent attack could look like because it would require technology we have not even thought about to date. Nevertheless, the absolute security aspiration of quantum key distribution makes it desirable to provide security against any sophisticated attack whatsoever which is exactly covered by the security against coherent attacks.

Furthermore, there is the class of *device independent* (DI) security which does not necessarily depend on the assumed strength of attack. The idea is to make no assumptions on the devices of Alice and Bob, the source of the quantum states and the transmission channel in the security proof by implementation of an adequate scheme. That way Eve can tamper with the devices without compromising the security of the protocol. Schemes providing device independent security are in general experimentally more demanding. For example, a fully device independent protocol requires the violation of a Bell inequality [Aci07]. As we have seen in Chapter 4 a Bell inequality violation means that a prediction of the measurement results is never possible. This implies that at no point in the experiment could the measurement statistics have been forged by a classical algorithm. Therefore, a Bell inequality violation guarantees maximum security, as not one of the devices in use has to be trusted. Where the experimental violation of a Bell inequality is difficult, a weaker version can be achieved in measurement device independent schemes [Bra12, Lo12, Pir15]. Here the source has to be trusted but no assumptions on the measurement devices of Alice and Bob are required.

An important sub-class are *one-sided* device independent schemes (1sDI) [Wan13, Wal14]. In this case only the devices of one party do not appear in the security proof which requires that the statistics of this party could not have been forged. Since steerable states rule out the existence of a classical model for one party (see Chapter 4), they fulfill exactly this requirement and enable security proofs for one-sided device independence [Tom11, Brc12, Tom13]. We can take the intuitive understanding that if the state is not steerable from Bob to Alice and if Bob's devices are untrusted then Eve could gain full control of them, since there is a classical model describing Bob's subsystem [Fra12Th]. By certifying steering from Bob to Alice this possibility can be ruled out. The QKD protocol is then secure against side-channel attacks on Bob's devices, like attacks on the local oscillator [Ma13a, Ma14] or the shot noise calibration [Jou13b, Kun15], wavelength attacks on the homodyne beam splitter [Ma13b, Hua13] or saturation attacks on the electronic circuits in the detectors [Qin13]. In contrast to states violating a Bell inequality, steerable states are significantly easier to generate and to certify. Furthermore, they enable QKD with security against coherent attacks [Fur12] and provide security against Trojan-horse attacks on the source [Lo99, Jai14]. Therefore, if the trusted Alice possesses the quantum source and her laboratory is secured against the outside, the security of such a system is comparable to a fully device independent scheme.

Finally, the QKD protocol should provide composable security and the calculation of the secret key length should include finite-size effect. The composable security means that the QKD protocol can be combined with other secure protocols, for example the one-time pad encryption, and remains secure [Beo05, Ren05]. The finite-size effects emerge, since in any real world implementation only a finite number of samples will be recorded which reduces the accuracy of the statistical description [Lev10, Fur12]. Therefore, the inclusion of these effects generally reduces the secret key rate significantly and it is said to be ε-secure. Roughly speaking, if $\varepsilon = 10^{-10}$ then out of 10^{10} distributed samples Eve will on average achieve a successful attack on only one of them.

6.1.2 *The Continuous Variable QKD Project at the Leibniz University Hannover*

The aim of the project was to demonstrate the feasibility of entanglement based continuous variable quantum key distribution in local area fiber networks. To this end a cooperation between theoretical and experimental physicists at the Leibniz University Hannover was established within the QUEST cluster of excellence. The theoretical background as well as the mathematical proofs, analyses and simulations were provided by the Quantum Information group of R. F. Werner at the Institute for Theoretical Physics. The experimental implementations, the development of the necessary technology and all measurements were performed in the Quantum Interferometry group of R. Schnabel at the Institute for Gravitational Physics. Furthermore, in the later course of the project a cooperation with the Austrian Institute of Technologies (AIT) was started, that developed and contributed the classical post processing software required for the generation of a usable key. Thus, the project unified the whole process of the implementation of a QKD system from the first ideas of a security proof to the final secure bits.

Up to date, four PhD theses have been written in the context of the project. The first one by F. Furrer contributed the security proof which demonstrated that security against coherent attacks was possible with the experimentally feasible parameters [Fur12Th]. The second one by T. Franz contributed a general analysis of the QKD tasks especially in the context of EPR steering [Fra12Th]. The third one by T. Gehring demonstrated the experimental feasibility of the demands by the security proof and contributed the first usable key, at that point with security against collective attacks [Ebe13Th]. The fourth one by J. Duhme contributed a complete numerical simulation of all relevant parts of the experimental setup and an efficient post processing algorithm that was developed together with C. Pacher from the AIT [Duh15Th]. The thesis at hand marks the final step in the project and contributes the worldwide first usable key with composable security against coherent attacks generated from entangled continuous variables. Furthermore, it provides a study on the influence of transmission loss and demonstrates the feasibility of the scheme in local area fiber networks with up to 5 km transmission length. Together with F. Furrer's extensions of his security proof it also demonstrates the one-sided device independence of the implementation and, in the prospect of reverse reconciliation, the feasibility of transmission lengths of up to 16 km [Fur14].

6.2 CONTINUOUS VARIABLE QUANTUM KEY DISTRIBUTION WITH COMPOSABLE AND ONE-SIDED DEVICE INDEPENDENT SECURITY AGAINST COHERENT ATTACKS

In this section we will present the experimental techniques and results of the entanglement-based QKD system. The results of a study on possible fiber transmission are presented in Section 6.3. An introduction to Gaussian quantum information theory that lays the foundation of the system can be found in [Fra12Th, Ebe13Th, Duh15Th]. The security proof for the protocol is given in [Fur12] and is based on entropic uncertainty relations.

6.2.1 *The QKD Protocol*

The protocol implemented in this experiment is based on the one developed in [Fur12] and used in [Ebe13Th]. It only differs in the formula for the key length, that here also takes imperfections of the X and P measurements into account, and a slightly different binning of the measurement space. For completeness and because it is a good example of a generic QKD protocol, we will present the full protocol here directly following our publication [Geh15] and complement it with some explanatory comments.

PRELIMINARIES Alice and Bob use a pre-shared key to authenticate the classical communication channel for post-processing [Sti94]. This can in principle be performed with classical algorithms, as long as the security can be guaranteed for the time required to execute the protocol. After a first successful run all future authentication can be based on a part of the quantum key from a previous run. Furthermore, Alice and Bob negotiate all parameters needed during the protocol run and Alice performs a shot-noise calibration measurement by blocking the signal beam input of her homodyne detector.

MEASUREMENT PHASE Alice prepares an entangled state using her EPR source and sends one of the output modes to Bob along with a local oscillator beam. The one-sided device independence guarantees that Bob's local oscillator may be altered by Eve without compromising security. Both Alice and Bob choose, randomly and independently from each other, a quadrature X or P, which they simultaneously measure by homodyne detection of their light field. The random number for the choice is generated from a measurement of the fluctuations of a vacuum field with an additional homodyne detector, similar to the scheme in [Gab10]. The outcome of a measurement on the entangled beams is called a sample. This step is repeated until 2N samples have been obtained.

SIFTING Alice and Bob announce their measurement bases and discard all samples measured in different quadratures. This leaves them on average with N samples for the remaining protocol. The aspiration of security against arbitrary attacks forbids the reconstruction of the covariance matrix, since this would require strong additional assumptions. Therefore, the discarded samples can not be used for channel estimation like in protocols with security against collective attacks.

DISCRETIZATION The continuous spectrum of the measurement outcomes is discretized by the analogue-to-digital converter used to record the measurement (see Section 6.2.2). During the discretization step, Alice and Bob map the fine-grained discretization of their remaining samples caused by the analogue-to-digital converter to a coarser one consisting of 2^d consecutive bins. In the interval $[-\alpha, \alpha]$ a binning with equal length δ is used, which is complemented by two bins $(-\infty, -\alpha)$ and (α, ∞). The parameter α is used to include the finite range of the homodyne detectors into the security proof. If one of Alice's measurement's absolute value exceeds α the protocol is aborted.

CHANNEL PARAMETER ESTIMATION The secret key length is calculated using the average distance between Alice's and Bob's samples. To estimate it, the two parties randomly choose a common subset of length k from the sifted and discretized data $\mathbf{X}_A^{pe}$ and $\mathbf{X}_B^{pe}$, which they communicate over the public channel. Using these, they calculate

$$d_{pe}(\mathbf{X}_A^{pe}, \mathbf{X}_B^{pe}) = \frac{1}{k} \sum_{\mu=1}^{k} \left| (\mathbf{X}_A^{pe})_\mu - (\mathbf{X}_B^{pe})_\mu \right| ,$$

and abort if it exceeds a threshold d_{pe}^0 agreed on in the preliminary step. This is a calculation of the correlation strength present in the distributed quantum state. Note, that it is not a steering criterion, although the equation looks similar to the additive convex steering criterion in [Cac09]. There is no simple connection of the two criteria, since for QKD with security against coherent attacks we are not allowed to make any assumption on the statistical distribution of the measurement results. Especially, we may not assume Gaussianity and cannot use the covariance matrix for a full description of the correlations.

ERROR RECONCILIATION Bob corrects the errors in his data to match Alice's using the hybrid error reconciliation algorithm introduced in [Geh15]. The algorithm divides into two stages that exploit the Gaussian character of the correlations. The first stage corrects the d_l least significant bits of each sample by directly communicating them to Bob. In the second stage the remaining errors in the d_m most significant bits ($d = d_l + d_m$) are corrected with a non-binary low density parity check (LDPC) algorithm. Later, Alice and Bob confirm that the reconciliation was successful.

CALCULATION OF SECRET KEY LENGTH Using the results from the channel parameter estimation and considering the number of published bits during error reconciliation l_{LK}, Alice and Bob calculate the secret key length l according to the formula

$$l \leqslant n \left(\log_2 \frac{1}{c(\delta)} - \frac{V_X + V_P}{2 \ln 2} - \log_2 \gamma(d_{pe}^0) \right) - l_{LK} - O\left(\log_2 \frac{1}{\varepsilon} \right) . \quad (6.1)$$

If the secret key length is negative, they abort the protocol. Here, $n = N - k$ is the number of samples used for key generation. The first term in the bracket is the lower bound of the entropic uncertainty relation from Equation (2.3). It is used to replace the smooth min-entropy of the state after Alice's measurement and conditioned on Eve under the assumption that Eve holds the subsystem purifying the overall state. Therefore, the functions $c(\delta)$ refers to the overlap of the discretized X and P measurements of Alice. The entropic uncertainty relation introduces the smooth max-entropy of Alice's state conditioned on Bob into the formula. This is lower bounded in the third term where the function γ is calculated for an upper bound on the average distance between Alice's and Bob's measurement outcomes, taking into account the probability of not a single measurement laying outside of the α-interval. The second term takes an imperfect measurement of X and P into account. V_X and V_P describe the variances of the measured basis around the exact quadrature under the assumption of a Gaussian distribution due to phase noise. Hence, the first three terms describe the maximum information that can be securely extracted from the quantum part of the protocol. The leakage term l_{LK} of the classical post processing has to be subtracted from this information. Furthermore, the last term is an upper bound for the finite size effects that also has to be subtracted. Roughly speaking, ε is the remaining uncertainty in the measurement statistics due to the finite number of samples. A detailed derivation of the secret key length can be found in [Fur12Th] and [Ebe13Th]. The proof for the phase noise term is given in [Geh15]. Note that the formula only depends on Alice's devices and that Bob's devices do not appear at all. This proves the one-sided device independence of the security.

PRIVACY AMPLIFICATION Alice and Bob apply a hash function that is randomly chosen from a two universal family [Car79] to their corrected strings to produce the secret key of length l. A hash function can be seen as a trap door. After its application there is no way to reconstruct the raw key from the reduced string. Therefore, any information that exceeds the secret key length is definitely removed from the final key and any knowledge of Eve about it becomes impossible.

REMAINING ASSUMPTIONS There are five assumptions remaining to make the protocol secure against arbitrary attacks [Geh15].

I Alice's station is a private space [Bra12] and from Bob's station neither his measurement choice nor his measurement outcomes are leaking. This assumption is natural to (almost) all QKD implementations and can be fulfilled by locking their stations to the outside.

II The energy of Alice's mode of the EPR state is bounded, which allows her to determine the probability for measuring a quadrature amplitude absolute value exceeding α. This can be assured by placing the source into Alice's private station.

III Alice switches randomly between the X- and P-quadrature with 50% probability. This can be implemented by the use of a quantum random number generator (see Section 6.2.2).

IV Bob chooses randomly between two (not necessarily orthogonal) measurements that are assumed memoryless. Here, memoryless means that a measurement result does not depend on any previous result. By choosing the frequencies of the data acquisition system appropriately this can be excluded [Ebe13Th]. The randomness can again be guaranteed by a quantum random number generator.

V The phase noise in Alice's measurements is Gaussian to allow an inclusion in the secret key length formula in the presented way. To assure the Gaussianity a separate measurement of the phase noise at Alice's detector can be performed (see Section 6.2.2).

6.2.2 *Implementation of the Protocol*

GENERATION OF S-CLASS ENTANGLEMENT The second squeezed-light source required for the full two-mode squeezing setup was built identically to the first one. It delivered a maximum of 10.9 dB noise reduction at a pump power of 180 mW. This resulted in a total of more than 500 mW pump power required, which was hardly achievable in the setup. Therefore, the first squeezed-light source from Chapter 5 was replaced, as all attempts to change its pump threshold to a lower value were unsuccessful. This was probably due to optical loss in the crystal but maybe also due to unfortunate mode degeneracy or even a lower non-linearity of the crystal material. The new squeezed-light source was originally established by M. Mehmet [Meh11] and was adapted to the existing setup with slightly different wavelengths by carefully changing the cavity's air gap. After successfully increasing the conversion efficiency it achieved a pump threshold comparable to the second one and delivered 11.7 dB of squeezing at 150 mW pump power. With these values a simultaneous stable operation of both squeezed-light sources became possible.

The next step was to establish a phase lock between the squeezed fields at the entanglement beam splitter. For perfect two-mode squeezing the one field should contribute squeezing in the amplitude quadrature and the other in the phase quadrature. As both fields contribute vacuum squeezing there is no definite amplitude and phase quadrature. Therefore, the orthogonal-squeezing requirement was re-

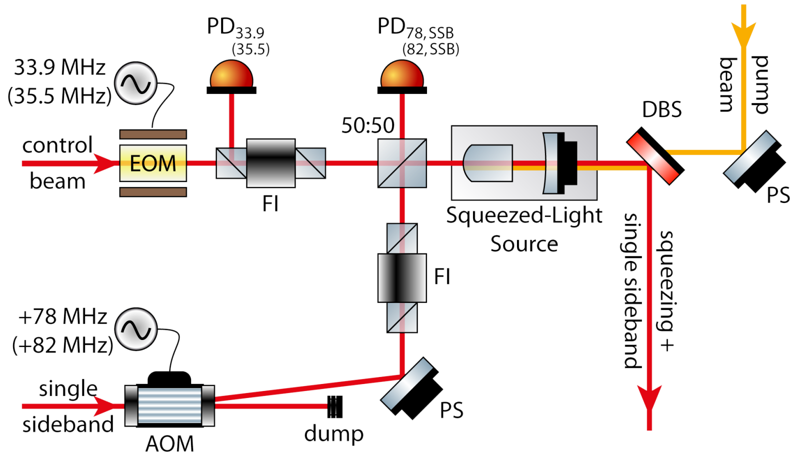


Figure 6.1: Schematic of the squeezed-light source stabilization. The control beam carried a phase modulation from an electro-optical modulator (EOM) of 33.9 MHz (35.5 MHz for the second source). Using a Pound-Drever-Hall locking scheme the length of the cavity was stabilized to resonance for the 1550 nm field. By demodulating the signal in the orthogonal quadrature a signal for the stabilization of the pump phase could be generated at the same photo diode ($\mathrm{PD}_{33.9}$). The SSB was generated by an acousto-optical modulator (AOM), superimposed with the control beam before entering the cavity and phase locked to it. Thereby it became a phase reference for the squeezing angle, as locked phases are transitive. FI: Faraday isolator, PS: phase shifter, DBS: dichroic beam splitter. A similar figure was published in [Ebe13Th].

alized by locking the fields 90° out of phase. To this end a single sideband (SSB) technique was used. Two tap-offs from the main laser of a few µW were shifted with acousto-optic modulators (AOMs) in frequency, the one by 78 MHz, the other by 82 MHz. Each of these fields was superimposed with one of the control beams of the squeezed-light sources at a 50:50 beam splitter before entering the cavity. The second output was detected by a photo diode and demodulated at the corresponding sideband frequency. With this sinusoidal error signal a phase lock between the SSB and the control beam was established using a PZT-mounted mirror as phase shifter (PS) for the SSB. Since the phase of the pump field (and thereby the squeezing angle) was locked to the control beam as well, this lock immediately established a fixed phase relation between the SSB and the squeezed quadrature. A schematic of this setup is shown in Figure 6.1

After superimposing the two squeezed fields (now each accompanied by a SSB) at a 50:50 beam splitter (for obvious reasons we will call it the *entanglement beam splitter*), a small tap-off of about 1% was taken from one of the output ports to generate an error signal for phase locking the two squeezed fields as shown in Figure 6.2. Since this field was very weak it was superimposed with about 5 mW of local oscillator power at a 50:50 beam splitter. One port was demodu-

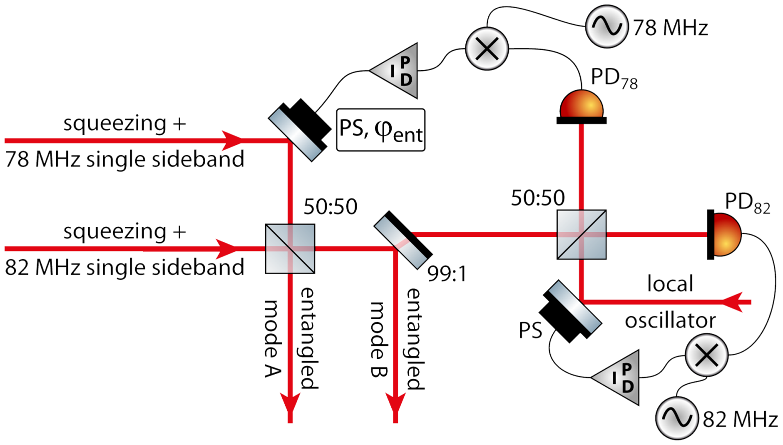


Figure 6.2: Schematic of the entanglement phase lock. After superimposing the two squeezed fields at a 50:50 beam splitter 1% was tapped of from one of the output modes, superimposed with an auxiliary local oscillator to enhance the signal and detected by two photo diodes (PD_{78} and PD_{82}). One signal was demodulated at 82 MHz to establish a phase lock for this superposition while the other was demodulated at 78 MHz to generate an error signal for the entanglement phase lock. The latter was fed back to the phase shifter (PS) in the path of the 78 MHz SSB to avoid cross talk of the two locks. A similar figure was published in [Ebe13Th].

lated at 82 MHz to establish a phase lock between the auxiliary local oscillator while the other was demodulated at 78 MHz delivering the desired phase lock signal for the superposition at the entanglement beam splitter. The error signal was fed back to a phase shifter in the path of 78 MHz SSB to avoid unnecessary cross talk with the phase lock of the auxiliary local oscillator.

