Realization of Finite-Size Quantum Key Distribution based on Einstein-Podolsky-Rosen Entangled Light

Von der Fakultät für Mathematik und Physik
der Gottfried Wilhelm Leibniz Universität Hannover
zur Erlangung des Grades

Doktor der Naturwissenschaften
– Dr. rer. nat. –

genehmigte Dissertation
von

Dipl.-Phys. Tobias Eberle

geboren am 15. März 1983 in Heidelberg

2013

Referent:	Prof. Dr. Roman Schnabel
Korreferent:	Prof. Dr. Karsten Danzmann
Korreferent:	Prof. Dr. Ulrik L. Andersen
Tag der Promotion:	05.07.2013

Abstract

Quantum key distribution (QKD) is the task of generating a mathematically proven secret key, shared between two remote parties. It is probably the most mature application of quantum mechanics. QKD protocols based on continuous variables, like the amplitude and phase quadratures of light fields, have made great progress in this field during the last years, offering high key rates in local area networks under the assumption that potential adversaries are restricted to collective attacks. Recently, a security proof for continuous variables appeared, which provides security without imposing any restrictions to adversaries, and which also considers effects due to the finite number of measurements. The proof considers a QKD protocol based on Einstein-Podolsky-Rosen (EPR) entangled states and requires strong correlations between the quadratures of the two subsystems.

In this thesis the feasibility of QKD under arbitrary attacks is experimentally demonstrated by an execution of the protocol up to the error correction step. Requirements for the error correction, which would be necessary to generate a secret key, are given. In the presented implementation, EPR entanglement was generated by superimposing two squeezed vacuum modes. The generated continuous-wave squeezed vacuum states represent the first demonstration of such actively stabilized states at the telecommunication wavelength of 1550 nm, with a noise variance more than 10 dB smaller than the vacuum noise variance. Furthermore, a phase-locking scheme was developed that was able to stabilize the generation and measurement of the EPR entangled states with unprecedented strong entanglement.

Restricting potential adversaries to collective attacks relaxes the requirements for the experimental implementation. In this thesis simulations show that distances between the two parties of up to 30 km are feasible for a reasonable number of measurements. This was also shown for entangled states which were generated from a squeezed vacuum mode and a vacuum mode. For such states the first demonstration of the EPR paradox is presented. A complete run of the QKD protocol, including the key generation, was implemented using the EPR entangled states from two squeezed vacuum resources and a post-selection technique.

Keywords: quantum key distribution, continuous variables, Einstein-Podolsky-Rosen entanglement, two-mode squeezed states, coherent attacks, collective attacks.

Kurzfassung

Quantenschlüsselverteilung bezeichnet die Verteilung eines mathematisch beweisbar sicheren Schlüssels zwischen zwei Parteien und ist vermutlich die am weitesten entwickelte Anwendung der Quantenmechanik. Protokolle zur Quantenschlüsselverteilung, die auf kontinuierlichen Variablen, wie z.B. den Amplituden- und Phasenquadraturen von Lichtfeldern, beruhen, haben in den letzten Jahren große Fortschritte gemacht und versprechen unter der Annahme von kollektiven Attacken hohe Schlüsselraten in lokalen Telekommunikationsnetzwerken. Erst kürzlich erschien ein Sicherheitsbeweis, der keinerlei Annahmen bezüglich mögliche Attacken macht und auch berücksichtigt, dass der Schlüssel eine endliche Länge hat. Das im Beweis verwendete Protokoll basiert auf Einstein-Podolsky-Rosen (EPR) verschränkten Zuständen und setzt starke Korrelationen zwischen den Quadraturen der beiden Untersysteme voraus.

Im Rahmen dieser Arbeit wurde die Durchführbarkeit von Quantenschlüsselverteilung unter beliebigen Attacken durch Ausführung des Protokolls bis hin zur Fehlerkorrektur experimentell nachgewiesen. Die Voraussetzungen, die ein möglicher Fehlerkorrekturalgorithmus erfüllen müsste, um mit den korrigierten Daten einen Schlüssel zu erzeugen, werden dargestellt. In der präsentierten Implementierung des Protokolls wurde EPR Verschränkung durch die Überlagerung zweier gequetschter Vakuummoden erzeugt. Dabei wurden erstmals gequetschte Vakuummoden bei einer Wellenlänge von 1550 nm mit einer mehr als 10 dB niedrigeren Varianz als die des Vakuums aktiv stabilisiert. Zudem wird ein Phasenstabilisierungsschema vorgestellt, mit dem sowohl die Erzeugung, als auch die Messung von EPR Zuständen mit der bisher stärksten gemessenen Verschränkung stabilisiert werden konnte.

Wie in dieser Arbeit mit Simulationen gezeigt wird, verringert eine Beschränkung auf kollektive Attacken die Anforderungen an die experimentelle Umsetzung und ermöglicht Distanzen bis zu 30 km zwischen beiden Parteien für eine realisierbare Anzahl an Messungen. Weiterhin erlauben kollektive Attacken auch die Benutzung von EPR Zuständen, die durch Überlagerung einer gequetschten Vakuummode mit einer Vakuummode erzeugt werden. Für solche Zustände wurde in dieser Arbeit die erste Demonstration des EPR Paradoxons präsentiert. Weiterhin wurde mittels der verschränkten Zustände, die aus zwei gequetschten Vakuummoden erzeugt wurden, und mit Hilfe von Postselektion ein vollständiger Lauf eines Quantenschlüsselverteilungsprotokolls implementiert.

Schlüsselworte: Quantenschlüsselverteilung, kontinuierliche Variablen, Einstein-Podolsky-Rosen Verschränkung, zwei-moden gequetschte Zustände, kohärente Attacken, kollektive Attacken.

Contents

Abstract iii

Kurzfassung v

List of Figures xi

List of Tables xv

Glossary xvii

1 Introduction 1
- 1.1 Continuous-Variable Quantum Key Distribution 2
- 1.2 Einstein-Podolsky-Rosen Entanglement 4
- 1.3 Structure of the Thesis 5

2 Gaussian Quantum Information Theory 7
- 2.1 Quadrature Operators 8
- 2.2 Symplectic Transformations 10
- 2.3 Fock States 10
- 2.4 Density Operator 12
- 2.5 Wigner Function 12
- 2.6 Statistical Moments of Quantum States 15
- 2.7 Gaussian States 16
- 2.8 Linear Optical Elements 17
- 2.9 Williamson Form and Symplectic Eigenvalues 19
- 2.10 Symplectic Invariants of Two-Mode Gaussian States 20
- 2.11 Measures of Entanglement 21
  - 2.11.1 Inseparability Criteria 21
  - 2.11.2 Einstein-Podolsky-Rosen Entanglement Criteria 22

2.12 Von Neumann Entropy and Mutual Information 25
2.13 Partial Homodyne Measurement on a Bipartite Gaussian State 28

3 Experimental Techniques 29
3.1 Coherent Light Preparation 29
3.2 Pump Beam Preparation for Parametric Down-Conversion 30
3.3 Squeezed-Light Generation 31
3.4 Balanced Homodyne Detection 33
3.5 Tomographic Reconstruction of the Covariance Matrix 35
3.6 Data Acquisition 36
3.7 Filters and Sample Correlations 40
    3.7.1 Analog Filters 42
    3.7.2 Digital Filters 43

4 Generation of EPR Entanglement at 1550 nm 45
4.1 Experimental Results of Squeezed-Light Generation at 1550 nm 46
4.2 Generation of Entanglement 48
4.3 Einstein-Podolsky-Rosen Steering 49
4.4 EPR Entanglement Generation Using a Single Squeezed Vacuum Resource 51
    4.4.1 Theoretical Description 51
    4.4.2 Experimental Setup 54
    4.4.3 Results 56
4.5 Entanglement Generation Using Two Squeezed Vacuum Resources . . . 58
    4.5.1 Experimental Realization and Locking Scheme 58
    4.5.2 Results 61
4.6 Summary 65

5 Theory of Gaussian Finite-Size Quantum Key Distribution 67
5.1 Security 67
    5.1.1 Universally Composable Security 68
5.2 Generic Protocol 69
5.3 Secure Key Length 71
    5.3.1 Security Definitions 71
    5.3.2 Smooth Min-Max Entropies 71
    5.3.3 Privacy Amplification 73
    5.3.4 Finite-Key Length 75
    5.3.5 Estimation of the Error Correction Leakage Term 76
    5.3.6 Key Rate in the Regime of Infinite Samples 77

5.4 Collective Attacks . . . 77
5.4.1 Protocol . . . 77
5.4.2 Secure Key Length . . . 79
5.4.3 Parameter Estimation . . . 81
5.5 General Attacks . . . 82
5.5.1 Protocol . . . 82
5.5.2 Secure Key Length . . . 84

6 Realization of Quantum Key Distribution under Collective Attacks 85
6.1 Secure Key Rates for Entanglement Using a Single Squeezed Vacuum Resource . . . 86
6.2 Secure Key Rates for Entanglement Using Two Squeezed Vacuum Resources . . . 92
6.3 Implementation of Random Amplitude and Phase Quadrature Measurements . . . 97
6.4 Quantum Random Number Generation . . . 103
6.4.1 Experimental Setup . . . 104
6.4.2 Random Number Generation . . . 105
6.4.3 Statistical Tests of the Generated Random Numbers . . . 107
6.5 Experimental Quantum Key Distribution Results . . . 109
6.5.1 Verification of Simulation Results . . . 109
6.5.2 Generation of a Secret Key using Post Selection . . . 111
6.6 Towards a Possible Local-Area Quantum Key Distribution Link . . . 115
6.7 Summary . . . 118

7 Quantum Key Distribution under General Attacks 119
7.1 Determination of Protocol Parameters . . . 119
7.2 Demonstration of the Feasibility of Secret Key Generation . . . 121
7.3 Summary . . . 124

8 Summary and Outlook 125

A Electronics 127

B Random Number Test Results 131

C Modified Gray Code 141

D Generated Key 143

Bibliography 147

Acknowledgements **159**

Curriculum Vitae **161**

List of Publications **163**

List of Figures

2.1 Wigner Function of the Vacuum State 14

3.1 Coherent Light Preparation 30
3.2 Second Harmonic Generation 31
3.3 Squeezed Light Generation 32
3.4 Balanced Homodyne Detection 33
3.5 Sampling of a Continuous Time Signal 36
  (a) continuous time signal 36
  (b) discrete time signal 36
3.6 Illustration of Aliasing 37
3.7 Frequency and Phase of Sampled Signals Versus Their Physical Frequency 38
  (a) Frequency changes due to aliasing 38
  (b) Phase changes due to aliasing 38
3.8 Data Acquisition with Slow ADC 39
3.9 Data Acquisition with Fast ADC 39
3.10 Impulse and Step Response of a Digital Filter 40
  (a) Impulse response 40
  (b) Step response 40
3.11 Frequency Response of a Digital Filter 41
  (a) Magnitude 41
  (b) Phase 41
3.12 Autocorrelation Function of a Digital Filter 42
3.13 Frequency responses of Analog Filters 43
  (a) Magnitude 43
  (b) Phase 43
3.14 Autocorrelation Functions of Analog Filters 43

4.1 Characterization of a Squeezed State 46

4.2 Principle of the Generation of Continuous-Variable Entanglement . . . 48
4.3 Illustration of Einstein-Podolsky-Rosen Steering 50
4.4 Simulation of EPR Entanglement Versus Single Mode Input Squeezing 52
4.5 Simulation of EPR Entanglement Versus Optical Loss 53
4.6 Experimental Setup of EPR Entanglement Generation Involving a Single Squeezed Vacuum Mode 55
4.7 Characterization of EPR Entanglement Generated by Superimposing a Squeezed Vacuum Mode with a Vacuum Mode 57
4.8 Locking Scheme of The Squeezed-Light Source and Intruduction of Single Sideband Fields 59
4.9 Locking Scheme for the Entanglement Phase 60
4.10 Locking Scheme of the Homodyne Detectors 61
4.11 Duan Inseparability for Entangled States Generated by Superimposing Two Squeezed Vacuum Modes 62
4.12 EPR Entanglement for Entangled States Generated by Superimposing Two Squeezed Vacuum Modes 63
4.13 Stability of the Phase Locks 64

6.1 Secure key rate versus the number of measured samples, only samples from X quadrature 87
6.2 Secure key rate versus the number of measured samples, only samples from P quadrature 87
6.3 Secure key rate versus the number of measured samples, samples from X and P quadrature 88
6.4 Secure key rate versus distance 89
6.5 Secure key rate in dependence of ϵ_{pe} versus distance 91
6.6 Secure key rate for an infinite number of samples in dependence of the error correction efficiency versus distance 91
6.7 Secure key rate versus the number of measured samples, only samples from X quadrature 93
6.8 Secure key rate versus the number of measured samples, only samples from P quadrature 93
6.9 Secure key rate versus the number of measured samples, samples from X and P quadrature 94
6.10 Secure key rate versus distance 95
  (a) For the simulation only samples measured in the X quadrature were taken into account, i.e. $p_X = 1$. 95
  (b) For the simulation only samples measured in the P quadrature were taken into account, i.e. $p_X = 0$. 95

6.11 Secure key rate versus distance, samples from X and P quadrature . . 96
6.12 Secure key rate in dependence of ϵ_{pe} versus distance 98
6.13 Secure key rate in dependence of the error correction efficiency versus distance 98
6.14 Experimental Setup for Local Oscillator Switching 99
6.15 Illustration of the Measurement Process with Random Quadrature Choice 100
6.16 Test of Gaussianity for the Measured Samples 101
  (a) vacuum state 101
  (b) thermal state 101
6.17 Autocorrelation Function of the Measured Samples 102
6.18 Experimental Setup for Quantum Random Number Generation 104
6.19 Characterization of a Vacuum State Measurement 105
  (a) Linear Spectral Density 105
  (b) Autocorrelation 105
6.20 Extractable Information from a Vacuum State Measurement 107
6.21 Secure Key Rate Versus Number of Bins for QKD with Security Under Collective Attacks 110
6.22 Secure Key Rate under Collective Attacks Versus Number of Samples used for Parameter Estimation 110
6.23 Scatter Plots of the Measured Samples with Post Selection 112
  (a) Amplitude Quadrature 112
  (b) Phase Quadrature 112
6.24 Illustration of Encoding Schemes 113
  (a) Regular Gray Code 113
  (b) Modified Gray Code 113
6.25 Bit Error Rate Versus Measurement Time 114
6.26 Proposed Experimental Setup for a Remote Detector 115
6.27 Estimation of the Secure Key Rate for Bob being at the Institute for Quantum Optics 117
  (a) Number of total measurements: $2N = 10^8$. 117
  (b) Number of total measurements: $2N = 10^9$. 117

7.1 Simulated Secure Key Rate under General Attacks versus the Number of Measured Samples 121
7.2 Secure Key Rate under General Attacks versus Number of Samples used for Parameter Estimation 122
7.3 Histogram of Security Parameter d_{PE} 123
7.4 Secure key rate versus error correction efficiency. 123

A.1 Schematic of a Resonant Photo Detector used for Locking of the Squeezed-Light Source 128
A.2 Schematic of a Homodyne Detector 130

List of Tables

6.1 Results of the TestU01 Crush Test Suite 108
6.2 Summarized Test Results of the NIST Test Suite 108
6.3 Summarized Test Results of the Dieharder Test Suite 109

7.1 Scaling Parameters for General Attacks Quantum Key Distribution Protocol 120
7.2 Check of Abort Conditions 121

B.1 Detailed Test Results of the NIST Test Suite 136
B.2 Detailed Test Results of the Dieharder Test Suite 139

Glossary

List of Abbreviations

AC	Alternating Current
ADC	Analog-to-Digital Cconverter
AIT	Austrian Institute of Technology
AOM	Acousto-Optical Modulator
cq-state	Classical-Quantum State
DBS	Dichroic Beam Splitter
DC	Direct Current
EOM	Electro-Optical Modulator
EPR	Einstein-Podolsky-Rosen
FIR filter	Finite Impulse Response Filter
FPGA	Field Programmable Gate Array
FR	Faraday Rotator
GPS	Global Positioning System
i.i.d.	Identically and Independently Distributed
LDPC	Low-Density-Parity-Check
MC	Mode Cleaner
PD	Photo Detector
PDH	Pound-Drever-Hall
POM	Polyoxylmethylene
PPKTP	Periodically Poled Potassium Titanyl Phosphate
PPT	Positive Partial Transpose
PRN	Pseudo-Random Number
PS	Phase Shifter
QKD	Quantum Key Distribution
QRNG	Quantum Random Number Generator

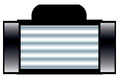
List of Symbols

$(\boldsymbol{d}, S)$	Symplectic map, $\boldsymbol{d}$ translation vector, S symplectic matrix
α	Quadrature measurement abort value
β	Error correction efficiency
χ	Wigner characteristic function
δ	Width of an interval
$\delta(\cdot)$	Delta distribution
ℓ	Number of secure bits
ℓ_{EC}	Number of bits communicated during error correction
ϵ_0	Electric permittivity of the vacuum
ϵ_c	Correctness parameter
ϵ_s	Security parameter
η	Optical efficiency
γ	Covariance matrix
$\hbar$	Planck's constant $h/2\pi$
$\lvert n\rangle$	Eigenstate of photon-number operator
$\lvert P_k\rangle$	Eigenstate of phase quadrature operator
$\lvert X\rangle$	Eigenstate of amplitude quadrature operator
λ	Error correction leakage parameter
$\lVert\cdot\rVert$	Trace norm
$\mathcal{H}$	Hilbert space
$\mathcal{P}(\mathcal{H})$	Set of non-negative operators on $\mathcal{H}$
Ω	Symplectic form
ω_k	Angular frequency of mode k
$\hat{\rho}$	Density operator
$\hat{a}_k$	Bosonic annihilation operator of mode k
$\hat{a}_k^\dagger$	Bosonic creation operator of mode k
$\hat{D}$	Weyl operator
$\hat{n}$	Photon-number operator
$\hat{P}$	Phase quadrature operator
$\hat{X}$	Amplitude quadrature operator
$\overline{x}, \langle x\rangle$	Mean of x
Cov	Covariance
θ, φ	Optical phase
Tr	Trace
Var	Variance
φ_{ent}	Phase between the two modes at the entangling beam splitter
φ_A	Local oscillator phase of Alice's balanced homodyne detector

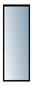
φ_B	Local oscillator phase of Bob's balanced homodyne detector
$\hat{\boldsymbol{b}}$	Vector of bosonic annihilation operators
$\hat{\boldsymbol{E}}$	Quantized electric field operator
$\hat{\boldsymbol{x}}$	Vector of quadrature operators
$\boldsymbol{k}$	Wave-vector of mode k
$\boldsymbol{r}$	Position
C	Correlation coefficient
d_{PE}	Hamming distance as parameter estimation test
f	Fourier frequency
H	Von Neumann entropy
$H_{\max}$	Max-Entropy
$H_{\min}$	Min-Entropy
$I(A:B)$	Mutual Information Between A and B
I_1, I_2, I_3, I_4	Symplectic invariants
k	Number of samples used for parameter estimation
N	Number of modes of a system
n	Number of samples used for generation of a raw key, i.e. after sifting and parameter estimation
n_{bits}	Length of bit encoding
P	Pump power of parametric down-conversion process
p_{pass}	Probability that the protocol does not abort
P_{th}	Threshold pump power
p_θ	Probability of a sample to be measured in quadrature θ
p_X	Probability of a sample to be measured in the amplitude quadrature. $p_P = 1 - p_X$.
s	Symplectic eigenvalue
S_{BS}	Symplectic matrix of a beam splitter
S_{rot}	Symplectic matrix of a phase rotation
S_{sqz}	Symplectic matrix of a squeezing operation
t	Time
V_{sqz}	Variance of a squeezed state normalized to the variance of a vacuum state
W	Wigner function
MP	Moore-Penrose pseudo-inverse
r	Squeezing parameter

List of Pictograms

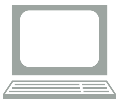
The following pictograms were used in schematics of experimental setups. They were designed by Alexander Franzen.



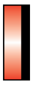
Acousto-Optical Modulator



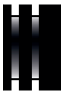
Beam Splitter



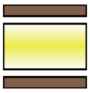
Computer



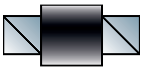
Dichroic Beam Splitter



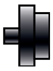
Beam Dump



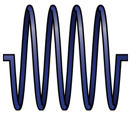
Electro-Optical Modulator



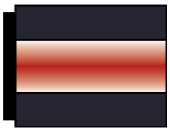
Faraday Isolator



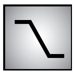
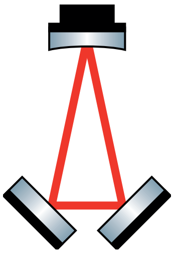
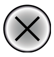
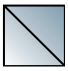
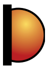
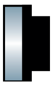
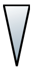
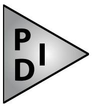
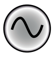
Fiber Coupler



Optical Fiber



Laser

	Lowpass Filter
	Mode Cleaning Ring Cavity
	Double Balanced Mixer
	Polarizing Beam Splitter, Beam Splitter
	Photo Detector
	Phase Shifter
	Phase Shifter
	Servo Controller
	Sine Frequency Generator

CHAPTER 1

Introduction

Quantum key distribution is a quantum information protocol which enables two parties, Alice and Bob, to exchange a key to cipher messages which are sent over an insecure channel, e.g. the internet. Cryptographic algorithms used for secure communication can be classified into two categories: symmetric and asymmetric ciphers [Gis02]. For symmetric ciphers both parties need to share the same key, Alice for encrypting the message and Bob for decrypting it. Hence, the key needs to be shared before the actual communication, as otherwise Bob cannot read the message. To overcome this problem asymmetric algorithms were invented. The key used in asymmetric algorithms consists of two parts, a public one which is known to the general public, and a private one which is kept secret. Alice then uses Bob's public key to encrypt a message and only Bob, who possesses the private key, can decrypt the message. As these algorithms are usually slow to compute, public key algorithms are most often used to exchange a key for a symmetric cipher. The security of such public key algorithms is only based on the fact that present computers are slow in factoring large numbers into their prime number decompositions. Indeed, with today's computers it would last many thousands of years to decipher an encrypted message. Nevertheless, it was shown that this time can be dramatically reduced by quantum computers, since with quantum algorithms the computing time for a prime number decomposition of a number is only polynomial in the length of its bit representation and not exponential as with classical algorithms [Sho97]. A cipher whose security is based on the assumption that present computers are too slow to decipher a message within reasonable time is called *computationally secure*.

The *one-time pad* algorithm, which is a symmetric cipher that is mathematically secure instead of just computationally secure, was already invented during World War I and published in 1926 by G. Vernam [Ver26]. To guarantee its security the following requirements must be fulfilled

(i) the key has to be as long as the message,

(ii) the key has to be uniformly random,

(iii) the key has to be known only to Alice and Bob,

(iv) the key has to be used only once.

While this scheme is perfectly secure as long as the requirements are fulfilled, the key has still to be distributed between the communicating parties without anybody else being able to gain knowledge about it. This problem is addressed by quantum key distribution (QKD). The first QKD protocol, BB84, was invented by Bennett and Brassard in 1984 [Ben84]. Here, Alice prepares a photon in a certain polarization state and sends it to Bob. The polarization of the photon is prepared in either the vertical/horizontal basis or in the anti-diagonal/diagonal basis. A vertically or anti-diagonally polarized photon encodes bit 0 and a horizontally or diagonally polarized photon encodes bit 1. As Bob does not know which basis Alice has chosen, he chooses one at random and measures the polarization. After Alice has sent a certain number of photons to Bob they communicate their choice of bases and discard all measurements performed in a different basis. They proceed by revealing a part of Bob's measurement results and compare them with Alice's preparation. If the number of different values from the revealed measurement outcomes is above a certain threshold they abort, as an eavesdropper may have been present. Otherwise, they correct the errors in their unrevealed outcomes and generate a key. The security of this protocol is based on the no-cloning theorem [Sak11], which states that quantum states cannot be copied without introducing errors. It is also based on the fact that a measurement of a non-eigenstate changes the quantum state.

1.1 Continuous-Variable Quantum Key Distribution

While the protocol described above uses discrete polarization states of single photons to distribute a key between Alice and Bob, in principle any two non-commuting observables of a quantum system would work. Besides the polarization, two commonly used ones are the amplitude and phase quadratures of light fields which have continuous eigenspectra. Using amplitude and phase modulation of Gaussian states for encoding a key and homodyne detection for decoding it, enables the use of fast and cheap standard telecommunication components like amplitude and phase modulators and PIN photo diodes. In comparison, implementations of the BB84 protocol have to employ specialized single photon sources and single photon detectors. The first protocol using continuous variables was introduced by Cerf in 2001 [Cer01] and was based on squeezed states. Shortly afterwards a QKD protocol based on Gaussian modulation of coherent states was proposed [Gro02] and implemented [Gro03]. Further developments of the implementation of this protocol can be found in [Lod07, Fos09, Jou12]. Recently, distances between Alice and Bob of up to 80 km were reached using this scheme [Jou13].

Instead of prepare-and-measure schemes, like the BB84 protocol for discrete variable QKD and like the Gaussian modulation protocol for continuous variables, entanglement-based systems can also be used [Eke91, Urs07, He06, Rod07, Su09]. In such systems a bipartite entangled state is generated and distributed to Alice and Bob, who perform measurements by randomly choosing an observable from two non-commuting ones. While in prepare-and-measure schemes the key has to be generated *a priori* by a random number generator and has to be encoded to a quantum state by state preparation, in entanglement-based schemes the key is directly provided by the quantum measurement. A combination of the two protocols, a Gaussian modulation of entanglement, was reported to be beneficial in terms of achievable distance between the two communicating parties [Mad12].

To analyse the security of a given protocol, possible attacks by an adversary are classified into individual, collective and coherent (general) attacks. Individual attacks are attacks for which the adversary does not need a quantum memory [App08, Jen10, Ari10] to store quantum states and thus measures all exchanged states individually. If the adversary instead possesses a quantum memory, the quantum states can be stored and measured collectively. However, to fall into this class of attacks, the same observable has to be measured for all states. Coherent attacks, also called general attacks in the following, are attacks where instead of measuring the same observable for each quantum state, different observables might be employed on different quantum states. For this class of attacks no assumptions on the adversary's ability are made.

Assuming that an infinite number of continuous-variable quantum states are exchanged reduces general attacks to collective attacks [Ren09]. Indeed, Gaussian attacks are optimal collective attacks [GP06, Nav06] and a secure key rate can be deduced from the Devetak-Winter bound [Dev05, Lod07, Ren05a]. However, if only a finite number of quantum systems are exchanged, as is the case in every real implementation, the situation is more complicated. For collective attacks the security of the QKD protocol using Gaussian modulation was proven [Lev10]. An implementation of this protocol can be found in [Jou13]. Using the smooth min-entropy formalism [Ren05a], a QKD protocol with security for general attacks was provided in [Fur12b]. This protocol, as well as a similar protocol for collective attacks [Fur12b], employs quadrature entangled states. With these two protocols, as well as with the one for Gaussian modulation, the generated key is universally composable secure [Can01, Ren05a]. This means that if combined with other cryptographic primitives, like the one-time pad, the key will remain secret. Proofs based on the mutual information, as for instance the Devetak-Winter bound, are instead not composable secure [Ren05a].

This thesis describes an experimental implementation of the entanglement-based protocol of Ref. [Fur12b] for distributing a finite key which is composable secure under collective attacks. Furthermore, it provides a first implementation of a contin-uous-variable QKD setup which is able to generate a key with finite size that is secure against general attacks.

1.2 Einstein-Podolsky-Rosen Entanglement

The security proof of the finite-size continuous-variable QKD protocol for general attacks demands quadrature entangled states with strong Einstein-Podolsky-Rosen (EPR) entanglement [Fur12b]. EPR entanglement [Rei89] is stronger than inseparability, and is connected to the famous EPR Gedanken experiment in which Einstein, Podolsky and Rosen questioned the completeness of quantum mechanics by presuming local realism [Ein35]. Only in 1981, Aspect et al. [Asp81] proved the completeness of quantum mechanics by demonstrating a violation of the Bell inequalities [Bel64]. The first demonstration of the EPR paradox was performed in 1992 by Ou et al. [Ou92]. Recently the concept of steering, which was introduced by Schrödinger in his response to EPR's paper [Sch35], gained new attention due to theoretical work by Wiseman et al. [Wis07], who showed that for Gaussian states a demonstration of steering is equivalent to a demonstration of the EPR paradox.

This thesis presents an instructive description of steering, as well as the first experimental demonstration of the EPR paradox and steering using quadrature entangled states that are generated by superimposing a squeezed vacuum state with a vacuum state. Furthermore, it describes the generation of the strongest EPR entangled states to date, which were phase controlled in all degrees of freedom. Highly entangled states that are stable over long time scales are not only necessary for the QKD protocol providing security against general attacks, but also for other demanding quantum information protocols like the superactivation of zero-capacity quantum channels [Smi08, Smi11].

1.3 Structure of the Thesis

The structure of the thesis is as follows:

- Chapter 2 introduces the theory of Gaussian quantum information. This chapter provides the necessary theoretical background.
- Chapter 3 describes the experimental techniques used throughout the thesis.
- Chapter 4 presents experimental results of the generation and characterization of squeezed vacuum states at 1550 nm. It further gives an instructive description of the steering process, which is followed by the description of the first experimental realization of the EPR paradox and steering with two-mode entangled states generated by superimposing a squeezed vacuum mode with vacuum mode. The generation and stable control of EPR entangled states generated by superimposing two squeezed vacuum modes concludes the chapter.
- Chapter 5 is devoted to the theoretical description of Gaussian finite-size quantum key distribution. Here, the QKD protocols are introduced used in the following two chapters.
- Chapter 6 describes the realization of the QKD protocol providing security under collective attacks. First, the secure key rates for the two types of entanglement generated in Chapter 4 are analyzed. A description of the experimental setup to gain a secret key follows, including a description of the generation of quantum random numbers. Furthermore the generation of a secure key using a post selection technique is provided.
- Chapter 7 describes and analyzes the first experimental continuous-variable setup which is able to generate a key with security against general attacks. The feasibility of generating a key is discussed.
- Chapter 8 summarizes the experimental results and concludes the thesis.

CHAPTER 2

Gaussian Quantum Information Theory

In this chapter the theory of continuous variable gaussian quantum information is reviewed. The basics given here are used in the following chapters. The chapter follows with some additions the review “Gaussian Quantum Information” by Weedbrook et al. [Wee12].

We start by postulating the quantized electric field operator $\hat{\boldsymbol{E}}$ of an N-mode free space radiation field at position $\boldsymbol{r}$ and time t to be

$$\hat{\boldsymbol{E}}(\boldsymbol{r},t) = i\sum_{k=1}^{N} \boldsymbol{\mathcal{E}_k} \left(\hat{a}_k e^{i(\boldsymbol{k}\cdot\boldsymbol{r}-\omega_k t)} + \hat{a}_k^\dagger e^{-i(\boldsymbol{k}\cdot\boldsymbol{r}-\omega_k t)}\right) \ , \tag{2.1}$$

where $\boldsymbol{\mathcal{E}_k} = \boldsymbol{e}_k(\hbar\omega_k/2\epsilon_0 V)^{\frac{1}{2}}$ with $\boldsymbol{e}_k$ being the polarization vector, $\hbar$ is Planck's constant $h/2\pi$, ω_k is the angular frequency of the kth mode, ϵ_0 is the electric permittivity of the vacuum and V is an arbitrary volume. $\boldsymbol{k}$ denotes the wave-vector of the kth mode. $\hat{a}_k$ and $\hat{a}_k^\dagger$ are the kth mode bosonic annihilation and creation operators, respectively. Hence, the N quantized radiation fields are described by N quantum harmonic oscillators. The $2N$ annihilation and creation operators can be arranged in vectorial form

$$\hat{\boldsymbol{b}} := (\hat{a}_1, \hat{a}_1^\dagger, \ldots, \hat{a}_N, \hat{a}_N^\dagger)^T \ . \tag{2.2}$$

They satisfy the bosonic commutation relation

$$[\hat{b}_\mu, \hat{b}_\nu] = \Omega_{\mu\nu} \quad (\mu,\nu = 1,\ldots,2N) \ , \tag{2.3}$$

where Ω is given by

$$\Omega := \bigoplus_{k=1}^{N} \omega = \begin{pmatrix} \omega & & \\ & \ddots & \\ & & \omega \end{pmatrix} \ , \ \omega := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \ . \tag{2.4}$$

Hereby, we chose the normalization such, that $\hbar = 2$, which yields a variance of the vacuum noise of 1, cf. Section 2.3. As there is no common consensus, other normalizations like $\hbar = 1$ or $\hbar = 1/2$ can be found in the literature, corresponding to a vacuum noise variance of 1/2 or 1/4, respectively. Ω is also known as the *symplectic form* which will become clear in Section 2.2.

We define the *photon-number operator* by

$$\hat{n}_k := \hat{a}_k^\dagger \hat{a}_k \ , \tag{2.5}$$

which accounts for the number of photons in the kth mode.

2.1 Quadrature Operators

With the annihilation and creation operators we can define the quadrature field operators

$$\hat{X}_k := \hat{a}_k + \hat{a}_k^\dagger \ , \tag{2.6}$$

$$\hat{P}_k := i(\hat{a}_k^\dagger - \hat{a}_k) \ . \tag{2.7}$$

In contrast to the annihilation and creation operators the quadrature field operators are Hermitian and hence observables. We call $\hat{X}_k$ the amplitude quadrature operator and $\hat{P}_k$ the phase quadrature operator of the kth mode. The operators correspond to the position and momentum operators of the quantum harmonic oscillator. In vectorial form they read

$$\hat{\boldsymbol{x}} := (\hat{X}_1, \hat{P}_1, \dots, \hat{X}_N, \hat{P}_N)^T \ . \tag{2.8}$$

The quadrature operators satisfy the commutation relation

$$[\hat{x}_\mu, \hat{x}_\nu] = 2i\Omega_{\mu\nu} \quad (\mu, \nu = 1, \dots, 2N) \ , \tag{2.9}$$

which follows from Eq. (2.3). Using this result the Heisenberg uncertainty relation [Sak11] of the quadrature operators reads

$$\mathrm{Var}(\hat{x}_\mu)\,\mathrm{Var}(\hat{x}_\nu) \geq \frac{1}{4}|[\hat{x}_\mu, \hat{x}_\nu]|^2 = (\Omega_{\mu\nu})^2 = |\Omega_{\mu\nu}| \ , \tag{2.10}$$

where $\mathrm{Var}(\hat{A})$ denotes the variance $\langle \hat{A}^2 \rangle - \langle \hat{A} \rangle^2$ of an operator $\hat{A}$. Here $\langle \hat{A} \rangle$ denotes the mean of $\hat{A}$.

As the quadrature operators $\hat{X}_k$ and $\hat{P}_k$ are observables, they have eigenstates $|X_k\rangle$ and $|P_k\rangle$,

$$\hat{X}_k|X_k\rangle = X_k|X_k\rangle \ , \tag{2.11}$$

$$\hat{P}_k|P_k\rangle = P_k|P_k\rangle \ , \tag{2.12}$$

with continuous eigenvalues $X_k \in \mathbb{R}$ and $P_k \in \mathbb{R}$. We call these eigenstates the *quadrature states* [Leo97]. Quadrature states are orthogonal

$$\langle X_k|X'_k\rangle = \delta(X_k - X'_k) \ , \quad \langle P_k|P'_k\rangle = \delta(P_k - P'_k) \tag{2.13}$$

and complete

$$\int \mathrm{d}X_k |X_k\rangle\langle X_k| = \int \mathrm{d}P_k |P_k\rangle\langle P_k| = 1 \ . \tag{2.14}$$

Although quadrature states are not normalizable and hence experimentally not feasible, they are useful to define the *quadrature wave functions* of the quantum state $|\Psi\rangle$ [Leo97]

$$\Psi(X_k) := \langle X_k|\Psi\rangle \ , \tag{2.15}$$

$$\tilde{\Psi}(P_k) := \langle P_k|\Psi\rangle \ . \tag{2.16}$$

The moduli square of these wave functions, $|\Psi(X_k)|^2$ and $|\tilde{\Psi}(P_k)|^2$, are the quadrature probability distributions of $|\Psi\rangle$ which are measurable by homodyne detection, cf. Chapter 3.4.

For N modes Eqs. (2.11) and (2.12) can be written as

$$\hat{\boldsymbol{x}}|x\rangle^T = \boldsymbol{x}|x\rangle^T \tag{2.17}$$

with $\boldsymbol{x} \in \mathbb{R}^{2N}$ and $|x\rangle := (|x_1\rangle, \ldots, |x_{2N}\rangle)^T$. Here, the continuous variables $\boldsymbol{x}$ are the continuous eigenvalues of the $2N$ quadrature operators $\hat{\boldsymbol{x}}$. Together with the bilinear form Ω, cf. Eq. (2.4), the continuous variables $\boldsymbol{x}$ form a symplectic space, the *phase space* $\mathcal{K} := (\mathbb{R}^{2N}, \Omega)$. For two vectors $\boldsymbol{\xi}, \boldsymbol{\eta} \in \mathbb{R}^{2N}$, Ω acts as the symplectic scalar product

$$(\boldsymbol{\xi},\boldsymbol{\eta}) = \boldsymbol{\xi}^T \cdot \Omega \cdot \boldsymbol{\eta} = \sum_{\mu,\nu=1}^{2N} \Omega_{\mu\nu}\xi_\mu\eta_\nu \ .$$

2.2 Symplectic Transformations

Symplectic transformations are a change of basis in the phase space $\mathcal{K}$. Like all basis transformations in linear algebra symplectic transformations must keep the scalar product invariant. Hence, a symplectic transformation S must fulfill

$$\begin{aligned}\boldsymbol{\xi}^T \cdot \Omega \cdot \boldsymbol{\eta} &\overset{!}{=} (S\boldsymbol{\xi})^T \cdot \Omega \cdot (S\boldsymbol{\eta}) \\ &= \boldsymbol{\xi}^T \cdot S^T \Omega S \cdot \boldsymbol{\eta}\end{aligned}$$

for all $\boldsymbol{\xi},\boldsymbol{\eta} \in \mathbb{R}^{2N}$. Thus,

$$\Omega = S^T \Omega S \ . \tag{2.18}$$

As the symplectic form originates from the commutation relation, cf. Eq. (2.3), symplectic transformations keep the commutation relation invariant, i.e. physical quantum states are transformed into physical quantum states.

2.3 Fock States

Fock states, named after V. A. Fock, are the eigenstates $|n_k\rangle$ of the photon-number operator $\hat{n}_k$ as defined in Eq. (2.5)

$$\hat{n}_k|n_k\rangle = n_k|n_k\rangle \ . \tag{2.19}$$

If $|n_k\rangle$ is a Fock state with eigenvalue n_k, $\hat{a}_k|n_k\rangle$ and $\hat{a}_k^\dagger|n_k\rangle$ are also Fock states, having the eigenvalues $n_k - 1$ and $n_k + 1$, respectively,

$$\hat{a}_k|n_k\rangle = \sqrt{n_k}|n_k - 1\rangle \ , \tag{2.20}$$

$$\hat{a}_k^\dagger|n_k\rangle = \sqrt{n_k + 1}|n_k + 1\rangle \ . \tag{2.21}$$

These equations show why $\hat{a}_k$ and $\hat{a}_k^\dagger$ are called annihilation and creation operator, respectively. $\hat{a}_k$ annihilates a photon from the kth mode of the field, while $\hat{a}_k^\dagger$ instead creates a photon in that mode.

Since n_k is an integer and the photon number cannot be negative [Leo97]

$$\hat{a}_k|0\rangle = 0 \ . \tag{2.22}$$

Hence, $|0\rangle$ is the ground state with mean photon number 0. As it contains no photons this state is called the *vacuum state*. Its quadrature wave function $\Psi_0(X_k) = \langle X_k|0\rangle$ can be obtained by solving

$$\begin{aligned}
0 &= \langle X_k|\hat{a}_k|0\rangle && (2.23)\\
&= \frac{1}{2}\langle X_k|\left(\hat{X}_k + i\hat{P}_k\right)|0\rangle && (2.24)\\
&= \frac{1}{2}\int \mathrm{d}X'_k \langle X_k|\left(\hat{X}_k + i\hat{P}_k\right)|X'_k\rangle\langle X'_k|0\rangle && (2.25)\\
&= \frac{1}{2}\int \mathrm{d}X'_k \left(X'_k\langle X_k|X'_k\rangle + 2\frac{\partial}{\partial X_k}\langle X_k|X'_k\rangle\right)\langle X'_k|0\rangle && (2.26)\\
&= \frac{1}{2}\left(X_k + 2\frac{\partial}{\partial X_k}\right)\langle X_k|0\rangle\ , && (2.27)
\end{aligned}$$

where in the first line we used the property $\hat{a}|0\rangle = 0$ from Eq. (2.22). The second line used the definition of the quadrature operators, Eq. (2.6) and (2.7), whereas in the third line the closure relation for the quadrature states from Eq. (2.14) was inserted. In the fourth line the relation $\langle X_k|\hat{P}_k|X'_k\rangle = -2i(\partial/\partial X_k)\langle X_k|X'_k\rangle$ from quantum mechanics text books, e.g. [Sak11], was applied[1]. The fifth and final line made use of the closure relation for quadrature states again and yields a differential equation for the quadrature wave function of the vacuum state. This differential equation is solved by

$$\Psi_0(X_k) = (2\pi)^{-1/4}\exp\left(-\frac{X_k^2}{4}\right)\ . \qquad (2.28)$$

The normalization factor was chosen to yield $\int \mathrm{d}X_k|\Psi_0(X_k)|^2 = 1$. Taking the modulus square gives the probability distribution of the vacuum state for a measurement of the X_k quadrature

$$|\Psi_0(X_k)|^2 = (2\pi)^{-1/2}\exp\left(-\frac{X_k^2}{2}\right)\ . \qquad (2.29)$$

By computing the Fourier transform of $\Psi_0(X_k)$ we can obtain the phase quadrature wave function of the vacuum

$$\tilde{\Psi}_0(P_k) = (2\pi)^{-1/4}\exp\left(-\frac{P_k^2}{4}\right)\ , \qquad (2.30)$$

---

[1] remember that we have chosen $\hbar = 2$ for normalization purposes

which yields for the probability distribution

$$|\tilde{\Psi}_0(P_k)|^2 = (2\pi)^{-1/2} \exp\left(-\frac{P_k^2}{2}\right) \ . \tag{2.31}$$

Hence, the vacuum state has a Gaussian quadrature probability distribution with mean 0 and variance 1 in both amplitude and phase quadrature.

2.4 Density Operator

The physical information about a quantum system is encoded in its quantum state, which is described by its density operator

$$\hat{\rho} = \sum_i p_i |\phi_i\rangle\langle\phi_i| \tag{2.32}$$

on a Hilbert space $\mathcal{H}$. Here, p_i is the probability to find the system in the state $|\phi_i\rangle$ with $\sum_i p_i = 1$. The density operator is Hermitian ($\hat{\rho} = \hat{\rho}^\dagger$) and positive semi-definite ($\hat{\rho} \geq 0$), which means that all its eigenvalues are real and positive.

The trace of an arbitrary operator $\hat{A}$ is defined as

$$\operatorname{Tr} \hat{A} = \sum_i \langle i|\hat{A}|i\rangle \ , \tag{2.33}$$

where $\{|i\rangle\}$ forms an orthonormal basis. The trace of a density operator is $\operatorname{Tr} \hat{\rho} = 1$. In general $\operatorname{Tr} \hat{\rho}^2 \leq 1$, and the identity $\operatorname{Tr} \hat{\rho}^2 = 1$ only holds if $\hat{\rho}$ is in a pure state, i.e. $\hat{\rho} = |\phi\rangle\langle\phi|$. $\operatorname{Tr} \hat{\rho}^2$ is called the *purity* of the quantum system.

With the trace we can now define the mean of an arbitrary operator $\hat{A}$. It is given by

$$\langle \hat{A} \rangle = \operatorname{Tr} \hat{\rho}\hat{A} \ . \tag{2.34}$$

2.5 Wigner Function

Any density operator, as defined in Section 2.4, has a representation defined on a real symplectic space, a phase space. This representation is called *Wigner Function*. It was introduced by Eugene Wigner in 1932 in his paper [Wig32].

We start by introducing the Weyl operator, which is defined as

$$\hat{D}(\boldsymbol{\xi}) := \exp(i\hat{\boldsymbol{x}}^T \cdot \Omega \cdot \boldsymbol{\xi}) \ , \tag{2.35}$$

where $\hat{\boldsymbol{x}}$ is the vector of the $2N$ quadrature operators as defined in Eq. (2.8), Ω is the symplectic form and $\boldsymbol{\xi} \in \mathbb{R}^{2N}$ a phase space vector. The Weyl operator describes a translation in phase space, i.e. it translates the mean of the quadrature operators by $\boldsymbol{\xi}$.

Using the Weyl operator an arbitrary density operator $\hat{\rho}$ corresponds to a Wigner characteristic function

$$\chi(\boldsymbol{\xi}) = \mathrm{Tr}\, \hat{\rho} \hat{D}(\boldsymbol{\xi}) \ . \tag{2.36}$$

The Wigner characteristic function can be transformed into a Wigner function via Fourier transformation

$$W(\boldsymbol{x}) = \int \frac{\mathrm{d}^{2N}\boldsymbol{\xi}}{(2\pi)^{2N}} \exp\left(-i\boldsymbol{x}^T \cdot \Omega \cdot \boldsymbol{\xi}\right) \chi(\boldsymbol{\xi}) \ , \tag{2.37}$$

where $\boldsymbol{x} \in \mathbb{R}^{2N}$ is a phase space vector. The Wigner function is real for any density operator and is normalized to 1, i.e.

$$\int \mathrm{d}x_1 \dots \mathrm{d}x_{2N} W(\boldsymbol{x}) = 1 \ .$$

While the Wigner function is a representation of a quantum system, it is not a probability distribution as it can take negative values for certain quantum states. Nevertheless, it can be treated as a quasi-probability distribution. A projection of the Wigner function to an arbitrary quadrature x_μ yields a probability distribution for this quadrature

$$\langle x_\mu | \hat{\rho} | x_\mu \rangle = \int \mathrm{d}x_1 \dots \mathrm{d}x_{\mu-1}\, \mathrm{d}x_{\mu+1} \dots \mathrm{d}x_{2N} W(\boldsymbol{x}) \ . \tag{2.38}$$

The purity of a quantum state can be expressed by the Wigner function via

$$\mathrm{Tr}\, \hat{\rho}^2 = 4\pi \int \mathrm{d}x_1 \dots \mathrm{d}x_{2N} \left(W(\boldsymbol{x})\right)^2 \ . \tag{2.39}$$

Let us now compute the Wigner function of the vacuum state as an example. For one mode Eq. (2.37) can be simplified to [Leo97]

$$W(X,P) = \frac{1}{4\pi} \int \mathrm{d}x \exp(iPx/2) \langle X - \frac{x}{2} | \hat{\rho} | X + \frac{x}{2} \rangle \ . \tag{2.40}$$

Plugging in the density operator of the vacuum state $\hat{\rho} = |0\rangle\langle 0|$ yields

$$W(X,P) = \frac{1}{4\pi} \int \mathrm{d}x \exp(iPx/2) \Psi_0\left(X - \frac{x}{2}\right) \Psi_0^*\left(X + \frac{x}{2}\right) \ , \tag{2.41}$$

where $\Psi_0(X)$ is the quadrature wave function of the vacuum state from Eq. (2.28). By carrying out the integration we obtain the Wigner function of the vacuum state

$$W(X,P) = \frac{1}{2\pi} \exp\left(-\frac{X^2}{2} - \frac{P^2}{2}\right) . \tag{2.42}$$

By projecting the Wigner function on X or P, cf. Eq. (2.38), the quadrature probability density functions from Eq. (2.29) and (2.31), respectively, are obtained. Figure 2.1 shows a plot of the Wigner function and the quadrature probability distributions.

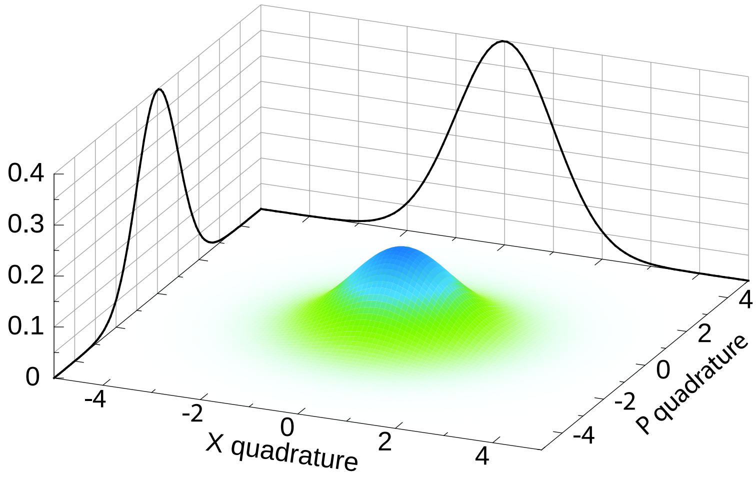


Figure 2.1: Wigner function of the vacuum state. The black traces show the probability distributions of the X and P quadratures obtained by projecting the Wigner function on the respective quadrature.

The Wigner function can also be used to calculate quantum mechanical averages. We assume $\hat{A}(\hat{\boldsymbol{x}})$ to be an arbitrary operator defined as a function of the quadrature operators $\hat{\boldsymbol{x}}$. Its average with respect to the quantum state $\hat{\rho}$ can be calculated by

$$\langle \hat{A}(\hat{\boldsymbol{x}}) \rangle = \int \mathrm{d}x_1 \ldots \mathrm{d}x_{2N} A(\boldsymbol{x}) W(\boldsymbol{x}) . \tag{2.43}$$

Here, $A(\boldsymbol{x})$ is the c-number representation of $\hat{A}(\hat{\boldsymbol{x}})$

$$\hat{A}(\hat{\boldsymbol{x}}) \to A(\boldsymbol{x}) .$$

To make this work, $\hat{A}$ must be in Weyl-Wigner ordering which is described in detail in [Sch01]. For what follows we note, that any symmetric ordered operator is already Weyl-Wigner ordered.

2.6 Statistical Moments of Quantum States

The properties of a quantum state $\hat{\rho}$ are described by its statistical moments. In particular, we consider here the first and second moments of a state. For a certain class of quantum states, the so-called *Gaussian states*, the first two moments are sufficient to fully characterize the state. The quantum states that we are interested in in this thesis belong to this class of states.

The first moment, also known as the mean value, is given by

$$\overline{\boldsymbol{x}} := \langle \hat{\boldsymbol{x}} \rangle = \operatorname{Tr} \hat{\rho} \hat{\boldsymbol{x}} \ . \tag{2.44}$$

Using Eq. (2.43) this can be rewritten in terms of the Wigner function which yields for the μth component

$$\langle x_\mu \rangle = \int \mathrm{d}x_1 \ldots \mathrm{d}x_{2N} x_\mu W(\boldsymbol{x}) \ . \tag{2.45}$$

The second moment is called the covariance matrix γ. An arbitrary element of the covariance matrix is defined by

$$\gamma_{\mu\nu} := \frac{1}{2} \langle \Delta\hat{x}_\mu \Delta\hat{x}_\nu + \Delta\hat{x}_\nu \Delta\hat{x}_\mu \rangle \tag{2.46}$$

$$= \frac{1}{2} \operatorname{Tr} \hat{\rho} \left(\Delta\hat{x}_\mu \Delta\hat{x}_\nu + \Delta\hat{x}_\nu \Delta\hat{x}_\mu \right) \ , \tag{2.47}$$

where $\Delta\hat{x}_\mu = \hat{x}_\mu - \langle \hat{x}_\mu \rangle$. Using the linearity property of the mean Eq. (2.46) can be rewritten as

$$\gamma_{\mu\nu} = \frac{1}{2} \langle \hat{x}_\mu \hat{x}_\nu + \hat{x}_\nu \hat{x}_\mu \rangle - \langle \hat{x}_\mu \rangle \langle \hat{x}_\nu \rangle \ ,$$

where the first term is the mean of a symmetric operator. Applying Eq. (2.43) the covariance matrix element can be calculated from the Wigner function by

$$\gamma_{\mu\nu} = \left(\int \mathrm{d}x_1 \ldots \mathrm{d}x_{2N} x_\mu x_\nu W(\boldsymbol{x}) \right) - \langle \hat{x}_\mu \rangle \langle \hat{x}_\nu \rangle \ . \tag{2.48}$$

Taking the example of the vacuum state, whose Wigner function is given by Eq. (2.42), the mean and the covariance matrix calculated from Eq. (2.45) and (2.48), respectively, are

$$\overline{\boldsymbol{x}} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \ , \quad \gamma = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \ . \tag{2.49}$$

Given the mean $\overline{\boldsymbol{x}}$ and the covariance matrix γ from a general N-mode Gaussian state, the Wigner function can be written as [Wee12]

$$W(\boldsymbol{x}) = \frac{1}{(2\pi)^N \sqrt{\det \gamma}} \exp\left(-\frac{1}{2} (\boldsymbol{x} - \overline{\boldsymbol{x}})^T \gamma^{-1} (\boldsymbol{x} - \overline{\boldsymbol{x}}) \right) . \tag{2.50}$$

2.7 Gaussian States

In the last section we have seen the statistical properties of the vacuum state, a state which is probably the most fundamental Gaussian state. Another state that will become useful later, is a *thermal state.* A thermal state is a state which maximizes the von Neumann entropy for a fixed number of photons $\mathrm{Tr}\, \hat{\rho}_{th} \hat{n} = \overline{n}$. The density operator of such a state is given by [Bar97]

$$\hat{\rho}_{th} = \sum_{n=0}^{\infty} \frac{\overline{n}^n}{(\overline{n}+1)^{n+1}} |n\rangle\langle n| \ . \tag{2.51}$$

Following the procedure given above for the vacuum state, the Wigner function obtained for the thermal state takes a Gaussian form. Hence, a thermal state is also a Gaussian state and its mean and covariance matrix is given by

$$\overline{\boldsymbol{x}} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \ , \quad \gamma = \begin{pmatrix} 2\overline{n}+1 & 0 \\ 0 & 2\overline{n}+1 \end{pmatrix} \ . \tag{2.52}$$

To identify further Gaussian states, we will have a look at the following map

$$\overline{\boldsymbol{x}} \to S\overline{\boldsymbol{x}} + \boldsymbol{d} \ , \quad \gamma \to S\gamma S^T \ , \tag{2.53}$$

where S is a symplectic matrix, i.e. $S\Omega S^T = \Omega$, and $\boldsymbol{d} \in \mathbb{R}^{2N}$ is a translation vector. Obviously Gaussian states will be transformed into Gaussian states and since S is symplectic, the new state will be physical. In the following we denote $(\boldsymbol{d}, S)$ as symplectic map.

A translation of the vacuum state in phase space by $\boldsymbol{d}_\alpha \in \mathbb{R}^2$, i.e.

$$\overline{\boldsymbol{x}} = \boldsymbol{d}_\alpha = \begin{pmatrix} x \\ p \end{pmatrix} \ , \quad \gamma = \mathbb{1}_2 \ , \tag{2.54}$$

where $\mathbb{1}_2$ is the 2×2 identity matrix, is called a *displaced vacuum state* or a *coherent state* [Wee12]. $\alpha = (x + ip)/2$ is called the complex amplitude and the coherent state is denoted as $|\alpha\rangle$, satisfying $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$ [Gla63]. Hence, the coherent state is an eigenstate of the annihilation operator.

