Quantum Key Security: Theory and Analysis of Experimental Realisations

Von der QUEST-Leibniz-Forschungsschule
der Gottfried Wilhelm Leibniz Universität Hannover

zur Erlangung des Grades
Doktor der Naturwissenschaften
Dr. rer. nat.

genehmigte Dissertation
von

Dipl. Phys. Jörg Duhme

geboren am 05.09.1978, in Rheda-Wiedenbrück

2015

Referent:	Prof. Dr. Reinhard F. Werner,	Leibniz Universität Hannover
Korreferent:	Prof. Dr. Andreas Ruschhaupt,	University College Cork
Tag der Promotion:	02.03.2015	

Abstract

We focus on the task of secret communication using continuous quantum key distribution protocols. This thesis is part of the collaboration *Crypto on Campus* consisting of the theoretical *Quantum Information* group under Prof. Dr. R. F. Werner and the experimental *Quantum Interferometry* group led by Prof. Dr. R. Schnabel. The experiments were carried out at the *Albert Einstein Institute* in Hannover. We connect the results of the experiments with the theoretical analysis which we present in this thesis.

In the first section we start with a general runtime analysis of an experimental realisation of quantum key distribution protocols. We show that it is convenient to use protocols which allow for a non-uniform choice of measurement basis in order to maximise the amount of secure key that can be generated in one run of an experiment. Motivated by this we extend existing protocols such that they allow for a non-uniform choice of the basis. We compare the various protocols using the runtime analysis and experimental results to show the importance of non-uniform-basis choice in quantum key distribution. The chapter closes with a discussion of an urban quantum key distribution network using the new protocols which we developed.

In the second section we discuss the generation of an actual key in an experiment and focus especially on classical reconciliation protocols, which are needed to correct the errors between the raw keys of the legitimate participating parties. We show that the quantum key distribution protocols which we discuss in this thesis raise special demands on the reconciliation schemes. We propose a new reconciliation scheme (hybrid reconciliation) which is specifically designed for the needs of these quantum key distribution protocols and demonstrate its performance in an experiment. The chapter closes with a full technical analysis of the performance of the hybrid reconciliation scheme.

Keywords: Continuous Variable Quantum Cryptography, Hybrid Reconciliation, Runtime Analysis, Asymmetric Protocol

Zusammenfassung

Wir beschäftigen uns mit dem Austausch geheimer Nachrichten anhand quantenkryptografischer Protokolle, die kontinuierliche Variablen verwenden. Diese Arbeit entstand im Zuge der Kollaboration *Crypto on Campus* der Arbeitsgruppe *Quanteninformation* von Prof. Dr. R. F. Werner mit der Arbeitsgruppe *Quanteninterferometrie*. Die Experimente wurden auf dem Gelände des *Albert Einstein Institus* in Hannover durchgeführt. Wir verwenden die experimentellen Ergebnisse und kombinieren sie mit den theoretischen Analysen, die wir in dieser Arbeit präsentieren.

Zunächst beschäftigen wir uns im ersten Hauptkapitel mit der allgemeinen Laufzeitanalyse von experimentellen Umsetzungen quantenkryptografischer Protokolle. Dabei zeigen wir, dass Protokolle, die eine ungleiche Gewichtung der Messbasen erlauben, die Schlüssellänge, die in einem Laufe eines Experiments generiert werden kann, maximieren. Davon motiviert, erweitern wir existierende quantenkryptografische Protokolle um genau diese Möglichkeit der ungleichen Gewichtung der Messbasen. Anhand von Laufzeitanalysen und Simulation vergleichen wir die neuen Protokolle mit ihren Vorgängern. Abschließend diskutieren wir auf Grundlage der neuen quantenkryptografischen Sicherheitsprotokolle ein kommunales Netzwerk, das physikalisch sichere Kommunikation ermöglicht.

Das zweite Hauptkapitel beschäftigt sich mit der Erzeugung eines sicheren Schlüssels im Experiment. Dabei beschäftigen wir uns insbesondere mit der klassischen Fehlerkorrektur, die benötigt wird, um einen sicheren Schlüssel generieren zu können. Der Grund dafür ist, dass die quantenkryptografischen Protokolle, die wir in dieser Arbeit untersuchen, spezielle Anforderungen an die klassische Fehlerkorrektur stellen. Wir präsentieren eine hybride Fehlerkorrektur, die speziell für diese quantenkryptografischen Protokolle geeignet ist und verwenden sie in einem Experiment. Abschließend zeigen wir die Effizienz der hybriden Fehlerkorrektur anhand einer allgemeineren technischen Analyse.

Stichworte: Quanten-Schlüsselerzeugung, Hybride Fehlerkorrektur, Laufzeitanalyse, Asymmetrische Protokolle

Contents

1. Glossary

AEI	Albert Einstein Institut
QIG	Quantum Information Group
ITP	Institut für Theoretische Physik
LUH	Leibniz Universität Hannover
QKD	Quantum Key Distribution
DV-QKD	Discrete Variable QKD
CV-QKD	Continuous Variable QKD
SHG	Second Harmonic Generation
OPA	Optical Parametric Amplification
BER	Bit Error Rate
ABER	Alphabet Error Rate
LDPC	Low Density Parity Check
s-class	Two Squeezed States
v-class	One Squeezed State
sqz	Squeezing
asqz	Anti-Squeezing
SNR	Signal to Noise Ratio
SNF	Simon Normal Form
PPKTP	Periodically Poled Potassium Titanyle Phosphate
LO	Local Oscillator
i.i.d.	Identically and Independently Distributed Random Variable
Tuples	All Synchronised Measurements of Alice and Bob
Samples	Synchronised and Correlated Measurements of Alice and Bob
FER	Frame Error Rate
$\mathcal{N}$	Gaussian distribution
W	Wishart Distribution
$\mathcal{W}$	Wigner Function
T_{run}	Runtime
$\mathcal{GF}$	Galois Field
χ	Alphabet
F_m^e	Runtime Protocol Family
F_{m,T_M,T_S}^e	Runtime Family with Independent Switching
$F_{m,T_{MS}}^e$	Runtime Family without Independent Switching

T_M	Time of Measurement
T_S	Time of Switching
Q	General Quadrature
X	Amplitude Quadrature
P	Phase Quadrature
Q_{45}	Linear Combination of X and P
q_i	Weight of i'th Basis
k_{pot}	Potential Secure Key Rate
k_{sec}	Extractable Secure Key Rate
γ	General Covariance Matrix
γ_{AB}	Bipartite Covariance Matrix
γ_X	Amplitude Sub Phase Space
γ_P	Phase Sub Phase Space
C_X	Amplitude Quadrature Correlation
C_P	Phase Quadrature Correlation
$\lvert\nu\rangle$	Squeezed State
$\lvert\text{vac}\rangle$	Vacuum State
$\text{tr}\left[\rho\right]$	Trace of State ρ
$\langle A\rangle$	Expectation Value of A
δ	Spacing Parameter
α	Cut Off Parameter of CV-QKD Protocol
α_{EC}	Cut Off Parameter of Reconciliation Protocol
χ_{KG}	Key Generation Alphabet
G_{KG}	Key Generation Grid
N_{tot}	Number of Measurements of One Participant
N_{pe}	Number of Parameter Estimation Samples
N_{EC}	Number of Reconciliation Samples
N_{sift}	Number of Samples Dropped by Sifting
N_{key}	Number of Key Generation Samples
M_{AB}	Measurement Samples of Alice and Bob
K_{AB}	Raw Key Samples of Alice and Bob
$\mathcal{H}(X)$	Von Neumann Entropy of Variable X
$\mathrm{S}(X)$	Shannon Entropy of Variable X
σ	Uncertainty (Standard Deviation)
C_{ε_s}	Confidence Set
d_0	Protocol Parameter of Coherent Protocol
ΔT_{sync}	Synchronisation Time Interval
ν	Gaussian Damping
β_{EC}	Efficiency of Reconciliation
DN	Classical Noise
$\Delta\phi_{\text{PN}}$	Phase Noise
$\mathrm{I}(X_A : X_B)$	Mutual Information of X_A Conditioned on X_B

$\lambda = \mathrm{Var}(X)$	Variance of Variable X
ε_0	Permittivity of Vacuum
ε_C	Correctness of QKD Protocol
ε_S	Secrecy of QKD Protocol
$H_{\min}$	Min Entropy
$H_{\max}$	Max Entropy
$H^{\epsilon}_{\min}$	Smoothed Min Entropy
$H^{\epsilon}_{\max}$	Smoothed Max Entropy
$\varepsilon\left(\gamma_{AB}\right)$	Peres-Horodecki-Simon Entanglement Criterion
ρ^{i}	Correlation Coefficient with $i \in \{X, P\}$
$\mu\left(\gamma_{AB}\right)$	Purity
R	Coding Rate

2. Introduction

2.1. Classical Secret Communication

One prominent manifestation of our information age is the *internet*, which was founded in 1969 by the *US Government of Defence* under the project *advanced research project agency* (ARPA) [Abb99]. It was initially designed to link the resources of universities and research facilities. Since its further development in the 1970's and the parallel advancement in computer technology, its usage has been enlarged more and more to the private and business sectors, with servers connecting the computers of all the participants. For example, nowadays people share private information via the internet using social platforms or mail and companies use it for presentation, advertisement, taking order and market research. With this development, several levels of security requirements arose because some of the participants do not want to publicly share their information (secret communication). These classical information theory tasks lead to the development of new classical encryption techniques like RSA (asymmetric) [RSA78] and AES (symmetric) [Inf01].

Let us focus on two parties participating in secret communication, who are conventionally referred to as Alice and Bob. The information which is to be secretly shared between the participants is encrypted by the sender before it is sent over the insecure classical channel (the internet) to the receiver. The receiver (Bob) then has to decrypt the message to make it readable again.

One important loophole of classical secret communication is the generation of the keys used to encrypt and decrypt the message [DFSW10a, DFSW10b]. If only deterministic algorithms are used to generate the keys a possible attacker could use them to break the security of the system with higher probability. Using random numbers in the process of key generation algorithms circumvents this problem. Note that real randomness can in principle not be found in classical physics, given full knowledge of the state, it is always deterministic. This problem is partly circumvented by using very complicated classical algorithms which are especially hard to predict. One could also, for example, use thermal noise to generate the random numbers [Sai03]. Although thermal noise is, in principle, also deterministic it is very hard to

predict the outcomes if the physical system is large enough. Note that, in this sense, classical cryptography aims to maximise the key space using (preferably complicated) algorithms [Sin99].

Another way to increase the security of secret communication is to use a key which is as long as the message (*one-time pad*). This avoids redundancies in the encrypted message which necessarily occur when the key is shorter than the message. The problem of such techniques is that the key must first be distributed between the participants of the secret communication using a secure classical channel and classical channels are, in principle, never really secure as information can, in classical physics, be copied arbitrarily often without anyone noticing.

In 2013 a major attack on the whole internet was made public by Edward Snowden, a former employee of the National Security Agency (NSA). He leaked important information about a group of states (USA, Canada, United Kingdom, New Zealand, Australia) concerning large scale eavesdropping on the internet. Some of their projects aim directly at storing, at minimum, the meta data of entire countries for days or even months, while others allow for real-time surveillance. One special project (Bullrun, USA) even attempts to make encrypted texts readable in real-time. It attacks the certification and random number generation of encryption protocols.

To summarise, one problem of classical ciphering is that it can, in principle, always be decoded as there is no real randomness in classical theory. The other problem is, that information can, in classical theory, be copied arbitrarily often. Quantum Key Distribution (QKD) offers an elegant way to circumvent classical drawbacks. It combines real randomness with the quantification of the security of the one time pad, which is distributed between Alice and Bob under the assumption of different classes of eavesdropping. The security of QKD relies not on the computational complexity of the secret communication but instead on the laws of quantum physics. The best strategy to break the security under the assumption of different classes of eavesdropping is to either directly intrude the laboratories of the honest parties or guessing the one time pad.

2.2. Quantum Key Distribution

The history of QKD can be traced back to a publication by Stephen Wiesner [Wie84]. In that publication he presented a scheme which uses only fun-

damentals of quantum physics to render money uncopyable. He assumed, that every banknote has a quantum memory containing a number of photons with a specific combination of polarisations (its serial number) which is unique for that banknote and only known to the bank[1].

Every time the banknote is used in transactions, the bank measures the state of the polarisations of the photons in the banknote. Assuming an ideal quantum memory, the polarisations of the photons carrying the serial number are perfectly maintained. If someone tried to copy a banknote, he would necessarily have to copy the polarisations of the photons (which are unknown to him) too. It is very likely that he does not measure all the photons in the correct measurement bases, which disturbs the state of the photons in the original banknote. Furthermore, as the photons have not been measured properly, the polarisations of the copied banknote are partly incorrect. This is detected the next time the banknote is used in transactions. The major problem of Wiesner's quantum money is the assumption of almost-ideal quantum memories. Even today quantum-memories are at most stable only for seconds [SAA$^+$10].

In 1984 Bennett and Brassard presented the first QKD protocol [BB84], where they used the ideas of Wiesner to certify the security of a quantum channel used to share a secure key (one time pad) between two participating parties (Alice and Bob). We call the attacker who eavesdrops on the quantum channel 'Eve'.

In this setting Alice prepares single photons randomly in one of the four states of the two bases $\times$ and $+$ and sends them to Bob. Bob subsequently measures the incoming states and stores his measurement outcomes. Afterwards, Alice sends Bob the bases in which she prepared the photons over an authenticated classical channel. Alice and Bob use this knowledge to quantify the amount of secure information that can be shared and use the measurement tuples to generate their raw keys. The raw keys have to be corrected as they are generally not perfectly correlated in an non-ideal setup. The raw keys are equal after the classical reconciliation and are folded to the secure length, which is determined by the secure key rate. Alice and Bob then use their secure key as a one-time pad to perform secret communication. Alice encodes the text which is to be secretly transmitted using her secure key and sends it over an authenticated classical channel to Bob who decodes it. The first proof of principle experiment was realised in 1992 [BBB$^+$92].

[1] Wiesner proposed to use the horizontal 0° and vertical 90° basis (the $+$ bases) and the diagonal bases $\times$ with 45° and 135°.

QKD has become a mature branch of quantum information in the last 30 years of research. Many different protocols and setups have been proposed and experimentally verified since then [SBPC+09]. They can generally be sorted into four major fields [SBPC+09] as described in Figure 2.1. Some QKD protocols generate the key from discrete variables (commonly the polarisation of light fields or single photons). Such protocols are called discrete variable protocols (DV-QKD). The very first QKD protocol ([BB84]) uses the polarisation of single photons and is a good representative of a prepare and measure DV-QKD protocol. There also exist entanglement-based DV-QKD protocols which generate the key from the correlations of, for example, the polarisation of entangled photons [Eke91]. One can additionally use continuous variable systems to distribute the raw keys, as in, for example, Gaussian modulated prepare and measure CV-QKD protocols [SBPC+09]. In this thesis we analyse CV-QKD protocols which use entangled coherent laser beams and balanced homodyne detection to distribute the information from which the one-time pad is generated. The raw keys are generated from the synchronised and correlated amplitude or phase measurements of the two parties.

	Prepare and Measure	**Entanglement Based**
DV-QKD	BB84 [BB84]	E91 [Eke91]
CV-QKD	Gaussian Modulated [SBPC+09]	*"Crypto on Campus"* [GHD+14]

Figure 2.1.: The classification of QKD protocols with examples.

The main difference between coherent laser beams and single photon pulses is that single photons always have a finite but possibly very small probability of arriving at the detector. In an ideal setting, single photon QKD allows for arbitrary large distances depending only on how long one can or wants to wait to generate a secure key. The maximum distance of experimental im-

plementations is limited by dark counts of the detectors [BLMS00]. Coherent laser beams experience some damping as they travel and the maximum distance of CV-QKD systems is thus defined by the maximum amount of noise the system can sustain whilst still generating a positive raw key.

2.3. Continuous Variable Quantum Key Distribution

Note that we focus in this thesis on a specific experimental realisation of CV-QKD amongst many others [BvL05]. The experimental setup under consideration uses entangled two-mode squeezed states and balanced homodyne detection to generate the raw key [GHD+14]. The initially independent squeezed states are generated using second harmonic generation and optical parametric down conversion in a cavity [MAE+11]. A bipartite entangled state of Alice and Bob is realised by entangling the two squeezed Gaussian states using a $50:50$ beam splitter. Alice and Bob perform synchronised homodyne detection on their states to generate the measurement tuples which are used later on in the CV-QKD protocol. The bases are chosen identically and independently using a quantum random number generator (see for example [FWN+10]). Note that Alice's and Bob's Gaussian states may experience different physical effects before they are measured by homodyne detection. We will explain the setup (see [EHS13]) in detail in Section 3.3 and assume that Alice holds the source of the entangled bipartite state unless otherwise noted.

Let us focus on the usage of the experimental setup in CV-QKD protocols. The measurement tuples are used for the tomography of the state and for raw key generation [SBPC+09]. The tomography of the state allows us to compute the secure rate k_{sec} of the setup. The classical post processing corrects the errors and folds the generated bit strings to the secure length k_{sec}. The outcome is a one-time pad which can be used to encrypt and decrypt a text which is then sent over an authenticated classical channel (possibly the internet). The security of the one-time pad relies on the assumptions of the CV-QKD protocol and is certified on the level of quantum physics.

2.4. Crypto on Campus

The motivation for this thesis was simultaneously the main topic of a cooperation with the *Quantum Interferometry* group led by Prof. Dr. R. Schnabel at the *Albert Einstein Institute* (*Max-Planck Institute*) *Hannover* [Sch]. The aim

of the cooperation, named *Crypto on Campus*, was the experimental realisation of a CV-QKD experiment on the campus of the Leibniz University. It was financed by the QUEST excellence cluster from 2008 - 2013 [WFD13] and the DFG from 2013 - 2015 [WSDH14]. Figure 2.2 shows a part of the experiment which was assembled during the collaboration and used for CV-QKD.

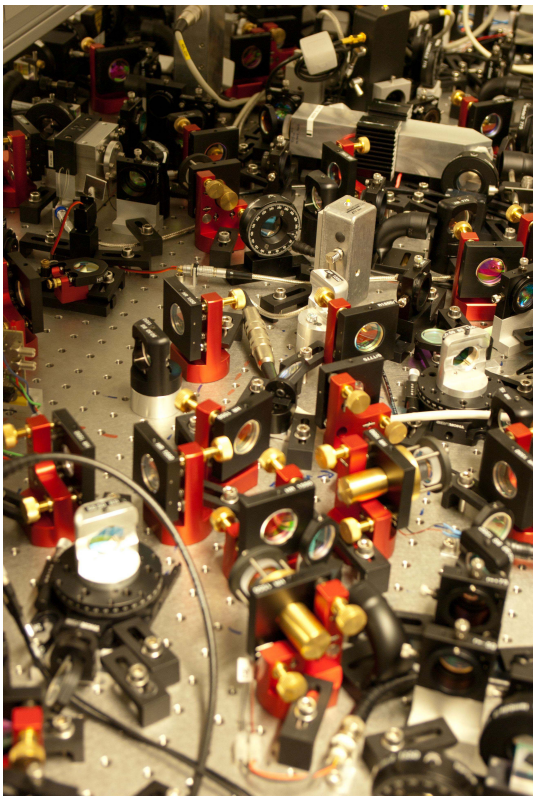

Figure 2.2.: A picture of the experimental setup. We thank the *Albert Einstein Institute* in Hannover (i.e. Sandra Marschke) for the picture.

The mathematical *Quantum Information Group* (QIG) of Prof. Dr. R. F. Werner [Wer] provided theoretical background and analysis as well as novel security proofs [FFB+14] and new reconciliation algorithms [PMD+14]. The actual implementation was realised by the group of Prof. Dr. R. Schnabel who was able to provide the entangled states needed for this task [EHS13]. In addi-

tion, several theoretical and experimental side projects have been triggered [HES+12, FFW11, Fur14].

Up to now four Ph.D. theses are directly concerned with this cooperation [Fur12, Fra13, Ebe13] (and this one) and a fifth from Dipl.-Phys. Vitus Haendchen is yet to come. This thesis is related to the aforementioned publications as it provides an overview of the whole process, the algorithms needed for its successful accomplishment, and extensions of the protocols proposed by Dr. F. Furrer *et al.* [FFB+14].

First we prepared for upcoming experiments showing that the setup is information theoretically secure against collective attacks in the limit of infinitely many measurements following the protocol of [DHF+07]. The QIG began to develop new security proofs for the setup at hand, thereby exploiting the characteristics of squeezed Gaussian states in the realm of the (smooth) Min- Max-entropy formalism which was introduced by Prof. Dr. R. Renner [Ren05]. This ansatz allows for a security analysis including finite-size effects inevitable in experiment. Basic theoretical results on the first feasible protocol for CV-QKD are described in wide detail in the Ph.D.-theses of Dr. F. Furrer [Fur12] and Dr. T. Franz [Fra13]. They describe a protocol under which the actual experimental setup is information theoretically secure against most general, so called coherent, attacks. They achieve this by including a finite size analysis based on one-shot entropies and entropic uncertainty relations. One-shot means in this sense one synchronised measurement tuple of Alice and Bob.

Crypto on Campus ended when a key secure against coherent attacks was generated from a table-top experiment as described in Section 6.3.6 and published in [GHD+14]. In that experiment we used the new reconciliation scheme which we present in this thesis in Chapter 6 to generate the secure key.

2.5. Contributions

We describe in this section the contributions of this thesis to the project *Crypto on Campus* and to the field of QKD.

Chapter 5 explains how non-uniform weights of the two involved bases can improve the key which is generated by a QKD protocol. The chapter begins with a general investigation of the runtime of QKD protocols and shows that asymmetric protocols generate more key than their symmetric variants in a

given time interval. We use this as motivation for CV-QKD protocols which allow for a non-uniform choice of the basis to be measured and extend the symmetric protocols proposed in [FFB+14] to the level of asymmetric protocols. The improvements of the new asymmetric protocols are shown in a simulation which is based on experimental results. The chapter concludes with an investigation of the experimental realisation of an urban QKD network using the asymmetric protocols and closes with a discussion. Our publications affiliated with the chapter are [EHD+13] and [EHD+11].

The nature of the CV-QKD protocols we used in the experiments raises special demands on the reconciliation scheme which is needed to correct the errors between the raw keys of Alice and Bob during the classical post processing. Chapter 6 describes a reconciliation scheme which exploits exactly the correlations on which the key generation of the protocols relies, thus achieving high efficiency. We discuss the new reconciliation scheme in detail, together with a numerical simulation of the algorithm, and show how it was used in an experiment which generated a key secure against coherent attacks. The reconciliation scheme is compared with standard non-binary reconciliation using low density parity check matrices. The chapter closes with a full technical analysis of the new reconciliation scheme and a discussion. Our publications affiliated with the chapter are [GHD+14] and [PMD+14].

This thesis furthermore provides, in the introductory Chapters 3 and 4, a solid connection between the theory and its realisation in an experiment. We also provide an overview of the project *Crypto on Campus*.

3. Preliminaries: Quantum Optics

3.1. Overview

We start in Section 3.2 with the basic phase-space theory needed for a full quantum mechanical description of the setup under consideration. We detail in Section 3.3 the experimental setup and continue with Section 3.4 where we explain the experimental parts and their theoretical description. Section 3.5 explains the full tomography of a bipartite Gaussian state. We focus on Gaussian bipartite states during the whole thesis and provide a detailed introduction to the theoretical basics and the experimental realisations in this chapter.

As this chapter is explicitly meant as an introduction we do not present any novel physics in it, when not otherwise noted. Note that we provide a solid connection between the theoretical background and the experimental setups discussed within this section.

3.2. Theoretical Background

Before going into the details of the CV-QKD setup in Section 3.3 we introduce the basic mathematical framework for the representation of Gaussian states using the Wigner function [Wig32] in this section. Since we focus on Gaussian states which can in very good approximation describe the laser beams used in the experimental setup, the canonical Hilbert space is of infinite dimension, which could hinder further analysis. One possible solution is the usage of phase-space variables as they greatly simplify the description of the situation. As the following chapters rely on this description, we will explain the theory in more detail.

3.2.1. Gaussian Systems

We start with the general description of quantum states in the realm of unbounded canonical conjugated operators as described in [RS78] and continue with a specific selection of two canonically conjugated operators, namely

the amplitude (position, X) and phase (momentum, P) quadrature operators. Good indroductions in this topic are also naturally the other Ph. D. theses which have been written as part of the collaboration *Crypto on Campus* [Fur12, Fra13, Ebe13]. We continue with a general description of Gaussian states in phase-space using the Wigner function and close the section with some functions which are needed to characterise Gaussian states.

Let us start with the expectation value of an operator F for a quantum state ρ which is in general defined by

$$\langle F \rangle_\rho \coloneqq \mathrm{tr}\left[F\rho\right]. \tag{3.1}$$

As laser beams with many photons are at the center of our interest we now focus on quadrature measurements described by two canonically conjugated operators. This can be realised by associating the system with a phase-space together with an appropriate set of field operators, namely the aforementioned amplitude and the phase quadrature. Note that the operators enable a full description of the state by the Wigner quasi-probability function $\mathcal{W}_\rho(x,p)$. For these states a Weyl-ordered function $F(X,P)$ of the canonical conjugated variables exists. We can find for every $F(X,P)$ a classical function $f(x,p)$ such that

$$\langle F(X,P)\rangle_\rho = \mathrm{tr}\left[F\rho\right] = \int \mathcal{W}_\rho(x,p)\cdot f(x,p)\mathrm{d}x\,\mathrm{d}p,$$

following the formulation of Wigner as described in [Wig32]. The formulation was extended to all Weyl ordered functions in [Moy49].

In the commutation relation

$$[X,P]_\rho = 2i$$

the operators are chosen with $\hbar = 2$. This is a common convention in quantum optics and results in a variance of the vacuum state equal to one as we will show later[1]. The two measurement operators are usually realised by homodyne detection as we will describe in more detail in Section 3.4.5. Together with the symplectic form

$$\sigma = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{3.2}$$

[1] Note, that $\hbar = 1$ is also sometimes used in quantum mechanics which results in a variance of the vacuum state equal to $1/2$.

we can map the parameter space of one mode to a real plane which we call the phase-space. As we are especially interested in entangled bipartite states, we focus in the following on a multi-mode of several beams. Such a system can be described by a $2n$-dimensional phase-space for the $2n$ field operators $\{R_i\}$ with $i \in \{1,...,2n\}$ where the symplectic form is given by

$$\sigma_n = \bigoplus_{k=1}^{n} \sigma.$$

After having explained the mathematical background necessary to describe the system, we show how it is linked to experimentally measurable quantities. For this, we write all the field operators as elements of a vector $\vec{R}$ in phase-space with $\vec{R} = (R_1, R_2, ..., R_{2n-1}, R_{2n})^T$ and define

$$\vec{R} := (X_1, P_1, ..., X_n, P_n)^T$$

which is a specific set of field operators, namely the amplitude X (phase P) quadrature operators $R_{2n-1} = X_n$ ($R_{2n} = P_n$) of the light field. We use this vector to define the family of Weyl operators [HOSW84] by

$$\mathcal{W}(\vec{\xi}) = \exp\left[i\vec{\xi}^T \sigma_N \vec{R}\right],$$

where $\vec{\xi} \in \mathbb{R}^n$ is another phase-space vector. If we choose the order of its elements to be $\vec{\xi} = (x_1, p_1, ..., x_n, p_n)$ we can write

$$\mathcal{W}(\vec{\xi}) = \exp\left[i\sum_{i}^{n}(x_i X_i - p_i P_i)\right],$$

which is a phase-space translation. With this we can write down the connection between the Weyl operator $\mathcal{W}$ and the multi-mode quantum state ρ describing the system by its characteristic function

$$\chi(\vec{\xi}) = \mathrm{tr}\left[\rho\mathcal{W}(\vec{\xi})\right].$$

The Wigner function can now be written as the symplectic Fourier transform of the characteristic function

$$\mathcal{W}_\rho\left(\vec{\xi}\right) = \frac{1}{2\pi}\int \chi(\vec{\eta})\cdot\exp(i\vec{\eta}\sigma\vec{\xi})\mathrm{d}\eta_1...\mathrm{d}\eta_{2n}. \tag{3.3}$$

Wigner function:

The Wigner function describes the representation of any state ρ in phase-space. In the following we focus on Gaussian quantum states. This class of states is defined by a Gaussian distribution in phase-space. The Wigner functions of Gaussian states thus have positive values for the whole parameter space and can hence be interpreted as quasi-probability functions in phase-space[2].