PHASE LOCKED HOMODYNE DETECTION At the homodyne detectors the signal was demodulated at 82 MHz to get an error signal for the quadrature phase lock as depicted in Figure 6.3. To this end, the electronics of the detector had to be redesigned to avoid the SSB frequency entering the AC signal output port. The signal for demodulation was tapped of and buffered by an additional operational amplifier and a cascade of passive notch filters yielding a suppression of more than 80 dB was integrated to suppress the SSB frequency in the AC port below the noise level of the subsequent data acquisition system. The notch filters were centered at 80 MHz to have the freedom of changing the lock from the 78 MHz SSB to the 82 MHz SSB and achieve a comparably good suppression for both.

RANDOM SWITCHING The protocol by Furrer *et al.* requires a random choice of the detected quadrature at the homodyne detectors for each recorded signal. Since the phase lock of the local oscillator with a PZT-mounted mirror reaches unity gain frequencies of only the order of a few kHz (resulting in about 1000 quadrature switchings per sec-

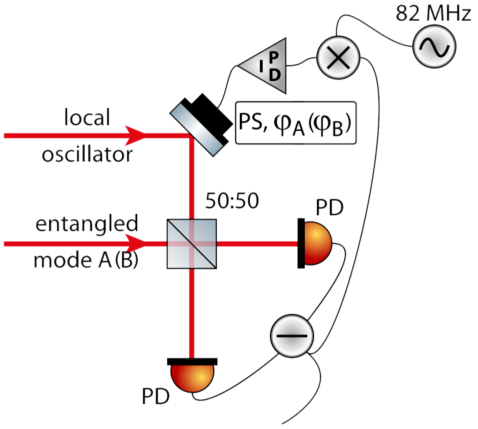


Figure 6.3: Schematic of the homodyne detection. The two entangled modes were detected on separate homodyne detectors each consisting of two photo diodes (PD). In both cases the signal was demodulated at 82 MHz and fed back to the phase shifter (PS) of the local oscillator. A similar figure was published in [Ebe13Th].

ond) the time for measuring the required 10^8 samples would exceed days. This is obviously not desirable and an additional fast phase shifting was implemented. The local oscillator was sent through a fiber-coupled electro-optical modulator (fcEOM) which allows bandwidths of hundreds of MHz (see Figure 6.4). By applying voltage shifts to the fcEOM a fast switching of the detected quadrature became possible. This technique was developed and implemented in [Ebe13Th] in cooperation with the author and used for this study without any changes.

Since the original phase lock of the homodyne detector should keep working to compensate for slow drifts of the phase while the fcEOM processes a fast switching, a sophisticated voltage pattern was implemented [Ebe13Th]. Before applying the voltage for the desired quadrature the voltage for the orthogonal quadrature is applied. This ensures that maximally for twice the inverted switching frequency the same voltage is applied. Therefore, if the frequency is significantly higher than the unity gain of the PZT phase lock, the latter always sees the average of both phases. Hence, even if for a longer time, say, 100 measurements the same quadrature is detected, the slow phase lock will not start to follow to compensate the offset.

Using this scheme a switching frequency of 200 kHz was achieved resulting in a signal frequency of 100 kHz. This leads to a measurement time of 16 min and 40 sec for 10^8 samples. The switching frequency was limited by high frequency components of the steep edge of the applied voltage. Although these are in principle not in the detected frequency band they tend to saturate the operational amplifiers of the signal path in the homodyne detectors electronic circuit and corrupt the signal.

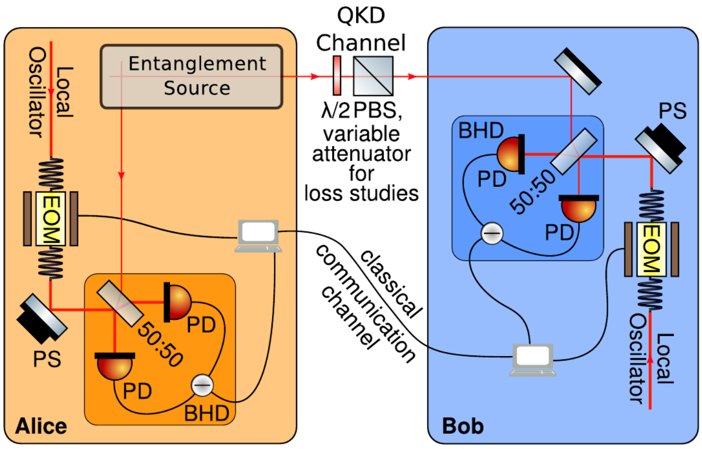


Figure 6.4: Schematic of the QKD setup. The two entangled modes were transmitted to Alice and Bob and measured by balanced homodyne detectors (BHD) each consisting of two photo diodes (PD). Apart from a slow phase control of the local oscillator with a PZT mounted mirror (PS) a fast, fiber-coupled electro-optical modulator (EOM) was implemented for switching of the quadratures. In the transmission line to Bob a half-wave plate and a polarizing beam splitter (PBS) were implemented to serve as a variable attenuator simulating long distance transmission loss.

QUANTUM RANDOM NUMBER GENERATION The random numbers for the switching were generated with an additional independent homodyne detector measuring vacuum noise. The second port of the homodyne beam splitter was mechanically blocked to ensure no parasitic signal could enter. The vacuum noise was flattened over the recorded bandwidth of 2 MHz using a whitening filter matching the electronic properties of the detector. Each measurement point was than mapped to a 0 or 1 depending on the values sign. A total of 10^{10} samples was recorded and standardized random number tests were performed on the data. After the tests were passed the random numbers were saved to a look-up table. For each QKD run a new set from this table was chosen for the random switching of the homodyne detectors. Although these random numbers were generated in advance for experimental convenience, in principle the process could be automatized to generate them on the fly during the QKD run to ensure they can not be compromised. For a detailed description see [Ebe13Th] where the system was implemented and analyzed.

SIMULATION OF LONG DISTANCE TRANSMISSION The two homodyne detectors of Alice and Bob were situated on the same table with a distance of about 50 cm, hence, the transmission line was rather short. To simulate the optical transmission loss of a more realistic scenario with several km of distance between the two parties a variable beam splitter was implemented in the path to Bob's detector as shown in Figure 6.4. Assuming 0.2 dB/km suppression of standard telecommunication fibers and an additional 0.22 dB for coupling in and out of a fiber the set optical transmissivity could be mapped to fiber length. Though this setup does not include all possible flaws of a transmission through optical fibers (see Section 6.3) it gives a good first approximation to test the robustness of the protocol.

DATA ACQUISITION AND POST PROCESSING The data acquisition system was developed, implemented and analyzed in [Ebe13Th] and only minor changes to some parameters were conducted in this thesis. It employed a two channel Signatec PX14400A PCI Express card with a 256 MHz analogue-to-digital converter. The AC signals of the homodyne detectors were lowpass filtered at 50 MHz before entering the signal inputs of the card to avoid aliasing. The sampling of the card was triggered by the pattern generator that provided the signal for the random switching. This assured that the samples were recorded precisely in the time interval described in the switching process. At each trigger event the signal was recorded with 256 MHz sampling frequency for 1 µs yielding 256 samples. These were digitally mixed with a signal between 7 MHz and 9 MHz. Due to a mysterious peak in the noise spectra of the homodyne detectors (see Figure 6.11) that occurred on a daily basis with different center frequencies between approximately 5 MHz and 7.5 MHz, the demodulation frequency of the data acquisition had to be adapted before each measurement run to avoid spurious signals. The demodulated samples were lowpass filtered at 200 kHz with a 200-tap FIR filter and down sampled by taking only the 200th sample yielding precisely the single sample that we referred to in the description of the protocol. All samples of Alice and Bob for one run of the protocol were saved to a single hdf5-file together with their appertaining quadrature choice.

The classical post processing was implemented using the software package of the AIT and the newly developed hybrid error reconciliation [Geh15]. To this end the files containing the samples were uploaded to the server of the AIT and processed by C. Pacher. This of course compromised the security of the final key. But for a proof of principle study with the unrealistic scenario of both raw keys recorded on the same computer and with no actual cryptographic application of the key we refrained from implementing the software on the laboratory computer. In principle this could be done and by furthermore implementing a parallelization of the post processing to several CPU cores the algorithm could run in real time on the recorded samples. In the current configuration on a single core the processing took approximately 2.5 hours for $2 \cdot 10^8$ samples which is about five times as long as the measurement phase. A detailed description of the software and the algorithms can be found at [AQS15].

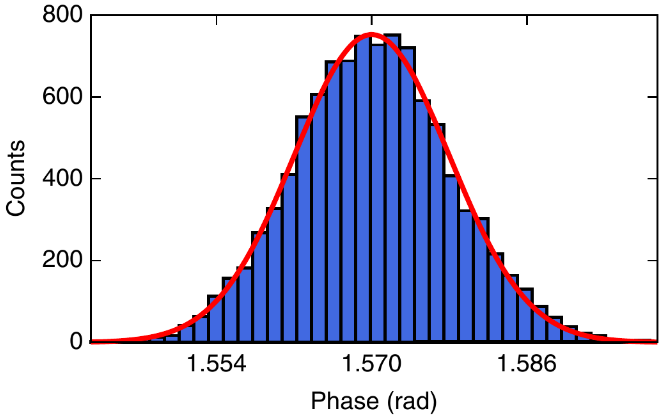


Figure 6.5: Estimation of phase noise at Alice's detector. The DC voltage of the beat between LO and control beam was recorded for 10^5 samples and fitted with a Gaussian distribution in a histogram. A standard deviation of $(0.46 \pm 0.01)^\circ$ was calculated.

PHASE NOISE ESTIMATION To estimate the phase noise of Alice's quadrature choice the DC signal of the beat between local oscillator and control beam was investigated. The output voltage of the homodyne detectors DC amplifier was calibrated to the relative phase of the signal and the LO by scanning the PZT mounted mirror for the low frequency phase lock. Afterwards a random switching was applied to the fiber-coupled EOM and the resulting voltage pattern was observed on an oscilloscope. For 10^5 switching processes a sample of the voltage was acquired in the same time interval used for data acquisition. Figure 6.5 shows a histogram of theses samples for the phase quadrature together with a fit of a Gaussian distribution plotted in red. The standard deviation of the distribution is 0.46° with an error of 0.01° determined by bootstrapping the data. This is a fairly low value considering the switching procedure [Meh11]. Since the switching was random the phase noise was identical for amplitude and phase quadrature, i.e. $V_X = V_P$.

6.2.3 *Secret Key Distribution Results*

DEPENDENCE OF THE KEY LENGTH ON THE NUMBER OF SIGNALS With the squeezed light sources delivering 10 dB and 10, 9 dB of noise reduction to the homodyne detectors, the protocol was performed and a total of $2 \cdot 10^8$ signals were recorded. The transmission loss to Bob was set to zero for this measurement. Using the reconciliation software by C. Pacher a total of 97.5 MBit of secret key could be extracted and actual bits were generated. By bootstrapping the data a reduced amount of samples was generated to investigate the performance of the protocol for fewer signals. The result for the length of generated key is shown in Figure 6.6 together with a numerical simulation fitted to the experimental data points. The simulation was conducted by T. Gehring and is based on the models developed in [Ebe13Th]. A minimum of $6 \cdot 10^6$ is required to achieve any key at all. For more than 10^8 signals the key rate approaches saturation, as expected for large numbers of samples. The maximum key rate of 0.4875 Bit/sample is achieved for the maximum recorded number of $2 \cdot 10^8$ samples.

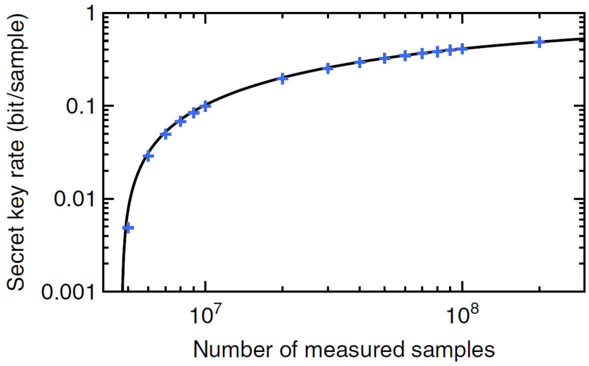


Figure 6.6: Secret key rate versus number of recorded samples. A minimum of $6 \cdot 10^6$ samples is required to achieve any key at all. For more than 10^8 samples the key rate starts to saturate. The maximum of 0.4875 Bit/sample is achieved for $2 \cdot 10^8$ samples. The black curve is a numerical simulation fitted to the experimental data points.

DEPENDENCE OF THE KEY LENGTH ON THE TRANSMISSION LOSS

The transmission loss to Bob was step wise increased by 3% points and $2 \cdot 10^8$ signals were recorded each time. The maximum possible loss was 16% or 0.76 dB, corresponding to 2.7 km optical fiber when assuming an attenuation of 0.2 dB/km and 95% coupling efficiency. Beyond this value the entanglement and homodyne phase locks became unstable due to a high suppression of the classical signals, making a QKD measurement impossible. Although this was not a fundamental limitation, a successive chain of locks were to be changed to circumvent this problem and no working point could be found to operate the experiment at 0% loss as well as at 30%. Nevertheless, the main goal of this analysis was achieved and the result is shown in Figure 6.7. Also for this measurement a numerical simulation was conducted by T. Gehring and fitted to the experimental data. The key rate decreases for increasing attenuation and drops to approximately 0.1 Bit/sample for 16% loss. This is still a reasonable amount and already demonstrates the applicability to local area networks. Additionally, the numerical simulations indicates a maximum attenuation of 1.19 dB would be possible, corresponding to 4.85 km. This is an unprecedented distance for CV QKD with security against coherent attacks and marks a milestone on the road to its application. Furthermore, in a recent extension of the security proof it was shown that the protocol is compatible with reverse reconciliation [Fur14], i.e. Alice corrects here data on Bob's measurement outcomes. With an inclusion of this in the classical post-processing a transmission length of even 16 km would become possible. Note that, in contrast to other CV-QKD implementation achieving several tens of kilometers [Lev10, Jou13a], in this realization the finite key length was taken into account, the security could not be compromised in any way by tampering with Bob's devices and no restrictions on the attack strength of an eavesdropper were made.

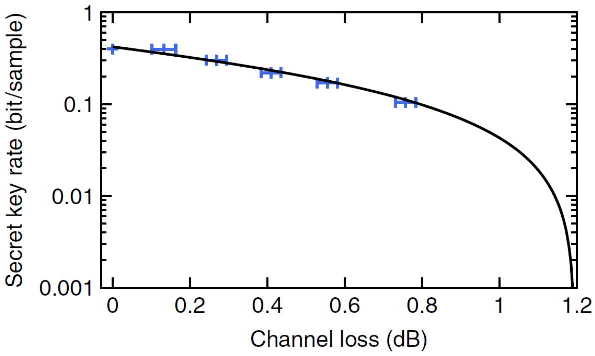


Figure 6.7: Secret key length versus transmission loss. For each attenuation $2 \cdot 10^8$ samples were recorded. The key rate decreases significantly with increasing loss. A maximum of 0.76 dB could be tolerated by the experimental setup for stable operation of the locks. The black curve is a numerical simulation fitted to the experimental data and indicates a maximum attenuation of 1.19 dB would be possible. This corresponds to 4.85 km of standard optical fiber including the coupling efficiencies.

Furthermore, we can investigate the steerability of the distributed state and extend the discussion from Section 5.3.3. The two-mode squeezed state in the experiment can in good approximation be described by the covariance matrix from Equation (4.9) to which an additional optical loss on Bob's mode has to be applied (see Appendix A.2 for a general description of the calculation). The steering criterion that we try to violate has to be the additive convex criterion from Reference [Cac09] since the security proof is based on the average distance between the data strings (see Section 6.2.1). Although there is no direct connection of this steering criterion and the channel parameter estimation, this approach gives a qualitative insight. The scaling factors in the reconciliation are chosen such that Alice and Bob observe the same variance in their X and P measurements, respectively [Geh15]. We can express this with the parameters g and h in the inferred variances (see Section 4.4), by setting them to

$$g = \sqrt{\frac{\mathrm{Var}(X_A)}{\mathrm{Var}(X_B)}},$$
$$h = \sqrt{\frac{\mathrm{Var}(P_A)}{\mathrm{Var}(P_B)}}$$

for direct reconciliation and to the inverse values for reverse reconciliation, respectively. Calculating the additive steering criterion from these inferred variances, we find the maximally tolerable transmission loss to be 46% for steering from Bob to Alice and 90% for steering from Alice to Bob. Qualitatively, this corresponds to the maximum transmission lengths of 5 km and 16 km. But the actual transmission losses in these cases are 24% and 54%, respectively, which shows a large gap between the theoretical analysis of steering and the achievable positive key rates in the QKD application. One reason is that the key length formula in Equation (6.1) does not assume the Gaussianity of the state and the measurements, in contrast to the derivation of the steering criterion. Therefore, the bounds for the relevant amounts of information have to be chosen more generally which reduces the key length drastically. Another reason is that the key length formula also includes imperfections of the measurements, the leakage of the error correction and the finite-size effects. But in [Brc12] a smaller but still significant gap between the tolerable optical losses (50% for steering and 33% for a positive key rate) was observed for a 1sDI DV QKD protocol, although none of these corrections was implemented in the corresponding key length formula. Furthermore, the authors noted that a similar gap occurs in the comparison of the violation of Bell inequalities (17%) and fully DI QKD protocols (9%) and that the effect is worth further theoretical investigation.

Finally we note that with 16 km transmission length (corresponding to 54% optical loss) the two-mode squeezed state under consideration is one-way steerable. Therefore, the analysis in [Fur14] shows that one-way steering enables 1sDI security if reverse reconciliation is employed in the protocol.

6.3 IMPLEMENTATION OF A 1 KM FIBER BASED QUANTUM CHANNEL

In the last part of this chapter we will present experiments that were made to achieve an actual fiber transmission of one of the entangled modes. In particular we will review concepts for an independent remote homodyne detector and some preliminary experimental test that were performed in the lab with a 1 km single mode fiber.

6.3.1 *Concepts for a Remote Homodyne Detector*

To set up an independent remote homodyne detector for Bob several experimental challenges have to be addressed. The homodyne detection requires an intense local oscillator that needs to be phase locked to the main laser source. This can either be realized by sending the local oscillator from the main laser through the fiber as well, or by taking a second laser at Bob's site. In the second case a phase lock of the local laser on some auxiliary field propagating trough the fiber is required. For example a small tap off from the control beam, that accompanies the distributed entangled field, could be used as phase reference. Also the influence of the fiber itself on the distributed field has to be addressed. Polarization stabilization is required to compensate for stress-induced birefringence and noise sources have to be investigated and suppressed if possible. Furthermore, the detector requires radio frequency signals that need to be phase locked to the ones of Alice's site to establish a working quadrature phase lock. Additionally, a timing signal is required to ensure that Alice and Bob will perform their measurements at the correct time, as otherwise the correlations would be spoiled.