A *squeezed state* [Bar97] is generated by

$$\boldsymbol{d} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \ , \quad S_{\text{sqz}}(r) = \begin{pmatrix} e^{-r} & 0 \\ 0 & e^{r} \end{pmatrix} \ , \tag{2.55}$$

where $r \in \mathbb{R}$ is the squeezing parameter. For $r > 0$ the state is squeezed in the amplitude quadrature, while for $r < 0$ it is squeezed in the phase quadrature. Applying S_{sqz} to a vacuum state yields a *squeezed vacuum state*, while applying it to a thermal state it generates a *squeezed (thermal) state*. In the same manner S_{sqz} generates a *squeezed displaced vacuum state* or *squeezed coherent state*, when applied to a coherent state. The generation of squeezed states is described in Chapter 3.3.

2.8 Linear Optical Elements

In this section we will introduce two passive optical elements that keep Gaussian states Gaussian, namely a (static) phase shifter and a beam splitter. Based on the transformation caused by a beam splitter we will be able to describe two-mode squeezed vacuum states and optical loss.

Phase Shifts A phase shift, or phase rotation, of a mode with respect to another mode is usually introduced by changing its propagation length. The phase shift by an angle θ is described in phase space by the transformation

$$\boldsymbol{d} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \ , \quad S_{\text{rot}}(\theta) = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \ . \tag{2.56}$$

So far we have only given the symplectic maps from Eqs. (2.54), (2.55) and (2.56) on 1-mode systems. Applying such a transformation to a submode of an N-mode system can be described by

$$\boldsymbol{d} = (0, 0, \ldots, d'_1, d'_2, \ldots, 0, 0)^T \ , \quad S = \mathbb{1}_2 \otimes \cdots \otimes S' \otimes \cdots \mathbb{1}_2 \ , \tag{2.57}$$

where $(\boldsymbol{d}' = (d'_1, d'_2)^T, S')$ is a symplectic transformation according to Eq. (2.53) and $\mathbb{1}_2$ denotes the 2×2 identity matrix.

Beam Splitters and Two-Mode Squeezed Vacuum States A beam splitter is an optical element which combines two modes with a ratio given by the power transmissivity $\tau \in [0, 1]$ yielding two output modes. Let γ be a 4×4 covariance matrix which describes the input fields prior to the combination by a beam splitter.

For example these modes are given by

$$\overline{\boldsymbol{x}} = \mathbf{0} \; , \tag{2.58}$$

$$\gamma = \begin{pmatrix} S_{\mathrm{sqz}}(r) & 0 \\ 0 & S_{\mathrm{sqz}}(-r) \end{pmatrix} \mathbb{1}_4 \begin{pmatrix} S_{\mathrm{sqz}}(r)^T & 0 \\ 0 & S_{\mathrm{sqz}}(-r)^T \end{pmatrix} = \begin{pmatrix} e^{-2r} & 0 & 0 & 0 \\ 0 & e^{2r} & 0 & 0 \\ 0 & 0 & e^{2r} & 0 \\ 0 & 0 & 0 & e^{-2r} \end{pmatrix} , \tag{2.59}$$

which describes two squeezed vacuum modes squeezed with squeezing parameters r and $-r$.

The symplectic map $(\boldsymbol{d}, S)$ of a beam splitter is defined by

$$\boldsymbol{d} = \mathbf{0} \; , \quad S_{\mathrm{BS}}(\tau) = \begin{pmatrix} \sqrt{1-\tau}\mathbb{1}_2 & \sqrt{\tau}\mathbb{1}_2 \\ -\sqrt{\tau}\mathbb{1}_2 & \sqrt{1-\tau}\mathbb{1}_2 \end{pmatrix} , \tag{2.60}$$

where τ is the power transmissivity. It transforms Eqs. (2.58) and (2.59) according to Eq. (2.53) for $\tau = 0.5$ into

$$\overline{\boldsymbol{x}}' = \mathbf{0} \; , \tag{2.61}$$

$$\gamma' = \begin{pmatrix} \cosh(2r) & 0 & \sinh(2r) & 0 \\ 0 & \cosh(2r) & 0 & -\sinh(2r) \\ \sinh(2r) & 0 & \cosh(2r) & 0 \\ 0 & -\sinh(2r) & 0 & \cosh(2r) \end{pmatrix} . \tag{2.62}$$

This state is called a *two-mode squeezed vacuum state*. In general we call all states "two-mode squeezed vacuum states" that are generated by superimposing two squeezed vacuum states with possibly different squeezing parameters r_1 and r_2, at a beam splitter with arbitrary power transmissivity. We include into this definition states which have either $r_1 = 0$ *or* $r_2 = 0$ and are, hence, generated by superimposing a squeezed vacuum state with a vacuum state.

For an N-mode system a beam splitter combining modes k and l can be described by the symplectic map

$$\boldsymbol{d} = \mathbf{0} \; , \tag{2.63}$$

$$\left(S_{\mathrm{BS}}^{k,l}(\tau)\right)_{i,j} = \left\{ \begin{array}{ll} \sqrt{1-\tau}\delta_{i,j} + \sqrt{\tau}(\delta_{2k-i,2l-j} - \delta_{2l-i,2k-j}) & i,j \in M \\ \delta_{i,j} & i,j \in [1,2N] \setminus M \end{array} \right. , \tag{2.64}$$

where $M = \{2k-1, 2k, 2l-1, 2l\}$.

Optical Loss Optical loss to a mode A with mean $\overline{\boldsymbol{x}}_A$ and covariance matrix γ_A can be described by superimposing this mode with a vacuum mode at a beam splitter. Thereby the beam splitter's transmissivity τ describes the amount of optical loss $\epsilon \in [0,1]$. The output modes of the beam splitter are given by

$$\begin{pmatrix}\overline{\boldsymbol{x}}_A\\ \mathbf{0}\end{pmatrix} \to S_{\mathrm{BS}}(\epsilon)\begin{pmatrix}\overline{\boldsymbol{x}}_A\\ \mathbf{0}\end{pmatrix} , \tag{2.65}$$

$$\gamma_A \otimes \mathbb{1}_2 \to S_{\mathrm{BS}}(\epsilon)(\gamma_A \otimes \mathbb{1}_2)S_{BS}(\epsilon)^T . \tag{2.66}$$

Taking the partial trace over the mode that contains the loss yields

$$\overline{\boldsymbol{x}}_A \to \sqrt{1-\epsilon}\,\overline{\boldsymbol{x}}_A \tag{2.67}$$

$$\gamma_A \to (1-\epsilon)\gamma_A + \epsilon\mathbb{1}_2 . \tag{2.68}$$

Often the optical efficiency $\eta = 1-\epsilon$ instead of the optical loss ϵ is given. Assuming two different optical efficiencies η_1 and η_2 on mode A, the new state reads

$$\overline{\boldsymbol{x}}_A \to \sqrt{\eta_1\eta_2}\,\overline{\boldsymbol{x}}_A \tag{2.69}$$

$$\gamma_A \to \eta_1\eta_2\gamma_A + (1-\eta_1\eta_2)\mathbb{1}_2 , \tag{2.70}$$

which can be derived by applying Eqs. (2.67) and (2.68) twice. Hence, subsequent optical efficiencies can be multiplied to yield a total efficiency.

2.9 Williamson Form and Symplectic Eigenvalues

Every N-mode covariance matrix γ can be transformed by a symplectic transformation S into its Williamson form [Wil36, Wee12]

$$S\gamma S^T = \begin{pmatrix} s_1 & & & & \\ & s_1 & & & \\ & & \ddots & & \\ & & & s_N & \\ & & & & s_N \end{pmatrix} , \tag{2.71}$$

where $s_1, \dots, s_N$ are positive, real values, called the N *symplectic eigenvalues*. The symplectic eigenvalues can be determined by taking the modulus of the eigenvalues of $i\Omega\gamma$.

Equation (2.71) describes that every N-mode Gaussian state γ can be obtained from an N-mode thermal state with $\overline{n}_\mu = \frac{1}{2}(s_\mu - 1)$, $(\mu = 1, \dots, N)$, cf. Eq. (2.52), by a symplectic transform S. Hereby, S can be decomposed into an appropriate sequence of $S_{\text{sqz}}, S_{\text{rot}}$ and S_{BS}. This means that γ can be obtained from a thermal state by squeezing, phase rotating and combining modes.

As the covariance matrix of Eq. (2.71) has to describe physical thermal states, i.e. $\forall\mu : \overline{n}_\mu \geq 0$, it follows $\forall\mu : s_\mu \geq 1$. Therefore the symplectic spectrum of a covariance matrix can be used to check whether the covariance matrix is bonafide, i.e. whether it describes a physical quantum state. Hence, in terms of covariance matrices the Heisenberg uncertainty principle, cf. Eq. (2.10), is equivalent to

$$\gamma > 0 \ , \quad i\Omega\gamma \geq 1 \ , \tag{2.72}$$

where $A > x$, with $A \in \mathbb{R}^{2N\times 2N}$ symmetric, means that all eigenvalues of $A - x\mathbb{1}_{2N}$ are larger than 0.

Symplectic eigenvalues are also useful to determine whether a state is inseparable or separable, cf. Section 2.11.1, and to compute the entropy of a state, cf. Section 2.12.

2.10 Symplectic Invariants of Two-Mode Gaussian States

Symplectic invariants are, as the name implies, quantities that do not change under symplectic transformations. For a 2-mode state the covariance matrix reads in block form

$$\gamma = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix} \ . \tag{2.73}$$

The symplectic invariants of this state are [Ser04, Buo10]

$$I_1 = \det A \ , \tag{2.74}$$

$$I_2 = \det B \ , \tag{2.75}$$

$$I_3 = \det C \tag{2.76}$$

and

$$I_4 = \det \gamma \ . \tag{2.77}$$

The symplectic invariants can be used to express certain quantities of the state. For example the purity of a Gaussian state $\hat{\rho}$ can be evaluated by plugging Eq. (2.50) into

Eq. (2.39) which yields

$$\mathrm{Tr}\,\hat{\rho}^2 = \frac{1}{\sqrt{\det\gamma}} = 1/\sqrt{I_4}\ , \tag{2.78}$$

where in the last step Eq. (2.77) has been used.

2.11 Measures of Entanglement

In Section 2.8 we have introduced two-mode squeezed states which are bipartite entangled states. In this section we will describe different measures of entanglement. In general, we can distinguish between separable and inseparable (i.e. entangled) states. Criteria for inseparability are described in Section 2.11.1. A subclass of all inseparable states are the so-called *Einstein-Podolsky-Rosen* (EPR) entangled states. EPR entanglement is a direction dependent property and will be described in Section 2.11.2. A subclass of the EPR states which necessarily shows the EPR property in both directions, are states that violate a Bell inequality. A Bell inequality [Bel64] can never be violated in the Gaussian setting, i.e. using exclusively Gaussian states and Gaussian measurements [Bel86, Ban98]. Since this thesis deals with the Gaussian setting, we will not consider Bell states here.

2.11.1 Inseparability Criteria

Inseparability of bipartite states can be certified using two independent criteria, the positive partial transpose (PPT) criterion [Sim00] and the Duan criterion [Dua00].

PPT criterion The PPT criterion works by transposing one of the modes in the covariance matrix of the bipartite system. If the new system after this transformation is physical, the system is separable, while it is inseparable if the partially transposed system is unphysical. The partial transposition of mode μ is described in terms of covariance matrices by

$$\gamma \to R_\mu \gamma R_\mu^T =: \gamma^{(T_\mu)} \qquad \mu = 1, 2\ , \tag{2.79}$$

where $R_1 = \mathrm{diag}(1, -1, 1, 1)$ and $R_2 = \mathrm{diag}(1, 1, 1, -1)$. The partial transposition therefore flips the Wigner function describing the respective subsystem at the P_μ axis. The physicality of $\gamma^{(T_\mu)}$ can be checked by the Heisenberg uncertainty relation from Eq. (2.72),

$$i\Omega\gamma^{(T_\mu)} \geq 1\ , \tag{2.80}$$

which is equivalent to computing the symplectic eigenvalues of $\gamma^{(T_\mu)}$ which have to be ≥ 1.

The PPT criterion is also applicable for systems with more than two modes. However, only for bipartite systems it is necessary and sufficient inseparability criterion.

Duan criterion The Duan criterion directly employs the correlations of amplitude quadrature measurements and the correlations of phase quadrature measurements at both subsystems. It reads

$$\mathrm{Var}\left(|a|\hat{X}_A + \frac{1}{a}\hat{X}_B\right) + \mathrm{Var}\left(|a|\hat{P}_A - \frac{1}{a}\hat{P}_B\right) \geq 2\left(a^2 + \frac{1}{a^2}\right) , \tag{2.81}$$

where we denoted the first subsystem by A and the second by B, and a is an arbitrary nonzero real number. A violation of this inequality certifies inseparability of the quantum state. To maximize the violation the optimal parameter a can be determined by minimizing the left hand side of Eq. (2.81) which yields

$$a = \pm\left(\frac{\mathrm{Var}(\hat{X}_B) + \mathrm{Var}(\hat{P}_B) - 2}{\mathrm{Var}(\hat{X}_A) + \mathrm{Var}(\hat{P}_A) - 2}\right)^{\frac{1}{4}} , \tag{2.82}$$

where the sign of a is determined by the sign of $\mathrm{Cov}(\hat{X}_A, \hat{X}_B)$. Here, Cov denotes the covariance. For symmetric states, i.e. for states with $\mathrm{Var}(\hat{X}_B) + \mathrm{Var}(\hat{P}_B) = \mathrm{Var}(\hat{X}_A) + \mathrm{Var}(\hat{P}_A)$, $a = \pm 1$ and Eq. (2.81) simplifies to

$$\mathrm{Var}\left(\hat{X}_A \pm \hat{X}_B\right) + \mathrm{Var}\left(\hat{P}_A \mp \hat{P}_B\right) \geq 4 . \tag{2.83}$$

Symmetric states are obtained when using a balanced beam splitter for entanglement generation and by having the same optical loss in both output arms of the beam splitter.

Note, that the Duan criterion is sufficient but not necessary for inseparability.

2.11.2 Einstein-Podolsky-Rosen Entanglement Criteria

In 1935 Einstein, Podolsky and Rosen formulated their famous Gedanken experiment [Ein35] which led Schrödinger in his reply introduce the notion of entanglement [Sch35]. EPR argued that quantum mechanics is not a complete theory. A theory is said to be complete if "every element of the physical reality [has] a counter part in the physical theory" [Ein35]. Their argument is based on the assumption of "local realism" which means that "if, without in any way disturbing a system, we can predict with certainty [...] the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity" [Ein35]. In their Gedankenexperiment EPR considered two spatially separated particles A and B, whose positions *and* momenta are maximally correlated. Measuring the position of particle A yields both particles to be in individual but correlated position eigenstates as the wave function collapses. Hence, the position of particle B can be predicted with certainty by the position measurement of particle A. The position of particle B therefore has physical reality. Otherwise, measuring the momentum of particle A yields both particles to be in individual but correlated momentum eigenstates. Thus, the momentum has physical reality and can be predicted with certainty. Since the physical reality of a quantity of particle B cannot depend on the choice of measurement at particle A due to the assumption of local realism, both quantities, position and momentum, must have physical reality. However, this leads to a contradiction in quantum mechanics as position and momentum operators do not commute and thus cannot have physical reality at the same time. This paradox was solved by EPR by dropping the assumption that quantum mechanics is a complete theory as they strongly believed in local realism. This was ruled out later by the violation of Bell inequalities [Bel64, Asp81], showing that the EPR paradox can only be solved by dropping the assumption of local realism. Using amplitude and phase quadrature measurements of light fields the EPR paradox was first demonstrated by Ou et al., in 1992 [Ou92]. The criterion they used was introduced by Reid in 1989 [Rei89] and will be discussed in the following.

Amplitude and phase quadratures of two-mode squeezed states are not maximally correlated as this can only be the case for infinite squeezing which can only be reached with infinite energy. Nevertheless, Reid showed that the EPR paradox can even be realized for less than maximum correlations. Using the quantum mechanical Cauchy-Schwarz inequality the correlation coefficient of the field quadratures $\hat{x}_\mu$ and $\hat{x}_\nu$ can be defined as [Rei89]

$$C(\hat{x}_\mu, \hat{x}_\nu) = \frac{\mathrm{Cov}(\hat{x}_\mu, \hat{x}_\nu)}{\sqrt{\mathrm{Var}(\hat{x}_\mu)\,\mathrm{Var}(\hat{x}_\nu)}} \ . \tag{2.84}$$

Perfect correlations, as for the position and momentum operators of the correlated particles, yield $|C(\hat{X}_A, \hat{X}_B)| = |C(\hat{P}_A, \hat{P}_B)| = 1$. As the field quadratures are not maximally correlated the prediction of a measurement outcome at subsystem B of the correlated system cannot be made with certainty after a measurement at subsystem A. The uncertainty of the inference can be quantified as

$$\Delta^2_{\mathrm{inf}}\hat{X}_B = \mathrm{Var}(\hat{X}_B - g\hat{X}_A) \tag{2.85}$$

for the amplitude quadrature and

$$\Delta^2_{\text{inf}}\hat{P}_B = \text{Var}(\hat{P}_B - h\hat{P}_A) \tag{2.86}$$

for the phase quadrature. g and h are thereby arbitrary scaling parameters that can be used to maximize the inference accuracy. By requiring $\frac{\partial \Delta^2_{\text{inf}}\hat{X}_B}{\partial g} = 0$ and $\frac{\partial \Delta^2_{\text{inf}}\hat{P}_B}{\partial h} = 0$ we obtain

$$g = \frac{\text{Cov}(\hat{X}_B, \hat{X}_A)}{\text{Var}(\hat{X}_A)} \tag{2.87}$$

and

$$h = \frac{\text{Cov}(\hat{P}_B, \hat{P}_A)}{\text{Var}(\hat{P}_A)} \tag{2.88}$$

which yields

$$\text{Var}_{B|A}(\hat{X}_A, \hat{X}_B) := \min_g \Delta^2_{\text{inf}}\hat{X}_B = \text{Var}(\hat{X}_B) - \frac{\text{Cov}(\hat{X}_B, \hat{X}_A)^2}{\text{Var}(\hat{X}_A)} \tag{2.89}$$

and

$$\text{Var}_{B|A}(\hat{P}_A, \hat{P}_B) := \min_h \Delta^2_{\text{inf}}\hat{P}_B = \text{Var}(\hat{P}_B) - \frac{\text{Cov}(\hat{P}_B, \hat{P}_A)^2}{\text{Var}(\hat{P}_A)} \ . \tag{2.90}$$

Thus, a measurement of $\hat{X}_A$ specifies a value of $\hat{X}_B$ with an uncertainty of at least $\text{Var}_{B|A}(\hat{X}_A, \hat{X}_B)$, and a measurement of $\hat{P}_A$ specifies a value of $\hat{P}_B$ with an uncertainty of at least $\text{Var}_{B|A}(\hat{P}_A, \hat{P}_B)$. EPR's concept of local realism leads to the conclusion that values for both $\hat{X}_B$ and $\hat{P}_B$ must have been predetermined with the uncertainties specified above as the physical reality of a quantity cannot depend on the choice of measurement at the spatially separated subsystem A. However, as amplitude and phase quadratures are non-commuting operators, the Heisenberg uncertainty relation from Eq. (2.10) requires

$$\text{Var}_{B|A}(\hat{X}_A, \hat{X}_B) \cdot \text{Var}_{B|A}(\hat{P}_A, \hat{P}_B) \geq 1 \ . \tag{2.91}$$

Thus, a demonstration of a violation of this inequality shows the EPR paradox. The inequality (2.91) shows a directional dependence as swapping the roles of subsystems A and B yields

$$\text{Var}_{A|B}(\hat{X}_A, \hat{X}_B) \cdot \text{Var}_{A|B}(\hat{P}_A, \hat{P}_B) \geq 1 \ . \tag{2.92}$$

The inequalities (2.91) and (2.92) do not have to be violated at the same time [Hae12] as violating one of those is sufficient to demonstrate the EPR paradox. Note, that the EPR paradox is also demonstrated if the Heisenberg uncertainty relation for the inferred variances, $\Delta^2_{\mathrm{inf}}\hat{X}_B \cdot \Delta^2_{\mathrm{inf}}\hat{P}_B \geq 1$, is violated with a non-optimal choice of the scaling parameters g and h.

Using the symplectic invariants from Section 2.10, the EPR criteria from Eqs. (2.91) and (2.92) can be expressed as [Fra12]

$$\mathrm{Var}_{B|A}(\hat{X}_A, \hat{X}_B) \cdot \mathrm{Var}_{B|A}(\hat{P}_A, \hat{P}_B) = \frac{I_4}{I_2} \ , \tag{2.93}$$

and

$$\mathrm{Var}_{A|B}(\hat{X}_A, \hat{X}_B) \cdot \mathrm{Var}_{A|B}(\hat{P}_A, \hat{P}_B) = \frac{I_4}{I_1} \ . \tag{2.94}$$

2.12 Von Neumann Entropy and Mutual Information

The von Neumann entropy of a quantum state $\hat{\rho}$ is defined as [Wil12]

$$H(\hat{\rho}) := -\operatorname{Tr}\left(\hat{\rho}\log_2\hat{\rho}\right) \ . \tag{2.95}$$

Assume that one party, called Alice, prepares quantum states $|\Psi_x\rangle$ with probability $p(x)$ and sends them to another party, called Bob. Bob does not know which quantum state was sent to him, but what he knows is that it will be $|\Psi_x\rangle$ with probability $p(x)$. The density operator of Alice's state as expected by Bob can then be written as $\hat{\rho} = \sum_x p(x)|\Psi_x\rangle\langle\Psi_x|$. The von Neumann entropy $H(\hat{\rho})$ quantifies the uncertainty of Bob's knowledge about Alice's state or in other words it quantifies the information Bob gains when he measures Alice's state.

The von Neumann entropy has the following properties:

- $H(\hat{\rho}) \geq 0$. $H(\hat{\rho}) = 0 \Leftrightarrow \hat{\rho}$ is a pure state.
- $H(\hat{\rho}) = H(\hat{U}\hat{\rho}\hat{U}^\dagger)$, where $\hat{U}$ is a unitary operator. Because a symplectic transformation can be written as a unitary transformation of the density matrix, the von Neumann entropy does not change under symplectic transformations.
- The von Neumann entropy is additive for tensor product states, i.e. $H(\hat{\rho}_1 \otimes \hat{\rho}_2) = H(\hat{\rho}_1) + H(\hat{\rho}_2)$.

- The von Neumann entropy is concave, i.e. $H\left(\sum_x p(x)\hat{\rho}_x\right) \geq \sum_x p(x)H(\hat{\rho}_x)$. The concavity property means that the entropy increases when mixing states.

In the following we assume a bipartite system with parties A and B. We denote the density operator of the whole system as $\hat{\rho}_{AB}$ and the density operators of the subsystems as $\hat{\rho}_A = \mathrm{Tr}_B\, \hat{\rho}_{AB}$ and $\hat{\rho}_B = \mathrm{Tr}_A\, \hat{\rho}_{AB}$ with the partial traces Tr_A and Tr_B taken over the respective subsystem.

The *joint entropy* of the state is then given by

$$H(AB) := H(\hat{\rho}_{AB}) = -\operatorname{Tr}\left(\hat{\rho}_{AB} \log_2 \hat{\rho}_{AB}\right) \tag{2.96}$$

and the *marginal entropies* by

$$H(A) := H(\hat{\rho}_A) = -\operatorname{Tr}\left(\hat{\rho}_A \log_2 \hat{\rho}_A\right) \tag{2.97}$$

and

$$H(B) := H(\hat{\rho}_B) = -\operatorname{Tr}\left(\hat{\rho}_B \log_2 \hat{\rho}_B\right)\ . \tag{2.98}$$

If $\hat{\rho}_{AB}$ is a pure state, the marginal entropies are equal, $H(A) = H(B)$, which is also true for multipartited systems, e.g. if $\hat{\rho}_{ABE}$ is pure, $H(AB) = H(E)$. This property is called the self-duality property of the von Neumann entropy.

The conditional entropy is given by

$$H(A|B) := H(AB) - H(B)\ . \tag{2.99}$$

$H(A|B)$ can be smaller than zero, as for entangled states the uncertainty of the whole system is smaller than for any subsystem, i.e. $H(AB) < H(A)$. This can be seen for the two-mode squeezed state from Eq. (2.62). $H(AB) = 0$ as the state is pure, but $H(B) = H(A) > 0$ as the local subsystems are thermal states. After introducing the mutual information, we will see how to calculate the entropy of arbitrary Gaussian states.

The *mutual information* quantifies the amount of information, measured in bits, which both subsystems share. It is given by

$$\begin{aligned} I(A:B) &:= H(A) + H(B) - H(AB) && (2.100)\\ &= H(A) - H(A|B) && (2.101)\\ &= H(B) - H(B|A)\ . && (2.102) \end{aligned}$$

Hence, the mutual information quantifies also how much the knowledge about a subsystem, e.g. about subsystem B, reduces the uncertainty $H(A)$ about the other subsystem.

In the following we will calculate the von Neumann entropy of an arbitrary N-mode Gaussian state with covariance matrix γ [Ser04]. The Williamson form of γ is given by

$$S\gamma S^T = \otimes_{i=1}^{N} s_i \mathbb{1}_2$$

by means of a symplectic transformation S. s_i are the symplectic eigenvalues of γ. As a symplectic transformation of a covariance matrix can be written as a unitary transformation of the corresponding density matrix, the von Neumann entropy of the state does not change. Hence, using the additivity property of the von Neumann entropy for tensor product states, we can write

$$H(\gamma) = \sum_{i=1}^{N} H(s_i \mathbb{1}_2) \ , \tag{2.103}$$

which reduces the calculation of the entropy to the entropy of thermal states with mean photon number $\overline{n}_i = \frac{1}{2}(s_i - 1)$.

The density operator of a thermal state with mean photon number $\overline{n}$ is given by [Bar97]

$$\hat{\rho}_{th} = \sum_{n=0}^{\infty} \frac{\overline{n}^n}{(\overline{n}+1)^{n+1}} |n\rangle\langle n| \ , \tag{2.104}$$

cf. Eq. (2.51). Plugging this into the von Neumann entropy from Eq. (2.95) yields

$$H(\hat{\rho}_{th}) = -\frac{1}{1+\overline{n}} \sum_{n=0}^{\infty} \left(\frac{\overline{n}}{1+\overline{n}}\right)^n \log_2 \frac{\overline{n}^n}{(1+\overline{n})^{n+1}} \tag{2.105}$$

$$= \frac{1}{1+\overline{n}} \left(-\sum_{n=0}^{\infty} \left(\frac{\overline{n}}{1+\overline{n}}\right)^n n \log_2 \overline{n} + \sum_{n=0}^{\infty} \left(\frac{\overline{n}}{1+\overline{n}}\right)^n (n+1) \log_2 (1+\overline{n}) \right) \ . \tag{2.106}$$

Using the geometric series $\sum_{n=0}^{\infty} \left(\frac{\overline{n}}{1+\overline{n}}\right)^n = 1 + \overline{n}$ and $\sum_{n=0}^{\infty} \left(\frac{\overline{n}}{1+\overline{n}}\right)^n n = \overline{n}(1+\overline{n})$ simplifies $H(\hat{\rho}_{th})$ to

$$H(\hat{\rho}_{th}) = \overline{n} \log_2 \frac{1+\overline{n}}{\overline{n}} + \log_2(1+\overline{n}) \ . \tag{2.107}$$

In terms of symplectic eigenvalues this is transformed into

$$H(\hat{\rho}_{th}) = H(s_i \mathbb{1}_2) = f(s_i) \ , \tag{2.108}$$

with

$$f(s) = \frac{s+1}{2}\log_2\left(\frac{s+1}{2}\right) - \frac{s-1}{2}\log_2\left(\frac{s-1}{2}\right) \ . \tag{2.109}$$

Hence, for an N-mode Gaussian state with symplectic eigenvalues s_i the von Neumann entropy can be calculated by

$$H(\gamma) = \sum_{i=1}^{N} f(s_i) \ . \tag{2.110}$$

Using this result all quantities given in this section can be calculated for Gaussian states.

2.13 Partial Homodyne Measurement on a Bipartite Gaussian State

Quadrature measurements can be performed by homodyne detection as we will see in Chapter 3.4. We will now assume the situation where we perform a measurement on subsystem B of a bipartite Gaussian system and we are interested in the state of subsystem A after the measurement. We write the covariance matrix γ of the bipartite state in block form as in Eq. (2.73). Performing a measurement in the X quadrature on subsystem B leaves the subsystem A in the state [Wee12]

$$\gamma'_A = A - C(M_X B M_X)^{\mathrm{MP}} C^T \ , \tag{2.111}$$

while performing a P quadrature measurement leaves A in the state

$$\gamma'_A = A - C(M_P B M_P)^{\mathrm{MP}} C^T \ . \tag{2.112}$$

Here, $M_X = \mathrm{diag}(1,0)$ and $M_P = \mathrm{diag}(0,1)$. MP denotes the Moore-Penrose pseudo-inverse since $M_{\{X,P\}} B M_{\{X,P\}}$ are singular. The pseudo-inverse can be evaluated by $(M_X B M_X)^{\mathrm{MP}} = B_{11}^{-1} M_X$ and $(M_P B M_{PX})^{\mathrm{MP}} = B_{22}^{-1} M_P$, where B is written as $B = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}$.

We will use this result later in Chapter 5 to calculate the key rates for quantum key distribution.

CHAPTER 3

Experimental Techniques

Overview

In this chapter the experimental techniques used in this thesis are introduced. Section 3.1 describes the preparation of the main laser beam and its source. Section 3.2 introduces the second-harmonic generation which generated the pump beam for the squeezed-light source, which is described in Section 3.3. Balanced homodyne detection was used for measurements of the field quadratures and is described in Section 3.4. The reconstruction process of a state's covariance matrix is introduced in Section 3.5. Section 3.6 describes the data acquisition process used to obtain digitized samples from the output of the balanced homodyne detection, and Section 3.7 gives an insight in how lowpass filters, which were used for the preparation of signals for data acquisition, introduce correlations between samples.

3.1 Coherent Light Preparation

The main light source of the experiments described in the following chapters, was a 1 W fiber laser at a wavelength of 1550 nm from NKTPhotonics. Figure 3.1 shows the light preparation, which the beam had passed before it was used for these experiments. The laser beam from the source was coupled out of a polarization-maintaining fiber which had a mode-field diameter of 10.5 µm. The beam was collimated using an aspheric lens. For spatial mode and noise filtering as well as for being a beam reference for the downstream experiment, the beam was fed through an impedance matched three-mirror travelling-wave ring cavity, called *mode cleaner* (MC), which had a finesse of about 300. To keep the cavity on resonance a Pound-Drever-Hall (PDH) scheme [Bla01] was used to generate an error signal for a control loop [Abr00] which actuated the position

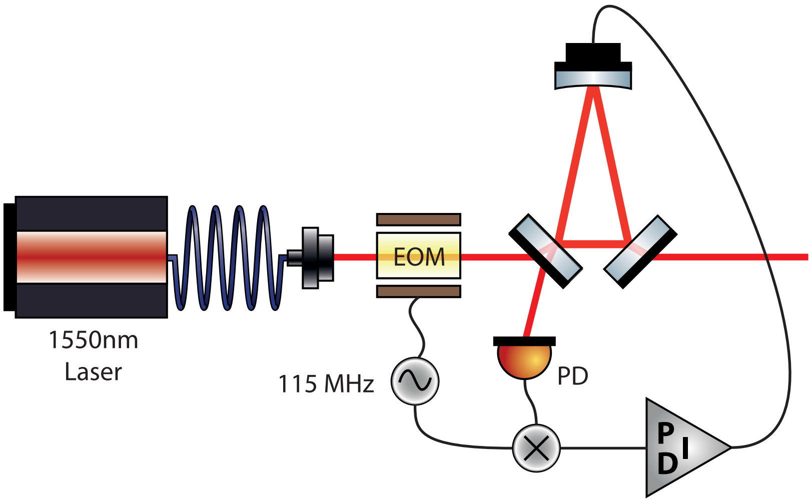


Figure 3.1: Coherent light preparation. The light from a 1550 nm fiber laser is coupled out of the fiber. The free beam passes a mode cleaning ring cavity which is locked using a Pound-Drever-Hall scheme. EOM: electro-optical modulator, PD: photo detector.

of one of the cavity's mirrors with a piezo-electric transducer. The PDH scheme employed phase modulation sidebands at 115 MHz which were imprinted on the laser beam by an electro-optical modulator (EOM). The reflected light from the cavity was detected by a resonant photo detector whose photo current was demodulated at 115 MHz and lowpass filtered. The electronic sinusoidal signal used for the generation of the phase modulation and for the demodulation of the photo current was served by a computer programmable AD9959 digital synthesizer.

3.2 Pump Beam Preparation for Parametric Down-Conversion

Figure 3.2 shows the generation of the 775 nm pump beam for the parametric squeezed-light sources described in the next Section. We used parametric up-conversion in a periodically poled potassium titanyl phosphate (PPKTP) crystal for the generation of the second harmonic of the fundamental beam at 1550 nm. To enhance the conversion efficiency from 1550 nm to 775 nm the crystal with a length of 9.3 mm was placed in a standing-wave cavity formed by the curved end-face of the crystal which was coated high-reflective for both wavelengths, and an external coupling mirror with a reflectivity of about 90 % for the fundamental and a small residual reflectivity for the harmonic. The curved end-face of the crystal had a radius of curvature of 12 mm and the coupling mirror had a radius of curvature of 25 mm. The plane end-face of the crystal

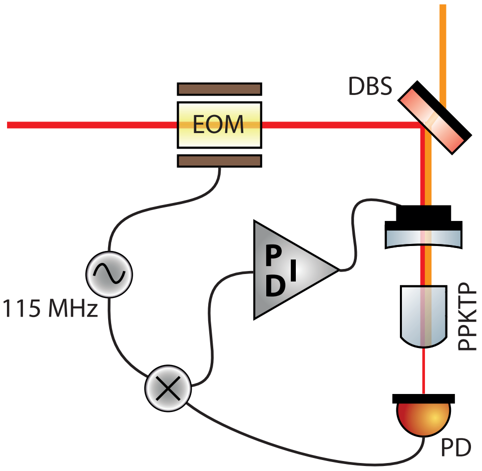


Figure 3.2: Second harmonic generation using parametric up-conversion in PPKTP. The linear cavity is locked to the fundamental beam using a Pound-Drever-Hall scheme. The generated harmonic beam at 775 nm is separated from the fundamental by a dichroic beam splitter. EOM: electro-optical modulator, PD: photo detector, DBS: dichroic beam splitter.

was coated anti-reflective for both wavelengths. To reach phase-matching the crystal was covered by a copper housing whose temperature could be actuated by a Peltier element. For thermal isolation the copper housing was encased by polyoxylmethylene (POM). A resistor with negative temperature coefficient served as temperature sensor and was used together with a servo controller and the Peltier element to keep the crystal at a constant temperature. The cavity was kept on resonance by a control loop which employed the same PDH scheme as described above. For the second-harmonic generation the phase modulation sidebands were also at 115 MHz. The generated 775 nm beam was separated from the fundamental field by a dichroic beam splitter (DBS).

Using the same scheme and the same wavelengths a conversion efficiency of about 95 % was reported in [Ast11]. Due to a lower fundamental light power the conversion efficiency of the second-harmonic generation used in this thesis was about 85 %.

3.3 Squeezed-Light Generation

Figure 3.3 shows the experimental setup for squeezed-light generation. Squeezed vacuum states are generated by degenerate parametric down-conversion [Ger05] which was implemented using PPKTP as nonlinear medium like for the second-harmonic generation. Hence, the mechanical implementation of the squeezed-light source was the same as described in Section 3.2, except for the reflectivity of the coupling mirror which was 90 % for 1550 nm and 20 % for 775 nm. To lock the cavity on resonance

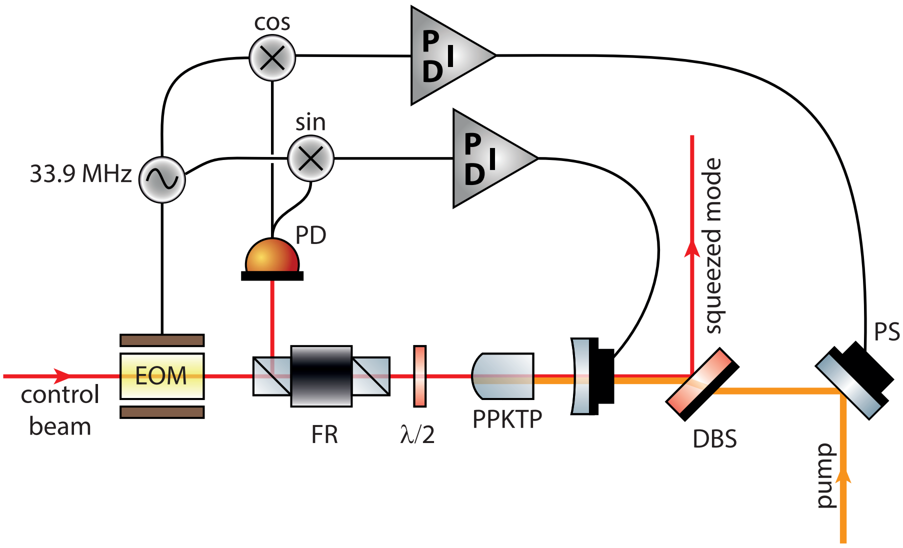


Figure 3.3: Squeezed-light generation using degenerate type I parametric down-conversion in PPKTP in a linear standing-wave cavity. The cavity length is locked using a control beam with phase modulation sidebands coupled into the cavity from the left. The back reflected light is separated from the incoming light with a Faraday rotator and a polarizing beam splitter and detected by a resonant photo detector. The pump field is coupled into the cavity from the right. Its phase is locked using an error signal generated by demodulating the photo detector's output out-of-phase to the demodulation of the output for the cavity length error signal. The squeezed beam is separated from the pump by a dichroic beam splitter. EOM: electro-optical modulator, FR: Faraday rotator, PD: photo detector, DBS: dichroic beam splitter, PS: phase shifter.

we employed a control beam with a power of about 800 μW which was coupled into the cavity through the high-reflective mirror. The back reflected light was separated from the incoming light by a Faraday rotator and a polarizing beam splitter and was detected by a resonant photo detector. Phase modulation sidebands at 33.9 MHz imprinted on the control beam were used to generate an error signal for the length of the cavity. The pump beam at 775 nm was coupled into the cavity from the partial reflective side. The phase of the pump with respect to the control beam was locked using an error signal generated by demodulating the photo detector's output. For this purpose the electronic local oscillator for the demodulation was shifted by 90° in phase to the electronic local oscillator used for the generation of the error signal for the cavity length. In the figure this is indicated by `cos` and `sin` next to the demodulation symbol. The phase of the pump was actuated by a mirror attached to a piezo and controlled to a phase angle which yielded deamplification of the control beam. The squeezed beam was separated from the pump by a dichroic beam splitter. To generate squeezed vacuum states with this setup the control beam had to be shot-noise limited

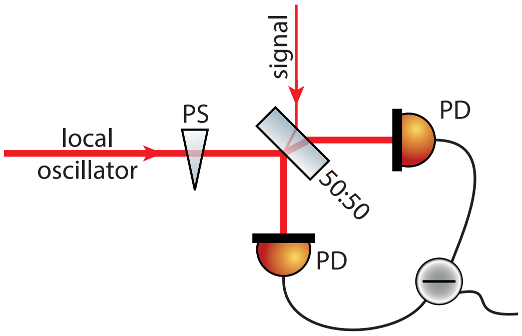


Figure 3.4: Principle of balanced homodyne detection. A strong optical local oscillator was superimposed with the signal field at a balanced beam splitter. Both output beams were detected by photo diodes whose photo currents were subtracted. The phase of the local oscillator field with respect to the signal field defined the measured quadrature angle and could be actuated by a phase shifter. PS: phase shifter, PD: photo detector.

in the frequency band of the measurement. This requirement limited the power that could be used for the control beam as well as the lower end of the measured frequency band because the control beam was only shot-noise limited above about 7 MHz for the power we used. Indeed we were not able to use less power in the control beam as the locks for the cavity length and the pump phase got unstable otherwise. The demodulation of the photo detector's signal with two electronic local oscillators which were 90° out of phase, was implemented on a single printed circuit board. The schematic of this electronic circuit is shown in Appendix A, Fig. A.1.

3.4 Balanced Homodyne Detection

The measurement of the field quadratures was performed by balanced homodyne detection. The experimental setup for balanced homodyne detection is depicted in Fig. 3.4. A bright local oscillator beam was superimposed with the signal field at a balanced beam splitter. Both output beams were detected by photo diodes whose photo currents were subtracted. The phase of the local oscillator beam thereby defined the measured quadrature angle and could be actuated by a mirror attached to a piezo.

Let us denote the mode of the local oscillator by $\hat{b}$ and the mode of the signal field by $\hat{a}$. The phase between these modes is denoted by φ. According to Eq. (2.2) we can write the operators in vectorial form

$$\hat{\boldsymbol{x}} = (\hat{b}e^{i\varphi}, \hat{b}^\dagger e^{-i\varphi}, \hat{a}, \hat{a}^\dagger)^T \ .$$

Applying the symplectic form $S_{\mathrm{BS}}(\tau)$ from Eq. (2.60) with $\tau = 0.5$ yields

$$S_{\mathrm{BS}}(0.5)\hat{\boldsymbol{x}} = \begin{pmatrix} \frac{1}{\sqrt{2}}\left(\hat{b}e^{i\varphi} + \hat{a}\right) \\ \frac{1}{\sqrt{2}}\left(\hat{b}^\dagger e^{-i\varphi} + \hat{a}^\dagger\right) \\ \frac{1}{\sqrt{2}}\left(-\hat{b}e^{i\varphi} + \hat{a}\right) \\ \frac{1}{\sqrt{2}}\left(-\hat{b}^\dagger e^{-i\varphi} + \hat{a}^\dagger\right) \end{pmatrix} . \tag{3.1}$$

The photo current of each photo diode is proportional to the number of detected photons. Thus,

$$\hat{i}_1 \propto \frac{1}{2}\left(\hat{b}^\dagger e^{-i\varphi} + \hat{a}^\dagger\right)\left(\hat{b}e^{i\varphi} + \hat{a}\right) \tag{3.2}$$

$$= \frac{1}{2}\left(\hat{b}^\dagger\hat{b} + \hat{b}^\dagger\hat{a}e^{-i\varphi} + \hat{a}^\dagger\hat{b}e^{i\varphi} + \hat{a}^\dagger\hat{a}\right) \tag{3.3}$$

$$= \frac{1}{2}\left(\hat{b}^\dagger\hat{b} + (\hat{a}^\dagger\hat{b}e^{i\varphi})^\dagger + \hat{a}^\dagger\hat{b}e^{i\varphi} + \hat{a}^\dagger\hat{a}\right) \tag{3.4}$$

and

$$\hat{i}_2 \propto \frac{1}{2}\left(-\hat{b}^\dagger e^{-i\varphi} + \hat{a}^\dagger\right)\left(-\hat{b}e^{i\varphi} + \hat{a}\right) \tag{3.5}$$

$$= \frac{1}{2}\left(\hat{b}^\dagger\hat{b} - (\hat{a}^\dagger\hat{b}e^{i\varphi})^\dagger - \hat{a}^\dagger\hat{b}e^{i\varphi} + \hat{a}^\dagger\hat{a}\right) . \tag{3.6}$$

By subtracting the photo currents we obtain

$$\hat{i}_1 - \hat{i}_2 \propto (\hat{a}^\dagger\hat{b}e^{i\varphi})^\dagger + \hat{a}^\dagger\hat{b}e^{i\varphi} , \tag{3.7}$$

where we assumed that the photo diodes have the same gain and, hence, the proportionality factor is the same. We now rewrite both modes by $\hat{a} = |\alpha| + \delta\hat{\alpha}$ and $\hat{b} = |\beta| + \delta\hat{\beta}$ Here, $|\alpha|$ and $|\beta|$ describe a coherent excitation of the field and $\delta\hat{\alpha}$ and $\delta\hat{\beta}$ are the noise contributions. We assume $\delta\hat{\alpha}$ and $\delta\hat{\beta}$ to be small und thus take only first order noise terms into account. With this linearization of the modes, Eq. (3.7) can be written as

$$\hat{i}_1 - \hat{i}_2 \propto 2|\beta||\alpha|\cos\varphi + |\beta|\left(\delta\hat{\alpha}^\dagger e^{i\varphi} + \delta\hat{\alpha}e^{-i\varphi}\right) + |\alpha|\left(\delta\hat{\beta}^\dagger e^{-i\varphi} + \delta\hat{\beta}e^{i\varphi}\right) . \tag{3.8}$$

Generalizing the definition of the quadrature operators from Eq. (2.6) and (2.7) to an arbitrary angle φ,

$$\hat{X}_{\hat{a}_k}(\varphi) := \hat{a}_k e^{-i\varphi} + \hat{a}_k^\dagger e^{i\varphi} , \tag{3.9}$$

where the X quadrature operator from Eq. (2.6) is reproduced with $\varphi = 0$ and the

P quadrature operator from Eq. (2.7) is reproduced with $\varphi = \frac{\pi}{2}$, the equation of the subtracted photo currents takes the form

$$\hat{i}_1 - \hat{i}_2 \propto 2|\beta||\alpha| \cos\varphi + |\beta|\hat{X}_{\delta\hat{a}}(\varphi) + |\alpha|\hat{X}_{\delta\hat{b}}(\varphi) \ . \tag{3.10}$$

To measure only $\hat{X}_{\delta\hat{a}}(\varphi)$ the local oscillator power $|\beta|$ has to be much larger than $|\alpha|$. Indeed for squeezed vacuum states $|\alpha| = 0$. As described in Section 3.3 we use a control beam for locking purposes of the squeezed-light source, thus, $|\alpha| \neq 0$, and the requirement $|\beta| \gg |\alpha|$ has to hold. The first term of Eq. (3.10) describes the beat between the local oscillator and the control beam and can be used as an error signal for a lock of the local oscillator's phase to $\frac{\pi}{2}$, i.e. to the phase quadrature. Arbitrary quadratures can be measured by locking the local oscillator's phase to an appropriate value using other techniques [DiG07, Ebe13b].

3.5 Tomographic Reconstruction of the Covariance Matrix

For the characterization of our generated state we reconstructed the full covariance matrix according to a protocol presented and experimentally demonstrated in [DiG07]. Assuming the two modes of a bipartite states are possessed by Alice and Bob, the protocol works as follows:

1. Alice and Bob both measure simultaneously the amplitude quadrature.
2. Alice and Bob both measure simultaneously the phase quadrature.
3. Alice measures the amplitude quadrature, whereas Bob simultaneously measures the phase quadrature.
4. Alice measures the phase quadrature, whereas Bob simultaneously measures the amplitude quadrature.
5. Alice and Bob both measure a linear combination of the amplitude and phase quadrature. In our case we chose the 45° angle for both parties.

Including a vacuum noise measurement for reference, the covariance matrix can be reconstructed using the measurements given above by

$$\gamma = \begin{pmatrix} \langle \hat{X}_A^2 \rangle & \frac{1}{2}\langle \hat{X}_A\hat{P}_A + \hat{P}_A\hat{X}_A \rangle & \langle \hat{X}_A\hat{X}_B \rangle & \langle \hat{X}_A\hat{P}_B \rangle \\ & \langle \hat{P}_A^2 \rangle & \langle \hat{P}_A\hat{X}_B \rangle & \langle \hat{P}_A\hat{P}_B \rangle \\ & & \langle \hat{X}_B^2 \rangle & \frac{1}{2}\langle \hat{X}_B\hat{P}_B + \hat{P}_B\hat{X}_B \rangle \\ & & & \langle \hat{P}_B^2 \rangle \end{pmatrix} . \tag{3.11}$$

Here, we omitted the lower part of the covariance matrix for readability as the matrix is symmetric. $\frac{1}{2}\langle\hat{X}\hat{P}+\hat{P}\hat{X}\rangle$ can be calculated by

$$\frac{1}{2}\langle\hat{X}\hat{P}+\hat{P}\hat{X}\rangle = \langle\hat{X}(45^\circ)^2\rangle - \frac{1}{2}\left(\langle\hat{X}^2\rangle + \langle\hat{P}^2\rangle\right) \tag{3.12}$$

using the 45° measurement. This can be seen by using the definition of the quadrature operators $\hat{X}$ and $\hat{P}$ given in Eqs. (2.6) and (2.7) and the definition of the generalized quadrature operator in Eq. (3.9). A detailed calculation can be found for instance in [Sam12].

3.6 Data Acquisition

While the measurement of noise variances can be performed by using a spectrum analyzer, for quantum cryptography we are interested in the correlated homodyne signals between Alice and Bob in the time domain. For this purpose we used an analog-to-digital converter (ADC) that converts the analog output signal of the homodyne detector's electronics into a time series of samples.

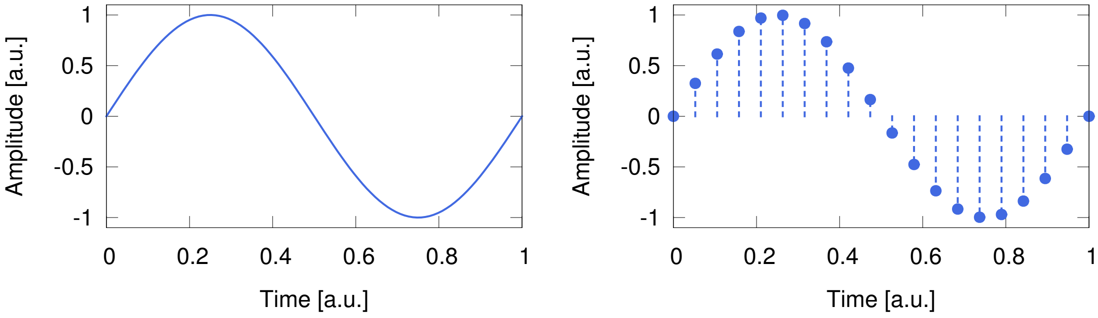
Let us assume that the signal we would like to digitize is of the form

$$x(t) = \sin(2\pi f_0 t)\ .$$

An analog-to-digital converter which samples this signal with frequency f_s, converts this into

$$x(n) = \sin(2\pi f_0 n/f_s)\ ,$$

where n is the sample number. This situation is displayed in Fig. 3.5. f_s is called the *sampling frequency* and is usually given in samples per second. Sampling at a certain



(a) continuous time signal **(b)** discrete time signal

Figure 3.5: Sampling of a continuous time signal.

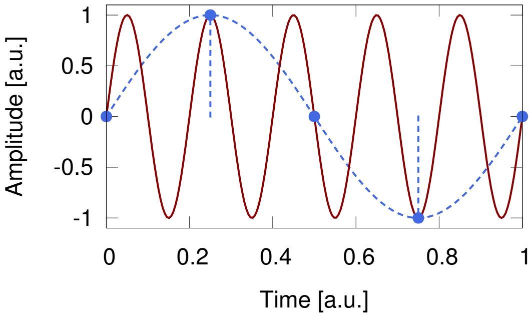


Figure 3.6: Ambiguity of the sampled values when sampling with $f_s = 4f_0$. Blue: $\sin(f_0)$, red: $\sin(5f_0)$.

rate might lead to ambiguities in the frequency domain as shown in Fig. 3.6, where we sampled the continuous time signal from above with a sampling frequency of $f_s = 4f_0$. Sampling a sinusoidal signal with frequency $5f_0$ with the same sampling frequency would lead to exactly the same samples. Indeed, while sampling with frequency f_s we cannot distinguish between signals of frequency f_0 and signals of frequency $f_0 + kf_s$ for any integer k [Lyo04]. Thus, the signal at $5f_0$ in the example is *aliased* to a signal at f_0. The aliasing effect in frequency domain is depicted in Fig. 3.7a. From 0 to $\frac{f_s}{2}$ the digital frequency is the same as the physical frequency. Higher physical frequencies are aliased into the digital frequency band from 0 to $\frac{f_s}{2}$, where $\frac{f_s}{2}$ is called the *Nyquist* frequency. However, not only the frequency of signals with frequencies larger than the Nyquist frequency changes after digitalization, the phase of these signals also changes [Smi03]. This is shown in Fig. 3.7b. For frequencies between $\frac{f_s}{2}$ and f_s the phase of the sampled signal is shifted by $\frac{\pi}{2}$.

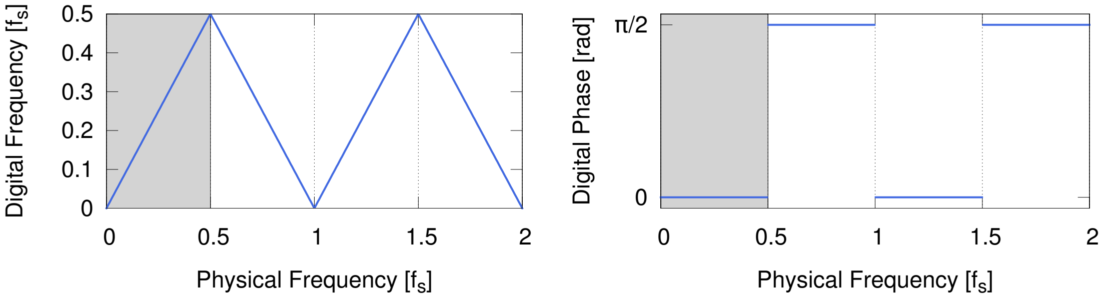
The resolution of an ADC is given by the number of bins the range of the converter is divided into. Using a pre-amplifier the range of the signal can usually be adjusted to fit well within the ADC range. The ADCs used throughout this thesis both have a resolution of $n = 14\,\text{bits}$, yielding $2^n = 16384$ different conversion outcomes. The resolution voltage, i.e. the voltage span of a single bin, is given for an n bit ADC by

$$V_{\text{res}} = \frac{V_{\text{max}} - V_{\text{min}}}{2^n} \ ,$$

where $V_{\text{max}} - V_{\text{min}}$ is the voltage range of the ADC. Assuming a symmetric voltage swing around zero, i.e. $V_{\text{max}} = -V_{\text{min}}$, we obtain

$$V_{\text{res}} = \frac{V_{\text{max}}}{2^{n-1}} \ .$$

To avoid aliasing the amplitude of a sinusoidal signal at a frequency larger than $\frac{f_s}{2}$



(a) Frequency changes due to aliasing **(b)** Phase changes due to aliasing

Figure 3.7: Frequency and phase of sampled signals versus their physical frequency before sampling. The grey shaded area illustrates where the sampled signals correspond to the physical ones, while the white area illustrates where signal frequencies are aliased to the digital frequency band.

needs to be attenuated by a lowpass filter to have an amplitude smaller than the resolution voltage. The maximum possible amplitude of a signal that is within the signal range and therefore does not saturate the ADC, is V_{max}. Hence, the amplitude of such a signal has to be attenuated by

$$20 \cdot \log_{10} \frac{V_{\mathrm{max}}}{V_{\mathrm{res}}} = 20 \cdot \log_{10}(2^{n-1}) \approx 6(n-1)[\mathrm{dB}] \ .$$

Thus, for our 14 bit ADCs the attenuation of a lowpass filter has to be at least 78 dB at the Nyquist frequency. In practice smaller attenuation values than the one calculated above might be sufficient, depending on the signal range compared to the range of the ADC, the frequency content of the analog signal and the noise of the ADC. Lowpass filters are discussed in detail in Section 3.7.