An n-mode quantum system in state ρ together with the field operators $\vec{R} = (X_1, P_1, ..., X_n, P_n)$ is a Gaussian state if its Wigner function can be written as

$$\mathcal{W}_\rho(\xi,\gamma) = \frac{1}{(2\pi)^n\sqrt{\det(\gamma)}} \exp\left[-\frac{1}{2}(\vec{\xi}-\vec{\xi}_0)^T\gamma^{-1}(\vec{\xi}-\vec{\xi}_0)\right], \tag{3.4}$$

with the physicality (positivity) condition

$$\rho \geq 0 \quad \Leftrightarrow \quad \gamma + i\sigma \geq 0 \tag{3.5}$$

where γ is the covariance matrix of the setup. The quantum state can hence be fully described by its first and second moments which are given by

$$\vec{\xi}_0 = \mathrm{tr}\left[\rho\vec{R}\right]$$

and

$$\gamma_{i,j} = \mathrm{tr}\left[\rho\left\{R_i, R_j\right\}_+\right].$$

We focus on states which have a mean value equal to zero and are thus fully described by their covariance matrix. The important entries of the covariance matrix can be experimentally determined by homodyne detection of the canonically conjugated measurement quadratures (see Section 3.4.5 for details). We call an experimental reconstruction of such a system the full tomography of the state and define the following three different classes [WM04] of interest:

Vacuum state	$\Leftrightarrow$	$\vec{\xi}_0 = \vec{0}$	&	$\gamma = \mathbb{1}$
Thermal state	$\Leftrightarrow$	$\vec{\xi}_0 \neq \vec{0}$	&	$\gamma = \mathrm{const}\cdot\mathbb{1}.$
Squeezed state	$\Leftrightarrow$	$\vec{\xi}_0 = \vec{0}$	&	$\gamma \neq \mathrm{const}\cdot\mathbb{1}$

Covariance matrix:

[2] There exist states which show negative values of the Wigner function [LHA+01].

The covariance matrix of a bipartite Wigner state consisting of the subsystems of Alice A and Bob B can be decomposed as

$$\gamma_{AB} = \begin{pmatrix} \gamma_A & \gamma_C \\ \gamma_C^T & \gamma_B \end{pmatrix} \tag{3.6}$$

where the sub-matrix γ_C describes the correlations between Alice's and Bob's subsystems γ_A and γ_B.

In the following we discuss some properties of the covariance matrix. The covariance matrix has 16 independent parameters, but as a covariance matrix is symmetric, we are left with ten independent values

$$\gamma_{AB} = \left(\begin{array}{cc|cc} \lambda_{1,1} & \lambda_{2,1} & \lambda_{3,1} & \lambda_{4,1} \\ \lambda_{2,1} & \lambda_{2,2} & \lambda_{3,2} & \lambda_{4,2} \\ \hline \lambda_{3,1} & \lambda_{3,2} & \lambda_{3,3} & \lambda_{4,3} \\ \lambda_{4,1} & \lambda_{4,2} & \lambda_{4,3} & \lambda_{4,4} \end{array}\right). \tag{3.7}$$

Each measured bipartite state can be diagonalised by a specific choice of local rotations followed by an additional squeezing of the sub-blocks of Alice and Bob. Such a diagonalisation operation is given by the Simon Normal Form (SNF) of the covariance matrix of the corresponding Gaussian state [Sim00] which is in general

$$\gamma_{AB} = \left(\begin{array}{cc|cc} \lambda_A & 0 & C_X & 0 \\ 0 & \lambda_A & 0 & -C_P \\ \hline C_X & 0 & \lambda_B & 0 \\ 0 & -C_P & 0 & \lambda_B \end{array}\right) \tag{3.8}$$

where C_X and C_P describe the correlations between the synchronised amplitude or phase measurements of Alice and Bob. Note that two different kinds of asymmetries of the bipartite state of Alice and Bob can be seen in this representation. Firstly, the asymmetry between the variances of Alice's and Bob's amplitude (phase) measurements $\lambda_A \neq \lambda_B$ and secondly, the asymmetry in the covariances $C_X \neq C_P$ between their sub-systems.

The SNF of any covariance matrix is only a function of four instead of ten parameters. The reason is, that information about the possible squeezing of Alice's and Bob's subsystem is lost during the 're-squeezing' and the local rotations which are needed to transform the covariance matrix γ_{AB} to the SNF. The four parameters are mathematically independent albeit obeying

$$0 \leq C_X \leq \min\{\lambda_A, \lambda_B\}$$
$$0 \leq C_P \leq \min\{\lambda_A, \lambda_B\}.$$

We can now identify four functions that are invariant under local symplectic transformations of the covariance matrix [Sim00]:

$$\begin{aligned} I_1 &= \det[\gamma_A] = \lambda_A^2 \\ I_2 &= \det[\gamma_B] = \lambda_B^2 \\ I_3 &= \det[\gamma_C] = -C_X C_P \\ I_4 &= \det[\gamma_{AB}] = \left(C_X^2 - \lambda_A \lambda_B\right) \cdot \left(C_P^2 - \lambda_A \lambda_B\right). \end{aligned} \tag{3.9}$$

We call these functions in the following the symplectic invariants and use them to evaluate important physical values like, for example, the purity or the Peres-Horodecki-Simon entanglement criterion. As we have identified the symplectic invariants as a function of the determinants of the three sub-matrices and the full covariance matrix, we can now directly compute them without mapping the actual covariance matrix to the SNF.

The purity of quantum states is, in general, given by

$$\mu(\rho) = \mathrm{tr}\left[\rho^2\right].$$

Using the symplectic invariants, we can rewrite the purity of a bipartite Gaussian state by [SIPDS04]

$$\mu(\gamma) = \frac{1}{\sqrt{\det[\gamma]}} = \frac{1}{\sqrt{I_4}}. \tag{3.10}$$

The symplectic eigenvalues can be written as [BND+10]

$$d_\pm = \sqrt{1/2 \cdot \left((I_1 + I_2 + 2I_3) \pm \sqrt{(I_1 + I_2 + 2I_3)^2 - 4I_4}\right)}. \tag{3.11}$$

We can use the symplectic eigenvalues to define the Peres-Horodecki-Simon entanglement criterion $\mathcal{E}$ for bipartite entangled system [Sim00]

$$\mathcal{E}\left(\gamma_{AB}\right) = \max\left\{0, -\log[-2d_-]\right\}, \tag{3.12}$$

which is also known as the logarithmic negativity [SIPDS04].

For later tasks we define four different sub-phase-spaces of special interest:

γ_A	Alice's block describing her local X and P measurements
γ_B	Bob's block describing his local X and P measurements
γ_{AB}^X	Describing bipartite synchronised X measurements
γ_{AB}^P	Describing bipartite synchronised P measurements

Most important are the sub-matrices describing the quasi-probability of Alice's and Bob's outcomes of synchronised amplitude X or phase P measurements. The synchronised amplitude measurement outcomes are described in terms of the covariance matrix γ_{AB} by

$$\gamma_{AB}^{X} = \begin{pmatrix} \gamma_{11} & \gamma_{31} \\ \gamma_{31} & \gamma_{33} \end{pmatrix}, \tag{3.13}$$

where γ_{31} describes the correlations between their outcomes. Accordingly, the synchronised phase measurements are

$$\gamma_{AB}^{P} = \begin{pmatrix} \gamma_{22} & \gamma_{42} \\ \gamma_{42} & \gamma_{44} \end{pmatrix}. \tag{3.14}$$

3.2.2. Squeezed States

Here we give an example of the simplifications possible when using the description of Gaussian states in phase-space, starting with one mode in canonic number representation. We additionally define the operators for the amplitude and phase measurement of a Gaussian beam as we need the operators to describe the homodyne detection in Section 3.4.5. Good introductions to quantum optics in general and Gaussian states are [WM04, MW95, GK05, Lou97]. Let us start with the description of coherent states.

Coherent states:
We begin with the basic description of a one-mode coherent state $|\nu\rangle$ in Fock representation $|n\rangle \in \mathbb{F}_+(\mathcal{H})$ where the $|n\rangle$ are a complete orthonormal basis:

$$\begin{aligned} |\nu\rangle &= \exp\left[-\frac{|\nu|^2}{2}\right] \cdot \sum_{n=0}^{\infty} \frac{\nu^n}{\sqrt{n!}} |n\rangle \\ &= \exp\left[-\frac{|\nu|^2}{2}\right] \cdot \sum_{n=0}^{\infty} \frac{\nu^n a^\dagger}{\sqrt{n!}} |\text{vac}\rangle \\ &= \exp\left[-\frac{|\nu|^2}{2}\right] \cdot \exp\left\{\nu a^\dagger\right\} |\text{vac}\rangle \\ &= \mathcal{D}(\nu) \cdot |\text{vac}\rangle \end{aligned}$$

where a ($a^\dagger$) is the annihilation (creation) operator and $\mathcal{D}(\nu)$ the displacement operator. Let us additionally define the number operator $n = a^\dagger a$ as we

will need it later. We are again interested in measuring the amplitude (phase) quadrature of the light field and define

$$X = \left(\frac{\hbar}{2\omega}\right)^{\frac{1}{2}} \cdot \left(a + a^{\dagger}\right), \tag{3.15}$$

which is the canonical amplitude quadrature operator and

$$P = i\left(\frac{\hbar\omega}{2}\right)^{\frac{1}{2}} \cdot \left(a^{\dagger} - a\right), \tag{3.16}$$

the canonical phase quadrature operator with ω denoting the frequency of the described light beam which is usually $\omega = 1$ for the rest of this thesis. The variance of an operator A is in general defined by

$$\begin{aligned} \mathrm{Var}(A) &:= \langle A^2 \rangle - \langle A \rangle^2 = \lambda_A \\ \sigma_A &:= \sqrt{\lambda_A} \end{aligned}$$

where we additionally introduced the uncertainty (standard deviation) σ_A of the operator A. Evaluating the variance (and the uncertainty) of the amplitude X and phase P quadrature operator for a coherent state we find

$$\begin{aligned} \mathrm{Var}(X)_{|\nu\rangle} &= (\sigma_X)^2 = \frac{\hbar}{2} \\ \mathrm{Var}(P)_{|\nu\rangle} &= (\sigma_P)^2 = \frac{\hbar}{2}. \end{aligned}$$

The uncertainties of a coherent vacuum state ($\mathcal{D}(\nu) = \mathcal{D}(\nu = 0)$) are illustrated in Figure 3.1. We now evaluate Heisenberg's uncertainty relation [Hei27] of the two quadratures for a coherent state by

$$\sigma_X \cdot \sigma_P = \frac{\hbar}{2} \tag{3.17}$$

and see that ideal coherent states are of minimal uncertainty. Remembering $\hbar = 2$ from Section 3.2.1 we see that

$$\sigma_X \cdot \sigma_P = 1 \tag{3.18}$$

which is the reason why we chose $\hbar = 2$. Note that all the states we use in this thesis are given in terms of the vacuum which is in this sense normalised to one.

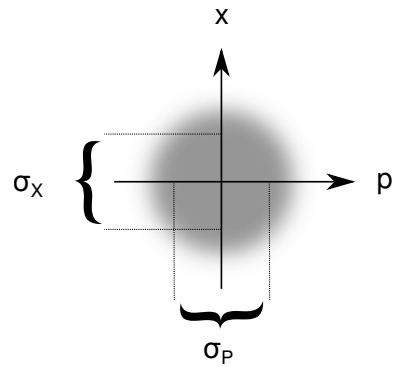

Figure 3.1.: A Gaussian vacuum state in phase-space has, given to our choice of physical constants ($\hbar = 2$), a variance of $\sigma_X = \sigma_P = 1$ and minimal uncertainty. If $\nu \neq 0$ the vacuum state is displaced in phase-space. We focus for the rest of this thesis on Gaussian states with $\nu = 0$.

Squeezed states:
The class of coherent states is a sub group of a larger class of states having the same property. To show this we introduce a unitary squeezing operator

$$\mathcal{S}(\Theta) = \exp\left[\Theta\left(a^2 - (a^\dagger)^2\right)\right],$$

where $\Theta \in \mathbb{R}$, and let it act on the coherent state

$$|\nu, \Theta\rangle = \mathcal{S}(\Theta)\mathcal{D}(\nu)|\text{vac}\rangle \tag{3.19}$$

resulting in a squeezed state when $\Theta \neq 0$. The name comes from the profile of a squeezed state in phase space as explained in Figure 3.2. We now calculate the variances (uncertainties) of X and P of a squeezed state

$$\begin{aligned}\text{Var}(X)_{|\nu,\Theta\rangle} &= (\sigma_X)^2 = \exp[-2\Theta] \cdot \text{Var}(X)_{|\nu\rangle} \\ \text{Var}(P)_{|\nu,\Theta\rangle} &= (\sigma_P)^2 = \exp[2\Theta] \cdot \text{Var}(P)_{|\nu\rangle}\,.\end{aligned}$$

It follows again that

$$\sigma_X \cdot \sigma_P = 1, \tag{3.20}$$

showing that ideal squeezed states allow for minimal uncertainty, too[3].

[3] Non-ideal squeezed states do not fulfill this property although they are assumed to be normalised to the vacuum as we will show later.

Let us assume that a person (for example Alice) measures a one mode squeezed state. The descriptions presented in this section are connected to the covariance matrix which is presented in the former Section 3.2.1 by

$$\mathrm{Var}(X)_{|\nu=0,\Theta\rangle} = (\gamma_A)_{1,1}$$
$$\mathrm{Var}(P)_{|\nu=0,\Theta\rangle} = (\gamma_A)_{2,2}$$

where γ_A is the covariance matrix which describes Alice's state. Note that $(\gamma_A)_{1,2} = (\gamma_A)_{2,1} = 0$ as the quadrature measurements are assumed to be ideal which is not the case in an experiment as we will show later.

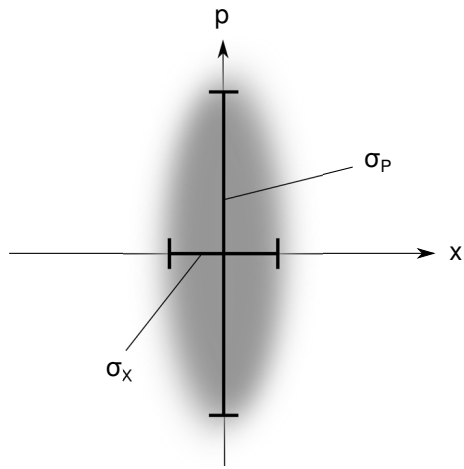

Figure 3.2.: The Wigner function of a squeezed vacuum state in phase-space. The state is chosen such that the semi-axes of the ellipse coincide with the coordinate system which relates to a perfect measurement of the amplitude and phase quadrature. The amplitude quadrature is squeezed while the phase quadrature is anti-squeezed. This example shows a squeezed vacuum state with $\mathcal{D}(\nu = 0)$. Such states are used in the CV-QKD setups which we discuss later.

Squeezed states gained a lot of interest in recent years, especially in the field of quantum metrology. The reduced uncertainty allows for the construction of a class of interferometers operating below the shot noise limit. Such interferometers are for example already in use to detect gravitational waves as part of GEO600 [GC08], LIGO [Aea13, GtLSC10, Aea12] and VIRGO [Col09].

3.3. Experimental Setup

We are about to analyse an entanglement-based CV-QKD setup using squeezed Gaussian states [GHD+14, EHD+13], certifying the security of the generated key against different classes of attacks. The corresponding experiments were realised by the group *Quantum Interferometry* which is led by Prof. Dr. Schnabel (*Albert Einstein Institute Hannover*) and which is part of the collaboration *Crypto on Campus*. Note that we focus here on one specific CV-QKD experiment amongst many possible other realisations as presented in [BvL05] and [GG02] for example.

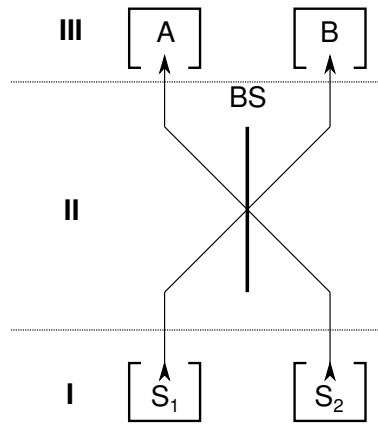

Figure 3.3.: The experiment can be split into three main parts. First, the two states are prepared by some source (I). Then they become entangled at a beam splitter and distributed to Alice and Bob through some quantum channel (II). The last stage (III) is the synchronised balanced homodyne detection by Alice and Bob followed by classical post processing.

In the setup under consideration, two sources emit initially uncorrelated squeezed Gaussian vacuum states which afterwards become entangled via a 50:50 beam splitter. The resulting beams are sent to Alice and Bob thereby experiencing different effects which can mostly in very good approximation be described by Gaussian channels as we will show later. The beams of Alice and Bob are measured by homodyne detection of either the amplitude X or the phase P quadrature. The correlations of the measurement outcomes, which are described by the covariance matrix of the bipartite state of Alice and Bob,

are the key ingredient of all the CV-QKD security proofs we use as we will show later. We subsume the operations acting on the quantum states before they are measured into the quantum channel. In this sense, the setup is naturally parted in three stages, the preparation of the sources, the quantum channel and the homodyne measurement as illustrated in Figure 3.3. The measurement basis are chosen identically and independently (i.i.d.) from a quantum random number generator.

A secure key is generated using a chosen CV-QKD protocol with appropriate classical post processing over an authenticated channel. The security of a setup can be certified by assuming some kind of classical post processing, but if one wants to generate a secure key, the classical post processing has actually to be implemented. The various parts of the setup and their theoretical description in terms of the covariance matrix are described in more detail in the next Section 3.4.

3.4. Theoretical Description of Experimental Parts

This section explains the setup under consideration in wide detail. We explain the theoretical models used to describe the setup which is introduced in the former Section 3.3. We start with a description of the sources and the initial beams and continue by explaining their superposition via a 50:50 beam splitter. The two outcoming beams are transmitted to Alice and Bob over different channels thereby experiencing different effects. Usually we assume that Alice holds the source whereby Bob can be arbitrarily far away. For further details of the experimental realisation we refer to the thesis of Dr. T. Gehring [Ebe13] and Dipl.-Phys. V. Haendchen [Hae10].

3.4.1. Sources

We explain now how the two initially independent Gaussian squeezed vacuum states, which have already been introduced in Section 3.2.2, are generated in experiment [MAE+11]. First we discuss the general physical effect in use and explain later how it is realised and used in experiment.

In the setup under consideration a source is typically made of two stages. The first stage is used for the generation of the pump beam with frequency ω_P needed to prepare the squeezed vacuum beams with frequency ω_0 in the second stage. Note, that the experimental setup is the same for both steps, the only difference is, whether the non-linear cavity (resonator) in use is working

above or below its threshold. If the cavity operates above threshold, we call the process second harmonic generation (SHG), otherwise it supports optical parametric amplification (OPA). Figure 3.4 shows the setup of the cavity. The cavity and its dimensions are chosen such that a second-order non-linear interaction between the crystal and the pump beam generates a squeezed vacuum beam in the second step. This squeezed vacuum beam can then be used for QKD tasks.

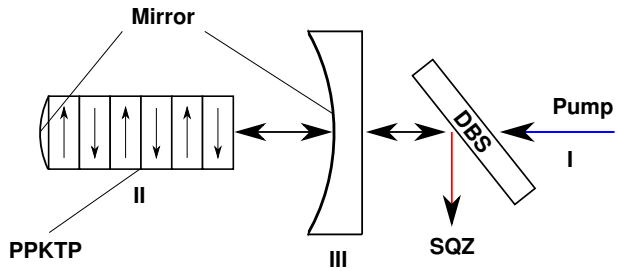

Figure 3.4.: The non-linear medium (II) is cut such that its left end is curved with a radius of 12.5 mm and the right side is plane [CVDS07]. The dominant conversion process in the crystal can be steered by the power of the pump beam (I). The crystal (II) is enclosed between two mirrors where the left one has full reflectivity for both beams and is coated towards the curved face of the crystal. The mirror on the right (III) has a transmittance of 10% for photons with frequency ω_0 and 100% for photons of frequency ω_P. Together, both mirrors form a cavity which supports a TEM_{00} mode for the beam at ω_0. A dichroic partial beam splitter (DBS) couples the converted beam out of the system for later usage.

We start the theoretical description by assuming an ideal non-linear medium (crystal) which we disturb with a laser field $\vec{E}$. The response of the crystal's valence electrons to the electric field is described by the interaction of the electric field with the polarisation of the molecules

$$\vec{P} = \varepsilon_0 \left(\eta^{(1)} \vec{E}^1 + \eta^{(2)} \vec{E}^2 + \sum_{k=3}^{\infty} \eta^{(k)} \vec{E}^k \right).$$

Here, ε_0 is the permittivity of the vacuum and $\eta^{(n)}$ the susceptibility of the crystal which describes the n'th order reaction of the valence electrons of

some molecule to an electric field. As we describe the effect of the electric field as a disturbance of the system, the first-order correction term has the largest contribution of order ≈ 1. The dynamics of the interaction are described by the corrections of higher order with $n > 1$ where the second-order susceptibility $n = 2$ is experimentally already of the order $\eta^{(2)} \approx 10^{-10}$. Note that the higher-order corrections $n > 2$ are even smaller and thus neglected. The second-order correction can be viewed as an interaction in which two incoming photons convert to one, or one photon splits into two, which is illustrated in Figure 3.5.

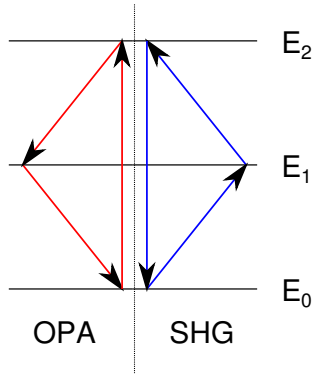

Figure 3.5.: Up conversion (blue): Two photons of lower frequency unify to one with double energy. The process is called second harmonic generation (SHG) and is used to generate the pump beam. It is the simplest case of the class of sum-frequency conversions [CBMS13]. Down conversion (red): One photon of higher energy converts into two of half the frequency.

However, these processes have to obey energy and momentum conservation

$$\vec{k}_1 + \vec{k}_2 = \vec{k}_3$$
$$\omega_1 + \omega_2 = \omega_3,$$

where the ω_i are the frequencies and the $\vec{k}_i$ the wave vectors of the three involved photons.

We provide now a more detailed description of one source:

Step 1 - SHG:
This step is needed because, for the second step, no laser with appropriate characteristics is available. Note that as the cavity operates above threshold, it can be interpreted as a laser itself.

An initial laser emits a strong beam of photons of mean frequency ω_0. The photons enter a non-linear medium positioned in a cavity with properties and geometry supporting the process of SHG for the generation of the pump beam.

As the power of the initial beam is above the threshold of the cavity, we start by assuming a strong coherent continuous initial laser. We can write the electric field at the position $\vec{r} = 0$ of some specific molecule and at time t as

$$\vec{E}(t) = \vec{E}_0 \cdot \cos\left(\vec{k}\vec{r} - \omega_0 t\right)$$

where $\vec{E}_0$ is the vector of the electric field. Choosing a proper coordinate system allows us to simplify our analysis to scalar valued functions. It follows for the second-order interaction term of the polarisation, that

$$\begin{aligned} P^{(2)}(E) &= \eta^{(2)} E_0^2 \varepsilon_0 \cdot \cos^2(\omega_0 t) \\ &= \frac{\eta^{(2)}}{2} E_0^2 \varepsilon_0 \cdot \left(1 + \cos^2(\omega_P t)\right) \end{aligned}$$

which is, apart from a constant term, a polarisation wave. This wave can, in good approximation, be treated as a Hertz dipole which itself emits an electro-magnetic wave of frequency ω_P, the pump beam[4]. Due to energy conservation, two initial photons are needed to stimulate the polarisation wave. The forced admittance thereby maintains the phase lock of the photons.

A problem of this implementation is that, for any fixed atom of the non-linear medium, we can always find another atom emitting a pump beam photon with a phase difference of $\pi/2$. Hence, the two photons undergo destructive interference and the resulting overall pump beam is approximately zero for large enough media. One solution is to break the symmetry of the crystal by introducing layers with inverse polarisation of the molecules. Such a non-linear crystal is experimentally realised as periodically poled potassium titanyle phosphate (PPKTP). If the dimensions of such a composition are chosen appropriately the constructive interference of all photons is on

[4] Note that the pump beam is, due to its experimental realisation, polarised. The polarisation is defined by the direction of the electromagnetic field.

average maintained as illustrated in Figure 3.6. The outcome of this operation are photons of frequency $\omega_P = 2 \cdot \omega_0$ serving as the pump beam, which is used in the next step to generate the squeezed vacuum states for the CV-QKD task. Such SHG's have been realised in various experiments, like for example [ANS+11].

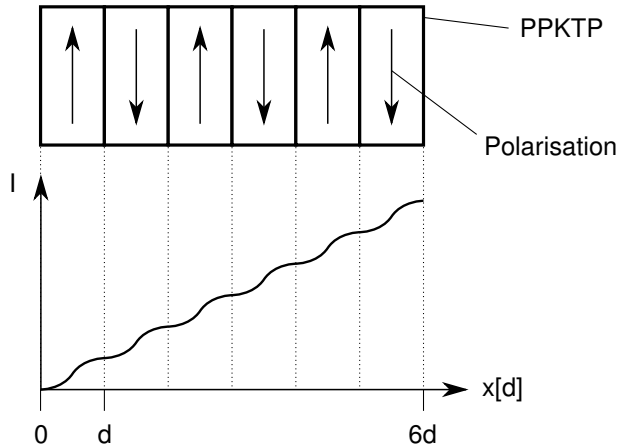

Figure 3.6.: Upper picture: The non-linear medium is composed of layers of thickness l_d with alternating directions of polarisation. l_d is chosen such, that the two beams of differing frequency (and thus different refraction index) are on average in phase, which allows for constructive interference of the pump beam photons. Lower picture: Here we sketch the increasing intensity of the generated pump beam as a function of the distance x and therefore of the amount of layers l_d it passed.

Step 2 - OPA:
The pump beam is coupled into a second cavity which outputs the squeezed vacuum beam necessary for the CV-QKD experiment. This cavity has the same configuration as the one used in the first stage (SHG), but the cavity now supports OPA as the pump beam now operates below the threshold of the cavity, so that the SHG process is thus no longer the most probable.

In this process photons of energy $\omega_P = 2 \cdot \omega_0$ are converted by the interaction with the molecules of the PPKTP crystal into pairs of photons with frequency ω_0, which we refer to as the signal beam from now on. The signal

beam is coupled out of the system by a dichroic partial beam splitter allowing for different reflectivity for different frequencies as shown in Figure 3.4. It can be shown that the two entangled down converted photons generated in each such second-order process obey the statistics of a squeezed coherent vacuum state of light [GK05].

The probability for the signal photons to be coupled out of the cavity is of the order of 10%, thus most of the photons are reflected, thereby increasing the squeezing. The portion of the signal being coupled out is the squeezed vacuum state used in the following CV-QKD experiments.

An analytic description of the variance of the squeezed and the anti-squeezed quadrature of a single state is given by [YMHA07, TYYF07]

$$\mathrm{Var}_{\substack{\mathrm{sqz}\\ \mathrm{asqz}}} = 1 \pm \eta \cdot \frac{4\sqrt{P/P_{\mathrm{th}}}}{(1 \mp \sqrt{P/P_{\mathrm{th}}})^2 + 4K^2}. \tag{3.21}$$

Most of the parameters are determined by the experimental setup of the system [EHD+11]. $P_{\mathrm{th}} \approx 10^2 mW$ is the threshold power of the system and $K \approx 10^{-1}$ is a damping mainly described by the cavity line width. $\eta \leq 1$ is the overall efficiency of the setup. The only variable left is the pump power $P \in [0, P_{\mathrm{th}})$. The Gaussianity of the resulting covariance matrix can be checked by the positivity (physicality) criterion (see Equation 3.5) or other Gaussianity tests as described in [BDP+10].

Note especially that the product of the variances of the two quadratures describing one such state is not pure

$$\mathrm{Var}_{\mathrm{sqz}} \cdot \mathrm{Var}_{\mathrm{asqz}} = \sigma_X^2 \cdot \sigma_P^2 \geq 1 \quad \forall P > 0 \quad \forall 0 \leq \eta < 1 \tag{3.22}$$

which results in product of the uncertainties of

$$\sigma_X \cdot \sigma_P > 1.$$

The generated squeezed states are hence always non-ideal and never pure.