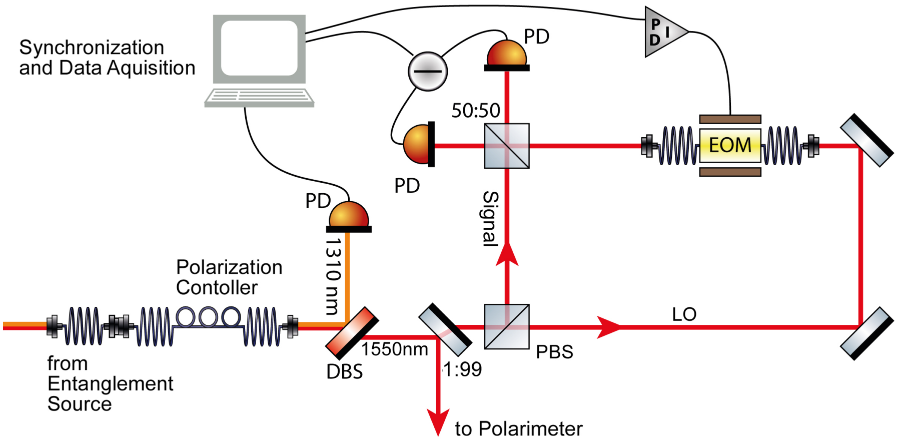


Figure 6.8: Concept for a remote detector with copropagating local oscillator. The signal and the local oscillator enter the remote detection site in orthogonal polarizations. A dynamic polarization controller ensures a stable output polarization. The auxiliary field at 1310 nm for timing and frequency locking is split from the main field at a dichroic beam splitter (DBS) and detected on a photo diode (PD). From the transmitted 1550 nm field 1% is tapped off for the lock of the polarization controller. At a polarizing beam splitter (PBS) signal and local oscillator are separated again and the local oscillator (LO) is coupled into a fast fiber-coupled electro-optical modulator (EOM) to apply the switching phases before it reaches the homodyne detector.

Figure 6.8 shows a schematic of a detector concept with copropagating local oscillator. Before entering the fiber, the entangled field and the local oscillator are superimposed at a polarizing beam splitter in orthogonal polarizations, hence, they do not interfere. This is called *polarization multiplexing*. After transmission the fields can be separated again at another polarizing beam splitter and the local oscillator is send through a fiber coupled EOM to enable fast switching of the quadratures. The fields are then brought back together at the homodyne detector, that now can be identical to the ones used in the table-top setup of the experiment. To ensure a good splitting of signal and locals oscillator a *dynamic polarization controller* is implemented directly after the km-fiber. For details of the principle and the polarization controller see Section 6.3.2. In particular a 1% tap-off has to be taken from the 1550 nm field to lock the polarization. Furthermore, a 1310 nm field is copropagating through fiber carrying frequency and timing information. This field is split off at a dichroic beam splitter and the detected signals are given to Bob's computer to establish synchronous locks and measurements.

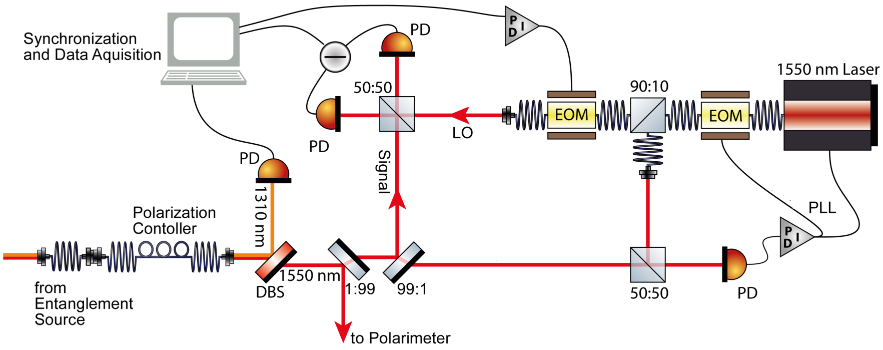


Figure 6.9: Concept for a remote detector with local oscillator from a local laser. In contrast to the previous scheme no polarization multiplexing is performed. However, the polarization of the transmitted signal has still to be controlled and a second tap-off is required to phase lock the local laser to the signal. This is done with a phase locking loop (PLL) by actuating on the lasers cavity as well as on an external fiber-coupled EOM to achieve a high bandwidth. The rest of the setup is identical to the previous concept in Figure 6.8.

Figure 6.9 shows a schematic with a second laser serving as local oscillator. In contrast to the previous scheme no polarization multiplexing is performed. Nevertheless, a polarization control is required to ensure a high contrast at the homodyne detector which again needs some tap-off from the signal beam for locking purposes. Furthermore, a second tap-off is required to establish a phase lock between the signal and the local laser source. To this end a control of the laser source itself (namely the temperature and the cavity length of the resonator) as well as an external phase control by a fast EOM is required to achieve a high unity gain frequency and, thereby, a high phase stabilized bandwidth. Otherwise the reasonably detectable bandwidth of the homodyne detector would be limited by phase noise of the local laser source against Alice's main laser. As in the scheme with copropagating local oscillator, a fiber-coupled EOM is used to apply the switching phases and also the 1310 nm field serves the same auxiliary purpose.

In comparison the second setup is technically more demanding. Not only does it require the phase locking of a fiber amplified laser source but also the signals gained for locking are rather small, as from the already weak copropagating control beams only a small fraction can be split off to not unnecessarily attenuate the signal. Therefore, in the framework of this thesis only the first concept was realized and investigated. Furthermore, the remote detector was for testing purposes set up in the same lab as Alice's site and no optical link for frequency and timing synchronization was required, since this could still be realized with longer cables.

6.3.2 *Scheme for Dynamic Polarization Control*

When light is transmitted through a single mode fiber its polarization will in general not be maintained. Stress on the fiber induces birefringence, i.e. pressure and bending will lead to a static change of the polarization and temperature fluctuations and acoustic vibrations will dynamically change it. Where the static changes can be compensated by waveplates the dynamic changes have to be actively controlled. Therefore, an all-fiber dynamic polarization controller (DPC) from General Photonics was used. The light is coupled into a single mode fiber that is placed under four PZTs. The first and the third exert pressure under 90° in respect to the table plane while the second and fourth are acting under 45°. By changing the voltage on the PZTs the induced birefringence can be controlled, while the angles under which these forces are applied stay fixed. Hence, the device can be seen as four *variable waveplates* with fixed angle of the slow axis.

To understand the control scheme of the DPC we first have to get some background on the description of polarization. We will use the Jones vector formalism where an arbitrary state of polarization of a light field propagating in z-direction can be written as

$$\vec{E} = \begin{pmatrix} E_x e^{i\psi_x} \\ E_y e^{i\psi_y} \\ 0 \end{pmatrix} e^{i(kz-\omega t)}.$$

Here $E_{x,y}$ are the amplitudes of the field in x- and y-direction and $\psi_{x,y}$ their corresponding phases. Normalizing this vector, omitting the zero z-component and neglecting the overall phase we can reduce this to

$$\vec{e} = \begin{pmatrix} \cos\varphi \\ \sin(\varphi)e^{i\psi} \end{pmatrix},$$

where ψ is the difference of ψ_x and ψ_y. Thus, for $\psi = 0$ or integer multiples of π the state is linearly polarized and φ gives the angle of polarization with respect to the x-axis.

The action of optics on the state of polarization can now be described by matrices. For example a polarizer (or one output port of a PBS) becomes a 2D-projector,

$$P_x = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad , \quad P_y = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

A half waveplate with slow axis rotated by θ with respect to the x-direction becomes an improper rotation (a rotation including a reflection),

$$\Lambda_{\frac{1}{2}}(\theta) = \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix}.$$

And a quarter waveplate with corresponding θ becomes a rotation in the complex plane,

$$\Lambda_{\frac{1}{4}}(\theta) = \frac{i-1}{2}\begin{pmatrix} \cos 2\theta - i & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta - i \end{pmatrix}.$$

All these objects can be rotated by arbitrary angles in the x-y-plane with the standard rotations of linear algebra. The actuators of the DPC have fixed angles and can therefore be described by

$$A_{1,3} = \begin{pmatrix} e^{i\kappa_{1,3}} & 0 \\ 0 & 1 \end{pmatrix} \quad , \quad A_{2,4} = \frac{1}{2}\begin{pmatrix} e^{i\kappa_{2,4}} + 1 & e^{i\kappa_{2,4}} - 1 \\ e^{i\kappa_{2,4}} - 1 & e^{i\kappa_{2,4}} + 1 \end{pmatrix},$$

where $\kappa_{1,2,3,4}$ are the phases introduced by the birefringence and depend on the voltages applied to the PZTs.

To determine the state of polarization the polarimeter depicted in Figure 6.10 was implemented. A small fraction of the light from the fiber was taken for detection and split at a 50:50 beam splitter to two detectors that consist of a PBS and a photo diode in each port whose photo currents are subtracted. In a simplified manner one could say that one detector measures the angle of polarization while the other measures the ellipticity. In the path to one detector a quarter waveplate was implemented under 45° while in the other a half waveplate was set up under 22.5°. Taking the imperfection of the PBS into account these angles had to be adjusted with a known state of perfect linear polarization so that an actual 50:50 splitting at the PBS occurred. Doing the math for an arbitrary input state of polarization $\vec{e}$, with the algebra from above we find for the two output signals

$$\begin{aligned}&|P_x \cdot \Lambda_{\frac{1}{4}}(\pi/4)\cdot\vec{e}|^2 - |P_y \cdot \Lambda_{\frac{1}{4}}(\pi/4)\cdot\vec{e}|^2\\ &= |(-i,1)\cdot\vec{e}|^2 - |(1,-i)\cdot\vec{e}|^2\\ &= -2\sin 2\varphi \sin\psi,\end{aligned}$$

and

$$\begin{aligned}&|P_x \cdot \Lambda_{\frac{1}{2}}(\pi/8)\cdot\vec{e}|^2 - |P_y \cdot \Lambda_{\frac{1}{2}}(\pi/8)\cdot\vec{e}|^2\\ &= \frac{1}{4}|(1,1)\cdot\vec{e}|^2 - \frac{1}{4}|(1,-1)\cdot\vec{e}|^2\\ &= \sin 2\varphi \cos\psi.\end{aligned}$$

Hence, both signals depend on the the polarization angle φ and the ellipticity ψ and we see that the angle has to be stabilized to an uneven integer multiple of $\pi/4$ to obtain maximum signal amplitude.

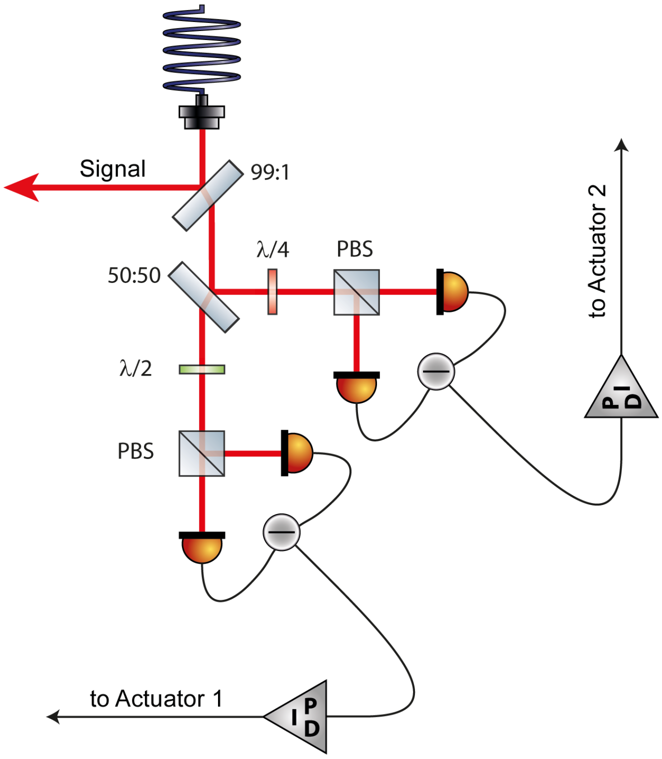


Figure 6.10: Schematic of the polarimeter. A 1% tap-off from the signal is used to analyze the state of polarization. The tap-off is split up at a 50:50 beam splitter. One output is send through a λ/2-waveplate under 22.5° to a polarizing beam splitter (PBS) while the other is sent through a λ/4-waveplate under 45°. The intensities of the two outputs of each PBS are subtracted which gives two error signals for the polarization controller.

Now the first three actuators of the DPC are used to change the state of polarization. The fourth is just needed for polarization scrambling. The calculation for the signals from the actuated state get a bit lengthy and have been performed in a Mathematica script. A commented version of the script can be found in appendix A.3 and we will just state the result here. The signals from the two detectors read

$$\begin{aligned} S_1 &:= |(-i,1)\cdot A_3 \cdot A_2 \cdot A_1 \cdot \vec{e}|^2 - |(1,-i)\cdot A_3 \cdot A_2 \cdot A_1 \cdot \vec{e}|^2 \\ &\propto \sin 2\varphi\,[\sin\kappa_3 \cos(\kappa_1-\psi) + \cos\kappa_2 \cos\kappa_3 \sin(\kappa_1-\psi)] \\ &\quad - \cos 2\varphi\,[\sin\kappa_2 \cos\kappa_3]\,, \end{aligned}$$

and

$$\begin{aligned} S_2 &:= \frac{1}{4}|(1,1)\cdot A_3 \cdot A_2 \cdot A_1 \cdot \vec{e}|^2 - \frac{1}{4}|(1,-1)\cdot A_3 \cdot A_2 \cdot A_1 \cdot \vec{e}|^2 \\ &\propto \sin 2\varphi\,[\cos\kappa_3 \cos(\kappa_1-\psi) - \cos\kappa_2 \sin\kappa_3 \sin(\kappa_1-\psi)] \\ &\quad + \cos 2\varphi\,[\sin\kappa_2 \sin\kappa_3]\,. \end{aligned}$$

By plotting these signals in Mathematica and investigating their behavior for changing offsets of the phases κ_1 to κ_3, a configuration could be found where independent sinusoidal error signals for φ and ψ are obtained. A detailed description can be found in the comment of the script. One solution is obtained for the offsets $\kappa_1 = \kappa_2 = \kappa_3 = \pi/2$. The signals than read

$$\begin{aligned} S_1 &\propto \sin 2\varphi \sin\psi, \\ S_2 &\propto \cos 2\varphi. \end{aligned}$$

By feeding back signal S_1 to actuator A_1 and signal S_2 to actuator A_2 with a PID controller, the PZTs were controlled in such a way that both signals vanished. Hence, ψ is stabilized to 0 while φ is stabilized to $\pi/4$. The resulting output state is the input state with these values to which the three actuations with the given offsets of the PZT induced phases have been applied,

$$A_3(\pi/2)\cdot A_2(\pi/2)\cdot A_1(\pi/2)\cdot \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix},$$

We see that it is linearly polarized in x-direction. Note that no actuation is given to κ_3 because it only acts as a compensation for the initial offset of κ_1. All the "magic" is happening with the first two actuators and the third one is only needed to achieve usable error signals. The reader might want to take a look at the mentioned description in the appendix.

6.3.3 *Distribution of a Squeezed Field Through a 1 km Fiber*

With the polarization controller operational, a homodyne detector was set up at the remote site, which was identical to the detectors at the local site except that the fiber coupled EOM was not implemented for the first test. As all classical signals were copropagating through the fiber as well, all electronics for the quadrature lock could simply be copied from the local detector of Bob. Using this setup a preliminary test was made by measuring the vacuum noise at the remote detector. No signal was coupled into the fiber to solely investigate the influence of the fiber transmission, the polarization control and the polarization splitting on a pure coherent state. The result is shown in Figure 6.11. The power of the transmitted local oscillator beam was tuned from 5 mW down to 100 µW and for each setting the noise level was measured with the signal port of the homodyne detector once open and once blocked. These two corresponding curves are depicted in the same color. Additionally, the dark noise of the detector is shown in black. The noise level was observed from 2 MHz to 100 MHz sideband frequency. A significant difference in the noise levels is visible for all powers with the higher noise level always belonging to the measurement with the open signal port. This would make a squeezing measurement impossible because it would completely be covered by noise that obviously stems from the local oscillator. But the additional noise diminishes for lower powers and for 100 µW the two curves are pretty close to each other at least in the targeted detection band at about 8 MHz.

The characteristic power dependence and the pattern of the peaks in the noise spectra with open signal port indicated that the additional noise stems from guided acoustic wave Brillouin scattering [She85]. Brillouin scattering is the process of a photon being scattered by a phonon while transmitting through a solid body like a glass fiber. The effect strongly depends on the power of the transmitted field, since the scattering gets more likely when more photons are present. The scattered photons get a frequency shift and typically the first peak from a transmission through an optical fiber arises around 20 MHz. Furthermore the scattered photons are also shifted in their polarization. Therefore, even though the polarization controller stabilized the local oscillators polarization to reflection at the PBS, the scattered photons also occurred in the orthogonal polarization and were transmitted through the PBS. This resulted in a signal at the homodyne detector and spoiled the vacuum noise. Furthermore, the aforementioned mysterious peak in the dark noise spectrum of the homodyne detectors is visible in the figure at about 6.5 MHz.

To circumvent this problem the measurements of the squeezing transmission were performed with as low locals oscillator power as possible. As visible in Figure 6.11 the dark noise clearance for 100 µW

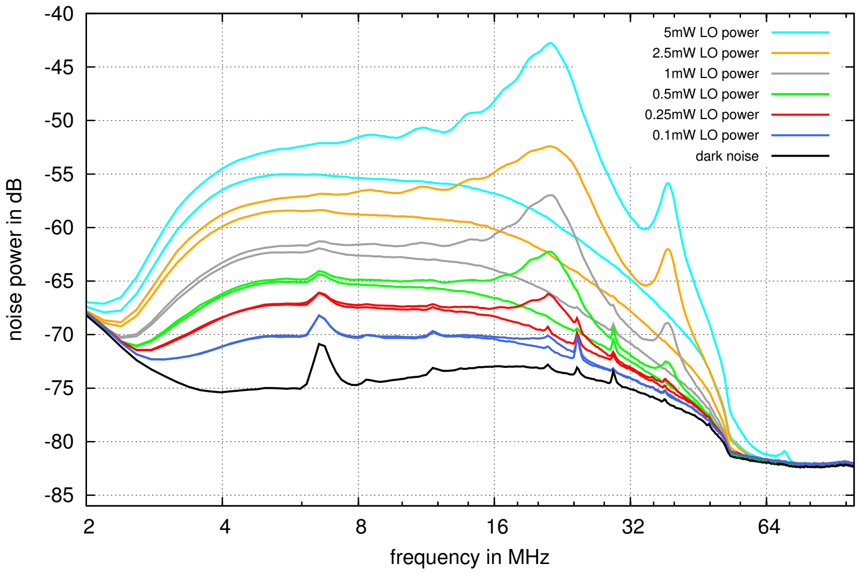


Figure 6.11: Noise measurement at the remote detector for different LO powers. For each power of local oscillator the noise power at the homodyne detector was measured with the signal port once open and once closed, depicted for each power in the same color. The significant and power dependent difference of the noise levels could be traced back to Brillouin scattering and made a squeezing measurement with higher local oscillator powers impossible. See the main text for details.

local oscillator was only about 5 dB at 8 MHz. By reducing the power to 60 μW the clearance was even further decreased to only 3 dB. Therefore, from all noise measurements the dark noise level was subtracted to obtain meaningful results. By doing so the linearity of the homodyne power could be proven as visible in Figure 6.12. Decreasing the power by a factor of two resulted in a drop of the noise power by 3 dB and the squeezing measurement could be performed with only 60 μW of local oscillator power.