Usually, we are only interested in a measurement of signals within a certain frequency band. As we already discussed in Section 3.3 the control beam used to lock the squeezed-light source is only shot-noise limited above 7 MHz. Hence, only measurements at Fourier frequencies above 7 MHz are not deteriorated by additional excess noise. To achieve such a measurement two different methods were implemented within this thesis depending on the properties of the used ADC. The first one is depicted in Fig. 3.8 and uses a slow ADC with a sampling frequency of $f_s = 500\,\mathrm{kHz}$. To map the desired measurement frequency band to the frequency band of the ADC, the output of the homodyne detector's circuit was demodulated at the measurement frequency, e.g. 8 MHz, using a double-balanced mixer. Subsequently the output of the double-balanced mixer was lowpass filtered to achieve the necessary attenuation of frequencies above the Nyquist frequency of the sampling process. Thus, the bandwidth

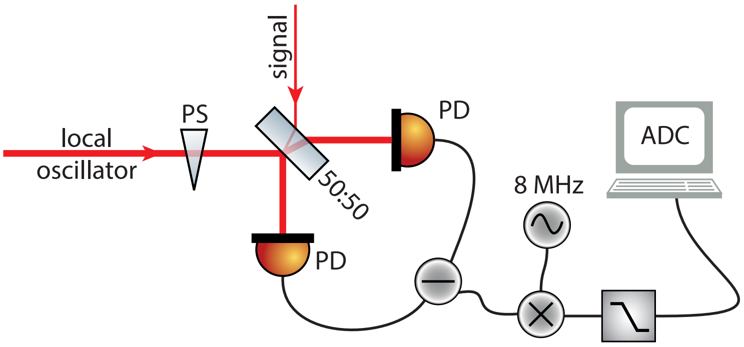


Figure 3.8: Data acquisition of the homodyne detector's output using a slow ADC. The output signal of the homodyne detector is electronically demodulated at a frequency of 8 MHz and lowpass filtered before it is sampled by the ADC. PS: phase shifter, PD: photo detector, ADC: analog-to-digital converter.

of the measurement was determined by the -3 dB cutoff frequency of the lowpass filter.

The second method used a fast ADC with a sampling frequency of 256 MHz. This setup is shown in Fig. 3.9. The output of the homodyne detector's circuit was lowpass filtered to attenuate frequencies above the Nyquist frequency of 128 MHz and sampled by the fast ADC. After sampling, the samples were digitally mixed with a sinusoid at, for instance, 8 MHz and lowpass filtered with a digital finite impulse response filter (FIR filter). Such filters are described in Section 3.7. Afterwards the samples were down-sampled to a lower sampling frequency. Here, the FIR filter had to be designed such that it sufficiently attenuates frequencies above the new Nyquist frequency. Due to the digital mixing process the resolution of the post processed samples is larger

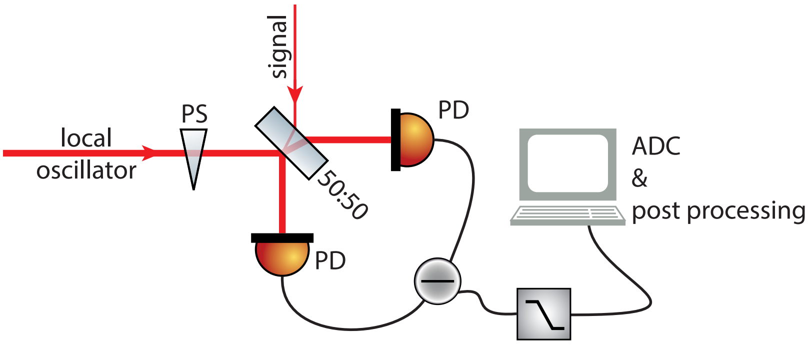


Figure 3.9: Data acquisition of the homodyne detector's output using a fast ADC. The output signal of the homodyne detector is lowpass filtered and sampled with a high sampling frequency of, for instance, 256 MHz. The demodulation is performed digitally in a post processing step. PS: phase shifter, PD: photo detector, ADC: analog-to-digital converter.

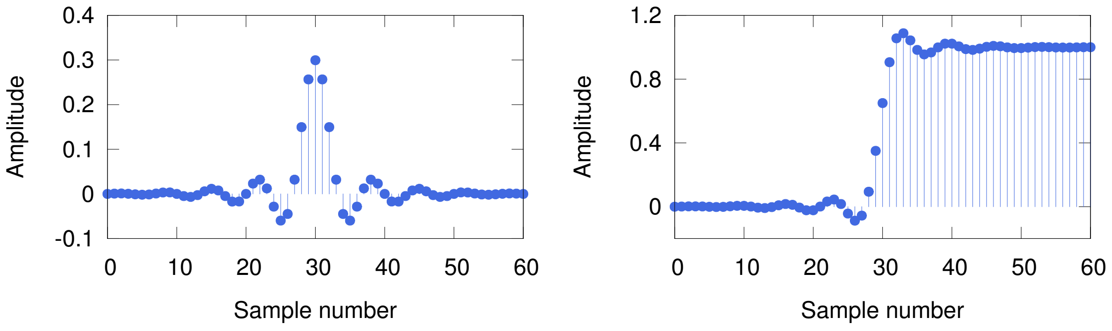
than the resolution of the ADC.

The advantage of the second method in comparison to the first is that less analog electronic components are needed. In particular when sampling more than one channel, analog filters have the disadvantage that the frequency responses of two copies is never exactly the same. Furthermore a higher bandwidth of the demodulated signal is easier to achieve with the second method. On the contrary the digital post processing needed for the second method is quite demanding concerning computing power. For the quantum cryptography experiment described in Chapter 5, the second method is a necessary ingredient as the lowpass filter for anti-aliasing purposes of the first, has a cutoff frequency below the frequency of the measurement intervals.

3.7 Filters and Sample Correlations

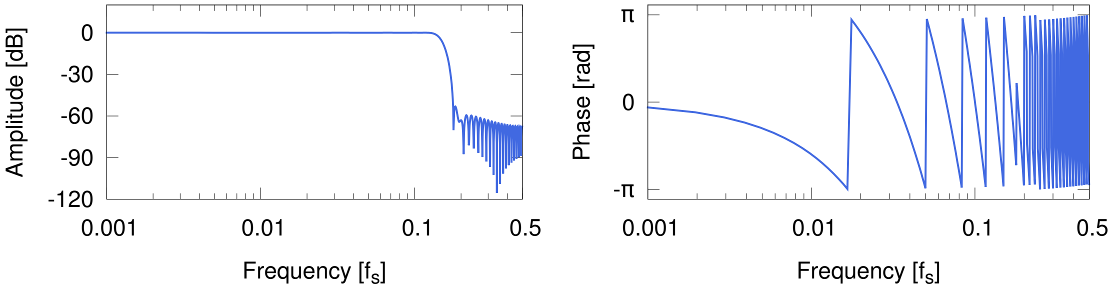
As we have seen in the last section, (lowpass) filters are unavoidable for data acquisition. In this section we briefly introduce the response functions of analog and digital filters and how the filters correlate formerly uncorrelated signals or samples. A more detailed introduction to digital filters can be found for instance in [Lyo04] and [Smi03].

The response of a filter can be described equivalently by its impulse, step and frequency response. Figure 3.10a shows the impulse response of an exemplary digital finite impulse response filter. The impulse response is the output of a filter on an input signal that describes a short impulse, i.e. an input signal that is zero except for one sample. After filtering the impulse is broadened and shows ringing. By integrating the impulse response we obtain the step response which is shown in Fig. 3.10b. The step response is the response of a filter to a sharp step in the input signal. The figure shows that the slope of the step decreased after filtering and that the output signal shows overshoot and ringing. By calculating the Fourier transform of the impulse response



(a) Impulse response **(b)** Step response

Figure 3.10: Impulse and step response of an exemplary finite impulse response filter.



(a) Magnitude **(b)** Phase

Figure 3.11: Frequency response of an exemplary finite impulse response filter.

the frequency response of the filter as depicted in Fig. 3.11 is obtained. The frequency response is displayed as a Bode plot expressing both the magnitude and phase of the filter versus frequency. Here, the frequency axis is plotted in units of the sampling frequency.

From the frequency response we can calculate the autocorrelation function of the filter. The autocorrelation function of a continuous function in time $f(t)$ is defined as

$$\mathrm{Autocorr}(\tau) = \int_{-\infty}^{\infty} \mathrm{d}t f(t) f^*(t-\tau) \ , \tag{3.13}$$

where $f^*(t)$ is the complex conjugate of $f(t)$. It can easily be computed using the Fourier transform $\mathcal{F}$

$$\mathrm{Autocorr}(\tau) = \mathcal{F}^{-1}\left[|\mathcal{F}(f)|^2\right] \ , \tag{3.14}$$

which also works for sampled data using the *Fast Fourier Transform* algorithm. The autocorrelation function of sampled data describes the amount of correlation between one sample and its neighbours. The autocorrelation of our exemplary finite impulse response filter is shown in Fig. 3.12. From this figure we see that formerly uncorrelated samples that are filtered with a lowpass filter, get correlated as the autocorrelation is not zero for lags between 1 and about 15. In fact this is always true for any non-uniform frequency response. Measuring for instance a vacuum state with a homodyne detector and sampling the output of the detector with the data acquisition method that uses an analog mixer and a lowpass filter for anti-aliasing purposes, yields correlated samples despite the fact that vacuum state measurements are uncorrelated in time. This has to be taken into account for the quantum key distribution experiment, cf. Chapter 5, where samples obtained from subsequent measurements are not allowed to be correlated. While the filter used in the example above has an autocorrelation which

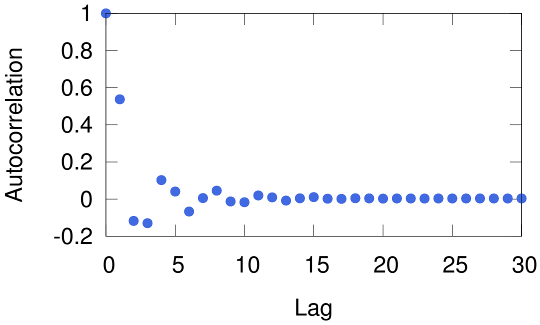


Figure 3.12: Autocorrelation function of an exemplary finite impulse response filter.

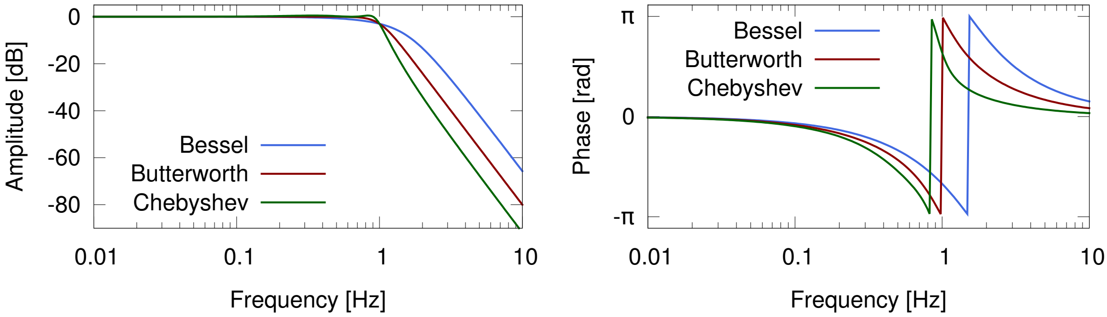
shows ringing, a filter with linear phase in the passband like a Bessel type filter, does not, and therefore reduces the number of correlated samples. Reducing the order of the filter as much as possible also reduces the number of correlated samples.

3.7.1 Analog Filters

Analog filters are implemented using resistors, capacitors and coils, and for active designs also include operational amplifiers. Specific topologies of implementations of such filters can be found in [Hor89]. Three main types of frequency responses of analog filters exists, namely, Bessel, Butterworth and Chebyshev filters. All of them differ in the flatness of the passband magnitude, the phase, and the roll-off at frequencies larger than the cutoff frequency. Bessel filters are designed to have a maximally linear phase response in the passband, Butterworth filters to have maximally flat magnitude in the passband and Chebyshev filters to have a much steeper roll-off at the expense of passband or stopband ripples. The frequency response of Bessel filters implemented with analog electronics depends much less on the actual component values as for Butterworth or even Chebyshev filters, making them preferable when two or more filters with exactly the same frequency response are needed.

As an example the frequency responses of 4th order lowpass filters of all three types with a cutoff frequency of 1 Hz are shown in Fig. 3.13.

The corresponding autocorrelation functions are depicted in Fig. 3.14. Note, that the x-axis in the figure scales with the sampling frequency, while the shape stays the same. The sampling frequency used here is $f_s = 40\,\mathrm{Hz}$. The autocorrelation function of the Bessel filter drops fast towards 0 and shows no ringing, while for a Butterworth filter some ringing occurs. For a Chebyshev filter the ringing is much worse, yielding many correlated samples. Hence, a Bessel filter used as anti-aliasing filter is the best choice concerning the correlation of samples. To reach the same attenuation at the Nyquist frequency however, a higher order is needed for the Bessel filter than for the



(a) Magnitude **(b)** Phase

Figure 3.13: Frequency responses of 4th order Bessel, Butterworth and Chebyshev type lowpass filters with a cutoff frequency of 1 Hz.

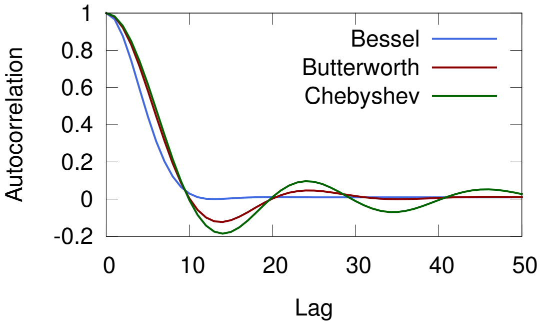


Figure 3.14: Autocorrelation functions of a 4th order Bessel, Butterworth and Chebyshev filter with a cutoff frequency of 1 Hz. Note, that the x-axis depends on the actual sampling frequency.

other types.

3.7.2 Digital Filters

Finite impulse response filters (FIR filters) are filters with a finite impulse response as their name implies, i.e. they are filters with an impulse response that becomes zero after a finite number of samples. The order of a FIR filter is given by its number of coefficients h, called *taps*. Denoting the input samples by $x(n)$, the output $y(n)$ of an M-tap FIR filter is defined as [Lyo04]

$$y(n) = \sum_{k=0}^{M-1} h(k)x(n-k) \ . \tag{3.15}$$

This equation shows that a FIR filter computes weighted averages over the input samples both for low- and highpass filters. Hence, this gives an intuition for why a filter correlates samples. For the determination of the filter's taps, i.e. for the design of the filter to match a certain requirement, we refer to the literature, e.g. [Lyo04].

CHAPTER 4

Generation of EPR Entanglement at 1550 nm

Overview

Since the foundation of quantum mechanics, entanglement has proven to be a valuable resource in quantum information tasks and has spread a variety of applications [Hor09] ranging from teleportation [Bou97, Fur98] and quantum dense coding [Ben92, Bra00] to quantum dense metrology [Was10, Ste12] and quantum cryptography [Wee12]. It is also an important ingredient to quantum repeaters [Bri98] and quantum computation [DiV95].

This chapter is organized as follows. Section 4.1 describes the characterization of the squeezed-light source and presents the first ever measurement of stably locked squeezed states with more than 10 dB squeezing at the telecommunication wavelength of 1550 nm. An introduction and overview about generation of continuous variable entanglement is given in Section 4.2. Section 4.3 describes the concept of EPR steering which goes back to Schrödinger. The first experimental demonstration of the EPR paradox and EPR steering using bipartite states generated from a single squeezed vacuum mode is described in Section 4.4. The results of this section were published in [Ebe11, Ebe13a]. Section 4.5 is about entanglement generated by two squeezed vacuum modes. There, more than 10 dB two-mode squeezed states were generated with a setup that was fully locked in all degrees of freedom. The experiment demonstrated the feasibility of demanding applications like a recently published quantum information protocol about superactivation of zero-capacity channels [Smi11], and like finite-size continuous variable quantum key distribution with security against most general attacks, cf. Chapter 5 and the following and [Fur12b]. The results of this experiment were published in [Ebe13b].

4.1 Experimental Results of Squeezed-Light Generation at 1550 nm

Using the devices described in Chapter 3 the following presents a characterization of the squeezed-light source. For the lock of the squeezed-light source the control beam had a power of 800 μW. The phase-matching temperature of the nonlinear crystal was about 50 °C. For the homodyne measurement the local oscillator power was 10 mW. The phase of the local oscillator could be locked to the phase and amplitude quadrature, respectively. It was locked to the phase quadrature which corresponds to the anti-squeezed quadrature, using the direct-current (DC) output of the homodyne detector's electronics as an error signal. As shown in Eq. (3.10) the output has the form $|\beta||\alpha|\cos\varphi$, where $|\beta|$ is the local oscillator's power, $|\alpha|$ is the power of the control beam transmitted through the nonlinear cavity and φ is the phase between the beams. To lock to the amplitude quadrature and thus to measure the squeezed quadrature, phase modulation sidebands imprinted on the control beam were employed. To generate an error signal, the alternating current (AC) output of the homodyne detector was demodulated at the modulation frequency and lowpass filtered subsequently.

Figure 4.1 shows the results. For each pump power of the parametric down-con-

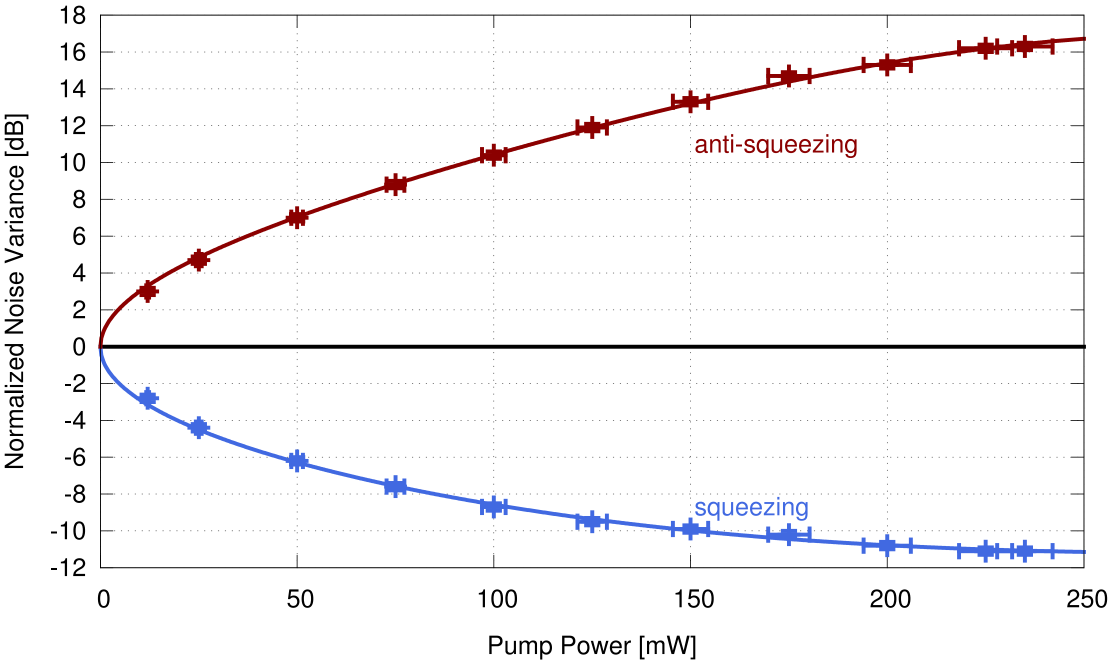


Figure 4.1: Measurement of the squeezed and anti-squeezed quadrature noise variances normalized to the noise variance of a vacuum state. The solid lines show a theoretical model fitted to the data, see Eq. (4.1).

version process the quadrature angle of the homodyne detector was locked to the squeezed quadrature first and then to the anti-squeezed quadrature. At both quadrature settings we measured the noise variance at a Fourier frequency of 8.5 MHz with a bandwidth of 300 kHz using a spectrum analyzer. Prior to the measurement the signal port of the homodyne detector was blocked and the noise variance of a vacuum state was measured for reference. Both squeezing and anti-squeezing noise variances were normalized to this reference measurement of a vacuum state. The error bars in the abscissa of the graph are due to the systematic error of the power meter used for the pump power measurement which was assumed to be 3 %. For a pump power of 235 mW a nonclassical noise reduction of 11.1 dB compared to the vacuum noise variance was achieved. The corresponding anti-squeezed noise variance was 16.3 dB above noise variance of the vacuum.

The solid lines in the figure show a theoretical model fitted to the data. The squeezed (sqz) and anti-squeezed (asqz) quadrature variances of the field can be described as a function of the pump power P by [Tak07]

$$\mathrm{Var}_{\mathrm{sqz,asqz}} = 1 \pm \eta \frac{4\sqrt{P/P_{\mathrm{th}}}}{(1 \mp \sqrt{P/P_{\mathrm{th}}})^2 + 4K(f)^2} \, , \tag{4.1}$$

where η is the detection efficiency, P_{th} is the threshold power and $K(f) = 2\pi f/\kappa$ the ratio between Fourier frequency $f = 8.5$ MHz and the cavity decay rate $\kappa = (T+L)c/l$ with the output coupler transmission T, the intra-cavity loss, the speed of light in vacuum c and the cavity's optical round trip length $l = 79.8$ mm. The model fits best with a total optical loss of $1 - \eta = 5.8\,\%$, a threshold power of $P_{\mathrm{th}} = 268$ mW and $T + L = 0.1018$.

The results above represent the first generation and measurement of more than 10 dB squeezed vacuum states with a setup that was locked in all degrees of freedom. In [Ebe11] squeezed vacuum states with 9.9 dB were presented, generated at the same experiment, but with another squeezed-light source that had more optical loss, but was also fully locked. Squeezed vacuum states with more than 10 dB nonclassical noise reduction with a manual control of the source's resonance condition and a manually controlled phase of the local oscillator for homodyne detection were first reported in [Vah08] using lithium niobate as nonlinear medium at 1064 nm. Using PPKTP this result was later improved to 12.7 dB [Ebe10]. At 1550 nm 12.3 dB were reported in [Meh11] using a similar setup but also without locks. Squeezed vacuum states in the audio band which are not accessible with our locking scheme due to the bright control beam at the carrier frequency, are for instance reported in [Vah10, The11].

4.2 Generation of Entanglement

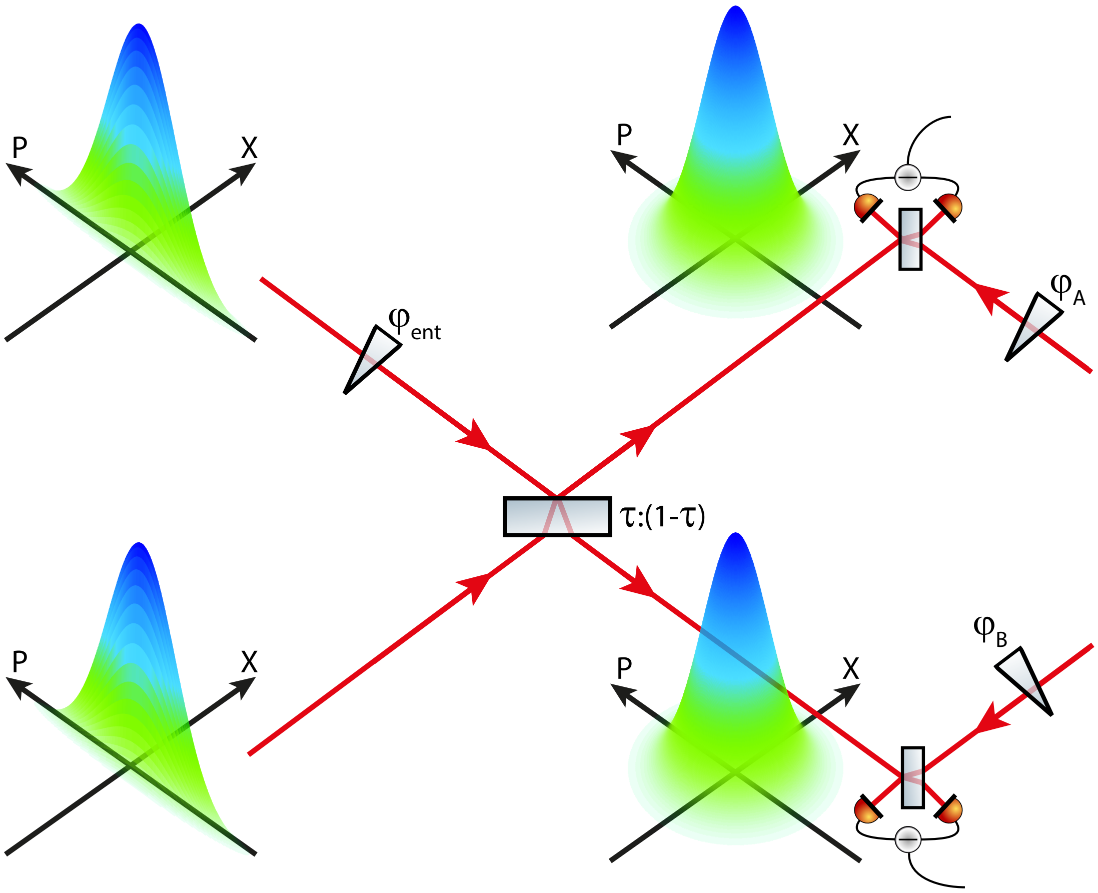


Figure 4.2: Principle of generating and detecting Gaussian continuous-variable entanglement. Two squeezed vacuum modes, here represented by their Wigner functions, are superimposed with phase $\varphi_{\mathrm{ent}} = \pi/2$ at a beam splitter with power transmissivity τ. The two output modes are entangled and measured by balanced homodyne detection. The detected quadratures are determined by the phase φ_A and φ_B of the local oscillators.

Bipartite Gaussian continuous variable entanglement can be generated by superimposing two squeezed vacuum modes at a beam splitter with power transmissivity τ [Fur98, Bow03]. This principle is depicted in Fig. 4.2. As described in Chapter 3.3 the squeezed vacuum modes in the experiment were squeezed in the amplitude quadrature X and anti-squeezed in the phase quadrature P. Prior to the superposition of the modes the phase of one of them is shifted with respect to the other by φ_{ent}. In the figure we chose $\varphi_{\mathrm{ent}} = \frac{\pi}{2}$ and a power transmissivity of the beam splitter of $\tau = 0.5$. The output modes of the beam splitter are quadrature entangled and can be measured by homodyne detection. Using the formalism presented in Chapter 2 and allowing the squeezing parameters r_1 and r_2 for the squeezed modes to be different, the covariance matrix of the bipartite state after the superposition reads

$$\gamma = S_{\mathrm{BS}}(\tau)(S_{\mathrm{sqz}}(r_1) \otimes S_{\mathrm{sqz}}(r_2))\mathbb{1}_4(S^T_{\mathrm{sqz}}(r_1) \otimes S^T_{\mathrm{sqz}}(r_2))S^T_{\mathrm{BS}}(\tau) \ . \tag{4.2}$$

Since we consider only modes without coherent excitation, the first statistical moments vanish. In the model we allow to set either r_1 or r_2 to 0, yielding a bipartite state that is generated by splitting a squeezed vacuum mode at a beam splitter. This special type of entanglement will be the topic of Section 4.4, while the case for $r_1 \neq 0$ and $r_2 \neq 0$ will be described in Section 4.5. As experimental settings are never lossless, a full theoretical description of the output modes has to include optical loss, cf. Chapter 2.8. The verification of entanglement is described in Chapter 2.11.

Continuous variable entanglement was first observed by Ou et al. [Ou92] using type II parametric down-conversion and by Furusawa et al. [Fur98] using type I parametric down-conversion as we do in this thesis. Further observations of CV entanglement using these schemes were reported for instance in [Zha00, Sch02, Lau05, Kel08, Wan10] with type II parametric down-conversion, in [Bow03, Tak06, DiG07, Hag11, Ebe11, Ste13] with type I parametric down-conversion and in [Sil01] with the optical Kerr effect.

4.3 Einstein-Podolsky-Rosen Steering

In his reply to the seminal EPR paper [Ein35] Schrödinger coined the concept of *steering* [Sch35]. His findings were that if the finest description of a quantum system is its decomposition into pure states, quantum mechanics has a process that violates local realism. The modern view of steering, which gave rise to a new interest in this phenomenon, was introduced by Wiseman et al. in [Wis07]. In their paper they showed that for Gaussian states steering is equivalent to the demonstration of the EPR paradox by the violation of inequality (2.91) or (2.92) introduced by Reid, cf. Section 2.11.2. While there is also a description of steering in terms of classical and quantum models of states [Fra12], we will consider steering here as the question whether there is a common refinement of quantum states. The argument given here was published in [Hae12] and is equivalent to the description in [Fra12] and [Wis07].

We start with the same situation as in Section 2.11.2, namely, Alice and Bob share the subsystems A and B of a two-mode squeezed state. Bob locally observes a mixed state, which can be decomposed into a convex combination of purer states. This decomposition yields a more precise description of Bob's quantum system. Using any information Alice has on the state gives a decomposition into conditional states, i.e. into states that are conditioned on Alice's measurement outcomes. Indeed these

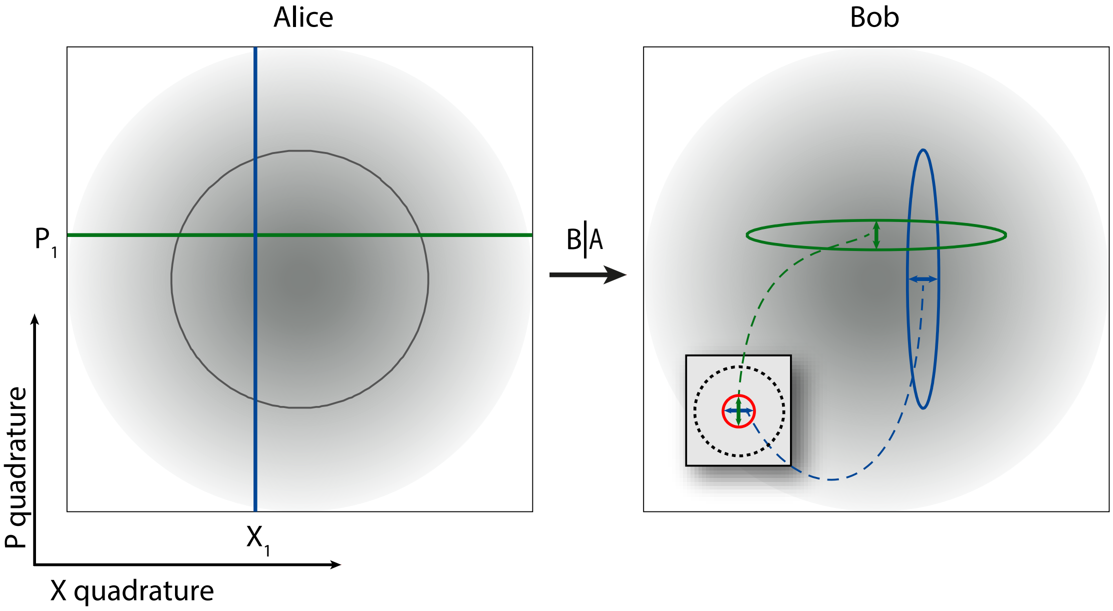


Figure 4.3: Illustration of EPR steering. Bob's locally mixed state can be decomposed using two distinct sets of states that are conditioned on Alice's measurement outcomes and are purer than Bob's mixed state. Here, the blue ellipse at Bob depicts a state conditioned on Alice X quadrature measurement outcome X_1. Similarly the green ellipse shows a state conditioned on the P quadrature measurement outcome P_1. According to local realism the set used to decompose Bob's state cannot depend on Alice's choice of measurement. Hence, the blue and the green conditional state should have a common refinement. Such a refined state is displayed in the inset by the red circle. The black dashed circle shows a pure state for reference. Thus, no common refinement exists as the red circle depicts an unphysical state.

conditional states are purer than Bob's mixed state. This situation is shown in Fig. 4.3, where exemplary measurement outcomes X_1 and P_1 for Alice measuring the amplitude quadrature and phase quadrature, respectively, are depicted by the blue and green lines on the left hand side. The related conditional states on Bob's system are indicated by the accordingly colored ellipses on the right hand side of the figure. For all outcomes Alice can obtain for an amplitude quadrature measurement, the conditional states on Bob's side have the same shape but have different position along the X-axis. Similarly, for all outcomes she can obtain by measuring the phase quadrature, the conditional states have the same shape but have different position along the P-axis. Both sets of conditional states form a decomposition of Bob's mixed state. According to EPR's argument of local realism the set of conditional states used for decomposing Bob's mixed state cannot depend on Alice's choice of measurement. Hence, there must exist a common refinement of both sets. As such a decomposition is required to be of purer states than the conditional states for X and P, a state belonging to the common refinement must have a noise variance in the X quadrature smaller than the noise variance of the X-conditional states and a noise variance in the P quadrature smaller than the P-conditional states. Such a state is depicted in the inset of the figure by the red circle. For reference a pure state is shown by the black dashed ellipse. Hence, the common refinement of the conditional states is unphysical and does therefore not exist. The bipartite entangled state is thus called *steering* from Alice to Bob.

Like EPR entanglement, steering has a directional dependence. Steering from Alice to Bob does not imply steering from Bob to Alice and vice versa [Hae12]. Non steering is certified in the picture given above by the red, refined state being physical.

4.4 EPR Entanglement Generation Using a Single Squeezed Vacuum Resource

The EPR paradox was first demonstrated by Ou et al., in 1992 [Ou92] using two-mode squeezed states generated by type II parametric down-conversion. As shown by Bowen et al., in 2003 [Bow03], the total optical loss induced to those states has to be lower than 50 % to observe the EPR paradox. In this section we will demonstrate the EPR paradox, and hence EPR steering, for the first time using states generated by superimposing a squeezed vacuum and a vacuum mode. As we will see, for such states the maximal allowable loss to still observe the EPR paradox is more severe. The applicability for quantum key distribution of the EPR states described in this section will be analyzed in Chapter 6.1.

4.4.1 Theoretical Description

Starting with a squeezed vacuum mode, entanglement can be generated by splitting it at a beam splitter, i.e. superimposing it with a vacuum mode. In terms of the description given in Section 4.2, $r_2 = 0$. For a perfect setup without optical loss, the bipartite state is always EPR entangled for any squeezing parameter $r := r_1 \neq 0$ as we will see in the following. Assuming the amplitude quadrature to be squeezed, the covariance matrix of the bipartite state reads for a balanced beam splitter

$$\gamma = \frac{1}{2}\begin{pmatrix} 1+e^{-2r} & 0 & 1-e^{-2r} & 0 \\ 0 & 1+e^{2r} & 0 & 1-e^{2r} \\ 1-e^{-2r} & 0 & 1+e^{-2r} & 0 \\ 0 & 1-e^{2r} & 0 & 1+e^{2r} \end{pmatrix} . \tag{4.3}$$

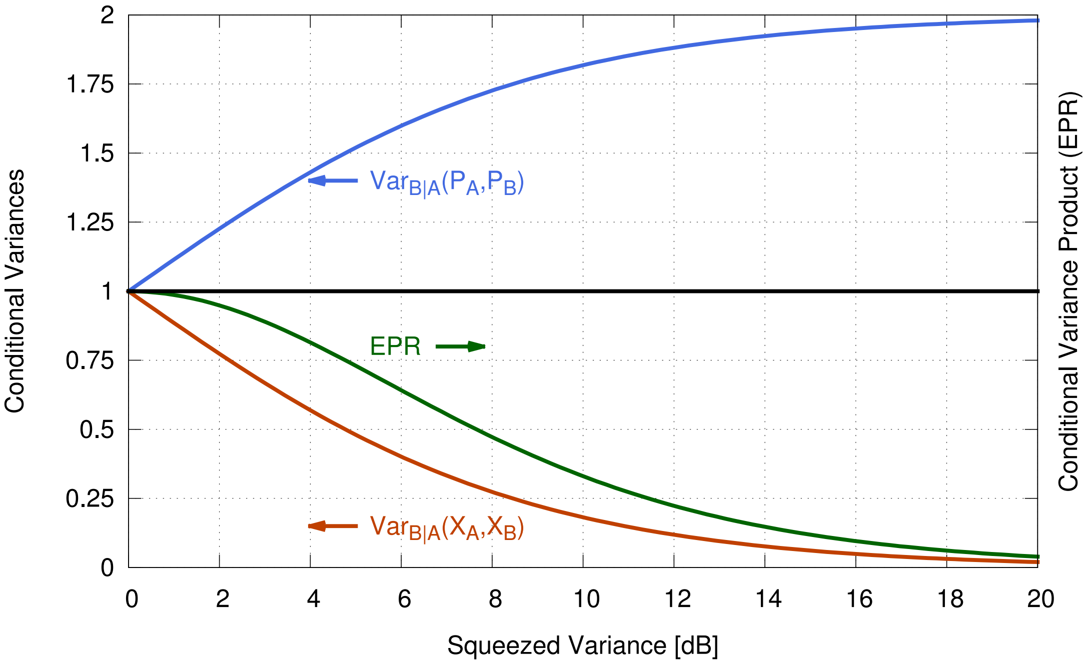


Figure 4.4: Conditional variances for amplitude and phase quadratures and the EPR criterion calculated for a pure bipartite entangled state generated by superimposing a squeezed vacuum mode with a vacuum mode. On the X-axis the variance of the squeezed quadrature of the squeezed vacuum mode normalized to the variance of a vacuum state is shown.

Hence, the conditional variances from Eqs. (2.89) and (2.90) take the form

$$\mathrm{Var}_{B|A}(\hat{X}_A,\hat{X}_B) = \mathrm{Var}_{A|B}(\hat{X}_A,\hat{X}_B) = \frac{2}{1+e^{2r}} \ , \tag{4.4}$$

$$\mathrm{Var}_{B|A}(\hat{P}_A,\hat{P}_B) = \mathrm{Var}_{A|B}(\hat{P}_A,\hat{P}_B) = \frac{2}{1+e^{-2r}} \ . \tag{4.5}$$

Using this results, the conditional variance product, i.e. the criterion for EPR entanglement, reads

$$\mathrm{Var}_{B|A}(\hat{X}_A,\hat{X}_B)\cdot\mathrm{Var}_{B|A}(\hat{P}_A,\hat{P}_B) = \mathrm{Var}_{A|B}(\hat{X}_A,\hat{X}_B)\cdot\mathrm{Var}_{A|B}(\hat{P}_A,\hat{P}_B) = \frac{2}{1+\cosh 2r} \ , \tag{4.6}$$

which is smaller than 1 for all $r \neq 0$.

The conditional variances and the EPR conditional variance product for the pure bipartite state are plotted in Fig. 4.4 versus the squeezed noise variance of the input state which is connected to the squeezing parameter r by $V_{\mathrm{sqz}} = e^{-2r}$. While for increasing squeezing $\mathrm{Var}_{B|A}(\hat{P}_A,\hat{P}_B)$ increases up to the bound of 2, $\mathrm{Var}_{B|A}(\hat{X}_A,\hat{X}_B)$ decreases towards 0. The EPR criterion also decreases for increasing squeezing to-

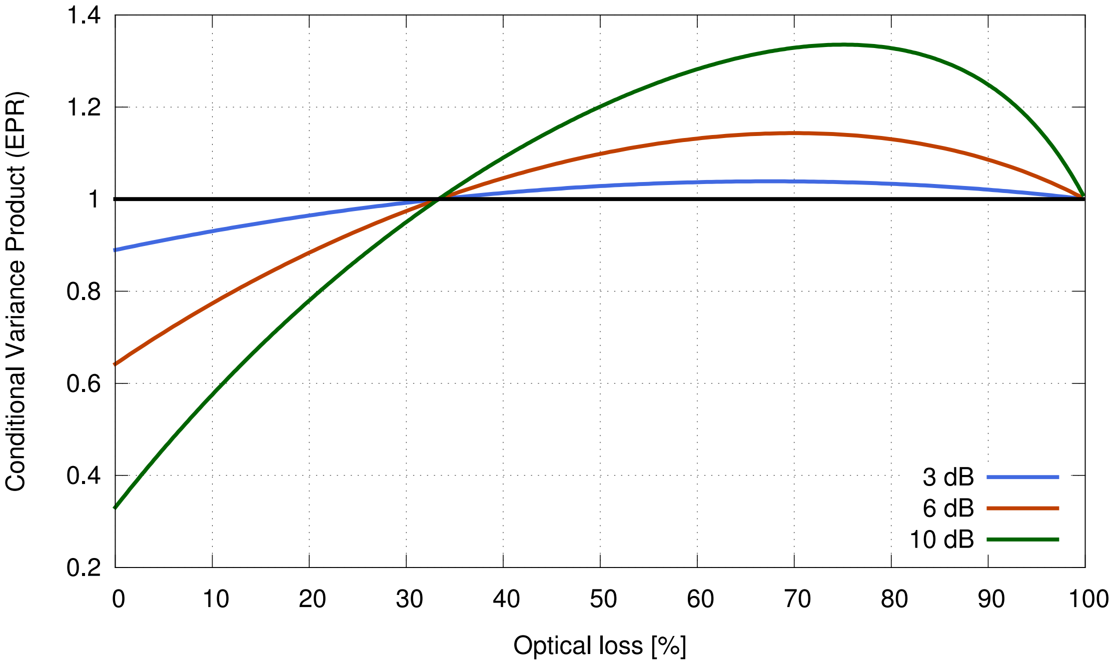


Figure 4.5: Simulation of the EPR conditional variance product of a bipartite entangled state generated by superimposing a squeezed mode with a vacuum mode at a balanced beam splitter, versus symmetrical optical loss. The different curves were calculated for 3 dB, 6 dB and 10 dB squeezed vacuum.

wards 0. Hence, the achievable EPR conditional variance product is only limited by the variance of the squeezed quadrature of the squeezed input state.

However, as experimental implementations are never lossless the optical loss of a setup has to be taken into account. Let us denote the amount of optical loss induced by the setup by ϵ and the covariance matrix describing the state prior to entanglement generation by γ. Since

$$S_{\mathrm{BS}}(\tau)\left[(1-\epsilon)\gamma+\epsilon\mathbb{1}_4\right]S_{\mathrm{BS}}^T(\tau) = (1-\epsilon)S_{\mathrm{BS}}(\tau)\gamma S_{\mathrm{BS}}^T(\tau)+\epsilon S_{\mathrm{BS}}(\tau)S_{\mathrm{BS}}^T(\tau) \tag{4.7}$$

$$= (1-\epsilon)S_{\mathrm{BS}}(\tau)\gamma S_{\mathrm{BS}}^T(\tau)+\epsilon\mathbb{1}_4\ , \tag{4.8}$$

optical loss introduced to the squeezed mode before the superposition with a vacuum mode at a beam splitter with power transmissivity τ is the same as applying the loss to both output modes of the beam splitter. Hence, symmetrical loss introduced to the entangled modes can be modeled by applying the loss to the squeezed mode.

The EPR conditional variance product versus the amount of symmetrical optical loss is shown in Fig. 4.5 for an initially pure squeezed vacuum state with a squeezed noise variance of 3 dB, 6 dB and 10 dB below the vacuum noise variance. In the calculation the beam splitter was balanced. Independent of the squeezed variance of the squeezed input state, the optical loss is allowed to be at most 33.3 % to observe EPR entanglement. Indeed, EPR entanglement can be observed with this scheme if

$$(1 - V_{\text{sqz}})^2(1 - \epsilon)\left(\frac{1}{3} - \epsilon\right) > 0 \tag{4.9}$$

holds [Ebe11]. Here, V_{sqz} is the variance of the squeezed state normalized to the variance of a vacuum state.

4.4.2 Experimental Setup

The experimental setup to demonstrate EPR entanglement is shown in Fig. 4.6. The coherent light preparation, the pump beam generation and the squeezed-light source, including its locking scheme, used in this setup has been described in Chapter 3. The squeezed output mode of the squeezed-light source was split at a balanced beam splitter and thus superimposed with a vacuum mode. Both output modes of the beam splitter were detected by homodyne detection. Homodyne detection has been introduced in Chapter 3.4. For the lock of the phase of both local oscillators a single sideband technique was employed. For this purpose a small fraction of about 15 mW of the main laser beam was frequency shifted using an acousto-optical modulator (AOM) and superimposed with the squeezed beam at the dichroic beam splitter that separated the squeezed vacuum mode from the pump. To become a reference for the squeezed quadrature, the single sideband was phase locked to the control beam. The frequency shifted light field reflected by the dichroic beam splitter and the small fraction of about 500 ppm of the control beam leaking through it were detected by a resonant photo detector in transmission of another dichroic beam splitter which was highly reflective for the pump and highly transmissive for the fundamental. The output of the photo detector was demodulated at the single sideband's frequency of 80 MHz and fed back to a phase shifter in the path of the single sideband using a servo controller. Since the AOM introduced also an amplitude modulation at the AOM's frequency, the demodulation phase for the error signal generation should have been set to the phase quadrature. Due to the large phase noise of our fiber laser this was not possible as the generated error signal was very noisy. Thus, we measured the amplitude quadrature instead and stabilized the power of the frequency shifted beam to have a more stable offset caused by the amplitude modulation. To generate error signals for the homodyne detectors' local oscillator phases at Alice's and Bob's side, the AC outputs of their respective detectors were demodulated with an electronic 80 MHz sinusoid, called *electronic local oscillator*. By changing the phase of the electronic local oscillator, the phase of the optical local oscillator could be locked to arbitrary values.

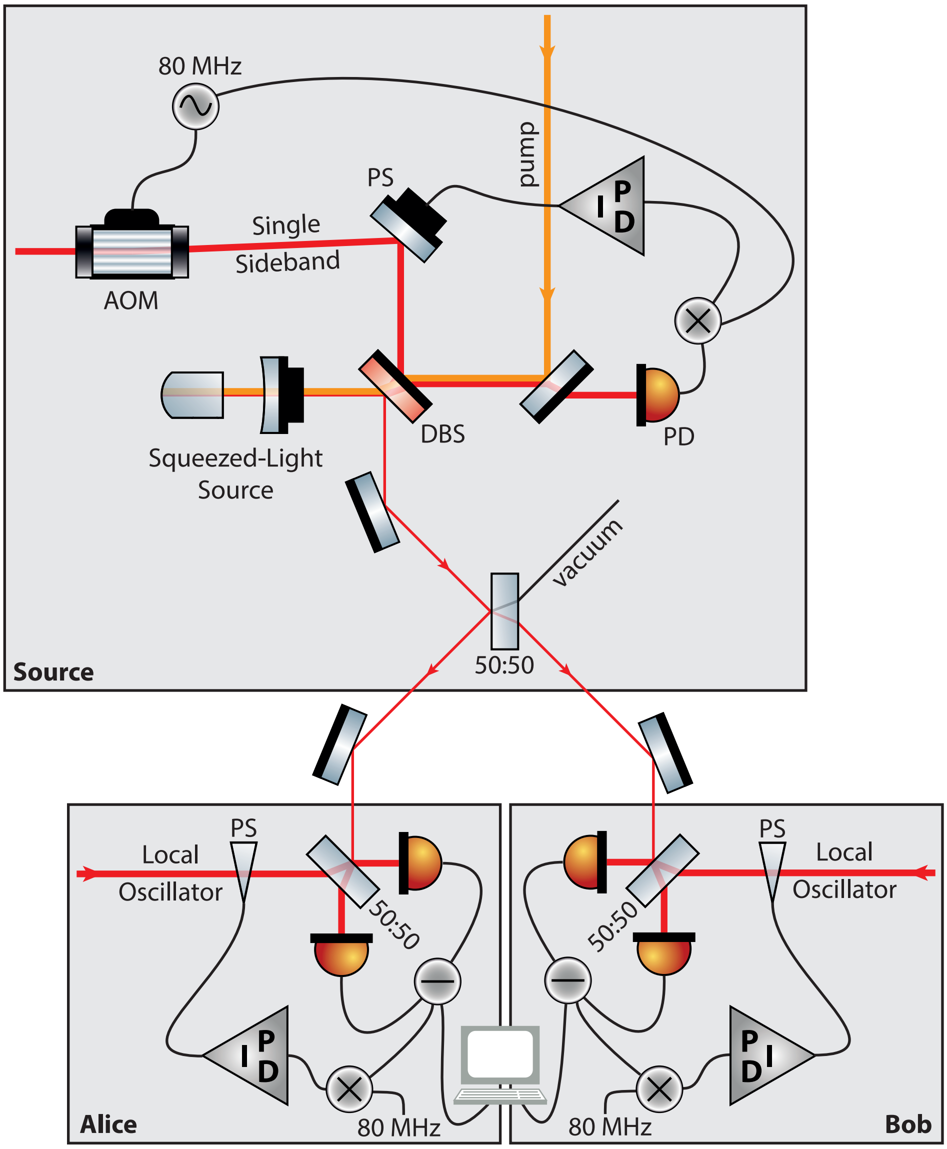


Figure 4.6: Experimental setup of EPR entanglement generation by superimposing a squeezed mode with a vacuum mode. At the source a squeezed mode was generated by parametric down-conversion and then split at a balanced beam splitter. Both outputs of the beam splitter were detected by homodyne detection. To lock the local oscillators' phases at Alice and Bob we employed a single sideband technique. A fraction of the main laser beam was frequency shifted by 80 MHz using an acousto-optical modulator (AOM) and phase locked to the control beam of the squeezed-light source. The beat of the single sideband and the local oscillator was detected by the homodyne detector whose high frequency output was demodulated at 80 MHz to generate an error signal for the phase of the local oscillator. Both homodyne detectors' outputs were recorded simultaneously by a data acquisition system. AOM: acousto-optical modulator, PS: phase shifter, DBS: dichroic beam splitter, PD: photo detector.

To record data the AC outputs of both homodyne detectors were plugged into the slow data acquisition system described in Chapter 3.6 which sampled with a sampling frequency of 500 kHz.

4.4.3 Results

For each quadrature combination of the tomographic reconstruction protocol, cf. Chapter 3.5, we recorded 5×10^6 samples. Furthermore, we recorded 5×10^6 samples of a vacuum state measurement by blocking the signal ports of Alice's and Bob's homodyne detectors. For a pump power of 235 mW the reconstructed covariance matrix reads

$$\gamma = \begin{pmatrix} 0.541 & 0.135 & 0.459 & -0.095 \\ 0.135 & 24.633 & -0.037 & -23.293 \\ 0.459 & -0.037 & 0.548 & 0.264 \\ -0.095 & -23.293 & 0.264 & 23.840 \end{pmatrix} . \tag{4.10}$$

One can directly see certain properties of the state from the entries in the matrix. The values on the principal diagonal are the variances for the amplitude and phase quadrature measurements at Alice's and Bob's detector. The diagonal entries of the two 2×2 blocks in the upper right and lower left give the strengths of the correlations in the amplitude quadrature and the anti-correlations in the phase quadrature between both detectors, respectively. In a perfect orthogonal measurement the remaining entries should turn out to be zero since they give the covariance between amplitude and phase quadratures. The small deviations from zero show that the measurements were not perfectly orthogonal but close.

Figure 4.7 shows the EPR covariance product for the Alice to Bob direction versus the pump power used to pump the squeezed-light source. For each pump power setting the recorded data was divided into 10 chunks. For each chunk the covariance matrix was reconstructed and the EPR-Reid criterion from Eq. (2.91) was calculated. The standard deviation of these 10 values are shown as error bars. For the pump power a systematic error of the power meter of 3 % was assumed. All states generated during the measurement were EPR entangled and for a pump power of 235 mW an EPR conditional variance product of 0.31 was reached. The solid line in the figure shows a theoretical model fitted to the data. The simulation is based on the model from Eq. (4.1) for the noise variances of the squeezed and anti-squeezed quadratures of a squeezed vacuum state versus pump power. The fitting parameters of this model were obtained from the characterization of our squeezed-light source in Section 4.1. Using this model the covariance matrix of the bipartite entangled state was simulated taking into account additional optical loss which was a free parameter in the fit. The model fitted best with an additional optical loss of 0.9 % in both arms which could be due

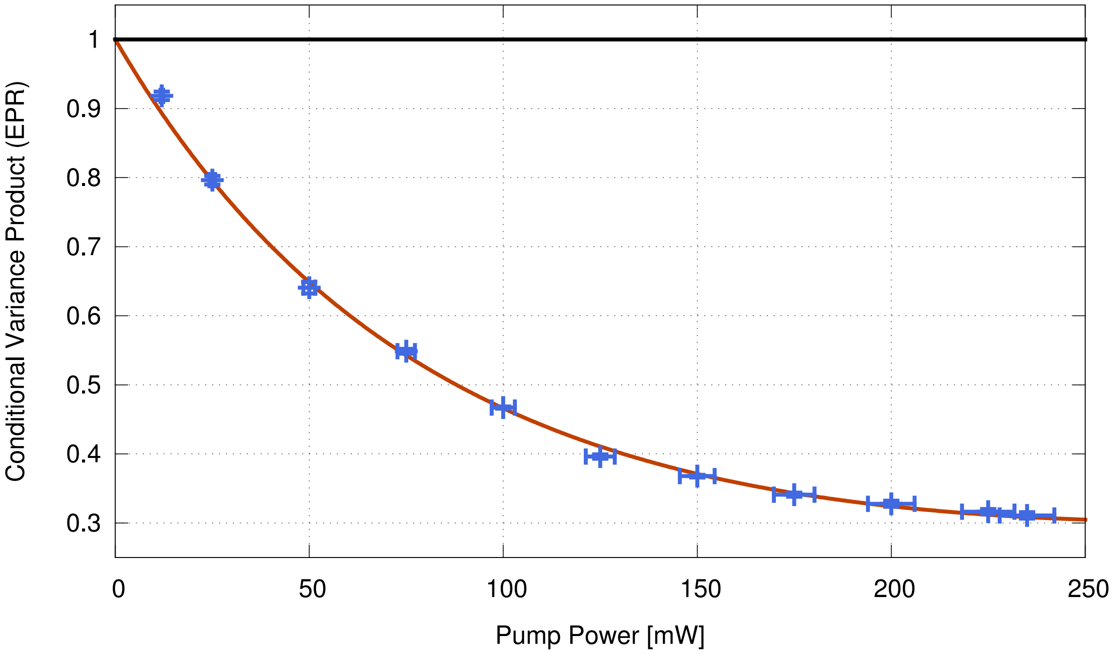


Figure 4.7: Conditional variance product versus pump power for the squeezed-light source. EPR entanglement was certified for all pump powers we used and an EPR-value of 0.31 was reached for 235 mW. The red solid line shows a theoretical model fitted to the data.

to additional anti-reflective coatings compared to the measurement of the squeezed state. Hence, the total optical loss introduced to our state was 6.6 %. Calculating the EPR-Reid criterion for the direction from Bob to Alice yielded similar values as expected for a state with symmetrical optical loss.