Another, slightly more idealised description starts with a pure squeezed vacuum state which experiences some Gaussian damping. Although it does not respect the threshold power of the system P_{th}, it allows for a good description of the state.

The typical covariance matrix representation of a Gaussian single-mode squee-

zed vacuum is

$$\gamma := \begin{pmatrix} \lambda_{\text{sqz}} & 0 \\ 0 & \lambda_{\text{asqz}} \end{pmatrix}, \tag{3.23}$$

where the amplitude quadrature is chosen to be squeezed and the phase quadrature is anti-squeezed. A rotation of such a state by $\pi/2$ in phase-space, reflected by the relative phase between the pump beam and the signal, allows for another description of a Gaussian squeezed vacuum state

$$\gamma := \begin{pmatrix} \lambda_{\text{asqz}} & 0 \\ 0 & \lambda_{\text{sqz}} \end{pmatrix}, \tag{3.24}$$

where the amplitude quadrature is anti-squeezed.

3.4.2. Beam Splitter

Beam splitters are a widely used component in classical and quantum laser systems. They are for example a main ingredient in interferometers [ESB+10].

A beam splitter is a mirror with specific reflectivity $\nu_{\text{ref}} \in [0,1]$ and transmittance $\nu_{\text{trans}} = 1 - \nu_{\text{ref}}$. It is usually constructed for specific wave lengths. In classical laser systems, a beam splitter can be used to actually split up one incoming laser beam into two with less intensity but equal characteristics. This allows copying the characteristics of the incoming laser beam which is not possible in the quantum description of the same setup as we will show now. We use a beam splitter to induce correlations between the two outcoming states as shown in Figure 3.7. We furthermore assume that the two incoming light fields have the same main frequency ω_0. These two initially independent Gaussian states are described by the covariance matrices γ_A and γ_B.

We write the direct sum of the two initially independent sub-spaces of Alice and Bob as

$$\begin{aligned} \widetilde{\gamma}_{AB} &= \gamma_A \oplus \gamma_B \\ &= \begin{pmatrix} \gamma_A & 0 \\ 0 & \gamma_B \end{pmatrix}. \end{aligned}$$

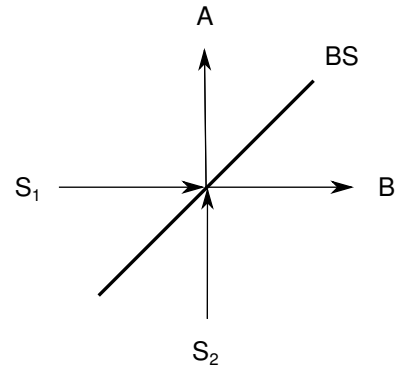

Figure 3.7.: Two Gaussian states (S_1 and S_2) are entangled via a beam splitter (BS). The correlations induced in the outcoming states (A and B) are later the key ingredient of the CV-QKD experiment.

Mathematically, a beam splitter acting on $\widetilde{\gamma}_{AB}$ is described by the unitary transformation

$$\mathrm{U}_{\mathrm{BS}} = \left(\begin{array}{cc|cc} e^{i\phi}\cos(\nu_{\mathrm{BS}}) & 0 & \sin(\nu_{\mathrm{BS}}) & 0 \\ 0 & e^{-i\phi}\cos(\nu_{\mathrm{BS}}) & 0 & \sin(\nu_{\mathrm{BS}}) \\ \hline -\sin(\nu_{\mathrm{BS}}) & 0 & e^{-i\phi}\cos(\nu_{\mathrm{BS}}) & 0 \\ 0 & -\sin(\nu_{\mathrm{BS}}) & 0 & e^{i\phi}\cos(\nu_{\mathrm{BS}}) \end{array}\right),$$

where the parameter $\nu_{\mathrm{BS}} \in [0, \pi/2]$ describes the reflectivity of the system. The operator acts on the covariance matrix as

$$\gamma_{AB}^{\mathrm{BS}} = \mathrm{U}_{\mathrm{BS}}^{-1} \cdot \widetilde{\gamma}_{AB} \cdot \mathrm{U}_{\mathrm{BS}}. \tag{3.25}$$

For the rest of this thesis we consider only 50:50 beam splitters with[5] $\nu_{\mathrm{ref}} = \nu_{\mathrm{trans}} = 0.5$ and, without loss of generality, we set the general phase $\phi = 0$. In the rest of the thesis we mainly focus on the two following sets of states:

S-class:
Both of the input states are squeezed vacuum states. To achieve maximum correlation between Alice's and Bob's amplitude and phase measurements, one beam is squeezed while the other is anti-squeezed in the amplitude quadrature or vice versa for the phase quadrature.

[5] Note that there exists a trigonometric bijective mapping between $\nu_{\mathsf{BS}} \in [0, \pi/2]$ and $\nu_{\mathsf{ref}} = 1 - \nu_{\mathsf{trans}} \in [0, 1]$.

V-class:
One of the input states is squeezed while the other is a vacuum state. The correlations of an v-class state are less strong when compared to an s-class state with similar squeezing as we will show later.

The resulting state $\gamma_{AB}^{\mathrm{BS}}$ is Gaussian if the initial covariance matrix $\widetilde{\gamma}_{AB}$ represents a Gaussian state.

3.4.3. Gaussian Damping

Gaussian damping preserves the Gaussianity of the initial state by a convex combination of it with a Gaussian vacuum state. Optical loss can be mostly described by Gaussian damping as it stems in general from absorption, scattering, the non-ideal quantum efficiency of the balanced homodyne detector and non-perfect mode-matching.

For one signal mode (for example Alice's) it can be directly modelled by a convex combination of the signal γ_A itself with a vacuum state γ_{vac} [FFB+14] as described by

$$\gamma_A^{\mathrm{damp}} = (1-\nu_A)\cdot\gamma_A + \nu_A\cdot\gamma_{\mathrm{vac}}, \tag{3.26}$$

where $\nu_A \in [0,1]$ is the reflectivity (the optical loss) parameter of the system. This can, for convenience, be rewritten as

$$\gamma_A^{\mathrm{damp}} = U(\nu_A)\cdot\gamma_A\cdot U^T(\nu_A) + \nu_A\cdot\gamma_{\mathrm{vac}}, \tag{3.27}$$

with

$$U(\nu) = \begin{pmatrix} \sqrt{1-\nu_A} & 0 \\ 0 & \sqrt{1-\nu_A} \end{pmatrix}.$$

We use this equation to describe possible losses in the two independent squeezed vacuum states before they become entangled by the beam splitter. An extension of this equation allows for a description of different losses in Alice's and Bob's sub systems after the beam splitter.

The damping in Alice's subsystem in an entangled bipartite Gaussian state

γ_{AB} can be described by

$$\gamma_{AB}^{\text{damp}} = \left(\begin{array}{cc|cc} \sqrt{1-\nu_A} & 0 & 0 & 0 \\ 0 & \sqrt{1-\nu_A} & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right) \cdot \gamma_{AB} \cdot \left(\begin{array}{cc|cc} \sqrt{1-\nu_A} & 0 & 0 & 0 \\ 0 & \sqrt{1-\nu_A} & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right) + \left(\begin{array}{cc|cc} \nu_A & 0 & 0 & 0 \\ 0 & \nu_A & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right),$$

with $\nu_A \in [0,1]$. The damping in Bob's subsystem is constructed analogously. The resulting state $\gamma_{AB}^{\text{damp}}$ is Gaussian if the initial state γ_{AB} represents a Gaussian state as $\gamma_{AB}^{\text{damp}}$ is in this case a convex combination of two Gaussian covariance matrices. In theory, beam splitters as described in Section 3.4.2 can also be used to describe Gaussian damping of laser beams.

In our analysis we assume fibres to distribute the bipartite state γ_{AB} to Alice and Bob. The states experience a damping of about 0.25 dB/km when propagating in a fibre. The process of coupling a beam into a fibre is described in the next section.

3.4.4. Coupling Process

In this section we discuss the effects that appear when a laser beam is coupled into a fibre [Nol07]. In an ideal setting, coupling leaves the input state unchanged. Under realistic circumstances the coupling process has some imperfections, which can be described by a Gaussian damping of the input state.

Under standard experimental conditions one can, for example, achieve a damping of $\nu_{\text{damp}} \approx 0.025$ for every coupling process [Ebe09]. Note, that if fibres are used to distribute the states, two coupling processes per fibre are necessary. The beam at first has to be coupled in and then out of the fibre for later homodyne detection. In experiment, both operations are realised by the same setup which is illustrated in Figure 3.8.

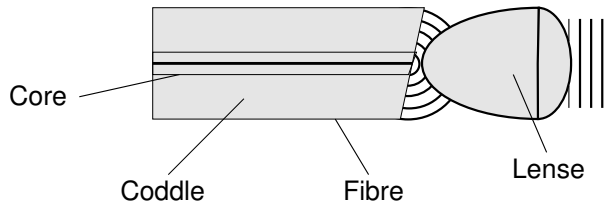

Figure 3.8.: The fibre has a core with diameter $\approx 10\mu$m and refractive index ≈ 1.4 and is coated with a cladding of diameter $\approx 100\mu$m and refractive index ≈ 1.6. The two layers with different refractive indices cause total internal reflection for photons in the core, which usually have a sufficiently small angle of incidence. The end of the fibre is cut at an angle such that reflected photons do not propagate back into the fibre. After transition, the electro magnetic wave is, to good approximation, described by a spherical wave. An aspherical lens transforms this wave back into plane waves. The reversed setup is used when coupling a beam into a fibre.

3.4.5. Balanced Homodyne Detection

In the QKD setup under consideration, balanced homodyne detection is used to measure the Gaussian bipartite subsystems of Alice and Bob [EHS13]. Note that homodyne detection allows for full tomography of Gaussian states in the phase-space which is spanned by the amplitude and phase of the bipartite state, if necessary. Good references for homodyne detection are [WM04, WVO99, Lou97].

The experimental setup of a balanced homodyne detector is depicted in Figure 3.9. The two fields, namely the signal beam which we want to measure and the local oscillator (LO), are superimposed using a 50:50 beam splitter. The LO is an additional relatively strong laser beam with equal wavelength and an arbitrary but constant phase of ϕ. Both fields are assumed to have the same frequency ω_0, thus they can only differ in amplitude and phase.

We start the theoretical analysis of the setup by considering two input fields which are described by the Fock spaces $\mathbb{F}_+^a(\mathcal{H})$ and $\mathbb{F}_+^b(\mathcal{H})$ and two output fields $\mathbb{F}_+^c(\mathcal{H})$ and $\mathbb{F}_+^d(\mathcal{H})$, respectively, as shown in Figure 3.10. We now want to describe the output field operators as a function of the input field operators. For this we use the description of a 50:50 beam splitter in Fock representation [MW95]

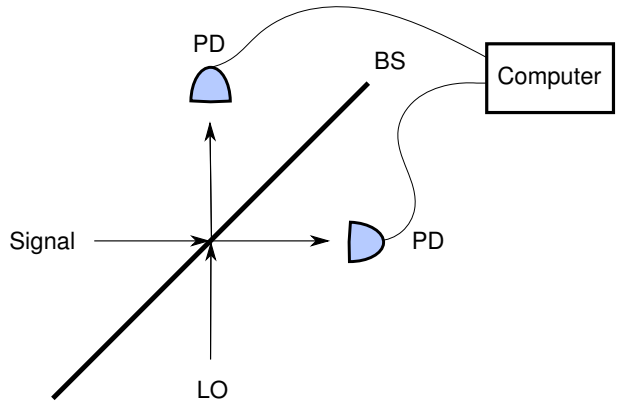

Figure 3.9.: In experiment a homodyne detector is realised by a beam splitter, two photo diodes, an additional laser beam (the local oscillator - LO) and some classical post processing. The outcomes of the photo diodes (PD) are subtracted and post processed on a computer to generate the measurement outcomes. The relative phase $\Delta\phi$ between the LO and the signal is adjusted by a piezo crystal which controls the path length of the LO.

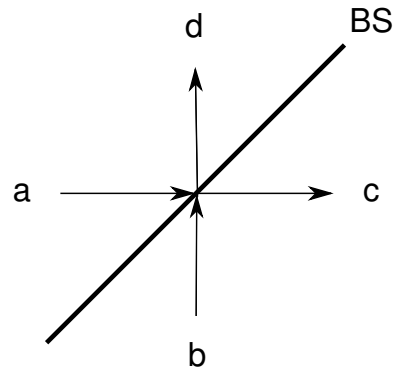

Figure 3.10.: Each of the four fields is identified with a Fock space and the corresponding creation and annihilation operators. The operators $a = a_0 \exp(i\phi_a)$ and $b = b_0 \exp(i\phi_b)$ describe the input and c and d the output fields.

$$\begin{pmatrix} a \\ b \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} c \\ d \end{pmatrix}.$$

which leads to

$$c = \frac{1}{\sqrt{2}}(a-b)$$
$$d = \frac{1}{\sqrt{2}}(a+b).$$

The photo current $I_i \in \{I_1, I_2\}$ as detected by the two photo diodes is proportional to the trace of the corresponding number operators $n_j \in \{n_c, n_d\}$ as explained by

$$I_1 \propto n_c = c^\dagger c = \frac{1}{2} \cdot \left(a^\dagger a - a^\dagger b - b^\dagger a + b^\dagger b\right)$$
$$I_2 \propto n_d = d^\dagger d = \frac{1}{2} \cdot \left(a^\dagger a + a^\dagger b + b^\dagger a + b^\dagger b\right).$$

We now assume that we can linearise the operators describing the input fields to

$$a = (\langle a_0 \rangle + \delta a_0) \cdot \exp\left(i\phi_a\right)$$
$$b = (\langle b_0 \rangle + \delta b_0) \cdot \exp\left(i\phi_b\right)$$

where $\langle a_0 \rangle = \text{const}$ ($\langle b_0 \rangle = \text{const}$) describes the coherent excitations and δa_0 (δb_0) their fluctuations. This assumption is valid if the fluctuations are much smaller than the coherent excitations which justifies dropping higher order corrections and mixed terms like $\delta a_0 \cdot \delta b_0$ in the following. We furthermore choose $\phi_a = 0$ and introduce the relative phase $\Delta\phi = 2 \cdot \phi_b$.

In balanced homodyne detection, one has to subtract the photo currents of the two photo diodes which are described by their number operators

$$\langle \Delta I \rangle \propto \langle n_c - n_d \rangle$$

to measure some quadrature with this setup[6]. One arrives, after some algebra and trigonometric identities, at

$$\Delta I \propto 2 \cdot \left(\langle a_0 \rangle \langle b_0 \rangle \cos\left[\Delta\phi\right] + \langle a_0 \rangle Q_b(-\Delta\phi) + \langle b_0 \rangle Q_a(\Delta\phi)\right) \tag{3.28}$$

[6] In non-balanced homodyne detection, only one photo diode measures the state.

where we introduce the general description of a quadrature operator

$$Q_a\left(\Delta\phi\right) = a_0 \exp\left(-i\Delta\phi\right) + a_0^\dagger \exp\left(i\Delta\phi\right)$$

and Q_b analogously. This general representation includes the cases of the amplitude (phase) quadrature[7] for $\Delta\phi = 0$ ($\Delta\phi = \frac{\pi}{2}$) which have already been introduced in Section 3.2.2.

We now choose the Fock space $\mathbb{F}_+^a(\mathcal{H})$ to represent the signal beam and $\mathbb{F}_+^b(\mathcal{H})$ the LO. This justifies the assumption $\langle b_0\rangle >> \langle a_0\rangle$ and we can write

$$\Delta I \propto 2 \cdot \left(\langle a_0\rangle\langle b_0\rangle \cos\left[\Delta\phi\right] + \langle b_0\rangle Q_a(\Delta\phi)\right), \tag{3.29}$$

where, for a constant $\Delta\phi$, the quadrature operator $Q_a(\Delta\phi)$ makes the only non-trivial contribution.

The minimum variance is described by some specific quadrature operator which is called the squeezed (sqz) quadrature[8]. In experiment the homodyne detection is calibrated by steering the relative phase $\Delta\phi$ such that the outcomes when measuring a squeezed vacuum have the smallest variance $\min_{\Delta\phi}\left\{\mathrm{Var}\left(Q_a(\Delta\phi)\right)\right\}$ for all $\Delta\phi$. Having found the required $\Delta\phi$, it is fixed for the rest of the runtime of the experiment and we say that the phase is locked. All other important quadratures are calibrated relatively to this quadrature. For further details we refer to the Ph.D. thesis of Dr. T. Gehring [Ebe13].

Note that it depends on the definition which quadrature we actually call the amplitude or phase quadrature. If the measured quadratures are orthogonal (but possibly not exactly the amplitude and phase quadrature) and if the initial state is Gaussian, the measurement outcomes always result in a covariance matrix of a Gaussian state which can be checked by the physicality (positivity) criterion (see Equation 3.5) or other Gaussianity tests as described in [BDP+10].

3.4.6. Phase Noise

In the calibration process, for an ideal measurement of the amplitude and the phase quadrature, the homodyne detection of the signal beam has to be perfectly phase locked to the LO for the whole experiment as explained in the

[7] Note that we additionally need the $\Delta\phi = \pi/4$ quadrature measurement for the full reconstruction of the state in terms of the covariance matrix. We explain the usage of this third measurement basis in detail in Section 3.5.

[8] The anti-squeezed (asqz) quadrature is found by a further phase difference of $\Delta\phi = \pi/2$.

former section. In realistic setups this is generally not the case as, for example, pressure or temperature changes could have an effect on the path length of the way of light which disturbs the phase lock. Another source causing local imperfect measurement basis could be the piezo crystal used to steer the relative phase between the signal beam and the LO [EHS13]. In theory we subsume every imperfect measurement basis under the topic phase noise. In this sense, phase noise can be modelled by a probability distribution function F which describes the relative rotations of the measurement quadratures.

We describe phase noise as a time-dependent random rotation in phase-space given by a distribution F, as described in [FHD+06]. As phase noise is not a Gaussian channel, we define the full action on an quantum state ρ by

$$\rho^{\mathrm{PN}} = \int \mathcal{N}(\Delta\sigma, \alpha_t) U(\alpha_t)^\dagger \rho U(\alpha_t) d\alpha_t \tag{3.30}$$

where $U(\alpha_t)$ describes the rotation while $F = \mathcal{N}(\Delta\sigma, \alpha_t)$ is chosen as a Gaussian distribution with mean α_t and variance $\Delta\sigma$.

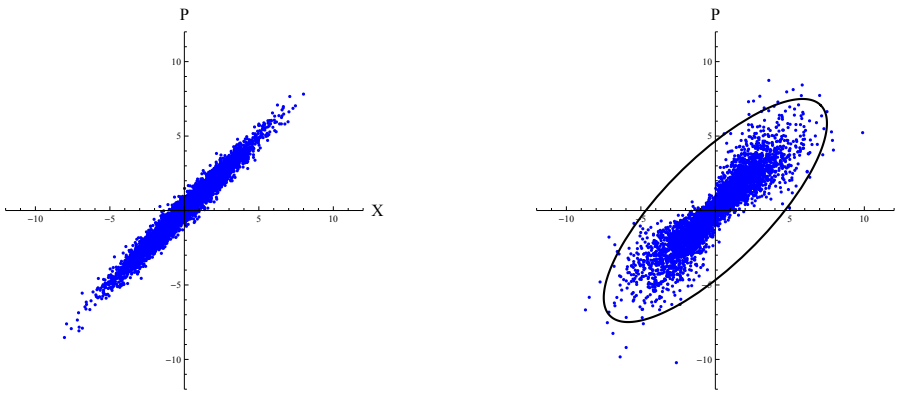

Figure 3.11.: Left: The phase-space of a squeezed state (sqz = 4, asqz = 6). Right: A squeezed state having experienced phase noise where the basis mismatch is weighted by a Gaussian distribution with variance of $\Delta\phi = \frac{\pi}{8}$. The resulting state cannot be fully described by its second moments only. The black ellipse sketches a Gaussian state enveloping the initial Gaussian state with phase-noise.

This equation represents a superposition of Gaussian states with different relative phases which are distributed around $\Delta\phi$ with variance $\Delta\sigma$. One can see

in Figure 3.11 that phase noise is not a Gaussian process. The resulting state cannot be fully described by its second moments [FHD+06, HDF+08], which significantly reduces the Gaussian character of the state.

Nevertheless one can always compute the Wigner function of the Gaussian state which envelopes the initial Gaussian state which experienced phase noise. We write [DiG10]

$$\widetilde{\mathcal{W}}(\alpha) = \int_{-\infty}^{+\infty} \mathcal{W}\left(\gamma_i, \vec{\xi}_0 = \vec{0}, \vec{\xi}(\alpha)\right) \cdot \mathcal{N}(\alpha) d\alpha, \tag{3.31}$$

with

$$\vec{\xi}(\alpha) = \begin{pmatrix} \xi_1 \cos(\alpha) + \xi_2 \sin(\alpha) \\ \xi_2 \cos(\alpha) - \xi_1 \sin(\alpha) \end{pmatrix} = \vec{\xi} \cdot U^T(\alpha).$$

3.4.7. Detection Noise

In the experimental setup we are about to describe, detection noise mostly stems from the electronic dark noise of the classical post processing of the measurement processes of Alice and Bob.

We assume the noise to be i.i.d. and describe it by a Gaussian distribution with variance DN_i, with $i \in \{AB\}$ denoting the laboratories (i.e. the measurement devices) of Alice and Bob. As the measurement outcomes are (by their Wigner functions) described by Gaussian distributions too, we can describe the effect of detection noise as a convolution of two centred Gaussian distributions. This allows us to simply add the variance of detection noise to the covariance matrix γ_{AB} which describes the bipartite Gaussian state as described in [FFB+14]. Hence, we can model the detection noise in the homodyne detectors by

$$\gamma_{AB}^{\mathrm{DN}} = \gamma_{AB} + \left(\begin{array}{cc|cc} \mathrm{DN}_A^X & \widetilde{\mathrm{DN}}_A & 0 & 0 \\ \widetilde{\mathrm{DN}}_A & \mathrm{DN}_A^P & 0 & 0 \\ \hline 0 & 0 & \mathrm{DN}_B^X & \widetilde{\mathrm{DN}}_B \\ 0 & 0 & \widetilde{\mathrm{DN}}_B & \mathrm{DN}_B^P \end{array}\right) \tag{3.32}$$

with $\mathrm{DN}_i \in \mathbb{R}_+$ and $\widetilde{\mathrm{DN}}_i \in \mathbb{R}_+$. The off-diagonal entries of γ_C (see Equation 3.6) are left unchanged as the detection noise of Alice and Bob is not correlated. The off-diagonal elements $\widetilde{\mathrm{DN}}_A$ and $\widetilde{\mathrm{DN}}_B$ are measured by the $Q_{\pi/4}$ quadrature. In further analysis, we take $\mathrm{DN} = \widetilde{\mathrm{DN}}_A = \mathrm{DN}_A^X = \mathrm{DN}_A^P = \widetilde{\mathrm{DN}}_B = \mathrm{DN}_B^X = \mathrm{DN}_B^P$ for simplification as Alice and Bob are assumed to have only one homodyne

detector available each. As detection noise represents classical noise which is added to an initial Gaussian covariance matrix the resulting state is again a Gaussian state.

3.5. Full Tomography

We need a full tomography of the bipartite Gaussian state in terms of the covariance matrix to characterise the Gaussian bipartite state of Alice and Bob. Local displacement of the beams is neglected, and, hence, the state can be fully described by its covariance matrix γ_{AB}. As we are about to perform a reconstruction of a covariance matrix using finitely many measurement outcomes, we need a confidence set $\mathcal{C}_{\varepsilon_S}$ to quantify the quality of the reconstruction to fulfill the requirements of composable security as described in Section 4.2. The method for the full tomography which we describe here has been published in [Sam12] and [DHF+07] but our representation is, to the best knowledge of the authors, novel.

We can fully reconstruct covariance matrices of Gaussian bipartite states by assuming a perfectly orthogonal measurement basis $\{X = Q_0, P = Q_{\pi/2}\}$ together with $\{Q_{\pi/4}, Q_{3\pi/4}\}$ of Alice and Bob. In what follows we have to keep in mind, that the measurement basis X and P might not be perfectly matched, which can be checked by measuring the appropriate $Q_{\pi/4}$ quadrature. Nevertheless, experimental results show, that the orthogonality of the two basis is chosen almost perfectly as described in [HES+12]. One covariance matrix is a function of a set of two orthogonal measurement bases. Since we have four different measurement basis (namely $\{X = Q_0, P = Q_{\pi/2}\}$ and $\{Q_{\pi/4}, Q_{3\pi/4}\}$) we have in principle two covariance matrices. In the following we describe how we reconstruct the bipartite Gaussian state from two covariance matrices which are both partly reconstructed using the Wishart distribution [JW07].

The confidence set $\mathcal{C}_{\varepsilon_S}$ is defined such that the sample covariance matrix lies within $\mathcal{C}_{\varepsilon_S}$ with probability $1-\varepsilon_S$. We assume N_{pe} measurements M_{AB} with $N_{\text{pe}} = |M_{AB}|$ available for the estimation of the covariance matrix γ_{AB}. The different fractions which amount to the entries of the covariance matrix are given at the end of this section. First, we assume that Alice and Bob measured the X, $Q_{\pi/4}$ and P quadrature chosen i.i.d. with the statistical weights q_X, $q_{\pi/4}$ and q_P for generality.

All N_{pe} measurement outcomes are used to reconstruct the covariance matrix thereby following the protocol described in [DHF+07]:

1. Alice and Bob perform simultaneous measurements of the amplitude quadrature.
2. Alice and Bob perform simultaneous measurements of the phase quadrature.
3. Alice measures the amplitude quadrature and Bob measures the phase quadrature.
4. Alice measures the phase quadrature and Bob measures the amplitude quadrature.
5. Alice and Bob both measure simultaneously the $Q_{\pi/4}$ quadrature.

First we focus on the covariance matrix γ_{AB} described by $\{X = Q_0, P = Q_{\pi/2}\}$. We assume the bipartite state to be Gaussian and describe it by the covariance γ_{AB} matrix, which is in general

$$\gamma_{AB} = \left(\begin{array}{cc|cc} \gamma_{1,1} & \gamma_{1,2} & \gamma_{1,3} & \gamma_{1,4} \\ \gamma_{1,2} & \gamma_{2,2} & \gamma_{2,3} & \gamma_{2,4} \\ \hline \gamma_{1,3} & \gamma_{2,3} & \gamma_{3,3} & \gamma_{3,4} \\ \gamma_{1,4} & \gamma_{2,4} & \gamma_{3,4} & \gamma_{4,4} \end{array}\right) = \left(\begin{array}{cc} \gamma_A & \gamma_C \\ \gamma_C^T & \gamma_B \end{array}\right).$$

The entries of the covariance matrix are estimated as follows:

The variance is defined as

$$\gamma_{i,i} = \sqrt{\frac{1}{N_i} \cdot \sum_{k=1}^{k=N_i} x_k^2} \tag{3.33}$$

with $x_k \in M_{i,i} \subset M_{AB}$ and $N_i = |M_{i,i}|$ for $i \in \{1,2,3,4\}$. We use $M_{i,i}$ to compute the entries $\gamma_{1,1}$, $\gamma_{2,2}$, $\gamma_{3,3}$ and $\gamma_{4,4}$ which are the diagonal entries of the sub-matrices γ_A and γ_B.

The covariance is defined as

$$\gamma_{i,j} = \sqrt{\frac{1}{N_{i,j}} \cdot \sum_{k=1}^{k=N_{i,j}} x_{i,k} x_{j,k}} \quad \forall i > j \in \{1,2,3,4\} \tag{3.34}$$

with $\{x_{i,k}, x_{j,k}\} \in M_{i,j} \subset M_{AB}$ and $N_{i,j} = |M_{i,j}|$ for $i, j \in \{1,2,3,4\}$ with $i \neq j$. We use the $M_{i,j}$ to compute the entries $\gamma_{1,3}$, $\gamma_{1,4}$, $\gamma_{2,3}$ and $\gamma_{2,4}$, giving us estimates of all the entries of γ_C.