The result of the squeezing transmission is shown in Figure 6.13 together with a theoretical model following Equation (5.1) with the parameter settings $\Omega = 8\,\mathrm{MHz}$, $l = 64.6\,\mathrm{mm}$, $T = 0.1$ and $L = 0.043$. The pump power was varied from 25 mW to 225 mW and each time the squeezed and the anti-squeezed noise level was measured. The theoretical description was fitted to the data points using the detection efficiency η and the pump threshold P_{th} and were found to be $\eta = 0.515$ and $P_{th} = 250\,\mathrm{mW}$.

The overall detection efficiency consists of several contributing factors. The squeezed light source has an outcoupling efficiency of $\eta_{coup} = 0.965$. Four mirrors of a periscope in the path to fiber were hit in p-polarization for which they are not optimized and each contributing an efficiency of $\eta_{mi} = 0.99$. A Faraday isolator was implemented before the fiber incoupling to prevent access to the squeezed-light source from the quantum channel in prospect of the QKD applica-

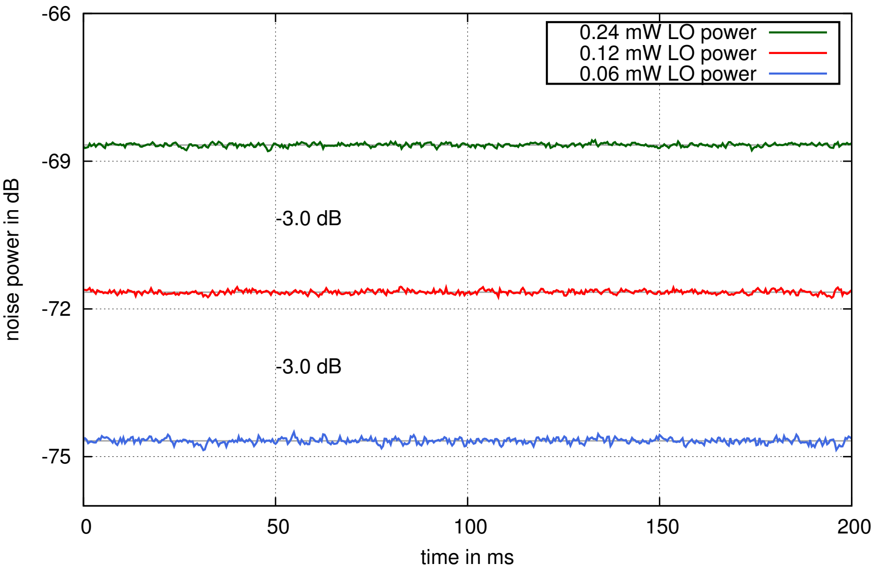


Figure 6.12: Investigation of the linearity of the homodyne detector at low LO powers. The vacuum noise at the homodyne detector was measured at three different powers of the local oscillator (LO), each time decreased by a factor of two. The dark noise level was subtracted and each time a decrease by 3 dB was observed which proved the homodyne detector to be linear even at very low local oscillator powers.

tion and contributed a transmission efficiency of $\eta_{\mathrm{FI}} = 0.95$. The fiber itself had a transmission efficiency of $\eta_{\mathrm{fi}} = 0.656$ including the in- and outcoupling efficiency. The DPC had a measured transmission efficiency of $\eta_{\mathrm{DPC}} = 0.92$. Further propagation loss was estimated to result in $\eta_{\mathrm{prop}} = 0.98$ and the homodyne detector contributed with a contrast of $\eta_{\mathrm{con}} = 0.995$ and a quantum efficiency of the photo diodes of $\eta_{\mathrm{PD}} = 0.99$. Hence, the total detection efficiency is calculated to be $\eta = \eta_{\mathrm{coup}} \cdot \eta_{\mathrm{mi}}^4 \cdot \eta_{\mathrm{FI}} \cdot \eta_{\mathrm{fi}} \cdot \eta_{\mathrm{DPC}} \cdot \eta_{\mathrm{prop}} \cdot \eta_{\mathrm{con}}^2 \cdot \eta_{\mathrm{PD}} = 0.515$ in accordance with the fitted value. Of all the values only the transmissivity of the fiber link was unexpectedly high in comparison to usual values of 0.97 per coupling and 0.95 per kilometer. Since also the LO beam experienced the high damping, a problem with coupling the beam from a squeezed-light source into a fiber could be excluded. Furthermore, a direct coupling of a light field via a fiber-fiber coupler from the remote (Bob's) end of the fiber showed that the channel itself did not exceed the expected 5% loss per kilometer. Therefore, only the coupler at Alice's end of the fiber could have caused the loss, probably due to a production fault of the connector. Thus, only a replacement of the fiber would have overcome the problem, but a second kilometer scale fiber was not available for this study.

Where in the case of the local oscillator the high loss could be compensated by increasing the power, for the squeezed field, the low transmissivity meant a drastic limitation of the achievable noise reduction at the remote homodyne detector. Nevertheless, a maximum

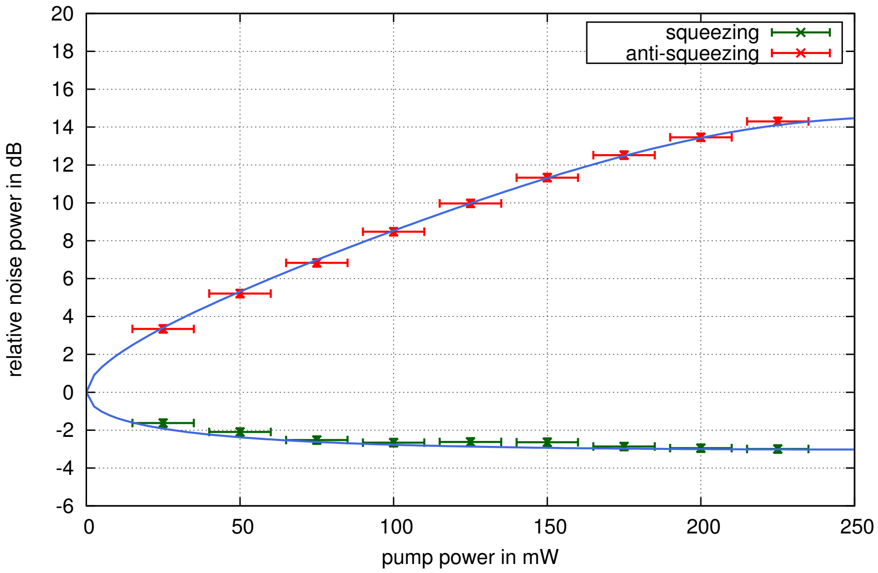


Figure 6.13: Measurement of squeezing after 1 km of fiber for varying pump power. The pump power was changed between 25 mW and 225 mW in steps of 25 mW and each time the squeezed and the anti-squeezed noise was measured and normalized to the vacuum noise level. The theoretical model fitted to the data is described in the text.

of 3 dB squeezing could be achieved which still is a very convincing level of non-classicality considering 1 km optical path length.

6.3.4 *Distribution of Entanglement Through a 1 km Fiber*

As a final test, one mode of an entangled state was distributed through the fiber. In contrast to the squeezing measurement no dark noise subtraction is possible in an entanglement measurement, since the determination of the correlations has to happen on the raw measurements before any noise levels can be calculated. So the expected amount of entanglement was ultimately limited by the dark noise clearance of the homodyne detector. Note that uncorrelated electronic dark noise has the same influence as optical loss, i.e. the approximately 3 dB dark noise clearance resulted in an additional 50% loss. Furthermore, in the data acquisition system a delay had to be implemented for the recorded data stream of Bob's channel. This had to compensate the travel time of about 5 µs of the light trough the fiber, as the correlations from entanglement only are observed on fields that were at the same time at the entanglement beam splitter. This time delay had also to be tunable to change it from time to time, as temperature fluctuations changed the exact travel time of the light.

The measurement was performed with v-class states as well as with s-class states. In each case a partial tomographic measurement was performed and the covariance matrices were reconstructed, yielding

$$\gamma_{\text{v-class}} = \begin{pmatrix} 0.58 & (0) & 0.22 & (0) \\ (0) & 11.01 & (0) & -5.80 \\ 0.22 & (0) & 0.89 & (0) \\ (0) & -5.80 & (0) & 4.27 \end{pmatrix}$$

and

$$\gamma_{\text{s-class}} = \begin{pmatrix} 17.94 & (0) & 9.68 & (0) \\ (0) & 15.19 & (0) & -8.12 \\ 9.68 & (0) & 6.08 & (0) \\ (0) & -8.12 & (0) & 5.23 \end{pmatrix}.$$

The values in brackets were not reconstructed. The v-class measurement showed a violation of the Duan criterion from Equation (4.1) by $-1.09\,\text{dB}$ with the optimal scaling parameter chosen as $a = 0.758$. This is a significant demonstration of entanglement being distributed. Furthermore, the state violated the EPR-Reid criterion for Bob conditioning his measurements on Alice's (Equation (4.7)) with a value of 0.98, i.e. it was concisely showing steering from Alice and Bob. On the other hand steering from Bob to Alice was not present as expected and the state delivered a value of 1.65 from the criterion in Equation (4.8). The s-class measurement showed with $-1.72\,\text{dB}$ a stronger violation of the Duan criterion. In Figure 6.14 a time series of the difference variance of the amplitude quadratures (blue) and the sum variance of the phase quadratures (red) is shown. Both traces are normalized to the vacuum (black). The optimal scaling parameter was $a = 0.74$. The steering from Alice to Bob was also more significant and the criterion was violated with a value of 0.76. Also with the s-class state no steering from Bob to Alice could be observed and a value of 6.51 was obtained from the criterion. Therefore, this is a demonstration of one-way EPR-steering with s-class entanglement.

The results of the measurements show that the distribution of entanglement through 1 km of optical fiber is in principle possible. Nevertheless, the comparably weak violations of the entanglement criteria suggest that an application to QKD with the current achievements is not possible. The limited strength of the correlations would, on the one hand, give a large lower bound on the distance parameter d^0_{pe}. On the other hand, it would increase the overlap of independent measurements and the bin size δ would have to be increased. Also the leakage term would probably increase, as the weaker correlations would lead to more errors in Bob's bit string. Therefore the protocol, if not aborted anyway, would give a negative key length due to the

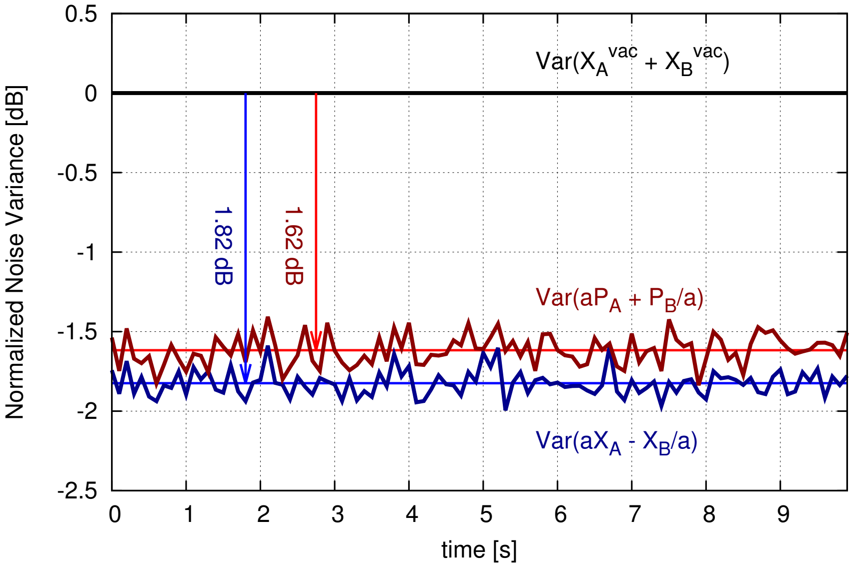


Figure 6.14: Measurement of s-class entanglement after 1 km of fiber. The difference variance of the amplitude quadrature (blue) and the sum variance of the phase quadratures (red) are plotted versus measurement time. The optimal scaling parameter was $a = 0.74$. The average variances are $-1.82\,\mathrm{dB}$ for the amplitude quadratures and $-1.62\,\mathrm{dB}$ for the phase quadratures, resulting in a violation of the Duan criterion from Equation (4.1) by $-1.72\,\mathrm{dB}$.

monotonic increase of c and γ in the relevant range of their arguments in Equation (6.1). Finally, the one-sided device independence of the security would also not be possible, because the distributed state only showed one-way steering but two-way steering is required to allow this feature in the current protocol.

We would like to point out that these limitations were not of fundamental quantum physical origin. The achieved values of the Duan and the EPR-Reid criterion, respectively, are completely explainable with the mentioned problems of the low LO power and the high transmission loss. From this we conclude that the limitations were purely technical and can be overcome with future developments. For example the results imply that a local laser has to be used as LO at Bob's remote station. Furthermore, the fiber should be replaced or a new connector should be spliced to it to achieve a high incoupling efficiency that should allow about 15% transmission loss over a 1 km distance. With these improvements a secure distribution of a quantum key should become feasible, as the loss analysis in Figure 6.7 shows.

7

CONCLUSION AND PROSPECT

Quantum key distribution is probably one of the most promising future communication technologies. It will allow secure information exchange based on quantum physical principles and mathematical proofs. Thereby, the security of the key is not only guaranteed during the distribution phase but also for all future times. Since the key is based on quantum measurements, it can never be accessed retroactively and anything encoded with it stays secret forever. This is maybe the biggest advantage of quantum key distribution over classical encryption algorithms. To enable such protocols a deep understanding of the quantum theoretical background as well as of the experimental realizations and technologies is necessary. The aim of this thesis was to examine Einstein-Podolsky-Rosen steering and to investigate its application for quantum key distribution with Gaussian continuous variables.

In Chapter 4 we have applied a thorough theory of entanglement on two-mode squeezed states and shown that certain states exhibit one-way steering. These states lead to the situation that two experimenters measuring the same observables on the same state would describe it in qualitatively different ways, as one of them would observe steering while the other does not. In Chapter 5 these findings were experimentally verified for the first time. The existence of Gaussian one-way steering was demonstrated with high statistical significance. The criterion (4.7) for steering from Alice to Bob was violated by more than 30 standard deviations whereas criterion (4.8) for steering from Bob to Alice was *not* violated with a significance of more than 50 standard deviations. Hence, depending on whether Alice tries to steer Bob's system, or Bob tries to steer Alice's system, the prepared state provided two opposing answers.

Furthermore, a detailed analysis of the states for varying experimental parameters showed an almost perfect accordance with the theoretical description. On the one hand, this means that the theory is thoroughly describing the states under consideration and predicts the measurement results with greatest possible accuracy. On the other hand, it shows that the experimental generation and control of Gaussian quantum optical states with very specific properties is well understood and achievable with current technology. The experimental result itself is of fundamental importance for our understanding of continuous variable entanglement. It does not only prove that the class of steerable states has to be divided into subclasses for the different steering directions but it also has implications on other entanglement applications and quantum information theory. By today the effect has already triggered a series of theoretical developments [Buo12, Che13, Qui15, He15] and is known in a variety of systems with continuous variables as well as with discrete variables [Lee13, Bol03b, Tan15, Ols15, Yan15]. Furthermore, the necessary absence of two-way steering for entanglement distribution by separable states can be proven. Also the connection between steering and one-sided device independent security of quantum key distribution has been known a couple of years. Here, the absence of two-way steering spoils the necessary conditions for the currently employed protocol. Only with the inclusion of reverse reconciliation one-way steering would enable one-sided device independence. This connection of one-way steering and data reconciliation was only presented in a heuristic way in this thesis. The coincidence in the description suggests a common foundation of both effects and is a topic of ongoing theoretical research.

In the second experiment presented in this work an application of steering for continuous variable quantum key distribution was successfully implemented. The measurement results presented in Chapter 6 demonstrate the generation of a usable quantum key from homodyne measurements on strongly entangled two-mode squeezed states. The maximum key length of 97.5 MBit is an unprecedented result for entanglement-based continuous variable quantum key distribution. The thorough implementation of the protocol was enabled by newly developed techniques for the stabilization of the squeezed light sources and the random switching of the homodyne measurements. It allowed composable and one-sided device independent security against the most general coherent attacks. This means the secrecy of the key was achieved without any assumptions on the eavesdropper and the devices of the remote party can be untrusted without compromising this security. The inclusion of finite size effects in the security proof also made the result directly applicable to real world implementations that will always be limited in the number of recorded samples. These real world implementations were further supported by a loss study on the entangled mode sent to Bob. The results suggest that a maximum transmission length of about 5 km through standard telecommunication fiber would be possible. With reverse reconciliation that, based on a recent extension of the security proof, can be implemented in the protocol, distances of about 16 km should become feasible. Therefore, the results of these experiments are a major step towards the application of entanglement-based continuous variable quantum key distribution with state-of-the-art security in local area fiber networks and demonstrate the relevance of steering for quantum information applications.

In further experiments the distribution of non-classical states with optical fibers was investigated. Technical problems were found to be a major obstacle for the generation of sufficiently strong correlations between the remote measurement outcomes after a 1 km fiber. Due to optical loss of 48.5%, the achievable non-classicality was ultimately limited. This high value was caused by a connector of the fiber which could not be replaced. Additionally, Brillouin scattering of the polarization multiplexed copropagating local oscillator required a drastic reduction of its power, which also resulted in a significant reduction of the dark noise clearance of the homodyne detection. Although these influence were purely technical limitation, they could not be overcome within the framework of this thesis. Nevertheless, with a local oscillator power of only 60 μW and a dark noise clearance of no more than 3 dB the distribution of a 3 dB squeezed vacuum state and a 1.7 dB two-mode squeezed vacuum state could be demonstrated. Where this was not sufficient for the generation of a secret quantum key, it still fundamentally demonstrates the feasibility of entanglement distribution through optical fibers. Especially since the achieved entanglement strength was in accordance with the observed level of decoherence in the setup, it shows that the distribution of reasonably strong entanglement should become possible by overcoming the technical issues.

The last results suggest that for future developments a local laser should be used as local oscillator at the remote detector and a significant reduction of the transmission loss should be achieved to allow a stronger non-classicality of the distributed state. In the table-top setup a change of the locking scheme for the squeezed light sources to the one used in [Vaho8Th] could be an upgrade. Alternatively, double-resonant squeezed-light sources could be used which stabilize the cavity length via the pump beam. Both options would spare the control beam that produces spurious signal at the homodyne detectors during switching. Therefore, an inclusion of such a scheme should allow a significant increase of the switching frequency, since in the current setup it was only limited by the settling time of the spurious signals. Furthermore, a future project could be to experimentally test other quantum communication tasks like the recently proposed protocols for oblivious transfer and bit commitment [Fur15]. On the theoretical side a further development of the mathematical techniques used in the security proofs would be desirable. On the one hand, the gap between the secret key rates for collective attacks and for coherent attacks could be closed. This would enable much longer keys with security against coherent attacks from the same number of samples and also increase the achievable transmission distances. On the other hand, a theoretical investigation could maybe even show that no EPR source is required but that the same level of security is achievable with Gaussian modulations. This would not only reduce the required experimental resources but also again increase the achievable transmission distance, since classical modulations are less sensitive to optical loss than entanglement.