The modulus of the correlation coefficients from Eq. (2.84) for the state generated with 235 mW pump power was about 0.84 for the amplitude and 0.96 for the phase quadrature. In comparison maximally entangled states as considered by EPR in their 1935 paper [Ein35] have a correlation coefficient of 1.

The measurement presented here is an improved version of the first demonstration of EPR entanglement and steering for an entangled state generated by involving only one squeezed mode, which was presented in [Ebe11]. The setup described here was improved to get rid of the excess noise observed in [Ebe11] which was due to an imperfect data acquisition process. Entanglement generated from a single squeezed mode was formerly generated for instance in [DiG07], however, no EPR entanglement was observed due to too high optical loss.

4.5 Entanglement Generation Using Two Squeezed Vacuum Resources

Recently a continuous variable quantum key distribution protocol which provides composable security against most general attacks with a finite number of samples was proven to be secure [Fur12b]. To perform such an experiment with a positive key rate, the protocol requires a high degree of two-mode squeezing, low channel loss and a large number of samples in the order of 10^8. To achieve these requirements not only more than 10 dB entanglement measured by the Duan criterion is necessary but also a stable control of the entanglement generation. This section describes an experiment providing both, a high degree of entanglement and a stable control in all degrees of freedom. A quantum key distribution experiment using these state is described in Chapter 5.

The principle of the entanglement generation by superimposing two squeezed vacuum modes was discussed in Section 4.2. As shown in Fig. 4.2 we denote the phase between the squeezed vacuum modes by φ_{ent}. The output modes of the beam splitter were detected by homodyne detection, cf. Chapter 3.4, where the phases of the local oscillators φ_A and φ_B determined the measured quadrature angle. While the setup presented in [Ste13] was intrinsically stable for about 500 ms without lock, our setup had to be stable for more than 15 min to make an application of the entanglement in the quantum key distribution experiment described in Chapter 5 possible. This was achieved by locking all degrees of freedom, including φ_{ent}. In particular φ_{ent} was difficult to lock, since the control and auxiliary beams were only allowed to have low power as they had to be shot-noise limited in the measurement frequency band. Otherwise, to achieve highly entangled states, the induced optical loss for locking purposes could only be small.

4.5.1 Experimental Realization and Locking Scheme

The second squeezed-light source implemented for the entanglement generation was build identically to the one described in Chapter 3.3, but had a slightly lower pump power threshold of about 190 mW, which might be due to slightly different outcoupling efficiencies, see below. The locking scheme used to lock φ_{ent}, φ_A and φ_B involved two single sidebands generated by frequency shifting a fraction of the main laser beam. A schematic of the identical experimental setups for both squeezed-light sources is depicted in Fig. 4.8. The lock of the cavity length and the pump phase worked exactly as described in Chapter 3.3. While for the first squeezed-light source the phase modulation sidebands had a frequency of 33.9 MHz, we used 35.5 MHz for the second one. In the figure the frequencies for the second squeezed-light source are denoted in

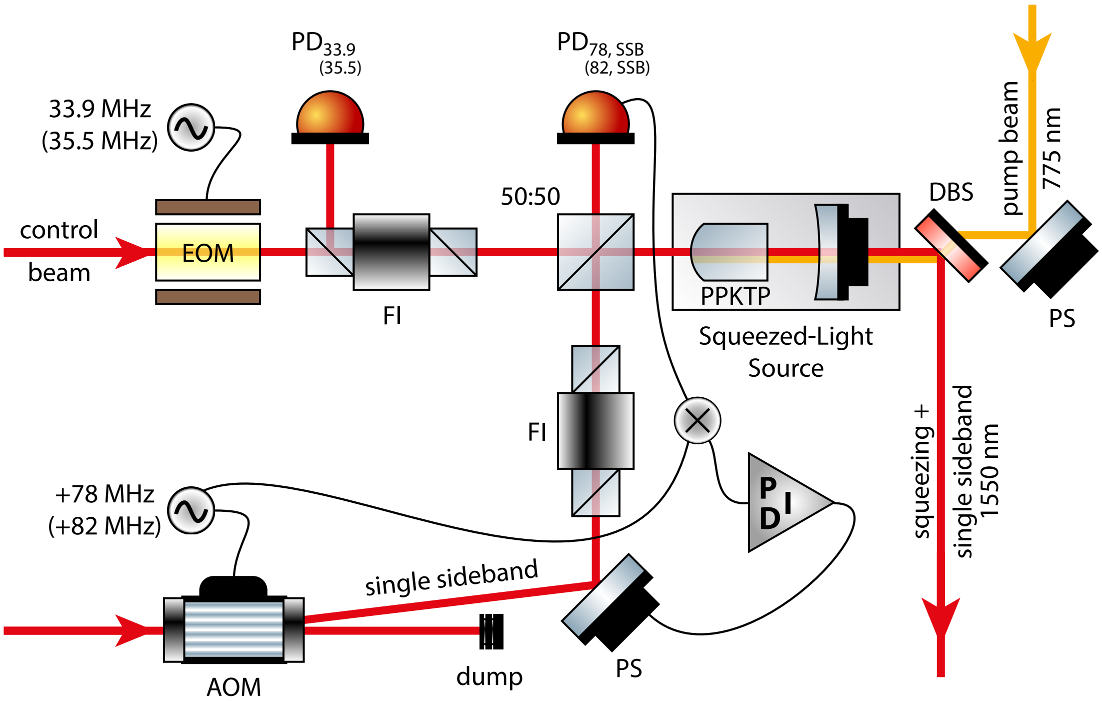


Figure 4.8: Locking scheme of the squeezed-light source and introduction of the single sideband. The cavity length and the pump phase were locked as described in Chapter 3.3. The single sideband was superimposed with the control beam in front of the cavity. A Faraday isolator in the path prevented parasitic cavities. $\mathrm{PD}_{78,\mathrm{SSB}}$ was used to generate an error signal for the phase lock of the single sideband to the control beam. The frequencies written in parentheses are the modulation frequencies used for the second squeezed-light source, while the frequencies without parentheses were used for the first one. EOM: electro-optical modulator, PD: photo detector, FI: Faraday isolator, AOM: acousto-optical modulator, PS: phase shifter, DBS: dichroic beam splitter, PPKTP: Periodically Poled Potassium Titanyl Phosphate.

parentheses. The single sideband, at 78 MHz for the first and 82 MHz for the second squeezed-light source, respectively, was generated by an AOM and had a power of about 30 μW. In contrast to the setup described in Section 4.4 for the entanglement generation involving only one squeezed vacuum mode, the single sideband was superimposed with the control beam before entering the cavity. A resonant photo detector, in the figure called $\mathrm{PD}_{78,\mathrm{SSB}}$, was used to generate an error signal for the phase lock of the single sideband to the control beam. The advantage of this setup over the previous one was, that the amplitude modulation of the single sideband was no longer important. Thus, the set point of the phase lock was much more stable.

Figure 4.9 shows schematically the experimental setup for the superposition of the squeezed modes and the phase lock of φ_{ent}. The fringe visibility of the superposition

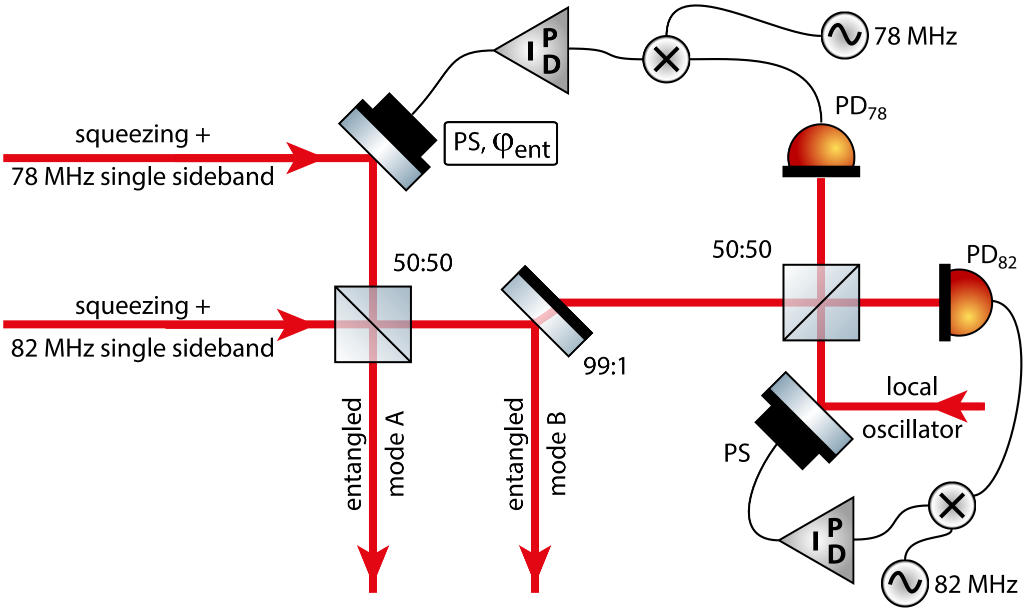


Figure 4.9: Locking scheme for the phase φ_{ent} between the squeezed vacuum modes. A small fraction of one of the output modes of the balanced beam splitter was superimposed with an auxiliary local oscillator whose beat with the 78 MHz single sideband was detected by the photo detector PD_{78}. To generate an error signal for φ_{ent} the output signal of this photo detector was demodulated at 78 MHz. To lock the phase of the auxiliary local oscillator, the beat with the 82 MHz single sideband was detected at the other output port. The phase of the electronic local oscillator used to demodulate the output signal of PD_{78} determined the set point for the lock of φ_{ent}. PS: phase shifter, PD: photo detector.

of the squeezed vacuum modes was 99.5 %. The output modes are labeled mode A and mode B in the figure. A fraction of 1 % of mode B was tapped-off and superimposed with an auxiliary local oscillator with a power of about 5 mW at a balanced beam splitter. One of the outputs was detected with a resonant photo detector at 82 MHz and used to generate an error signal for the phase of the auxiliary local oscillator. The other output was detected with a photo detector resonant at 78 MHz to generate an error signal for φ_{ent}. The phase of the electronic local oscillator used for the demodulation of the photo detector's signal determined the angle of φ_{ent}. While the usage of an auxiliary local oscillator involved an additional phase lock, the beat between the single sidebands at 4 MHz was too weak to be detectable.

Figure 4.10 shows a schematic of the homodyne detectors used to measure the field quadratures of both entangled modes A and B. At each homodyne detector a local oscillator field with a power of 10 mW was superimposed with an entangled mode at a balanced beam splitter with a fringe visibility of 99.5 %. The phase of each local oscillator was locked using an error signal generated by demodulating the output

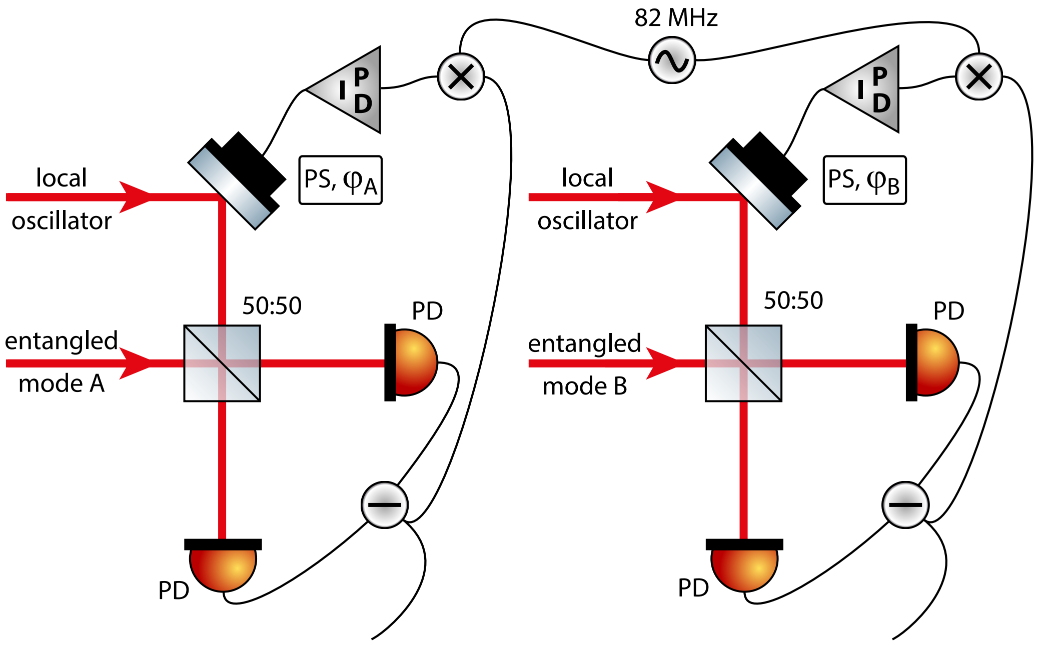


Figure 4.10: Schematic of the homodyne detection of both entangled modes A and B. The phases of the local oscillators were locked using error signals generated by demodulating the output signals of the respective homodyne detector's electronic circuit.

signal of the homodyne detector's electronics at 82 MHz. By tuning the phases of the electronic local oscillators used for the demodulation processes, the set points for the lock of φ_A and φ_B could be independently set to any angle.

Both output signals of the homodyne detectors were recorded simultaneously with the fast data acquisition system described in Chapter 3.6.

4.5.2 Results

A two-mode squeezed vacuum state was generated with a pump power of about 200 mW for the first and 150 mW for the second squeezed-light source. φ_{ent} was controlled to an angle of $\frac{\pi}{2}$. The vacuum noise reference was measured by blocking the signal ports of the homodyne detectors. By controlling φ_A and φ_B to the amplitude or phase quadrature we made a partial tomographic measurement, cf. Chapter 3.5. For each quadrature setting we recorded 10^6 data points from which we partially re-

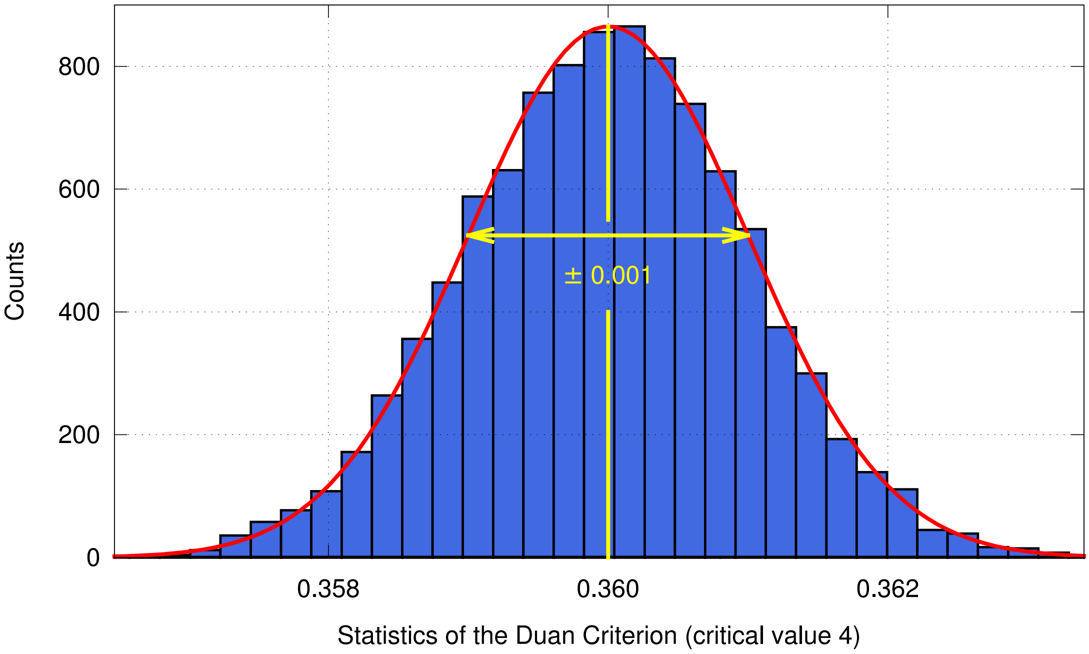


Figure 4.11: Histogram of the Duan inseparability criterion from Eq. (2.81) obtained by bootstrapping the measured samples. The solid line shows a fit of a Gaussian curve to the histogram.

constructed the covariance matrix

$$\gamma = \begin{pmatrix} 21.813 & (0) & -21.725 & -0.010 \\ (0) & 25.750 & -0.140 & 26.120 \\ -21.725 & -0.140 & 21.801 & (0) \\ -0.010 & 26.120 & (0) & 26.685 \end{pmatrix} . \tag{4.11}$$

Here, the values given in brackets could not directly be measured as they correspond to non-commuting operators. In principle, these entries of the covariance matrix can be calculated from additional measurements at a linear combination of the amplitude and phase quadrature, cf. Chapter 3.5. Since φ_{ent} was precisely controlled to $\frac{\pi}{2}$, as well as the phases of the homodyne detectors' local oscillators were precisely controlled to the amplitude and phase quadratures, the covariances, which were not determined, should be close to 0 [Ste13].

Figure 4.11 shows a histogram of the Duan inseparability criterion from Eq. (2.81). The histogram was calculated by bootstrapping the measured 10^6 samples into 10^4 chunks of 2×10^5 length [Efr86, Bic08]. A Gaussian function was fitted to the histogram yielding 0.360 ± 0.001 for the Duan criterion. This corresponds to 10.45 ± 0.01 dB below the threshold to separability.

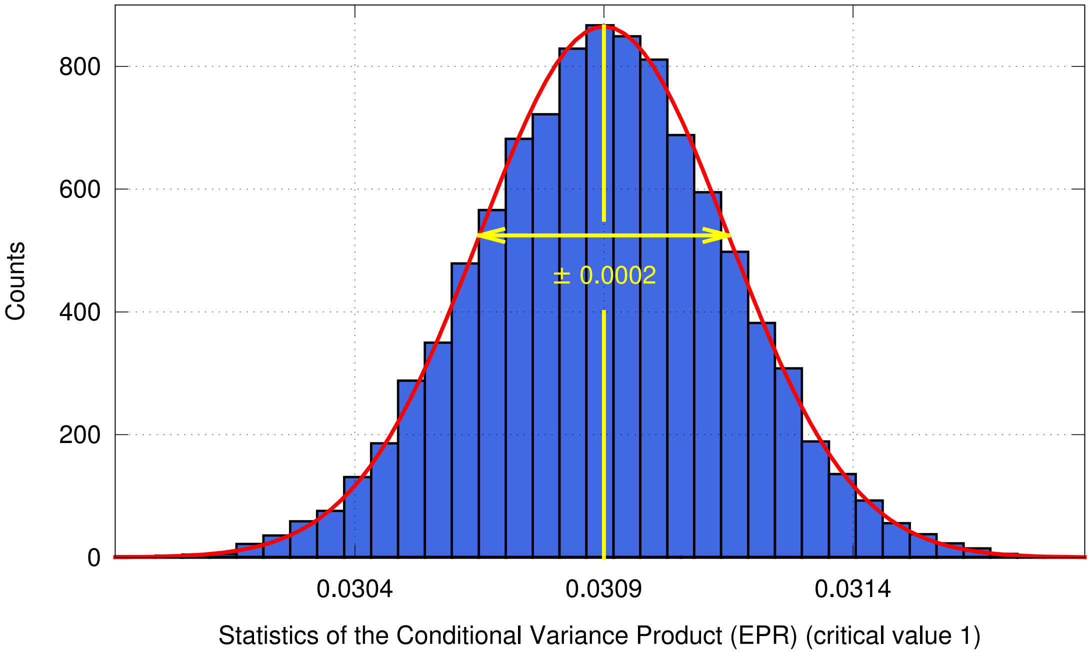


Figure 4.12: Histogram of the EPR entanglement criterion by Reid from Eq. (2.91) obtained by bootstrapping the measured samples. The solid line shows a fit of a Gaussian curve to the histogram.

Figure 4.12 shows a histogram of the EPR criterion by Reid in the direction from Alice to Bob from Eq. (2.91). The histogram was computed the same way as for the Duan criterion. The Gaussian fit yielded an EPR value of 0.0309 ± 0.0002. For the other direction similar results were obtained. In Ref. [Ste13] 0.41 for the Duan criterion and 0.04 for the EPR criterion were measured at 1064 nm, already outperforming all previous experiments on continuous variable entanglement.

The correlation coefficients from Eq. (2.84) for our state read

$$C(\hat{X}_A, \hat{X}_B) \approx C(\hat{P}_A, \hat{P}_B) \approx 0.996 \ . \tag{4.12}$$

This demonstrates that our states are quite close to the maximally entangled states considered in the original EPR paper [Ein35].

To demonstrate the stability of the active control loops, Fig. 4.13 shows the variance of the sum of the amplitude quadrature operators, $\mathrm{Var}(\hat{X}_A + \hat{X}_B)$, and the variance of the difference of the phase quadrature operators, $\mathrm{Var}(\hat{P}_A - \hat{P}_B)$, versus time. Both variances were normalized to a joint measurement of vacuum states at the homodyne detectors, $\mathrm{Var}(\hat{X}_A^{\mathrm{vac}} + \hat{X}_B^{\mathrm{vac}})$ and $\mathrm{Var}(\hat{P}_A^{\mathrm{vac}} - \hat{P}_B^{\mathrm{vac}})$, respectively. Over the measurement time of 10 s the noise variances were stable at about 10.0 dB and at about 10.9 dB for the amplitude and phase quadrature, respectively. Without our active control loops

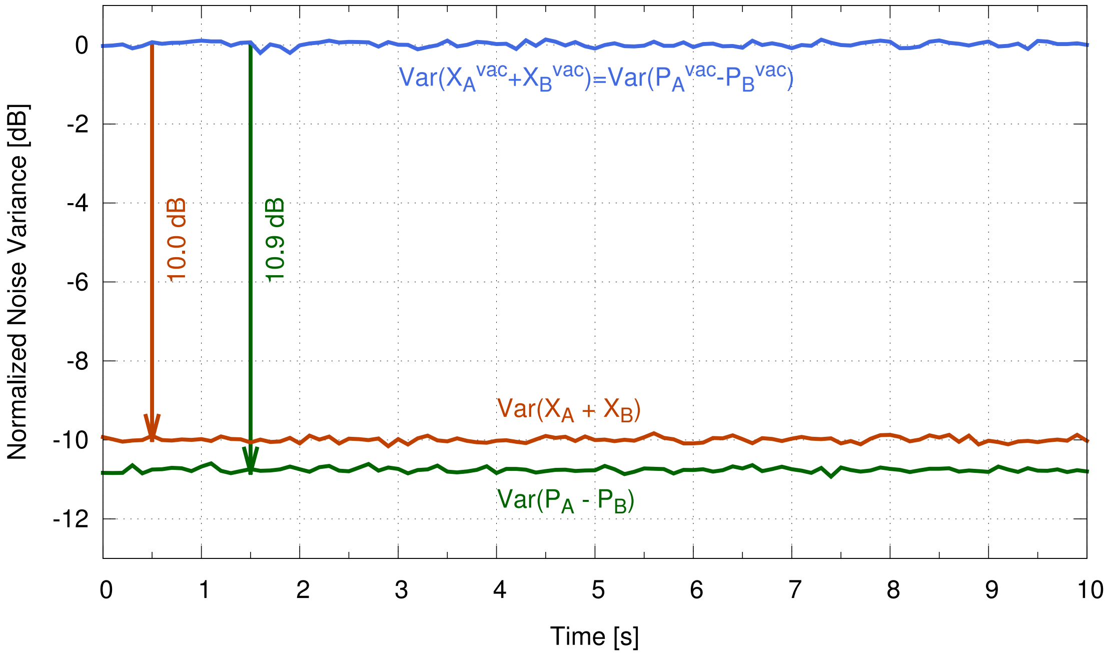


Figure 4.13: Stability of the phase locks. The noise variances Var$(\hat{X}_A + \hat{X}_B)$ and Var$(\hat{P}_A - \hat{P}_B)$ normalized to the variance of the sum or difference of the quadratures for a vacuum state are plotted versus time. The noise traces are stable over the measurement time.

the noise suppression would reach the same values, however, only stable over short time scales. For instance, in Ref. [Ste13], where φ_{ent} was not locked, the measurement time was only 200 μs. The stability of our phase lock was not limited to the 10 s being presented in the figure. Indeed, we observed the stable production of our entangled states for more than 15 min, cf. Chapter 6. In principle, our active control loops allow an extension of the measurement time to arbitrary duration if the dynamic ranges of the used piezo actuators are large enough to compensate for thermal drifts.

The optical loss of our squeezed-light sources was slightly asymmetric with an outcoupling efficiency of about 96 % for the first and about 97.5 % for the second source. The fringe visibility at the entangling beam splitter was about 99.5 %. Taking into account the 1 % optical loss introduced by the tap-off in one arm for the phase lock at the entangling beam splitter, the fringe visibility of about 99.5 % at the homodyne detectors' beam splitters, the quantum efficiency of the homodyne detector's photo diodes of about 99 % and propagation loss of about 1 %, the observed values for the Duan and EPR-Reid criterion are reproduced quite well. We observed no evidence for phase noise, showing the good performance of the implemented control scheme.

4.6 Summary

To summarize, a characterization of squeezed vacuum states at the telecommunication wavelength of 1550 nm was presented. The states were the first actively stabilized squeezed states with a noise variance in the squeezed quadrature of more than 10 dB below the vacuum noise. The generated states revealed 11.1 dB non-classical noise reduction in the squeezed quadrature and a corresponding anti-squeezed noise variance of 16.6 dB compared to the vacuum noise.

Futhermore, the observed squeezed vacuum states were used to demonstrate both the EPR paradox and EPR steering by superimposing them with a vacuum mode. This was possible since the experimental setup induced an optical loss of only 6.6 %, which is much less than the threshold of 33.3 % below which EPR entanglement can be observed for such bipartite states. Using a squeezed vacuum mode with a noise variance in the squeezed quadrature which was 11.1 dB below the vacuum noise variance, an EPR conditional variance product of $0.31 < 1$ was reached.

Using instead two squeezed vacuum modes which were superimposed at a balanced beam splitter, 10.45 ± 0.01 dB entanglement certified by the Duan inseparability criterion was observed. The EPR conditional variance product for this state was 0.0309 ± 0.0002. Both values represent the largest entanglement strength ever observed so far in the continuous variable regime. Since the correlation coefficients for the amplitude and phase quadratures were with about 0.996 very close to 1, the generated states were a good approximation for the states considered by Einstein, Podolsky and Rosen in their famous Gedanken experiment. Furthermore, the entanglement generation and detection process was locked in all degrees of freedom and was stable over more than 15 min which was the necessary measurement time to record 10^8 samples for the QKD experiments as described in Chapter 6.

CHAPTER 5

Theory of Gaussian Finite-Size Quantum Key Distribution

Overview

This chapter describes the protocols for entanglement-based quantum key distribution under collective and general attacks, respectively, as used in the implementations presented in Chapters 6 and 7. The security proofs of the protocols take, in particular, the finite key size into account as in real implementations an infinite number of measurements cannot be performed. The security proofs which are used in this chapter, were developed by F. Furrer et al. [Fur12b]. For collective attacks the security proof was extended to states with an asymmetry in the field quadrature variances in [Ebe13a].

This chapter is organized as follows. Section 5.1 introduces the definition of composable security. A generic protocol for quantum key distribution is described in Section 5.2. The secure key length of this generic protocol is given in Section 5.3. Section 5.4 is devoted to quantum key distribution with the restriction on an adversary to collective attacks. Here, the generic protocol is adapted to a more specific protocol that provides security against collective attacks, and the secure key length is given. The protocol and the secure key length for quantum key distribution without restrictions on the eavesdropper are given in Section 5.5.

5.1 Security

Quantum key distribution is the task of distributing keys between two parties in such a way that the keys are only known by them and completely unknown to an adversary. We call the two parties among which the key is distributed, Alice and

Bob, and the adversary Eve. As resource for the key distribution we use a bipartite entangled state whose density operator is denoted by $\hat{\rho}_{AB}$. If $\hat{\rho}_{AB}$ is in a pure state, it is completely detached from the environment. Hence, outcomes from measurements performed on this state are uncorrelated to any other system and thus secret. Since distributed continuous variable quantum states, as considered in the previous chapters, are affected by optical loss, e.g. when transmitted through optical fibers, the states are not pure. Let $\hat{\rho}_{ABE}$ describe a pure quantum state with $\mathrm{Tr}_E(\hat{\rho}_{ABE}) = \hat{\rho}_{AB}$. $\hat{\rho}_{ABE}$ is then called a *purification* of $\hat{\rho}_{AB}$. As the ABE system is pure it is uncorrelated with its environment and hence, the E system contains all correlations of $\hat{\rho}_{AB}$ with its environment. Thus, all optical loss of a state is contained by the E system.

5.1.1 Universally Composable Security

Key distribution is usually part of a larger cryptographic system. For example it is often used in combination with the one-time pad algorithm for encrypting messages. The notion of *universally composable security* [Can01] describes that the security of a cryptographic system is not compromised when it is composed with an other arbitrary system. If, for example, a part of a secret key is compromised by an adversary, universal security implies that any other bit remains secure [Ren05a, Koe07].

Definitions of universal composable security are based on the idea to compare the distance of a key S generated by a real cryptographic system, to a perfectly secure key U generated by an ideal system which is independent of any knowledge of potential adversaries. S is then said to be secure if it is close to U, where the distance measure has to be chosen appropriately [Ren05a].

Let S be a key distributed according to a probability distribution P_S. We will describe the classical key values s by orthogonal quantum states $|s\rangle$ on the Hilbert space $\mathcal{H}_S$. The state $\hat{\rho}_S$ is then given by

$$\hat{\rho}_S = \sum_{s \in S} P_S(s) |s\rangle\langle s| \ . \tag{5.1}$$

$\hat{\rho}_S$ might be part of a quantum system $\hat{\rho}_{SE}$ on $\mathcal{H}_S \otimes \mathcal{H}_E$, where the state $\hat{\rho}_E^s$ on $\mathcal{H}_E$ is a quantum state depending on the classical value s. $\hat{\rho}_{SE}$ is then given by

$$\hat{\rho}_{SE} = \sum_{s \in S} P_S(s) |s\rangle\langle s| \otimes \hat{\rho}_E^s \ , \tag{5.2}$$

which we call a *classical-quantum state* (cq-state).

Using this definition a key S is ϵ_s-secure if [Ren05a, Fur11]

$$\frac{1}{2}\|\hat{\rho}_{SE} - \hat{\rho}_U \otimes \hat{\sigma}_E\| \leq \epsilon_s \ , \tag{5.3}$$

where $\hat{\rho}_U = \sum_{s \in S} \frac{1}{|S|} |s\rangle\langle s|$ describes a perfectly secure key U which is separable to an arbitrary quantum state $\hat{\sigma}_E$ possessed by an adversary. The perfectly secure key U is thereby uniformly distributed, i.e. each key value has a probability of $\frac{1}{|S|}$. The distance between the real key and the perfect key, including a quantum adversary E, is measured with the trace norm $\|\cdot\|$ and bounded by $2\epsilon_s$. This means that if $\hat{\rho}_{SE}$ fulfills Eq. (5.3), the key S is identical to the secure key U with probability $(1 - \epsilon_s)$. In [Ren05a] it was shown that S keeps indeed secure if composed with other cryptographic systems as required by the definition of universally composable security.

5.2 Generic Protocol

This Section describes the protocol we will use to establish a secure key. The protocol is the same whether considering collective or coherent attacks, except for the parameter estimation phase.

Preliminaries For the classical post-processing Alice and Bob need an authenticated channel to communicate. So in a first step Alice and Bob need to establish such a channel and have to make sure that they prove to each other that they really are who they claim to be. This can be for instance realized by a pre-shared secret key. We will not go into detail of authentication but assume that Alice and Bob have such an authenticated channel. Further details can be found in [Sti94, Gem94]. Furthermore, Alice and Bob make sure that they both share the same parameters of the quantum key distribution protocol.

Distribution of Quantum States and Homodyne Measurements Alice prepares entangled states with her EPR source, keeps one subsystem and sends the other to Bob. Both parties simultaneously perform homodyne measurements in either the X or P quadrature which is chosen at random. An outcome of such a synchronous measurement is called a sample. This process is repeated until $2N$ measurements were performed on $2N$ quantum states, forming two strings of length $2N$.

Check of Abort Conditions and Sifting After having performed $2N$ measurements Alice and Bob check possible abort conditions of the generic protocol's actual implementation and abort if necessary. If they do not abort, they perform sifting, i.e.

they communicate which quadrature they measured. Samples measured with a different choice of quadrature are discarded leaving Alice and Bob with strings of length N in average. For collective attacks the discarded data can later be used for parameter estimation.

Parameter Estimation To perform parameter estimation Alice and Bob randomly choose a common subset of length k from the sifted data which they reveal. The actual procedure of the parameter estimation depends on whether collective or general attacks are considered. The details are therefore described in the respective Sections below. The output of the parameter estimation procedure is the number of secret bits ℓ, they can generate from their data.

Binning, Error Correction and Privacy Amplification Alice and Bob generate the raw key from their unrevealed measurement outcomes. For this purpose they map their samples to bins which were negotiated prior to the run of the protocol. For each sample they remember the index of the bin the sample was mapped to. Details will be given in the description of the respective protocol for security against collective and general attacks. The number of bins will be finite in both cases.

After binning, Alice and Bob have to make sure that they share the same raw key strings they proceed with. Because of the finite correlations between the two parts of the bipartite EPR state, errors are indispensable and have to be corrected by error correction algorithms. Error correction can either be processed by correcting Bob's data to match Alice's, which is called *direct reconciliation* or by correcting Alice's data to match Bob's which is called *reverse reconciliation.* When transmitting Bob's state through an optical fiber, reverse reconciliation enables larger distances as the eavesdropper's guess about Bob's state is worse than about Alice's as Bob's state is noisier [Gro03]. To check that they share the same string after error correction they perform a correctness test. This test is implemented by Alice and Bob each hashing their error corrected strings to a certain hash length using two-universal hash functions [Sti94] and comparing the outcomes.

Finally, Alice and Bob perform privacy amplification [Sti02, Ren05b, Ass06]. Using two-universal hash functions they reduce their raw key strings to the length calculated in the parameter estimation step. The correlations of the key to an eavesdropper are thereby removed from the strings, leaving Alice and Bob with a secret key.

5.3 Secure Key Length

In Section 5.1.1 we have already introduced ϵ_s-secrecy of a protocol to ensure universally composable security. In the following we will extend the security definitions to the protocol given above and then calculate the secret key rate.

5.3.1 Security Definitions

The security definitions follow the ones given in [Ren05a, Fur12b].

Robustness We call a protocol *robust* if it does not abort when no eavesdropper is present. This ensures that the protocol is not trivial.

Correctness Denoting Alice's key as S_A and Bob's key as S_B, a protocol is ϵ_c-correct if

$$\text{Probability}(S_A \neq S_B) \leq \epsilon_c \ .$$

Secrecy As introduced in Section 5.1.1, a protocol is ϵ_s-secret if

$$\frac{1}{2} p_{\text{pass}} \|\hat{\rho}_{S_A E} - \hat{\rho}_U \otimes \hat{\sigma}_E\| \leq \epsilon_s \ . \tag{5.4}$$

Here, p_{pass} denotes the probability that the protocol does not abort.

Security We call a protocol ϵ-secure if it is ϵ_c-correct and ϵ_s-secret with $\epsilon_c + \epsilon_s \leq \epsilon$.

5.3.2 Smooth Min-Max Entropies

In this section we will briefly introduce the formalism of smooth min- and max-entropies as they play a crucial role in calculating the secure key length. Although the smooth min- and max-entropies in the infinite dimensional case are defined using von Neumann algebras, we will stick here for the ease of presentation to the traditional approach using density operators on Hilbert spaces as the results will look the same. For the finite dimensional case we refer to [Ren05a], whereas for the extension to infinite dimensions we refer to [Fur11, Ber11, Fra12, Fur12a].

Let $\mathcal{H}$ be a Hilbert space. We define by $\mathcal{P}(\mathcal{H})$ the set of non-negative operators on $\mathcal{H}$. $\hat{\rho}$ is a density operator acting on $\mathcal{H}$, if $\hat{\rho} \in \mathcal{P}(\mathcal{H})$ and $\operatorname{Tr}\hat{\rho} = 1$.

The conditional min-entropy of a bipartite state $\hat{\rho}_{AB} \in \mathcal{P}(\mathcal{H}_A \otimes \mathcal{H}_B)$ with respect to $\hat{\sigma}_B \in \mathcal{P}(\mathcal{H}_B)$ is defined by

$$H_{\min}(\hat{\rho}_{AB}|\hat{\sigma}_B) = -\log_2 \inf\{\lambda \in \mathbb{R} | \lambda \mathbb{1} \otimes \hat{\sigma}_B \geq \hat{\rho}_{AB}\} \ , \tag{5.5}$$

with $H_{\min}(\hat{\rho}_{AB}|\hat{\sigma}_B) = -\infty$, if $\lambda \mathbb{1} \otimes \hat{\sigma}_B \geq \hat{\rho}_{AB}$ cannot be fulfilled for any λ. The min-entropy with respect to the subsystem B is defined as

$$H_{\min}(\hat{\rho}_{AB}|B) = \sup_{\hat{\sigma}_B \in \mathcal{P}(\mathcal{H}_B)} H_{\min}(\hat{\rho}_{AB}|\hat{\sigma}_B) \ . \tag{5.6}$$

The min-entropy has the interpretation of being the logarithm of the guessing probability of a classical variable X. The guessing of X is thereby assisted by a quantum state on Eve's system E depending on the classical value x [Fur11]. The density operator describing this cq-state is given by

$$\hat{\rho}_{XE} = \sum_{x \in X} P_X(x) |x\rangle\langle x| \otimes \hat{\rho}_E^x$$

with $P_X(x)$ being the probability distribution of X. The guessing probability is defined as the probability that Eve correctly guesses x by performing an optimal measurement on her state.

$$p_{\text{guess}} = \max_{\{\hat{E}_x\}} \sum_{x \in X} P_X(x) \operatorname{Tr}(\hat{\rho}_E^x \hat{E}_x) \ , \tag{5.7}$$

where $\{\hat{E}_x\}$ is the set of all possible measurements on Eve's system. The conditional min-entropy is then given by

$$p_{\text{guess}} = 2^{H_{\min}(X|E)} \ . \tag{5.8}$$

The max-entropy of $\hat{\rho}_{AB}$ conditioned on subsystem B is dual to the min-entropy and defined as

$$H_{\max}(\hat{\rho}_{AB}|B) = -H_{\min}(\hat{\rho}_{AE}|E) \ , \tag{5.9}$$

where $\hat{\rho}_{ABE}$ is a purification of $\hat{\rho}_{AB}$.

The smoothed versions of the min- and max-entropies take all states into account that are ϵ-close to $\hat{\rho}_{AB}$,

$$H_{\min}^{\epsilon}(\hat{\rho}_{AB}|B) = \sup_{\hat{\tilde{\rho}}_{AB} \in \mathbb{B}^{\epsilon}(\hat{\rho}_{AB})} H_{\min}(\hat{\tilde{\rho}}_{AB}|B) \ , \tag{5.10}$$

$$H_{\max}^{\epsilon}(\hat{\rho}_{AB}|B) = \inf_{\hat{\tilde{\rho}}_{AB} \in \mathbb{B}^{\epsilon}(\hat{\rho}_{AB})} H_{\max}(\hat{\tilde{\rho}}_{AB}|B) \ , \tag{5.11}$$

where $\mathbb{B}^{\epsilon}(\hat{\rho}_{AB})$ is the set of all states that are ϵ-close to $\hat{\rho}_{AB}$. Hence, the smoothed versions describe the min- and max-entropy of a state when we know the state only approximately. The duality condition of Eq. (5.9) is also valid for the smoothed versions, i.e.

$$H_{\max}^{\epsilon}(\hat{\rho}_{AB}|B) = -H_{\min}^{\epsilon}(\hat{\rho}_{AE}|E) \ . \tag{5.12}$$

An important property of the (smooth) min- and max-entropies is that they coincide with the von Neumann entropy in the limit of infinite identical but independed repetitions. For a state $\hat{\rho}_{AB} \in \mathcal{P}(\mathcal{H}_A \otimes \mathcal{H}_B)$ the state after n identical and independend repetitions is described by $\hat{\rho}_{AB}^{\otimes n}$. The *asymptotic equipartition property* of the smooth min- and max-entropies states that for any $\epsilon > 0$ and $n \geq \frac{8}{5} \log_2 \frac{2}{\epsilon^2}$

$$\frac{1}{n} H_{\min}^{\epsilon}(A^n|B^n) \geq H(A|B) - \frac{1}{\sqrt{n}} \Delta \tag{5.13}$$

and

$$\frac{1}{n} H_{\max}^{\epsilon}(A^n|B^n) \leq H(A|B) + \frac{1}{\sqrt{n}} \Delta \ , \tag{5.14}$$

if $H(A) < \infty$. Here,

$$\Delta = 4 \log_2 \left(2^{-\frac{1}{2} H_{\min}(A|B)} + 2^{\frac{1}{2} H_{\max}(A|B)} + 1 \right) \sqrt{\log_2 \frac{2}{\epsilon^2}} \ . \tag{5.15}$$

With this property the desired behaviour for the smooth min- and max-entropies can be seen

$$\lim_{\epsilon \to 0} \lim_{n \to \infty} \frac{1}{n} H_{\min}^{\epsilon}(A^n|B^n) = H(A|B) = \lim_{\epsilon \to 0} \lim_{n \to \infty} \frac{1}{n} H_{\max}^{\epsilon}(A^n|B^n) \ . \tag{5.16}$$

Another useful relation is the *entropic uncertainty relation*. For a state $\hat{\rho}_{ABE} \in \mathcal{P}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E)$ it reads

$$H_{\min}^{\epsilon}(X|B) + H_{\max}^{\epsilon}(Y|E) \geq -\log_2 c \ , \tag{5.17}$$

where $\hat{\rho}_{XB}$ is the cq-state after measuring $\hat{E}_A$ at Alice's subsystem, and $\hat{\rho}_{YE}$ is the cq-state after measuring $\hat{F}_A$ at the same subsystem. c is a constant describing the overlap between the measurement operators $\hat{E}$ and $\hat{F}$. It is given by $c = \max_{x,y} \| (\hat{E}_A^x)^{\frac{1}{2}} (\hat{F}_A^y)^{\frac{1}{2}} \|^2$. The entropic uncertainty relation can be used to estimate $H_{\min}^{\epsilon}$ by $H_{\max}^{\epsilon}$. The quality of the estimation is given by the constant c. This property will later be used to estimate the secure key length in the case of general attacks, cf. Section 5.5.

5.3.3 Privacy Amplification

Assume that Alice and Bob have already performed error correction and have obtained two identical raw key strings. As these strings still contain information possessed by Eve they have to perform so-called *privacy amplification* to remove her information. The result of this procedure is a new but shorter string that is uniformly distributed and uncorrelated to Eve. As Alice and Bob share the same strings we can reduce the description of privacy amplification to the bipartite problem involving only Alice and Eve in the following. Privacy amplification is implemented using a family of two-universal hash functions.

A hash function is a function $f : X \to K$ which maps a finite bit string X with length $|X|$ to a bit string K with length $|K| < |X|$. A set of such functions $\mathcal{F} = \{f\}$ is called a family of two-universal hash functions if any two distinct elements of X collide with probability of at most $\frac{1}{|K|}$ when the hash function f is drawn from $\mathcal{F}$ at random, i.e. [Sti94]

$$\underset{f\in\mathcal{F}}{\text{Probability}}(f(x) = f(y)) \leq \frac{1}{|K|} \quad \forall x, y \in X, x \neq y \ .$$

The leftover hash lemma states that using an input with sufficiently high entropy, the output of such a family of two-universal hash functions suffices the conditions of privacy amplification. Indeed the lemma was e.g. shown in [Ben95] for classical side-information and in [Tom11, Fur09, Fur12a] for quantum side-information. Hence, no matter whether Eve possesses classical or quantum side-information, applying a two-universal family of hash functions yields privacy amplification.

Given a cq-state $\hat{\rho}_{XE}$ which describes Alice's raw key string and Eve's side-information, the leftover hash lemma is given by

$$\langle \|\hat{T}_f(\hat{\rho}_{XE}) - \frac{1}{|K|}\hat{\rho}_U \otimes \hat{\sigma}_E\| \rangle_{\mathcal{F}} \leq \sqrt{|K| \cdot 2^{-H_{\min}(X|E)}} \ , \tag{5.18}$$

where $\hat{T}_f$ implements the hash function f, $\hat{\rho}_U = \sum_{k\in K} \frac{1}{|K|}|k\rangle\langle k|$ is the density operator describing the uniformly distributed keys, $\hat{\sigma}_E$ is the reduced state on Eve's subsystem and $\langle\cdot\rangle_{\mathcal{F}}$ is the expectation value over the hash functions f. The left hand side of Eq. (5.18) describes the distance of Alice's raw key given Eve's side information after hashing to a uniformly distributed string which is independent of Eve. The leftover hash lemma states that this distance can be made arbitrarily small by choosing $|K|$ appropriately small.

This result can be generalized to the smooth min-entropy by [Fur12a]

$$\langle \|\hat{T}_f(\hat{\rho}_{XE}) - \frac{1}{|K|}\hat{\rho}_U \otimes \hat{\sigma}_E\| \rangle_{\mathcal{F}} \leq \sqrt{|K| \cdot 2^{-H^{\epsilon}_{\min}(X|E)}} + 4\epsilon \ , \tag{5.19}$$

Using this result we can now derive a formula for the secure key length.

5.3.4 Finite-Key Length

We assume that Alice and Bob have already performed the quantum part of the protocol, checked the abort conditions and parameter estimation tests and binned their data to retrieve the raw key strings X_A and X_B. In the next step of the protocol they perform error correction. We will assume direct reconciliation, i.e. Alice communicates ℓ_{EC} bits to Bob who changes his key X_B to match Alice's. After error correction Alice and Bob check whether their keys are the same. For this purpose Alice draws a hash function from a family of two-universal hash functions at random and sends Bob both, the hash of her raw key string and the hash function. The hash function she uses maps the whole raw key string to a string of length $\log_2 \frac{1}{\epsilon_c}$ according to the correctness definition. Bob then checks whether he gets the same hash by applying the hash function to his raw key string and aborts the protocol if he does not. The correctness test leaks $\log_2 \frac{1}{\epsilon_c}$ bits to Eve through the public communication. In the following we denote the random variable which corresponds to the communication due to error correction, by M. The number of revealed bits is thereby assumed to be $\log_2|M| = \ell_{\mathrm{EC}} + \log_2 \frac{1}{\epsilon_c}$.

To derive the secret key length we start at the secrecy definition (5.4) which can be bounded by the privacy amplification result of Eq. (5.19) by applying a hash function drawn from a two-universal family of hash functions at random to the raw key string X_A. Thereby we denote the cq-state shared by Alice and Eve after successful parameter estimation by $\hat{\rho}_{X_A E}$. Substituting K with the alphabet S_A, which has a length of $\ell = \log_2|S_A|$, yields [Fur12a]

$$\frac{1}{2}\|\hat{\rho}_{X_A E} - \hat{\rho}_U \otimes \hat{\sigma}_E\| \leq \sqrt{2^{\ell - H^{\epsilon}_{\min}(X_A|EM)-2}} + 2\epsilon \leq \frac{\epsilon_s}{p_{\mathrm{pass}}} \ , \tag{5.20}$$

where the bound on the right is given by Eq. (5.4). This condition is fulfilled for

$$\ell \leq H^{\epsilon}_{\min}(X_A|EM) - 2\log_2 \frac{p_{\mathrm{pass}}}{\epsilon_1} + 2 \ , \tag{5.21}$$

where ϵ_1 is defined by $\epsilon \leq (\epsilon_s - \epsilon_1)/(2p_{\mathrm{pass}})$.

This can be further simplified by using [Fur12a]

$$H^{\epsilon}_{\min}(X_A|EM) \geq H^{\epsilon}_{\min}(X_A M|E) - \log_2|M| \geq H^{\epsilon}_{\min}(X_A|E) - \log_2|M| \ ,$$

and $-\log_2 p_{\mathrm{pass}} \geq 0$ which yields

$$\ell \leq H^{\epsilon}_{\min}(X_A|E) - \ell_{\mathrm{EC}} - \log_2 \frac{1}{4\epsilon_1^2\epsilon_c} \ . \tag{5.22}$$

In Sections 5.4 and 5.5 we will see how to estimate $H^{\epsilon}_{\min}(X_A|E)$ in the case of collective and coherent attacks.

5.3.5 Estimation of the Error Correction Leakage Term

In a real implementation of the quantum key distribution protocol given above, the number of bits ℓ_{EC} communicated from Alice to Bob or from Bob to Alice used to perform error correction can be exactly determined after each run. But for the theoretical analysis of possible key rates, ℓ_{EC} has to be estimated. In the case of infinite repetitions, i.e. $n \to \infty$, a lower bound for ℓ_{EC} is given by [Sle73, Sca09]

$$\ell_{\text{EC}} = \lambda H(X_A|X_B) \ , \tag{5.23}$$

where we assumed direct reconciliation, i.e. communication from Alice to Bob. Here, the parameter $\lambda \geq 1$ reflects that existing error correction algorithms do not achieve the theoretical bound of $H(X_A|X_B)$. An intuitive interpretation of Eq. (5.23) can be gained from the interpretation of the conditional entropy that describes the uncertainty about X_A in the case X_B is known. Hence, Alice has to send $H(X_A|X_B)$ bits to Bob to enable him to know Alice's string with certainty. More often instead of the leakage parameter λ, the error correction efficiency β is used. The number of perfectly correlated bits that can be extracted from partially correlated strings X_A and X_B is given by their mutual information [Sca09]. The efficiency of an algorithm to achieve this, is described by β with $0 < \beta \leq 1$. Hence,

$$\text{number of extractable bits} = \beta I(X_A : X_B) \ . \tag{5.24}$$

Using this, the leakage term can be written as

$$\begin{align}
\ell_{\text{EC}} &= \lambda H(X_A|X_B) \tag{5.25}\\
&= \lambda \left(H(X_A) - I(X_A : X_B) \right) \tag{5.26}\\
&= H(X_A) - \beta I(X_A : X_B) \ , \tag{5.27}
\end{align}$$

which connects the leakage parameter λ and the error correction efficiency β by

$$\lambda = \frac{H(X_A) - \beta I(X_A : X_B)}{H(X_A|X_B)} \ . \tag{5.28}$$

For our simulations in the following Chapters we will assume that the leakage term is close to the optimum for infinite repetitions.

5.3.6 Key Rate in the Regime of Infinite Samples

Taking Eq. (5.22) the key rate $r = \frac{\ell}{n}$ in the limit of $n \to \infty$ and $\epsilon \to 0$ becomes

$$\begin{aligned} r &= \lim_{n\to\infty} \lim_{\epsilon \to 0} \frac{\ell}{n} && (5.29) \\ &= \lim_{n\to\infty} \lim_{\epsilon \to 0} \frac{1}{n} \left(H^{\epsilon}_{\text{min}}(X_A|E) - \ell_{\text{EC}} - \log_2 \frac{1}{4\epsilon_1^2 \epsilon_c} \right) && (5.30) \\ &= H(X_A|E) - H(X_A|X_B) && (5.31) \\ &= I(X_A : X_B) - I(X_A : E) \ , && (5.32) \end{aligned}$$

where we have used Eq. (5.16), and Eq. (5.23) for the error correction leakage term with perfect error correction, i.e. $\lambda = 1$. Assuming imperfect error correction yields

$$r = \beta I(X_A : X_B) - I(X_A : E) \ . \tag{5.33}$$

This result is the Devetak-Winter bound for the secure key rate [Dev05, Sca09]. $I(X_A : E)$ is thereby known as the Holevo bound, usually written as $\chi(X_A : E)$.

5.4 Collective Attacks

We will now use the results of the last section to calculate the secure key length with the restriction of Eve to collective attacks. Collective attacks are attacks where Eve possesses a quantum memory and measures her states collectively. However, all states are measured with the same operation. Although Eve is restricted to this type of attacks, these attacks are rather powerful. Due to Eve's restriction to perform the same attacks on each quantum state, the distributed entangled states can be assumed to be identical and not correlated to each other. This is exactly the situation where the asymptotic equipartition property of Eq. (5.13) can be applied. The calculation presented in this section was first carried out in [Fur12b] and later extended to states with asymmetries in the field quadrature variances in [Ebe13a].

5.4.1 Protocol

The protocol for security against collective attacks is almost the same as the generic protocol described in Section 5.2.

Preliminaries Prior to executing the protocol Alice and Bob negotiate the binning intervals, the number of measured samples, the number of samples k used for parameter estimation and the security parameters.

Distribution of Quantum States and Homodyne Measurements This step is performed as described in the generic protocol.

Sifting Alice and Bob communicate the quadratures they used to measure their samples. Samples measured in different quadratures are discarded from the sample strings but are later used for parameter estimation. The discarded samples are therefore publicly announced.

Parameter Estimation Alice and Bob choose randomly a common subset of k samples from their sample strings which they reveal. From this data and the data discarded during sifting they reconstruct the covariance matrix as described in Chapter 3.5. In particular, they estimate a confidence set $\mathcal{C}_{\epsilon_{\mathrm{pe}}}$ with the property that with probability $1 - \epsilon_{\mathrm{pe}}$ the real covariance matrix lies within $\mathcal{C}_{\epsilon_{\mathrm{pe}}}$.

Discarding Samples from X or P Quadrature (Optional) When using entangled states that are generated from a single squeezed-light source, the samples measured in the anti-squeezed quadrature might be discarded and then publicly announced for use in the parameter estimation step. To take into account the three possibilities, namely discarding samples measured in the X quadrature, discarding samples measured in the P quadrature and discarding nothing at all, we introduce a parameter p_X which describes the probability of a remaining sample being measured in the X quadrature. This yields $p_X = 0$ for discarding X measurements, $p_X = 1$ for discarding P measurements and $p_X \approx 0.5$ for discarding none of them. For the latter the actual value of p_X depends on the run as we assume a finite number of measurements.

Binning To generate the raw key Alice and Bob map their unrevealed samples to bins $I_0 = \big(-\infty, -\alpha_{\{X,P\}} + \delta_{\{X,P\}}\big]$, $I_1 = \big(-\alpha_{\{X,P\}} + \delta_{\{X,P\}}, -\alpha_{\{X,P\}} + 2\delta_{\{X,P\}}\big]$, $\dots$, $I_{\frac{2\alpha}{\delta}-1} = \big(\alpha_{\{X,P\}} - \delta_{\{X,P\}}, \infty\big)$. Each sample is assigned the index of the bin the sample fell into, i.e. the alphabets of the raw keys are given by $\chi_X = \Big\{0, 1, \dots, \frac{2\alpha_X}{\delta_X} - 1\Big\}$ and $\chi_P = \Big\{0, 1, \dots, \frac{2\alpha_P}{\delta_P} - 1\Big\}$. In practice, we always choose α such that no sample exceeds α. In that sense, only δ is a free parameter in the protocol.

Post Selection (Optional) To reduce errors Alice and Bob can perform a simple post selection step. After binning Alice searches her data for samples which were mapped to a certain bin and sends Bob a remove flag for those samples. The two parties then remove the flagged samples from their sample strings. This procedure can be performed for more than one bin and also from Bob to Alice.