Note that we cannot estimate the entries $\gamma_{1,2}$ and $\gamma_{3,4}$ with the amplitude and phase quadrature as simultaneous measurements of X and P are not compatible with homodyne detection and simultaneous exact measurements of X and P are not even compatible with quantum mechanics. We introduce a second covariance matrix $\widetilde{\gamma}_{AB}$ which is described by the measurement operators $Q_{\pi/4}$ and $Q_{3\pi/4}$. We focus on the sub-blocks of Alice and Bob and write

$$\begin{aligned}\widetilde{\gamma}_i &= U_{\Delta\phi}\gamma_i U_{\Delta\phi}^{\dagger} \\ &= \begin{pmatrix} \widetilde{\gamma}_{1,1} & \widetilde{\gamma}_{1,2} \\ \widetilde{\gamma}_{1,2} & \widetilde{\gamma}_{2,2} \end{pmatrix} \\ &= \begin{pmatrix} \frac{\gamma_{1,1}+\gamma_{2,2}}{2} - \gamma_{1,2} & \frac{\gamma_{1,1}-\gamma_{2,2}}{2} \\ \frac{\gamma_{1,1}-\gamma_{2,2}}{2} & \frac{\gamma_{1,1}+\gamma_{2,2}}{2} + \gamma_{1,2} \end{pmatrix}\end{aligned}$$

where $U_{\Delta\phi}$ is a rotation matrix in $\mathbb{R}^2$ with $\Delta\phi = \pi/4$. This can be rewritten to

$$\gamma_{1,2} = \frac{\gamma_{1,1}+\gamma_{2,2}}{2} - \widetilde{\gamma}_{1,1} \tag{3.35}$$

which allows us to estimate the off-diagonal entry $\gamma_{1,2}$ of Alice from $\widetilde{\gamma}_{1,1}$. A similar analysis allows the estimation of Bob's γ_B off-diagonal entry by

$$\gamma_{3,4} = \frac{\gamma_{3,3}+\gamma_{4,4}}{2} - \widetilde{\gamma}_{3,3}. \tag{3.36}$$

As $\gamma_{1,1}$ and $\gamma_{2,2}$ have already been reconstructed, the only additional basis to be measured is $Q_{\pi/4}$. We can thus deduce the off-diagonal entries for Alice and Bob in γ_{AB} by following the protocol described in [DHF+07] by using two covariance matrices for two different sets of measurement operators, $\{X = Q_0, P = Q_{\pi/2}\}$ and $\{Q_{\pi/4}, Q_{3\pi/4}\}$. We only need the outcomes of $\widetilde{\gamma}_{1,1}$ and $\widetilde{\gamma}_{3,3}$ to reconstruct the entries $\gamma_{1,2}$ and $\gamma_{3,4}$.

We can now write the full tomography of the state as

$$\gamma_{AB} = \left(\begin{array}{cc|cc} \gamma_{1,1} & \frac{\gamma_{1,1}+\gamma_{2,2}}{2} - \widetilde{\gamma}_{1,1} & \gamma_{1,3} & \gamma_{1,4} \\ \frac{\gamma_{1,1}+\gamma_{2,2}}{2} - \widetilde{\gamma}_{1,1} & \gamma_{2,2} & \gamma_{2,3} & \gamma_{2,4} \\ \hline \gamma_{1,3} & \gamma_{2,3} & \gamma_{3,3} & \frac{\gamma_{3,3}+\gamma_{4,4}}{2} - \widetilde{\gamma}_{3,3} \\ \gamma_{1,4} & \gamma_{2,4} & \frac{\gamma_{3,3}+\gamma_{4,4}}{2} - \widetilde{\gamma}_{3,3} & \gamma_{4,4} \end{array}\right).$$

After having fully reconstructed the Gaussian bipartite state, we ask for the confidence interval C_{ε_S} and a value ε_S describing the probability of the real state lying within this interval. We use the Wishart distribution for the two covariance matrices to construct the confidence set. First we focus on the outcomes of the amplitude X and phase P measurements of Alice and Bob to estimate the confidence interval of γ_{AB}. Next we investigate the confidence interval of the second covariance matrix $\widetilde{\gamma}_{AB}$. Finally we ask for the confidence set when combining these two covariance matrices.

The distribution of a single measured covariance matrix γ_{AB} is estimated by

$$\overline{\gamma}_{AB} \propto \mathrm{W}\big(\gamma_{AB}, N_{\mathrm{pe}}-1\big)/N_{\mathrm{pe}},$$

where N_{pe} is the number of measurements used to reconstruct the covariance matrix at hand. For this estimation we use the Wishart distribution W which delivers a confidence set of the different parameters by computing

$$\sigma_{i,j} = \sqrt{\frac{\gamma_{i,j}^2 + \gamma_{i,i}\cdot\gamma_{j,j}}{N_{i,j}}}, \tag{3.37}$$

where $N_{i,j} < N_{\mathrm{pe}}$ is the number of measurement outcomes available for the corresponding entry as described above. From this we can describe a confidence set as

$$C_{\varepsilon_S} = \big\{\gamma_{i,j} - \Delta\gamma_{i,j}, \gamma_{i,j}, \gamma_{i,j} + \Delta\gamma_{i,j}\big\}$$

with $\Delta\gamma_{i,j} = z_{\mathrm{pe}}\cdot\sigma_{i,j}$, where z_{pe} is chosen such that it fulfils

$$1 - \mathrm{Erf}\left(\frac{z_{\mathrm{pe}}}{\sqrt{2}}\right) \leq \varepsilon_{\mathrm{pe}},$$

with

$$\mathrm{Erf}(x) = \frac{2}{\pi}\cdot\int_0^x \exp(-t^2)\,dt.$$

We now focus on the edges of the confidence intervals of the entries and write

$$\overline{\gamma}_{AB} = \left(\begin{array}{cc|cc} \gamma_{1,1}\pm\Delta\gamma_{1,1} & \gamma_{1,2}\pm\Delta\gamma_{1,2} & \gamma_{1,3}\pm\Delta\gamma_{1,3} & \gamma_{1,4}\pm\Delta\gamma_{1,4} \\ \gamma_{1,2}\pm\Delta\gamma_{1,2} & \gamma_{2,2}\pm\Delta\gamma_{2,2} & \gamma_{2,3}\pm\Delta\gamma_{2,3} & \gamma_{2,4}\pm\Delta\gamma_{2,4} \\ \hline \gamma_{1,3}\pm\Delta\gamma_{1,3} & \gamma_{2,3}\pm\Delta\gamma_{2,3} & \gamma_{3,3}\pm\Delta\gamma_{3,3} & \gamma_{3,4}\pm\Delta\gamma_{3,4} \\ \gamma_{1,4}\pm\Delta\gamma_{1,4} & \gamma_{2,4}\pm\Delta\gamma_{2,4} & \gamma_{3,4}\pm\Delta\gamma_{3,4} & \gamma_{4,4}\pm\Delta\gamma_{4,4} \end{array}\right).$$

The only confidence intervals that cannot be directly computed from measurement outcomes of the amplitude and phase quadrature are the off-diagonal elements of γ_A and γ_B. We write the confidence intervals leading to $\gamma_{1,2}$ and $\gamma_{3,4}$ as functions of the confidence sets of the covariance matrices $\widetilde{\gamma}_{AB}$ and γ_{AB}. For this task we look at the confidence intervals of the original measurements and use the standard Gaussian law of error propagation to compute

$$\begin{aligned}\Delta\gamma_{1,2} &= \sum_{i=1}^{3}\left|\frac{\mathrm{d}\left(\frac{\gamma_{1,1}+\gamma_{2,2}}{2}-\widetilde{\gamma}_{1,1}\right)}{\mathrm{d}x_i}\right|\cdot\Delta x_i \\ &= \frac{\Delta\gamma_{1,1}+\Delta\gamma_{2,2}}{2}+\Delta\widetilde{\gamma}_{1,1} \\ &= z_{\mathrm{pe}}\cdot\left[\frac{\sigma_{1,1}+\sigma_{2,2}}{2}+\widetilde{\sigma}_{1,1}\right],\end{aligned}$$

where $x_i \in \left\{\gamma_{1,1},\gamma_{2,2},\widetilde{\gamma}_{1,1}\right\}$ and Δx_i is the uncertainty of the corresponding entry. $\Delta\gamma_{3,4}$ is computed analogously. Under these assumptions ε_S is maintained while the confidence interval is recomputed.

For QKD tasks we need the covariance matrix in the confidence set with the worst correlations, which is in this sense

$$\overline{\gamma_{AB}} = \left(\begin{array}{cc|cc} \gamma_{1,1} & \gamma_{1,2} & \gamma_{1,3} & \gamma_{1,4} \\ \gamma_{1,2} & \gamma_{2,2} & \gamma_{2,3} & \gamma_{2,4} \\ \hline \gamma_{1,3} & \gamma_{2,3} & \gamma_{3,3} & \gamma_{3,4} \\ \gamma_{1,4} & \gamma_{2,4} & \gamma_{3,4} & \gamma_{4,4} \end{array}\right) + \left(\begin{array}{cc|cc} \Delta\gamma_{1,1} & \frac{\Delta\gamma_{1,1}+\Delta\gamma_{2,2}+2\Delta\widetilde{\gamma}_{1,1}}{2} & -\mathrm{Sgn}_{\gamma_{1,3}}\Delta\gamma_{1,3} & -\mathrm{Sgn}_{\gamma_{1,4}}\Delta\gamma_{1,4} \\ \frac{\Delta\gamma_{1,1}+\Delta\gamma_{2,2}+2\Delta\widetilde{\gamma}_{1,1}}{2} & \Delta\gamma_{2,2} & -\mathrm{Sgn}_{\gamma_{2,3}}\Delta\gamma_{2,3} & -\mathrm{Sgn}_{\gamma_{2,4}}\Delta\gamma_{2,4} \\ \hline -\mathrm{Sgn}_{\gamma_{1,3}}\Delta\gamma_{1,3} & -\mathrm{Sgn}_{\gamma_{2,3}}\Delta\gamma_{2,3} & \Delta\gamma_{3,3} & \frac{\Delta\gamma_{3,3}+\Delta\gamma_{4,4}+2\Delta\widetilde{\gamma}_{3,3}}{2} \\ -\mathrm{Sgn}_{\gamma_{1,4}}\Delta\gamma_{1,4} & -\mathrm{Sgn}_{\gamma_{2,4}}\Delta\gamma_{2,4} & \frac{\Delta\gamma_{3,3}+\Delta\gamma_{4,4}+2\Delta\widetilde{\gamma}_{3,3}}{2} & \Delta\gamma_{4,4} \end{array}\right).$$

The choice of the direction within the confidence set resulting in the worst covariance matrix depends heavily on the choice of the signs of the entries of the correction matrix. We chose them such that the entries of γ_A and γ_B sum up, leading to increasing variance of the measurement outcomes, whereas the correlations γ_C decrease. This special choice of the signs of the covariance matrix was verified numerically. Note that one always has to check, by the positivity criterion (see Equation 3.5), that the resulting state is still Gaussian.

4. Preliminaries: Continuous Variable Quantum Key Distribution

4.1. Overview

We describe in this chapter the quantum key distribution in general and its application to the setup which is introduced in Section 3.3.

We start in Section 4.2 by defining the different notions of security which are commonly discussed in the field. We then detail the specific CV-QKD protocol and the key generation which we use for the rest of this thesis in the Sections 4.3 and 4.4. Afterwards we explain the CV-QKD protocols providing security against collective and coherent attacks in the Sections 4.5 and 4.6. We close this chapter with explaining common classical reconciliation protocols and their connection to QKD in Section 4.7.

The current chapter is explicitly meant as introduction unless otherwise noted.

4.2. Security Definitions

As the distribution of the secure key between Alice and Bob is a sub-protocol of a complete cryptographic task (secret communication) itself, we have to ensure that the key generated within it remains secret when used in other cryptographic sub-protocols. Such as the encoding and decoding of the message which is to be kept secret by using the generated secure key as a one-time pad. This can be guaranteed by the composable security definitions from [Can01] and [Ren05]. Afterwards we discuss the classes defining Eve's attacks at the end of this section.

4.2.1. Composable Security

In the following, we denote by K_A^{sec} and K_B^{sec} the random variables associated with the secure keys held by Alice and Bob at the very end of the QKD protocol. The details of the setup from which the random variables (measurement outcomes) are generated is widely discussed in the Section 3.3. The definitions of composable security are:

Robustness:
A protocol is robust, if it does not abort with high probability when no eavesdropper is present. Robustness ensures, that the protocol has at least some resilience against additional noise thereby still producing a positive but possibly smaller secure key. Only robust protocols are experimentally relevant.

Correctness:
We call a protocol ε_C-correct if

$$\mathcal{P}\left[K_A^{\text{sec}} \neq K_B^{\text{sec}}\right] \leq \varepsilon_C \,. \tag{4.1}$$

For example, if $\varepsilon_C \ll 1$, Alice's and Bob's secure keys agree with high probability.

In every non-ideal setting noise is present, resulting in disagreements between Alice's and Bob's raw keys. A classical reconciliation step is needed to equalise their erroneous raw keys being followed by a classical confirmation step which checks the resulting keys for actual agreement. A naive confirmation step would simply compare the whole corrected raw keys of Alice and Bob, which would result in no measurement samples being left for key generation. More advanced confirmation procedures compute a checksum using a hash function, thereby disclosing only ≈ 100 bits [TLGR14]. The number of disclosed bits during the confirmation is to be considered in the privacy amplification and computed from the the correctness parameter ε_C by $\log_2[1/\varepsilon_C]$. But the price is that we cannot be perfectly sure whether the keys of Alice and Bob are really equivalent.

Secrecy:
Let $\omega_{K_{\text{sec}},E}$ describe the classical-quantum state of Alice's and Bob's final keys K_{sec} and a possible eavesdropper E conditioned on the case that the protocol passes. Such a state can always be written as

$$\omega_{K_{\text{sec}},E} = \sum_{k_{AB} \in K_{\text{sec}}} \mathcal{P}(k_{AB}) \cdot |k_{AB}\rangle\langle k_{AB}| \otimes \omega_E^{k_{AB}}, \tag{4.2}$$

where $\mathcal{P}(k_{AB})$ is the probability distribution of the secure key representing the rule by which the key is generated in a specific experiment. A protocol is ε_S-secure, if for any eavesdropper E,

$$\frac{\mathcal{P}_{\text{pass}}}{2}\|\omega_{K_{\text{sec}}E} - \tau_{K_{\text{sec}}} \otimes \omega_E\|_1 \leq \varepsilon_S \tag{4.3}$$

holds. Here, $\|\cdot\|_1$ is the trace norm, $\tau_{K_{\text{sec}}}$ is the uniform distribution over K_{sec}, ω_E is the reduced state of $\omega_{K_{\text{sec}}E}$ and $1-\mathcal{P}_{\text{pass}}$ is the probability that the protocol aborts. This equation combines the probability that the QKD protocol aborts $1-\mathcal{P}_{\text{pass}}$ with the secrecy of the protocol ε_S.

Security:
A protocol is ε-secure if it is ε_C-correct and ε_S-secret with $\varepsilon_C + \varepsilon_S \leq \varepsilon$.

We refer to [MQR09] for a more detailed discussion on the above security conditions.

4.2.2. Security Classes

The security analysis of QKD protocols rely on three commonly considered classes of attacks of Eve. Eve has unlimited classical computational power in all cases but she has no access to the laboratories of Alice and Bob. She is additionally allowed to listen to the authenticated classical channel which is needed for the classical post processing. The security classes differ in how Eve is allowed to attack the quantum channel which is used during the QKD protocol. Note that we omit device independent security [Hän10] in this presentation. In ascending order of Eve's attack strength the security classes are [SBPC$^+$09]:

Individual attacks:
Eve does not possess a quantum memory and measures each signal individually and instantaneously. In photonic QKD such an attack is for example realised by a beam splitter coupling out a certain portion of the signal beam from which certain properties of the state are measured by Eve.

Collective attacks:
Eve has a quantum memory and interacts with all signals independently and identically after completion of the CV-QKD task, i.e., her attacks are permutation invariant. This simplifies the security analysis as Eve's attack can be described by a tensor product form. Assuming n synchronised key gener-

ation measurement results[1] of Alice and Bob with outcomes x_A and x_B we can rewrite $\omega_{x_A^n,x_B^n,E^n} = \omega_{x_A,x_B,E}^{\otimes n}$. In this sense, collective attacks are a weaker assumption on the attacks of Eve than individual attacks and provide thus a higher security.

Coherent attacks:
Eve has a quantum memory and all attacks which can be described by quantum mechanics are allowed. As most general attacks are allowed, the security analysis is often much more complicated than in the case of collective or even individual attacks as the $\omega_{x_A^n,x_B^n,E^n}$ can no longer be assumed to have tensor product form.

In this thesis we analyse the collective and coherent security of different setups and further guarantee the composability with other cryptographic subprotocols.

4.3. Continuous Variable Quantum Key Distribution Protocol

In bipartite secret communication tasks two participants intend to share a message such that it is kept secret to the rest of the world (i.e. a potential eavesdropper - Eve). We use CV-QKD to distribute the secure key which is later used to encode and decode the message. Let us describe the sub-protocols of one such cryptographic task (secret communication) in wider detail in this section.

We assume that the source of the quantum states is placed in Alice's lab and is trusted. Note that in direct reconciliation Alice's raw key is assumed to be correct and Bob's raw key is treated as being erroneous. Bob has thus to reconcile his key using appropriate information from Alice. In reverse reconciliation the setting is simply interchanged. The choice whether to use direct or reverse reconciliation has a great effect on the secure key rate of the setup. For example, as Alice holds the source and Bob is remote, her data is less affected by loss than Bob's measurements. It follows directly, that Eve's guess about Alice's measurement outcomes is better then her guess about Bob's outcomes. Hence, one can expect higher key rates when assuming reverse reconciliation as we will show later.

[1] We call the synchronised and correlated outcomes of Alice and Bob when measuring the same basis a *sample*.

We focus here especially on the CV-QKD protocols proposed by Dr. F. Furrer *et al.* [FFB+14] which allow only direct reconciliation for the protocol offering security against coherent attacks[2] and both reconciliation methods for the protocol secure against collective attacks.

We focus in the following on the amplitude X and phase P quadrature. If analysing the protocol providing security against collective attacks one has to additionally consider the $Q_{\pi/4}$ quadrature for parameter estimation as described in Section 3.5 because the protocol parameter is in this case the full covariance matrix γ_{AB} (see Section 4.5). In contrary, the protocol parameter d_0 of the CV-QKD scheme providing security against coherent attacks is sufficiently described by the amplitude and phase quadrature alone (see Section 4.6).

4.3.1. General Stages

Every secret communication based on QKD is naturally parted into four stages of general sub-protocols [SBPC+09]:

I: Authentication
First of all, Alice and Bob identify themselves by some pre-shared information. This process is called the authentication of the classical channel which is needed in the following sub-protocols.

II: Quantum stage
Alice and Bob perform $|M_{AB}|$ synchronised measurements $\{x_A, x_B\}_i \in M_{AB}$ of their bipartite state which is used to distribute the raw keys. The potential secure key k_{pot} rate is computed from a protocol parameter which is estimated during the parameter estimation. The outcomes of this stage are the raw keys K_A and K_B of Alice and Bob together with the potential secure key rate k_{pot} of the setup.

III: Classical post processing
The classical reconciliation sub-protocol detects and corrects possible errors in the raw keys of Alice and Bob. Another classical post processing sub-protocol is privacy amplification where the common raw keys of Alice and Bob are, using some hash function, folded to their secure length k_{sec}. The

[2] It has been recently shown in [Fur14], that the CV-QKD protocol providing security against coherent attacks is also secure under reverse reconciliation. Note that we do not analyse this protocol in this thesis.

outcome of this stage is the secure key K_{sec} of Alice and Bob, the one-time pad.

IV: Encryption
In a this stage, the message T which Alice and Bob want to secretly share is encoded with the common secure key (one-time pad) K_{sec} and sent over a classical channel (possibly the internet) to Bob who can decode it. This step is independent of the actual generation of the secure key.

Note, that a typical QKD protocol assumes an authenticated classical channel (I) and focuses then mainly on the quantum stage (II). The classical post processing (III) is needed to correct the errors in the raw key and to shrink the raw key to its secure length. A QKD protocol is successful, if it provides a secure key which can be used in secret communication tasks. The encryption (IV) is in this sense not part of the QKD protocol but part of the whole secret communication task.

4.3.2. Detailed Steps

We now describe the four general stages presented in the former section in more detail and relate it to the setup which is presented in Chapter 3. Note, that the order of the different steps of the secret communication might vary if needed.

Step 0: Authentication
The two involved participants have to identify themselves for two reasons. Firstly, if Alice and Bob did not do so, a possible eavesdropper could pretend to be either Alice or Bob. Note at this point that Eve is allowed to listen to the classical channel. All the information which is send over the classical channel is hence assumed to be disclosed to Eve. Secondly, they might be using a multi-user QKD network [FFW11] where several parties can communicate. Alice identifies herself to Bob by sending a specific pre-shared secure hash to all the parties in the network over a classical channel. This is the initial procedure of every QKD protocol and has no influence on the security after it is successfully completed. Additionally, every classical sub-protocol needs an authentication procedure, as explained in [PAL+12].

Step 1: Quantum stage: Parameter agreement
At first Alice and Bob have to publicly agree on the security level of the QKD protocol. After this, they can continue by communicating the basic parameters of the specific protocol they have chosen to execute. In practice, this

is an optimisation procedure based on the knowledge about the available source, detectors and the channel. One should note that this optimisation might depend on further restrictions, like the availability of efficient reconciliation codes. Still, a non-optimal choice of parameters will only lead to a reduced key rate (possibly zero) and will not compromise the security of the setup. Note that the protocol parameter needed for the computation of the secure key rate is estimated in the parameter estimation later. Finally Alice and Bob have to agree on a number of signals $|M_{AB}|$ to be shared. They then know that after a non-aborted run of the setup, the extracted key will have the security level desired.

Step 2: Quantum stage: Preparation and measurement
Alice prepares an entangled bipartite Gaussian state, keeps one subsystem and sends the other to Bob. Both parties perform synchronised homodyne measurements in the amplitude X (phase P) quadrature[3] which are individually chosen at random with weight q_X ($q_P = 1 - q_X$). The outcome of each measurement is a real number, discretised with the precision of the measurement device. This process is repeated until $|M_{AB}|$ tuples are recorded, forming a string $M_{AB} = M_A \times M_B = \left\{x_{A,i}, x_{B,i}\right\}^{|M_{AB}|}$. Alice's and Bob's measurements are synchronised by a fixed common starting point in time (in the following chosen to be $T_0 = 0$) and the sequence of time bins $\Delta T_{\text{sync}} = \max\left\{T_S, T_M\right\}$ where T_S is the time needed for switching the basis and T_M is the time needed for a measurement.

Step 3: Quantum stage: Post selection (optional, if allowed)
In this step certain elements of the key generation alphabet are discarded. This can be realised by assuming them to stem from a hypothetical measurement basis E. This additional measurement basis has then to be accounted for in the sifting process where all such measurement tuples are additionally discarded from key generation. This can, for example, be used to reduce the error rate of the raw keys of Alice and Bob. Note that it depends on the QKD protocol which is used whether post selection is permitted or not as we will discuss later.

Step 4: Quantum stage: Protocol parameter estimation
Alice and Bob choose a common subset from M_{AB} of size N_{pe}, which they reveal. The rules by which the N_{pe} measurement tuples are chosen, are defined

[3] Note that additional basis (like, for example, the $Q_{\pi/4}$ quadrature) might be necessary for the purpose of parameter estimation. We focus in this description mainly on the quadratures which are used in the key generation to simplify the presentation. We discuss the case of additional basis later.

by the parameter estimation of the specific CV-QKD protocol. With this information they perform the estimation of the protocol parameter needed for the computation of the secure key rate. Discarding the revealed tuples from M_{AB} leaves some $|M_{AB}| - N_{\text{pe}}$ measurement outcomes $\widetilde{M}_{AB}$.

Step 5: Quantum stage: Sifting
Alice and Bob perform sifting, i.e. they communicate for every tuple in which basis they measured. Tuples including the additional measurement basis E and those measured with a different combination of quadratures (X, P) are discarded from $\widetilde{M}_{AB}$ leaving Alice and Bob with a string of correlated measurement samples K_{AB} of length $N_{\text{key}} = |K_{AB}|$ which is used for the generation of the raw key. The number of signals discarded by sifting is denoted by N_{sift}. Note that we refer the outcome tuples of such a synchronous and correlated measurement as sample[4].

Step 6: Quantum stage: Secure key rate
In this step Alice and Bob compute the secure key rate k_{sec} using the outcome of the parameter estimation sub-protocol. Note that the computation of the secure key rate already assumes exact pre-knowledge about the efficiency of the reconciliation method used to correct the errors in Alice's and Bob's raw keys by $k_{\text{sec}} = k_{\text{pot}} - \ell_{\text{EC}}/N_{key}$. It is sometimes more convenient to use the notion of the potential secure key rate k_{pot} as we will show in Chapter 6. The potential secure key rate per shot is the amount of secure information before subtracting the information disclosed during the reconciliation sub-protocol ℓ_{EC}. The reason is, that in a experimental realisation of a CV-QKD setup at this point Alice and Bob have no exact prior knowledge about the information which is disclosed during the reconciliation of their raw keys.

Step 7: Quantum stage: Partitioning
Alice and Bob group their N_{key} raw key samples K_{AB} into bins. The results are Alice's and Bob's partitioned raw keys $\text{Bin}[K_A]$ ($\text{Bin}[K_B]$) consisting of elements of the key generation alphabet χ_{KG}. We explain this process in detail in Section 4.4. Note that their raw keys are in a non-ideal setup in general not equal: $\text{Bin}[K_A] \neq \text{Bin}[K_B]$.

Step 8: Quantum stage: Bit Strings
Each element of the key generation alphabet χ_{KG} is assigned to a unique sequence of bits (bit sequence) such that, after the conversion, Alice (Bob) has

[4] Only simultaneous and synchronised measurements of Alice and Bob in either the amplitude or phase quadrature together can be used for the generation of the raw key. The tuples of the remaining combinations of the quadratures can be used for parameter estimation.

a bit string Bit[Bin[K_A]] (Bit[Bin[K_B]]) representing his correlated raw key on the level of bits.

Step 9: Classical post processing: Reconciliation
Alice and Bob perform reconciliation (error correction) to correct the differences between their raw keys. After this process they share with high probability $1-\varepsilon_C$ the same raw keys Bin[K_A] = Bin[K_B]. The reconciliation can either operate on Bin[K_{AB}] or Bit[Bin[K_{AB}]]. During reconciliation Alice and Bob disclose an amount ℓ_{EC} of potential secure key. With this knowledge Alice and Bob can finally compute the extractable secure key rate per shot $k_{\mathrm{sec}} = k_{\mathrm{pot}} - \ell_{\mathrm{EC}}/N_{key}$. If $k_{\mathrm{sec}} > 0$ they continue with the cryptographic protocol. The outcome of this sub-protocol is the corrected secure key Bin[K_{AB}] of Alice and Bob with Bin[K_A] = Bin[K_B].

Step 10: Classical post processing: Confirmation
This sub-protocol checks for the success of the reconciliation in the former step. Alice computes a hash of her raw key which can be described by approximately 100 bits and sends it, together with the hash function she chose, to Bob via the authenticated classical channel [TLGR14]. Bob receives the information and does the same computation with the same hash function. If he gets the same results the protocol is continued.

Step 11: Classical post processing: Privacy amplification
In the privacy amplification step both parties apply two-universal hash functions to fold the key to its secure length of k_{sec} bits per shot [BBCM95]. The output of this procedure is Bit$\big[$Bin$\big[K_{\mathrm{sec}}\big]\big]$, the secure key distributed by the quantum channel.

Formally we can define a hash function f as a mapping of the corrected raw keys Bit[Bin[K_{AB}]] to the secure key Bit$\big[$Bin$\big[K_{\mathrm{sec}}\big]\big]$. Note that the sizes of the different keys are $|\mathrm{Bit}[\mathrm{Bin}[K_{AB}]]| \geq |\mathrm{Bit}\big[\mathrm{Bin}\big[K_{\mathrm{sec}}\big]\big]|$. We now consider a class $\{f\}$ of hash functions. We call such a class two-universal if

$$\mathcal{P}\big(f(x)=f(y)\big)=\frac{1}{|\mathrm{Bit}\big[\mathrm{Bin}\big[K_{\mathrm{sec}}\big]\big]|} \quad \forall_{x,y\in \mathrm{Bit}[\mathrm{Bin}[K_{AB}]], x\neq y} \quad \forall_f \tag{4.4}$$

where f is randomly drawn from $\{f\}$ [Sti94]. The leftover hash lemma [BBR88] explains why two-universal hash functions can be used for the purpose of privacy amplification.