A

MATHEMATICAL AND COMPUTATIONAL DETAILS

A.1 INFLUENCE OF THE ELECTRONIC DEMODULATION PHASE ON THE HOMODYNE SIGNALS

We would like to make a comment on the electronic demodulation phase that we have set to zero in Section 3.3. If we shift the cosine in Equation (3.4) by an arbitrary phase β Equation (3.6) gives

$$\hat{X}_{\Omega_0,\theta,\beta}(t) = \mathcal{C}\left(\hat{X}_{\theta-\beta}(\Omega_0) + \hat{X}_{\theta+\beta}(-\Omega_0)\right). \tag{A.1}$$

Hence, the measured signal amplitude is no longer the sum of the same quadrature amplitudes of the two sidebands but of those quadratures tilted opposing by the angle β. Nevertheless, the resulting variance of this signal amplitude is still the same. This is because the angle β contributes in the variance only in terms of the form $\hat{a}_{\pm\Omega_0}\hat{a}^\dagger_{\mp\Omega_0}$ that obtain a phase $e^{\mp 2i\beta}$. And these combinations of mode operators have a vanishing expectation value with respect to a squeezed vacuum,

$$\begin{aligned}
\langle \hat{a}_{\pm\Omega_0}\hat{a}^\dagger_{\mp\Omega_0}\rangle_{sqz} &= \langle 0|\hat{S}(\xi)^\dagger \hat{a}_{\pm\Omega_0}\hat{S}(\xi)\hat{S}(\xi)^\dagger \hat{a}^\dagger_{\mp\Omega_0}\hat{S}(\xi)|0\rangle \\
&= \langle 0|\left(\hat{a}_{\pm\Omega_0}\cosh(r) - \hat{a}^\dagger_{\mp\Omega_0}e^{\pm i\varphi}\sinh(r)\right) \\
&\qquad \cdot \left(\hat{a}^\dagger_{\mp\Omega_0}\cosh(r) - \hat{a}_{\pm\Omega_0}e^{\mp i\varphi}\sinh(r)\right)|0\rangle \\
&= \langle 0|\left(\hat{a}_{\pm\Omega_0}\hat{a}^\dagger_{\mp\Omega_0}\cosh^2(r) - \hat{a}^{\dagger 2}_{\mp\Omega_0}e^{\pm i\varphi}\sinh(r)\cosh(r)\right) \\
&\qquad - \left(\hat{a}^2_{\pm\Omega_0}e^{\mp i\varphi}\sinh(r)\cosh(r) - \hat{a}^\dagger_{\mp\Omega_0}\hat{a}_{\pm\Omega_0}\sinh^2(r)\right)|0\rangle \\
&= 0.
\end{aligned} \tag{A.2}$$

We see that the detected quadrature variance will be completely independent of the demodulation phase β. This is in perfect accordance with the previous result, as we will see in the following argument. Suppose we have squeezing at the quadrature phase θ, and correspondingly anti-correlations in the sideband quadratures $\hat{X}_\theta(\pm\Omega_0)$. Then, setting β to $\pi/2$ will give the sum of the orthogonal, correlated sideband quadratures but with opposing signs, as they were rotated in opposing directions. So we actually get the difference of the aligned quadratures which has, as we have seen above, again a squeezed variance. This result shows that the demodulation phase at the homodyne detector is irrelevant for a squeezing measurement. It does not contradict our statement above, that there is no possibility to measure the difference of the sideband quadratures with a homodyne detector, but merely shows that there is no *ab initio* definition of which quadrature is the squeezed one and which the anti-squeezed. This arbitrariness in phase is only removed as soon as there is a LO as phase reference.

Furthermore, if we compare equation (A.1) with equation (3.5) we see that the demodulation phase β acts similar to the time-dependent quadrature angle χ. So proving that the demodulation phase does not change the variance also proves that the oppositely rotating quadratures at $\Omega \neq \Omega_0$ have the same combined variance as the quadrature at exactly Ω_0 with a fixed quadrature angle. So for number states and squeezed vacua we can actually restrict our description to equation (3.6).

A.2 DERIVATION OF ANALYTIC FUNCTIONS FOR GAUSSIAN STEERING

We will derive the left-hand sides of EPR-Reid criteria from Equations (4.7) and (4.8) as analytic functions of the experimental parameters. A detailed mathematical background can be found in [Fra12Th]. We start with two squeezed states described by the squeezing parameters ζ_1 and ζ_2 from Section 2.3.3. For simplicity let us make the assumption that $\zeta_1 = r_1$ and $\zeta_2 = -r_2$, hence, the first state is amplitude squeezed and the second is phase squeezed. Than the covariance matrix in our standard basis of not rotated quadrature operators is diagonal and reads

$$\gamma_{\text{in}} = \begin{pmatrix} e^{-2r_1} & 0 & 0 & 0 \\ 0 & e^{2r_1} & 0 & 0 \\ 0 & 0 & e^{2r_2} & 0 \\ 0 & 0 & 0 & e^{-2r_2} \end{pmatrix}. \tag{A.3}$$

Now we apply the beam splitter formalism from Equation (3.2) to entangle the two squeezed modes at a beam splitter with transmissivity t,

$$\gamma_{\text{ent}} = U_{BS}(t)\gamma_{\text{in}}U_{BS}(t)^T. \tag{A.4}$$

Next we have to take into account the optical loss $\varepsilon_A = 1 - \eta_A$ in the path to Alice and for Bob $\varepsilon_B = 1 - \eta_B$, respectively. To this end we have to expand the covariance matrix by two independent vacuum modes and embed it in a larger Hilbert space $\mathcal{H} \otimes \mathcal{H}_{\text{vac,A}} \otimes \mathcal{H}_{\text{vac,B}}$,

$$\gamma_{\text{ent,vac}} = \begin{pmatrix} \gamma_{\text{ent}} & \\ & \mathbb{1}_4 \end{pmatrix}. \tag{A.5}$$

By applying a beam splitter operation that mixes Alice's mode with the first vacuum and Bob's with the second we can then simulate the optical loss,

$$\gamma_{\text{ent,loss}} = U_{BS}^{1,3}(\sqrt{\eta_A})U_{BS}^{2,4}(\sqrt{\eta_B})\gamma_{\text{ent,vac}}U_{BS}^{2,4}(\sqrt{\eta_B})^T U_{BS}^{1,3}(\sqrt{\eta_A})^T. \quad \text{(A.6)}$$

Finally we have to take out the upper left 4×4 block which is the part that we can actually measure,

$$\gamma = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \gamma_{\text{ent,loss}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad \text{(A.7)}$$

to get the covariance matrix γ that describes the detected two-mode squeezed state. From this we can determine the symplectic invariants from Equation (2.44) to find the conditional variance products

$$\frac{I_4}{I_1} = e^{2(r_1+r_2)} \frac{f_1^2 - f_2^2}{g_1(\varepsilon_A, t) g_2(\varepsilon_A, t)} \quad \text{(A.8)}$$

and

$$\frac{I_4}{I_2} = e^{2(r_1+r_2)} \frac{f_1^2 - f_2^2}{g_1(\varepsilon_B, 1-t) g_2(\varepsilon_B, 1-t)}, \quad \text{(A.9)}$$

with

$$\begin{aligned} f_1 &= \sinh(r_1 + r_2)(\varepsilon_B - \varepsilon_A)(1-2t) + \sinh(r_1 - r_2)(1 - \varepsilon_A - \varepsilon_B), \\ f_2 &= \cosh r_1 \cosh r_2 - \sinh r_1 \sinh r_2 (1 - 2\varepsilon_A)(1 - 2\varepsilon_B), \\ g_1(\varepsilon, t) &= \varepsilon e^{2r_2} + (1-\varepsilon)\left[(1-t)e^{2(r_1+r_2)} + t\right], \\ g_2(\varepsilon, t) &= -\varepsilon e^{2r_1} - (1-\varepsilon)\left[t e^{2(r_1+r_2)} + (1-t)\right]. \end{aligned} \quad \text{(A.10)}$$

A.3 MATHEMATICA NOTEBOOK TO INVESTIGATE THE LOCKING SCHEME FOR THE DYNAMIC POLARIZATION CONTROLLER

As the calculation for the dynamic polarization controller (DPC) get rather involved, a Mathematica notebook was used to simulated the states of polarization as well as the error signals. All details are given in the comments between the code lines.

```
In[1]:=  Clear[φ, ψ, k1, k2, k3]

         (*Definition of the three actuators*)
         A1 = {{Exp[I * k1], 0}, {0, 1}}
         A2 = 1 / 2 * {{Exp[I * k2] + 1, Exp[I * k2] - 1}, {Exp[I * k2] - 1, Exp[I * k2] + 1}}
         A3 = {{Exp[I * k3], 0}, {0, 1}}

         (*Definition of the input state*)
         x = {{Cos[φ]}, {Sin[φ] * Exp[I * ψ]}}

         (*Definition of the actuated state*)
         y = A3.A2.A1.x

Out[2]=  {{ⅇ^(ⅈ k1), 0}, {0, 1}}

             1                  1                     1                   1
Out[3]=  {{ - (1 + ⅇ^(ⅈ k2)),  - (-1 + ⅇ^(ⅈ k2))}, { - (-1 + ⅇ^(ⅈ k2)),  - (1 + ⅇ^(ⅈ k2))}}
             2                  2                     2                   2

Out[4]=  {{ⅇ^(ⅈ k3), 0}, {0, 1}}

Out[5]=  {{Cos[φ]}, {ⅇ^(ⅈ ψ) Sin[φ]}}

             1                                          1
Out[6]=  {{ - ⅇ^(ⅈ k1+ⅈ k3) (1 + ⅇ^(ⅈ k2)) Cos[φ] +  - ⅇ^(ⅈ k3+ⅈ ψ) (-1 + ⅇ^(ⅈ k2)) Sin[φ]},
             2                                          2
            1                                    1
          { - ⅇ^(ⅈ k1) (-1 + ⅇ^(ⅈ k2)) Cos[φ] +  - ⅇ^(ⅈ ψ) (1 + ⅇ^(ⅈ k2)) Sin[φ]}}
            2                                    2

In[7]:=
         (*Substracted photo current from the detector with quater waveplate*)
         FullSimplify[FullSimplify[ComplexExpand[Conjugate[{{-I, 1}}.y]] * ComplexExpand[{{-I, 1}}.y]] -
           FullSimplify[ComplexExpand[Conjugate[{{1, -I}}.y]] * ComplexExpand[{{1, -I}}.y]]]

Out[7]=  {{2 (Cos[k1 - ψ] Sin[k3] Sin[2 φ] + Cos[k3] (-Cos[2 φ] Sin[k2] + Cos[k2] Sin[2 φ] Sin[k1 - ψ]))}}

In[8]:=
         (*Substracted photo current from the detector with half waveplate*)
         FullSimplify[
          FullSimplify[ComplexExpand[Conjugate[1 / 2 * {{1, 1}}.y]] * ComplexExpand[1 / 2 * {{1, 1}}.y]] -
           FullSimplify[ComplexExpand[Conjugate[1 / 2 * {{1, -1}}.y]] * ComplexExpand[1 / 2 * {{1, -1}}.y]]]

             1
Out[8]=  {{ - (Cos[2 φ] Sin[k2] Sin[k3] + Sin[2 φ] (Cos[k3] Cos[k1 - ψ] - Cos[k2] Sin[k3] Sin[k1 - ψ]))}}
             2
```

In[9]:=

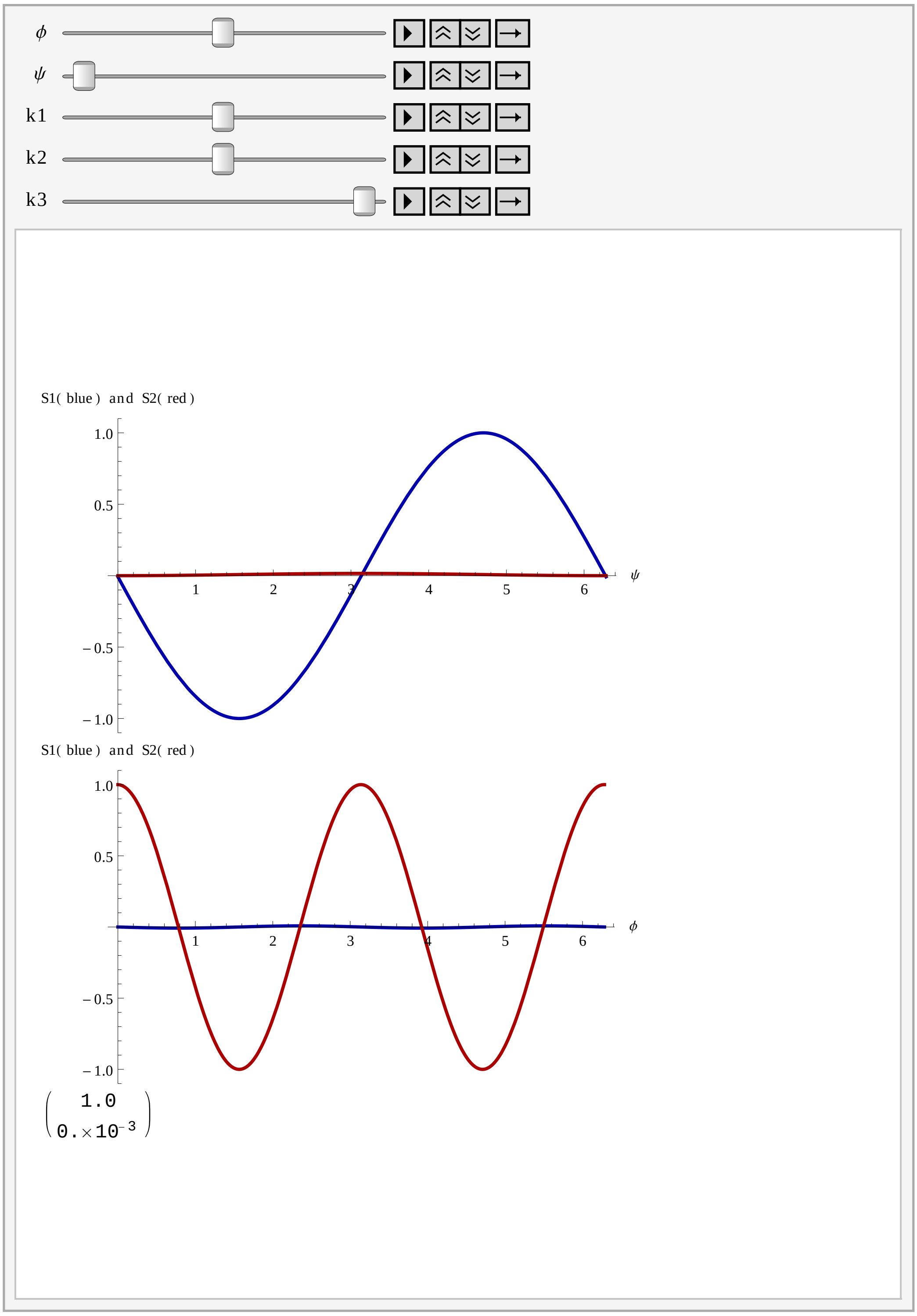
```
(*Definition of the error signals as functions
 of the input state and the actuation phase amplitudes*)
S1[ϕ_, ψ_, k1_, k2_, k3_] :=
 2 (Cos[k1 - ψ] Sin[k3] Sin[2 ϕ] + Cos[k3] (-Cos[2 ϕ] Sin[k2] + Cos[k2] Sin[2 ϕ] Sin[k1 - ψ]))
S2[ϕ_, ψ_, k1_, k2_, k3_] :=
 1
 — (Cos[2 ϕ] Sin[k2] Sin[k3] + Sin[2 ϕ] (Cos[k3] Cos[k1 - ψ] - Cos[k2] Sin[k3] Sin[k1 - ψ]))
 2

(*Definition of the actuated state of pollarization as function of all variables*)
                              1   ⅈ k1+ⅈ k3      ⅈ k2            1   ⅈ k3+ⅈ ψ        ⅈ k2
y1[ϕ_, ψ_, k1_, k2_, k3_] := {{— ⅇ          (1 + ⅇ    ) Cos[ϕ] + — ⅇ         (-1 + ⅇ    ) Sin[ϕ]},
                              2                                  2
   1   ⅈ k1        ⅈ k2            1   ⅈ ψ       ⅈ k2
  {— ⅇ      (-1 + ⅇ    ) Cos[ϕ] + — ⅇ    (1 + ⅇ    ) Sin[ϕ]}}
   2                               2

(*Graphical investigation of the error
 signals: animating the plot gives to possiblity to easily try different settings for the
   offset of the actuation signals and emmidiately see the effect on the error signals*)
Animate[Column[{Plot[{-1/2*S1[ϕ, ψ, k1, k2, k3], 2*S2[ϕ, ψ, k1, k2, k3]},
    {ψ, 0, 2 Pi}, PlotRange → {-1.1, 1.1},
    PlotStyle → {Directive[Thick, Darker[Blue]], Directive[Thick, Darker[Red]]},
    AxesLabel → {"ψ", "S1(blue) and S2(red)"}], Plot[
    {-1/2*S1[ϕ, ψ, k1, k2, k3], 2*S2[ϕ, ψ, k1, k2, k3]}, {ϕ, 0, 2 Pi}, PlotRange → {-1.1, 1.1},
    PlotStyle → {Directive[Thick, Darker[Blue]], Directive[Thick, Darker[Red]]},
    AxesLabel → {"ϕ", "S1(blue) and S2(red)"}],
   SetAccuracy[Abs[y1[ϕ, ψ, k1, k2, k3]], 3] // MatrixForm}],
 {ϕ, 0, Pi/2}, {ψ, 0, 3*Pi/2}, {k1, 0, Pi}, {k2, 0, Pi},
 {k3, -Pi/2, Pi/2},
 AnimationRunning → False]

(*The first plot shows the two error signals in depence of the elipticity ψ
 while second shows them in dependence of ϕ. Below the two plots the output state
 of polarization is given. Let us define the feedback to be negative, hence,
the PID will stabilized the angles to a decreasing slope crossing of 0. The two plots
  have to be consistent. So if the angles are changed the actuation signals have to
  be changed according to the direction of error signal change and the the resulting
  intersection of the signals with 0 should coincide with the new values of the
  angles. For all consistent settings the output state should be the same to proof the
  lock stabel. For example: If we set ϕ=π/4 and ψ=0 we have to set k1=k2=k3=π/2,
as shown in the first plots. The output state is then (1,0) which means it is s-
 polarized if we define the x-axis to be perpendicular to the table plane. For
  these settings signal S1 depends only on ψ and vanishes in the second plot,
while signal S2 behaves wise versa. Changing k1 results in a phase
 shift of S1 in the upper plot, while S2 stays unchanged. Hence,
S1 should give feedback to k1. The same is true for S2 in the lower plot if k2
 is changed. Since the feedback is negative, S1 will control k1 such that ψ=0,
while S2 will control k2 such that ϕ=π/4 (or ϕ=5π/4 which is equivalent). Hence,
the setting is consistent with the input state and ψ=0,
ϕ=π/4 is the point of operation of our lock for now.*)
```