Error Correction After binning Alice and Bob have to ensure that they both proceed with the same raw key. To achieve this they sacrifice ℓ_{EC} bits by classical communication. The size of ℓ_{EC} will be estimated for the simulations as described in Section 5.3.5. For an actual run of the protocol, ℓ_{EC} can be directly measured. After the run of the error correction algorithm Alice and Bob perform a correctness test as in the generic protocol.

Estimation of the Secret Key Length Alice and Bob compute the secret key length ℓ taking into account the number of bits used for error correction. If the key length is lower than zero they abort. Otherwise they proceed with the next step.

Privacy Amplification To obtain bit strings only known to Alice and Bob, both parties map the alphabet χ to a binary representation. Afterwards privacy amplification is implemented in the way described in the generic protocol.

5.4.2 Secure Key Length

For the calculation of the secure key length we start at the key length formula of Eq. (5.22) for the generic protocol but assume reverse information reconciliation, i.e. classical communication from Bob to Alice. Let us denote the classical variable corresponding to the n measurement outcomes of Alice and Bob after binning but before error correction and privacy amplification by X_A^n and X_B^n. We denote by $\hat{\rho}_{X_A^n X_B^n E^n}$ the corresponding cq-state conditioned on the event that the protocol passes, where E^n is the (infinite dimensional) quantum system of the eavesdropper. Under the assumption of collective attacks $\hat{\rho}_{X_A^n X_B^n E^n}$ has tensor-product structure, hence, $\hat{\rho}_{X_A^n X_B^n E^n} = \hat{\rho}_{X_A X_B E}^{\otimes n}$. Applying the asymptotic equipartition property from Eq. (5.13) yields

$$H_{\min}^{\epsilon}(X_B|E) \geq nH(X_B|E) - \sqrt{n}\Delta \ , \tag{5.34}$$

where Δ is given by [Fur12b]

$$\Delta = 4\log_2\left(2^{\frac{1}{2}H_{\max}(X_B)+1} + 1\right)\sqrt{\log_2 \frac{8}{(\epsilon_s - \epsilon_1)^2}} \ . \tag{5.35}$$

To compute $H(X_B|E)$ we use that the classical-quantum state $\hat{\rho}_{X_B E}$ has the form $\hat{\rho}_{X_B E} = p_X|X\rangle\langle X|_\theta \otimes \hat{\rho}_{X_B E}^X + (1-p_X)|P\rangle\langle P|_\theta \otimes \hat{\rho}_{X_B E}^P$ where $\hat{\rho}_{X_B E}^X$ and $\hat{\rho}_{X_B E}^P$ are the states obtained when Alice and Bob measured the X or P quadrature, respectively. Thereby the classical variable θ describes the system which keeps track of the measured quadrature angle and is known by the eavesdropper, [Ebe13a]

$$\begin{aligned}H(X_B|E\theta) &= H(X_B E\theta) - H(E\theta)\\ &= H(\theta) + \sum_\theta p_\theta H(X_B E)_\theta - H(\theta) - \sum_\theta p_\theta H(E)_\theta\\ &= p_X H(X_B|E)_X + (1-p_X) H(X_B|E)_P \ .\end{aligned}$$

Assuming Gaussian attacks we introduce a confidence set $\mathcal{C}_{\epsilon_{\mathrm{pe}}}$ which contains all covariance matrices compatible with the k samples used for parameter estimation. We assume that the parameter estimation is performed such that the real covariance matrix lies within $\mathcal{C}_{\epsilon_{\mathrm{pe}}}$ with probability of at least $1-\epsilon_{\mathrm{pe}}$. The length of the secure key length can then be bounded by

$$\ell \leq n \cdot \inf_{\gamma \in \mathcal{C}_{\epsilon_{\mathrm{pe}}}} \sum_\theta p_\theta H(X_B|E)_{\gamma,\theta} - \sqrt{n}\Delta - \ell_{\mathrm{EC}} - \log_2 \frac{1}{\epsilon_s^2 \epsilon_c} \ . \tag{5.36}$$

The infimum is thereby taken over the confidence set and we have chosen $\epsilon_1 = \frac{\epsilon_s}{2}$, because for large enough n the logarithm is neglegible small. As Eve's system purifies the state shared by Alice and Bob we can use the self-duality property of the von Neumann entropy, $H(E)_\gamma = H(AB)_\gamma$. Thus,

$$H(X_B|E)_{\gamma,\theta} = H(E|X_B)_{\gamma,\theta} + H(X_B)_{\gamma,\theta} - H(AB)_\gamma \ . \tag{5.37}$$

Using partial homodyne detecion, cf. Chapter 2.13, and results from [Fur12b] yields

$$H(E|X_B)_{\gamma,X} \geq H(E)_{\gamma(X=0)} = H\left(A - C(M_X B M_X)^{\mathrm{MP}} C^T\right)_\gamma$$

and

$$H(E|X_B)_{\gamma,P} \geq H(E)_{\gamma(P=0)} = H\left(A - C(M_P B M_P)^{\mathrm{MP}} C^T\right)_\gamma \ ,$$

where $H(E)_{\gamma(\{X,P\}=0)}$ is the post-measurement state at the eavesdropper's side when Bob measured $X=0$ or $P=0$. The bipartite covariance matrix is written in block form as in Eq. (2.73), M_X and M_P are defined as in Chapter 2.13 and MP denotes the Moore-Penrose inverse.

The Shannon entropy of the classical variable X_B, $H(X_B)_{\gamma,\theta}$, is given by

$$H(X_B)_{\gamma,\theta} = p_X H(X_B)_{\gamma,X} + (1-p_X) H(X_B)_{\gamma,P} \tag{5.38}$$

with

$$H(X_B)_{\gamma,X} = -\sum_y p^X_{X_B}(y) \log_2 p^X_{X_B}(y) \ , \tag{5.39}$$

where $p^X_{X_B}(y)$ is the probability that a measurement outcome from Bob, measured in the X quadrature, falls into bin y. Given the boundaries of this bin, x^y_B and x^{y+1}_B, $p^X_{X_B}(y)$ can be calculated by

$$\begin{aligned} p^X_{X_B}(y) &= \int_{x^y_B}^{x^{y+1}_B} \mathrm{d}x \frac{1}{\sqrt{2\pi\gamma_{3,3}}} \exp\left(-\frac{x^2}{2\gamma_{3,3}}\right) \\ &= \frac{1}{2}\left(\operatorname{erf}\left(\frac{x^{y+1}_B}{\sqrt{2\gamma_{3,3}}}\right) - \operatorname{erf}\left(\frac{x^y_B}{\sqrt{2\gamma_{3,3}}}\right)\right) \ , \end{aligned}$$

in the case that no post selection was performed. Here, $\gamma_{3,3}$ denotes the entry in the covariance matrix corresponding to the X quadrature variance of Bob's subsystem, and erf is the error function.

Similarly $H_{\max}(X_B)$, which is part of Δ, can be estimated by [Fur11]

$$H_{\max}(X_B) \leq 2\log_2\left(\sqrt{p_X}\sum_y \sqrt{p^X_{X_B}(y)} + \sqrt{(1-p_X)}\sum_y \sqrt{p^P_{X_B}(y)}\right) \ . \tag{5.40}$$

In a real run of this protocol both $H(X_B)$ and $H_{\max}(X_B)$ can be calculated directly from Bob's measurement outcomes. Thus, the infimum is only taken of

$$H(E)_{\gamma(\{X,P\}=0)} - H(AB)_\gamma \ .$$

Plugging it all together, the key rate, defined as $r = \frac{\ell}{n}$, has the form

$$\begin{aligned} r = \frac{\ell}{n} = &\inf_{\gamma\in\mathcal{C}_{\epsilon_{\mathrm{pe}}}} p_X \left[H(E|X_B)_{\gamma,X} + H(X_B)_{\gamma,X}\right] \\ &+ (1-p_X)\left[H(E|X_B)_{\gamma,P} + H(X_B)_{\gamma,P}\right] - H(AB)_\gamma \\ &- \frac{1}{\sqrt{n}}\Delta - \frac{\ell_{\mathrm{EC}}}{n} - \frac{1}{n}\log_2\frac{1}{\epsilon_s^2\epsilon_c} \ . \end{aligned} \tag{5.41}$$

5.4.3 Parameter Estimation

To calculate the secure key rate we need to construct the confidence set $\mathcal{C}_{\epsilon_{\mathrm{pe}}}$, which is defined such that the covariance matrix describing the real state lies within $\mathcal{C}_{\epsilon_{\mathrm{pe}}}$ with probability $1-\epsilon_{\mathrm{pe}}$. As our states are two-mode squeezed vacuum states, only the second order moments do not vanish and the state is fully described by its covariance matrix. It is reconstructed during the parameter estimation step from the discarded samples and the revealed common subset of length k using a maximum likelihood estimator. The sample covariance matrix is estimated by

$$\tilde{\gamma}_{\mu\nu} = \frac{1}{n_{\mu\nu}} \sum_{i=1}^{n_{\mu\nu}} x_i^\mu x_i^\nu \ ,$$

where x_i^μ and x_i^ν are the samples measured simultaneously by Alice and Bob in μ and ν quadrature, respectively. $n_{\mu\nu}$ is the number of samples used for the covariance estimation. The distribution of the sample covariance matrix $\tilde{\gamma}$ is given by [Joh07]

$$n\tilde{\gamma} \sim W_4(\gamma, n-1) \ ,$$

where $W_4(\gamma, n-1)$ is the Wishart distribution. Hence, the standard deviation for a single entry of the covariance matrix takes the form

$$\sigma_{\mu\nu} \approx \sqrt{\frac{\tilde{\gamma}_{\mu\nu}^2 + \tilde{\gamma}_{\mu\mu}\tilde{\gamma}_{\nu\nu}}{n_{\mu\nu}}} \ .$$

For a sufficiently large number of samples the confidence set is constructed by

$$\mathcal{C}_{\epsilon_{\text{pe}}} = \left\{\gamma | \tilde{\gamma}_{\mu\nu} - z_{\epsilon_{\text{pe}}}\sigma_{\mu\nu} \leq \gamma_{\mu\nu} \leq \tilde{\gamma}_{\mu\nu} + z_{\epsilon_{\text{pe}}}\sigma_{\mu\nu}\right\} \ , \tag{5.42}$$

where $z_{\epsilon_{\text{pe}}}$ is chosen such that

$$1 - \operatorname{erf}\left(\frac{z_{\epsilon_{\text{pe}}}}{\sqrt{2}}\right) \leq \epsilon_{\text{pe}}$$

is fulfilled.

5.5 General Attacks

While collective attacks are relatively easy to analyse, the security when we make no assumptions on the attacks of the eavesdropper, is hard to proof in the continuous variable regime. The following protocol allows to distill a key which cannot be eavesdropped even with general attacks. It was published in [Fur12b].

5.5.1 Protocol

The protocol for security against general attacks is almost the same as the generic protocol described in Section 5.2.

Preliminaries Prior to executing the protocol Alice and Bob negotiate the binning interval length δ and the cut-off value α, the number of measured samples $2N$, the number of samples k used for parameter estimation, and the security parameters.

Distribution of Quantum States and Homodyne Measurements This step is performed as in the generic protocol.

Check of Abort Condition and Sifting Alice and Bob check their measurement results whether they are within the allowed region $[-\alpha, \alpha]$. If they find a value outside this interval, they abort the protocol. Otherwise they perform sifting as in the generic protocol.

Binning After sifting Alice and Bob map their remaining samples to the bins $I_0 = (-\infty, -\alpha+\delta]$, $I_1 = (-\alpha+\delta, -\alpha+2\delta]$, ..., $I_{\frac{2\alpha}{\delta}-2} = (\alpha-2\delta, \alpha-\delta]$, $I_{\frac{2\alpha}{\delta}-1} = (\alpha-\delta, \infty)$. For each sample they remember the index of the bin the sample was mapped to, i.e. the outcome range is $\chi = \left\{0, 1, \ldots, \frac{2\alpha}{\delta} - 1\right\}$ with $|\chi| = \frac{2\alpha}{\delta}$.

Parameter Estimation For parameter estimation Alice and Bob choose randomly a common subset of length k from the sifted and binned data which they reveal. The parameter estimation test is performed by calculating the (generalized) Hamming distance

$$d_{\mathrm{pe}}(X_A^{\mathrm{pe}}, X_B^{\mathrm{pe}}) = \frac{1}{k} \sum_{\mu=1}^{k} |(X_A^{\mathrm{pe}})_\mu - (X_B^{\mathrm{pe}})_\mu| \ , \tag{5.43}$$

where X_A^{pe} and X_B^{pe} are the revealed binned sample strings from Alice and Bob, respectively.

Error Correction By performing error correction Bob corrects his binned data to match Alice's. During the run of the algorithm they track the number of communicated bits. Reverse reconciliation is currently not supported by the security proof of the protocol [Fur12b]. After error correction the correctness is determined as in the generic protocol.

Estimation of the Key Length With the number of bits communicated during error correction Alice and Bob can calculate the number of secret bits.

Privacy Amplification Using almost two-universal hash functions Alice and Bob reduce their raw keys to the length calculated in the last step. This procedure provides Alice and Bob a secret key which is unknown to the eavesdropper.

5.5.2 Secure Key Length

We recall the secure key length for the generic protocol from Eq. (5.22) which reads

$$\ell \leq H^{\epsilon}_{\min}(X_A|E) - \ell_{\mathrm{EC}} - \log_2 \frac{1}{4\epsilon_1^2\epsilon_c} \ . \tag{5.44}$$

Since we do not restrict the eavesdropper to a certain class of attacks, we cannot, for instance, use the asymptotic equipartition theorem as it was possible for the restriction to collective attacks. While the smooth min-entropy cannot be calculated for impure two-mode squeezed states, it can be estimated using the entropic uncertainty relation from Eq. (5.17). Its application yields [Fur12a]

$$\ell \leq n \cdot \log_2 \frac{1}{c(\delta)} - H^{\epsilon'}_{\max}(X_A|X_B) - \ell_{\mathrm{EC}} - \log_2 \frac{1}{4\epsilon_1^2\epsilon_c} \ , \tag{5.45}$$

where we have used that the overlap of a sequence of n measurements is c^n. The overlap $c(\delta)$ is thereby given by

$$c(\delta) = \frac{\delta^2}{2\pi} S_0^{(1)} \left(1, \frac{\delta^2}{4}\right)^2 \ , \tag{5.46}$$

where $S_0^{(1)}$ is the radial prolate spheroidal wave function of the first kind. For small δ it can be approximated by $S_0^{(1)}\left(1, \frac{\delta^2}{4}\right) \approx 1$.

The remaining smooth max-entropy can be estimated by

$$H^{\epsilon'}_{\max}(X_A|X_B) \leq n \log_2 \gamma(d_{\mathrm{pe}} + \mu) \ , \tag{5.47}$$

where

$$\gamma(t) = (t + \sqrt{1+t^2}) \left(\frac{t}{\sqrt{1+t^2} - 1}\right)^t \tag{5.48}$$

and

$$\mu = \frac{2\alpha}{\delta} \sqrt{\frac{N(k+1)}{nk^2} \ln \frac{1}{\epsilon_s - \epsilon_1 - 2\sqrt{2g(p_X^\alpha, p_P^\alpha, N)}}} \ . \tag{5.49}$$

Remember, that N is the number of samples left after sifting, k is the number of samples used for parameter estimation and $n = N - k$. $g(p_X^\alpha, p_P^\alpha, N)$ is the pass probability, i.e. the probability that no sample in the amplitude and phase quadrature is outside of $[-\alpha, \alpha]$. Thereby, p_X^α and p_P^α are the probabilities that the modulus of a single sample measured in the amplitude and phase quadrature, respectively, does not exceed α. Thus,

$$g(p_X^\alpha, p_P^\alpha, N) = 1 - (p_X^\alpha p_P^\alpha)^{\frac{N}{2}} \ . \tag{5.50}$$

CHAPTER 6

Realization of Quantum Key Distribution under Collective Attacks

Overview

This chapter describes the realization of a table-top continuous-variable QKD system under collective attacks using the EPR entangled states characterized in Chapter 4. Collective attacks are a certain type of attacks that are, although a restriction to an eavesdropper, experimentally difficult to implement. For a collective attack the eavesdropper has a quantum memory and measures all his states collectively using the same operation. The employed protocol for collective attacks was introduced in Chapter 5 and takes the finite key size into account.

This chapter is organized as follows: Section 6.1 presents simulation results of the secure key rate for EPR entangled states generated by superimposing a squeezed vacuum mode with a vacuum mode. The generation and characterization of such entangled states is described in Chapter 4.4. By omitting samples measured in the anti-squeezed quadrature, which are less correlated than samples measured in the squeezed quadrature, reasonable distances between Alice and Bob can be achieved when sending one of the entangled modes through an optical fiber. While the necessary resources to generate entanglement are reduced to a minimum by using such states, EPR entangled states generated by superimposing two squeezed vacuum states, cf. Chapter 4.5, provide better key rates. Simulations for such states are shown in Section 6.2. The experimental implementation of a setup which is able to perform many measurements that are randomly chosen between the amplitude and phase quadrature, is presented in Section 6.3. Section 6.4 describes the generation of quantum random numbers by measuring the field quadratures of a vacuum state. The random numbers were utilized for the random choice of quadratures by Alice and Bob. Section 6.5 describes the results of the performed table-top QKD. The first part of this section is devoted to the verification of some of the simulation results, while the second part describes the generation of a secret key using a post selection technique, cf. Chapter 5. Section 6.6 proposes an experimental setup of a synchronized remote detector which can be used to place Bob at another location. Expected secure key rates for a distribution of a secret key between the Institute for Gravitational Physics and the Institute of Quantum Optics in Hanover, are presented. Section 6.7 summarizes the results.

6.1 Secure Key Rates for Entanglement Using a Single Squeezed Vacuum Resource

In this section the secure key rate is investigated that can be obtained when performing the protocol described in Chapter 5.4 using entanglement generated by superimposing a squeezed vacuum mode with a vacuum mode at a balanced beam splitter. The experimental setup used to generate such entangled states is described in Chapter 4.4. The starting point for the investigation is the reconstructed covariance matrix of the measured states given in Eq. (4.10).

Figure 6.1 shows the key rate given in secure bits normalized to the number of measured samples versus the number of measured samples. Only samples from the X quadrature were taken into account for raw key generation ($p_X = 1$). The security parameters were chosen to be $\epsilon_c = \epsilon_s = \epsilon_{\text{pe}} = 10^{-16}$ and α was chosen as 8 times the standard deviation of the X quadrature sample distribution, cf. Chapter 5.4. The number of samples k revealed for parameter estimation was optimized to yield a maximal number of secure bits in the key. To improve the parameter estimation we assumed the diagonal entries of the covariance matrix to be computed from all measured samples in the respective quadratures and the covariances to be computed from the omitted samples or from the k revealed samples, respectively. The error correction efficiency was assumed to be $\beta = 0.9$. The different curves in the figure are plotted for a different number of intervals $2^{n_{\text{bits}}}$, yielding interval lengths of $\delta = 2\alpha/2^{n_{\text{bits}}}$. From the figure we read that the maximal key rate is achieved with $n_{\text{bits}} \geq 6$. For 10^9 samples the key rate is about 0.16 bits/sample and even for 10^8 samples it is not much less with about 0.13 bits/sample.

Figure 6.2 shows the same simulations as Fig. 6.1 but this time with the X quadrature measurements omitted ($p_X = 0$). Due to the lower correlations in the P quadrature the key rate drops below 0.08 bits/sample, reaching its maximum for $n_{\text{bits}} \geq 8$. The number of samples necessary to reach a positive key rate is about the same as when omitting the P quadrature samples.

As the key rates for both quadratures alone are positive, a key can, in principle, be

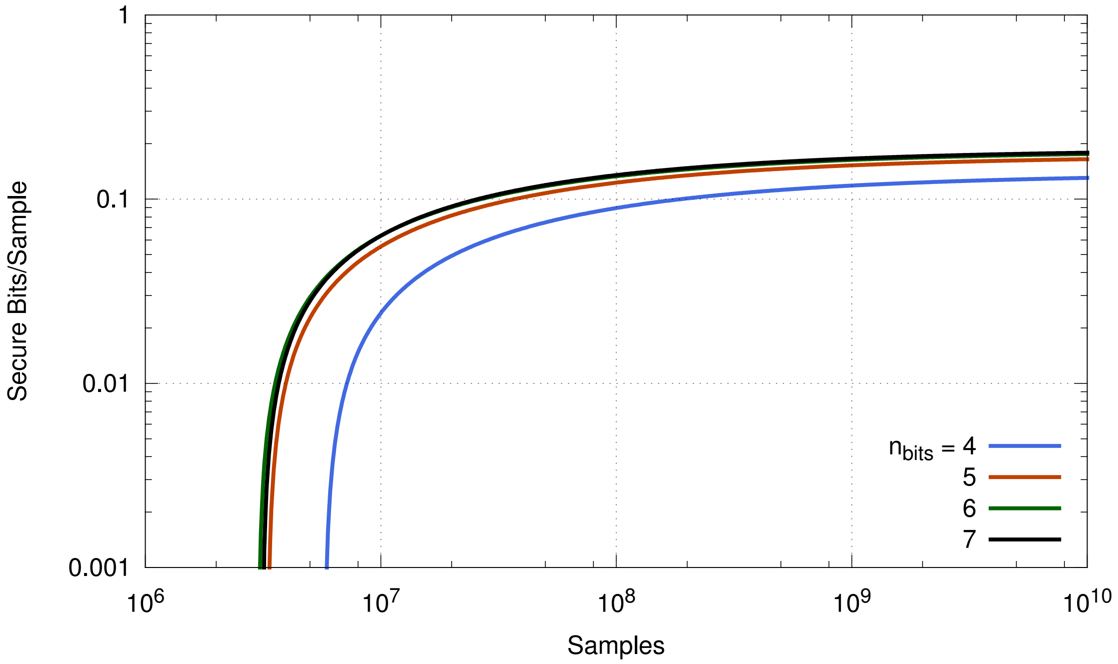


Figure 6.1: Secure key rate in secure bits per measured sample versus the number of measured samples. Here, only X quadrature measurements are included, i.e. $p_X = 1$. The number of samples k used for parameter estimation was optimized for each curve and each number of measured samples to yield a maximal number of secure bits.

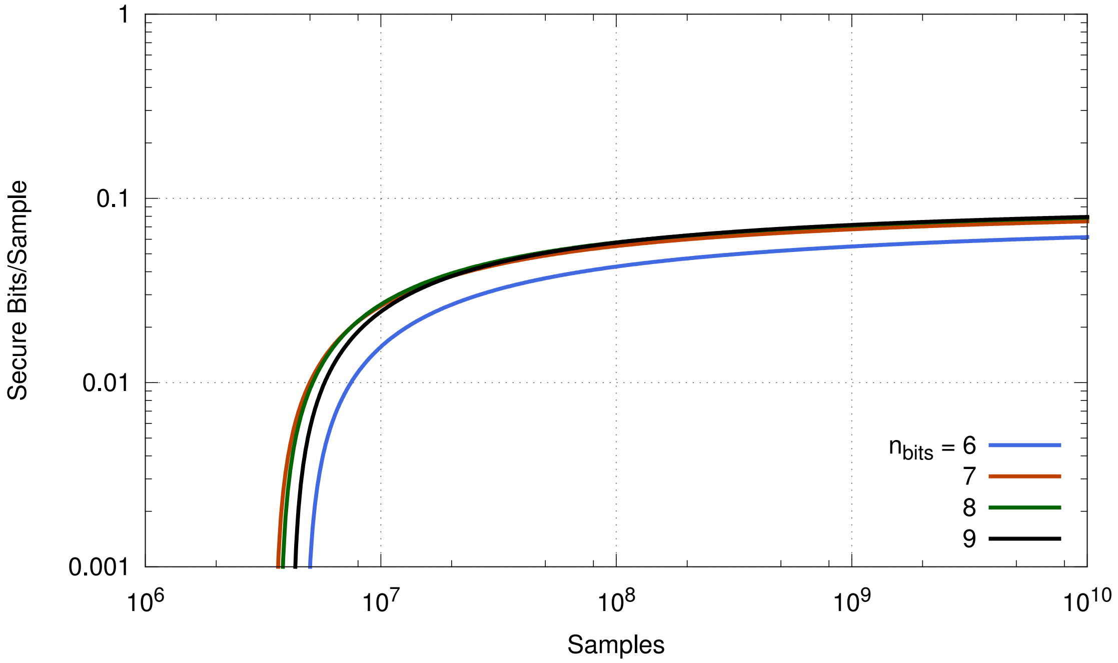


Figure 6.2: Secure key rate in secure bits per measured sample versus the number of measured samples. Here, only P quadrature measurements are included, i.e. $p_X = 0$. The number of samples k used for parameter estimation was optimized for each curve and each number of measured samples to yield a maximal number of secure bits.

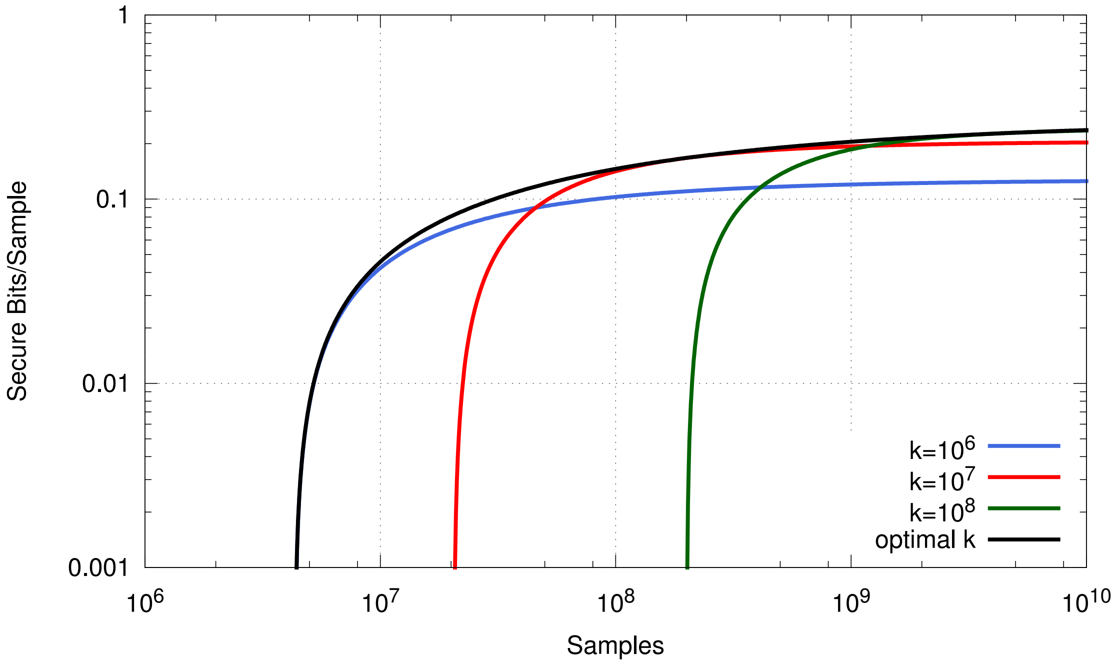


Figure 6.3: Number of secure bits per measured sample versus the number of measured samples. Here, both X and P quadrature measurements are included, i.e. $p_X = 0.5$. $n_{\text{bits}} = 6$ for the X quadrature and $n_{\text{bits}} = 8$ for the P quadrature. The number of samples k used for parameter estimation was optimized for the black solid curve to yield a maximal number of secure bits. The other curves are plotted with a fixed k.

generated from the X and P quadrature samples independently by first considering only samples from the X quadrature and then considering only samples from the P quadrature. The security analysis above allows us to simplify this process and to generate a key from both quadratures simultaneously. For this purpose we set $p_X = 0.5$. The key rate for this situation is shown in Fig. 6.3 with $n_{\text{bits}} = 6$ for the X quadrature and $n_{\text{bits}} = 8$ for the P quadrature as determined from the previous two figures. The black curve in the figure shows the key rate with an optimized number of samples k used for parameter estimation. To see the effect of k also curves with a fixed number of $k = 10^6$, 10^7 and 10^8 are plotted. As the number of secure bits per sample with about 0.20 bits/sample at 10^9 samples is larger than when omitting the P quadrature samples, it is advantageous to draw a key from both quadratures in a table-top setup.

Figure 6.4 shows the key rate for $n_{\text{bits}} = 6$ versus the distance between Alice and Bob when both parties are connected with an optical standard telecommunication fiber with an attenuation of 0.2 dB/km. For the calculation we assumed that the entanglement source is located at Alice's site and that the eavesdropper only has

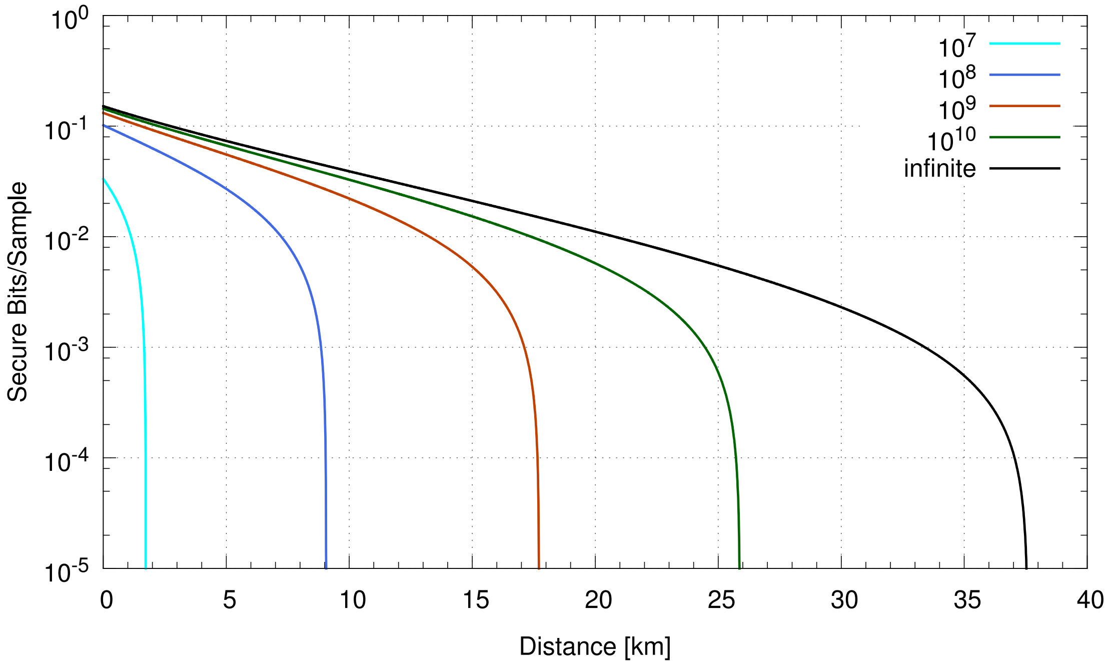


Figure 6.4: Secure key rate versus distance when sending one part of the entangled beam through an optical fiber. The key rate is given as the number of secure bits per measured sample, i.e. before sifting. We assumed a coupling efficiency of 95 % into the optical fiber and an optical loss of 0.2 dB/km. The curves are plotted for different number of measured samples.

access to the subsystem which is transmitted to Bob through the fiber and is therefore affected by optical loss of the transmission line. In addition to the optical attenuation of the fiber we assumed a coupling efficiency of the free beam to the fiber of 95 % as measured in [Meh10]. According to [Lod05], who considered a similar system, no excess noise is introduced by the fiber. Excess noise introduced by the homodyne detector's electronic dark noise instead is already included in the covariance matrix given in Eq. (4.10). Furthermore, we assumed that phase noise is not present in the setup as the local oscillator for homodyne detection could be served by an auxiliary laser at Bob's site which is phase locked to the control beam accompanying the entangled mode. Besides using reverse information reconciliation, all samples measured in the P quadrature were omitted ($p_X = 1$). Taking into account only samples from the P quadrature would yield a maximum transmission line length for an infinite number of measurements of 3 km and taking into account both would yield about 9 km in comparison to about 37.5 km when only samples from the squeezed quadrature are considered. The curves in the figure are calculated for different numbers of measured samples, including a curve calculated for an infinite number of samples, which is shown for reference, and which was also calculated with the assumption of 90 % error correction efficiency. For 10^8 number of samples the maximal possible transmission line has a length of about 9 km and for 10^9 samples the transmission line can have a length of up to 17.5 km. As shown in [Jou13] the measurement of 10^9 samples is challenging but experimentally feasible.

So far we assumed $\epsilon_{\mathrm{pe}} = 10^{-16}$. Figure 6.5 shows the dependence of the key rate, and thus the maximal length of the transmission line, on ϵ_{pe} for a number of measured samples of $2N = 10^8$ and 10^9. The key rate for an infinite number of measurements is shown for reference. For 10^9 samples the maximal length of the transmission line increases from about 17.5 km for $\epsilon_{\mathrm{pe}} = 10^{-16}$ to about 19 km for $\epsilon_{\mathrm{pe}} = 10^{-10}$. The figure also shows that the key rate for a fiber link of about 5 km length does not depend significantly on ϵ_{pe} for 10^9 samples.

Figure 6.6 shows the secure key rate for an infinite number of samples for different error correction efficiencies β. As it is clearly visible in the figure the error correction efficiency becomes more crucial for increasing length of the transmission line between Alice and Bob. While for short transmission lines the achievable key rate only drops by no more than 50 %, for long transmission lines the maximal achievable distance ranges from about 25 km for 70 % error correction efficiency to about 41.5 km for 95 % efficiency. Nowadays the best available binary codes have an error correction efficiency of up to 95 % [Jou11, Jou13]. Non-binary codes [Dav98], as used here for the calculation of the key rate, are also under active development [Ulr57, Sas10, And12]. Note, that the achievable efficiency of error correction codes is crucially dependent on the signal-to-noise ratio and therefore the code that works best for each distance has to be found. Note further, that the given key rates in the figure are for an infinite number of samples. The effect of the finite number of the measured samples on the key rate was shown above for an error correction efficiency of 90 %.

We have seen that entanglement-based quantum key distribution under the restriction of the eavesdropper to collective attacks is possible within a reasonable distance between Alice and Bob and for a reasonable number of measurements that have to be performed, despite the fact that a vacuum mode was involved in the entanglement generation process. In comparison to the full scheme involving two squeezed modes which will be analysed in the next Section, the scheme investigated here, reduces the complexity of the source as no phase lock at the beam splitter that generates the entanglement, is necessary. To address the fact that we have to omit the samples measured in the P quadrature, one could tune the probability with which Alice and Bob measure X or P to have only as much samples measured in the P quadrature as are needed to have a reasonably small confidence set. With more samples measured in the X quadrature the overall key length increases for the same number of total measurements.

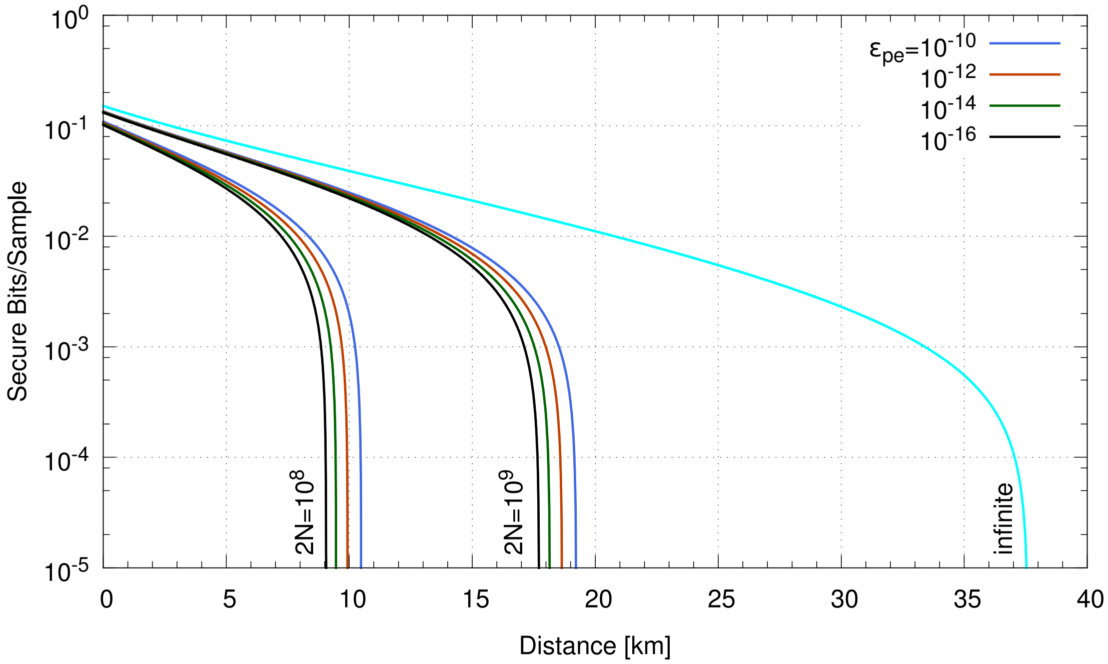


Figure 6.5: Secure key rate versus distance like in Fig. 6.4, but for different parameter estimation parameters ϵ_{pe}. The array of curves are plotted for a total number of measured samples of 10^8 and 10^9. For reference the key rate is also plotted for an infinite number of samples.

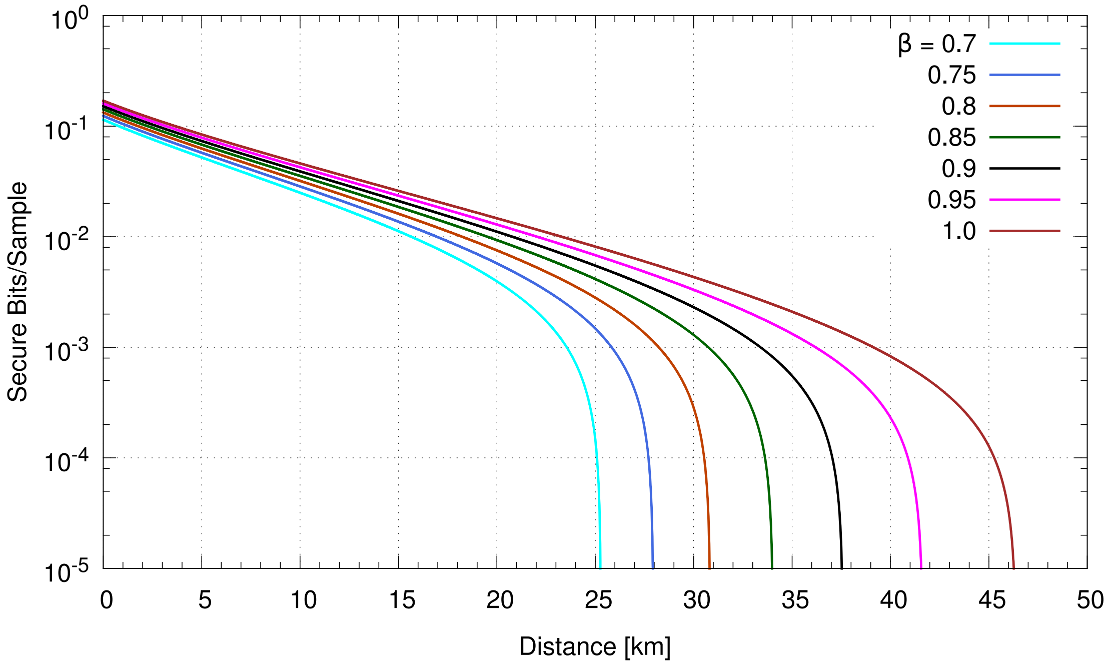


Figure 6.6: Secure key rate versus distance between Alice and Bob for an infinite number of samples for different assumed error correction efficiencies.

6.2 Secure Key Rates for Entanglement Using Two Squeezed Vacuum Resources

In comparison to entanglement generated by superimposing a squeezed vacuum mode with a vacuum mode, entanglement generated by two squeezed vacuum modes is much stronger according to entanglement measures such as the Duan inseparability criterion or the EPR-Reid entanglement criterion, cf. Chapter 2.11. In this section the secure key rate for such states is investigated. The experimental setup and a characterization of the entanglement is given in Chapter 4.5. The starting point for the following analysis is the reconstructed covariance matrix of the measured states given in Eq. (4.11). It was shown that in a table-top setup the key rates are about 3 times larger for 10^9 samples than with entanglement generated from a single squeezed vacuum resource. Furthermore, the achievable distance for 10^9 samples is about 1.5 times larger for 90 % error correction efficiency. However, for small error correction efficiencies the achievable distances are smaller and it is beneficial to use only a single squeezed vacuum resource.

The analysis is started by assuming a table-top setting for which the secure key rate is investigated which can be achieved by the states from Chapter 4.5. The security parameters were chosen as $\epsilon_c = \epsilon_s = \epsilon_{\mathrm{pe}} = 10^{-16}$ if not stated otherwise. α was chosen 8 times the standard deviation of the respective quadrature sample distribution. For parameter estimation we used the same procedure as in Section 6.1. The error correction efficiency was assumed to be $\beta = 0.9$.

Figure 6.7 shows the secure key rate, i.e. the number of secure bits per measurement (before sifting), which can be extracted when the P quadrature measurements were discarded ($p_X = 1$). The different curves in the figure are plotted for different number of intervals $2^{n_{\mathrm{bits}}}$. From the figure we read that at least $n_{\mathrm{bits}} = 8$ are needed to extract the most bits. While for a total of 10^8 samples about 0.19 bits/sample can be extracted, about 0.29 bits/sample can be extracted for 10^9 samples.

The secure key rate which can be achieved when the samples measured in the X quadrature are discarded instead, is shown in Fig. 6.8. The curves in the figure look quite similar to the ones in Fig. 6.7 as the state is almost symmetric. The number of samples needed to reach a positive key rate is a little smaller than when discarding samples from the X quadrature. Also the number of extractable bits per sample is higher. This is due to the state's better correlations in the P than in the X quadrature. For 10^8 samples 0.28 bits/sample can be extracted and for 10^9 samples 0.37 bits/sample.

To increase the number of secure bits per sample a key can be extracted from both quadratures. Figure 6.9 shows this situation for $n_{\mathrm{bits}} = 8$ for both quadratures. The green solid line shows the key rate with an optimized number of samples k for

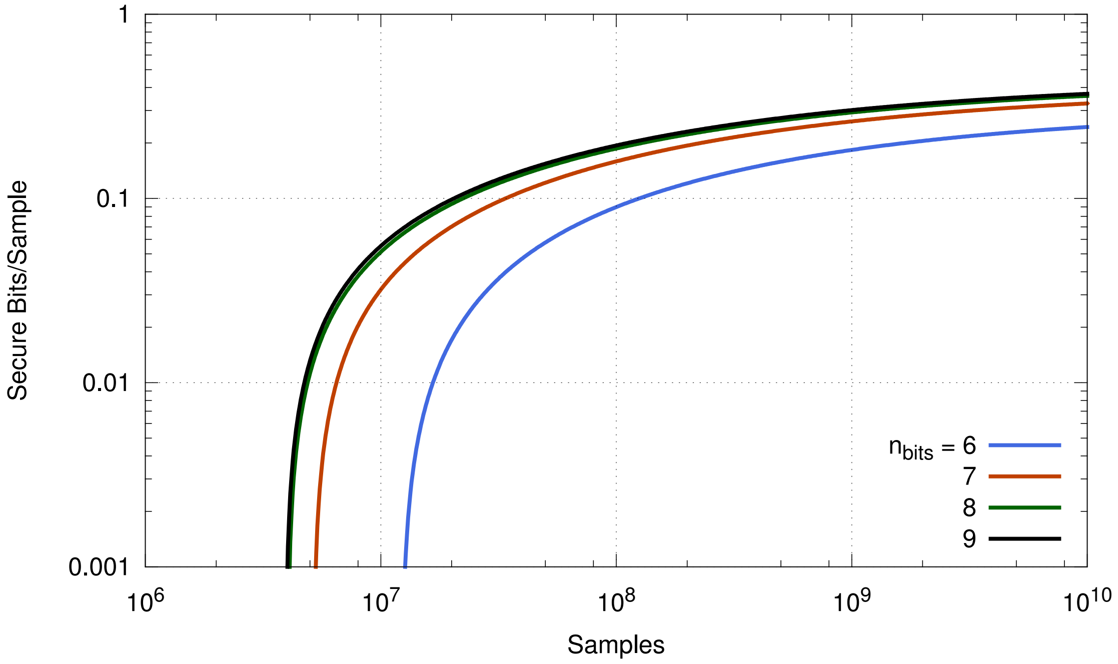


Figure 6.7: Secure key rate versus the number of measured samples. Here, only X quadrature measurements were included, i.e. $p_X = 1$. The number of samples k used for parameter estimation were optimized to yield a maximal key rate.

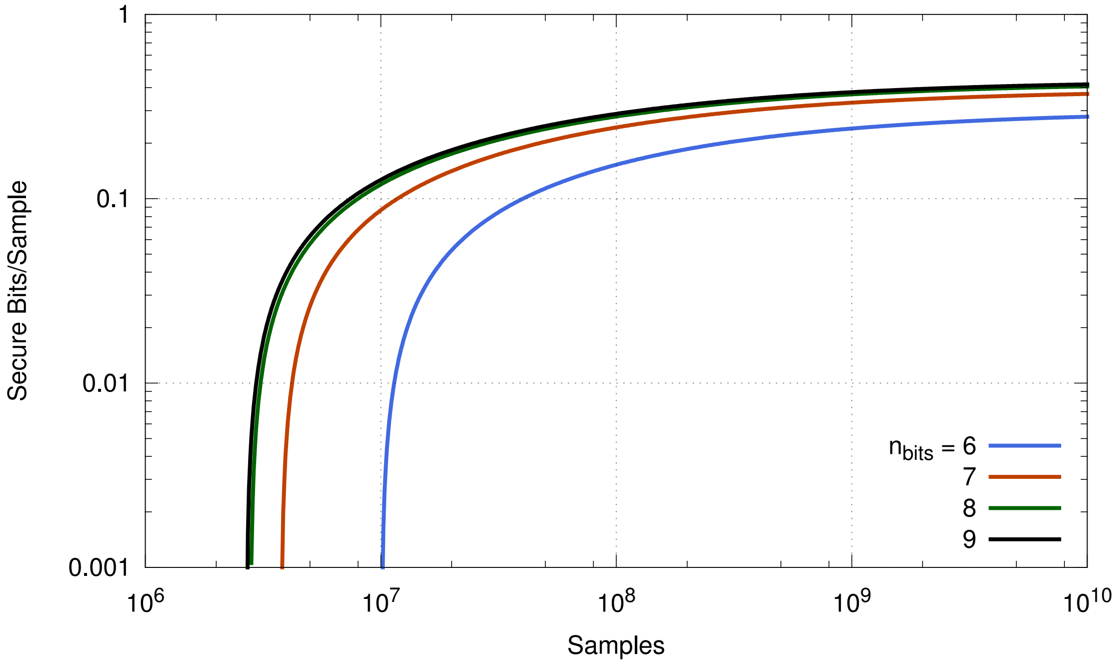


Figure 6.8: Secure key rate versus the number of measured samples. Here, only P quadrature measurements were included, i.e. $p_X = 0$. The number of samples k used for parameter estimation were optimized to yield a maximal key rate.

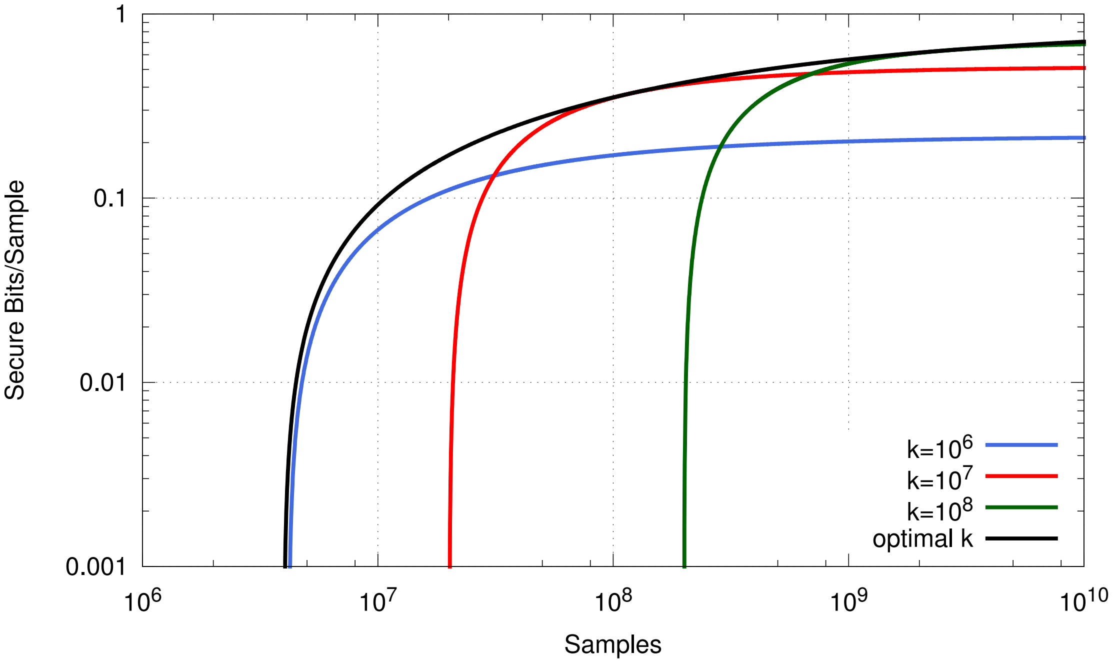
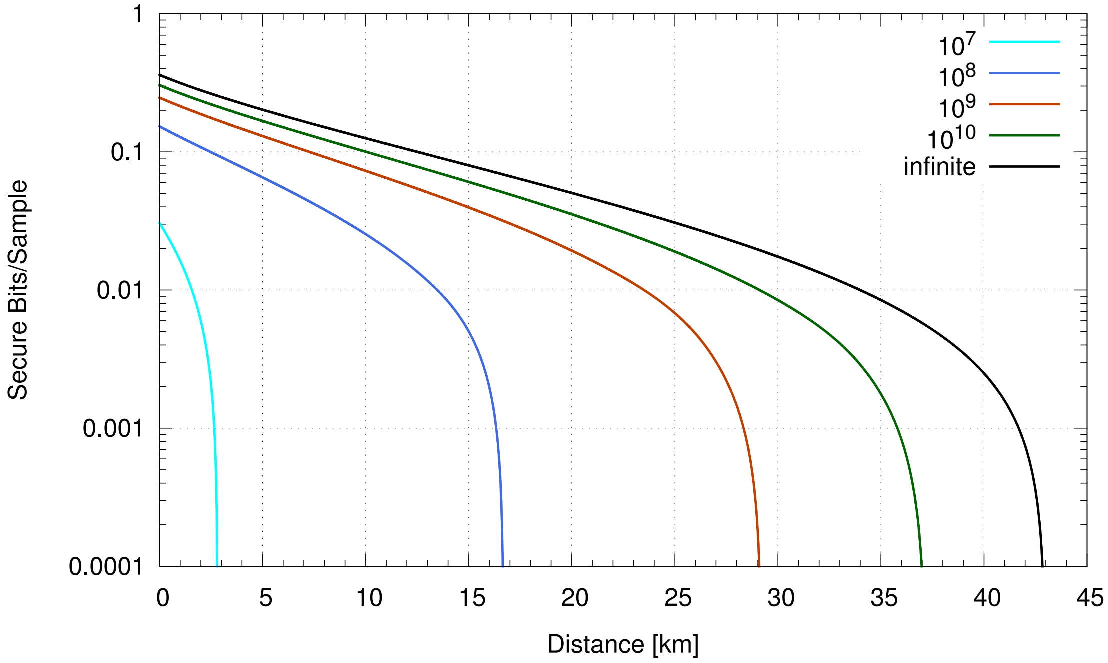


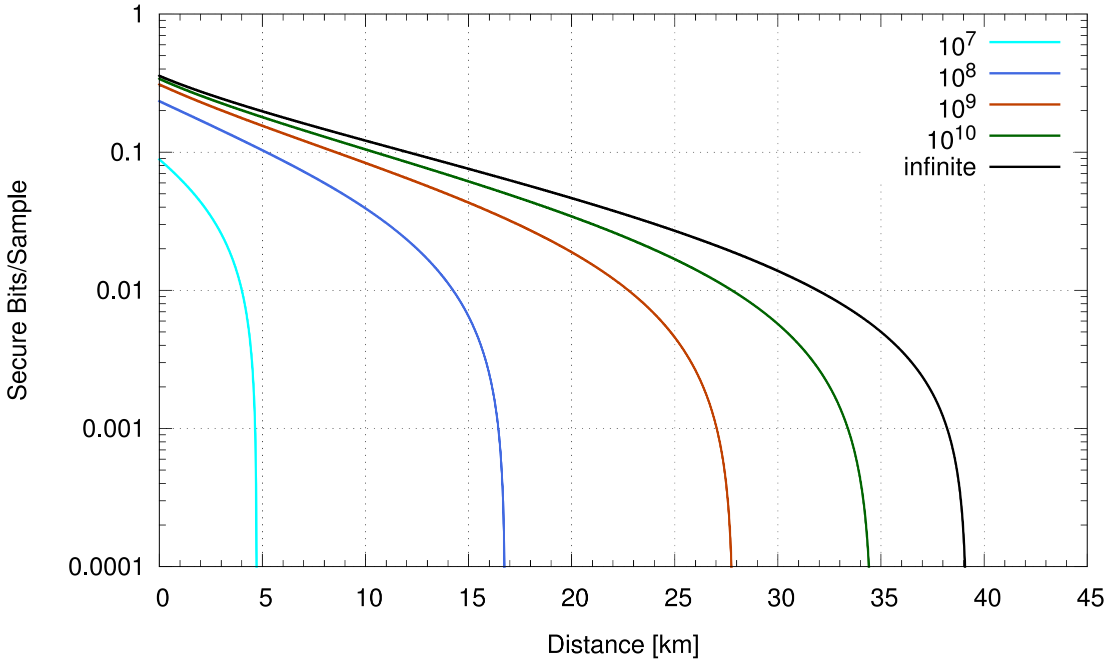
Figure 6.9: Secure key rate versus the number of measured samples. Here, both X and P quadrature measurements were included, i.e. $p_X \approx 0.5$. For the green solid line the number of samples k used for parameter estimation was optimized to yield a maximal key rate. For comparison the key rates for k=10^6, 10^7 and 10^8 are shown.

parameter estimation. To make the effect of k on the key rate visible curves for $k = 10^6$, 10^7 and 10^8 are also shown. For 10^8 samples a maximum of 0.35 bits/sample can be extracted. Here, the blue solid line shows that the optimal k is about 10^7. In comparison, for 10^9 samples 0.57 secret bits/sample are possible to extract. Compared to the key rates when omitting samples measured either in the X quadrature or in the P quadrature, the secret bits per sample are not twice as large. This penalty is due to the larger confidence set, cf. Chapter 5.4.3, for keys extracted from both quadrature settings since $\mathrm{Cov}(\hat{X}_A, \hat{X}_B)$ and $\mathrm{Cov}(\hat{P}_A, \hat{P}_B)$ have to be estimated from only about $\frac{k}{2}$ samples each. If omitting the samples from one of the quadratures, the respective covariance can be estimated with about $\frac{N}{2}$ samples instead.