Step 12: Encryption: Message encoding

In this step Alice encodes the secret text T by using the generated secure key $\mathrm{Bit}\left[\mathrm{Bin}\left[K_{\mathrm{sec}}\right]\right]$ as a one-time pad. The simple bitwise XOR operation already provides full security. The encoded message is then sent to Bob via the authenticated classical channel. A one-time pad has the same length as the message to be encoded and must only be used once [Sin99]. The security of the key implies the security of the encoded message T. A part of the secure key should be saved for later authentication purposes when starting the protocol again.

Step 13: Encryption: Message decoding
Bob receives the encoded message T sent by Alice and decodes it by using the secure key $\mathrm{Bit}\left[\mathrm{Bin}\left[K_{\mathrm{sec}}\right]\right]$ he shares with Alice. As long as the message initially encoded by Alice and sent over the authenticated classical channel is known only to her, the message is kept secret up to the security assumption on which Alice and Bob had agreed on in step 1.

We restrict ourself in the following to the Quantum-stage and the classical post processing. We discuss new CV-QKD security proofs in Chapter 5 and describe a new reconciliation scheme in Chapter 6.

4.4. Key Generation

In this section we explain the key generation of the CV-QKD protocols [FFB+14] we discuss in this thesis in detail (see Sections 4.5 and 4.6). Although the parameter estimation is different for the protocols secure against collective or coherent attacks, the key generation protocol is the same.

We start with Alice's and Bob's raw keys $\mathrm{Bin}[K_{AB}]$ of length $N_{\mathrm{key}} = |\mathrm{Bin}[K_{AB}]|$ after sifting as described in Section 4.3.2. For simplicity we focus on one sub-phase-space spanned by, for example, the amplitude quadrature X. The phase quadrature P is treated analogously.

The key $\mathrm{Bin}[K_{AB}]$ is generated from some equidistant grid which is to be properly laid in the phase sub-space where each partition is uniquely identified with an element of the key generation alphabet χ_{KG}, which has size $|\chi_{\mathrm{KG}}|$. The elements of the key generation alphabet are $\chi_{\mathrm{KG}} = \{1,2,...,2\cdot\alpha_X/\delta_X\} = \left\{1,2,...,|\chi_{\mathrm{KG}}|\right\}$. The parameters defining the key generation grid are the cut off parameter α_X denoting the borders of the grid around the point of origin of the phase sub-space, and the spacing δ_X which is the width of the partitions as explained in Figure 4.1.

The cut off parameter is chosen such that the probability of a measurement outside the grid is negligible:

$$\alpha_X = \min\left\{ \alpha'_X \middle| \mathcal{W}[\gamma^X_{AB}, \alpha'_X] \leq \varepsilon_S \right\}$$

where ε_S is the secrecy of the protocol. thus leaving, in principle, δ_X as the only free parameter of the grid. Hence, the partitions $[-\infty, -\alpha_X]$ and $[\alpha_X, \infty]$, which have generally to be considered in the key generation process, do in practice not contribute to the raw keys of Alice and Bob. For practical purposes, and without compromising the security of the CV-QKD protocol, we do not consider these partitions for the rest of this thesis.

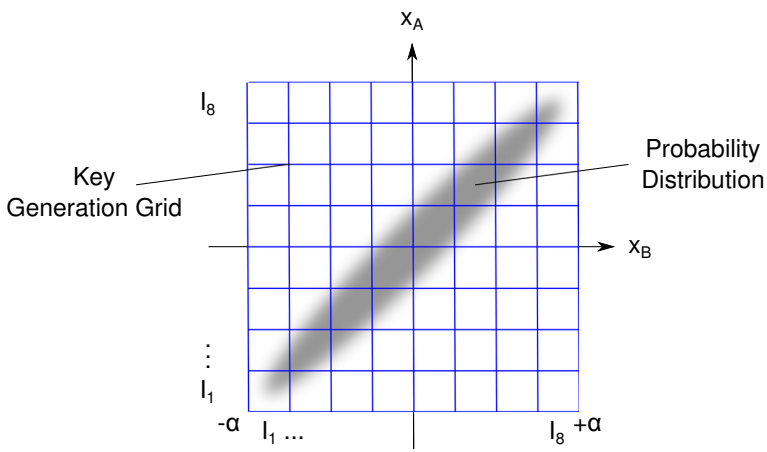

Figure 4.1.: The correlations between synchronised measurements of Alice and Bob of either the amplitude or phase quadrature. The axes of Alice and Bob are divided into several intervals I_i with $i \in \{1, 2, ...|\chi_{\mathrm{KG}}|\}$, all of which are uniquely projected to elements of the key generation alphabet χ_{KG}.

We consider the following key generation grid

$$G^X_{\mathrm{KG}} = \{I_1, I_2, \ldots, I_N\} = \{(-\alpha_X, -\alpha_X + \delta_X], \ldots, (\alpha_X - \delta_X, \alpha_X)\}. \tag{4.5}$$

To generate the raw keys $\mathrm{Bin}[K_{AB}]$ of Alice and Bob from their key generation samples K_{AB} we have to uniquely map the partitioned outcomes to the

associated alphabet elements $\chi_i \in \chi_{\mathrm{KG}}$. We choose the mapping such that the measurement outcome in the i'th partition is mapped to the i'th element of the key generation alphabet $I_i = \chi_i$. We call this whole process the partitioning of the samples and write the partitioned raw keys of Alice and Bob $\mathrm{Bin}[K_{AB}]$. We assume that, after this step, Alice and Bob end up with exactly N_{key} alphabet elements of χ_{KG}.

A similar mapping relates the alphabet elements uniquely to their corresponding bit sequences and is described by the mapping M. Note that we do not assume a specific mapping M at this point. If $|\chi_{\mathrm{KG}}| = |\mathcal{GF}(2^d)| = 2^d$ we identify the key generation alphabet with a Galois field of dimension d. This allows to uniquely identify each element of the alphabet with a unique combination of d bits (a bit sequence) whereby all possible combinations of bits in the sequence are covered. Note that the mapping M has an effect on the efficiency of the reconciliation if it operates on the level of $\mathrm{Bit}[\mathrm{Bin}[K_{AB}]]$ as we will show in Section 6.2.1. If the reconciliation operates on the level of the key generation alphabet $\mathrm{Bin}[K_{AB}]$ instead, any M can be used for the generation of the bit sequences.

The key generation grids could, in principle, be different for Alice and Bob and X and P, one only has to maintain the size of the key generation alphabet $|\chi_{\mathrm{KG}}|$. We will show in Chapter 5 that the key can be generated from one quadrature only without losing potential secret information, which simplifies the key generation. This allows to either focus on the amplitude or the phase quadrature in the process of key generation. But the grids of Alice and Bob could in principle still be different. We discuss this problem in wider detail in Section 4.4.1.

4.4.1. Origin of Errors in the Raw Keys

This section describes the two different origins of errors in the partitioned raw keys of Alice and Bob.

We focus here on direct reconciliation which defines Alice's raw key $\mathrm{Bin}[K_A]$ as reference for Bob's raw key $\mathrm{Bin}[K_B]$. It follows that Alice holds the correct raw key whereas Bob's raw key is assumed to be noisy. Alice sends Bob in a mono directional setting of this kind information about her raw key to enable Bob to reconcile his raw key $\mathrm{Bin}[K_B]$. Hence Bob has to correct his noisy raw key using all the information he has and all the information he additionally gets from Alice over the authenticated classical channel. The situation for reverse reconciliation is computed analogously.

We discuss Alice's probability distribution function of her partitioned measurement outcomes conditioned on Bob's outcomes in this section. The probability distribution function describes the errors between Alice's and Bob's raw keys Bin$[K_A]$ and Bin$[K_B]$. We assume that Alice and Bob measure in the same basis, for example the amplitude quadrature. The distribution of Alice's and Bob's outcomes is a Gaussian distribution with the general covariance matrix

$$\gamma_X = \begin{pmatrix} \lambda_A & C_X \\ C_X & \lambda_B \end{pmatrix}.$$

We will now discuss two different sources of errors in Bob's raw key:

Grid errors:
We focus at first on the general covariance matrix and write

$$\gamma_X = \begin{pmatrix} \lambda_A & C_X \\ C_X & \lambda_B \end{pmatrix} = \begin{pmatrix} \lambda_A & \rho\sqrt{\lambda_A\lambda_B} \\ \rho\sqrt{\lambda_A\lambda_B} & \lambda_B \end{pmatrix}$$

which is asymmetric for $\lambda_A \neq \lambda_B$. Note that in this description $\rho \in [0,1]$ measures the strength of the correlation.

We can now describe the effect of $\lambda_A \neq \lambda_B$ on the expectation value of Alice's outcomes and the key generation grid as shown in Figure 4.2.

The expectation value of Alice's conditional distribution is in general

$$\mu_{x_{A,i}} = \langle \mathcal{W}\left(\gamma_{A|B}, x_{A,i}|x_{B,i}\right)\rangle_{x_{A,i}} = x_{B,i} \cdot \frac{\sqrt{\lambda_A}}{\sqrt{\lambda_B}} \cdot \rho \geq x_{B,i} \cdot \rho. \tag{4.6}$$

One can directly see, that, assuming Alice's and Bob's synchronised and simultaneous measurements $x_{A,i}$ and $x_{B,i}$ to be perfectly correlated[5] they do not end up with $\overline{x}_{B,i} = \mu_{x_{A,i}}$ for $\lambda_A \neq \lambda_B$. It follows furthermore, that, when the key generation samples are partitioned, their key elements Bin$\left[x_{A,i}\right]$ and Bin$\left[x_{B,i}\right]$ might not necessarily be equal.

This problem can either be solved by an appropriate scaling of the key generation samples or by different key generation grids for Alice and Bob. Assuming direct reconciliation allows to rescale Bob's key generation outcomes

[5] Perfect correlation means in this sense $\rho = 1$.

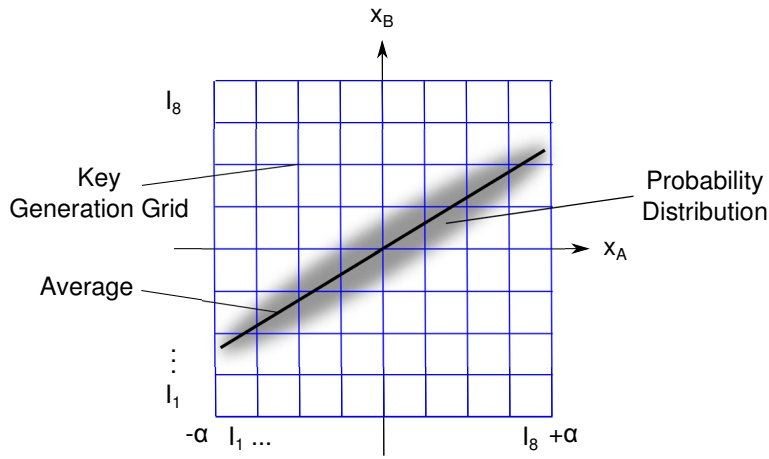

Figure 4.2.: This figure illustrates the errors that appear in Alice's and Bob's raw key for a asymmetric state if the outcomes are not scaled. The black line denotes the outcomes of Alice and Bob in average.

K_A such, that the key generation grids of both are equal which simplifies the reconciliation. We propose in Section 6.3.7.1 a scaling of the measurements which allows us to circumvent the grid errors and refer to this chapter for further details.

After scaling Bob's partitioned outcomes, the only origin of errors left between the raw keys of Alice and Bob is the conditional variance of Bob's measurement outcomes which we will discuss in the following.

Conditional probability errors:
We assume $\lambda = \lambda_A = \lambda_B$ in the following which means, that Bob's outcomes K_B are scaled properly. Let us now focus on the symmetric covariance matrix:

$$\gamma_X = \begin{pmatrix} \lambda & C_X \\ C_X & \lambda \end{pmatrix}.$$

Bob's knows his outcome $x_{B,i}$ and asks for the probability distribution of Alice's outcome $x_{A,i}$ which is given by the Shur complement of the covariance

matrix γ_{AB} [ESP02]

$$\gamma_{A|B} = \gamma_B - C\left(X_j \gamma_A X_j\right)^{\mathrm{MP}} C^T \tag{4.7}$$
$$\mathcal{P}[x_{A,i}|x_{B,i}] = \mathcal{P}[x_{A,i}|x_{B,i}] = \mathcal{W}\left(\gamma_{A|B}, x_{A,i}|x_{B,i}\right)$$

where MP denotes the Moore Penrose inverse [Pen55] and

$$X_X = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, X_P = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

being the matrices corresponding to the perfect amplitude X_X and phase X_P measurement of Alice. We call the Equation 4.7 in the following the *conditional probability distribution function*. The Gaussian distribution as sketched in Figure 4.3 describes Alice's measurement variance $\lambda_{A|B}$ conditioned on Bob's outcome and quantifies the errors of his raw key Bin$[K_B]$.

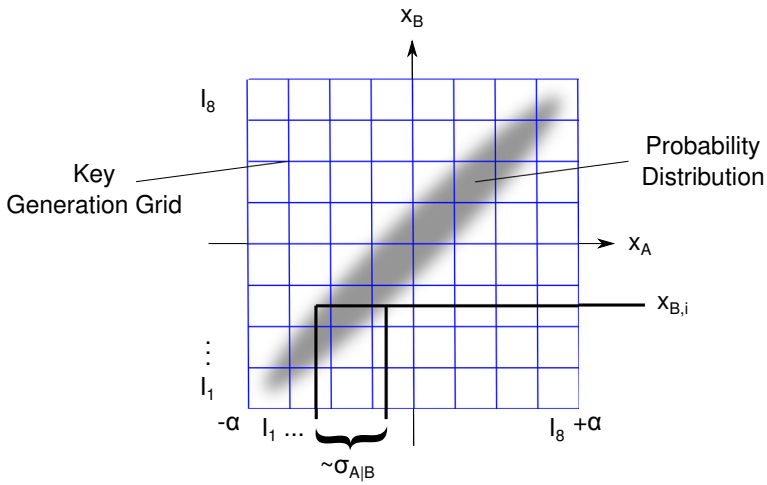

Figure 4.3.: The Gaussian probability distribution function which describes Alice's and Bob's measurement outcomes. Bob's distribution conditioned on Alice's measurement outcome is described by the conditional variance (standard deviation) $\lambda_{A|B}$ ($\sigma_{A|B}$). This correlation is the key ingredient in all the CV-QKD protocols we discuss in this thesis.

Alice's conditional variance (standard deviation) can be written as

$$\lambda_{A|B} = \left(\frac{\lambda_A \cdot \lambda_B - C_X^2}{\lambda_B} \right) \tag{4.8}$$

$$\sigma_{A|B} = \left(\frac{\lambda_A \cdot \lambda_B - C_X^2}{\lambda_B} \right)^{\frac{1}{2}}. \tag{4.9}$$

It can be shown, that $\lambda_{A|B}$ ($\sigma_{A|B}$) is independent of Bob's outcome $x_{B,i}$ and thus constant. As the outcomes of Alice and Bob are assumed to be scaled properly, this is the only origin of errors which is left in the key generation. We refer to this distribution from now on as the *origin of noise* in Bob's raw key. Bob uses this knowledge to reconcile his raw key Bin$[K_B]$.

4.5. Security against Collective Attacks

This security class assumes that Eve has a quantum memory and measures the states after completion of the QKD protocol such, that her attack can be written in tensor product form. Her attacks are thus all equal.

For the estimation of the potential key rate of the CV-QKD protocol providing security against collective attacks as proposed by Dr. F. Furrer *et al.* in [FFB+14], we have to perform a full tomography of the covariance matrix of the bipartite Gaussian state of Alice and Bob as explained in Section 3.5. This requires the state to be Gaussian, which is a drawback of this protocol as this might not always be true. One has to either check the Gaussianity of the state in experimental realisations [BDP+10] or find an information theoretical tool to circumvent this problem. It has been shown in, for example, [NGA06] that Gaussian attacks are optimal in the limit of infinitely many measurements. Remember that all the CV-QKD protocols we discuss in this thesis consider the finite-size effects of finitely many samples which is why we can not use that theoretical tool to circumvent the problem. We discuss this problem in Section 5.5.1.

The collective protocol allows for the post selection of certain measurement samples in M_{AB} and for direct and reverse reconciliation. This CV-QKD protocol is similar to former works [CLA01, GP01, DHF+07] which also discussed CV-QKD providing security against collective attacks of Alice and Bob.

The protocol parameter which is to be estimated in tomography is the covariance matrix γ_{AB}, which fully describes the bipartite Gaussian state in use. In

Section 5.4.1 we present an extension of the security proof proposed by Dr. F. Furrer *et al.* which allows us to generate the key from one quadrature only.

We certified the security of an experimental setup which used a v-class state (see Section 5.4.1.2) against collective attacks.

In Section 6.2.1 we describe an experiment in which a real secure key was generated from an s-class state by performing key generation, post selection and classical post processing.

4.6. Security against Coherent Attacks

In this setting Eve has a quantum memory which she can use to store all her information from one run for a later coherent measurement after completion of the whole CV-QKD task. As this security analysis includes all attacks which are compatible quantum mechanics, the protocol is less resilient to noise than in the case of collective attacks. Additionally, post selection is not allowed. Achieving a positive secure key rate is thus a very challenging experimental task. The Gaussian states produced by the group of R. Schnabel are strongly enough squeezed to allow for a positive key rate with reasonable experimental losses. Although it was recently shown in [Fur14] that the CV-QKD protocol secure against coherent attacks is also secure under reverse reconciliation, we restrict ourself to direct reconciliation in this thesis.

The security proof against coherent attacks as proposed by Dr. F. Furrer [FFB+14] does not require a full tomography of the bipartite Gaussian state in terms of the covariance matrix γ_{AB}. It only requires a tomography of the correlations between Alice's and Bob's synchronised and partitioned measurement tuples $\{I_{A,i}, I_{B,i}\} \in \mathrm{Bin}[M_{AB}]$ using N_{pe} tuples in the sense of

$$d(\mathrm{Bin}[M_A], \mathrm{Bin}[M_B]) = \frac{1}{k} \cdot \sum_{k=1}^{N_{\mathrm{pe}}} \left| I_{A,k} - I_{B,k} \right|, \tag{4.10}$$

which is the (generalised) Hamming distance[6] of the k synchronised measurement tuples. $d(\mathrm{Bin}[M_A], \mathrm{Bin}[M_B])$ is the protocol parameter which is computed during the parameter estimation of the corresponding CV-QKD protocol. One checks if the protocol parameter exceeds a specifically chosen value d_0, which is used for the estimation of the potential secure key rate,

[6] Note that this is also known as the distance in sequence space ℓ^1.

otherwise the protocol aborts.

Chapter 6.2.1 describes an experiment in which a secure key was generated by performing classical post processing using a new reconciliation scheme.

In Section 5.4.2 we analyse the security of an extension of this CV-QKD protocol which allows to generate the key from one quadrature alone.

4.7. Classical Reconciliation

Reconciliation protocols are used to correct the errors which can occur during the distribution of a message. This is a result of non-ideal channels in experimental realisations. To correct the errors, redundancies are either introduced directly into the message or computed from the message and sent afterwards over an authenticated channel.

There exist theoretical descriptions of reconciliation algorithms which operate directly on the level of quantum states, but as they are, for reasonable parameter sets, not efficient enough [SFL+13] and experimentally very involved [CLS+04, CPM+98], we focus on classical reconciliation protocols.

Remember, that the security of classical ciphering depends on either using methods unknown to the adversary (steganography) or encoding the text using a ciphering protocol which generates the key from a key space so large that an adversary can only reconstruct the original text in a finite but very large time. The security of her classical ciphering protocol does not depend on what happens to the encoded text while it is communicated over an authenticated classical channel, it could for example be copied arbitrarily many times by the adversary without corrupting the security of the cipher [Sin99]. This allows to send the text arbitrarily many times over the classical channel which introduces the redundancies necessary to correct possible errors at the receiver. More involved classical reconciliation schemes communicate only some redundancies thereby reducing the communication cost as we will explain later.

In QKD the security of the setup originates from the well-known no-cloning theorem [Bru03] and the fact that it is not the text which is distributed over the quantum-channel but the key (one-time pad). Introducing redundancies directly into the key (like, for example, sending the key twice) would break the i.i.d. assumption, an assumption common to all QKD protocols we anal-

yse in this thesis. Thus, only those classical reconciliation protocols which compute additional redundancies from the text to be sent afterwards over a classical channel can be used in QKD.

We have to consider an additional constraint on the reconciliation methods. The potential secure key rate k_{pot} can be seen as an upper bound on the information that can be disclosed for different purposes. This makes it more important that the reconciliation scheme used afterwards only reveals as few bits as necessary to correct the errors between the raw keys. The minimum necessary amount of bits needed for the reconciliation is, in the infinite case, given by the Shannon entropy [Sha48]. The task is to invent reconciliation schemes which operate as close as possible to the Shannon limit.

Additional assumptions about the origin of errors in the raw keys could increase the efficiency of reconciliation. This becomes especially important if the outcome of the key generation is not an element of $\mathcal{GF}(2)$ but of $\mathcal{GF}(2^d)$, where the Hamming distance of the partitioned samples could additionally carry some information too. In the case of key generation resulting directly in elements of $\mathcal{GF}(2)$, the Hamming distance of the samples can be maximally 1, thus carrying no additional information.

One prominent reconciliation protocol which is still used in, for example, DV-QKD is Cascade, a bitwise reconciliation scheme using two-way communication and checksums as we will show in Section 4.7.1. Another example is low density parity check (LDPC) reconciliation which uses checksums combined with an additional maximum-likelihood estimator using only one-way communication as we will explain in the Sections 4.7.2 and 4.7.3.

Cascade and binary LDPC do not make any assumption about the quantum origin of the errors appearing between the raw keys of Alice and Bob. They are sufficiently described by the average possibility of a bit flip [MK04][7]. Non-binary reconciliation schemes, like non-binary LDPC, could, in principle, use the Hamming distance as an additional information source for error detection.

All the reconciliation schemes we present in the following can be used in either direct or reverse reconciliation. Remember that, in direct reconciliation, Alice's raw key is the reference used to correct the errors in Bob's raw key. In reverse reconciliation Bob's raw key is the reference and Alice's is corrected.

[7] Note that the quantum channel used to distribute the raw keys is in our case not an erasure channel. The only error which can appear is the bit flip error.

4.7.1. Cascade

Cascade is a bitwise reconciliation protocol which was introduced in 1993 by Brassard and Salvail [BS93]. Another good discussion of Cascade is [MMPP+15].

Cascade was especially designed for the usage in QKD protocols with key generation alphabet size $|\mathcal{GF}(2)| = 2$ which always generate exactly one bit of raw key per shot. One prominent example of such protocols is the well-known DV-QKD BB84 [BB84] scheme, which was proposed by Bennett and Brassard in 1984. This prepare-and-measure protocol encodes the bits in the polarisation of single photons which are then sent to Bob.

The errors between the raw keys of Alice and Bob originate in this example from two different physical effects. The first effect is photon absorption due to damping, such that Bob sometimes measures nothing. Such errors can be described by a binary erasure channel [MK04]. A second type of error can occur if the polarisation of the photon being sent to Bob changes on its way. This can result in bit flip errors between the raw keys. The errors can be described by a binary symmetric channel [MK04]. The errors originating from absorbed photons are corrected by simply discarding the corresponding samples in the sifting procedure. As Alice and Bob are synchronised, Bob can simply communicate when he did not measure anything at all. As the bit flip errors pass the sifting procedure they end up in the raw keys of Alice and Bob. Cascade is designed to correct for these errors.

In the first stage of the protocol Alice and Bob agree to split their raw keys into several sub-strings. Now Alice computes the modulus two of the XOR checksum of, say, the first of the sub-strings and communicates her result to Bob over a classical channel. Every time Alice communicates the modulus two of some sub-string one bit of information about the raw key is disclosed to a possible adversary. Bob does the same and sends Alice a request to continue with the error detection if his result does not match with Alice's outcome. In case they do not match, Alice splits her sub-string again and sends the modulus two of its checksum to Bob, who again compares with his result. Alice and Bob continue with this error detection, subsequently breaking down the sub-strings to the one wrong bit which is flipped and correct it. This is why this scheme is called Cascade.

Obviously, Cascade is a protocol which uses classical two-way communication. This is a problem for many security proofs as they assume often one-way reconciliation. We furthermore note that the computational complexity

of the Cascade protocol is very low as only the modulus two of checksums is computed, communicated and compared. This reconciliation can, additionally, be easily parallelised, thus allowing for real-time reconciliation in QKD setups. Today's standard computational power allows for more complex reconciliation protocols like, for example, LDPC which we explain in the next section.

4.7.2. Binary Low Density Parity Check

Binary LDPC reconciliation protocols were invented in 1963 by Robert G. Gallager in his Ph.D. thesis [Gal63]. They combine XOR-checksums and a maximum likelihood estimator with one-way classical communication, operating on the level of bits ($\mathcal{GF}(2)$). Although they generally provide very good efficiency, LDPC codes are accompanied by a high computational complexity.

As the computational power of computers did not enable a real-time reconciliation in the 60's, LDPC codes were nearly forgotten until the early 90's, when Neal and McKay [MN95] effectively re-invented them by introducing more advanced LDPC codes which allowed for real-time reconciliation on standard computers. Several similar block codes have been invented since then for various, but mostly classical reconciliation purposes [Ple82]. Today, many different LDPC codes are used in a variety of classical reconciliation tasks, for example, television, telephones, satellite systems and computers.

We now describe the basics of LDPC reconciliation. Let us assume that Alice and Bob hold the correlated but erroneous binary raw keys $K_{AB}^{\mathrm{Bit}} = \mathrm{Bit}[\mathrm{Bin}[K_{AB}]]$ of length N_{key} which are generated by some QKD protocol (for example BB84). Note that we focus only on bit-flip errors. Although it is in principle not necessary, we assume Alice and Bob divide their raw keys into several sub-strings $K_{AB,i}^{\mathrm{Bit}}$ before reconciliation. As we focus on direct reconciliation, Alice, as the reference, encodes her sub-string $K_{A,i}^{\mathrm{Bit}}$ into a vector $S_{A,i}$, which we call the syndrome, as

$$\mathrm{mod}_2\left(H \cdot K_{A,i}^{\mathrm{Bit}}\right) = S_{A,i},$$

where $H \in \mathrm{Mat}_{n\times\, m}$ and $n > m$ is a randomly generated sparse matrix. Alice communicates her syndrome together with H to Bob over some classical channel who then performs the same computation on his sub-string

$$\mathrm{mod}_2\left(H \cdot K_{B,i}^{\mathrm{Bit}}\right) = S_{B,i}.$$

Now Bob compares his syndrome with the one sent by Alice and tries to correct his sub-string using a maximum-likelihood estimator. To explain the maximum-likelihood estimator, we assume a specific LDPC matrix like, for example,

$$\mathrm{mod}_2 \left[\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \right] \cdot \begin{pmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \\ u_5 \\ u_6 \end{pmatrix} = \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{pmatrix} \tag{4.11}$$

where the relations between Alice's raw key nodes and her syndrome nodes induced by the LDPC matrix can be visualised by a Tanner graph [Sho02] as depicted in Figure 4.4.

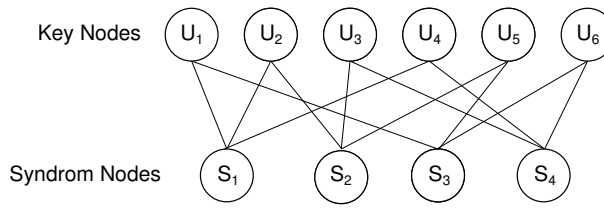

Figure 4.4.: The raw key nodes, the syndrome nodes and the relations between them as described by an LDPC-matrix H. Every syndrome node s_j depends on three different raw key nodes u_j via a bitwise XOR operation. As every raw key node contributes to two syndrome nodes, the results of the four syndrome nodes are correlated.