Out[12]=

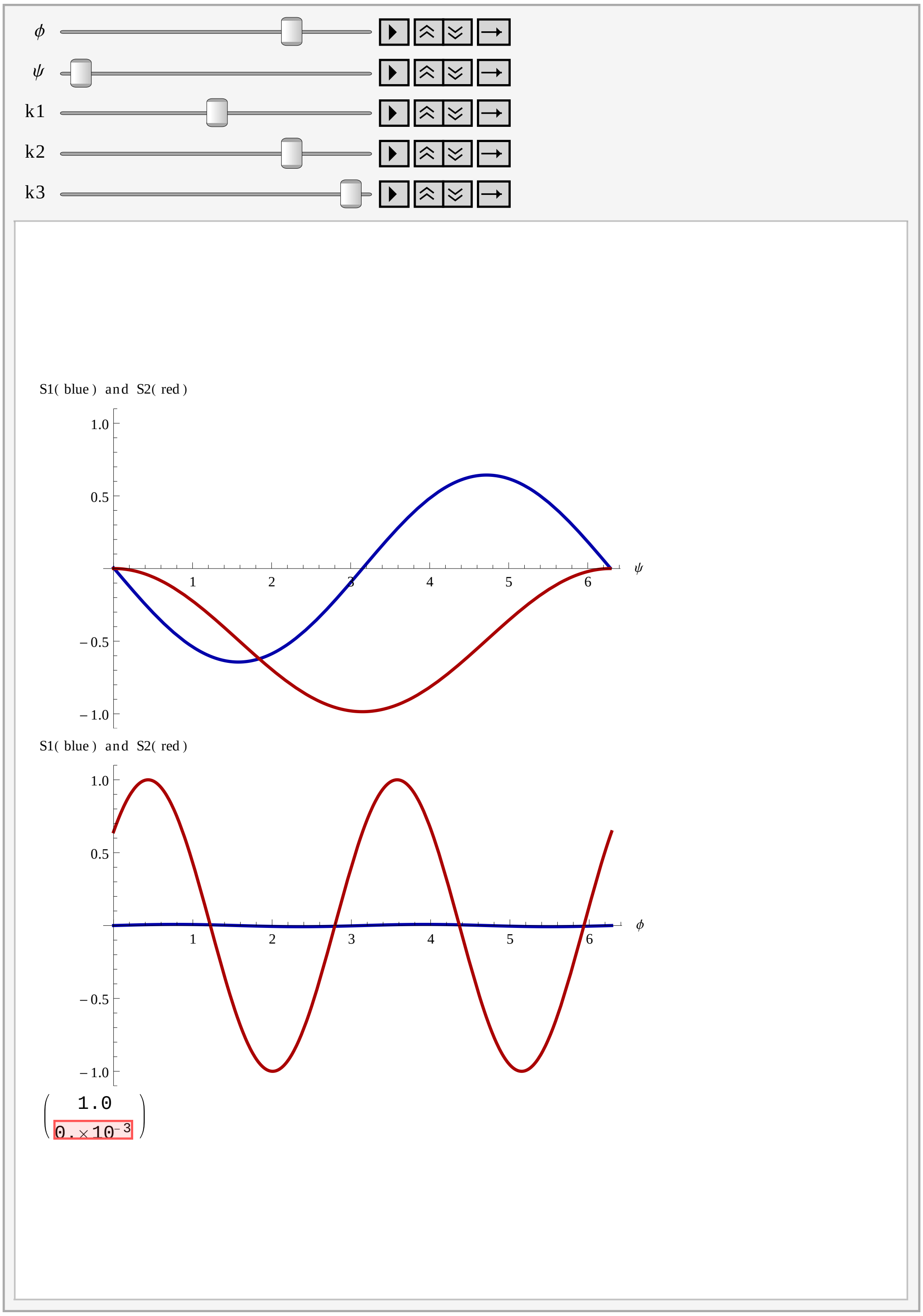


$$\begin{pmatrix} 1.0 \\ 0.\times 10^{-3} \end{pmatrix}$$

```
Animate[
 Column[{Plot[{-1/2*S1[ϕ, ψ, k1, k2, k3], 2*S2[ϕ, ψ, k1, k2, k3]}, {ψ, 0, 2 Pi}, PlotRange →
     {-1.1, 1.1}, PlotStyle → {Directive[Thick, Darker[Blue]], Directive[Thick, Darker[Red]]},
    AxesLabel → {"ψ", "S1(blue) and S2(red)"}], Plot[
    {-1/2*S1[ϕ, ψ, k1, k2, k3], 2*S2[ϕ, ψ, k1, k2, k3]}, {ϕ, 0, 2 Pi}, PlotRange → {-1.1, 1.1},
    PlotStyle → {Directive[Thick, Darker[Blue]], Directive[Thick, Darker[Red]]},
    AxesLabel → {"ϕ", "S1(blue) and S2(red)"}],
   SetAccuracy[Abs[y1[ϕ, ψ, k1, k2, k3]], 3] // MatrixForm}],
 {ϕ, 0, Pi/2}, {ψ, 0, 3*Pi/2}, {k1, 0, Pi}, {k2, 0, Pi},
 {k3, -Pi/2, Pi/2},
 AnimationRunning → False]

(* If ϕ now increases, say, to 3π/8,
S2 in the upper plott becomes significantly negative at ψ=
 0 and the output state is drastically changed. The PID will now increase k2 to a
   value where S2 becomes 0 at ψ=0 again, which is due to our scaling at exactly k2=
 3π/8 the case. Taking a look at the lower plot we see that the negative slope
   intersection of 0 was shifted to ϕ=3π/8, hence, the plots are consistent. And even
 better: the output state is again (1,0) which means it was maintained by this operation.*)
```

Out[13]=

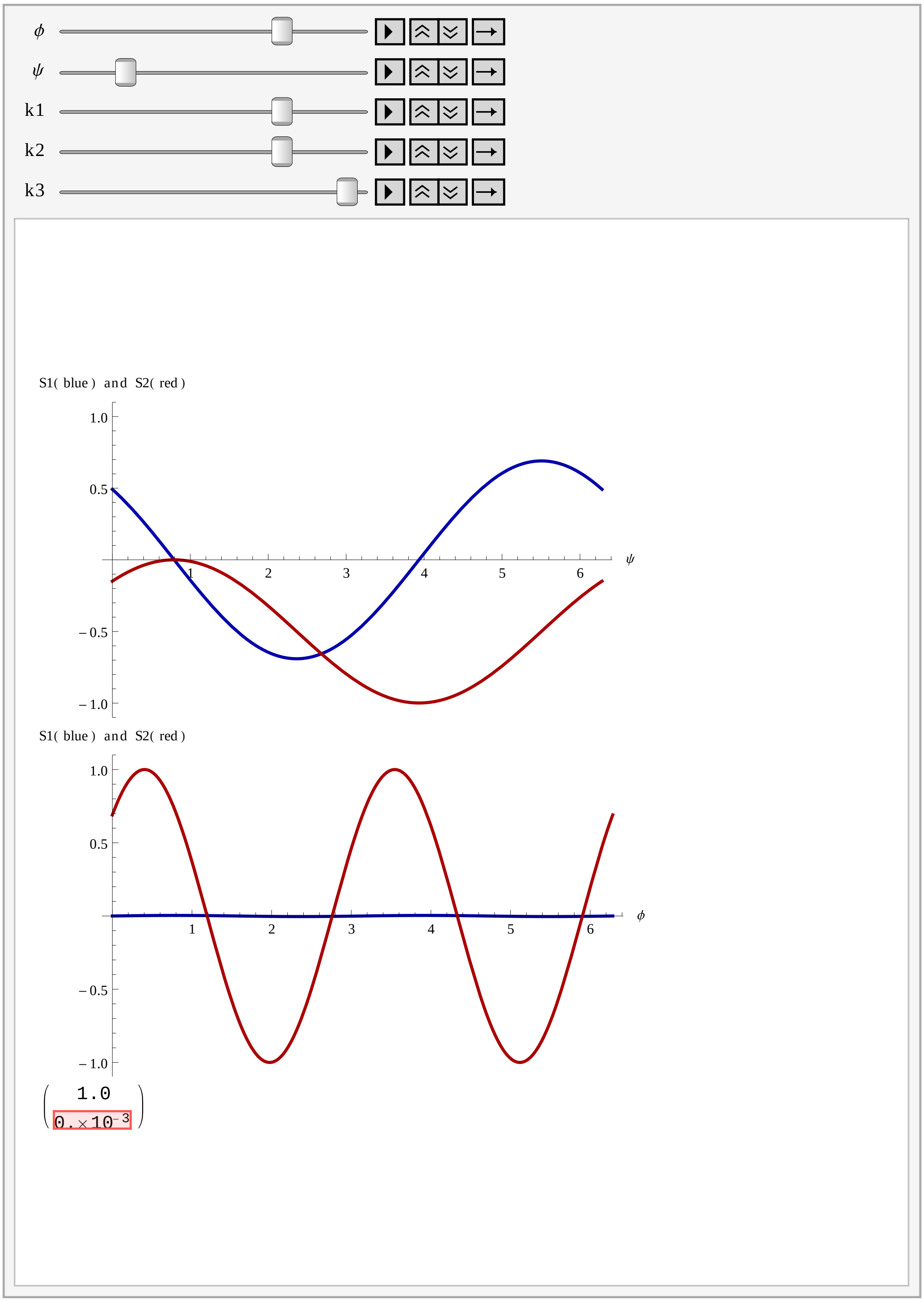


$$\begin{pmatrix} 1.0 \\ 0. \times 10^{-3} \end{pmatrix}$$

```
Animate[
 Column[{Plot[{-1/2*S1[ϕ, ψ, k1, k2, k3], 2*S2[ϕ, ψ, k1, k2, k3]}, {ψ, 0, 2 Pi}, PlotRange →
     {-1.1, 1.1}, PlotStyle → {Directive[Thick, Darker[Blue]], Directive[Thick, Darker[Red]]},
    AxesLabel → {"ψ", "S1(blue) and S2(red)"}], Plot[
    {-1/2*S1[ϕ, ψ, k1, k2, k3], 2*S2[ϕ, ψ, k1, k2, k3]}, {ϕ, 0, 2 Pi}, PlotRange → {-1.1, 1.1},
    PlotStyle → {Directive[Thick, Darker[Blue]], Directive[Thick, Darker[Red]]},
    AxesLabel → {"ϕ", "S1(blue) and S2(red)"}],
   SetAccuracy[Abs[y1[ϕ, ψ, k1, k2, k3]], 3] // MatrixForm}],
 {ϕ, 0, Pi/2}, {ψ, 0, 3*Pi/2}, {k1, 0, Pi}, {k2, 0, Pi},
 {k3, -Pi/2, Pi/2},
 AnimationRunning → False]

(* On the other hand if ψ is increased to, say,
π/4 signal S1 in the lower plot becomes negative at ϕ=
 3π/8 (if we leave the settings from the previous operation). Hence,
the PID will increase k1 to 3π/8 were the signal becomes 0 again. Looking
  at the upper plot we see that the negative slope intersetion of S1 was
  shifted to π/4 by this operation and the plots are consistent again. And
  also here the output state was maintained and is again perfectly s-
 polarized. So the result is that the locking scheme will be operational
  and stabilize the output state of polarization if the offsets of k1,
k2 and k3 are all tuned to π/2. Note that k3 allways stays at this value and
  is not actuated. It is more like a compensation for the required offset of
  k1. One last tricky thing happens if ϕ=0 or any integer multiple of π/2. In
  this case S1 vanishes identical for all possible settings of the other variable,
hence, there will not be any error signal for k1. But,
apart from the PID drifting around a bit,
this is not actually a problem because in this case no elipticity has to be compensated
  for. A change of ψ in will result only in an overall phase change of the light
  field but not influence the polarization. S2 will still give a correct error
  signal for k2 and the output state will still be stabilized to s-polarization.*)
```

Out[14]=



```
( 1.0        )
( 0.×10^-3   )
```

```
In[15]:= (*Finally, we take a lock at the error signals for the found settings of k1, k2 and k3,
         where we have chosen the prefactors accordingly to match the description from above. As
          we see S1 will now give an error signal for ψ and its amplitude depends on ϕ,
         while S2 gives an error signal for ϕ which is shifted by π/4
          due to the Cosine and the factor of 2 in the argument*)
         -1/2*S1[ϕ, ψ, Pi/2, Pi/2, Pi/2]
         2*S2[ϕ, ψ, Pi/2, Pi/2, Pi/2]

Out[15]= -Sin[2 ϕ] Sin[ψ]

Out[16]= Cos[2 ϕ]
```

BIBLIOGRAPHY

[Aci07] Acín, A., Brunner, N., Gisin, N., Massar, S., Pironio, S. & Scarani, V., DEVICE-INDEPENDENT SECURITY OF QUANTUM CRYPTOGRAPHY AGAINST COLLECTIVE ATTACKS. *Phys. Rev. Lett.* **98**, 230501 (2007).

[Arm15] Armstrong, S., Wang, M., Teh, R. Y., Gong, Q., He, Q., Janousek, J., Bachor, H. A., Reid, M. D. & Lam, P. K., MULTIPARTITE EINSTEIN-PODOLSKY-ROSEN STEERING AND GENUINE TRIPARTITE ENTANGLEMENT WITH OPTICAL NETWORKS. *Nat. Phys.* **11**, 167-172 (2015).

[AQS15] Pacher, C., Maurhart, O., Poppe, A., Tamas, C. & Peev, M., THE AIT QKD R10 SOFTWARE SUITE. *https://sqt.ait.ac.at/software/projects/qkd* (2015).

[Asp81] Aspect, A., Grangier, P. & Roger, G., EXPERIMENTAL TEST OF REALISTIC LOCAL THEORIES VIA BELL'S THEOREM. *Phys. Rev. Lett.* **47**, 460-463 (1981).

[Bel64] Bell, J. S., ON THE EINSTEIN PODOLSKY ROSEN PARADOX. *Physics* **1**, 195-200 (1964).

[Bel81] Bell, J. S., BERTLMANN'S SOCKS AND THE NATURE OF REALITY. *J. Phys. (Paris) Colloq.* **42**, C2-41-C2-62 (1981).

[Ben84] Bennett, C. H. & Brassard, G., QUANTUM CRYPTOGRAPHY: PUBLIC KEY DISTRIBUTION AND COIN TOSSING. *P. IEEE, International Conference on Computers, Systems, and Signal Processing*, 175-179 (1984).

[Ben92] Bennett, C. H., Brassard, G. & Marim, N. D., QUANTUM CRYPTOGRAPHY WITHOUT BELL'S THEOREM. *Phys. Rev. Lett.* **68**, 557-559 (1992).

[Ben93] Bennett, C. H., Brassard, G., Crépeau, C., Jozsa, R., Asher, P. & Wootters, W. K., TELEPORTING AN UNKNOWN QUANTUM STATE VIA DUAL CLASSICAL AND EINSTEIN-PODOLSKY-ROSEN CHANNELS. *Phys. Rev. Lett.* **70**, 1895-1899 (1993).

[Beo05] Ben-or, M., Horodecki, M., Leung, D. W., Mayers, D. & Oppenheim, J., THE UNIVERSAL COMPOSABLE SECURITY OF QUANTUM KEY DISTRIBUTION. *Theory Cryptogr.* **3378**, 386-406 (2005).

[Bla01] Black, E. D., AN INTRODUCTION TO POUND-DREVER-HALL LASER FREQUENCY STABILIZATION. *Am. J. Phys.* **69**, 79-87 (2001).

[Bou97] Bouwmeester, D., Pan, J. W., Mattle, K., Eibl, M., Weinfurter, H. & Zeilinger, A., EXPERIMENTAL QUANTUM TELEPORTATION. *Nature* **390**, 575-579 (1997).

[Bow03a] Bowen, W. P., Schnabel, R., Lam, P. K. & Ralph, T. C., EXPERIMENTAL INVESTIGATION OF CRITERIA FOR CONTINUOUS VARIABLE ENTANGLEMENT. *Phys. Rev. Lett.* **90**, 043601 (2003).

[Bow03b] Bowen, W. P., Treps. N., Buchler, B. C., Schnabel, R., Ralph, T. C., Bachor, H. A., Symul, T. & Lam, P. K., EXPERIMENTAL INVESTIGATION OF CONTINUOUS-VARIABLE QUANTUM TELEPORTATION. *Phys. Rev. A* **67**, 032302 (2003).

[Bol03b] Bowles, J., Vértesi, T., Quintino, M. T. & Brunner, N., ONE-WAY EINSTEIN-PODOLSKY-ROSEN STEERING. *Phys. Rev. Lett.* **112**, 200402 (2014).

[Brc12] Braciard, C., Cavalcanti, E., Walborn, S., Scarani, V. & Wiseman, H., ONE-SIDED DEVICE-INDEPENDENT QUANTUM KEY DISTRIBUTION: SECURITY, FEASIBILITY, AND THE CONNECTION WITH STEERING. *Phys. Rev. A* **85**, 010301(R) (2012).

[Bra98] Braunstein, S. L. & Kimble, H. J., TELEPORTATION OF CONTINUOUS QUANTUM VARIABLES. *Phys. Rev. Lett.* **80**, 869-872 (1998).

[Bra05] Braunstein, S. L. & van Loock, P., QUANTUM INFORMATION WITH CONTINUOUS VARIABLES. *Rev. Mod. Phys.* **77**, 513-577 (2005).

[Bra12] Braunstein, S. L. & Pirandola, S., SIDE-CHANNEL-FREE QUANTUM KEY DISTRIBUTION. *Phys. Rev. Lett.* **108**, 130502 (2012).

[Bri98] Briegel, H. J., Dür, W., Cirac, J. I. & Zoller, P., QUANTUM REPEATERS: THE ROLE OF IMPERFECT LOCAL OPERATIONS IN QUANTUM COMMUNICATION. *Phys. Rev. Lett.* **81**, 5932-5935 (1998).

[Bri99] Briegel, H. J., Cirac, J. I. & Zoller, P., QUANTENCOMPUTER: WIE SICH VERSCHRÄNKUNG FÜR DIE INFORMATIONSVERARBEITUNG NUTZEN LÄSST. *Phys. Bl.* **55**, 37-43 (1999).

[Buo10] Buono, D., Nocerino, G., D'Auria, V., Porzio, A., Olivares, S. & Paris, M. G. A., QUANTUM CHARACTERIZATION OF BIPARTITE GAUSSIAN STATES. *J. Opt. Soc. Am. B* **27**, 110-118 (2010).

[Buo12] Buono, D., Nocerino, G., Porzio, A. & Solimeno, S., EXPERIMENTAL ANALYSIS OF DECOHERENCE IN CONTINUOUS-VARIABLE BIPARTIE SYSTEMS. *Phys. Rev. A* **86**, 042308 (2012).

[Car79] Carter, J. L. & Wegman, M. N., UNIVERSAL CLASSES OF HASH FUNCTIONS. *J. Compu. Syst. Sci.* **18**, 142-154 (1979).

[Cac09] Cavalcanti, E. G., Jones, S. J., Wiseman, H. M. & Reid, M. D., EXPERIMENTAL CRITERIA FOR STEERING AND THE EINSTEIN-PODOLSKY-ROSEN PARADOX. *Phys. Rev. A* **80**, 032112 (2009).

[Cav81] Caves, C. M., QUANTUM-MECHANICAL NOISE IN AN INTERFEROMETER. *Phys. Rev. D* **23**, 1693-1708 (1981).

[Cer01] Cerf, N., Lévy, M. & van Assche, G., QUANTUM DISTRIBUTION OF GAUSSIAN KEYS USING SQUEEZED STATES. *Phys. Rev. A* **63**, 052311 (2001).

[Che13] Chen, J. L., Ye, X. J., Wu, C., Su, H. Y., Cabello, A., Kwek, L. C. & Oh, C. H., ALL-VERSUS-NOTHING PROOF OF EINSTEIN-PODOLSKY-ROSEN STEERING. *Sci. Rep.* **3**, 2143 (2013).