Figure 6.10 shows the secure key rate versus the distance between Alice and Bob when sending Bob's part of the state through an optical standard telecommunication fiber. For the calculation an optical coupling efficiency of the free-space mode into the optical fiber of 95 % and an optical loss of 0.2 dB/km was assumed, cf. Section 6.1. Figure 6.10a shows the number of secure bits when only samples from the X quadrature were taken into account, while for Fig. 6.10b only samples from the P quadrature were used. The different curves in the figures were plotted for a different number of



(a) For the simulation only samples measured in the X quadrature were taken into account, i.e. $p_X = 1$.



(b) For the simulation only samples measured in the P quadrature were taken into account, i.e. $p_X = 0$.

Figure 6.10: Secure bits per measured sample versus distance when sending one part of the entangled beams through an optical fiber. We assumed a coupling efficiency of 95 % into the optical fiber and an optical loss of 0.2 dB/km. The curves are plotted for different number of measured samples.

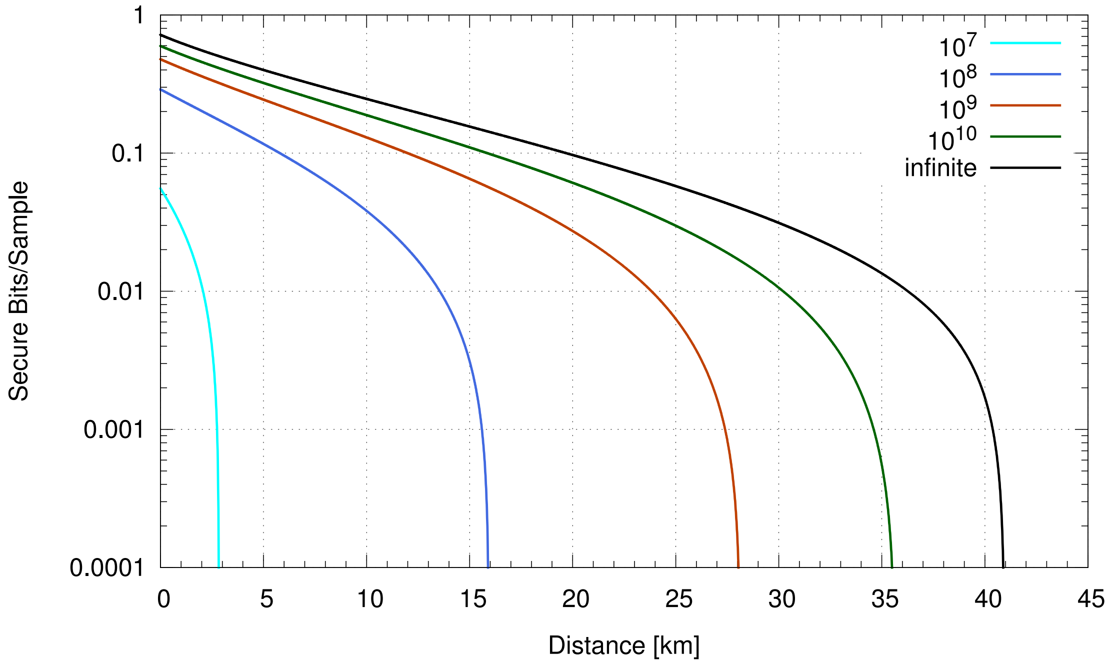


Figure 6.11: Secure bits per measured sample versus the distance between Alice and Bob when sending one part of the entangled beams through an optical fiber. We assumed a coupling efficiency of 95 % into the optical fiber and an optical loss of 0.2 dB/km. For each distance and each curve the number of samples k used for parameter estimation was optimized to achieve the largest number of secure bits. The curves are plotted for different total number of measured samples. Samples from both quadratures were used in the simulation to generate a key.

total samples. To maximize the number of secret bits the number of samples used for parameter estimation was optimized for each distance and each number of total samples. For comparison the number of secure bits for an infinite number of samples is shown. Here, the error correction efficiency was also assumed to be 90 %. The difference in the achievable distance between both figures are due to the different squeezing in both quadratures. For 10^8 samples a distance of about 16.5 km can be achieved, while for 10^9 samples the transmission line length can be up to about 28 km. The same calculation is shown in Fig. 6.11 for a key generated from both quadratures. While the achievable distances are about the same, the number of secure bits per sample are larger as more samples exist from which a key can be generated. Hence, it is preferable to generate a key from both quadratures.

The dependence of the secure key rate and the achievable distance on the parameter estimation security parameter ϵ_{pe} is shown in Fig. 6.12 for a total number of samples of 10^8 and 10^9. While for short distances the number of secure bits is only slightly increased with a larger security parameter the achievable distance increases for about

2 km for both 10^8 and 10^9 samples when relaxing ϵ_{pe} to 10^{-10}.

Figure 6.13 shows the effect of the error correction efficiency β on the achievable distance. For the calculation an infinite number of samples was assumed as this gives an upper limit to the achievable distance. When assuming a finite number of samples, the distances reduce as shown above. The effect of the error correction efficiency is severe as for 70 % a distance of only about 10 km is reached. For 90 % efficiency which was assumed for the simulations above, about 40 km are possible. The best available codes for a binary alphabet have 95 % efficiency [Jou13]. If such an algorithm would be available for a non-binary alphabet as used in our protocol, up to 67 km would be possible. With a perfect error correction, even a distance of 177 km could be bridged.

To briefly summarize Section 6.1 and Section 6.2, entanglement generated by two squeezed vacuum resources performs better in terms of key rate and communication distance than entanglement generated by a single squeezed vacuum resource with a realistic number of samples in the order of 10^8 and 10^9 for high error correction efficiencies. For low error correction efficiencies, however, larger communication distances between Alice and Bob can be achieved with entanglement generated by a single squeezed vacuum resource. Since the achievable key rate and also the achievable distance between Alice and Bob depend strongly on the error correction efficiency, large effort has to be put into these algorithms.

6.3 Implementation of Random Amplitude and Phase Quadrature Measurements

To implement the quantum key distribution protocol for collective or general attacks, Alice and Bob have to choose randomly the quadrature in which they measure a sample. The security proof requires that the quadratures are identically and independently distributed (i.i.d.). This is accomplished by using a quantum random number generator, which is described in Section 6.4. This section describes the experimental implementation of the switching process of the local oscillator used for homodyne detection. The presented scheme was developed in the framework of this thesis.

Figure 6.14 shows the experimental setup of the homodyne detection process that allows to measure the amplitude and phase quadratures randomly with a rate much higher than the usual unity gain frequencies of about 1 kHz of phase locks with piezo mounted mirrors used as actuators. The local oscillator was phase locked to the signal by employing the locking scheme described in Chapter 4.5 using a low frequency actuator. The output of the servo controller was lowpass filtered by an analog filter with a cutoff frequency of about 100 kHz with a sufficiently high order. We applied phase shifts of 0 or $\frac{\pi}{2}$ to a fast fiber-coupled electro-optical phase modulator to measure

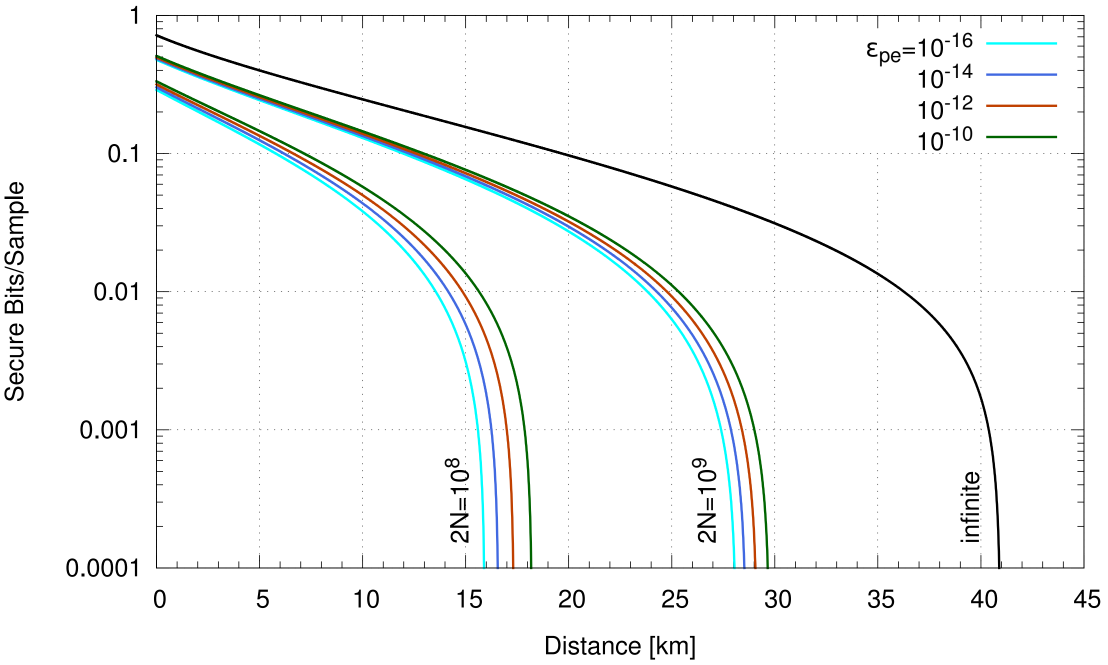


Figure 6.12: Secure bits per measured sample versus distance in dependence of the parameter estimation security parameter ϵ_{pe}.

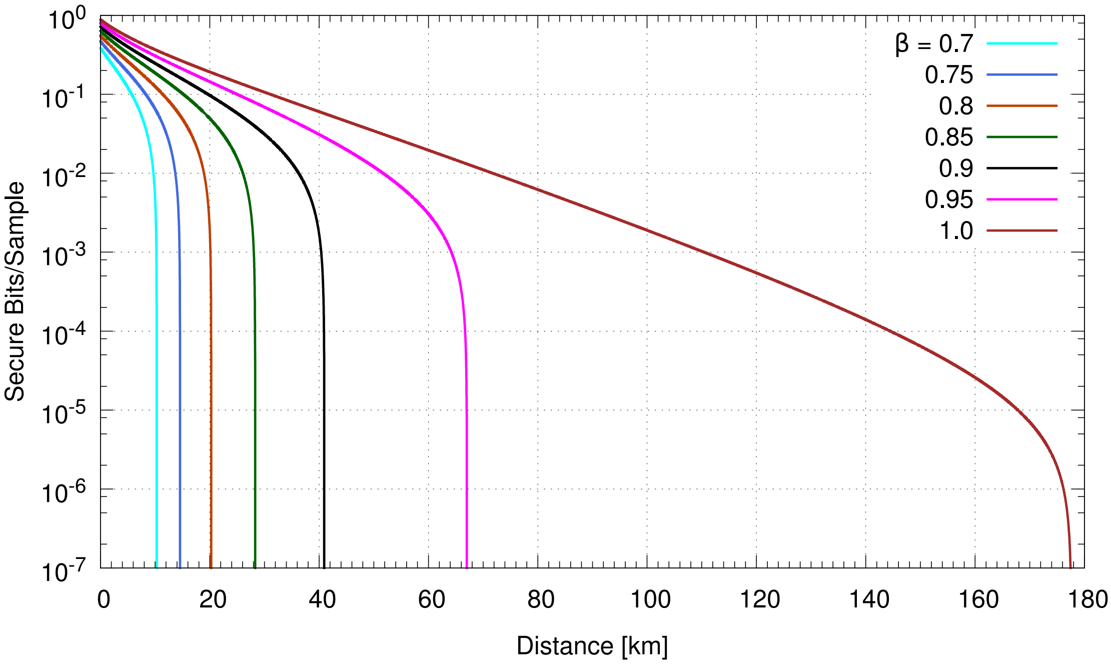


Figure 6.13: Effect of the error correction efficiency β on the achievable distance. The key rates are calculated for an infinite number of samples.

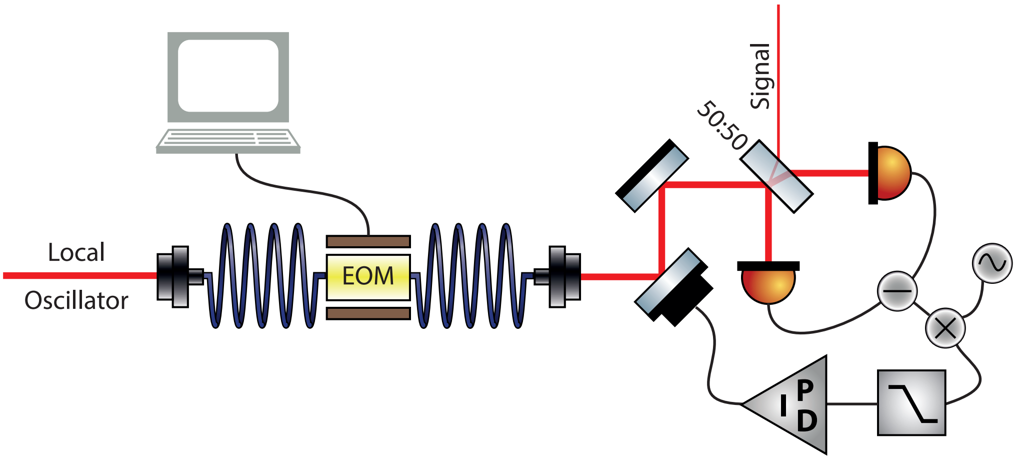


Figure 6.14: Experimental setup for a fast random choice of measuring amplitude or phase quadrature. A piezo driven mirror is used to phase lock the local oscillator to the signal. The servo controller for this lock has a high order lowpass filter to average over the actual phase of the local oscillator which is driven to 0 or $\frac{\pi}{2}$ by a fiber-coupled electro-optical phase modulator (EOM) using a digital pattern generator PCI Express card with programmable high voltage level.

either the amplitude or phase quadrature. The fiber-coupled phase modulator had a half-wave voltage of about 3.5 V and was connected to a digital pattern generator PCI Express card, which had a programmable voltage for the high level. If the rate of switching between amplitude and phase quadrature is high enough, the phase lock's servo controller averages over the phase of the local oscillator. If the average is stable over time the local oscillator can be locked to measure exactly the amplitude and phase quadrature. Here it is important that the local oscillator phase lock can be set to arbitrary values as the average is somewhere between both quadratures.

In practice, measuring the amplitude and phase quadrature randomly, usually yields an unstable average over time as long sequences of, for instance, the amplitude quadrature are not unlikely. To circumvent this problem we used a scheme shown in Fig. 6.15. For both Alice and Bob, a possible choice of quadratures is plotted versus time. For each quadrature choice phase shifts are applied to the fiber-coupled phase modulator. For a choice of an amplitude quadrature measurement (X), we first apply a phase shift to the local oscillator of $\frac{\pi}{2}$ which is followed by a phase shift of 0 with respect to the signal beam. For a choice of a phase quadrature measurement (P) instead, a phase shift of 0 is followed by a phase shift of $\frac{\pi}{2}$. This scheme allows the average over the local oscillator's phase to be constant in time as it can only happen that the local oscillator has the same phase for the time of a whole interval. This can be seen in the figure when for instance Alice chooses to measure first X and then P. If she chooses

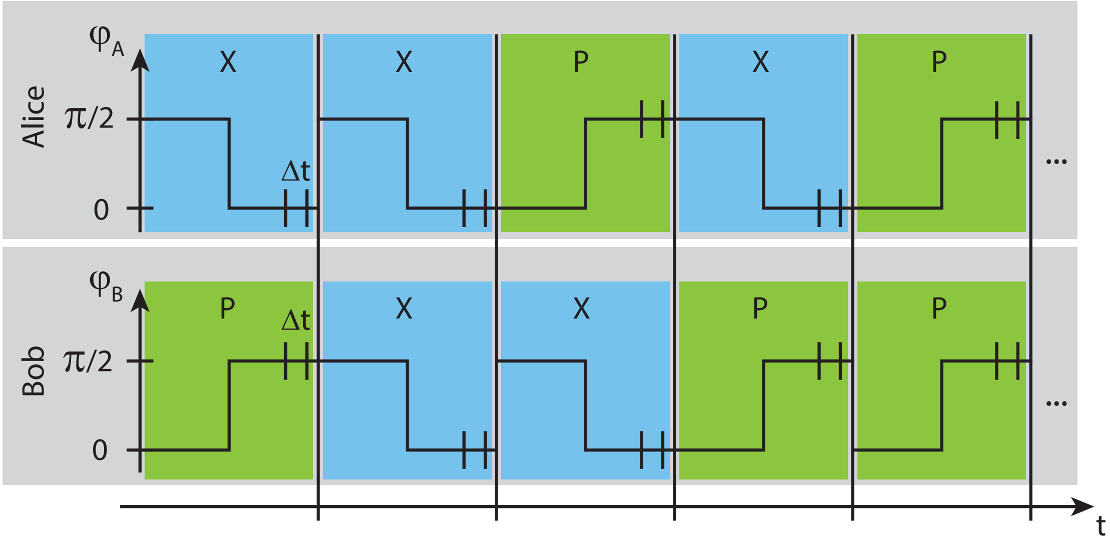


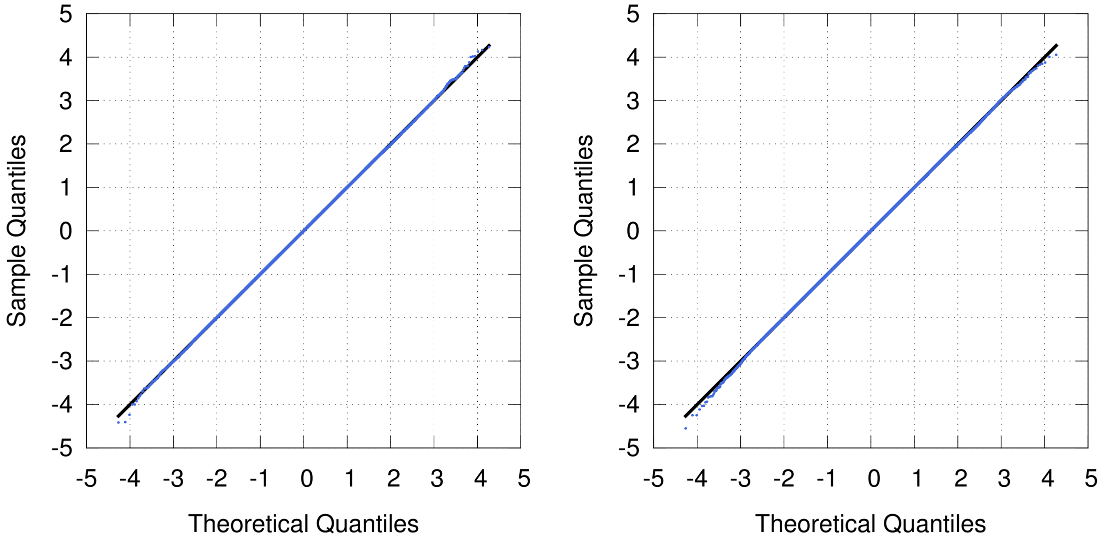
Figure 6.15: Measurement process with random quadrature choice. For an X quadrature choice a phase shift of the local oscillator by $\frac{\pi}{2}$, followed by a phase shift of 0, is applied. For a P quadrature choice instead a phase shift of 0 is followed by a phase shift of $\frac{\pi}{2}$. A measurement of length Δt is performed synchronously in the second half of the interval. Using this scheme the mean phase of the local oscillator is independent of the quadrature choices.

to measure X twice instead, the phase of the local oscillator switches between X and P after half an interval.

While in this thesis the probabilities of measuring X or P were always 50 %, the presented scheme provides the possibility to use unequal probabilities without any modification.

Both parties agree on synchronous measurements in the second half of the interval. In particular they wait some time between the step of the phase of the local oscillator and the start of the measurement as the classical control signals at DC and at the single sideband frequencies give rise to overshoot and ringing in the homodyne detector's output. To not saturate the front-end of the analog-to-digital converter card we implemented a sample-and-hold circuit that holds the homodyne detector's output at a constant level during a certain time interval around phase changes. The implementation of the homodyne detector's electronics including a sample-and-hold circuit can be found in the Appendix, Fig. A.2.

To record both homodyne detectors' output signals simultaneously, we used a PCI Express card, Signatec PX14400A, with a fast analog-to-digital converter with two channels. For this purpose the outputs of the homodyne detectors were anti-alias filtered with a 4th-order Butterworth filter with a cutoff frequency of 50 MHz. The



(a) vacuum state

(b) thermal state

Figure 6.16: QQ-plot of a homodyne measurement of a vacuum state and a thermal state with Alice's homodyne detector to test the Gaussianity of the measurement outcomes. The thermal state was part of an entangled state. For the thermal state the measured quadratures where chosen at random and samples measured in the P quadrature were omitted. The quadrature variances of both states were normalized to 1. The figures show that the implemented scheme with a randomly chosen quadrature for each measured sample does not change the Gaussian distribution of the measurement outcomes. Thus, no significant phase noise was introduced.

recording was triggered by an output signal of the pattern generator which also drove the fiber-coupled phase modulators. 256 samples were recorded with a sampling frequency of 256 MHz at each trigger event, yielding a measurement time of 1 μs. The repetition rate of the trigger events was 100 kHz. For each channel the samples were digitally mixed at 8 MHz, lowpass filtered with a 200-tap FIR filter with 200 kHz cutoff frequency and down sampled by taking only the 200th sample.

To check whether the fast switching process between the quadratures caused any undesired non-Gaussian effects in the homodyne detector's output signal, we determined the Gaussianity of the measured samples. For reference we blocked the input port of Alice's homodyne detector and recorded 10^5 samples of a vacuum state measurement. The Gaussianity was checked with a QQ-plot which is shown in Fig. 6.16a. A QQ-plot compares the quantiles of the measured samples to the theoretical quantiles of a Gaussian distribution. Samples drawn from a Gaussian distribution therefore follow a straight line in the QQ-plot. More details about checking the Gaussianity of samples can be found in [Sam12]. Figure 6.16b shows a QQ-plot for 10^5 measured samples

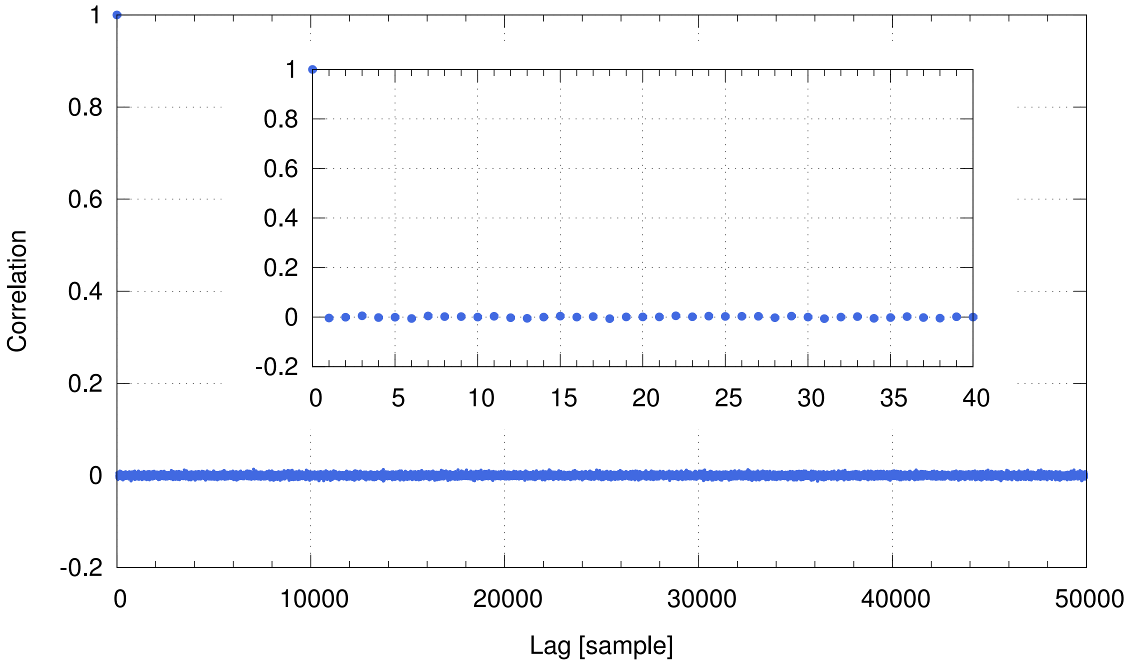


Figure 6.17: Autocorrelation function of 10^5 samples measured with blocked signal port of Alice's homodyne detector. The inset represents a zoom into the first 40 data points. The autocorrelation function shows that the measurement process does not introduce any correlations between subsequent samples.

from a thermal state in the X quadrature. Here, the measured quadrature was chosen at random as described above and measurements performed in the P quadrature were omitted. For comparison we normalized the thermal state's X quadrature variance to 1. The QQ-plot does not show a significant deviation from a straight line for both the vacuum and the thermal state. Hence, the switching process does not introduce non-Gaussian effects which cannot be described by the first two statistical moments. QQ-plots of the P quadrature data and also of Bob's homodyne measurement look similar to the ones in Fig. 6.16.

A prerequisite for quantum key distribution is that subsequently measured samples are independent of each other. This was checked by calculating the autocorrelation function of the samples recorded when measuring a vacuum state. Figure 6.17 shows the autocorrelation of 10^5 samples measured with Alice's homodyne detector with blocked signal port. The measurement was performed and timed as described above. As it is clearly visible from the inset which shows a zoom into a lag between 0 and 40, subsequent samples were independent of each other. This shows that the measurement apparatus does not introduce correlations.

6.4 Quantum Random Number Generation

Random numbers have a wide range of applications like gambling, simulations and cryptography. Nowadays mostly pseudo-random numbers (PRNs) are used which employ deterministic numeric algorithms, called *generators*, to produce numbers that appear random to outsiders who do not know the algorithm [Jam90]. The randomness of random numbers is tested with a large number of complicated statistical tests. Accepted test suites are TestU01 [Lec07], NIST [Ruk01] and dieharder [Bro12]. Even though PRNs are easy to calculate, generators with good statistical properties are hard to find [Hel98].

In this thesis random numbers are utilized in the quantum cryptography experiment by Alice and Bob independently to determine the quadrature, amplitude or phase, they measure. Pseudo-random numbers, even those produced by good generators, weaken the protocol as an adversary knows, by definition, which generators were used and therefore only has to find out the so-called *seed*, the start value for the deterministic numeric algorithm. Hence, the number of bits the adversary needs knowledge about to gain information about the measured quadratures is rather limited. Therefore, we used a *quantum random number generator* (QRNG) to generate these random numbers. QRNGs, also called truly random number generators, rely on random physical processes making the generated numbers random and unpredictable. Perfectly suitable for this task are quantum mechanical systems as measurement outcomes of non-eigenstates of the measurement observable are postulated to be truly random and unpredictable. While quantum mechanics ensures the randomness of the measurement results, the measured quantum states have to be carefully chosen as they also need to be uncorrelated with some adversary. For example using one part of a bipartite entangled state yields random results, but as long as the adversary has access to the other subsystem the random numbers are no longer unique. Hence, the quantum state, which the random number generator processes, has to be pure (which is indeed not the case for a subsystem of a bipartite entangled state). In this thesis we used field quadrature measurements on a vacuum state. Such a QRNG was first implemented by [Gab10] and [Sym11]. Quantum random number generators exhibiting also the randomness feature of quantum mechanics, but using different quantum systems are for example [Jen00, Ste00, Dyn08, Bro09, Fue10, Wah11, Xu12].

The following protocol to generate random numbers from field quadrature measurements on a vacuum state relies on the protocol published by Gabriel et al., in [Gab10].

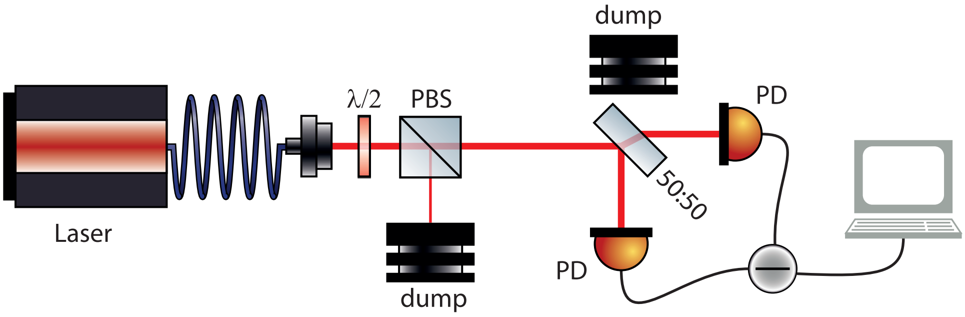
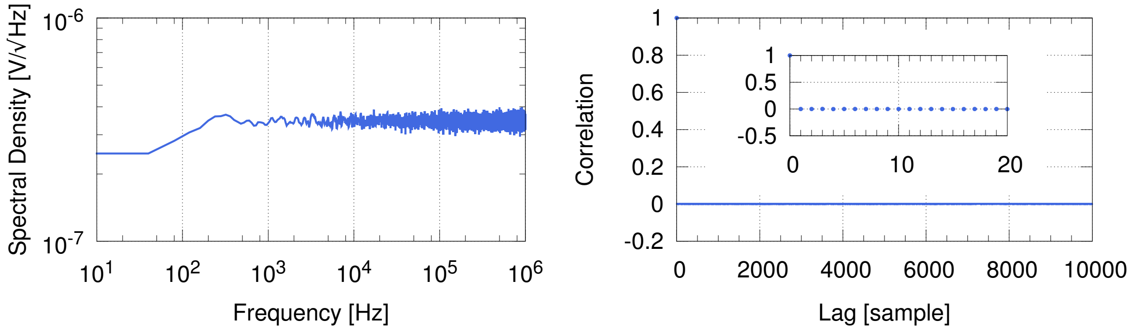


Figure 6.18: Experimental setup for quantum random number generation by exploiting the randomness of quadrature field measurements on a vacuum state. The laser's output was attenuated by a variable beam splitter and used as local oscillator beam for homodyne detection of a vacuum mode. To make sure that really a vacuum mode was measured, the signal port of the homodyne detector was blocked with a beam dump. PBS: Polarizing Beam Splitter, PD: Photo Diode.

6.4.1 Experimental Setup

The experimental setup is shown in Fig. 6.18. We used a homodyne detector, as described in Chapter 3.4, to measure a field quadrature of a vacuum state. The homodyne detector's local oscillator was served by an NP Photonics, Inc., fiber laser at 1550 nm with an output power of about 25 mW which was reduced to about 6 mW by a combination of a half-waveplate and a polarizing beam splitter. The beam was split at a 50 : 50 beam splitter and detected by two FCI-InGaAs-300 photo diodes. To ensure measurements on a vacuum state and to prevent a possible adversary from injecting an entangled state, the signal port was blocked. The photo current of the two photo diodes was subtracted and converted to a voltage by a transimpedance amplifier. The output of the homodyne detector electronics was anti-alias filtered by a 50 MHz forth-order Butterworth filter and sampled with a sampling frequency of 256 MHz by a Signatec PX14400A data acquisition card. The sampled data was digitally highpass filtered to remove the DC offset, mixed with a sinusoidal at 8 MHz, lowpass filtered at 5 MHz with a 200-tap FIR filter and downsampled to 2 MHz. This undersampling removed all correlations between the samples introduced by the lowpass filtering after the mixing process, cf. Chapter 3.7. The output of this postprocessing procedure is the raw data for the random number generation. It shows a white power spectral density and an autocorrelation indicating that the samples are independent, as depicted in Fig. 6.19. The electronic dark noise clearance was measured to be about 18 dB.

The whole setup was placed on a portable $30 \times 30\,\mathrm{cm}^2$ breadboard to allow for transportation to future experiments which need quantum random numbers. The breadboard features a fiber coupler for the input beam. Hence, the laser serving the



(a) Linear Spectral Density **(b)** Autocorrelation

Figure 6.19: Linear spectral density and autocorrelation of a quadrature measurement of a vacuum state. The inset in the right figure shows a zoom into the first 20 data points. The linear spectral density shows a white spectrum and the autocorrelation that the measured samples were uncorrelated.

local oscillator is not part of the breadboard and can be replaced easily.

6.4.2 Random Number Generation

The measurement of the vacuum fluctuations is distorted by the electronic dark noise of the measurement device, the homodyne detector electronics. Since we want to extract the inherent randomness of the vacuum state measurement and not the randomness of the electronic dark noise, the amount of information which can be extracted is given by

$$S_{\text{extractable}} = S(X_{\text{vac}}) - S(X_{\text{dark noise}}) \ , \tag{6.1}$$

where S is the Shannon entropy and X describes the classical distribution of the measurement outcomes of the field quadratures of the vacuum state, X_{vac}, and the electronic dark noise, $X_{\text{dark noise}}$, respectively. For this purpose we divide the measurement outcomes of the homodyne detection of the vacuum state into N distinct intervals with same probability p. $S(X_{\text{vac}})$ is then given by

$$S(X_{\text{vac}}) = -\sum_{k=1}^{N} p \log p = \log N \ , \tag{6.2}$$

where the logarithm is taken to basis 2, and where we used the fact that $N \cdot p = 1$. The Shannon entropy of the electronic dark noise is calculated by

$$S(X_{\text{dark noise}}) = -\sum_{k=1}^{N} p_k \log p_k \ , \tag{6.3}$$

where p_k is the probability of an electronic dark noise measurement outcome to be within the kth interval. Assuming the electronic dark noise to follow a Gaussian distribution, p_k can be calculated by

$$p_k = \int_{x_k}^{x_{k+1}} \mathrm{d}x \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{x^2}{2\sigma^2}\right) \tag{6.4}$$

$$= \frac{1}{2}\left(\mathrm{erf}\left(\frac{x_{k+1}}{\sqrt{2\sigma^2}}\right) - \mathrm{erf}\left(\frac{x_k}{\sqrt{2\sigma^2}}\right)\right) , \tag{6.5}$$

where σ^2 is the variance of the electronic dark noise normalized to the variance of the vacuum and erf is the error function. x_k and x_{k+1} are the boundaries of the kth interval which can be derived iteratively, starting with $x_1 = -\infty$, by evaluating

$$x_{k+1} = \sqrt{2}\,\mathrm{erf}^{-1}\left(\frac{2}{N} + \mathrm{erf}(x_k/\sqrt{2})\right) . \tag{6.6}$$

Here, the variance of the vacuum is assumed to be 1.

Taking the number of intervals N as a power of 2, each interval can be assigned a unique bit combination of n bits, where there is no bit combination belonging to no interval. The Shannon entropy of the vacuum is then given by $S(X_{\mathrm{vac}}) = \log N = n$. Figure 6.20 shows the extractable amount of information $S_{\mathrm{extractable}}$ given in bits versus the number of bits n for an electronic dark noise clearance of 18 dB, i.e. $\sigma^2 = 10^{-18\,\mathrm{dB}/10}$. From the figure we deduce an optimal n of 5 bits, yielding $S_{\mathrm{extractable}} = 2.51$ bits.

Assigning each measurement outcome a bit combination of n bits yields a string of raw random numbers. To remove the residual information from the electronic dark noise, we use randomness extraction by hash functions [Sti02, Tom11]. A hash function is a mathematical one-way function projecting an arbitrary number of bits to a fixed number of bits, called the message digest, in such a way that small changes in the input string changes the output string dramatically. In our particular implementation we use `SHA512` [RFC11] which was developed by the National Security Agency (NSA) and published in 2001 by the National Institute of Standards and Technology (NIST). The message digest of `SHA512` has a size of 512 bits. Hence, to reduce 5 bits to 2.51 bits we put several measurements into a single bit string of $(5/2.51) \cdot 512$ bits length which was reduced to 512 bits by a single run of `SHA512`.

While in principle the speed of the random number generation would be about 5 MBit/s, limited by the bandwidth of the homodyne detector, our setup is limited by the speed of the post processing. Indeed our setup reached about 1.5 MBit/s. Implementing the post processing, in particular the mixing and down sampling process, using a field programmable gate array (FPGA) this can easily be improved.

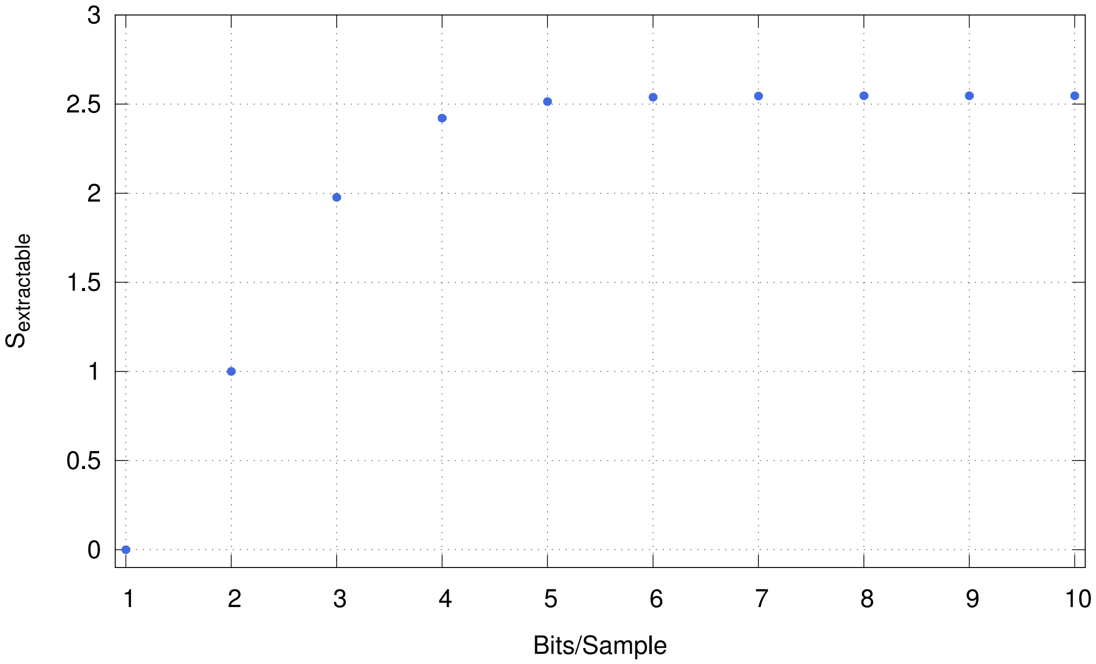


Figure 6.20: Extractable information in bits given by the Shannon entropy $S_{\text{extractable}}$ versus the number of bits n assigned to a measured sample.

6.4.3 Statistical Tests of the Generated Random Numbers

We tested our quantum random numbers with three different statistical test suites. The results of the Crush battery of the TestU01 test suite are shown in Tab. 6.1. Since most tests were run many times with different parameter sets, the results are given as the number of test runs passed per the number of total test runs.

The test results of the NIST test suite are summarized in Tab. 6.2. Here also most tests were run with different parameter sets. Each statistical test was run 1000 times and is indicated as passed if the minimum pass rate was reached. More detailed results can be found in Appendix B.

Table 6.3 shows the summarized results of the dieharder test suite. Detailed results can be found in Appendix B.

To summarize, all tests of all test suites were passed, indicating that the generated random numbers were really random.

Test	Result	Test	Result
Serial Over	2/2	Collision Over	8/8
Birthday Spacings	7/7	Close Pairs	3/3
Close Pairs Bit Match	2/2	Simp Poker	4/4
Coupon Collector	4/4	Gap	4/4

Run	2/2	Permutation	2/2
Collision Permut	2/2	Max Oft	4/4
Sample Prod	2/2	Sample Mean	1/1
Sample Corr	1/1	Appearance Spacings	2/2
Weight Distrib	4/4	Sum Collector	1/1
Matrix Rank	6/6	Savir 2	1/1
GCD	2/2	Random Walk 1	6/6
Linear Comp	2/2	Lempel Ziv	1/1
Fourier 3	2/2	Longest Head Run	2/2
Periods in Strings	2/2	Hamming Weight 2	2/2
Hamming Corr	3/3	Hamming Indep	6/6
Run	2/2	Auto Cor	4/4

Table 6.1: Results of the TestU01 Crush test suite.

Test	Passed	Test	Passed
Frequency	1/1	Block Frequency	1/1
Cumulative Sums	2/2	Runs	1/1
Longest Run	1/1	Rank	1/1
FFT	1/1	Non Overlapping Template	148/148
Overlapping Template	1/1	Universal	1/1
Approximate Entropy	1/1	Random Excursions	8/8
Random Excursion Variants	18/18	Serial	2/2
Linear Complexity	1/1		

Table 6.2: Summarized test results of the NIST test suite.

Test	Passed	Test	Passed
diehard birthdays	1/1	diehard operm5	1/1
diehard rank 32x32	1/1	diehard rank 6x8	1/1
diehard bitstream	1/1	diehard opso	1/1
diehard oqso	1/1	diehard dna	1/1
diehard count 1s str	1/1	diehard count 1s byt	1/1
diehard parking lot	1/1	diehard 2dsphere	1/1
diehard 3dsphere	1/1	diehard squeeze	1/1
diehard sums	1/1	diehard runs	2/2
diehard craps	2/2	marsaglia tsang gcd	2/2

sts monobit	1/1	sts runs	1/1
sts serial	30/30	rgb bitdist	12/12
rgb minimum distance	4/4	rgb permutations	4/4
rgb lagged sum	32/32	rgb kstest test	1/1
dab bytedistrib	1/1	dab dct	1/1
dab filltree	2/2	dab filltree 2	2/2
dab monobit 2	1/1		

Table 6.3: Summarized test results of the Dieharder test suite.

6.5 Experimental Quantum Key Distribution Results

This section describes the experimental results of the implemented QKD system. In the first part some of the simulation results from Section 6.5.1 are verified. Since no non-binary error correction algorithm was available, Section 6.5.2 describes the key generation using a post selection procedure and a binary error correction algorithm.

6.5.1 Verification of Simulation Results

Using the entangled states generated by superimposing two squeezed vacuum states, cf. Chapter 4.5, and the random measurement of amplitude and phase quadratures described in Section 6.3, we recorded $2N = 10^8$ samples. Assuming a non-binary error correction algorithm with 90 % efficiency, Fig. 6.21 shows the number of secure bits per sample versus the number of intervals $2^{n_{\text{bits}}}$ when taking samples from both quadratures to generate a key ($p_X \approx 0.5$). The two curves are plotted for $k = 1 \times 10^7$ and $k = 2 \times 10^7$ samples used for parameter estimation, respectively, which were chosen at random. α was chosen 6 times the standard deviation of the respective quadrature, which is just above the modulus of the largest measured sample. The security parameters were chosen $\epsilon_c = \epsilon_s = \epsilon_{\text{pe}} = 10^{-16}$. For $n_{\text{bits}} \geq 8$ the maximal key rate was achieved. For less than $n_{\text{bits}} = 5$ the key rate was zero and no secure key could be extracted.

Figure 6.22 shows the secure key rate for $n_{\text{bits}} = 8$ versus the number samples k used for parameter estimation. For each value of k, k samples were chosen at random from the total of $N \approx 5 \times 10^7$. The random choice explains the noisy curve which gets less noisy for larger k. In the range of $k = 6 \times 10^6$ to $k = 10^7$ the maximum number of secure bits is achieved.

Both $n_{\text{bits}} = 8$ and $k = 10^7$ are in good agreement with the optimal values obtained

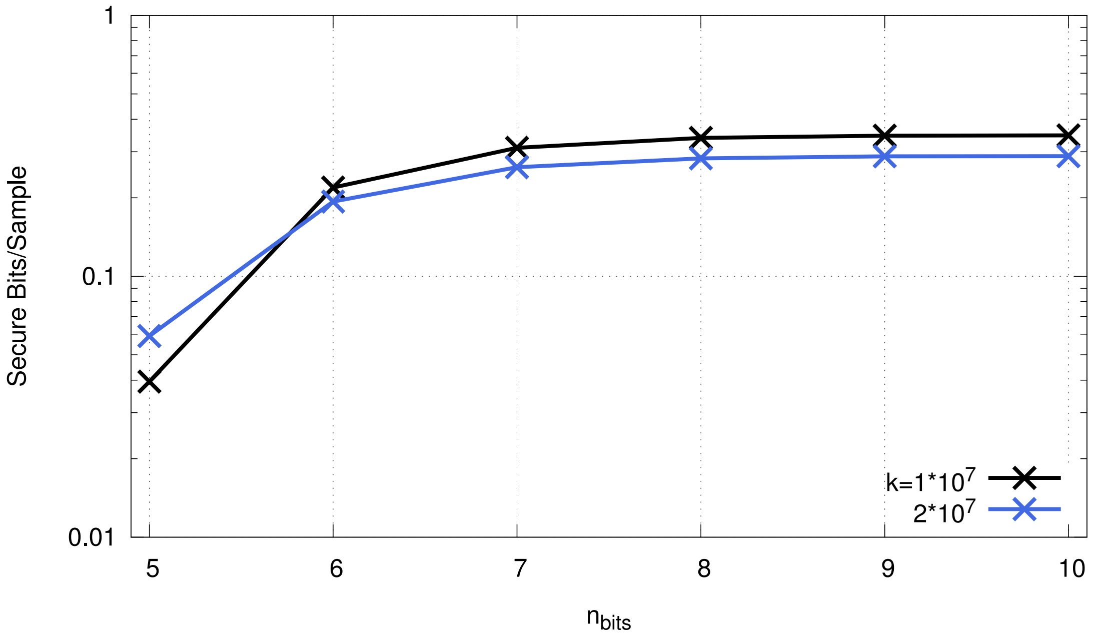


Figure 6.21: Secure key rate for $2N = 10^8$ measurements for two different number of samples k used for parameter estimation. For $n_{\text{bits}} \geq 8$ the number of secure bits is maximized.

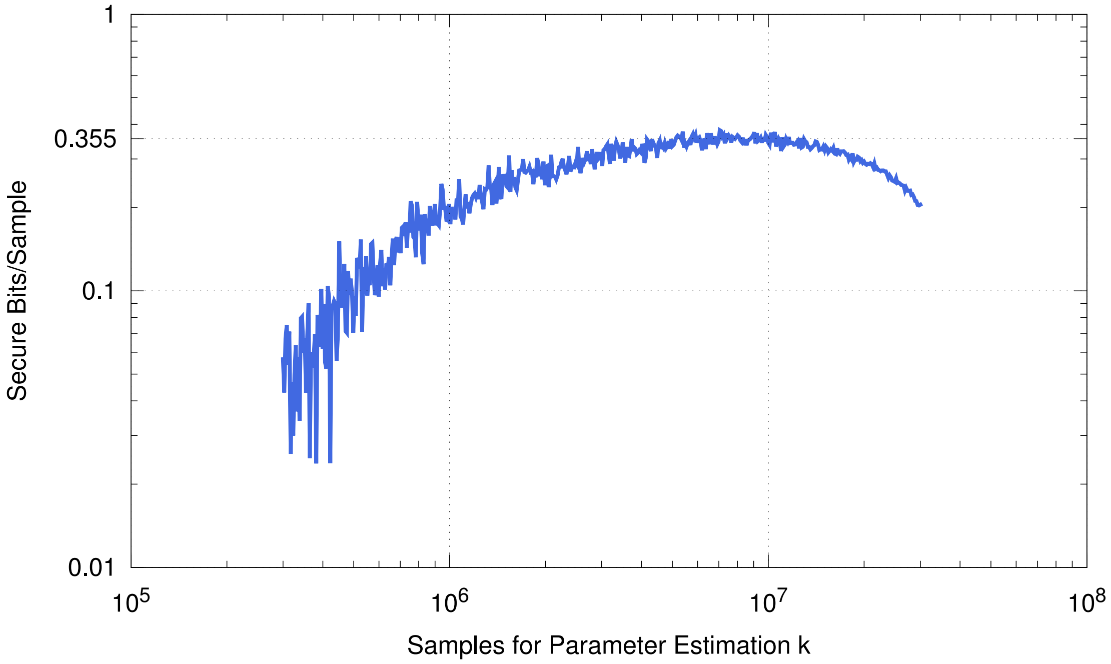


Figure 6.22: Secure key rate versus the number of samples k used for parameter estimation for $n_{\text{bits}} = 8$.

from the simulations described in Section 6.2. With this choice the length of the secure key generated from a total of 10^8 samples, is 0.355×10^8 bits which is also in good agreement with the value obtained from Fig. 6.9.

6.5.2 Generation of a Secret Key using Post Selection

With the measured $2N = 10^8$ samples we generated a secure key from both quadratures using the post selection feature introduced in Chapter 5.4 and a binary error correction algorithm. To be able to use an error correction algorithm that works on a binary alphabet instead of a non-binary one as assumed in the simulations, the obtained bit error rate needs to be reduced. This is accomplished by the post selection. The protocol parameters we used were α as 6 times the standard deviation of the respective quadrature, $n_{\text{bits}} = 6$, $\epsilon_s = \epsilon_c = 10^{-16}$, $\epsilon_{\text{pe}} = 10^{-10}$ and $k = 10^7$. The non-optimal choice of n_{bits} was devoted to the fact that with an increasing number of intervals the number of bit errors after binning increases. However, better error correction efficiencies are achieved with less errors.

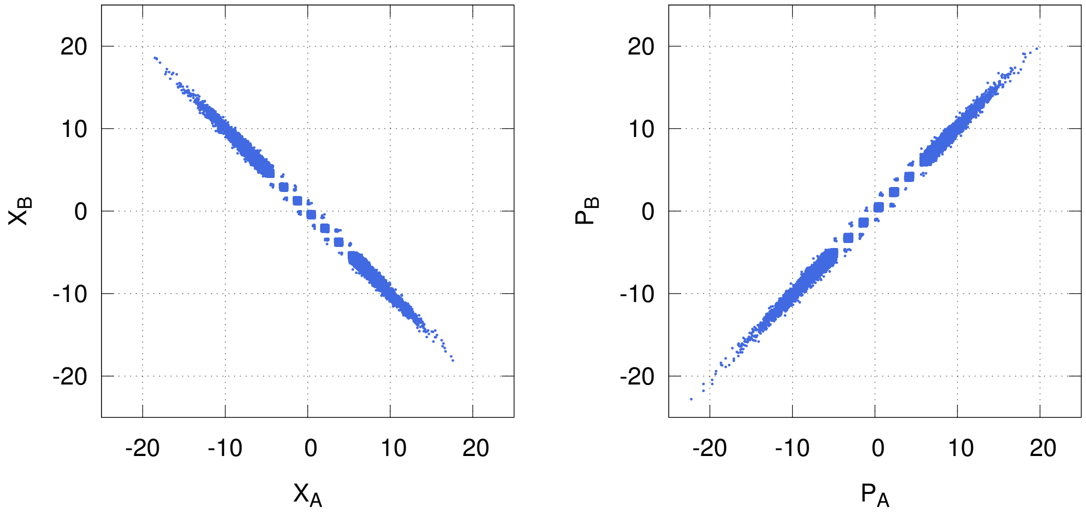
Parameter Estimation From the k revealed samples the covariance matrix of the state was estimated. It reads

$$\gamma = \begin{pmatrix} 19.696 & (0) & -19.678 & (0) \\ (0) & 23.311 & (0) & 23.708 \\ -19.678 & (0) & 19.817 & (0) \\ (0) & 23.708 & (0) & 24.314 \end{pmatrix}, \tag{6.7}$$

where the numbers in parentheses were not determined.

Binning and Post Selection Enumerating the 64 intervals like in the protocol description in Section 5.4.1 from the left to the right, we omitted the intervals $27, 29, 31, 33, 35$ and 37 by post selecting both Alice's and Bob's data. The effect of the post selection is shown in Fig. 6.23. Figure 6.23a shows a scatter plot of the amplitude quadrature measurement outcomes of simultaneous measurements at Alice and Bob. A scatter plot for phase quadrature outcomes at both parties is shown in Fig. 6.23b. While without post selection a histogram of the measurement outcomes would follow a Gaussian distribution, the pattern visible in the middle of the plots is caused by the post selection. The plots indicate not only the width of the remaining intervals in the middle but also the reduction of the error rate. Note, that because of the equal width of the intervals most samples belong into the inner intervals.

To obtain a bit representation of the raw key, each interval is assigned a unique bit combination of 6 bits. Thus, each of the remaining samples after post selection is

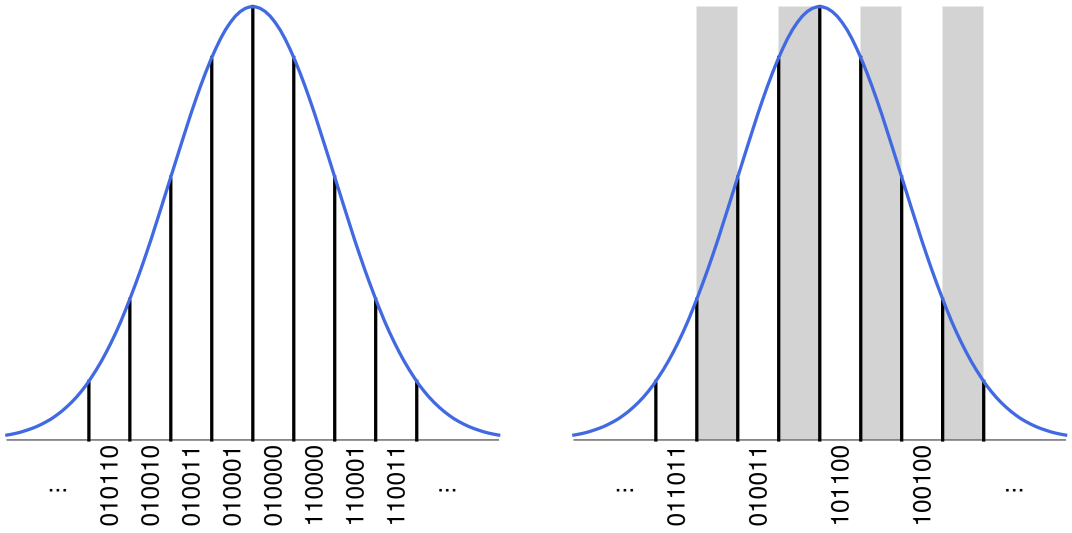


(a) Amplitude Quadrature **(b)** Phase Quadrature

Figure 6.23: Scatter plots of the outcomes of Alice and Bob simultaneously measuring amplitude or phase quadrature. The figure shows the effect of the post selection procedure. The interval width can clearly be seen by the five small squares in the middle.

assigned a bit string representing the interval the sample is mapped to. Since the error correction works best for small bit error rates and a uniform distribution of zeros and ones, special care has to be taken of the bit assignment to the intervals. For the bit assignment we used a modification of a common Gray code, where the modification was developed in collaboration with Jörg Duhme. A Gray code [Gra53] is designed such that the bit representation of intervals next to each other differ only in one bit. This design keeps the error rate small as it is quite likely that a measurement outcome of one of the two parties falls into an adjacent interval of the one the outcome of the other party has fallen into. A part of a 6 bit Gray code is shown in Fig. 6.24a.