Although the chosen LDPC matrix is not really sparse in this example, it will suffice to explain the LDPC-reconciliation protocol. The construction of LDPC-reconciliation protocols allows for a probabilistic maximum-likelihood estimator used later by Bob to correct his key. In a real situation the size of one sub-string is normally much larger $|K_{AB}^{\mathrm{Bit}}| \geq 10^3$ [SBPC+09] than in this example. The example represents a regular LDPC matrix because the number of ones is constant for every row (3) and constant for every column (2). An irregular LDPC matrix does not fulfill this constraint.

Alice sends her syndrome together with the corresponding LDPC matrix over

a classical channel to Bob, disclosing thereby the amount of information carried by the syndrome to a potential eavesdropper ($|S_{A,i}|$ bits). Bob stores the information and computes his syndrome $S_{B,i}$. Then he compares all his syndrome nodes one after another with Alice's, marking the contributing raw key nodes either correct or incorrect depending on whether the corresponding syndrome nodes coincide or not. After normalisation he ends up with a table consisting of the probabilities $\mathcal{P}_{\text{cor}}$ of the different raw key nodes being correct $\mathcal{P}_{\text{cor}}$ or not $(1-\mathcal{P}_{\text{cor}})$. At this point he has to use a specific maximum-likelihood estimator to correct the raw key nodes that do not coincide with high probability. We assume, for the purpose of this example, a simple majority vote. That is, Bob chooses (depending on $\mathcal{P}_{\text{error}}$) a constant $\mathcal{P}_{\text{decision}}$ and flips all the raw key nodes which have $\mathcal{P}_{\text{cor}} < \mathcal{P}_{\text{decision}}$.

We note here that only one round of communication over a classical channel is necessary to correct the errors in Bob's raw key. Furthermore, we see that the maximum likelihood estimator increases the computational complexity in comparison to Cascade, where only bitwise XOR operations are used [DF07].

4.7.3. Non-Binary Low Density Parity Check

Non-binary LDPC reconciliation protocols have been discussed for the first time in 1963 by Robert G. Gallager in his Ph.D. thesis [Gal63]. They represent a natural extension of binary LDPC reconciliation to alphabets $\mathcal{GF}(2^d)$ with $d \geq 1$ [DF07].

The Hamming distance between the elements of $\mathcal{GF}(2^d)$ carries additional information for $d > 1$ which was not the case in binary LDPC. Thus non-binary LDPC codes disclose fewer bits of the potential secure key than binary LDPC if the key generation alphabet $\chi_{\text{KG}} = \mathcal{GF}(2^d)$ has dimension $|\mathcal{GF}(2^d)| > 2$.

In principle, non-binary LDPC follows the same ideas as its binary counterpart, it merely operates on a larger alphabet [Sho02]. As the CV-QKD protocols discussed in this thesis operate on higher dimensional key generation alphabets, this is always the case in our analysis. We thus identify non-binary LDPC as being well suited for the purpose of reconciliation in this thesis.

An easy example of a non-binary LDPC matrix can be generated by simply inserting randomly chosen numbers $\{0,1,2,3\}$ in the non-zero entries of a

binary LDPC matrix H [HEA05] like for example

$$H = \begin{pmatrix} 1 & 3 & 0 & 2 & 0 & 0 \\ 0 & 1 & 1 & 0 & 2 & 0 \\ 2 & 0 & 0 & 0 & 3 & 1 \\ 0 & 0 & 1 & 3 & 0 & 1 \end{pmatrix} \tag{4.12}$$

which represents a non-binary LDPC matrix for the finite field $\mathcal{GF}(4)$.

The reconciliation algorithm is analogue to the binary LDPC protocol. We abdicate the detailed description of the non-binary LDPC reconciliation protocol as it is only more complicated than the example we presented in Section 4.7.2 without providing more insight.

4.7.4. Efficiency Estimation

We describe in this section how the communication cost ℓ_{EC} of a reconciliation procedure is estimated.

Let us assume that Alice and Bob hold the raw keys $\mathrm{Bin}[K_A]$ and $\mathrm{Bin}[K_B]$ with $\mathrm{Bin}[K_A] \neq \mathrm{Bin}[K_B]$. Note that it makes a difference whether binary or non-binary reconciliation is evaluated. If non-binary reconciliation is considered the raw keys have to be available on the level of the key generation alphabet $\widetilde{K}_{AB} = \mathrm{Bin}[K_{AB}]$. In contrast, if binary reconciliation is to be analysed the raw keys are assumed to be present on the level of bits $\widetilde{K}_{AB} = \mathrm{Bit}[\mathrm{Bin}[K_{AB}]]$.

The direction of the communication during the reconciliation procedure is predefined by the QKD protocol used to generate the keys. In direct reconciliation Alice sends information over a authenticated classical channel to Bob. Alice's raw key is assumed to be correct and Bob has to reconcile his raw key using the information he got from Alice. In reverse reconciliation Alice has to reconcile her raw key.

We assume the term describing the communication cost to be in the asymptotic limit of infinitely many measurements and direct reconciliation of the form [SBPC+09, SW71]

$$\ell_{\mathrm{EC}} = \lambda \cdot \mathrm{H}\left(\widetilde{K}_A | \widetilde{K}_B\right) \tag{4.13}$$

where $\mathrm{H}\left(\widetilde{K}_A | \widetilde{K}_B\right)$ describes the minimum of information which Alice has to send to Bob for a successful reconciliation of his raw key as described in Section A.3. In reverse reconciliation one has to consider $\mathrm{H}\left(\widetilde{K}_B | \widetilde{K}_A\right)$. We

use these equations to simulate real-life implementations of reconciliation schemes. Such real-life implementations are never perfect which is reflected by $\lambda > 1$.

The connection between the communication cost ℓ_{EC} and the efficiency β_{EC} of real-life implementations is given by

$$\begin{aligned} \lambda \, \mathrm{H}\left(\widetilde{K}_A|\widetilde{K}_B\right) &= \lambda\big(\, \mathrm{H}\left(\widetilde{K}_A\right) - \mathrm{I}\left(\widetilde{K}_A : \widetilde{K}_B\right)\big) \\ &= \mathrm{H}\left(\widetilde{K}_A\right) - \beta_{\mathrm{EC}} \cdot \mathrm{I}\left(\widetilde{K}_A : \widetilde{K}_B\right) \end{aligned}$$

which evaluates to

$$\lambda = \frac{\mathrm{H}\left(\widetilde{K}_A\right) - \beta_{\mathrm{EC}} \cdot \mathrm{I}\left(\widetilde{K}_A : \widetilde{K}_B\right)}{\mathrm{H}\left(\widetilde{K}_A|\widetilde{K}_B\right)}. \tag{4.14}$$

We use these equations to measure the efficiency of real-life implementations in terms of $0 \leq \beta_{\mathrm{EC}} < 1$. The entropies which are needed to theoretically describe the communication cost of reconciliation schemes are explained in Appendix A.3.

5. Runtime Analysis

5.1. Overview and Contributions

For simplicity QKD protocols often assume a uniform choice of the measurement basis which are relevant during the key generation process. From this point on in this thesis, we refer to such protocols as *symmetric* QKD protocols. However, certain security analysis [EMLW09, ZWZ+13, EMLW09, YHJ+13] allow for a *non-uniform* choice of the basis[1] and thus open the the possibility of improvement of the key rate. We refer to such protocols as *asymmetric* QKD protocols.

Firstly we motivate asymmetric QKD protocols by analysing their overall runtime T_{run} and compare them with the performance of symmetric protocols in Section 5.2. We continue with extending the symmetric security analysis described in [FFB+14] by introducing a non-uniform choice of the measurement basis in the Sections 5.4.1 and 5.4.2. We conclude by explaining the importance of such protocols in experimental realisations. This work was accomplished in cooperation with Dr. F. Furrer and Dr. Ciara Morgan.

5.2. Motivation

We focus on the task of key generation and ask the following question: What is the maximum length of secure key $|K_{\text{sec}}|$ that can be collected during an experiment in a given time interval T_{run}? This question is motivated by the time needed to fulfill different experimental tasks which are required by the QKD protocol, i.e. the duration of one measurement process T_M and the switching time T_S between the basis choices[2]. The runtime analysis provides a connection between the theoretical computation of the secure key rate k_{sec} of a QKD protocol and a experimental realisation of the setup.

[1] Note, that such protocols are also known as biased basis QKD protocols.

[2] Note that the time of the measurement process T_M^i and the time of the switching T_S^i might depend on the basis $i \in \{1,2,...m\}$ which is to be measured. We define $T_M = \max\{T_M^i\}$ and $T_S = \max\{T_S^i\}$.

The processes have to be synchronised between the participants. Thus, they have to start together with the QKD protocol at some point in time, denoted T_0, which is, without loss of generality chosen to be $T_0 = 0$.

As the basis are chosen i.i.d. (from some QRNG), none of the participants knows in advance which measurement basis will be chosen next, and therefore whether the measurement basis is actually to be switched. The participants have thus to agree on some ΔT_{sync} in order to synchronise their processes [EHS13]. We call such time dependent analysis of some setup in the following the *runtime analysis* of QKD protocols. Firstly we introduce our ansatz for the runtime analysis before going into the details. We show how asymmetric protocols can increase the amount of key generated during the stable runtime of the setup T_{run}.

5.3. Runtime Analysis: Quantum Key Distribution Protocols

We will now analyse the runtime of QKD experiments with two participants and two measurement bases. Let us subsume all QKD setups which are possible in such a setup into the family of runtime protocols F_m^e with $e = 2$ for two participants (Alice and Bob) and $m = 2$ for two measurement basis.

We denote the parameters which describe the weight with which a basis is chosen by q_1 and $q_2 = 1 - q_1$. We furthermore write the finite number of measurement tuples of a stable run of the setup $M_{AB} = M_A \times M_B$ and identify $q_i = |M_{i,A}|/|M_A|$ with $i \in \{1,2\}$, where $M_{i,A} \subset M_A$, is the number of measurement outcomes generated by Alice using the i-th measurement operator. The total number of measurements of one participant is $N_{\text{tot}} = |M_A| = |M_B|$. The runtime analysis we propose can analogously be carried over to other families F_m^e. But we especially focus on F_2^2 as we combine it later with CV-QKD protocols assuming two participants.

The family F_2^2 of runtime protocols can be divided into two sub-classes:

F^2_{2,T_M,T_S}:
This family represents those QKD setups where the measurement and switching process can be triggered independently from one another. To synchronise these processes, Alice and Bob have to agree on some time interval $\Delta T_{\text{sync}} \geq \max\{T_M, T_S\}$. This protocol family allows us to combine a non-uniform ba-

sis choice security analysis with a non-trivial runtime analysis. We formally discard the measurement tuples in the ΔT_{sync} where either Alice or Bob or both switched their basis by treating the switching process itself as an additional third measurement basis which we denote by E (for *empty*). They are detected and removed in the sifting sub-protocol as described in Section 4.3. Note, that the removed tuples can additionally be used for parameter estimation.

$$F^2_{2,T_M,T_S} = \left\{ F^e_m | \Delta T_{\text{sync}} \geq \max\left\{T_M, T_S\right\}, e = 2, m = 2 \right\} \tag{5.1}$$

$\boldsymbol{F^2_{2,T_{MS}}}$**:**
This represents the family of QKD-setups which does not allow us to trigger the measurement and switching process independently. That is, a switching process is included in every time step $\Delta T_{\text{sync}} \geq T_{MS} = T_M + T_S$. In this sense every runtime protocol of F^2_{2,T_M,T_S} has always a natural variant in $F^2_{2,T_{MS}}$ (and vice versa). This family can additionally mimic such QKD-setups where $T_M >> T_S$ ($T_S >> T_M$ analogously) which admits us to neglect the shorter process. Such setups allow for a security analysis which includes non-uniform basis choice too, however the runtime analysis is trivial as no independent switching processes can occur in this case.

$$F^2_{2,T_{MS}} = \left\{ F^e_m | \Delta T_{\text{sync}} \geq T_M + T_S, e = 2, m = 2 \right\} \tag{5.2}$$

5.3.1. Runtime Parameters of Experiment

We now describe the runtime implementation in the CV-QKD experiments as performed by the group of Prof. Dr. Schnabel [Ebe13].

The runtime protocol is a member of $F^2_{2,T_{MS}}$ since it accounts for the case

$$T_{MS} = T_M + T_S$$

with $T_S = 13 \cdot T_M$ as described in Figure 5.1. The relatively long time needed for a switching process stems from the mechanical back-reactions of the piezo on the electric field used to calibrate the system to the chosen quadrature measurement. Note that it is still possible to perform asymmetric CV-QKD protocols in this setup although the experiment is designed such, that a switching process is assumed even when the measurement basis is not changed.

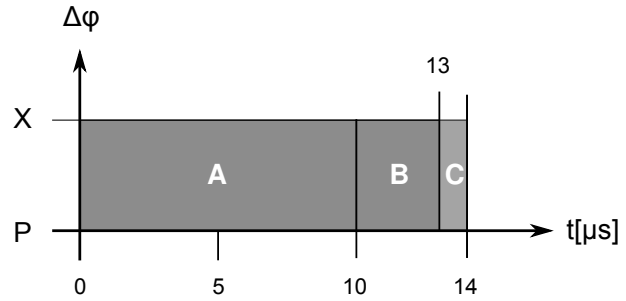

Figure 5.1.: Time resolution of a measurement and switching process as realised in experiment. Interval A shows the time needed for switching to the desired basis by changing the relative phase $\Delta\phi$ of the local oscillator by a piezo crystal. This excites a mechanical oscillation in the crystal which is damped after another $3\mu s$ (B). The whole switching process thus takes $T_S = 13\mu s$ whereas the measurement process itself is only $T_M = 1\mu s$ (C).

5.3.2. Analysis

We analyse the runtime of a two-party QKD setup of family F^2_{2,T_M,T_S} by focusing on the weights of only one of the participants (for example Alice) at first. The analysis is later extended to describe the statistics of both participants thus allowing for an analysis of the runtime protocol of the family F^2_{2,T_M,T_S}. We show how the length of the collected secure key N_{key} of one run T_{run} of a setup can be computed considering the additional switching processes. Similar analysis would allow us to describe the cases F^e_m with more than two $e > 2$ participants or $m > 2$ basis involved. We provide an example of the runtime analysis of the family F^2_3 in Appendix A.1.

We are given the weights with which the measurements in the two orthogonal basis of one participant are weighted, q_1 and $q_2 = 1 - q_1$. We furthermore assume a finite number of measurements of one participant $N_{\text{tot}} = \text{const}$ and know, in the case of F_{2,T_M,T_S}, that N_{tot} is just a fraction of many more time steps $N = N_{\text{tot}} + N_{\text{sw}}$ whereby N_{sw} denotes the number of switching processes in one run as explained in Figure 5.2. We start with the weights which describe how often one participant measures in one of the orthogonal basis. The final task is to estimate N as a function of q_1, q_2 and N_{tot}.

In general for the weight $\tilde{q}_{\text{sw}}$ of a switching process to occur in $N = N_{\text{tot}} + N_{\text{sw}}$

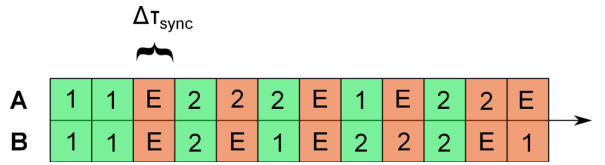

Figure 5.2.: A time line with Alice's and Bob's synchronised (ΔT_{sync}) time steps with the corresponding basis (1 or 2) or switching processes E (for empty - no measurement outcome). The red blocks denote the measurement tuples where either Alice or Bob (or both) switched the basis. The switching processes can be treated as a third measurement basis E which is additionally sorted out in the sifting procedure of the QKD protocol.

time steps [3], the following holds

$$\tilde{q}_{\text{sw}} = \frac{N_{\text{sw}}}{N} = \frac{N_{\text{sw}}}{N_{\text{tot}} + N_{\text{sw}}} = \frac{\frac{N_{\text{sw}}}{N_{\text{tot}}}}{1 + \frac{N_{\text{sw}}}{N_{\text{tot}}}}.$$

The weight of the switching processes needed to measure N_{tot} measurement outcomes is defined by

$$q_{\text{sw}} := \frac{N_{\text{sw}}}{N_{\text{tot}}}.$$

We now estimate q_{sw} as a function of the initial weights q_1 and q_2 and the number of measurement outcomes N_{tot}. We ask for the transition weights[4] $q_{i,j}$ of one participant to measure first in the basis i followed by a measurement in j with $i \neq j$.

We already confined ourself in the following analysis to the family where $i, j \in \{1,2\}$ and look at first at the transitions $q_{1,2}$ and $q_{2,1}$ of one participant, since the transitions $q_{1,1}$ and $q_{2,2}$ correspond to the cases where no switching oc-

[3] Note here, that the $\tilde{q}_i$ describe the weights normalised to N, which is the number of time steps of one participant with a runtime of $T_{\text{run}} = N \cdot \Delta T_{\text{sync}}$. The q_i are normalised to N_{tot}, which is the amount of measurement outcomes without the switching processes of one participant.

[4] These weights are the entries of the corresponding transition matrix [Fel57]. At this point the analysis can be extended to $m > 2$.

curs. We can identify the weight of the switching processes by

$$\begin{aligned} q_{\text{sw}} &= \sum_{i \neq j} q_{i,j} \\ &= q_1 q_2 + q_2 q_1 \\ &= 2q_1 \cdot \big(1 - q_1\big). \end{aligned}$$

The renormalised weight of the number N_{sw} of switching process to occur in $N = N_{\text{tot}} + N_{\text{sw}}$ time steps can now be written as

$$\tilde{q}_{\text{sw}} = \frac{N_{\text{sw}}}{N} = \frac{N_{\text{sw}}}{N_{\text{tot}} + N_{\text{sw}}} = q_{\text{sw}} \frac{1}{1 + q_{\text{sw}}}. \tag{5.3}$$

We additionally have to renormalise q_1 and q_2 by

$$\begin{aligned} \tilde{q}_1 &= \frac{N_1}{N} = \frac{N_1}{N_{\text{tot}} + N_{\text{sw}}} = q_1 \frac{1}{1 + q_{\text{sw}}} \\ \tilde{q}_2 &= \frac{N_2}{N} = \frac{N_2}{N_{\text{tot}} + N_{\text{sw}}} = q_2 \frac{1}{1 + q_{\text{sw}}} \end{aligned} \tag{5.4}$$

where N_1 (N_2) is the portion of N_{tot} which has been measured in the first (second) measurement basis. Of course

$$\sum_{i=1}^{3} \tilde{q}_i = 1.$$

We treat a switching process as an additional third basis E with weight $\tilde{q}_{\text{sw}}$ as already described in Figure 5.2. This allows for a full description of the runtime protocol of one participant. Figure 5.3 shows the weights with switching as a function of q_1.

We now lift this analysis to the case of two participants[5] $e = 2$. As all measurement basis of the two participants are assumed to be chosen i.i.d. we can identify the following

$$\begin{aligned} \tilde{N}_1 &= N \cdot \tilde{q}_1^2 = N_{\text{tot}} \cdot q_1^2 \\ \tilde{N}_2 &= N \cdot \tilde{q}_2^2 = N_{\text{tot}} \cdot q_2^2 \\ N_{\text{key}} \leq \tilde{N}_{12} &= N \cdot \big(\tilde{q}_1^2 + \tilde{q}_2^2\big) \end{aligned}$$

[5] Note, that this is the point where the runtime analysis can be easily lifted to more than two participants $e > 2$ to describe the setups F_2^e and furthermore F_m^e.

where N is the total number of synchronised time steps of both participants. The $\tilde{N}_i$ above describe the simultaneous measurements of Alice and Bob in either the amplitude or the phase quadrature. We have, in general, $N_{\text{key}} \leq \tilde{N}_{12}$ samples left for the key generation because some of the tuples of $\tilde{N}_{12}$ are usually needed for the parameter estimation.

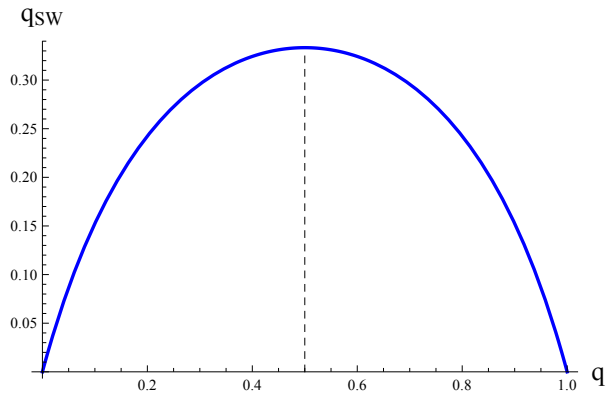

Figure 5.3.: The weight of one participant of switching processes to occur $\tilde{q}_{\text{sw}}$ as a function of the initial weights q_i. Note, that $\tilde{q}_{\text{sw}}$ is symmetric under permutation of the q_i.

Let us additionally identify

$$N_{\text{key}} = N_{\text{key}} \cdot \left(q_1^{\text{key}} + q_2^{\text{key}} \right)$$

with

$$\sum_i^2 = q_i^{\text{key}} = 1$$

where the $q_i^{\text{key}} = N_{\text{key}}^i / N_{\text{key}}$ with $N_{\text{key}}^i \subset N_{\text{key}}$ for $i \in \{1,2\}$ as we will need this notation in later sections where we combine the runtime analysis with specific CV-QKD protocols.

We include now the synchronised timing ΔT_{sync} into the runtime analysis in these computations and arrive at

$$T_{\text{run}} = \Delta T_{\text{sync}} \cdot N$$

which is the total time needed for one run of the setup, i.e. the time the experiment is assumed to be at minimum stable. The runtime analysis enables us to optimise the q_i's under the assumption of a specific CV-QKD protocol and a stable runtime T_{run} of a specific experiment.

The defining parameters of one specific CV-QKD realisation of the protocol family F_2^2 are:

Parameter	Value
Runtime protocol	F_2^2
q_1	Weight to measure the first basis
T_{run}	Stable runtime of the experiment
ΔT_{sync}	Synchronised time step

One could naively choose the weights corresponding to the basis choice to be $q_1 = 0$ or $q_2 = 0$ to optimise the over-all runtime analysis of all F_2^2 protocols, but this is not compatible with the parameter estimation under consideration as explained in Section 4.5 and Section 4.6. We focus thus on minimising the over-all weight of the switching processes q_{sw}.

5.3.3. Example

In this section we compare the runtime analysis of the asymmetric protocol of family $F^2_{2,T_M=1,T_S=1}$ with it's symmetric variant of family $F^2_{2,T_{MS}=1}$ for a fixed number of time steps N.

Let us simplify the following example by assuming that the key rate per sample, as a function of N_{key}, has saturated to some $k_{\text{sec}} = \text{const}$. This is usually the case for sufficiently many key generation samples N_{key} and sufficient parameter estimation N_{pe} of Alice and Bob.

Note that we omit, in this section, that the choice of a specific q_1 can have an effect on the secure key rate k_{sec}. We chose here $k_{\text{sec}} = 1$ Bit$\forall q_1$ for the whole section to simplify the simulation and focus especially on $q_1 \in [0.1, 0.9]$ to simulate a sufficient parameter estimation.

The function describing the secure key collected by the protocols is

$$|K_{\text{sec}}^{\text{sym}}| = N \cdot \left(0.5^2 + 0.5^2\right) - N_{\text{pe}}^{(1)} - N_{\text{pe}}^{(2)} = \text{const}$$
$$|K_{\text{sec}}^{\text{asym}}| = N \cdot \left(\tilde{q}_1^2 + \tilde{q}_2^2\right) - N_{\text{pe}}^{(1)} - N_{\text{pe}}^{(2)} \neq \text{const}$$

where the $\tilde{q}_i$ are computed according to Section 5.3.2. The $N_{\text{pe}}^{(1)} = N_{\text{pe}}^{(2)} = N \cdot \min\left[\left(q_1\right)^2\right] = N \cdot 10^{-2}$ represent the fraction of the tuples in $\tilde{N}_{12}$ which are needed for the parameter estimation.

We compare the asymmetric protocol $F^2_{2,T_M=1,T_S=1}$ with it's symmetric variant $F^2_{2,T_{MS}=1}$ with instantaneous switching processes in Figure 5.4.

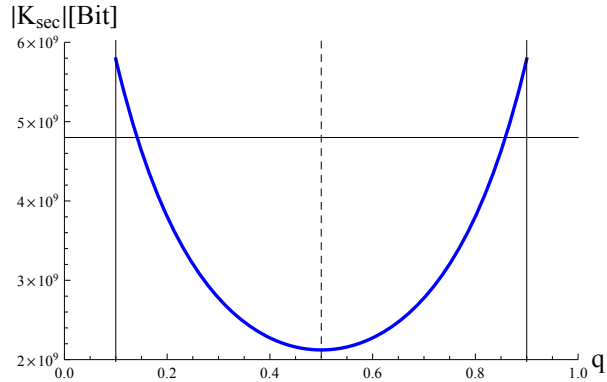

Figure 5.4.: The blue curve shows the length of the secure key $|K_{\text{sec}}^{\text{asym}}|$ generated by the asymmetric protocol $F^2_{2,T_M=1,T_S=1}$ for $q_1 \in [0.1, 0.9]$. The horizontal black line denotes the amount of secure key $|K_{\text{sec}}^{\text{sym}}| = \text{const}$ generated by the symmetric variant $F^2_{2,T_{MS}=1}$ which is independent of q_1. The secure key rate, the total runtime and the total number of synchronised time steps are chosen to be $k_{\text{sec}} = 1 = \text{const}$ and $T_{\text{run}} = N \cdot \Delta T_{\text{sync}}$ with $N = 10^{10}$ for both protocols, respectively. Note, that the asymmetric protocol generates more key $|K_{\text{sec}}^{\text{asym}}|$ for $q_1 < 0.14$ or, equivalently, $q_1 > 0.86$.

The amount of secure key generated for $q_1 = 0.1$ ($q_1 = 0.9$) is $|K_{\text{sec}}^{\text{asym}}| = 5.789 \cdot 10^9$ Bit (vertical black lines). This means, that an asymmetric protocol can,

in this example, generate $R_{1,2} = 1.157$ times more key per runtime T_{run}. This underlines the strength of asymmetric QKD protocols as they could, for certain parameter sets, even outperform their symmetric variants with perfect switching where ideally $T_{MS} = T_M$ with $T_S = 0$.

One can see in Figure 5.4 that the runtime analysis is symmetric around $q_1 = 0.5$. We give several examples in the following sections where we combine the runtime analysis of family F_2^2 with appropriate CV-QKD protocols either providing security against collective (in Section 5.4.1.3) or coherent (in Section 5.4.2.3) attacks with an experimental realisation.

5.4. Asymmetric Continuous Variable Quantum Key Distribution Protocols

In this section we will show how the ideas of the runtime analysis as discussed in Section 5.3.2 can be implemented in existing security proofs.

We extend the two symmetric CV-QKD protocols providing security against collective and coherent attacks of Dr. F. Furrer *et al.* [FFB+14] to asymmetric protocols and discuss their performance on the basis of experiments. We combine the two security analysis in numerical simulations with a full runtime analysis of CV-QKD setups and show the advantage of the non-uniform choice of basis in QKD.

5.4.1. Security against Collective Attacks

In this section we present a proof for an asymmetric CV-QKD protocol providing security against collective attacks. Considering finitely many samples N_{key} we analyse a corresponding asymmetric protocol following the ideas of runtime analysis. The first security analysis of a symmetric CV-QKD protocol assuming collective attacks and finite size effects is presented in [LGG10]. The entropies which are used in the security proof are explained in Appendix A.3.

This security proof analyses the security of the experimental setup described in Section 3.3 and is based on the entropies as presented in Section A.3. We write the secure key $K_{\text{sec}} = K_{\text{sec}}^X \cup K_{\text{sec}}^P$, where K_{sec}^X (K_{sec}^P) denotes the secure key which is generated from the amplitude (phase) quadrature. We can identify $q_1^{\text{key}} = q_X^{\text{key}} = K_{\text{sec}}^X / K_{\text{sec}}$ being the weight of both participants measuring

simultaneously the amplitude quadrature and $q_2^{\text{key}} = q_P^{\text{key}} = K_{\text{sec}}^P / K_{\text{sec}}$ representing the weight of a synchronised measurement in the phase quadrature. This connects the security analysis with the runtime analysis which is described in Section 5.3.2.

The non-uniform choice of basis is reflected by $q_X^{\text{key}} \neq q_P^{\text{key}}$ which are described by $q_P^{\text{key}} = 1 - q_X^{\text{key}}$.