[Dea02] Deamen, J. & Rijmen, V., THE DESIGN OF RIJNDAEL: AES - THE ADVANCED ENCRYPTION STANDARD. *Springer-Verlag, Berlin*, (2002), ISBN 978-3-540-42580-9.

[DAu09] D'Auria, V., Fornaro, S., Porzio, A., Solimeno, S., Olivares, S. & Paris, M. G. A., FULL CHARACTERIZATION OF GAUSSIAN BIPARTITE ENTANGLED STATES BY A SINGLE HOMODYNE DETECTOR. *Phys. Rev. Lett.* **86**, 4267 (2001).

[Dia15] Diamanti, E. & Leverrier, A., DISTRIBUTING SECRET KEYS WITH QUANTUM CONTINUOUS VARIABLES: PRINCIPLE, SECURITY AND IMPLEMENTATIONS. *Entropy* **17**, 6072-6092 (2015).

[Die82] Dieks, D., COMMUNICATION BY EPR DEVICES. *Phys. Lett. A* **92**, 271-272 (1982).

[DGu10Th] DiGuglielmo, J., ON THE EXPERIMENTAL GENERATION AND CHARACTERIZATION OF ENTANGLED STATES OF LIGHT. *PhD Thesis, Leibniz University Hannover* (2010).

[DGu11] DiGuglielmo, J., Samblowski, A., Hage, B., Pineda, C., Eisert, J. & Schnabel, R., EXPERIMENTAL UNCONDITIONAL PREPARATION AND DETECTION OF A CONTINUOUS BOUND ENTANGLED STATE OF LIGHT. *Phys. Rev. Lett.* **107**, 240503 (2011).

[Don08] Dong, R., Lasse, M., Jeersink, J., Marquardt, C., Filip, R., Leuchs, G. & Andersen, U. L., EXPERIMENTAL ENTANGLEMENT DISTILLATION OF MESOSCOPIC QUANTUM STATES. *Nat. Phys.* **4**, 919-923 (2008).

[Dua00] Duan, L. M., Giedke, G., Cirac, J. I. & Zoller, P., INSEPARABILITY CRITERION FOR CONTINUOUS VARIABLE SYSTEMS. *Phys. Rev. Lett.* **84**, 2722 (2000).

[Dua01] Duan, L. M., Lukin, M. D., Cirac, J. I. & Zoller, P., LONG-DISTANCE QUANTUM COMMUNICATION WITH ATOMIC ENSEMBLES AND LINEAR OPTICS. *Nature* **414**, 413-418 (2001).

[Duh10] Duhme, J., Franz, T., Schmidt, S. & Werner, R. F., VERSCHRÄNKUNG - SCHLÜSSEL ZUR QUANTENWELT. QUANTENINFORMATIONSTHEORIE TEIL 1: GRUNDLAGEN. *Physik in unserer Zeit* **41**, 236-242 (2010).

[Duh15Th] Duhme, J., QUANTUM KEY SECURITY: THEORY AND ANALYSIS OF EXPERIMENTAL REALISATIONS. *PhD Thesis, Leibniz University Hannover* (2015).

[Eke91] Ekert, A. K., QUANTUM CRYPTOGRAPHY BASED ON BELL'S THEOREM. *Phys. Rev. Lett.* **67**, 661-663 (1991).

[Ebe11] Eberle, T., Händchen, V., Duhme, J., Franz, T., Werner, R. F. & Schnabel, R., STRONG EINSTEIN-PODOLSKY-ROSEN ENTANGLEMENT FROM A SINGLE SQUEEZED LIGHT SOURCE. *Phys. Rev. A* **83**, 052329 (2011).

[Ebe13a] Eberle, T., Händchen, V., Duhme, J., Franz, T., Werner, R. F. & Schnabel, R., GAUSSIAN ENTANGLEMENT FOR QUANTUM KEY DISTRIBUTION FROM A SINGLE-MODE SQUEEZING SOURCE. *New J. Phys.* **15**, 053049 (2013).

[Ebe13b] Eberle, T., Händchen, V. & Schnabel, R., STABLE CONTROL OF 10 DB TWO-MODE SQUEEZED VACUUM STATES OF LIGHT. *Opt. Ex.* **21**, 11546-11553 (2013).

[Ebe13Th] Eberle, T., REALIZATION OF FINITE-SIZE QUANTUM KEY DISTRIBUTION BASED ON EINSTEIN-PODOLSKY-ROSEN ENTANGLED LIGHT. *PhD Thesis, Leibniz University Hannover* (2013).

[Ein05] Einstein, A., ÜBER EINEN DIE ERZEUGUNG UND VERWANDLUNG DES LICHTES BETREFFENDEN HEURISTISCHEN GESICHTSPUNKT. *Ann. d. Phys.* **17**, 132-148 (1905).

[Ein35] Einstein, A., Podolsky, B. & Rosen, N., CAN QUANTUM-MECHANICAL DESCRIPTION OF PHYSICAL REALITY BE CONSIDERED COMPLETE? *Phys. Rev.* **47**, 777-780 (1935).

[Fiu07] Fiurášek, J., Marek, P., Filip, R. & Schnabel, R., EXPERIMENTALLY FEASIBLE PURIFICATION OF CONTINUOUS-VARIABLE ENTANGLEMENT. *Phys. Rev. A* **75**, 050302 (2007).

[Fra12Th] Franz, T., QUANTUM CORRELATIONS AND QUANTUM KEY DISTRIBUTION. *PhD Thesis, Leibniz University Hannover* (2012).

[Fur12] Furrer, F., Franz, T., Berta, M., Leverrier, A., Scholz, V., Tomamichel, M. & Werner, R. F., CONTINUOUS VARIABLE QUANTUM KEY DISTRIBUTION: FINITE-KEY ANALYSIS OF COMPOSABLE SECURITY AGAINST COHERENT ATTACKS. *Phys. Rev. Lett.* **109**, 100502 (2012).

[Fur12Th] Furrer, F., SECURITY OF CONTINUOUS-VARIABLE QUANTUM KEY DISTRIBUTION AND ASPECTS OF DEVICE-INDEPENDENT SECURITY. *PhD Thesis, Leibniz University Hannover* (2012).

[Fur14] Furrer, F., REVERSE-RECONCILIATION CONTINUOUS-VARIABLE QUANTUM KEY DISTRIBUTION BASED ON THE UNCERTAINTY PRINCIPLE. *Phys. Rev. A* **90**, 042325 (2014).

[Fur15] Furrer, F., Schaffner, C. & Whener, S., CONTINUOUS-VARIABLE PROTOCOLS IN THE NOISY-STORAGE MODEL. *arXiv:1509.09123v1* (2015).

[Fus98] Furusawa, A., Sørensen, J. L., Braunstein, S. L., Fuchs, C. A., Kimble, H. J. & Polzik, E. S., UNCONDITIONAL QUANTUM TELEPORTATION. *Science* **282**, 706-709 (1998).

[Gab10] Gabriel, C., Wittman, C., Sych, D., Dong, R., Mauerer, W., Andersen, U. L., Marquardt, C. & Leuchs, G., A GENERATOR FOR UNIQUE QUANTUM RANDOM NUMBERS BASED ON VACUUM STATES. *Nat. Phot.* **4**, 711-715 (2010).

[Geh15] Gehring, T., Händchen, V., Duhme, J., Furrer, F., Franz, T., Pacher, C., Werner, R. F. & Schnabel, R., IMPLEMENTATION OF CONTINUOUS-VARIABLE QUANTUM KEY DISTRIBUTION WITH COMPOSABLE AND ONE-SIDED-DEVICE-INDEPENDENT SECURITY AGAINST COHERENT ATTACKS. *Nat. Commun.* **6**, 8795 (2015).

[Ger08] Gerry, C. C. & Knight, P.Ł., INTRODUCTORY QUANTUM OPTICS. *Cambridge University Press* (2008), 3rd edition, ISBN 0-521-52735-X.

[Gis02] Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H., QUANTUM CRYPTOGRAPHY. *Rev. Mod. Phys.* **74**, 145-195 (2002).

[Gro02] Grosshans, F. & Grangies, P., REVERSE RECONCILIATION PROTOCOLS FOR QUANTUM CRYPTOGRAPHY WITH CONTINUOUS VARIABLES. *arXiv:quant-ph/0204127v1* (2002).

[Hag08] Hage, B., Samblowski, A., DiGuglielmo, J., Franzen, A., Fiurášek, J. & Schnabel, R., PREPARATION OF DISTILLED AND PURIFIED CONTINUOUS-VARIABLE ENTANGLED STATES. *Nat. Phys.* **4**, 915-918 (2008).

[Hag11] Hage, B., Janousek, J., Armstrong, S., Symul, T., Bernu, J., Chrzanowski, H. M., Lam, P. K. & Bachor, H. A., DEMONSTRATING VARIOUS QUANTUM EFFECTS WITH TWO ENGANGLED LASER BEAMS. *Eur. Phys. J. D* **63**, 457-461 (2011).

[Hal13] Hall, B. C., QUANTUM THEORY FOR MATHEMATICIANS. *Springer Sience+Business Media, New York* (2013), ISBN 978-1-4614-7115-8.

[Hän12] Händchen, V., Eberle, T., Steinlechner, S., Samblowski, A., Franz, T., Werner, R. F. & Schnabel, R., Observation of One-Way Einstein-Podolsky-Rosen Steering. *Nat. Photon.* **6**, 596-599 (2012).

[He15] He, Q. Y., Gong, Q. H. & Reid, M. D., Classifying Directional Gaussian Entanglement, Einstein-Podolsky-Rosen Steering, and Discord. *Phys. Rev. Lett.* **114**, 060402 (2015).

[Hen15] Hensen, B., Bernien, H., Dréau, A. E., Reiserer, A., Kalb, N., Blok, M. S., Ruitenberg, J., Vermeulen, R. F. L., Schouten, R. N., Abellán, C., Amaya, W., Pruneri, V., Mitchell, M. W., Markham, M., Twitchen, D. J., Elkouss, D., Wehner, S., Timiniau, T. H. & Hanson, R., Loophole-Free Bell Inequality Violation Using Electron Spins Separated by 1.3 Kilometers. *Nature* **526**, 682-686 (2015).

[Hor99] Horodecki, P., Horodecki, M. & Horodecki, R., Bound Entanglement can be Activated. *Phys. Rev. Lett.* **82**, 1056-1059 (1999).

[Hua13] Huang, J. Z., Weedbrook, C., Yin, Z. Q., Wang, S., Li, H. W., Chen, W., Guo, G. C. & Han, Z. F., Quantum Hacking of a Continuous-Variable Quantum-Key-Distribution System Using a Wavelength Attack. *Phys. Rev. A* **87**, 062329 (2013).

[Jac03] Jacod, J. & Protter, P., Probability Essentials. *Springer-Verlag, Berlin* (2003), 2nd edition, ISBN 3-540-434871-8.

[Jai14] Jain, N., Anisimova, E., Khan, I., Makarov, V., Marquardt, C. & Leuchs, G., Trojan-Horse Attacks Threaten the Security of Practical Quantum Cryptography. *New J. Phys.* **16**, 123030 (2014).

[Jia04] Jia, X. J., Su, X. L., Pan, Q., Gao, J. R., Xie, C.,D. & Peng, K. C., Experimental Demonstration of Unconditional Entanglement Swapping for Continuous Variables. *Phys. Rev. Lett.* **93**, 250503 (2004).

[Jor15] Jorgenfors, J., Elhassan, A. M., Ahrens, J., Bourennane, M. & Larsson, J. A., Hacking the Bell Test Using Classical Light in Energy-Time Entanglement-Based Quantum Key Distribution. *Sci. Adv.* **1**, e1500793 (2015).

[Jou13a] Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P. & Diamanti, E., Experimental Demonstration of Long-Distance Continuous-Variable Quantum Key Distribution. *Nat. Photon.* **7**, 378-381 (2013).

[Jou13b] Jouguet, P., Kunz-Jacques, S. & Diamanti, E., Preventing Calibration Attacks on the Local Oscillator in

CONINUOUS-VARIABLE QUANTUM KEY DISTRIBUTION. *Phys. Rev. A* **87**, 062313 (2013).

[Jul04] Julsgaard, B., Sherson, J., Cirac, J. I., Fiurášek, J. & Polzik, E. S., EXPERIMENTAL DEMONSTRATION OF QUANTUM MEMORY FOR LIGHT. *Nature* **432**, 482-486 (2004).

[Kan98] Kant, I., KRITIK DER REINEN VERNUNFT. *Meiner Verlag, Hamburg* (1998), ISBN 3-7873-1319-2.

[Kel08] Keller, G., D'Auria, V., Treps, N., Coudreau, T., Laurat, J. & Fabre, C., EXPERIMENTAL DEMONSTRATION OF FREQUENCY-DEGENERATE BRIGHT EPR BEAMS WITH A SELF-PHASE-LOCKED OPO. *Opt. Ex.* **16**, 9351 (2008).

[Kog66] Kogelnik, H. & Li, T., LASER BEAMS AND RESONATORS. *Proc. IEEE* **54**, 1312-1329 (1966).

[Koz00] Kozhekin, A. E., Møler, K. & Polzik, E. S., QUANTUM MEMORY FOR LIGHT. *Phys. Rev. A* **62**, 033809 (2000).

[Krü06Th] Krüger, O., QUANTUM INFORMATION THEORY WITH GAUSSIAN SYSTEMS. *PhD Thesis, Technical Carolo-Wilhelmina University Braunschweig* (2006).

[Kun15] Kunz-Jacques, S. & Jouguet, P., ROBUST SHOT NOISE MEASUREMENT FOR CONTINUOUS VARIABLE QUANTUM KEY DISTRIBUTION. *Phys. Rev. A* **91**, 022307 (2015).

[Lat10] Latzka, N., NUMERICAL MODELLING OF CLASSICAL AND QUANTUM EFFECTS IN NON-LINEAR OPTICAL SYSTEMS. *PhD Thesis, Leibniz University Hannover* (2010).

[Lau05] Laurat, J., Coudreau, T., Keller, G., Treps, N. & Fabre, C., EFFECTS OF MODE COUPLING ON THE GENERATION OF QUADRATURE EINSTEIN-PODOLSKY-ROSEN ENTANGLEMENT IN A TYPE-II OPTICAL PARAMETRIC OSCILLATOR BELOW THRESHOLD. *Phys. Rev. A* **71**, 022313 (2005).

[Lee13] Lee, C. W., Ji, S. W. & Nha, H., QUANTUM STEERING FOR CONTINUOUS-VARIABLE STATES. *J. Opt. Soc. Am. B* **30**, 2483-2490 (2013).

[Lev10] Leverrier, A., Grosshans, F. & Grangier, P., FINITE-SIZE ANALYSIS OF CONTINUOUS-VARIABLE QUANTUM KEY DISTRIBUTION. *Phys. Rev. A* **81**, 062343 (2010).

[Lev13] Leverrier, A., Carcía-Patrón, R., Renner, R. & Cerf, N., SECURITY OF CONTINUOUS-VARIABLE QUANTUM KEY DISTRIBUTION AGAINST GENERAL ATTACKS. *Phys. Rev. Lett.* **110**, 030502 (2013).

[Lo99] Lo, H. K. & Chau, H. F., UNCONDITIONAL SECURITY OF QUANTUM KEY DISTRIBUTION OVER ARBITRARILY LONG DISTANCES. *Science* **283**, 2050-2056 (1999).

[Lo12] Lo, H. K., Curty, M. & Qi, B., MEASUREMENT-DEVICE-INDEPENDENT QUANTUM KEY DISTRIBUTION. *Phys. Rev. Lett.* **108**, 130503 (2012).

[Lod07] Lodewyck, J., Bloch, M., García-Patrón, R., Fossier, S., Karpov, E., Diamanti, E., Debuisschert, T., Cerf, N. J., Tualle-Brouri, R., McLaughlin, S. W. & Grangier, P., QUANTUM KEY DISTRIBUTION OVER 25 KM WITH AN ALL-FIBER CONTINUOUS-VARIABLE SYSTEM. *Phys. Rev. A* **76**, 042305 (2007).

[Lou00] Loudon, R., THE QUANTUM THEORY OF LIGHT. *Oxford University Press* (2000), 3rd edition, ISBN 978-0-19-850176-3.

[LSC11] The LIGO Scientific Collaboration, A GRAVITATIONAL WAVE OBSERVATORY OPERATING BEYOND THE QUANTUM SHOT-NOISE LIMIT. *Nat. Phys.* **7**, 962-965 (2011).

[LSC13] The LIGO Scientific Collaboration, ENHANCED SENSITIVITY OF THE LIGO GRAVITATIONAL WAVE DETECTOR BY USING SQUEEZED STATES OF LIGHT. *Nat. Photon.* **7**, 613-619 (2013).

[Lyd10] Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J. & Makarov, V., HACKING COMMERCIAL QUANTUM CRYPTOGRAPHY SYSTEMS BY TAILORED BRIGHT ILLUMINATION. *Nat. Photon.* **4**, 686-689 (2010).

[Ma13a] Ma, X. C., Sun, S. H., Jiang, M. S. & Liang, L. M., LOCAL OSCILLATOR FLUCTUATION OPENS A LOOPHOLE FOR EVE IN PRACTICAL CONTINUOUS-VARIABLE QUANTUM-KEY-DISTRIBUTION. *Phys. Rev. A* **88**, 022339 (2013).

[Ma13b] Ma, X. C., Sun, S. H., Jiang, M. S. & Liang, L. M., WAVELENGTH ATTACK ON PRACTICAL CONTINUOUS-VARIABLE QUANTUM-KEY-DISTRIBUTION SYSTEM WITH A HETERODYNE PROTOCOL. *Phys. Rev. A* **87**, 052309 (2013).

[Ma14] Ma, X. C., Sun, S. H., Jiang, M. S., Zhou, Y. L. & Liang, L. M., ENHANCEMENT OF THE SECURITY OF A PRACTICAL CONTINUOUS-VARIABLE QUANTUM-KEY-DISTRIBUTION SYSTEM BY MANIPULATING THE INTENSITY OF THE LOCAL OSCILLATOR. *Phys. Rev. A* **89**, 032310 (2014).

[Mad12] Madsen, L. S., Usenko, V. C., Lassen, M., Filip, R. & Andersen, U. L., CONTINUOUS VARIABLE QUANTUM KEY DISTRIBUTION WITH MODULATED ENTANGLED STATES. *Nat. Commun.* **3**, 1083 (2012).

[Meh11] Mehmet, M., Ast, A., Eberle, T., Steinlechner, S., Vahlbruch, H. & Schnabel, R., SQUEEZED LIGHT AT 1550 NM WITH A QUANTUM NOISE REDUCTION OF 12.3 dB. *Opt. Ex.* **19**, 25763-25772 (2011).

[Mid96] Middelton, D., AN INTRODUCTION TO STATISTICAL COMMUNICATION THEORY. *Wiley-IEEE Press* (1996).

[Mil10] Midgley, S. L. W., Ferris, A. J. & Olsen, M. K., ASYMMETRIC GAUSSIAN STEERING: WHEN ALICE AND BOB DISAGREE. *Phys. Rev. A* **81**, 022101 (2010).

[Nie00] Nielsen, M. A. & Chuang, I. L., QUANTUM COMPUTATION AND QUANTUM INFORMATION. *Cambridge University Press* (2000), ISBN 0-521-63503-9.