Figure 6.24b shows a part of the modified Gray code we used. The gray shaded intervals are the intervals that are removed by post selection. The bit representations of these intervals are not important and thus not shown. The code is designed such that the bit strings of the intervals that are next to each other without the removed ones again differ only in one bit. To obtain an as uniform bit distribution as possible, however, the two most inner intervals are represented by bit strings that are *bit flipped*. Even though this two intervals do not have exactly the same probability, the probabilities are similar as the interval width is small. Since at this interval the structure of the Gray code is broken, the bit error rate increases. However, the uniformity is more important for a high efficiency error correction algorithm than the error rate. The



(a) Regular Gray Code **(b)** Modified Gray Code

Figure 6.24: Illustration of a Gray code and the modified Gray code we used in our experiment. The gray shaded areas on the right indicate the intervals removed by post selection.

complete modified Gray code used in the experiment can be found in Appendix C.

With the modified Gray code we calculated the bit error rate versus measurement time which is shown in Fig. 6.25. For this purpose the remaining samples after post selection and parameter estimation were converted into two bit strings, one belonging to Alice and one belonging to Bob. The bit error rate was calculated by splitting Alice's and Bob's available bits into chunks of 10^5 bits and comparing them. The bit error rate showed only small drifts between 3.75 % and 3.90% during the measurement time which demonstrates the stability of the system.

Error Correction After raw key generation the unavoidable bit errors have to be corrected. The error correction algorithm used in this experiment was a low-density-parity-check (LDPC) code [Gal62]. An introduction to these codes can be found, for instance, in [Sho03]. The LDPC code we used here was implemented by the Austrian Institute of Technology (AIT). Since the algorithm worked on a block size of 256 kBit, the binary raw key was split into 446 blocks. For each block 68,160 parity bits were communicated from Alice to Bob, who corrected his raw key to fit Alice's. With a total of 446 processed blocks, 30,399,360 bits $\approx$ 30 MBit were disclosed. According to Chapter 5.3.5 the theoretical bound for the number of bits that have to be communicated to correct the errors, is given by $H(X_A|X_B)$. For the generated raw key it is 27,192,821 bits. Hence, the leakage parameter λ is given by ratio of

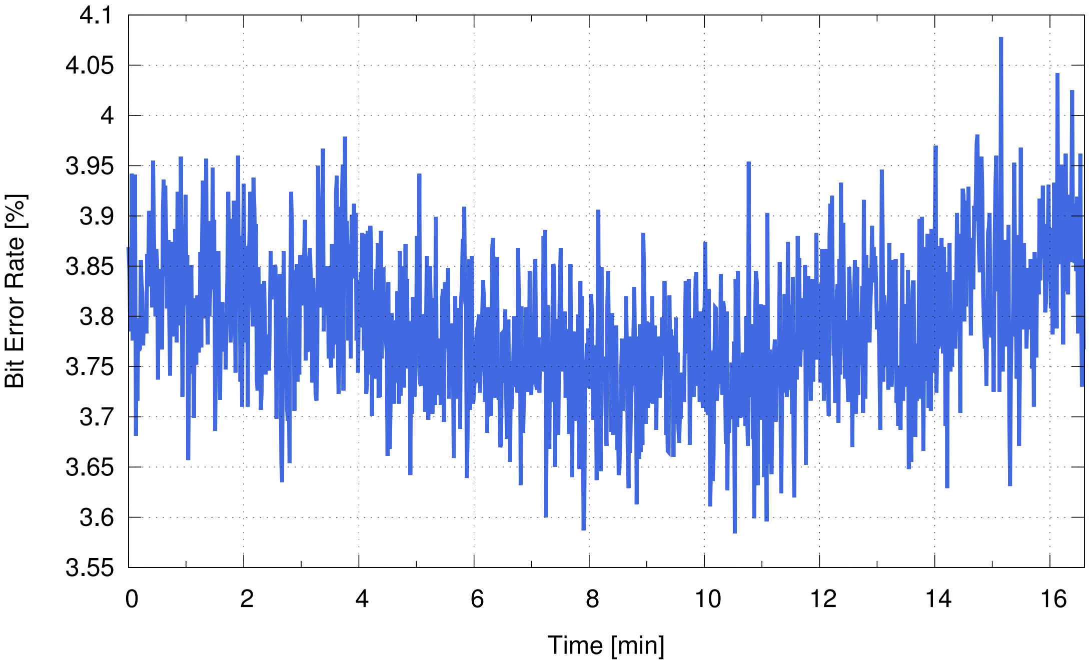


Figure 6.25: Bit error rate after post selection versus measurement time.

communicated bits and theoretical bound,

$$\lambda = \frac{30{,}399{,}360}{27{,}192{,}821} \approx 1.118 \ .$$

This corresponds to an error correction efficiency of $\beta = 96.4\,\%$, which is a remarkably high efficiency.

In the confirmation Alice and Bob check whether the error correction succeeded. For this purpose they both hashed their corrected raw key to 53 bits and compared the outcome. The size of the hash is given by the correctness parameter $\epsilon_c = 10^{-16}$ via $\log_2 \frac{1}{\epsilon_c}$. The correctness check was implemented by the software from the AIT.

Calculation of Secure Key Length Using the covariance matrix, which was reconstructed in the parameter estimation step, and calculating the entropy and max-entropy of the raw key from the measured samples (which includes the effect of the post selection), the secure key length was calculated to 42,353,303 bit. $\approx$ 42 MBit. From this the bits disclosed by the error correction had to be subtracted, however, the bits disclosed by the confirmation have already been included. Hence, the overall secure key length was 11,953,943 bit $\approx$ 11.95 MBit.

Privacy Amplification Privacy amplification reduces the total raw key length of 116,916,224 bit to the secure length of 11,953,943 bit by two-universal hash functions, cf. Chapter 5.4. This step was also implemented by the software from the AIT. With a reduction rate of 0.1022, the final secure key size was 11,948,832 bit ≈ 11.95 MBit or in bytes approximately 1.5 MB.

In Appendix D the first 7645 bits of the key are published.

6.6 Towards a Possible Local-Area Quantum Key Distribution Link

While in this thesis Alice and Bob were located at the same optical table, placing Bob somewhere else would demonstrate the feasibility of the protocol for real applications. The Institute for Gravitational Physics in Hanover is located about 1 km apart from the Institute of Quantum Optics. The two institutes are connected with two standard telecommunication fibers. A measurement of the transmission of these fibers yielded 43 % and 56 % for a wavelength of 1550 nm. The low transmission is probably due to the many fiber connectors as the transmission line is split into 8 pieces.

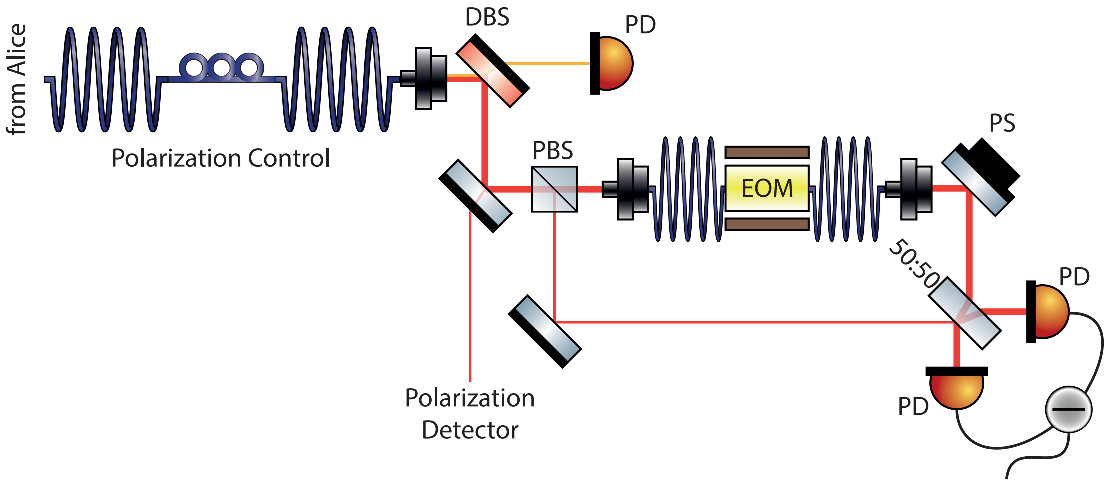
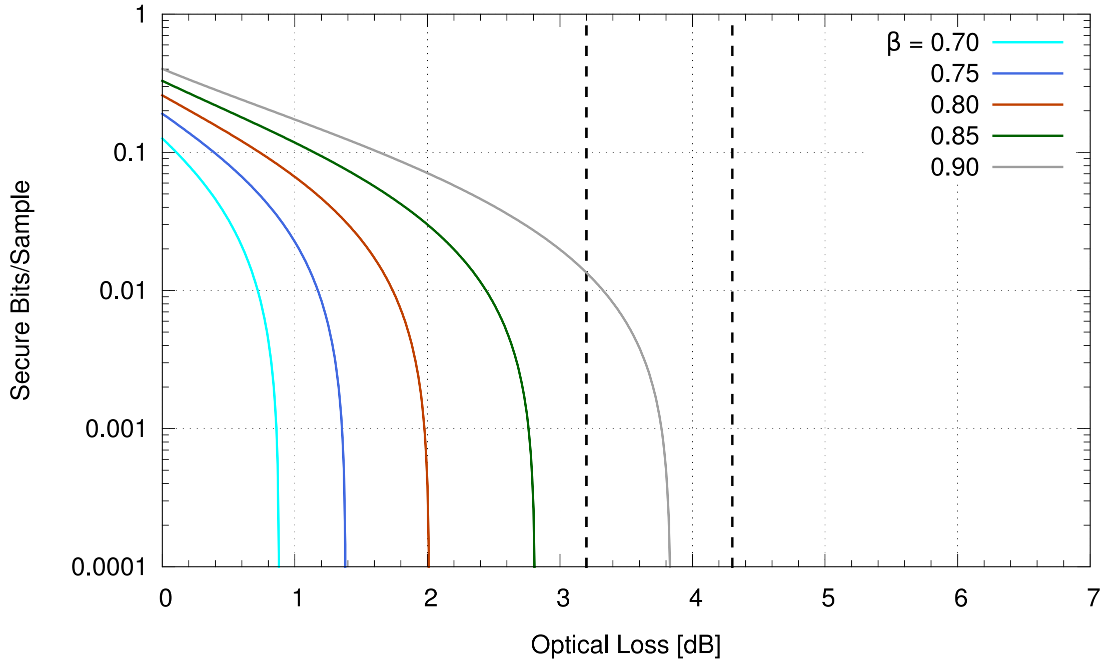


Figure 6.26: Proposed experimental setup for a remote detector. The local oscillator beam and the entangled mode are polarization multiplexed and transmitted through a standard telecommunication fiber. The two beams (red) are separated at a polarizing beam splitter and recombined at a balanced beam splitter for homodyne detection after the transmission of the local oscillator beam through a fiber-coupled electro-optical modulator which is used to apply phase shifts between both beams. For the synchronization of Alice's and Bob's measurement an auxiliary 1310 nm beam can be employed (orange). DBS: Dichroic Beam Splitter, PD: Photo Detector, PBS: Polarizing Beam Splitter, EOM: Electro-Optical Modulator, PS: Phase Shifter.

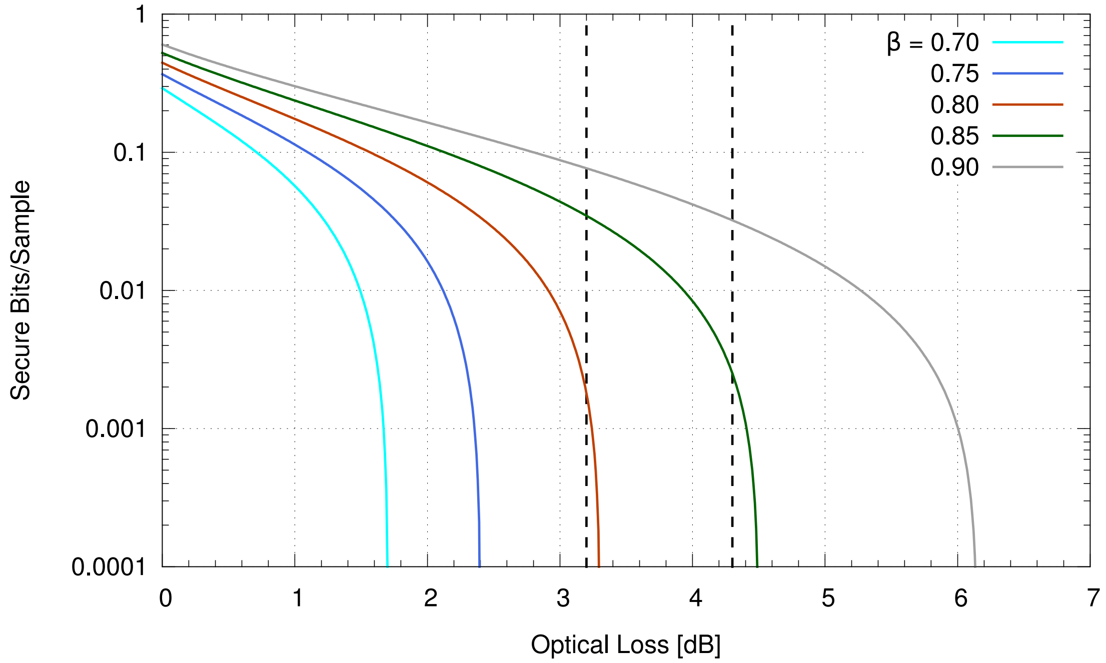
Figure 6.26 shows a possible implementation of a remote detector. The local oscillator, which is necessary for homodyne detection, is submitted through the fiber together with the entangled subsystem by polarization multiplexing. To separate the local oscillator beam from the entangled mode a polarizing beam splitter can be used. Since standard telecommunication fibers are not polarization maintaining, the polarization has to be controlled with a fiber-based polarization controller. To detect the polarization state a small fraction of the light can be tapped-off from the beam and detected by a polarization meter. Once the polarization is stabilized and the local oscillator is separated from the entangled mode, the local oscillator can be phase shifted with respect to the entangled mode according to the scheme presented in Section 6.3. For the locking of the local oscillator's phase the single sideband fields accompanying the entangled mode can be used. To be able to generate an error signal a phase-locked electronic local oscillator will be necessary. Such a signal may be obtained by frequency references used by the two parties which are locked to the global positioning system (GPS). To achieve synchronized measurements at Alice and Bob an auxiliary laser beam at 1310 nm can be employed which can be separated from the main 1550 nm beams by a dichroic beam splitter. By modulating the amplitude of this laser with a square wave, a clock for the measurements can be transferred. To close a possible loop-hole for an attacker, the power of the transmitted local oscillator has to be monitored during the QKD run [Lo07, Ma13]. If the local oscillator power is not monitored, an attacked could change the power and thereby the vacuum noise reference of Bob's balanced homodyne detector.

A simulation of the expected secure key rate is shown in Fig. 6.27. For the simulation we started at the covariance matrix from Eq. (4.11) which already includes detection loss. In the figure the secure key rates for different error correction efficiencies β are plotted versus the transmission line's optical loss. While for Fig. 6.27a the total number of measurements was 10^8, it was 10^9 for Fig. 6.27b. The black dashed lines in the figures indicate the expected total optical loss for the two available transmission lines. Besides the measured transmission of the fiber, we further included an optical coupling efficiency of 95 % of the free-space entangled mode to the optical fiber and additional propagation loss of 10 % caused by the polarization controller and imperfect optical components. For the simulation samples from both quadratures were taken into account, i.e. $p_X = 0.5$. Other simulation parameters were α as 8 times the standard deviation of the respective quadrature, $n_{\text{bits}} = 8$ for both quadratures and $\epsilon_s = \epsilon_c = \epsilon_{\text{pe}} = 10^{-16}$. The number of samples k used for parameter estimation was optimized to get the largest secure key rate.

For the available transmission line with the lower optical loss, a secure key can be generated for 10^8 samples with an error correction efficiency of 90 %, whereas for the transmission line with the higher optical loss no secure key is possible. Since a 90 %



(a) Number of total measurements: $2N = 10^8$.



(b) Number of total measurements: $2N = 10^9$.

Figure 6.27: Secure key rate for different error correction efficiencies β versus optical loss. The black dashed lines indicate the optical loss of the two transmission lines including additional propagation loss caused by the detection scheme.

error correction efficiency might be difficult to achieve for the given parameter regime, a measurement of 10^9 samples will be beneficial. Here, a secure key can already be generated with an error correction efficiency of 80 % for the low loss transmission line, and with 85 % efficiency for the lossier one.

6.7 Summary

To summarize, simulations have shown that QKD seems possible for the two EPR entanglement types described in Chapter 4. In both cases feasible distances between Alice and Bob are in the range of 10 to 20 km for reasonable numbers of measured samples on the order of 10^8 to 10^9. While for high error correction efficiencies entanglement generated by superimposing two squeezed vacuum modes yields larger key rates and distances for the same number of measured samples, for low error correction efficiencies it is beneficial to use entanglement generated by only one squeezed vacuum mode.

By the implementation of a sophisticated scheme for actively controlling all phases and for fast measurements with a random choice of quadrature for each measurement, 10^8 samples could be recorded. With these a key of about 1.5 MB size, which was secure under collective attacks, was generated. This was achieved by using a post selection technique and a binary error correction with a high efficiency.

Furthermore, an experimental setup for Bob's detector being at another location was proposed. Simulations have shown that a QKD link between the Institute for Gravitational Physics and the Institute of Quantum Optics in Hanover is feasible using the existing fiber connections.

CHAPTER 7

Quantum Key Distribution under General Attacks

Overview

The development of continuous-variable QKD began in the early 2000s, however, only in 2012 a security proof providing composable security under general attacks with a finite number of samples was published [Fur12b]. The protocol employs two-mode squeezed vacuum states with highly entangled states and low optical loss. This chapter experimentally demonstrates the feasibility of the generation of such a composable secret key with the setup presented in Chapter 6 by following the protocol which was introduced in Chapter 5.5.

This chapter is organized as follows. Section 7.1 describes the experimental determination of the optimal protocol parameters. Using these optimal parameters Section 7.2 presents the execution of the QKD protocol up to the error correction step. It is shown that the generation of a secret key is possible with an error correction code that has an efficiency larger than 83.7 %. Finally, Section 7.3 summarizes the results.

7.1 Determination of Protocol Parameters

Using a pump power of about 200 mW and 150 mW for the two squeezed-light sources, respectively, 2×10^8 samples were recorded measured with Alice's and Bob's homodyne detectors with random quadrature choice according to the scheme presented in Chapter 6.3. Furthermore, a vacuum noise reference was recorded prior to the run of the protocol for normalization purposes by blocking the signal input ports of the homodyne detectors. To determine the optimal parameters of the protocol, which are the cut-off value α, the scaling factors and the number of samples k used in the parameter estimation step, a characterization of the quantum states in a trusted environment is helpful. A trusted environment means that Alice and Bob are sure that no eavesdropper is present. If that is not possible, the protocol can still be executed with non-optimal parameters, which reduces the key rate. However, security can still be guaranteed. In a trusted environment Alice and Bob are able to characterize the quantum states by state tomography. For the state used here, the reconstructed covariance matrix reads

$$\gamma = \begin{pmatrix} 21.932 & (0) & -22.092 & (0) \\ (0) & 24.891 & (0) & 25.229 \\ -22.092 & (0) & 22.436 & (0) \\ (0) & 25.229 & (0) & 25.772 \end{pmatrix}, \tag{7.1}$$

where the numbers in the parentheses were not measured since they are unimportant for the characterization of the protocol's parameters. Due to a slight asymmetry of the field quadrature variances of Alice's and Bob's state, they have to scale their samples with the scaling factors given in Tab. 7.1 to yield the same variance. The asymmetries might have been arisen due to an imperfect balance of the beam splitter used for the generation of entanglement or due to asymmetric optical loss.

Quadrature	Alice	Bob
Amplitude	1.00569	0.99434
Phase	1.00873	0.99134

Table 7.1: Scaling parameters for Alice's and Bob's measured samples to yield a symmetric variance of the field quadratures.

From the covariance matrix we simulated the secure key rate under general attacks assuming an error correction efficiency of $\beta = 95\,\%$. Figure 7.1 shows the results given as secure bits per number of measured samples versus the number of measured samples. The security parameters were set to $\epsilon_s = \epsilon_c = 10^{-6}$. For each value on the x-axis the cut-off parameter α and the number of samples k used for parameter estimation were optimized to yield a maximal key rate. The different curves are shown for different interval widths δ defined by α and the number of intervals $2^{n_{\text{bits}}}$ by the relation $\delta = \frac{2\alpha}{2^{n_{\text{bits}}}}$. The optimal key rate is achieved using $n_{\text{bits}} \geq 10$. Positive key rates are expected for more than 2.8×10^7 measured samples. For 2×10^8 samples the expected key rate from the simulation is about 0.14 bits/sample. For this value the optimal cut-off parameter is $\alpha = 50.2$ and the optimal number of samples for parameter estimation is $k = 2 \times 10^7$. From the simulation we expect the security parameter d_{PE}, which is determined in the parameter estimation step of the protocol, to be approximately 3.54 for $n_{\text{bits}} = 10$.

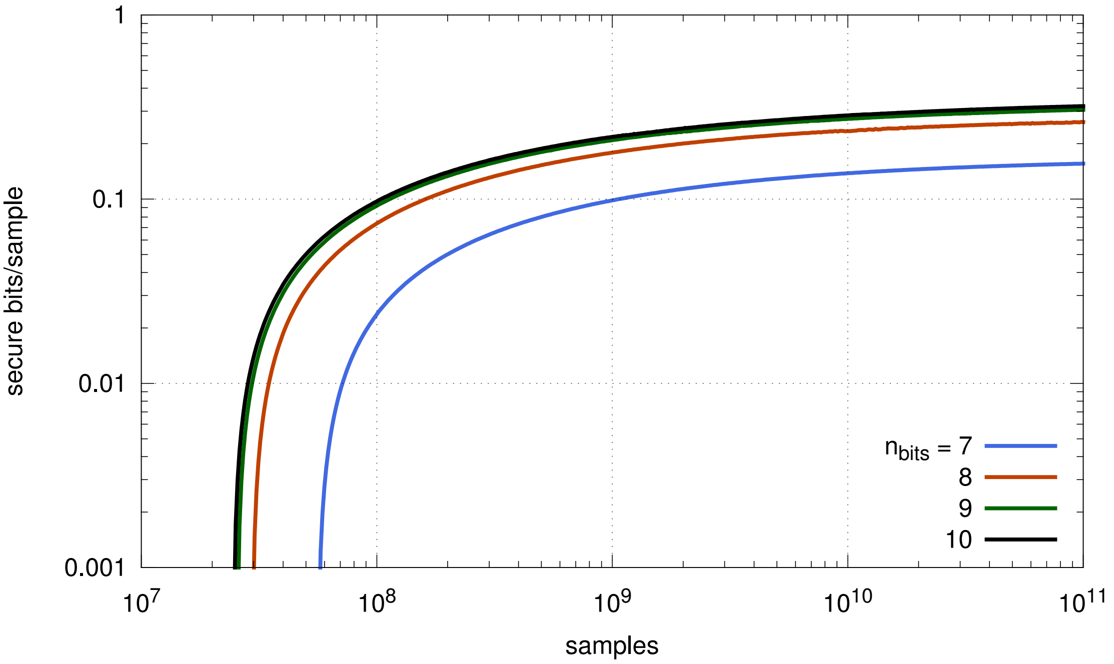


Figure 7.1: Simulated secure key rate under general attacks versus the number of measured samples. The different curves are plotted for a different number of intervals $2^{n_{\text{bits}}}$. The cut-off parameter α and the number of samples k used for parameter estimation were optimized to yield a maximal key rate.

7.2 Demonstration of the Feasibility of Secret Key Generation

After the determination of the protocol's optimal parameters the protocol was executed and 2×10^8 samples were recorded by homodyne measurements. Due to the lack of an error correction algorithm, we analyzed the measured samples to demonstrate the feasibility of extracting a secret key. In a first step the abort condition has to be checked, namely that no sample exceeded α. Table 7.2 shows the maximal and minimal values of the scaled data measured by Alice and Bob. Hence, $\alpha = 50.2$ is by far not exceeded and the protocol was not aborted.

	Alice	Bob
Min	-30.0505	-30.4676
Max	30.5348	29.7306

Table 7.2: Minimal and maximal measurement outcomes of Alice and Bob after scaling to check the abort conditions.

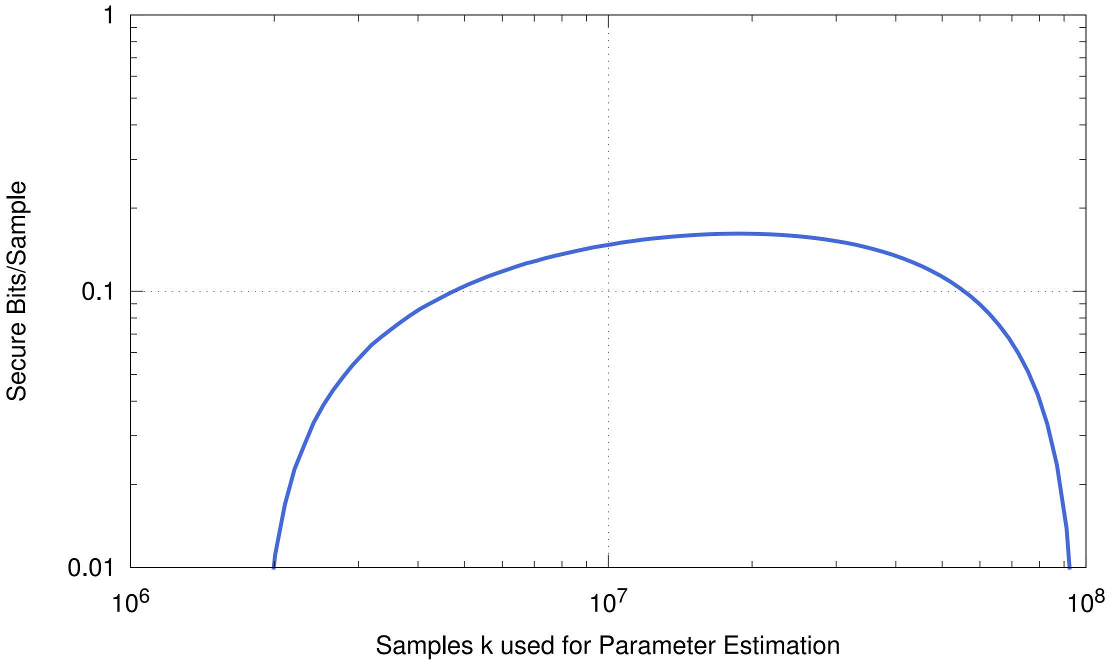


Figure 7.2: Secure key rate versus the number of samples k used for parameter estimation for $n_{\text{bits}} = 10$. For each value of k, k samples were chosen at random from the samples left after sifting and the secure key rate was determined.

After sifting 100,001,118 samples remained which were binned into intervals as given in the protocol description, cf. Chapter 5.5. Here, we used $n_{\text{bits}} = 10$.

To determine the effect of the number of samples k used for parameter estimation, we calculated the secure key rate for $n_{\text{bits}} = 10$ assuming an error correction efficiency of 95 %. The curve in Fig. 7.2 was calculated by drawing k samples at random from the samples left after sifting and by determining the security parameter d_{PE} according to Eq. (5.43). The maximal key rate of 0.16 bits/sample is achieved for $k = 1.87 \times 10^7$ samples.

Using this value for k we calculated a histogram of the security parameter d_{PE} which is shown in Fig. 7.3. The histogram was computed by drawing 3,000 times k samples at random and calculating d_{PE} for each set of samples. The histogram shows the narrow distribution of d_{PE}. A fit of a Gaussian distribution, shown as the red solid line in the figure, revealed $d_{\text{PE}} = 3.5386 \pm 0.0006$.

Figure 7.4 shows the dependence of the secret key rate under general attacks on the error correction efficiency. A secret key can be extracted with an error correction efficiency larger than 83.7 %. This shows that even though we assumed an error correction efficiency of 95 % to calculate the secure key rates above, a secret key can even be distilled with lower efficiencies which are more likely to be achieved.

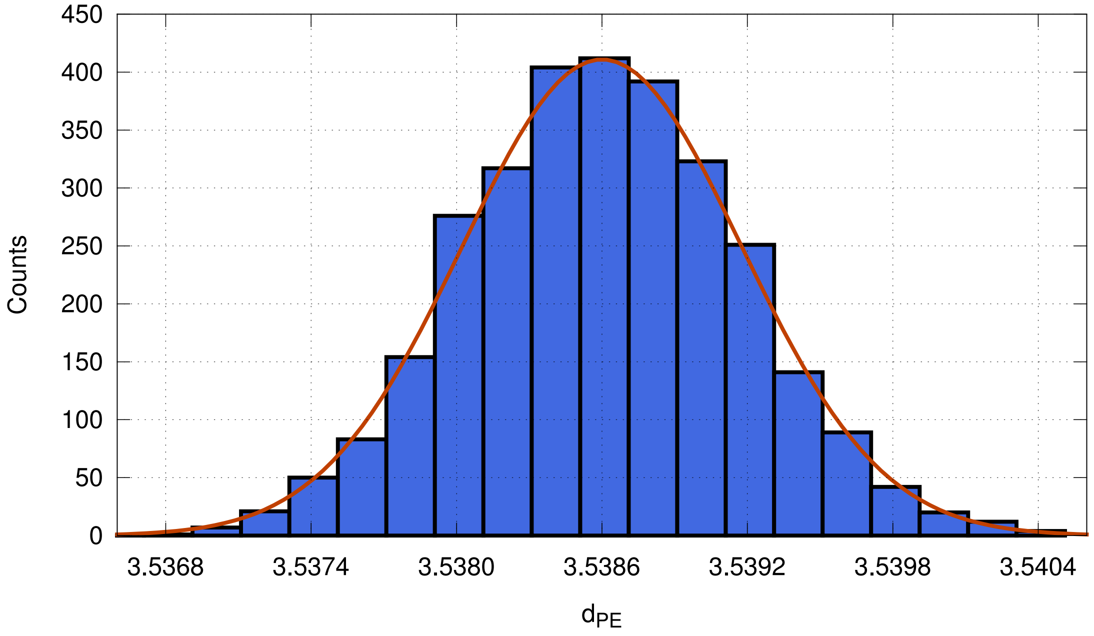


Figure 7.3: Histogram of security parameter d_{PE} calculated by drawing 3,000 times $k = 1.87 \times 10^7$ samples at random from the samples left after sifting. The red curve shows a Gaussian distribution fitted to the data.

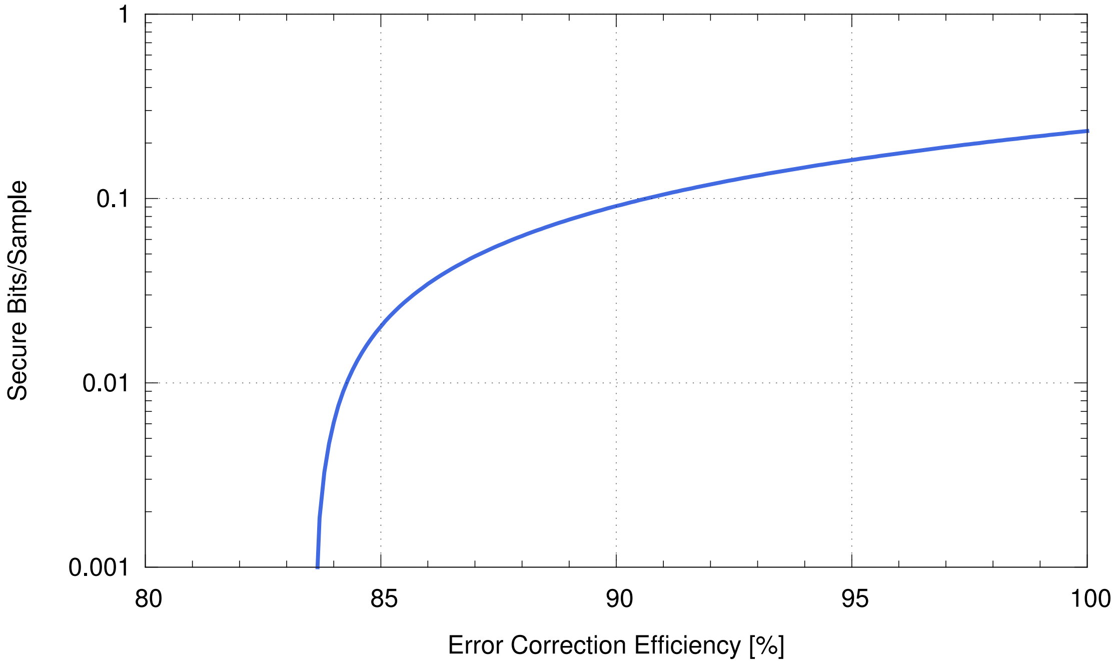


Figure 7.4: Secure key rate versus error correction efficiency.

7.3 Summary

To summarize, it was experimentally demonstrated for the first time that a continuous-variable QKD system, which is secure under general attacks, is feasible. By measuring 2×10^8 samples of two-mode squeezed vacuum states with a random quadrature choice an error correcting code with an efficiency larger than 83.7 % would be necessary to distill a secret key. Assuming an error correction efficiency of 85 % this would yield a secret key of 4 MBit size. The size of the secret key can be increased by a factor of 10 if an error correction with 95 % efficiency will be used instead.

Since error correction codes with high efficiencies are available for binary alphabets, cf. Chapter 6.5, and error correction codes working on a non-binary alphabet exist [Ulr57], it seems feasible that a code which fulfills the requirements set here, can be developed.

CHAPTER 8

Summary and Outlook

The demonstration of a complete implementation of a continuous-variable QKD system which is secure under general attacks, and whose keys have a finite size, is one of the most desired goals in the field of quantum cryptography. The first quantitative security analysis [Fur12b] of such a protocol is based on EPR entangled states with challenging but feasible parameters. Its realization requires 10 dB squeezed vacuum states, low optical loss and a measurement of at least 10^8 samples.

In this thesis the feasibility of such a continuous-variable QKD system with security under general attacks was demonstrated by an execution of the protocol up to the error correction step. Simulations have shown that the error correction efficiency which is at least necessary to distill a secret key is 83.7 %. While a non-binary error correction code with the required performance does not exist yet, this result provides a high motivation for the development of such an algorithm. Existing binary error correction codes can reach efficiencies of more than 95 % [Jou13] as demonstrated by the code provided by the AIT used in this thesis for another experiment. Thus, it seems feasible that non-binary codes might reach the required efficiency in the given setting by optimizing existing codes for Gaussian distributed values. Since the experimental data recorded for this thesis can be used to distill a secret key when an error correction code, which fulfills the requirements, becomes available, the results of this thesis pave the way for the first demonstration of a complete continuous-variable finite-size QKD system which is secure under general attacks.

The feasibility demonstration required a stable setup with strong EPR entangled states and a measurement of each of the 2×10^8 samples in either the amplitude or phase quadrature. The latter was achieved by a detection scheme developed in this thesis, which enabled homodyne measurements with random choice of quadrature at a rate of 100 kHz. The strong EPR entanglement was generated by superimposing two squeezed vacuum modes whose squeezed quadrature variances were more than 10 dB below the variance of the vacuum state. The observed entanglement at the telecommunication wavelength of 1550 nm exceeded 10 dB for the Duan inseparability criterion and represents the strongest EPR entanglement ever observed. The stable operation could be achieved by a new phase locking scheme, which was developed in this thesis. The observed entanglement and its stability will also make new highly demanding quantum information protocols possible, like the superactivation of zero-capacity channels [Smi11].

This thesis also presented the first demonstration of the EPR paradox for entangled states generated by superimposing a squeezed vacuum mode with a vacuum mode. Despite this vacuum contribution, remarkably strong EPR entanglement could be verified. This result might simplify the implementation of (future) quantum information protocols. One of them is continuous-variable QKD with the restriction of the adversary to collective attacks. Since an implementation of a collective attack requires quantum memories, collective attacks are, although a restriction, difficult to achieve experimentally. Simulations in this thesis have shown that QKD distances between Alice and Bob of up to 20 km are feasible with such states.

With the restriction to collective attacks a complete QKD protocol was implemented using the entangled states generated by two squeezed vacuum resources. With 10^8 measurements, a secret key of 1.5 MB size was distributed in a table-top setup. Since simulations in this thesis have shown that distances between Alice and Bob of up to 30 km are reasonable using these states and state-of-the-art fiber technology, a possible implementation of Bob's remote detector was proposed. By measuring 10^9 samples, a QKD link between the Institute for Gravitational Physics and the Institute of Quantum Optics in Hanover seems feasible with existing fiber links.

CHAPTER A

Electronics

In the following you will find the schematic of a resonant photo detector which was used to lock the squeezed-light source's cavity length and the pump phase. This circuit was developed in collaboration with Sebastian Steinlechner. You will also find a schematic of the homodyne detector which was developed for the QKD experiments within the framework of this thesis.

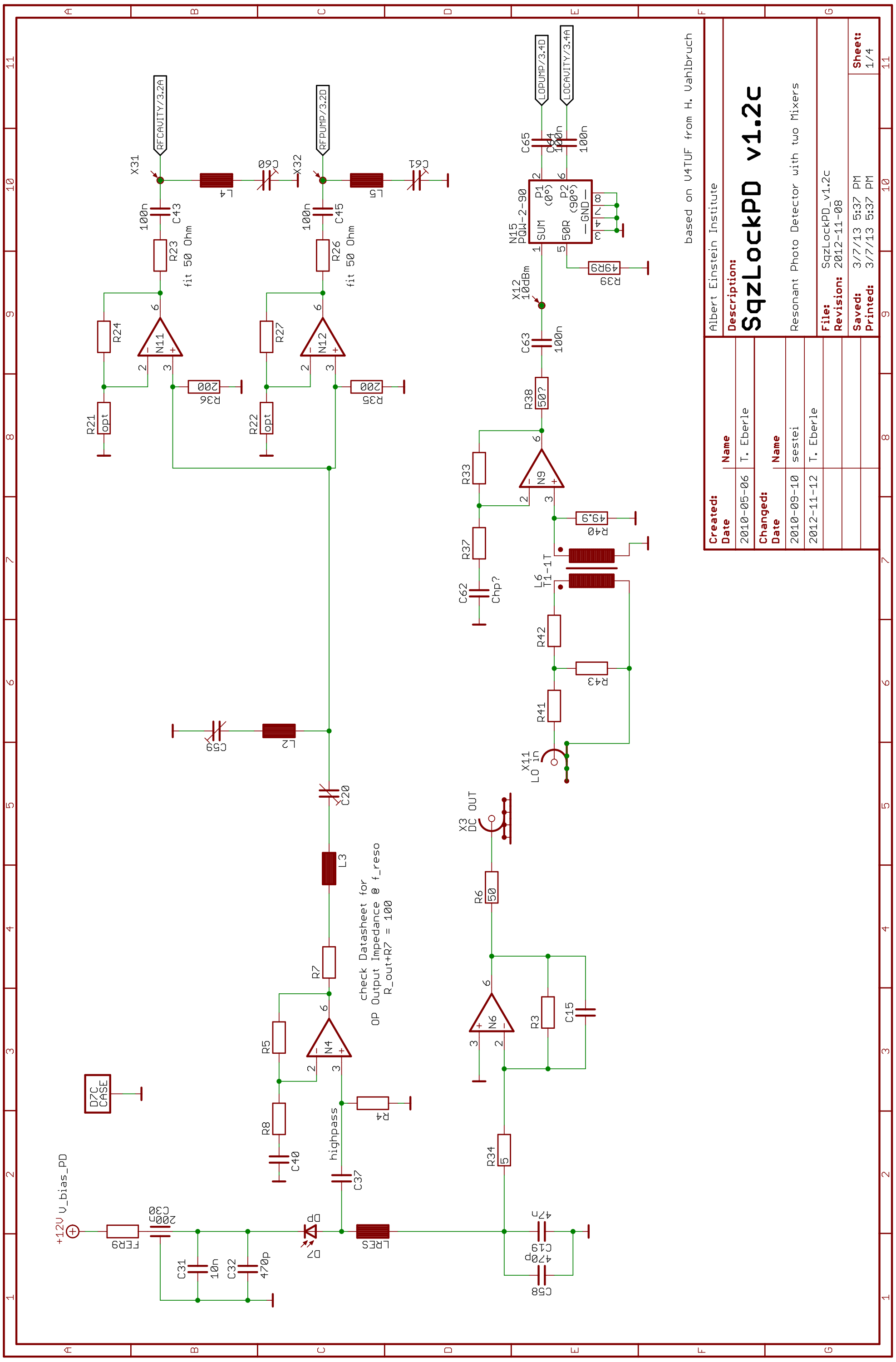
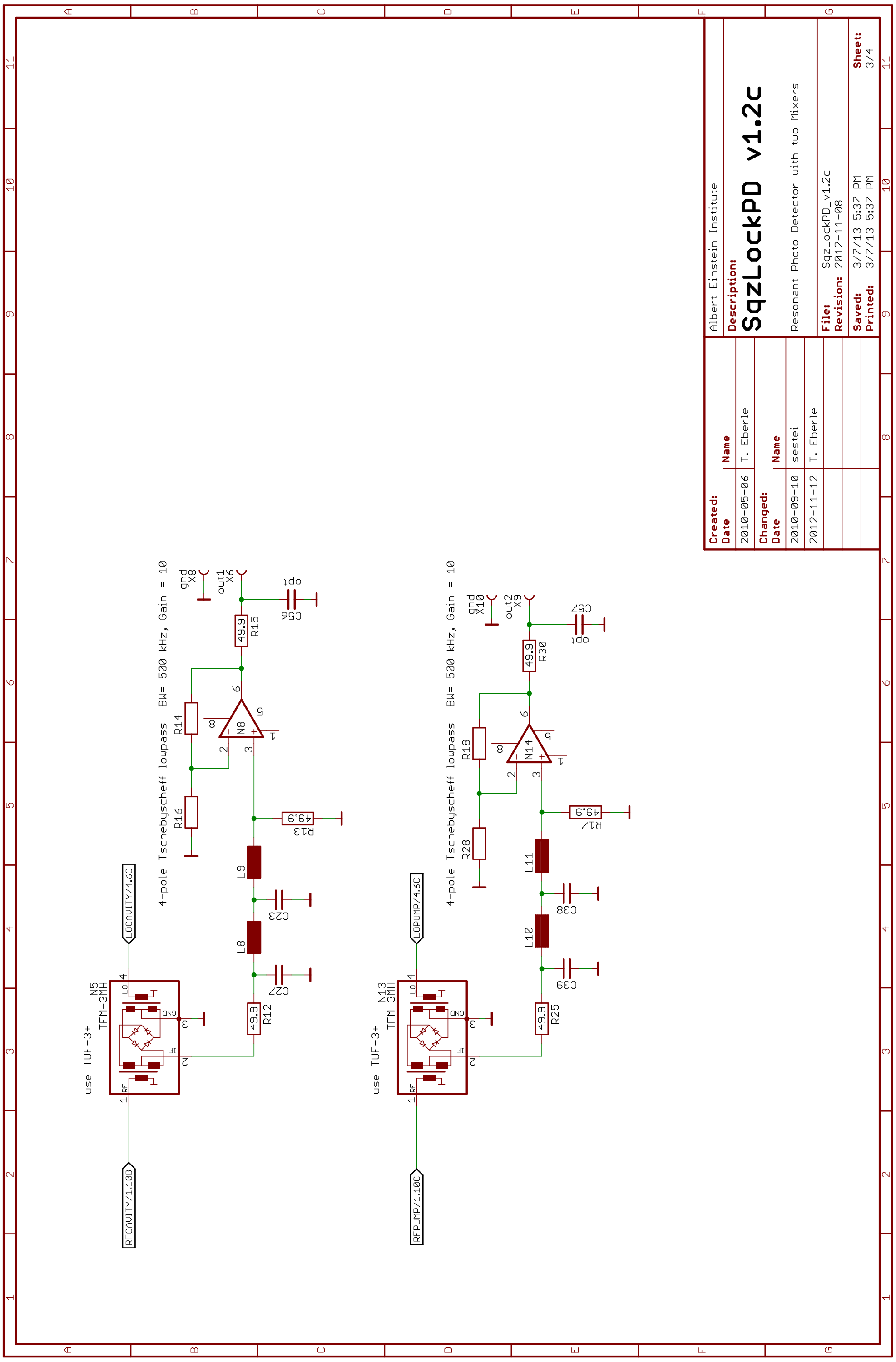


Figure A.1: Schematic of a resonant photo detector whose photo current is demodulated with two electronic local oscillators which are 90° out of phase. This circuit was developed in collaboration with Sebastian Steinlechner.


Albert Einstein Institute
Description:
SqzLockPD v1.2c
Resonant Photo Detector with two Mixers
File: SqzLockPD_v1.2c
Revision: 2012-11-08
Saved: 3/7/13 5:37 PM
Printed: 3/7/13 5:37 PM
Sheet: 3/4
Created:
Date
Name
2010-05-06
T. Eberle
Changed:
Date
Name
2010-09-10
sestei
2012-11-12
T. Eberle
4-pole Tschebyscheff lowpass BW= 500 kHz, Gain = 10
4-pole Tschebyscheff lowpass BW= 500 kHz, Gain = 10
use TUF-3+
TFM-3MH
N5
use TUF-3+
TFM-3MH
N13
RFCAVITY/1.10B
LOCAVITY/4.6C
RFPUMP/1.10C
LOPUMP/4.6C
RF
LO
GND
IF
R12
49,9
C27
L8
C23
L9
R13
49,9
R16
R14
N8
R15
49,9
C56
opt
out1
X6
gnd
X8
R25
49,9
C39
L10
C38
L11
R17
49,9
R28
R18
N14
R30
49,9
C57
opt
out2
X9
gnd
X10
A
B
C
D
E
F
G
1
2
3
4
5
6
7
8
9
10
11

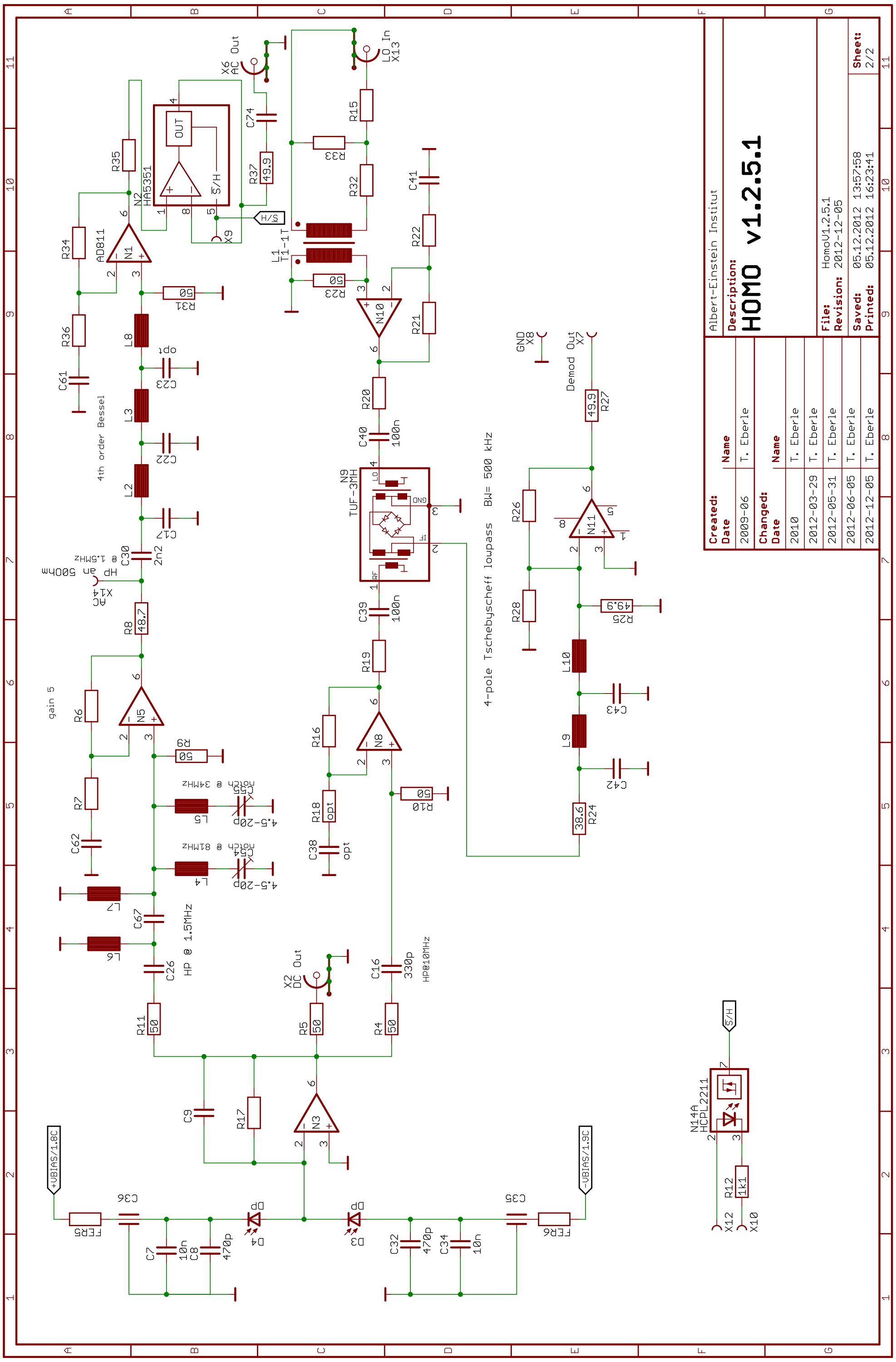


Figure A.2: Schematic of the homodyne detector electronics used for the quantum key distribution experiments. The electronic circuit was developed in the framework of this thesis. The AC output of the detector can be set to hold with a sample-and-hold circuit to prevent the analog-to-digital converter’s front-end to saturate during phase steps.

Chapter B

Random Number Test Results

In Tab. B.1 more detailed results of the NIST test suite testing the random numbers generated in Chapter 6.4 are given. The minimum pass rate is approximately 980 for 1000 test runs and approximately 591 for 605 test runs. The p-value gives the result of the uniformity test of the p-values of the statistical tests of the random numbers.

Test	Passed	p-value
Frequency	990/1000	0.422638
BlockFrequency	994/1000	0.26093
CumulativeSums	992/1000	0.478839
CumulativeSums	991/1000	0.402962
Runs	995/1000	0.202268
LongestRun	988/1000	0.518106
Rank	992/1000	0.5221
FFT	983/1000	0.120909
NonOverlappingTemplate	989/1000	0.820143
NonOverlappingTemplate	984/1000	0.572847
NonOverlappingTemplate	993/1000	0.285427
NonOverlappingTemplate	987/1000	0.846338
NonOverlappingTemplate	988/1000	0.890582
NonOverlappingTemplate	993/1000	0.980341
NonOverlappingTemplate	991/1000	0.721777
NonOverlappingTemplate	990/1000	0.607993
NonOverlappingTemplate	986/1000	0.903338
NonOverlappingTemplate	995/1000	0.017186
NonOverlappingTemplate	989/1000	0.225998

NonOverlappingTemplate	984/1000	0.568739
NonOverlappingTemplate	988/1000	0.635037
NonOverlappingTemplate	989/1000	0.869278
NonOverlappingTemplate	991/1000	0.146982
NonOverlappingTemplate	990/1000	0.404728
NonOverlappingTemplate	990/1000	0.897763
NonOverlappingTemplate	989/1000	0.014150
NonOverlappingTemplate	988/1000	0.437274
NonOverlappingTemplate	992/1000	0.282626
NonOverlappingTemplate	994/1000	0.635037
NonOverlappingTemplate	989/1000	0.999340
NonOverlappingTemplate	989/1000	0.653773
NonOverlappingTemplate	992/1000	0.697257
NonOverlappingTemplate	985/1000	0.530120
NonOverlappingTemplate	992/1000	0.217857
NonOverlappingTemplate	993/1000	0.146982
NonOverlappingTemplate	993/1000	0.897763
NonOverlappingTemplate	990/1000	0.741918
NonOverlappingTemplate	993/1000	0.900569
NonOverlappingTemplate	986/1000	0.620465
NonOverlappingTemplate	992/1000	0.999698
NonOverlappingTemplate	987/1000	0.229559
NonOverlappingTemplate	993/1000	0.866097
NonOverlappingTemplate	993/1000	0.632955
NonOverlappingTemplate	995/1000	0.253122
NonOverlappingTemplate	990/1000	0.651693
NonOverlappingTemplate	986/1000	0.645448
NonOverlappingTemplate	992/1000	0.153763
NonOverlappingTemplate	990/1000	0.442831
NonOverlappingTemplate	993/1000	0.345650
NonOverlappingTemplate	989/1000	0.666245
NonOverlappingTemplate	995/1000	0.745908
NonOverlappingTemplate	989/1000	0.365253
NonOverlappingTemplate	991/1000	0.973718
NonOverlappingTemplate	995/1000	0.289667
NonOverlappingTemplate	994/1000	0.465415
NonOverlappingTemplate	991/1000	0.177628
NonOverlappingTemplate	989/1000	0.105618
NonOverlappingTemplate	992/1000	0.550347

NonOverlappingTemplate	988/1000	0.279844
NonOverlappingTemplate	981/1000	0.112047
NonOverlappingTemplate	991/1000	0.945296
NonOverlappingTemplate	984/1000	0.496351
NonOverlappingTemplate	987/1000	0.908760
NonOverlappingTemplate	990/1000	0.928857
NonOverlappingTemplate	993/1000	0.490483
NonOverlappingTemplate	984/1000	0.378705
NonOverlappingTemplate	997/1000	0.148653
NonOverlappingTemplate	993/1000	0.429923
NonOverlappingTemplate	990/1000	0.614226
NonOverlappingTemplate	988/1000	0.637119
NonOverlappingTemplate	981/1000	0.162606
NonOverlappingTemplate	995/1000	0.486588
NonOverlappingTemplate	996/1000	0.484646
NonOverlappingTemplate	988/1000	0.366918
NonOverlappingTemplate	994/1000	0.169044
NonOverlappingTemplate	993/1000	0.896345
NonOverlappingTemplate	993/1000	0.444691
NonOverlappingTemplate	993/1000	0.593478
NonOverlappingTemplate	988/1000	0.530120
NonOverlappingTemplate	990/1000	0.452173
NonOverlappingTemplate	987/1000	0.953089
NonOverlappingTemplate	992/1000	0.126658
NonOverlappingTemplate	989/1000	0.790621
NonOverlappingTemplate	993/1000	0.837781
NonOverlappingTemplate	995/1000	0.853049
NonOverlappingTemplate	990/1000	0.796268
NonOverlappingTemplate	988/1000	0.262249
NonOverlappingTemplate	989/1000	0.163513
NonOverlappingTemplate	991/1000	0.245490
NonOverlappingTemplate	993/1000	0.002484
NonOverlappingTemplate	994/1000	0.662091
NonOverlappingTemplate	991/1000	0.242986
NonOverlappingTemplate	989/1000	0.684890
NonOverlappingTemplate	982/1000	0.792508
NonOverlappingTemplate	988/1000	0.783019
NonOverlappingTemplate	991/1000	0.083018
NonOverlappingTemplate	991/1000	0.156373

NonOverlappingTemplate	989/1000	0.141256
NonOverlappingTemplate	989/1000	0.556460
NonOverlappingTemplate	987/1000	0.274341
NonOverlappingTemplate	991/1000	0.292519
NonOverlappingTemplate	991/1000	0.105618
NonOverlappingTemplate	990/1000	0.212184
NonOverlappingTemplate	992/1000	0.739918
NonOverlappingTemplate	988/1000	0.108791
NonOverlappingTemplate	988/1000	0.753844
NonOverlappingTemplate	990/1000	0.928857
NonOverlappingTemplate	990/1000	0.672470
NonOverlappingTemplate	991/1000	0.719747
NonOverlappingTemplate	989/1000	0.624627
NonOverlappingTemplate	993/1000	0.811080
NonOverlappingTemplate	989/1000	0.612147
NonOverlappingTemplate	986/1000	0.486588
NonOverlappingTemplate	990/1000	0.731886
NonOverlappingTemplate	990/1000	0.067300
NonOverlappingTemplate	992/1000	0.915317
NonOverlappingTemplate	991/1000	0.463512
NonOverlappingTemplate	992/1000	0.837781
NonOverlappingTemplate	989/1000	0.220159
NonOverlappingTemplate	991/1000	0.424453
NonOverlappingTemplate	990/1000	0.591409
NonOverlappingTemplate	987/1000	0.111389
NonOverlappingTemplate	981/1000	0.203351
NonOverlappingTemplate	994/1000	0.272977
NonOverlappingTemplate	985/1000	0.301194
NonOverlappingTemplate	990/1000	0.777265
NonOverlappingTemplate	989/1000	0.446556
NonOverlappingTemplate	986/1000	0.786830
NonOverlappingTemplate	990/1000	0.345650
NonOverlappingTemplate	984/1000	0.928857
NonOverlappingTemplate	990/1000	0.622546
NonOverlappingTemplate	991/1000	0.632955
NonOverlappingTemplate	995/1000	0.110083
NonOverlappingTemplate	993/1000	0.459717
NonOverlappingTemplate	991/1000	0.889118
NonOverlappingTemplate	990/1000	0.016717

NonOverlappingTemplate	988/1000	0.190654
NonOverlappingTemplate	987/1000	0.126658
NonOverlappingTemplate	982/1000	0.328297
NonOverlappingTemplate	986/1000	0.411840
NonOverlappingTemplate	989/1000	0.680755
NonOverlappingTemplate	989/1000	0.678686
NonOverlappingTemplate	990/1000	0.605916
NonOverlappingTemplate	989/1000	0.213309
NonOverlappingTemplate	991/1000	0.344048
NonOverlappingTemplate	993/1000	0.864494
NonOverlappingTemplate	986/1000	0.614226
NonOverlappingTemplate	991/1000	0.248014
NonOverlappingTemplate	988/1000	0.115387
NonOverlappingTemplate	988/1000	0.896345
NonOverlappingTemplate	994/1000	0.439122
NonOverlappingTemplate	992/1000	0.751866
NonOverlappingTemplate	984/1000	0.459717
NonOverlappingTemplate	993/1000	0.526105
NonOverlappingTemplate	987/1000	0.43359
NonOverlappingTemplate	992/1000	0.13264
OverlappingTemplate	987/1000	0.154629
Universal	987/1000	0.676615
ApproximateEntropy	992/1000	0.61007
RandomExcursions	601/605	0.008316
RandomExcursions	596/605	0.71126
RandomExcursions	597/605	0.673507
RandomExcursions	600/605	0.373906
RandomExcursions	600/605	0.39101
RandomExcursions	598/605	0.104062
RandomExcursions	599/605	0.993624
RandomExcursions	595/605	0.006702
RandomExcursionsVariant	601/605	0.235792
RandomExcursionsVariant	600/605	0.489508
RandomExcursionsVariant	600/605	0.847183
RandomExcursionsVariant	601/605	0.139257
RandomExcursionsVariant	601/605	0.043982
RandomExcursionsVariant	600/605	0.607646
RandomExcursionsVariant	602/605	0.649265
RandomExcursionsVariant	602/605	0.417519

RandomExcursionsVariant	600/605	0.330628
RandomExcursionsVariant	598/605	0.231756
RandomExcursionsVariant	598/605	0.002775
RandomExcursionsVariant	604/605	0.052219
RandomExcursionsVariant	604/605	0.396813
RandomExcursionsVariant	603/605	0.171079
RandomExcursionsVariant	605/605	0.476590
RandomExcursionsVariant	605/605	0.399734
RandomExcursionsVariant	605/605	0.248226
RandomExcursionsVariant	603/605	0.001462
Serial	996/1000	0.807412
Serial	994/1000	0.262249
LinearComplexity	989/1000	0.162606

Table B.1: Detailed test results of the NIST test suite.