5.4.1.1. Security Analysis

A full reconstruction of the state whereby we assume Gaussian states is needed for the computation of the key rate.

Remember, that a bipartite Gaussian state is fully described by the corresponding covariance matrix γ_{AB}. The covariance matrix is reconstructed from the measurement tuples N_{pe} of Alice and Bob as explained in Section 3.5.

We present here the security analysis for reverse reconciliation, the proof for direct reconciliation follows analogously.

We know that the following equation gives a bound on the secure key rate which could be generated from a given QKD setup assuming $n = N_{\text{key}}$ synchronised and simultaneous measurements and reverse reconciliation

$$|K_{\text{sec}}| \geq H_{\min}^{\varepsilon}(x_B^n|E^n)_{\omega} - \ell_{\text{EC}}(n) - \log_2\left[\frac{1}{4\varepsilon_1^2\varepsilon_C}\right]$$

where E^n describes the quantum system of the eavesdropper (Eve) which could be of infinite dimension and $\omega = \omega_{X_A^n, X_B^n, E^n}$ denotes the corresponding classical-quantum state. Now x_B^n describes the fraction of Bob's measurement outcomes which are used in the key generation. Of course, the formula is only valid if the protocol does not abort in which case the secure key is zero. The ε_i are a function of the secrecy of the QKD protocol ε_S and the reconciliation (i.e. the confirmation) ε_C.

The term $H_{\min}^{\varepsilon}(x_B^n|E^n)_{\omega}$ denotes the conditional smooth min-entropy of $\omega_{x_B^n, E^n}$ for $\varepsilon \leq (\varepsilon_S - \varepsilon_1)/2$ introduced in [Ren05] and generalised to infinite-dimensional systems in [Can01]. Hence, it remains to obtain a lower bound on $H_{\min}^{\varepsilon}(x_B^n|E^n)_{\omega}$ for any possible eavesdropping strategy allowed by collective security assumptions.

Under the assumption of collective attacks, we can assume that the state $\omega_{x_A^n,x_B^n,E^n}$ has tensor product structure, i.e., $\omega_{x_A^n,X_B^n,E^n} = \omega^{\otimes n}_{x_A,x_B,E}$. The smooth min-entropy of a product state can then be approximated by the conditional von Neumann entropy $\mathrm{H}(x_B|E)_\omega$ of $\omega_{x_B,E}$ via the infinite dimensional asymptotic equipartition property [FAR11, TCR10, Ren05]

$$|K_{\mathrm{sec}}| \geq H^{\varepsilon}_{\min}(x_B|E)_\omega \geq n\,\mathrm{H}(x_B|E)_\omega - \sqrt{n}\Delta, \tag{5.5}$$

where n has to be sufficiently large and

$$\Delta = 4\cdot\log_2\left(2^{\frac{1}{2}H\max(x_B)+1}+1\right)\cdot\sqrt{\log_2\left[\frac{2}{\varepsilon^2}\right]}.$$

In the next step, we use that the state $\omega_{x_B,E}$ is of the form $\omega_{x_B,E} = q_X^{\mathrm{key}}|X\rangle\langle X|_\theta \otimes \omega^X_{x_B,E} + q_P^{\mathrm{key}}|P\rangle\langle P|_\theta \otimes \omega^P_{x_B,E}$ where $\omega^X_{x_B,E}$, $\omega^P_{x_B,E}$ are the states obtained when the honest parties are performing synchronised and simultaneous measurements of the amplitude or phase quadrature, respectively. The system denoted by θ is a classical register which is assigned to the eavesdropper and it keeps track of which measurements were performed by the honest parties, therefore $\theta \in \{X,P\}$.

Using elementary properties of the von Neumann entropy (i.e. the additivity), we can now expand $\mathrm{H}(x_B|E\theta)_\omega = q_X^{\mathrm{key}}\,\mathrm{H}(x_B|E)_{\omega^X} + q_P^{\mathrm{key}}\,\mathrm{H}(x_B|E)_{\omega^P}$. Combining this estimation of the smooth min-entropy with the assumption of Gaussian attacks, we can use the confidence set $\mathcal{C}_{\varepsilon_{\mathrm{pe}}}$ to obtain a bound on the key length given by

$$|K_{\mathrm{sec}}| \geq n\cdot\inf_{\gamma\in\mathcal{C}_{\varepsilon_{\mathrm{pe}}}}\sum_\theta p_\theta\,\mathrm{H}(x_B|E)_{\omega^\theta_\gamma} - \sqrt{n}\Delta - \ell_{\mathrm{EC}}(n) - \log_2\left[\frac{1}{\varepsilon_S^2\varepsilon_C}\right]. \tag{5.6}$$

Here, the infimum is taken over-all states compatible with covariance matrices γ within the confidence set. For simplicity, we have chosen $\varepsilon_1 = \varepsilon_S/2$ which can be justified by the fact that for large enough n the term in the logarithm can be neglected. Note further, that, due to the definition of $\mathcal{C}_{\varepsilon_{\mathrm{pe}}}$, the key length from Equation 5.6 is now ε-secure[6] with $\varepsilon = \varepsilon_{\mathrm{pe}} + \varepsilon_S + \varepsilon_C$.

The von Neumann entropy for both quadratures $\theta \in \{X,P\}$ can now be computed under the non-restricting assumption that the eavesdropper holds the purification of Alice's and Bob's state, that is, we assume that $\omega_{\gamma,ABE}$ is the

[6] The definitions for composable security are given in Section 4.2.

purification of the Gaussian state $\omega_{\gamma,AB}$ with covariance matrix γ. It then follows by applying the definition of the conditional von Neumann entropy $\mathrm{H}(x_B|E) = \mathrm{H}(x_B E) - \mathrm{H}(E)$ and the self-duality of von Neumann entropies $\mathrm{H}(E)_{\omega_\gamma} = \mathrm{H}(AB)_{\omega_\gamma}$ that

$$\mathrm{H}(x_B|E)_{\omega_\gamma^\theta} = \mathrm{H}(E|x_B)_{\omega_\gamma^\theta} + \mathrm{H}(x_B)_{\omega_\gamma^\theta} - \mathrm{H}(AB)_{\omega_\gamma}.$$

As shown in [ESP02]

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

and

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

where $\mathrm{H}(E)_{\omega_\gamma^X(x_X=0)}$ ($\mathrm{H}(E)_{\omega_\gamma^P(x_P=0)}$) is the post-measurement state at the eavesdropper's side when Bob measured $x_{B,X}=0$ ($x_{B,P}=0$). The bipartite covariance matrix is written in block form, i.e.

$$\gamma = \begin{pmatrix} \gamma_A & \gamma_C \\ \gamma_C^T & \gamma_B \end{pmatrix}$$

and $M_X = \mathrm{diag}(1,0)$ and $M_P = \mathrm{diag}(0,1)$ are the projectors to the X and P quadrature, respectively[7]. MP denotes the Moore-Penrose inverse [BH12].

To compute Δ, we have to estimate $H_{\max}(x_B)$ which can be approximated by [FFB+14]

$$H_{\max}(x_B) \leq 2\log_2\left[\sqrt{q_X^{\mathrm{key}}}\cdot\sum_y\sqrt{\omega_{x_B}^x(y)} + \sqrt{q_P^{\mathrm{key}}}\cdot\sum_y\sqrt{\omega_{x_B}^P(y)}\right]$$

where $\omega_{x_B}^x$ and $\omega_{x_B}^P$ are the probability distributions of Bob's X and P quadrature measurements, respectively. While in a practical experiment the number of bits $\ell_{\mathrm{EC}}(n)$ can be directly computed for each run of the setup, we need to estimate the leakage term here to allow for a theoretical analysis of the setup.

[7] One could insert here some rotation matrices for M_X or M_P which account for the experimental imperfections of the calibration of the amplitude and phase measurements. We chose for the following to assume (also for simplicity), that the imperfections are fully described by the tomography. We thus shift the calibration imperfections to the full tomography of the state as measured in experiment thereby maintaining $M_X = \mathrm{diag}(1,0)$ and $M_P = \mathrm{diag}(0,1)$ in the security analysis.

We will discuss a realisation of an reconciliation scheme in the next Chapter 6 in detail.

We assume the term to be of the form [SBPC+09] as explained in Section 4.7.4

$$\ell_{\mathrm{EC}}(n) = q_X^{\mathrm{key}} \cdot n \Big(\mathrm{H}(x_B)_{\omega_\gamma^X} - \beta_{\mathrm{EC}} \, \mathrm{I}(x_A|x_B)_{\omega_\gamma^X} \Big) \tag{5.7}$$

$$+ q_P^{\mathrm{key}} \cdot n \Big(\mathrm{H}(x_B)_{\omega_\gamma^P} - \beta_{\mathrm{EC}} \, \mathrm{I}(x_A|x_B)_{\omega_\gamma^P} \Big) \tag{5.8}$$

where $\beta_{\mathrm{EC}} \in (0,1)$ is the reconciliation efficiency and $\mathrm{I}(A|B)$ is the mutual information. We mostly assume an efficiency of the reconciliation of $\beta_{\mathrm{EC}} = 0.9$ [EMMM11, MEM12]. With these results the secure key rate $k_{\mathrm{sec}} = |K_{\mathrm{sec}}|/n$ can be calculated by

$$\begin{aligned} k_{\mathrm{sec}} = \inf_{\gamma \in \mathcal{C}_{\varepsilon \mathrm{pe}}} & \left[q_X^{\mathrm{key}} \cdot \left[\mathrm{H}(E|x_B)_{\omega_\gamma^X} + \mathrm{H}(x_B)_{\omega_\gamma^X} \right] \right] \\ & + \left[q_P^{\mathrm{key}} \cdot \left[\mathrm{H}(E|x_B)_{\omega_\gamma^P} + \mathrm{H}(x_B)_{\omega_\gamma^P} \right] - \mathrm{H}(AB)_{\omega_\gamma} \right] \\ & - \frac{1}{\sqrt{n}} \Delta - \frac{\ell_{\mathrm{EC}}(n)}{n} - \frac{1}{n} \log_2 \left[\frac{1}{\varepsilon_S^2 \varepsilon_C} \right]. \end{aligned}$$

We identify the potential secure key rate per shot to be

$$k_{\mathrm{pot}} = \inf_{\gamma \in \mathcal{C}_{\varepsilon \mathrm{pe}}} \left[q_X^{\mathrm{key}} \cdot \left[\mathrm{H}(E|x_B)_{\omega_\gamma^X} + \mathrm{H}(x_B)_{\omega_\gamma^X} \right] \right] \tag{5.9}$$

$$+ \left[q_P^{\mathrm{key}} \cdot \left[\mathrm{H}(E|x_B)_{\omega_\gamma^P} + \mathrm{H}(x_B)_{\omega_\gamma^P} \right] - \mathrm{H}(AB)_{\omega_\gamma} \right] \tag{5.10}$$

$$- \frac{1}{\sqrt{n}} \Delta - \frac{1}{n} \log_2 \left[\frac{1}{\varepsilon_S^2 \varepsilon_C} \right] \tag{5.11}$$

which is equivalent to $k_{\mathrm{pot}} = k_{\mathrm{sec}} + \ell_{\mathrm{EC}}(n)/n$ denoting the amount of key which is secure but possibly erroneous.

In the theoretical asymptotic limit for an infinite number of samples $n = N_{\mathrm{key}} \to \infty$ and perfect security $\varepsilon \to 0$, the key rate k_{sec} tends to

$$\begin{aligned} k_{\mathrm{sec}}^{\infty} = & q_X^{\mathrm{key}} \cdot \Big(\beta_{\mathrm{EC}} \, \mathrm{I}(x_A, x_B)_{\omega_\gamma^X} + \mathrm{H}(E)_{\omega_\gamma^X(x_{B,X}=0)} - \mathrm{H}(AB)_{\omega_\gamma} \Big) \\ & + q_P^{\mathrm{key}} \cdot \Big(\beta_{\mathrm{EC}} \, \mathrm{I}(x_A, x_B)_{\omega_\gamma^P} + \mathrm{H}(E)_{\omega_\gamma^P(x_{B,P}=0)} - \mathrm{H}(AB)_{\omega_\gamma} \Big). \end{aligned}$$

The length of the key secure against collective attacks is described by

$$|K_{\mathrm{sec}}| = N_{\mathrm{key}} \cdot k_{\mathrm{sec}}.$$

Note that the protocol strategy of this security proof is such that we estimate the key rate of the setup using the same quadrature (or combination of quadratures) from which the raw key is generated.

5.4.1.2. Results

We present here two experiments which allow us to discuss asymmetric CV-QKD protocols which are secure against collective attacks.

The experiments have been realised as part of the collaboration *Crypto on Campus* and were carried out by the group of Prof. Dr. R. Schnabel at the *Albert Einstein Institute* in *Hannover*. A v-class state was used in the first experiment [EHD+13] where we certified the security of the setup analytically from the full tomography. In the second experiment we generated a secure key from an s-class state [Ebe13]. The two states are characterised in Table B.1.

In this section we focus on the first experiment as the advantages of the asymmetric protocol are more obvious when using v-class states and refer the details concerning the second experiment to Section 6.2.1.

To compute key rates of theoretical setups, we have to agree on some parameters required by the protocol. Following Section 4.4 the required parameters are as presented in Table B.2. We discuss in this section table-top setups and assume non-binary LDPC reconciliation with an efficiency of $\beta_{\mathrm{EC}} = 0.9 = \mathrm{const}$ unless otherwise noted.

V-class setup:
This setup is perfect for this discussion as the vacuum being entangled with a squeezed state leads to a highly asymmetric covariance matrix [EHD+13]. A key was not generated in the corresponding experiment, but we certified the security of the setup by assuming some specific reconciliation (non-binary LDPC with efficiency $\beta_{\mathrm{EC}} = 0.9$).

All measurement tuples were used to reconstruct the covariance matrix by following the protocol as described in Section 3.5, which actually calls for three measurement basis $\left\{X, Q_{\pi/4}, P\right\}$ for a full tomography of the state. We will directly use the covariance matrix as it already includes all possible ex-

perimental imperfections in our theoretical setup.

The Gaussian v-class state as reconstructed from Alice's and Bob's measurement tuples is

$$\gamma_{AB} = \left(\begin{array}{cc|cc} 0.541 & 0.135 & 0.459 & -0.095 \\ 0.135 & 24.633 & -0.037 & -23.293 \\ \hline 0.459 & -0.037 & 0.548 & 0.264 \\ -0.095 & -23.293 & 0.264 & 23.840 \end{array}\right). \tag{5.12}$$

The deviations stemming from finitely many measurements available for tomography are quantified by $\varepsilon_{\text{pe}} = 10^{-10}$. In this estimation process, Alice and Bob measure $5 \cdot 10^6$ tuples for each combination of quadratures (X, P) and finally $Q_{\pi/4}$.

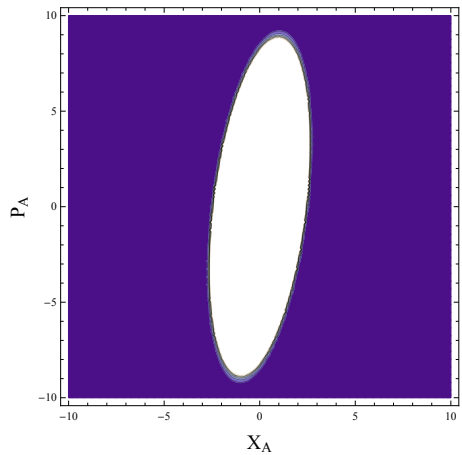

Figure 5.5.: The above graphic sketches the mismatch of Alice's amplitude x_A and phase p_A measurements. Note, that the quadratures are still assumed to be orthogonal. The mismatch can be quantitatively estimated by a third basis $(Q_{\pi/4})$ which is measured as described in Section 4.4.

A pump power of $235 mW$ generated a initial squeezed vacuum with 11.1 dB squeezing and 16.6 dB anti-squeezing. This squeezed state is superimposed with a vacuum state. The different conditional variances of Alice's and Bob's synchronised amplitude and phase measurements which are given in Table

B.1 reveal the asymmetry of the state.

Recall that we assumed perfectly orthogonal measurements in our security analysis. The outcomes of the quadrature $Q_{\pi/4}$ measure the off diagonal elements of the sub-blocks γ_A and γ_B, which should be zero in the case of perfect calibration of the system to the amplitude and phase quadrature. However a constant phase shift of the local oscillator resulted in a deviation from the ideal case. After all, the measurement quadratures can still be assumed to be orthogonal, since the relative phase can be controlled with high precision [HES+12]. As this is, in this case, only a function of a rotation in phase space, we continue to refer to the measurement quadratures as amplitude X and phase P.

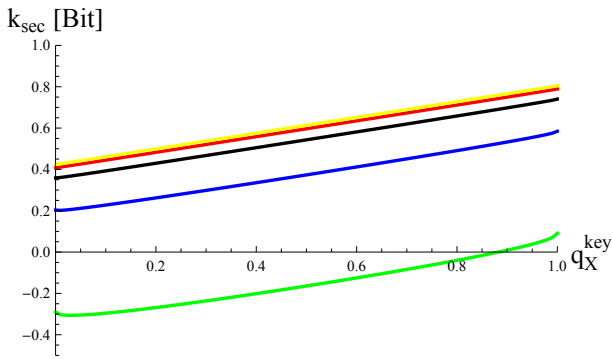

Figure 5.6.: V-class: The extractable secure key rate as a function of q_X^{key} for five different values of $N_{\text{key}} \in \{10^9, 10^8, 10^7, 10^6, 10^5\}$ (yellow, red, black, blue, green) under the assumption of the same classical post processing and direct reconciliation. One can see two important features of our asymmetric protocol. Firstly, the key rate can significantly be optimised for all N_{key} by choosing an appropriate q_X^{key} as, for example, $k_{\text{sec}}^X = 0.806$ Bit and $k_{\text{sec}}^P = 0.425$ Bit for $N_{\text{key}} = 10^9$. Secondly, a symmetric protocol cannot generate a key for $N_{\text{key}} = 10^5$.

For the covariance matrix under discussion this corresponds to an average mismatch (i.e. rotation in phase-space) of $\Delta\phi \approx 3°$ between the local oscillator and the signal beam as depicted in Figure 5.5. The Mathematica notebooks we implemented and used to compute the key rates of the collective

CV-QKD protocols allow for such a basis-mismatch.

Let us now focus on the secure key rate as a function of q_X^{key} for different N_{key} as shown in Figure 5.6. The important result is, that the rate is maximised for $q_X^{\text{key}} = 1$ for all values of N_{key}. We see furthermore that the key rate saturates at $N_{\text{key}} \geq 10^7$ for all values of q_X^{key}.

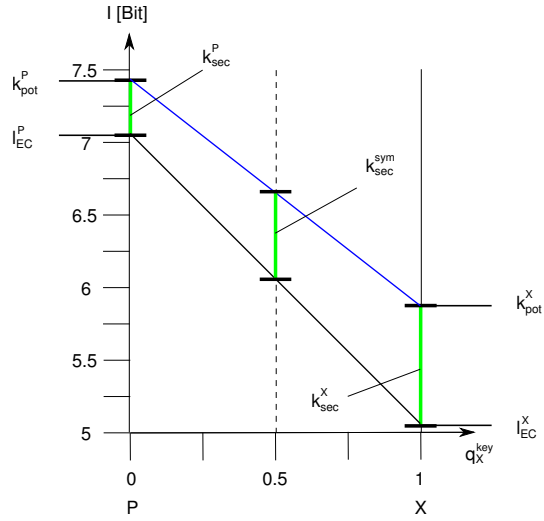

Figure 5.7.: V-class: The potential secure key rates k^i_{pot} together with the amount of disclosed bits ℓ^i_{EC} as a function of q_X^{key} assuming $N_{\text{key}} = 10^9$ and direct reconciliation. The blue line represents a convex combination of the potential key rates k^X_{pot} and k^P_{pot} and the black one the same for the ℓ^i_{EC}, respectively. The values of the security analysis correspond in both cases to the convex combination which reflects the additivity of the von Neumann entropy [LR38]. The green lines denote their difference (the secure key) for $q_X^{\text{key}} \in \{0, 0.5, 1\}$. We see that the secure key rate is maximised for $q_X^{\text{key}} = 1$ in case of the v-class state.

Note especially that $k^X_{\text{sec}} > k^{sym}_{\text{sec}} > k^P_{\text{sec}}$. This is interesting as, when looking in Table B.1, one can see that the phase quadrature is stronger correlated in terms of ρ which leads directly to a higher potential key rate of $k^P_{\text{pot}} =$

7.457 Bit for $N_{\text{key}} = 10^9$. The potential key rate of the amplitude quadrature is in contrast $k^X_{\text{pot}} = 5.874$ Bit for $N_{\text{key}} = 10^9$ which suggests to use the phase quadrature P for the key generation.

However, we use the amplitude quadrature $q_X^{\text{key}} = 1$ to generate the key. The argument is that, although the phase quadrature is stronger correlated, its conditional variance is much larger than the one of the amplitude quadrature as shown in Table B.1. The errors between the raw keys $\text{Bin}[K_A]$ and $\text{Bin}[K_B]$ and the amount of information disclosed during reconciliation ℓ_{EC} are proportional to the conditional variances. The communication cost of the non-binary reconciliation are $\ell^X_{\text{EC}} = 5.068$ Bit and $\ell^P_{\text{EC}} = 7.032$ Bit. It follows that the difference between the potential key rate k_{pot} and the disclosed information ℓ_{EC} (the secure key rate $k_{\text{sec}} = k_{\text{pot}} - \ell_{\text{EC}}$) is maximised for $q_X^{\text{key}} = 1$. We sketch and explain this behaviour in Figure 5.7.

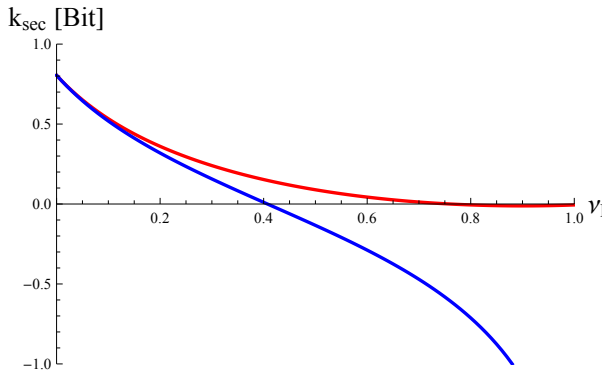

Figure 5.8.: V-class: This figure shows the extractable secure key rate as a function of the damping ν_B at Bob's side under the assumption of equal post processing for $N_{\text{key}} = 10^9$ samples and $q_X^{\text{key}} = 1$. The blue line shows the secure key rate assuming direct reconciliation and the red one shows the key rate for reverse reconciliation. The maximum damping ν_B by which the key rate remains positive is $\nu_B = 0.41$ for direct reconciliation and $\nu_B = 0.75$ for reverse reconciliation.

Figure 5.8 shows the key rate for $q_X^{\text{key}} = 1$ but different Gaussian damping for Bob and compares direct with reverse reconciliation. As Alice is assumed to hold the lab, only Bob is allowed to be remote which physically imprints

damping in his sub-space as explained in Section 3.4.3. We assume here only Gaussian damping in Bob's sub-system and describe the strength of the damping by the scalar ν_B.

In this setting, reverse reconciliation sustains more Gaussian damping before dropping below zero than direct reconciliation. This is not surprising, as Bob's sub-state naturally experiences more noise than Alice's. This renders the eavesdroppers guess about Bob's measurement outcome worse than about Alice's because it is noisier [SBPC+09]. This is reflected by the min-entropy $H_{\min}^{\varepsilon}(x_B|E)_{\omega}$ of Bob's measurement outcomes x_B conditioned on the eavesdropper E. Reverse reconciliation protocols can in general sustain more noise.

S-class setup:
We will now shortly discuss an experiment where two initially independent squeezed states are entangled on a 50:50 beam splitter which results in an entangled bipartite s-class state. Such a state is relatively symmetric when compared with an v-class state.

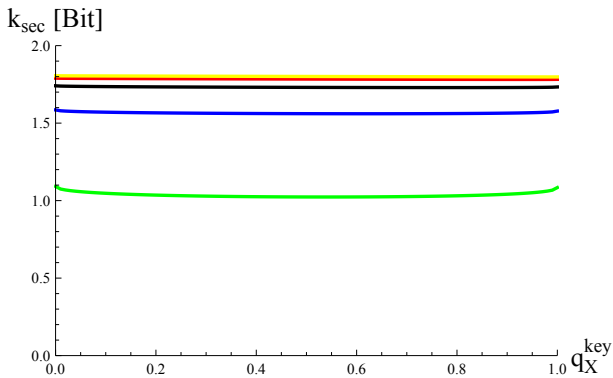

Figure 5.9.: S-class: The extractable secure key rate as a function of q_X^{key} for five different $N_{\text{key}} \in \{10^9, 10^8, 10^7, 10^6, 10^5\}$ (yellow, red, black, blue, green) under the assumption of the same classical post processing and direct reconciliation. Although the effect of q_X^{key} is very small as, for example, $k_{\text{sec}}^X = 1.799$ Bit and $k_{\text{sec}}^P = 1.807$ Bit for $N_{\text{key}} = 10^9$, the key rate can still be optimised a tiny bit for $q_X^{\text{key}} = 0$.

We refer to Section 6.2.1 for the details of the experiment and use the following covariance matrix [Ebe13]

$$\gamma_{AB} = \left(\begin{array}{cc|cc} 19.696 & (0) & 19.678 & (0) \\ (0) & 23.311 & (0) & -23.708 \\ \hline 19.678 & (0) & 19.817 & (0) \\ (0) & -23.708 & (0) & 24.314 \end{array}\right) \tag{5.13}$$

where the numbers in parenthesis have not been measured. The $Q_{\pi/4}$ quadrature, which is normally necessary for the full tomography of the state, was dropped for experimental reasons and because they can be assumed to be 10^{-2} times smaller than all the other entries of the covariance matrix.

Figure 5.9 shows the key rate of the s-class state as a function of q_X^{key} and N_{key}. The key rate saturates again at $N_{\text{key}} \geq 10^7$ but it is less sensitive to q_X^{key} than in the case of the v-class state, as shown before. Nevertheless, the key rate can still be optimised as a function of q_X^{key}.

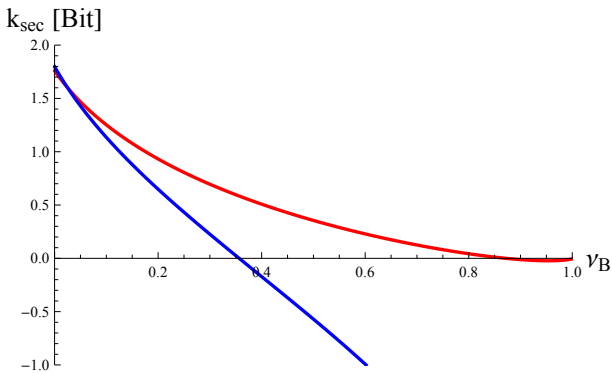

Figure 5.10.: S-class: The extractable secure key rate as a function of the damping ν_B at Bob's side under the assumption of the same classical post processing for $N_{\text{key}} = 10^9$ samples and $q_X^{\text{key}} = 0$. The blue line shows the secure key rates assuming direct and the red one assuming reverse reconciliation. The maximum damping ν_B by which the key rate remains positive is $\nu_B = 0.35$ for direct reconciliation and $\nu_B = 0.87$ for reverse reconciliation.

Figure 5.10 compares the secure key rates for direct and reverse reconcilia-

tion as a function of additional damping in Bob's subsystem and $q_X^{\text{key}} = 0$. We see again, that reverse reconciliation is more resilient to damping. Note that the key rates almost coincide for $\nu_B = 0$.

The maximum tolerable damping in this setting is higher when compared to an v-class state. This is a direct consequence of the strength of the entanglement of the states. S-class states are stronger entangled than v-class states, with comparable squeezed input. This is reflected by the Peres-Horodecki-Simon entanglement criterion as introduced in Section 3.2.1 which reveals a value of $\mathcal{E}^v\left(\gamma_{AB}\right) = 1.933$ for the v-class state and $\mathcal{E}^s\left(\gamma_{AB}\right) = 3.402$ for the s-class state.

5.4.1.3. Simulations

We now combine the runtime analysis (see Section 5.3.2) with the security analysis against collective attacks and use the parameters as presented in Table B.2 to compare the symmetric protocol with its asymmetric variant.