[Nyq28] Nyquist, H., CERTAIN TOPICS IN TELEGRAPH TRANSMISSION THEORY. *Trans. AIEE* **47**, 617-644 (1928).

[Oel14] Oelker, E., Barsotti, L., Dwyer, S., Sigg, D. & Mavalvala, N., SQUEEZED LIGHT FOR ADVANCED GRAVITATIONAL WAVE DETECTORS AND BEYOND. *Opt. Ex.* **22**, 21106-21121 (2014).

[Ols15] Olsen, M. K., ASYMMETRIC STEERING IN COHERENT TRANSPORT OF ATOMIC POPULATION WITH A THREE-WELL BOSE-HUBBARD MODEL. *J. Opt. Soc. Am. B* **32**, A15-A19 (2015).

[Ou92] Ou, Z. Y., Pereira, S. F., Kimble, H. J. & Peng, K. C., REALIZATION OF THE EINSTEIN-PODOLSKY-ROSEN PARADOX FOR CONTINUOUS VARIABLES. *Phys. Rev. Lett.* **68**, 3663-3666 (1992).

[Pir15] Pirandola, S., Ottaviani, C., SPedalieri, G., Weedbrook, C., Braunstein, S. L., Lloyd, S., Gehring, T., Jacobsen, C. S. & Andersen, U. L., HIGH-RATE MEASUREMENT-DEVICE-INDEPENDENT QUANTUM CRYPTOGRAPHY *Nat. Photon.* **9**, 397-402 (2015).

[Pla00] Planck, M., ZUR THEORIE DES GESETZES DER ENERGIEVERTEILUNG IM NORMALSPECTRUM. *Verhandlungen der Deutschen physikalischen Gesellschaft* **2**, 245-253 (1900).

[Qin13] Qin, H., Kumar, R. & Alléaume, R., SATURATION ATTACK ON CONTINUOUS-VARIABLE QUANTUM KEY DISTRIBUTION SYSTEM. *Proc. SPIE* **8899**, 88990N (2013).

[Qui15] Quintino, M. T., Vértesi, T., Cavalcanti, D., Augusiak, R., Demianowicz, M., Acín, A. & Brunner, N., INEQUIVALENCE OF ENTANGLEMENT, STEERING, AND BELL NONLOCALITY FOR GENERAL MEASUREMENTS. *Phys. Rev. A* **92**, 032107 (2015).

[Rei89] Reid, M. D., DEMONSTRATION OF THE EINSTEIN-PODOLSKY-ROSEN PARADOX USING NONDEGENERATE PARAMETRIC AMPLIFICATION. *Phys. Rev. A* **40**, 913-923 (1989).

[Ren05] Renner, R. & König, R., UNIVERSALLY COMPOSABLE PRIVACY AMPLIFICATION AGAINST QUANTUM ADVERSARIES. *Phys. Rev. A* **40**, 913-923 (1989).

[Ren09] Renner, R. & Cirac, J. I., DE FINETTI REPRESENTATION THEOREM FOR INFINITE-DIMENSIONAL QUANTUM SYSTEMS AND APPLICATIONS TO QUANTUM CRYPTOGRAPHY. *Phys. Rev. A* **40**, 913-923 (1989).

[Riv78] Rivest, R. L., Shamir, A., Adleman, L., A METHOD FOR OBTAINING DIGITAL SIGNATURES AND PUBLIC-KEY CRYPTOSYSTEMS. *Commun. ACM* **21**, 120-126 (1978).

[Sam07] Samblowski, A., VERSCHRÄNKUNG KONTINUIERLICHER VARIABLEN VON SEITENBÄNDERN OPTISCHER FELDER. *Diploma Thesis, Leibniz University Hannover* (2007).

[Sam12] Samblowski, A., STATE PREPARATION FOR QUANTUM INFORMATION SCIENCE AND METROLOGY. *PhD Thesis, Leibniz University Hannover* (2012).

[Sau10] Saunders, D. J., Jones, S. J., Wiseman, H. M. & Pryde, G. J., EXPERIMENTAL EPR-STEERING USING BELL-LOCAL STATES. *Nat. Phys.* **6**, 845-849 (2010).

[Sca00] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N. & Peev, M., THE SECURITY OF PRACTICAL QUANTUM KEY DISTRIBUTION. *Rev. Mod. Phys.* **81**, 1301-1350 (2009).

[Sna10] Schnabel, R., Mavalvala, N., McClelland, D. E. & Lam, P. K., QUANTUM METROLOGY FOR GRAVITATIONAL WAVE ASTRONOMY. *Nat. Commun.* **1**, 121 (2010).

[Sor02] Schori, C., Sorensen, J. L. & Polzik, E. S., NARROW-BAND FREQUENCY TUNABLE LIGHT SOURCE OF CONTINUOUS QUADRATURE ENTANGLEMENT. *Phys. Rev. A* **66**, 033802 (2002).

[Srö35] Schrödinger, E., DISCUSSION OF PROBABILITY RELATIONS BETWEEN SEPARATED SYSTEMS. *Proc. Cambridge Philos. Soc.* **31**, 555-563 (1935).

[Srö36] Schrödinger, E., PROBABILITY RELATIONS BETWEEN SEPARATED SYSTEMS. *Proc. Cambridge Philos. Soc.* **32**, 446 (1936).

[She85] Shelby, R. M., Levenson, M. D. & Bayer, P. W., GUIDED ACOUSTIC-WAVE BRILLOUIN SCATTERING. *Phys. Rev. B* **31**, 5244-5252 (1985).

[Sil01] Silberhorn, C., Lam, P. K., WeiÃ, O., König, F., Korolkova, N. & Leuchs, G., GENERATION OF CONTINUOUS VARIABLE EINSTEIN-PODOLSKY-ROSEN ENTANGLEMENT VIA THE KERR NONLINEARITY IN AN OPTICAL FIBER. *Phys. Rev. Lett.* **86**, 4267 (2001).

[Smi11] Smith, G., Smolin, J. A. & Yard, J., QUANTUM COMMUNICATION WITH GAUSSIAN CHANNELS OF ZERO QUANTUM CAPACITY. *Nat. Phot.* **5**, 624-627 (2011).

[Smi12] Smith, D. H., Gillett, G., de Almeida, M. P., Branciard, C., Fedrizzi, A., Weinhold, T. J., Lita, A., Calkins, B., Gerrits, T., Wiseman, H. M., Nam, S. W. & White, A. G., CONCLUSIVE QUANTUM STEERING WITH SUPERCONDUCTING TRANSITION-EDGE SENSORS. *Nat. Commun.* **3**, 625 (2012).

[Ste13] Steinlechner, S., Bauchrowitz, J., Meinders, M., Müller-Ebhardt, H., Danzmann, K. & Schnabel, R., QUANTUM-DENSE METROLOGY. *Nat. Phot.* **7**, 626-630 (2013).

[Sti94] Stinson, D. R., UNIVERSAL HASHING AND AUTHENTICATION CODES. *Des. Codes Cryptogr.* **4**, 369-380 (1994).

[Su09] Su, X., Wang, W., Wang, Y., Jia, X., Xie, C. & Peng, K. C., CONTINUOUS VARIABLE QUANTUM KEY DISTRIBUTION BASED ON OPTICAL ENTANGLED STATES WITHOUT SIGNAL MODULATION. *Europhys. Lett.* **87**, 20005 (2009).

[Tak06] Takei, N., Lee, N., Moriyama, D., Neergaard-Nielsen, J. S. & Furusawa, A., TIME-GATED EINSTEIN-PODOLSKY-ROSEN CORRELATION. *Phys. Rev. A* **74**, 060101(R) (2006).

[Tkn07] Takeno, Y., Yukawa, M., Yonezawa, H. & Furusawa, A., OBSERVATION OF -9 dB QUADRATURE SQUEEZING WITH IMPROVEMENT OF PHASE STABILITY IN HOMODYNE MEASUREMENT. *Opt. Ex.* **15**, 4321-4327 (2007).

[Tan99] Tan, S., CONFIRMING ENTANGLEMENT IN CONTINUOUS VARIABLE QUANTUM TELEPORTATION. *Phys. Rev. A* **60**, 2752-2758 (1999).

[Tan15] Tan, H., Zhang, X. & Li, G., STEADY-STATE ONE-WAY EINSTEIN-PODOLSKY-ROSEN STEERING IN OPTOMECHANICAL INTERFACES. *Phys. Rev. A* **91**, 032121 (2015).

[Tay13] Taylor, M. A., Janousek, J., Daria, V., Knittel, J., Hage, B., Bachor, H. A. & Bowen, W. P., BIOLOGICAL MEASUREMENT BEYOND THE QUANTUM LIMIT. *Nat. Phot.* **7**, 229-233 (2013).

[Tit98] Tittel, W., Brendel, J., Zbinden, H. & Gisin, N., VIOLATION OF BELL INEQUALITIES BY PHOTONS MORE THAN 10 KM APART. *Phys. Rev. Lett.* **81**, 3563-3566 (1998).

[Tom11] Tomamichel, M. & Renner, R., UNCERTAINTY RELATION FOR SMOOTH ENTROPIES. *Phys. Rev. Lett.* **106**, 110506 (2011).

[Tom13] Tomamichel, M., Fehr, S., Kaniewski, J. & Wehner, S., A Monogamy-of-Entanglement Game with Applications to Device-Independent Quantum Cryptography. *New J. Phys.* **15**, 103002 (2013).

[Urs07] Ursin, R., Tiefenbacher F., Schmitt-Manderbach, T., Weier, H., Scheidl, T., Lindenthal, M., Blauensteiner, B., Jennewein, T., Perdigues, J., Trojek, P., Oemer, B., Fürst, M., Meyenburg, M., Rarity, J., Sodnik, Z., Barbieri, C., Weinfurter, H. & Zeilinger, A., Entanglement-Based Quantum Communication Over 144 km. *Nat. Phys.* **3**, 481-486 (2007).

[Vah08Th] Vahlbruch, H., Squeezed Light for Gravitational Wave Astronomy. *PhD Thesis, Leibniz University Hannover* (2008).

[Vai94] Vaidman, L., Teleportation of Quantum States. *Phys. Rev. A* **49**, 1473-1476 (1994).

[vAs06] van Assche, G., Quantum Cryptography and Secret Key Distillation. *Cambridge University Press* (2006), ISBN 978-0-521-86485-5.

[Ver26] Vernam, G., Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications. *J. Am. Inst. Elect. Eng.* **XLI**, 295-301 (1926).

[Vol13] Vollmer, C. E., Schulze, D., Eberle, T., Händchen, V., Fiurášek, J. & Schnabel, R., Experimental Entanglement Distribution by Separable States. *Phys. Rev. Lett.* **111**, 230505 (2013).

[Wag08] Wagner, K., Janousek, J., Delaubert, V., Zou, H., Harb, C., Treps, N., Morizur, J. F., Lam, P. K. & Bachor, H. A., Entangling the Spatial Properties of Laser Beams. *Science* **321**, 541-543 (2008).

[Wag14] Wagner, K., Janousek, J., Armstrong, S., Morizur, J. F., Lam, P. K. & Bachor, H. A., Asymmetric EPR Entanglement in Continuous Variable Systems. *J. Phys. B* **47**, 225502 (2014).

[Wal94] Walls, D. F. & Milburn, G. J., Quantum Optics. *Springer-Verlag, Berlin*, (1994), ISBN 978-3-540-28573-1.

[Wan13] Wang, Y., Bao, W., Li, H., Zhou, C. & Li, Y., Finite-Key Analysis for One-Sided Device-Independent Quantum Key Distribution. *Phys. Rev. A* **88**, 052322 (2013).

[Wal14] Walk, N., Wiseman, H. M. & Ralph, T. C., Continuous-Variable One-Sided Device Independent Quantum Key Distribution. *arXiv:1405.6593v2* (2014).

[Wee12] Weeedbrook, C., Pirandola, S., García-Patrón, R., Cerf, N. J., Ralph, T. C., Shapiro, J. H. & Lloyd, S., GAUSSIAN QUANTUM INFORMATION. *Rev. Mod. Phys.* **84**, 621-668 (2012).

[Weh10] Wehner, S. & Winter, A., ENTROPIC UNCERTAINTY RELATIONS - A SURVEY. *New J. Phys.* **12**, 025009 (2010).

[Wei10] Weihs, G., Jennewein, T., Simon, C., Weinfurter, H. & Zeilinger, A., VIOLATION OF BELL'S INEQUALITY UNDER STRICT EINSTEIN LOCALITY CONDITIONS. *Phys. Rev. Lett.* **81**, 5039-5043 (1998).

[Wer89] Werner, R.F., QUANTUM STATES WITH EINSTEIN-PODOLSKY-ROSEN CORRELATIONS ADMITTING A HIDDEN-VARIABLE MODEL. *Phys. Rev. A* **40**, 4277-4281 (1989).

[Wig32] Wigner, E., ON THE QUANTUM CORRECTION FOR THERMODYNAMIC EQUILIBRIUM. *Phys. Rev.* **40**, 749-759 (1932).

[Wis07] Wiseman, H. M., Jones, S. J. & Doherty, A. C., STEERING, ENTANGLEMENT, NONLOCALITY, AND THE EINSTEIN-PODOLSKY-ROSEN PARADOX. *Phys. Rev. Lett.* **98**, 140402 (2007).

[Wit12] Wittmann, B., Ramelow, S., Steinlechner, F., Langford, N. K., Brunner, N., Wiseman, H. M., Ursin, R. & Zeilinger, A., LOOPHOLE-FREE EINSTEIN-PODOLSKY-ROSEN EXPERIMENT VIA QUANTUM STEERING. *New J. Phys.* **14**, 053030 (2012).

[Woo82] Wootters, W. K. & Zurek, W. H., A SINGLE QUANTUM CANNOT BE CLONED. *Nature* **299**, 802-803 (1982).

[Yan15] Yan, Y., Li, G. X. & Wu, Q. L., ENTANGLEMENT AND EINSTEIN-PODOLSKY-ROSEN STEERING BETWEEN A NANOMECHANICAL RESONATOR AND A CAVITY COUPLED WITH TWO QUANTUM DOTS. *Opt. Ex.* **23**, 21306-21322 (2015).

[Yue76] Yuen, H. P., TWO-PHOTON COHERENT STATES OF THE RADIATION FIELD. *Phys. Rev. A* **13**, 2226-2243 (1976).

[Zha00] Zhang, Y., Wang, H. Li, X., Jing, J., Xie, C. & Peng, K. C., EXPERIMENTAL GENERATION OF BRIGHT TWO-MODE QUADRATURE SQUEEZED LIGHT FROM A NARROW-BAND NONDEGENERATE OPTICAL PARAMETRIC AMPLIFIER. *Phys. Rev. A* **62**, 023813 (2000).

ACKNOWLEDGMENTS

This work would not have been possible without the assistance of many people. I would like to thank Karsten Danzmann for supporting the field of quantum information at the Albert-Einstein-Institute as well as Roman Schnabel and Reinhard Werner for realizing an interdisciplinary project on quantum key distribution and for promoting the studies of their PhD students. Furthermore, I thank Fabian Furrer, Torsten Franz and Jörg Duhme for their commitment to the project and for never getting tired to explain the mathematical subtleties to me. My biggest credit goes definitely to Tobias Gehring (aka E*rklär*berle) for his guidance through the first years of my PhD and his outstanding contribution to the experiment that cannot be expressed in a few words. Thanks a lot. Finally, I would like to thank all the people who supported me scientifically and personally throughout the last five years and, especially, the last months.

CURRICULUM VITAE

PERSONAL INFORMATION

Name	Vitus Händchen
Date of Birth	19.01.1987
Place of Birth	Bad Pyrmont
Nationality	German

EDUCATION

since 10/2010	Doctoral studies in physics at the Institute for Gravitational Physics, Leibniz University Hannover
10/2009 - 10/2010	Diploma thesis at the Institute for Gravitational Physics, Leibniz University Hannover
2008-2009	Study of philosophy at the Leibniz University Hannover
2005-2010	Study of physics at the Leibniz University Hannover, final grade: 1.0 (with distinction)
1999-2005	Viktoria-Luise-Gymnasium Hameln, final grade: 1.7

SCHOLARSHIPS

10/2010 - 09/2013	Doctoral scholarship of the Centre for Quantum Engineering and Space-Time Research, Leibniz University Hannover

LIST OF PUBLICATIONS

1. Eberle, T., Steinlechner, S., Bauchrowitz, J., **Händchen, V.**, Vahlbruch, H., Mehmet, M., Müller-Ebhardt, H. & Schnabel, R., Quantum Enhancement of the Zero-Area Sagnac Interferometer Topology for Graviational Wave Detection. *Phys. Rev. Lett.* **104**, 251102 (2010).

2. Eberle, T., **Händchen, V.**, Duhme, J., Franz, T., Werner, R. F. & Schnabel, R., Strong Einstein-Podolsky-Rosen Entanglement from a Single Squeezed Light Source. *Phys. Rev. A* **83**, 052329 (2011).

3. **Händchen, V.**, Eberle, T., Steinlechner, S., Samblowski, A., Franz, T., Werner, R. F. & Schnabel, R., Observation of One-Way Einstein-Podolsky-Rosen Steering. *Nat. Photon.* **6**, 596-599 (2012).

4. Eberle, T., **Händchen, V.**, Duhme, J., Franz, T., Werner, R. F. & Schnabel, R., Gaussian Entanglement for Quantum Key Distribution from a Single-Mode Squeezing Source. *New J. Phys.* **15**, 053049 (2013).

5. Eberle, T., **Händchen, V.** & Schnabel, R., Stable Control of 10 dB Two-Mode Squeezed Vacuum States of Light. *Opt. Ex.* **21**, 11546-11553 (2013).

6. Steinlechner, J., Ast, S., Krüger, C., Pal Singh, A., Eberle, T., **Händchen, V.** & Schnabel, R., Absorption Measurements of Pariodically Poled Potassium Titanyl Phosphate (PPKTP) at 775 nm and 1550 nm. *Sensors* **13**, 565-573 (2013).

7. Vollmer, C. E., Schulze, D., Eberle, T., **Händchen, V.**, Fiurášek, J. & Schnabel, R., Experimental Entanglement Distribution by Separable States. *Phys. Rev. Lett.* **111**, 230505 (2013).

8. Vollmer, C. E., Baune, C., Samblowski, A., Eberle, T., **Händchen, V.**, Fiurášek, J. & Schnabel, R., Quantum Up-Conversion of Squeezed Vacuum States from 1550 to 532 nm. *Phys. Rev. Lett.* **112**, 073602 (2014).

9. Berni, A. A., Gehring, T., Nielsen, B. M., **Händchen, V.**, Paris, M. G. A. & Andersen, U. L., Ab Initio Quantum-Enhanced Optical Phase Estimation Using Real-Time Feedback Control *Nat. Photon.* **9**, 577-581 (2015).

10. Gehring, T., **Händchen, V.**, Duhme, J., Furrer, F., Franz, T., Pacher, C., Werner, R. F. & Schnabel, R., Implementation of Continuous-Variable Quantum Key Distribution with Composable and One-Sided-Device-Independent Security Against Coherent Attacks. *Nat. Commun.* **6**, 8795 (2015).

COLOPHON

This document was typeset using the typographical look-and-feel `classicthesis` developed by André Miede. The style was inspired by Robert Bringhurst's seminal book on typography "*The Elements of Typographic Style*". `classicthesis` is available for both LaTeX and LyX:

`http://code.google.com/p/classicthesis/`