Test	ntup	tsamples	psamples	p-value	Assessment
diehard_birthdays	0	100	100	0.3884704	PASSED
diehard_operm5	0	1000000	100	0.55251594	PASSED
diehard_rank_32x32	0	40000	100	0.99410513	PASSED
diehard_rank_6x8	0	100000	100	0.97719572	PASSED
diehard_bitstream	0	2097152	100	0.60253587	PASSED
diehard_opso	0	2097152	100	0.07574160	PASSED
diehard_oqso	0	2097152	100	0.68587200	PASSED
diehard_dna	0	2097152	100	0.18255631	PASSED
diehard_count_1s_str	0	256000	100	0.95503950	PASSED
diehard_count_1s_byt	0	256000	100	0.84876632	PASSED
diehard_parking_lot	0	12000	100	0.76062712	PASSED
diehard_2dsphere	2	8000	100	0.70029124	PASSED
diehard_3dsphere	3	4000	100	0.90753640	PASSED
diehard_squeeze	0	100000	100	0.36167153	PASSED
diehard_sums	0	100	100	0.27127137	PASSED
diehard_runs	0	100000	100	0.95206939	PASSED
diehard_runs	0	100000	100	0.63807658	PASSED
diehard_craps	0	200000	100	0.72016648	PASSED
diehard_craps	0	200000	100	0.69167638	PASSED
marsaglia_tsang_gcd	0	10000000	100	0.42416794	PASSED
marsaglia_tsang_gcd	0	10000000	100	0.66397295	PASSED

sts_monobit	1	100000	100	0.21857258	PASSED
sts_runs	2	100000	100	0.92528417	PASSED
sts_serial	1	100000	100	0.79439247	PASSED
sts_serial	2	100000	100	0.95162417	PASSED
sts_serial	3	100000	100	0.67673321	PASSED
sts_serial	3	100000	100	0.44488057	PASSED
sts_serial	4	100000	100	0.97921100	PASSED
sts_serial	4	100000	100	0.61503056	PASSED
sts_serial	5	100000	100	0.96431388	PASSED
sts_serial	5	100000	100	0.81003836	PASSED
sts_serial	6	100000	100	0.45914896	PASSED
sts_serial	6	100000	100	0.83284907	PASSED
sts_serial	7	100000	100	0.21432008	PASSED
sts_serial	7	100000	100	0.70647400	PASSED
sts_serial	8	100000	100	0.44655300	PASSED
sts_serial	8	100000	100	0.95247071	PASSED
sts_serial	9	100000	100	0.35387383	PASSED
sts_serial	9	100000	100	0.59526540	PASSED
sts_serial	10	100000	100	0.75611550	PASSED
sts_serial	10	100000	100	0.90583829	PASSED
sts_serial	11	100000	100	0.90925764	PASSED
sts_serial	11	100000	100	0.79254373	PASSED
sts_serial	12	100000	100	0.21588964	PASSED
sts_serial	12	100000	100	0.23330235	PASSED
sts_serial	13	100000	100	0.08820465	PASSED
sts_serial	13	100000	100	0.18195414	PASSED
sts_serial	14	100000	100	0.04856379	PASSED
sts_serial	14	100000	100	0.91273832	PASSED
sts_serial	15	100000	100	0.64666580	PASSED
sts_serial	15	100000	100	0.12294428	PASSED
sts_serial	16	100000	100	0.69688422	PASSED
sts_serial	16	100000	100	0.86885641	PASSED
rgb_bitdist	1	100000	100	0.04644339	PASSED
rgb_bitdist	2	100000	100	0.13024664	PASSED
rgb_bitdist	3	100000	100	0.27828879	PASSED
rgb_bitdist	4	100000	100	0.52826795	PASSED
rgb_bitdist	5	100000	100	0.20056436	PASSED
rgb_bitdist	6	100000	100	0.40752888	PASSED
rgb_bitdist	7	100000	100	0.80573943	PASSED

rgb_bitdist	8	100000	100	0.67450283	PASSED
rgb_bitdist	9	100000	100	0.79206671	PASSED
rgb_bitdist	10	100000	100	0.92872550	PASSED
rgb_bitdist	11	100000	100	0.05891923	PASSED
rgb_bitdist	12	100000	100	0.81773369	PASSED
rgb_minimum_distance	2	10000	1000	0.26792489	PASSED
rgb_minimum_distance	3	10000	1000	0.92847498	PASSED
rgb_minimum_distance	4	10000	1000	0.69985331	PASSED
rgb_minimum_distance	5	10000	1000	0.33412276	PASSED
rgb_permutations	2	100000	100	0.19821866	PASSED
rgb_permutations	3	100000	100	0.72714891	PASSED
rgb_permutations	4	100000	100	0.80520528	PASSED
rgb_permutations	5	100000	100	0.15495129	PASSED
rgb_lagged_sum	0	1000000	100	0.13625584	PASSED
rgb_lagged_sum	1	1000000	100	0.57627143	PASSED
rgb_lagged_sum	2	1000000	100	0.92628115	PASSED
rgb_lagged_sum	3	1000000	100	0.61029073	PASSED
rgb_lagged_sum	4	1000000	100	0.11121035	PASSED
rgb_lagged_sum	5	1000000	100	0.80844367	PASSED
rgb_lagged_sum	6	1000000	100	0.51696720	PASSED
rgb_lagged_sum	7	1000000	100	0.40013489	PASSED
rgb_lagged_sum	8	1000000	100	0.92473452	PASSED
rgb_lagged_sum	9	1000000	100	0.92921267	PASSED
rgb_lagged_sum	10	1000000	100	0.52457511	PASSED
rgb_lagged_sum	11	1000000	100	0.89559666	PASSED
rgb_lagged_sum	12	1000000	100	0.62524584	PASSED
rgb_lagged_sum	13	1000000	100	0.96003619	PASSED
rgb_lagged_sum	14	1000000	100	0.45500972	PASSED
rgb_lagged_sum	15	1000000	100	0.71193312	PASSED
rgb_lagged_sum	16	1000000	100	0.45610632	PASSED
rgb_lagged_sum	17	1000000	100	0.05903645	PASSED
rgb_lagged_sum	18	1000000	100	0.43360572	PASSED
rgb_lagged_sum	19	1000000	100	0.03581270	PASSED
rgb_lagged_sum	20	1000000	100	0.08951826	PASSED
rgb_lagged_sum	21	1000000	100	0.84439253	PASSED
rgb_lagged_sum	22	1000000	100	0.59972137	PASSED
rgb_lagged_sum	23	1000000	100	0.57228060	PASSED
rgb_lagged_sum	24	1000000	100	0.08421815	PASSED
rgb_lagged_sum	25	1000000	100	0.58546967	PASSED

rgb_lagged_sum	26	1000000	100	0.22839848	PASSED
rgb_lagged_sum	27	1000000	100	0.07446733	PASSED
rgb_lagged_sum	28	1000000	100	0.99397643	PASSED
rgb_lagged_sum	29	1000000	100	0.98871515	PASSED
rgb_lagged_sum	30	1000000	100	0.82128134	PASSED
rgb_lagged_sum	31	1000000	100	0.31772728	PASSED
rgb_kstest_test	0	10000	1000	0.37105156	PASSED
dab_bytedistrib	0	51200000	1	0.75754608	PASSED
dab_dct	256	50000	1	0.47880465	PASSED
dab_filltree	32	15000000	1	0.28587930	PASSED
dab_filltree	32	15000000	1	0.17581146	PASSED
dab_filltree2	0	5000000	1	0.31178897	PASSED
dab_filltree2	1	5000000	1	0.29090704	PASSED
dab_monobit2	12	65000000	1	0.03318549	PASSED

Table B.2: Detailed test results of the Dieharder test suite.

Chapter C

Modified Gray Code

The modification of the 6 bit Gray code [Gra53] was developed in collaboration with Jörg Duhme.

000001
000011
100011
110011
110001
010001
011001
011101
011111
011110
011010
010010
000010
001010
001000
101000
111000
011000
010000
000000
000100
010100
010101
000101
001101
001111
001011
001001
011011
101001
010011
111001
101100
000110
100100
010110
110100
110110
110000
110010
111010
101010
101011
111011
111111
101111
100111
000111
010111
110111
110101
111101
101101
100101
100001
100000
100010
100110
101110
001110
001100
011100
111100
111110

CHAPTER D

Generated Key

These are the first 7645 bits of the key that was generated in Chapter 6.5.

10001011110101111110111100010100100010011110111100110001001101101000011000
111101110011111100010011111001010111010110110100101010001100111000100011101
000011010001010100111001110011111011101101000011100001101000101000000010010
100100010001000110001011001011111111000111010010110000001010000111111101101
111001100000111110111010000110010100101101010111001101010101011110010101101
001010010101011100101110000001110101111111101101111010010011011101010110001
000111100001100011100000111101000000110010111100000110100111110001101001111
111010100101000110110111000000011000000001101111000010101101001111101111001
000100110111111001011111111010100111101111111111001000000010001101110011101 1
100111101000100001111100001001111101011101110010010011111010100000100100011
111111001011011111111011010010101000100111001110110100111110000100110010011
010010110100101000110000100100100101110101000001010100100111010000100111011
010100010011111101011000101011011101011000011001100000000010000111001001100 0
111110011100001010000110100101000101100110001000001111010110011101010010011
001000001011000101110101001011000111100011010000010100001011011101011001001 0
111101010110111100001010111101000101000010110001100001001010000101110100010
101100101101110000110010100011101100011111000100011110011111101111010001001
001000000111011010000010010011000100011110111010111000011010111100110101001
001010100101101001010010010011111001001110111010111000100111110100001110100
010100101001010010011111010110010100100101000101001111110101000001001010111
100011001010011111001001011000011110010111110011000101111100101000110001101
110101101111010110100000110100010110010110110111010110100110110100010101100
110010010101100001010101111110110001110110001101111111011100011001100101101
011101100111101000100100100101011110010101111100010011000011101110010100000

```
110100100011101010001110111010011011100110111111100000000011100100100011000
1110000100100111011000001111110110010011111111100011110100001100000010111011
100000010101010111101011101100001001110010001000110111101001001001110100110
111111111001011101001101001100001011101100100011010101101011001111011011101
0000110111111010100100011010010010011000011101110011101000011110101100001000
010000000011101101111011010011100110110001101100001001100001011010111101011
111001011111110110110101101010110000011011110010011101000010110111000100101
011111000111100111001011100010111010111110111110110010100000100100001101101
001000011101111010000111100010010010111101111011111101111001110100010011101
0110111101010000000101110111000000011110110101100111101001111010000000100001
011100010001100111110001101110101101011110100011100111100101111011001110100
001001110000100011101101111001110101010100100101111111100010000100101011101
111101001100100100100001111001110001011110010100001001101101100111110000100
1101001111010110111101000001010000000100011000000111001001000010010011000111
001001101001001000100111010101100011010010100110101101010100111000010100001
101010110001110010111111010101110100011010111000100001100101100001100111110
001000111011010011010011101100010001010101010111010100111111100011111000100
101111110110011111100110111010110011101011101110111001101001110000100101000
101000100001000011100001010111010011111100001000110011000010010000010011110
111001000101111111101110101011100110011100101000110110001001001111011110100
100110101111111111010100100000010111011010101001000000111101010110100000100
0010011110001011101110000010110000000110000011001110101011100110000000101011
1110011010100010111001000100010000110111000011011000000001111100111101110010
0110110000000100111100010011100011010011111000100110111001110010110001110111
010100010101001110100100110001111001000010110000100011000110001111011011010
000111100111111110000001101111011111111011100001001111000010101011100111001
010111111011011001001000101101101000001100000110100001101110010011110101101
000110110010111110000010100001100110111110010011001010100111001100000010110
001000010100100001110001000110000100010100010010011011100011001000100111110
101010100011110101011000010111101110010001100011101111110010100000010000011
111110001100111101000100001101011100000010110001010111010110100111100000011
100111110000011000000010111110000110010010110110101001110011101010101001010
0000110001000101101010011111010101001111011111101000110001101110011110101111
000100011001111010010111101010010001010010100111010010010010011100001000100
0000100011001011111010110011100000111110010011011010000100000001100110001100
000100111111010110001100110110000110001011110101000110101001010011001000000
1011010101111111111001001010100100010000111111010011101111001010000000100000
111010111001011000001011010101101001001111000100101011100101000111011010101
000111101001101100100010111011100111111010100110010110110010101100000101100
```

000110110100101110110000011111001011100000100111101101111001111100011000010
111101000011100001010111011110000011011011011000101100010101000110100111100
010010010011111110111001101011101011110101110110111101110000000100111010011
101001111100001100001101100101011110110000111000111011000000011011101110011
000001000010100000000111001011101011010111000110101111010010000101000111011 0
111101010100000010110100101000110100001010101010100101010001111010001110101
000101001101100100101101101001101101101111001000101011010100101010101101110
010010111011011001001111000010001011100001110101000101111000010111011101111
100010111001011001101011101101101010111100100001000101001110101101011010101
100100100010110111111101101110010011010111110001100011110011111011111000110
110011011111000000111101111001110000110001101110111100110101010011101001110 0
111111000000001101100000101011010001001010111101100000010110100110001010110 11
010110000000111001001101010101000010100101100000011010010000000110001000011 10
001000111000100000110100101010010000010011011011111100011110000110011101111
100101010000001000100110010001001011001110111011110101100110010011111110011 1
111001000101111111101110000000101001000010010010010111011101001001011110111 1
100101101000001110111111000001011001001111011000110010010100000000100011011 01
111010110001000000000000101000000101001100001101101111011000000101111101010001
010110110111100110011111000011001000000100001100110011100001010111101110100 0
001010100010001010010010000111111000000011101000010001011111011101110000101 1
001011111101001011110011000100111000110011110011001001011111010000001100000 1
000011101110010111011010001101010010010010110011000101001100001001000000110 1
001010110011111100111100011010011001010100101111101111011110111010111001100
110010011100110100111000011101101000101111100100111011101001110111001110110
111010100111101110001110101011010110001111110010100010111011011011011111101
111001000111110010110000111100100111000011000100001010101011110100110100111
101111101011100011111101001110110010110001010101110011101011011011100001001
001011110111010110011110110011110010100001000110000000111000000000100101100
011010101101010110010011001111011010111100101010001000000100010101101011101
111000000000100011001011101110100111111000010011000111101011101010110101111 1
110010011011010001101111100010100111100000110111100111100001000101011110101
110011100000000111110000100010011010000001111111110010111011010111001001100 1
110100010000000000101111100001000111011110010000000011100101111011110111101
001111000101000110111011011011010011111001001000101100101110111111110110111
100111010111011010010000000001100100000101010110100011001000101101011101110
011000110110000101011001110010100000111110010101111000101100101001011101001
100011011011111100110010010110100101101110011000010100101110101001100111001
010001111111000111001000111011110000000101110100011101011010100100111010010 1
011100000000101100001001011110110000011110111101000000110101001100101111 0 . . .

Bibliography

[Abr00] A. Abramovici and J. Chapsky, *Feedback Control Systems, A Fast-Track Guide for Scientists and Engineers* (Kluwer Academic Publishers, Boston, 2000), ISBN 0-7923-7935-7.

[And12] I. Andriyanova and J.-P. Tillich, “Designing a Good Low-Rate Sparse-Graph Code,” *IEEE Transactions on Communications* **60**, 3181 (2012).

[App08] J. Appel, E. Figueroa, D. Korystov, M. Lobino and a. Lvovsky, “Quantum Memory for Squeezed Light,” *Physical Review Letters* **100**, 093602 (2008).

[Ari10] M. Arikawa, K. Honda, D. Akamatsu, S. Nagatsuka, K. Akiba, A. Furusawa and M. Kozuma, “Quantum memory of a squeezed vacuum for arbitrary frequency sidebands,” *Physical Review A* **81**, 021605 (2010).

[Asp81] A. Aspect, P. Grangier and G. Roger, “Experimental Tests of Realistic Local Theories vial Bell’s Theorem,” *Physical Review Letters* **47**, 460 (1981).

[Ass06] G. V. Assche, *Quantum cryptography and secret-key distillation* (Cambridge University Press, 2006), ISBN 9780521864855.

[Ast11] S. Ast, R. M. Nia, A. Schönbeck, N. Lastzka, J. Steinlechner, T. Eberle, M. Mehmet, S. Steinlechner and R. Schnabel, “High-efficiency frequency doubling of continuous-wave laser light,” *Optics Letters* **36**, 3467 (2011).

[Ban98] K. Banaszek and K. Wodkiewicz, “Nonlocality of the Einstein-Podolsky-Rosen state in the Wigner representation,” *Physical Review A* **58**, 4345 (1998).

[Bar97] S. M. Barnett and P. M. Radmore, *Methods in Theoretical Quantum Optics* (Oxford University Press, Oxford, 1997), ISBN 0-19-856362-0.

[Bel64] J. S. Bell, “On the Einstein Podolsky Rosen Paradox,” *Physics* **1**, 195 (1964).

[Bel86] J. S. Bell, “EPR correlations and EPW distributions,” *Annals of the New York Academy of Sciences* **480**, 263 (1986).

[Ben84] C. H. Bennett and G. Brassard, “Quantum Cryptography: Public Key Distribution and Coin Tossing,” *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore India* **175** (1984).

[Ben92] C. H. Bennett and S. J. Wiesner, “Communication via One- and Two-Particle Operators on Einstein-Podolsky-Rosen States,” *Physical Review Letters* **69**, 2881 (1992).

[Ben95] C. H. Bennett, G. Brassard, C. Crépeau and U. M. Maurer, “Generalized Privacy Amplification,” *IEEE Transactions on Information Theory* **41**, 1915 (1995).

[Ber11] M. Berta, F. Furrer and V. B. Scholz, “The Smooth Entropy Formalism on von Neumann Algebras,” *arXiv* 1107.5460 (2011).

[Bic08] P. J. Bickel and A. Sakov, “On The Choice Of m In The m Out Of n Bootstrap And Confidence Bounds For Extrema,” *Statistica Sinica* **18**, 967 (2008).

[Bla01] E. D. Black, “An introduction to Pound-Drever-Hall laser frequency stabilization,” *American Journal of Physics* **69**, 79 (2001).

[Bou97] D. Bouwmeester, J. Pan, K. Mattle and M. Eibl, “Experimental quantum teleportation,” *Nature* **390**, 575 (1997).

[Bow03] W. P. Bowen, R. Schnabel and P. K. Lam, “Experimental Investigation of Criteria for Continuous Variable Entanglement,” *Physical Review Letters* **90**, 043601 (2003).

[Bra00] S. Braunstein and H. Kimble, “Dense coding for continuous variables,” *Physical Review A* **61**, 042302 (2000).

[Bri98] H. Briegel, W. Dür, J. Cirac and P. Zoller, “Quantum repeaters: The role of imperfect local operations in quantum communication,” *Physical Review Letters* **81**, 5932 (1998).

[Bro09] P. Bronner, A. Strunz, C. Silberhorn and J.-P. Meyn, “Demonstrating quantum random with single photons,” *European Journal of Physics* **30**, 1189 (2009).

[Bro12] R. G. Brown, “http://www.phy.duke.edu/˜rgb/General/dieharder.php,” (2012).

[Buo10] D. Buono, G. Nocerino, V. D. Auria, A. Porzio, S. Olivares and M. G. A. Paris, "Quantum characterization of bipartite Gaussian states," *Journal of the Optical Society of America B* **27**, 110 (2010).

[Can01] R. Canetti, "Universally Composable Security : A New Paradigm for Cryptographic Protocols," in "Proc. 42nd IEEE Symp. on Foundations of Computer Science," 136–145 (2001), ISBN 0769513905.

[Cer01] N. Cerf, M. Lévy and G. Assche, "Quantum distribution of Gaussian keys using squeezed states," *Physical Review A* **63**, 052311 (2001).

[Dav98] M. Davey and D. MacKay, "Low density parity check codes over GF (q)," *Information Theory Workshop, 1998* **6**, 70 (1998).

[Dev05] I. Devetak and a. Winter, "Distillation of secret key and entanglement from quantum states," *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* **461**, 207 (2005).

[DiG07] J. DiGuglielmo, B. Hage, A. Franzen, J. Fiurášek and R. Schnabel, "Experimental characterization of Gaussian quantum-communication channels," *Physical Review A* **76**, 012323 (2007).

[DiV95] D. P. DiVincenzo, "Quantum Computation," *Science* **270**, 255 (1995).

[Dua00] L.-M. Duan, G. Giedke, J. Cirac and P. Zoller, "Inseparability criterion for continuous variable systems," *Physical Review Letters* **84**, 2722 (2000).

[Dyn08] J. F. Dynes, Z. L. Yuan, a. W. Sharpe and a. J. Shields, "A high speed, postprocessing free, quantum random number generator," *Applied Physics Letters* **93**, 031109 (2008).

[Ebe10] T. Eberle, S. Steinlechner, J. Bauchrowitz, V. Händchen, H. Vahlbruch, M. Mehmet, H. Müller-Ebhardt and R. Schnabel, "Quantum Enhancement of the Zero-Area Sagnac Interferometer Topology for Gravitational Wave Detection," *Physical Review Letters* **104**, 251102 (2010).

[Ebe11] T. Eberle, V. Händchen, J. Duhme, T. Franz, R. Werner and R. Schnabel, "Strong Einstein-Podolsky-Rosen entanglement from a single squeezed light source," *Physical Review A* **83**, 052329 (2011).

[Ebe13a] T. Eberle, V. Händchen, J. Duhme, T. Franz, F. Furrer, R. Schnabel and R. F. Werner, "Gaussian Entanglement for Quantum Key Distribution from a Single-Mode Squeezing Source," *arXiv* 1110.3977 (2013).

[Ebe13b] T. Eberle, V. Händchen and R. Schnabel, “Stable Control of 10 dB Two Mode Squeezed Vacuum States of Light,” *Optics Express* **21**, 11546 (2013).

[Efr86] B. Efron and R. Tibshirani, “Bootstrap Methods for Standard Errors, Confidence Intervals, and Other Measures of Statistical Accuracy,” *Statistical Science* **1**, 54 (1986).

[Ein35] A. Einstein, B. Podolsky and N. Rosen, “Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?” *Physical Review* **47**, 777 (1935).

[Eke91] A. K. Ekert, “Quantum Cryptography Based on Bell’s Theorem,” *Physical Review Letters* **67**, 661 (1991).

[Fos09] S. Fossier, E. Diamanti, T. Debuisschert, a. Villing, R. Tualle-Brouri and P. Grangier, “Field test of a continuous-variable quantum key distribution prototype,” *New Journal of Physics* **11**, 045023 (2009).

[Fra12] T. Franz, “Quantum Correlations and Quantum Key Distribution,” Ph.D. thesis, Leibniz University Hannover (2012).

[Fue10] M. Fuerst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer and H. Weinfurter, “High speed optical quantum random number generation.” *Optics Express* **18**, 13029 (2010).

[Fur98] A. Furusawa, J. L. Sorensen, S. L. Braunstein, C. A. Fuchs, H. Kimble and E. S. Polzik, “Unconditional Quantum Teleportation,” *Science* **282**, 706 (1998).

[Fur09] F. Furrer, “Min- and Max-Entropies as Generalized Entropy Measures in Infinite-Dimensional Quantum Systems,” Ph.D. thesis, ETH Zürich (2009).

[Fur11] F. Furrer, J. Aberg and R. Renner, “Min- and Max-Entropy in Infinite Dimensions,” *Communications in Mathematical Physics* **306**, 165 (2011).

[Fur12a] F. Furrer, “Security of Continuous-Variable Quantum Key Distribution and Aspects of Device-Independent Security,” Ph.D. thesis, Leibniz University Hannover (2012).

[Fur12b] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. Scholz, M. Tomamichel and R. Werner, “Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security against Coherent Attacks,” *Physical Review Letters* **109**, 100502 (2012).

[Gab10] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt and G. Leuchs, “A generator for unique quantum random numbers based on vacuum states,” *Nature Photonics* **4**, 711 (2010).

[Gal62] R. G. Gallager, “Low-Density Codes,” *IRE Transactions on Information Theory* 21–28 (1962).

[Gem94] P. Gemmell and M. Naor, “Codes for Interactive Authentication,” *Advances in Cryptology - CRYPTO’93* **773**, 355 (1994).

[Ger05] C. C. Gerry and P. L. Knight, *Introductory Quantum Optics* (Cambridge University Press, Cambridge, 2005), ISBN 0-521-52735-X.

[Gis02] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, “Quantum cryptography,” *Review of Modern Physics* **74**, 145 (2002).

[Gla63] R. J. Glauber, “Coherent and Incoherent States of the Radiation Field,” *Physical Review* **131**, 2766 (1963).

[GP06] R. García-Patrón and N. Cerf, “Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution,” *Physical Review Letters* **97**, 190503 (2006).

[Gra53] F. Gray, “Pulse code communication,” *US Patent* US2632058 (1953).

[Gro02] F. Grosshans and P. Grangier, “Continuous Variable Quantum Cryptography Using Coherent States,” *Physical Review Letters* **88**, 057902 (2002).

[Gro03] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf and P. Grangier, “Quantum key distribution using gaussian-modulated coherent states.” *Nature* **421**, 238 (2003).

[Hae12] V. Haendchen, T. Eberle, S. Steinlechner, A. Samblowski, T. Franz, R. F. Werner and R. Schnabel, “Observation of one-way Einstein–Podolsky–Rosen steering,” *Nature Photonics* **6**, 596 (2012).

[Hag11] B. Hage, J. Janoušek, S. Armstrong, T. Symul, J. Bernu, H. M. Chrzanowski, P. K. Lam and H. a. Bachor, “Demonstrating various quantum effects with two entangled laser beams,” *The European Physical Journal D* **63**, 457 (2011).

[He06] G. He, J. Zhu and G. Zeng, “Quantum secure communication using continuous variable Einstein-Podolsky-Rosen correlations,” *Physical Review A* **73**, 012314 (2006).

[Hel98] P. Hellekalek, "Good random number generators are (not so) easy to find," *Mathematics and Computers in Simulation* **46**, 485 (1998).

[Hor89] P. Horowitz and W. Hill, *The Art of Electronics* (Cambridge University Press, Cambridge, 1989), 2nd ed., ISBN 13-978-0-521-37095-0.

[Hor09] R. Horodecki, P. Horodecki, M. Horodecki and K. Horodecki, "Quantum entanglement," *Reviews of Modern Physics* **81**, 865 (2009).

[Jam90] F. James, "A review of pseudorandom number generators," *Computer Physics Communications* **60**, 329 (1990).

[Jen00] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter and A. Zeilinger, "A fast and compact quantum random number generator," *Review of Scientific Instruments* **71**, 1675 (2000).

[Jen10] K. Jensen, W. Wasilewski, H. Krauter, T. Fernholz, B. M. Nielsen, M. Owari, M. B. Plenio, a. Serafini, M. M. Wolf and E. S. Polzik, "Quantum memory for entangled continuous-variable states," *Nature Physics* **7**, 13 (2010).

[Joh07] R. Johnson and D. Wichern, *Applied multivariate statistical analysis* (Pearson Prentice Hall, Upper Saddle River, New Jersey, 2007), 6th ed., ISBN 978-0135143506.

[Jou11] P. Jouguet, S. Kunz-Jacques and A. Leverrier, "Long-distance continuous-variable quantum key distribution with a Gaussian modulation," *Physical Review A* **84**, 062317 (2011).

[Jou12] P. Jouguet, S. Kunz-Jacques, T. Debuisschert, S. Fossier, E. Diamanti, R. Alleaume, R. Tualle-Brouri, P. Grangier, A. Leverrier, P. Pache and P. Painchault, "Field test of classical symmetric encryption with continuous variables quantum key distribution," *Optics Express* **20**, 14030 (2012).

[Jou13] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," *Nature Photonics* **7**, 378 (2013).

[Kel08] G. Keller, V. D'Auria, N. Treps, T. Coudreau, J. Laurat and C. Fabre, "Experimental demonstration of frequency-degenerate bright EPR beams with a self-phase-locked OPO." *Optics Express* **16**, 9351 (2008).

[Koe07] R. Koenig, R. Renner, A. Bariska and U. Maurer, "Small Accessible Quantum Information Does Not Imply Security," *Physical Review Letters* **98**, 140502 (2007).

[Lau05] J. Laurat, T. Coudreau, G. Keller, N. Treps and C. Fabre, "Effects of mode coupling on the generation of quadrature Einstein-Podolsky-Rosen entanglement in a type-II optical parametric oscillator below threshold," *Physical Review A* **71**, 022313 (2005).

[Lec07] P. Lecuyer and R. Simard, "TestU01: A C Library for Empirical Testing of Random Number Generators," *ACM transactions on mathematical software* **33** (2007).

[Leo97] U. Leonhardt, *Measuring the Quantum State of Light* (Cambridge University Press, 1997), ISBN 0-521-49730-2.

[Lev10] A. Leverrier, F. Grosshans and P. Grangier, "Finite-size analysis of a continuous-variable quantum key distribution," *Physical Review A* **81**, 062343 (2010).

[Lo07] H.-K. Lo and N. Lütkenhaus, "Quantum Cryptography: from Theory to Practice," *arXiv* quant–ph/0702202 (2007).

[Lod05] J. Lodewyck, T. Debuisschert, R. Tualle-Brouri and P. Grangier, "Controlling excess noise in fiber-optics continuous-variable quantum key distribution," *Physical Review A* **72**, 050303 (2005).

[Lod07] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. Cerf, R. Tualle-Brouri, S. McLaughlin and P. Grangier, "Quantum key distribution over 25km with an all-fiber continuous-variable system," *Physical Review A* **76**, 042305 (2007).

[Lyo04] R. G. Lyons, *Understanding Digital Signal Processing* (Pearson Prentice Hall, Upper Saddle River, New Jersey, 2004), 2nd ed., ISBN 978-0-13-108989-1.

[Ma13] X.-C. Ma, S.-H. Sun, M.-S. Jiang and L.-M. Liang, "Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum key distribution system," *arXiv* 1303.6043 (2013).

[Mad12] L. S. Madsen, V. C. Usenko, M. Lassen, R. Filip and U. L. Andersen, "Continuous variable quantum key distribution with modulated entangled states." *Nature Communications* **3**, 1083 (2012).

[Meh10] M. Mehmet, T. Eberle, S. Steinlechner, H. Vahlbruch and R. Schnabel, "Demonstration of a quantum-enhanced fiber Sagnac interferometer," *Optics Letters* **35**, 1665 (2010).

[Meh11] M. Mehmet, S. Ast, T. Eberle, S. Steinlechner, H. Vahlbruch and R. Schnabel, “Squeezed light at 1550 nm with a quantum noise reduction of 12.3 dB,” *Optics Express* **19**, 25763 (2011).

[Nav06] M. Navascués, F. Grosshans and A. Acín, “Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography,” *Physical Review Letters* **97**, 190502 (2006).

[Ou92] Z. Y. Ou, S. F. Pereira, H. J. Kimble and K. C. Peng, “Realization of the Einstein-Podolsky-Rosen paradox for continuous variables,” *Physical Review Letters* **68**, 3663 (1992).

[Rei89] M. D. Reid, “Demonstration of the Einstein-Podolsky-Rosen paradox using nondegenerate parametric amplification,” *Physical Review A* **40**, 913 (1989).

[Ren05a] R. Renner, “Security of Quantum Key Distribution,” Ph.D. thesis, ETH Zürich (2005).

[Ren05b] R. Renner and K. Robert, “Universally Composable Privacy Amplification Against Quantum Adversaries,” in J. Kilian (editor), “Theory of Cryptography,” 407–425 (Springer Berlin Heidelberg, 2005), lecture no ed., ISBN 978-3-540-24573-5.

[Ren09] R. Renner and J. Cirac, “de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography,” *Physical Review Letters* **102**, 110504 (2009).

[RFC11] RFC6234, “http://tools.ietf.org/html/rfc6234,” (2011).

[Rod07] C. Rodo, O. Romero-Isart, K. Eckert and A. Sanpera, “Efficiency in Quantum Key Distribution Protocols with Entangled Gaussian States,” *Open Sys. & Information Dyn.* **14**, 69 (2007).

[Ruk01] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray and S. Vo, “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications,” *NIST Special Publication* **800-22** (2001).

[Sak11] J. Sakurai and J. Napolitano, *Modern Quantum Mechanics* (Addison-Wesley, 2011), 2nd ed., ISBN 978-0-8053-8291-4.

[Sam12] A. Samblowski, “State Preparation for Quantum Information Science and Metrology,” Ph.D. thesis, Leibniz University Hannover (2012).

[Sas10] L. Sassatelli and D. Declercq, “Nonbinary Hybrid LDPC Codes,” *IEEE Transactions on Information Theory* **56**, 5314 (2010).

[Sca09] V. Scarani, H. Bechmann-Pasquinucci, N. Cerf, M. Dušek, N. Lütkenhaus and M. Peev, “The security of practical quantum key distribution,” *Reviews of Modern Physics* **81**, 1301 (2009).

[Sch35] E. Schrödinger, “Discussion of Probability Relations Between Separated Systems,” *Proc. Camb. Phil. Soc.* **47**, 555 (1935).

[Sch01] W. P. Schleich, *Quantum Optics in Phase Space* (WILEY-VCH Verlag Berlin GmbH, 2001), ISBN 3-527-29435-X.

[Sch02] C. Schori, J. L. Sø rensen and E. S. Polzik, “Narrow-band frequency tunable light source of continuous quadrature entanglement,” *Physical Review A* **66**, 033802 (2002).

[Ser04] A. Serafini, F. Illuminati and S. D. Siena, “Symplectic invariants, entropic measures and correlations of Gaussian states,” *Journal of Physics B: Atomic, Molecular and Optical Physics* **37**, L21 (2004).

[Sho97] P. W. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” *SIAM Journal on Computing* **26**, 1484 (1997).

[Sho03] A. Shokrollahi, “LDPC Codes : An Introduction,” *Coding, Cryptography and Combinatorics* **23**, 1 (2003).

[Sil01] C. Silberhorn, P. K. Lam, O. Weiß, F. König, N. Korolkova and G. Leuchs, “Generation of Continuous Variable Einstein-Podolsky-Rosen Entanglement via the Kerr Nonlinearity in an Optical Fiber,” *Physical Review Letters* **86**, 4267 (2001).

[Sim00] R. Simon, “Peres-Horodecki Separability Criterion for Continuous Variable Systems,” *Physical Review Letters* **84**, 2726 (2000).

[Sle73] D. Slepian and J. K. Wolf, “Noiseless Coding of Correlated Information Sources,” *IEEE Transactions on Information Theory* **19**, 471 (1973).

[Smi03] S. W. Smith, *Digital Signal Processing* (Newnes, 2003), ISBN 978-0-7506-7444-7.

[Smi08] G. Smith and J. Yard, “Quantum communication with zero-capacity channels,” *Science* **321**, 1812 (2008).

[Smi11] G. Smith, J. A. Smolin and J. Yard, “Quantum communication with Gaussian channels of zero quantum capacity,” *Nature Photonics* **5**, 624 (2011).

[Ste00] A. Stefanov, N. Gisin and O. Guinnard, “Optical quantum random number generator,” *Journal of Modern Optics* **47**, 595 (2000).

[Ste12] S. Steinlechner, J. Bauchrowitz, M. Meinders, H. Müller-Ebhardt, K. Danzmann and R. Schnabel, “Quantum-Dense Metrology,” *arXiv* 1211.3570 (2012).

[Ste13] S. Steinlechner, J. Bauchrowitz, T. Eberle and R. Schnabel, “Strong Einstein-Podolsky-Rosen steering with unconditional entangled states,” *Physical Review A* **87**, 022104 (2013).

[Sti94] D. R. Stinson, “Universal hashing and authentication codes,” *Designs, Codes and Cryptography* **4**, 369 (1994).

[Sti02] D. R. Stinson, “Universal hash families and the leftover hash lemma , and applications to cryptography and computing,” *J. Combin. Math. Combin. Comput.* **42**, 3 (2002).

[Su09] X. Su, W. Wang, Y. Wang, X. Jia, C. Xie and K. Peng, “Continuous variable quantum key distribution based on optical entangled states without signal modulation,” *Europhysics Letters* **87**, 20005 (2009).

[Sym11] T. Symul, S. M. Assad and P. K. Lam, “Real time demonstration of high bitrate quantum random number generation with coherent laser light,” *Applied Physics Letters* **98**, 231103 (2011).

[Tak06] N. Takei, N. Lee, D. Moriyama, J. S. Neergaard-Nielsen and A. Furusawa, “Time-gated Einstein-Podolsky-Rosen correlation,” *Physical Review A* **74**, 060101(R) (2006).

[Tak07] Y. Takeno, M. Yukawa, H. Yonezawa and A. Furusawa, “Observation of -9 dB quadrature squeezing with improvement of phase stability in homodyne measurement.” *Optics Express* **15**, 4321 (2007).

[The11] The LIGO Scientific Collaboration, “A gravitational wave observatory operating beyond the quantum shot-noise limit,” *Nature Physics* **7**, 962 (2011).

[Tom11] M. Tomamichel, C. Schaffner, A. Smith and R. Renner, “Leftover Hashing Against Quantum Side Information,” *IEEE Transactions on Information Theory* **57**, 5524 (2011).

[Ulr57] W. Ulrich, “Non-Binary Error Correction Codes,” *The Bell System Technical Journal* 1341–1388 (1957).

[Urs07] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Oemer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter and A. Zeilinger, “Entanglement-based quantum communication over 144 km,” *Nature Physics* **3**, 481 (2007).

[Vah08] H. Vahlbruch, M. Mehmet, S. Chelkowski, B. Hage, A. Franzen, N. Lastzka, S. Goß ler, K. Danzmann and R. Schnabel, “Observation of Squeezed Light with 10-dB Quantum-Noise Reduction,” *Physical Review Letters* **100**, 033602 (2008).

[Vah10] H. Vahlbruch, A. Khalaidovski, N. Lastzka, C. Gräf, K. Danzmann and R. Schnabel, “The GEO600 squeezed light source,” *Classical and Quantum Gravity* **27**, 084027 (2010).

[Ver26] G. Vernam, “Cipher printing telegraph systems for secret wire and radio telegraphic communications,” *Journal of the American Institute for Electrical Engineers* **XLI**, 295 (1926).

[Wah11] M. Wahl, M. Leifgen, M. Berlin, T. Röhlicke, H.-J. Rahn and O. Benson, “An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements,” *Applied Physics Letters* **98**, 171105 (2011).

[Wan10] Y. Wang, H. Shen, X. Jin, X. Su, C. Xie and K. Peng, “Experimental generation of 6 dB continuous variable entanglement from a nondegenerate optical parametric amplifier.” *Optics Express* **18**, 6149 (2010).

[Was10] W. Wasilewski, K. Jensen, H. Krauter, J. J. Renema, M. V. Balabas and E. S. Polzik, “Quantum Noise Limited and Entanglement-Assisted Magnetometry,” *Physical Review Letters* **104**, 133601 (2010).

[Wee12] C. Weedbrook, S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. C. Ralph, J. H. Shapiro and S. Lloyd, “Gaussian Quantum Information,” *Review of Modern Physics* **84**, 621 (2012).

[Wig32] E. Wigner, “On the Quantum Correction For Thermodynamic Equilibrium,” *Physical Review* **40**, 749 (1932).

[Wil36] J. Williamson, “On the Algebraic Problem Concerning the Normal Forms of Linear Dynamical Systems,” *American Journal of Mathematics* **58**, 141 (1936).

[Wil12] M. M. Wilde, “From Classical to Quantum Shannon Theory,” *arXiv* 1106.1445 (2012).

[Wis07] H. M. Wiseman, S. J. Jones and a. C. Doherty, “Steering, Entanglement, Nonlocality, and the Einstein-Podolsky-Rosen Paradox,” *Physical Review Letters* **98**, 140402 (2007).

[Xu12] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng and H.-K. Lo, “Ultrafast quantum random number generation based on quantum phase fluctuations.” *Optics Express* **20**, 12366 (2012).

[Zha00] Y. Zhang, H. Wang, X. Li, J. Jing, C. Xie and K. Peng, “Experimental generation of bright two-mode quadrature squeezed light from a narrow-band nondegenerate optical parametric amplifier,” *Physical Review A* **62**, 023813 (2000).

Acknowledgements

I would like to take the opportunity to thank those who have helped and supported me to make this thesis possible. First of all I like to thank Roman Schnabel who has given me the opportunity to work in his group on a fascinating topic. Thank you for your support. Further, I would like to thank Karsten Danzmann for creating an incredible research environment at the Albert Einstein Institute. In particular, I would like to offer special thanks to Vitus Händchen. Thank you for – well, this cannot be expressed in a single sentence – so, for just everything.

The work presented in this thesis would not have been possible without theory support. I would like to thank Jörg Duhme, Torsten Franz, Fabian Furrer and Reinhard Werner for providing, not only a continuous variable security proof for arbitrary attacks just in time, but also for answering my permanent questions.

I am very grateful for the work done by Christoph Pacher and Oliver Maurhart from the Austrian Institute of Technology who made a very good job of the error correction just some days before I had to hand in this thesis.

I further would like to thank all of the quantum interferometry group for a great working atmosphere and lots of fruitful discussions.

For proof reading my thesis I would like to thank Christina Vollmer, Christoph Baune, Vitus Händchen, Alexander Khalaidovski, Axel Schönbeck, Christina Bogan, Daniela Schulze, Jörg Duhme, Moritz Mehmet and Sacha Kocsis.

Last, but no least, I wish to thank Nina Gehring, Jessica and Steini Steinlechner and Ulli Velte for the lovely coffee breaks after lunch.

Curriculum Vitae

Personal Information

Tobias Eberle
Marschnerstraße 23
30167 Hannover
Email: mail@tobiaseberle.de

Date of birth: 03/15/1983
Nationality: German

Education

since 06/2009	Doctoral studies in physics, Institute for Gravitational Physics, Leibniz University Hannover
04/2008 – 04/2009	Diploma thesis at Institute for Gravitational Physics, Leibniz University Hannover
03/2007 – 06/2007	Internship at Polytec GmbH
09/2006 – 01/2007	Study of physics at Lund University (Sweden)
2003 – 2009	Study of physics at the University of Heidelberg, final grade: 1.0 (with distinction)
10/2002 – 03/2003	Distance study of physics at Technical University Kaiserslautern
08/2002 – 05/2003	Civilian service at Nature Preservation Center Südschwarzwald, Feldberg (Black Forest)
1993 – 2002	Gymnasium Bildungszentrum Reutlingen Nord, Reutlingen, final grade: 1.3

Scholarships

since 06/2009	Doctoral scholarship of the International Max Planck Research School on Gravitational Wave Astronomy
06/2006 – 04/2009	Scholarship of "Studienstiftung des deutschen Volkes"

List of Publications

2013

1. **T. Eberle**, V. Händchen, J. Duhme, T. Franz, F. Furrer, R. Schnabel, RF. Werner, "Gaussian entanglement for quantum key distribution from a single-mode squeezing source", *New Journal of Physics* **15**, 053049
2. **T. Eberle**, V. Händchen, R. Schnabel, "Stable Control of 10dB Two-Mode Squeezed Vacuum States of Light", *Optics Express* **21**, 11546-11553
3. CE. Vollmer, D. Schulze, **T. Eberle**, V. Händchen, J. Fiurasek, R. Schnabel, "Experimental entanglement distribution by separable states", *arXiv preprint* quant-ph:1303.1082
4. S. Steinlechner, J. Bauchrowitz, **T. Eberle**, R. Schnabel, "Strong Einstein-Podolsky-Rosen steering with unconditional entangled states", *Physical Review A* **87**, 022104
5. J. Steinlechner, S. Ast, C. Krüger, A. Singh, **T. Eberle**, V. Händchen, R. Schnabel, "Absorption Measurements of Periodically Poled Potassium Titanyl Phosphate (PPKTP) at 775 nm and 1550 nm", *Sensors* **13**, 565-573
6. J. Aasi, J. Abadie, . . . , **T. Eberle**, . . . , "Einstein@Home all-sky search for periodic gravitational waves in LIGO S5 data", *Physical Review D* **87**, 042001
7. J. Aasi, J. Abadie, . . . , **T. Eberle**, . . . , "Search for gravitational waves from binary black hole inspiral, merger, and ringdown in LIGO-Virgo data from 2009–2010", *Physical Review D* **87**, 022002

2012

8. J. Abadie, BP. Abbott, . . . , **T. Eberle**, . . . , "Search for gravitational waves from low mass compact binary coalescence in LIGO's sixth science run and Virgo's

science runs 2 and 3", *Physical Review D* **85**, 082002

9. J. Abadie, BP. Abbott, . . . , **T. Eberle**, . . . , "All-sky search for periodic gravitational waves in the full S5 LIGO data", *Physical Review D* **85**, 022001
10. J. Abadie, BP. Abbott, . . . , **T. Eberle**, . . . , "Implementation and testing of the first prompt search for gravitational wave transients with electromagnetic counterparts", *Astronomy & Astrophysics* **539**, A124
11. V. Händchen, **T. Eberle**, S. Steinlechner, A. Samblowski, T. Franz, R. Werner, R. Schnabel, "Observation of one-way Einstein-Podolsky-Rosen steering", *Nature Photonics* **6**, 598-601
12. J. Abadie, BP. Abbott, . . . , **T. Eberle**, . . . , "First low-latency LIGO+ Virgo search for binary inspirals and their electromagnetic counterparts", *Astronomy & Astrophysics* **541**, A155
13. J. Abadie, BP. Abbott, . . . , **T. Eberle**, . . . , "Upper limits on a stochastic gravitational-wave background using LIGO and Virgo interferometers at 600–1000 Hz", *Physical Review D* **85**, 122001
14. J. Abadie, BP. Abbott, . . . , **T. Eberle**, . . . , "All-sky search for gravitational-wave bursts in the second joint LIGO-Virgo run", *Physical Review D* **85**, 122007
15. J. Abadie, BP. Abbott, . . . , **T. Eberle**, . . . , "Search for gravitational waves associated with gamma-ray bursts during LIGO science run 6 and Virgo science runs 2 and 3", *The Astrophysical Journal* **760**, 12
16. J. Abadie, BP. Abbott, . . . , **T. Eberle**, . . . , "Search for gravitational waves from intermediate mass binary black holes", *Physical Review D* **85**, 102004
17. J. Aasi, J. Abadie, . . . , **T. Eberle**, . . . , "The characterization of Virgo data and its impact on gravitational-wave searches", *Classical and Quantum Gravity* **29**, 155002
18. J. Abadie, BP. Abbott, . . . , **T. Eberle**, . . . , "Implications for the Origin of GRB 051103 from LIGO Observations", *The Astrophysical Journal* **755**, 2
19. S. Ast, A. Samblowski, M. Mehmet, S. Steinlechner, **T. Eberle**, R. Schnabel, "Continuous-wave nonclassical light with gigahertz squeezing bandwidth", *Optics Letters* **37**, 2367-2369
20. PA. Evans, JK. Fridriksson, . . . , **T. Eberle**, . . . , "Swift follow-up observations of candidate gravitational-wave transient events", *The Astrophysical Journal Supplement Series* **203**, 28

2011

21. J. Abadie, BP. Abbott, . . . , **T. Eberle**, . . . , “A gravitational wave observatory operating beyond the quantum shot-noise limit”, *Nature Physics* **7**, 962-965
22. J. Abadie, BP. Abbott, . . . , **T. Eberle**, . . . , “Search for gravitational waves from binary black hole inspiral, merger, and ringdown”, *Physical Review D* **83**, 122005
23. J. Abadie, BP. Abbott, . . . , **T. Eberle**, . . . , “Search for gravitational wave bursts from six magnetars”, *The Astrophysical Journal Letters* **734**, L35
24. J. Abadie, BP. Abbott, . . . , **T. Eberle**, . . . , “Beating the spin-down limit on gravitational wave emission from the Vela pulsar”, *The Astrophysical Journal* **737**, 93
25. **T. Eberle**, V. Händchen, J. Duhme, T. Franz, R. Werner, R. Schnabel, “Strong Einstein-Podolsky-Rosen entanglement from a single squeezed light source”, *Physical Review A* **83**, 052329
26. M. Mehmet, S. Ast, **T. Eberle**, S. Steinlechner, H. Vahlbruch, R. Schnabel, “Squeezed light at 1550 nm with a quantum noise reduction of 12.3 dB”, *Optics Express* **19**, 25763-25772
27. S. Ast, R. Nia, A. Schönbeck, N. Lastzka, J. Steinlechner, **T. Eberle**, M. Mehmet, S. Steinlechner, R. Schnabel, “High-efficiency frequency doubling of continuous-wave laser light”, *Optics Letters* **36**, 3467-3469
28. J. Abadie, BP. Abbott, . . . , **T. Eberle**, . . . , “Directional limits on persistent gravitational waves using LIGO S5 science data”, *Physical Review Letters* **107**, 271102

2010

29. J. Abadie, BP. Abbott, . . . , **T. Eberle**, . . . , “Predictions for the rates of compact binary coalescences observable by ground-based gravitational-wave detectors”, *Classical and Quantum Gravity* **27**, 173001
30. J. Abadie, BP. Abbott, . . . , **T. Eberle**, . . . , “Search for gravitational waves from compact binary coalescence in LIGO and Virgo data from S5 and VSR1”, *Physical Review D* **82**, 102001
31. J. Abadie, BP. Abbott, . . . , **T. Eberle**, . . . , “Calibration of the LIGO gravitational wave detectors in the fifth science run”, *Nuclear Instruments and Methods*

in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment **624**, 223-240

32. **T. Eberle**, S. Steinlechner, J. Bauchrowitz, V. Händchen, H. Vahlbruch, M. Mehmet, H. Müller-Ebhardt, R. Schnabel, “Quantum enhancement of the zero-area Sagnac interferometer topology for gravitational wave detection”, *Physical Review Letters* **104**, 251102
33. J. Abadie, BP. Abbott, …, **T. Eberle**, …, “First search for gravitational waves from the youngest known neutron star”, *The Astrophysical Journal* **722**, 1504
34. M. Mehmet, **T. Eberle**, S. Steinlechner, H. Vahlbruch, R. Schnabel, “Demonstration of a quantum-enhanced fiber Sagnac interferometer”, *Optics letters* **35**, 1665-1667
35. R. Schnabel, M. Britzger, F. Brückner, O. Burmeister, K. Danzmann, J. Duck, **T. Eberle**, D. Friedrich, H. Luck, M. Mehmet, “Building blocks for future detectors: Silicon test masses and 1550 nm laser light”, *Journal of Physics: Conference Series* **228**, 012029

2009

36. M. Mehmet, S. Steinlechner, **T. Eberle**, H. Vahlbruch, A. Thüring, K. Danzmann, R. Schnabel, “Observation of cw squeezed light at 1550 nm”, *Optics Letters* **34**, 1060-1062

2007

37. **T. Eberle**, J. Klemmer, “Design, Construction and Study of a New Gas Target for High-order Harmonic Generation: Report”,