We focus in this section on CV-QKD protocols of family F^2_{2,T_M,T_S}. We skip the weight of measuring the $Q_{\pi/4}$ basis as it does not contribute much to the result. This is because, in contrast to the other basis, correlated measurements of Alice and Bob in this quadrature are not necessary (see Section 3.5). The results including the $Q_{\pi/4}$ quadrature are shown in the technical Appendix A.1.

We focus on $F^2_{2,T_M=1,T_S=1}$ with $\Delta T_{\text{sync}} = \text{const}$ and use the v-class covariance matrix from Equation (5.12) to compare the symmetric with the asymmetric protocol on the level of a constant runtime T_{run}. Note that we are not necessarily interested in maximising the secure key rate k_{sec} but in maximising the generated secure key $|K_{\text{sec}}|$ per run T_{run} of an setup as a function of the weight q_X^{key} ($q_P^{\text{key}} = 1 - q_X^{\text{key}}$) of the amplitude (phase) quadrature. For the computation of the secure key rate we assume non-binary LDPC reconciliation protocol with an efficiency of $\beta_{\text{EC}} = 0.9 = \text{const}$.

Since we want to simulate the whole runtime of the process, that is parameter estimation and key generation, we have to take the additional tuples for parameter estimation into account such that $q_i \neq q_i^{\text{key}}$. We discuss in this section table-top setups and assume direct reconciliation unless otherwise noted. The results of this computation are shown in Table B.9.

Let us now compare the two CV-QKD protocols[8]:

(1) Asymmetric protocol:
Let us now consider the runtime analysis of a setup using the asymmetric CV-QKD protocol.

We start with the secure key rate k_{sec} as a function of q_X^{key} for different N_{key} as shown in Figure 5.6. The key generation saturates for $N_{\text{key}} \geq 10^7$ and is maximised for $q_X^{\text{key},(1)} = 1$. We choose to generate the key from $N_{\text{key}}^{(1)} = 10^8$ correlated and synchronised samples of Alice and Bob. But we still need some additional measurements N_{pe}^j in all combinations of the quadrature measurements j to perform adequate tomography of the Gaussian state. We assume $N_{\text{pe}} = \sum_j N_{\text{pe}}^j$ in total. It follows, that although $q_X^{\text{key},(1)} = 1$ the over-all weight must be $q_X \leq 1$.

We fix $\Delta T_{\text{sync}} = \text{const}$ for the rest of the section. And we know that the determination of the over-all weight of the quadrature depends on the needs of the parameter estimation as explained in Section 4.5. Following the experiment explained in Section 5.4.1.2, at least $N_{\text{pe}}^j = 5 \cdot 10^6$ tuples of any combination j of measurements are needed for the tomography to achieve $\varepsilon_{\text{pe}} = 10^{-10}$ for the confidence set.

As the key is completely generated from the amplitude measurements, $N_P^{(1)} = 5 \cdot 10^6$ samples have to be measured by Alice and Bob together in the phase quadrature, as described by

$$\begin{aligned} N_P^{(1)} &= 5 \cdot 10^6 \\ &= N_{\text{pe}}^P \\ &= N_{\text{tot}}^{(1)} \cdot \left(q_P^{(1)}\right)^2 \\ &= N_{\text{tot}}^{(1)} \cdot \left(1 - q_X^{(1)}\right)^2, \end{aligned}$$

[8] The number in parenthesis denotes the protocol under consideration. (1) represents the asymmetric protocol and (2) it's symmetric variant.

which is the first boundary condition for this analysis. We furthermore fix the number of synchronised amplitude measurements of Alice and Bob to be

$$\begin{aligned} N_X^{(1)} &= N_{\text{key}}^{(1)} + N_{\text{pe}}^X \\ &= 10^8 + 5 \cdot 10^6 \\ &= N_{\text{tot}}^{(1)} \cdot \left(q_X^{(1)}\right)^2 \end{aligned}$$

which is the second boundary condition.

We solve this system of equations and find $q_X^{(1)} = 0.817$ with $N_{\text{tot}}^{(1)} = 1.558 \cdot 10^8$ describing the weight of the basis and the number of measurements of one participant needed to maintain the boundary conditions. Now we can use the runtime analysis from Section 5.3.2 to deduce the weight of the switching processes of one participant and arrive at

$$\begin{aligned} \widetilde{q}_X^{(1)} &= 0.634 \\ \widetilde{q}_P^{(1)} &= 0.139 \\ \widetilde{q}_{\text{sw}}^{(1)} &= 0.227. \end{aligned}$$

We now raise the analysis to the level of two participants, where each chose their measurement basis independently, according to the weights above. We know

$$\begin{aligned} N_{\text{key}}^{(1)} &= N \cdot \left(\widetilde{q}_X^{(1)}\right)^2 - N_{\text{pe}}^X = N_{\text{tot}}^{(1)} \cdot \left(q_X^{(1)}\right)^2 - N_{\text{pe}}^X \\ &= N_X^{(1)} - 5 \cdot 10^6 = 10^8 = \text{const.} \end{aligned}$$

Obeying this boundary condition we arrive at $N = 2.609 \cdot 10^8$ ($T_{\text{run}} = 2.609 \cdot 10^8 \cdot \Delta T_{\text{sync}}$), which is the total number of time steps (the runtime) of the setup.

Having all the necessary information to compute the secure key rate of the asymmetric protocol, we can now focus on the parameters of the symmetric variant.

(2) Symmetric protocol:
The basic parameters for one participant are, in this case, given by

$$\begin{aligned} q_X^{(2)} &= 0.5 \\ q_P^{(2)} &= 0.5 \\ T_{\text{run}} &= 2.609 \cdot 10^8 \cdot \Delta T_{\text{sync}} \end{aligned}$$

which allows us to compute the weight for switching using the runtime analysis as described in Section 5.3.2. We find that

$$\begin{aligned}\widetilde{q}_X^{(2)} &= \frac{1}{3}\\ \widetilde{q}_P^{(2)} &= \frac{1}{3}\\ \widetilde{q}_{\text{sw}}^{(2)} &= \frac{1}{3}\end{aligned}$$

as expected and compute

$$N_{\text{key}}^{(2)} = N \cdot \left[\left(\widetilde{q}_X^{(2)}\right)^2 + \left(\widetilde{q}_P^{(2)}\right)^2\right] - N_{\text{pe}}^X - N_{\text{pe}}^P = 0.479 \cdot 10^8$$

where the $N_{\text{pe}}^X + N_{\text{pe}}^P = 2 \cdot 5 \cdot 10^6$ account for the number of measurements disclosed during the parameter estimation.

Key rates:
Having determined the total runtime T_{run} of the setups performing the asymmetric and symmetric CV-QKD protocol, we can start with the computations of the corresponding secure key rates $k_{\text{sec}}^{(i)}$ as a function of $q_X^{\text{key},(i)}$ and $N_{\text{key}}^{(i)}$. Note, that the $N_{\text{key}}^{(i)}$ are only a function of $\tilde{q}_X^{(i)}$ as $N = 2.609 \cdot 10^8$ is fixed.

Following the security analysis as described in Section 5.4.1 we find for the asymmetric protocol for

$$\begin{aligned}q_X^{\text{key},(1)} &= 1\\ k_{\text{sec}}^{(1)} &= 0.789 \text{ Bit}\\ N_{\text{key}}^{(1)} &= 10^8\\ |K_{\text{sec}}^{(1)}| &= 0.789 \cdot 10^8 = 78.94 \text{ MBit}\end{aligned} \tag{5.14}$$

and for the symmetric protocol

$$\begin{aligned}q_X^{\text{key},(2)} &= 0.5\\ k_{\text{sec}}^{(2)} &= 0.593 \text{ Bit}\\ N_{\text{key}}^{(2)} &= 0.479 \cdot 10^8\\ |K_{\text{sec}}^{(2)}| &= 0.284 \cdot 10^8 = 28.46 \text{ MBit.}\end{aligned} \tag{5.15}$$

The common parameter used to compare the two protocols is $T_{\text{run}} = 2.609 \cdot 10^8 \cdot \Delta T_{\text{sync}}$ ($N = 2.609 \cdot 10^8$). The key generated within T_{run} of the setup with the asymmetric protocol is approximately $R_{1,2} = 2.777$ times larger than in case of its symmetric variant. Note again that we used the v-class covariance matrix which is described in Section 5.4.1.2. We discuss the results in further detail in the next section.

5.4.1.4. Discussion

We have seen, that our CV-QKD asymmetric protocol has two key benefits in comparison to its symmetric variant:

Key rate:
In the case of asymmetric states, the asymmetric protocol can (significantly) optimise the secure key rate of the setup k_{sec} as function of q_X^{key}. In realistic setups, a measured state is always at least slightly asymmetric due to experimental imperfections. We found the maximum of the secure key for $q_X^{\text{key}} = 1$.

Switching processes:
Since asymmetric protocols can always minimise the number of switching processes, more N_{key} samples can then be used for key generation per runtime T_{run} of the setup which can, in principle, increase $|K_{AB}|$ and k_{sec}. Note that the key rate of the collective protocol saturates already for $N_{\text{key}} \geq 10^7$. It follows that the secure key rate k_{sec} can, in these simulations, not be significantly increased by larger values of $N_{\text{key}} > 10^7$.

We showed in Section 5.4.1.3 a numerical analysis by comparing the asymmetric protocol with its symmetric version. Thereby we assumed for the asymmetric protocol $N_{\text{pe}}^P = 5 \cdot 10^6$ simultaneous measurements in the phase and $N_{\text{key}}^{(1)} + N_{\text{pe}}^X = 10^8 + 5 \cdot 10^6$ correlated measurements in the amplitude quadrature. We chose these values because they are experimentally feasible. If we drop the assumption of experimental feasibility and increase N_{key} (N) drastically, the asymmetric protocol becomes even more superior as $q_X \rightarrow q_X^{\text{key}}$ with $N_{\text{pe}}/N_{\text{key}} \rightarrow 0$.

S-class states provide higher key rates k_{sec} than their v-class variants with equal input squeezing. Although the key rate of such states is not very sensitive to q_X^{key} any more, fewer switching processes q_{sw} can still improve the secure key rate k_{sec} and the raw key $|K_{AB}|$ generated of one run of the setup

T_{run}.

The simulation of our asymmetric CV-QKD protocol as presented in this section performs better than its symmetric variant.

5.4.2. Security against Coherent Attacks

We learned during the analysis of the asymmetric CV-QKD protocol which is secure against collective attacks assuming $\beta_{\text{EC}} = \text{const}$, that the raw key is best generated from the quadrature resulting in the higher secure key rate.

This confinement drastically simplifies the security analysis of the asymmetric protocol providing security against most general attacks assuming direct reconciliation. The following analysis is again based on the symmetric protocol providing security against coherent attacks [FFB+14] which is described in Section 4.6.

5.4.2.1. Security Analysis

In the original security analysis [FFB+14] a uniform basis choice ($q_X^{\text{key}} = 0.5$) was assumed in order to compute the secure key $K_{\text{sec}} = K_{\text{sec}}^X \cup K_{\text{sec}}^P$, where K_{sec}^X (K_{sec}^P) denotes the secure key which is generated from the amplitude (phase) quadrature. We briefly review the arguments here to make this point more clear. The entropies which are used in the security proof are explained in Appendix A.3.

(1) Symmetric protocol:
They started with the general equation describing the secure key that can be generated from some QKD-setup

$$|K_{\text{sec}}| \leq H_{\min}^{\varepsilon}(x_A^n|E)_{\omega} - \ell_{\text{EC}}(n) - \log_2\left[\frac{1}{\varepsilon_S \varepsilon_C}\right] \tag{5.16}$$

where $n = N_{\text{key}}$ for the purpose of simplification. The task was to estimate $H_{\min}^{\varepsilon}(x_A^n|E)_{\omega}$ assuming all attacks that are allowed by quantum mechanics.

In the original analysis they started by bounding the smooth min entropy of Alice measurements in Equation 5.16 by using an uncertainty relation which allowed them to bound Alice's smooth min entropy conditioned on Eve's attack. In this step they assumed a uniform choice of the amplitude and phase quadrature measurements. By combining the monogamy of entanglement

[CKW00] with the uncertainty principle for the two complementary measurements [BFS11] they estimated Eve's information by

$$H_{\min}^{\epsilon}\left(x_A^n|E\right) \geq -n \cdot \log\left[\frac{1}{c(\delta)}\right] - H_{\max}^{\epsilon}\left(x_A^n|x_B^n\right)$$

where x_A^n (x_B^n) are the outcomes of Alice's (Bob's) amplitude and phase quadrature measurements. The function $c(\delta)$ describes the overlap of the conjugated amplitude and phase quadratures estimated for an interval of length δ as is given by

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

where $S_0^{(1)}$ represents the radial prolate spheroidal wave function of the first kind [KW10] with $\delta = \delta_X = \delta_P$. They furthermore estimated the max-entropy by

$$H_{\max}^{\epsilon}\left(x_A^n|x_B^n\right) \leq n \cdot \log\left[\gamma\left(d_0 + \mu\right)\right]$$

where

$$\gamma(t) = \left(t + \sqrt{1+t^2}\right) \cdot \left(t / \left[\sqrt{1+t^2} - 1\right]\right)^t$$

with

$$d_0 = d(x_A^{N\text{pe}}, x_B^{N\text{pe}}) = 1/k \cdot \sum_{i=1}^{N\text{pe}} |x_{A,i} - x_{B,i}| \tag{5.17}$$

which is the protocol parameter of this analysis. Note that in the above N_{pe} denotes the number of measurements used to estimate $d(x_A^{N\text{pe}}, x_B^{N\text{pe}})$. The strings x_A^n and x_B^n represent Alice's and Bob's raw keys and μ takes the statistical deviations due to finitely many measurements into account.

The secure key that can be generated from this analysis is

$$\begin{aligned} |K_{\text{sec}}| = & N_{\text{key}} \cdot \left[\log\left(\frac{1}{c(\delta)}\right) - \log\left[\gamma\left(d_0 + \mu\right)\right]\right] - \ell_{\text{EC}}\left(N_{\text{key}}\right) \\ & - \log_2\left[\frac{1}{\varepsilon_S \varepsilon_C}\right]. \end{aligned} \tag{5.18}$$

(2) Asymmetric protocol:
We apply the uncertainty relation now to the case where the key is generated from one quadrature only as already in general discussed in [TLGR14] and [BCF+13]. The quation obeying the situation is in this case

$$|K_{\text{sec}}| \leq H_{\min}^{\varepsilon}(x_{X,A}^{k}|E)_{\omega} - \ell_{\text{EC}}(k) - \log_2\left[\frac{1}{\varepsilon_S \varepsilon_C}\right]. \tag{5.19}$$

We introduce an asymmetric protocol secure against most general attacks by

$$H_{\min}^{\epsilon}\left(x_{X,A}^{k}|E\right) \geq -n \cdot \log\left(\frac{1}{c(\delta)}\right) - H_{\max}^{\epsilon}\left(x_{P,A}^{l}|x_{P,B}^{l}\right)$$

where the measurements used for the key generation $k = N_{\text{key}}$ are generated from only one quadrature (in this example the amplitude $q_X^{\text{key}} = 1$) and the secure key is estimated from the other (in this example from the phase) quadrature. The $x_{P,\{A,B\}}^{l}$ (the hypothetical key generation outcomes) are used to estimate the secure key. Note that $c(\delta)$ is the same as in the symmetric protocol presented above as it describes the overlap of the two orthogonal quadratures X and P.

Now we have to estimate $H_{\max}^{\epsilon}\left(x_{P,A}^{l}|x_{P,B}^{l}\right)$. As the setup remains the same as in the symmetric protocol, we can use the already existing security analysis of Dr. F. Furrer and write

$$H_{\max}^{\epsilon}\left(x_{P,A}^{l}|x_{P,B}^{l}\right) \leq n \cdot \log\left[\gamma\left(d_0^P + \mu\right)\right].$$

This means that the protocol parameter $d_0^P = d(x_{P,A}^{l}, x_{P,B}^{l})$ is calculated from the phase quadrature measurements only:

$$d_0^P = d(x_{P,A}^{l}, x_{P,B}^{l}) = 1/l \cdot \sum_{i=1}^{N_{\text{pe}}} |x_{P,A}^{i} - x_{P,B}^{i}|$$

with $l = N_{\text{pe}}$. Note, that the key is in this protocol strategy completely generated from the amplitude measurements where the parameter estimation of d_0^P is fully described by the phase measurements.

Following this analysis we obtain a secure key of length

$$|K_{\text{sec}}| = N_{\text{key}} \cdot \left[\log\left(\frac{1}{c(\delta)} \right) - \log\left[\gamma\left(d_0^P + \mu \right) \right] \right] - \ell_{\text{EC}}\left(N_{\text{key}} \right) - \log_2 \left[\frac{1}{\varepsilon_S \varepsilon_C} \right] \tag{5.20}$$

where $k = N_{\text{key}}$. The secure key rate is

$$k_{\text{sec}} = \frac{|K_{\text{sec}}|}{N_{\text{key}}}.$$

We furthermore identify the potential secure key rate by

$$\begin{aligned} k_{\text{pot}} &= \log\left(\frac{1}{c(\delta)} \right) - \log\left[\gamma\left(d_0^P + \mu \right) \right] - \log_2 \left[\frac{1}{\varepsilon_S \varepsilon_C} \right] / N_{\text{key}} \\ &= k_{\text{sec}} + \frac{\ell_{\text{EC}}}{N_{\text{key}}}. \end{aligned} \tag{5.21}$$

Note that this protocol strategy is different to the case where we analysed the security against collective attacks which we presented in Section 5.4.1 where we certified the security of the setup using the same quadrature from which the raw key is generated. In the case of the protocol providing security against coherent attacks we estimate the key rate from one quadrature and generate the key from the other quadrature. This protocol strategy is a consequence of using the entropic uncertainty relation in order to bound Eve's information of the raw key assuming only one quadrature for the key generation.

5.4.2.2. Results

We use in this discussion again the two covariance matrices which describe an v-class and an s-class state as introduced in Section 5.4.1.2. The parameters of the CV-QKD protocols of family F_2^2 used for the analysis in this section are presented in Table B.3. We discuss in the following table-top setups (unless otherwise noted) which use the two different bipartite Gaussian states which are characterised in Table B.1 and direct reconciliation:

V-class setup:
The Gaussian state as reconstructed in the experiment is described by

$$\gamma_{AB} = \left(\begin{array}{cc|cc} 0.541 & 0.135 & 0.459 & -0.095 \\ 0.135 & 24.633 & -0.037 & -23.293 \\ \hline 0.459 & -0.037 & 0.548 & 0.264 \\ -0.095 & -23.293 & 0.264 & 23.840 \end{array}\right). \tag{5.22}$$

The protocol parameter d_0 can be directly computed from the covariance matrix. Figure 5.11 shows the key rates as a function of the key generation samples N_{key} for an v-class state. The key rates saturate for $N_{\text{key}} \geq 10^{10}$ but the rates of the asymmetric protocol are both higher than that one of the symmetric protocol.

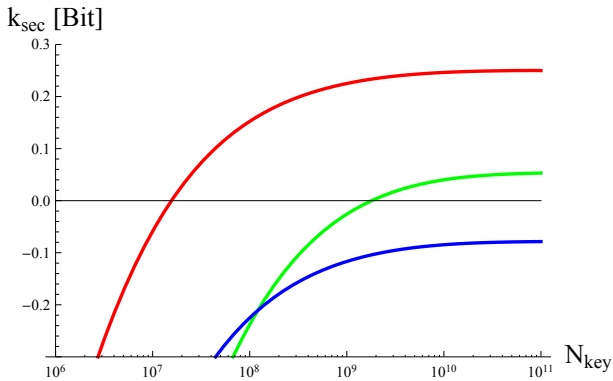

Figure 5.11.: V-Class: The key rates for $q_X^{\text{key}} = 1$ (red), $q_X^{\text{key}} = 0$ (green) and $q_{\text{sym}}^{\text{key}} = 0.5$ (blue) as a function of the measurement samples N_{key}. All key rates saturate at $N_{\text{key}} \geq 10^{10}$. Note, that the key rate for $q_{\text{sym}}^{\text{key}}$ is smaller (i.e. zero) when compared to the other two. We see that the secure key rate is optimised for $q_X^{\text{key}} = 1$ as $k_{\text{sec}}^X = 0.250$ Bit $> k_{\text{sec}}^P = 0.052$ Bit. Note furthermore that $k_{\text{sec}}^{\text{sym}} = -0.078$ Bit < 0 which means that no secure key can be generated using the symmetric protocol.

We see that the secure key rate is again optimised for $q_X^{\text{key}} = 1$ as it was also the case for the asymmetric collective protocol in Section 5.4.1.2. But the results are different in this case as $k_{\text{sec}}^X > k_{\text{sec}}^P > k_{\text{sec}}^{\text{sym}}$. The reason for $q_X^{\text{key}} = 1$ is again to be found in the different potential key rates ($k_{\text{pot}}^X = 9.370$ Bit $>$

$k^P_{\text{pot}} = 7.697$ Bit) and amounts of disclosed information ($\ell^X_{\text{EC}} = 7.447$ Bit $<$ $\ell^P_{\text{EC}} = 9.318$ Bit) during the reconciliation of the CV-QKD protocol assuming $N_{\text{key}} = 10^{10}$. Note that the potential key rates are in case of this protocol a function of the protocol parameter d_0 and not the covariance matrix γ_{AB} itself which is especially important because the protocol parameters $d^X_0 = 32.992 \cdot \delta < d^P_0 = 109.451 \cdot \delta$ are proportional to the conditional variances which are given in Table B.1. This means that the potential key rates of the quadratures are $k^X_{\text{pot}} > k^P_{\text{pot}}$ which suggests to generate the raw key from the phase quadrature $q^{\text{key}}_X = 0$ while estimating the potential key rate from the amplitude quadrature X.

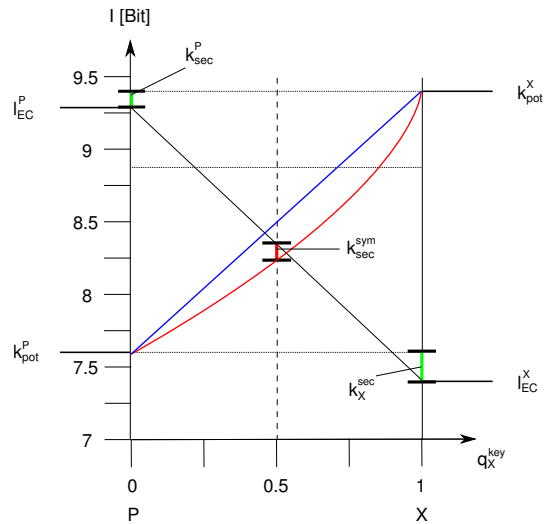

Figure 5.12.: A sketch of the potential secure key rates k^{pot}_i together with the amount of disclosed bits ℓ^{EC}_i as a function of q^{key}_X assuming $N_{\text{key}} = 10^{10}$. The blue line represents a convex combination of the potential key rates k^{pot}_X and k^{pot}_P and the black one of the ℓ^{EC}_i, respectively. The secure key rates are sketched for $q^{\text{key}}_X \in \{0, 0.5, 1\}$. The key rate for $q^{\text{key}}_X = 0.5$ deviates from the convex combination. The red line sketches a possible graph of the potential key rate as a function of q^{key}_X.

But the amount of disclosed bits when using the phase quadrature for the key generation is again, due to the corresponding conditional variances, so large, that the secure key is at best generated from the less correlated quadrature X with the smaller conditional variance. We sketch the behaviour $k_{\text{sec}}^{X} > k_{\text{sec}}^{P} > k_{\text{sec}}^{\text{sym}}$ in Figure 5.12.

S-class setup:
The covariance matrix is

$$\gamma_{AB} = \left(\begin{array}{cc|cc} 19.696 & (0) & 19.678 & (0) \\ (0) & 23.311 & (0) & -23.708 \\ \hline 19.678 & (0) & 19.817 & (0) \\ (0) & -23.708 & (0) & 24.314 \end{array}\right)$$

where the numbers in parenthesis have not been measured.

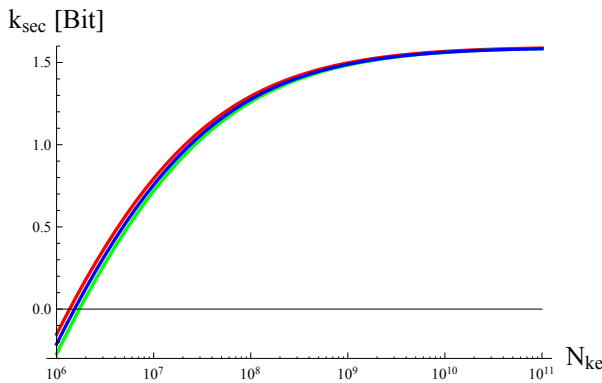

Figure 5.13.: This graph shows the key rates for $q_X^{\text{key}} = 1$ (red), $q_X^{\text{key}} = 0$ (green) and $q_{\text{sym}}^{\text{key}} = 0.5$ (blue) as a function of the measurement samples N_{key} for an s-class state. Note that, since the corresponding s-class state is highly symmetric, all the key rates almost overlap. Although we find the optimum of the secure key rate for $q_X^{\text{key}} = 1$ and $N_{\text{key}} = 10^{10}$ as $k_{\text{sec}}^{X} = 1.567$ Bit $> k_{\text{sec}}^{P} = 1.561$ Bit for $N_{\text{key}} = 10^{10}$ it can no longer be significantly increased by using the asymmetric CV-QKD protocol.

Figure 5.13 compares the secure key rates of the asymmetric protocol with

the symmetric protocol. The key rates saturate at $N_{\text{key}} \geq 10^9$ and are much less affected by q_X^{key} than in case of the v-class state, as expected. As $k_{\text{sec}}^X \approx k_{\text{sec}}^{\text{sym}} \approx k_{\text{sec}}^P$ the symmetry of the runtime analysis remains almost intact when combined with this asymmetric protocol and using an s-class state.

We compare, in Figure 5.14, the key rates of the symmetric and the asymmetric protocol for the v-class and the s-class state as a function of the damping ν_B at Bob's side. S-class states perform better than their v-class variants with equal input squeezing. Although the key rate of such states is a marginal function of q_X^{key}, fewer switching processes might still improve the key rate generated in one run of the setup T_{run}.

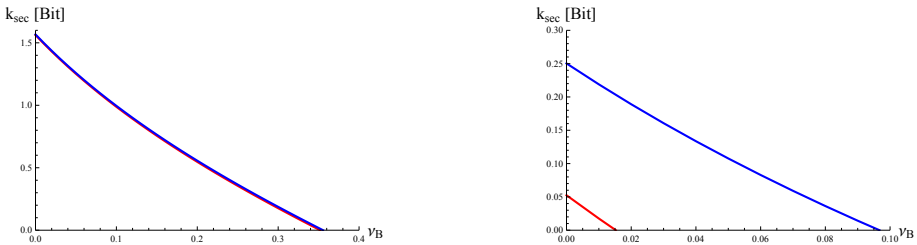

Figure 5.14.: The two plots show the key rate of the asymmetric protocol providing security against coherent attacks, as a function of the damping ν_B at Bob's side for $N_{\text{key}} = 10^{10}$. The red curve shows the key rate when the key is generated from the phase quadrature and the blue one for the amplitude quadrature, respectively. The picture on the left is generated by assuming the s-class state and the right picture on the right for the v-class state. The secure key rates are optimised for $q_X^{\text{key}} = 1$.

5.4.2.3. Simulations

We now combine the runtime analysis (see Section 5.3.2) with the security analysis against coherent attacks and use the parameters as presented in Table B.3 to compare the symmetric protocol with its asymmetric variant assuming direct reconciliation.

The results we show in this section follow the computations which are presented in Section 5.4.1.3. Hence, we give only a short version of it here and

focus mainly on the results. Remember that we discuss in this section CV-QKD protocols of family F^2_{2,T_M,T_S}. The results are summarised in Table B.10.

Let us now compare the two CV-QKD protocols[9]:

(1) Asymmetric protocol:
We now combine the runtime analysis which is presented in Section 5.3.2 with the asymmetric CV-QKD protocol providing security against coherent attacks as presented in Section 5.4.2. We focus, again, on $F_{2,T_M=1,T_S=1}$ and use the s-class covariance matrix from Equation 5.13 to compare the symmetric with the asymmetric protocol by setting the runtime $T_{\text{run}} = \text{const}$ and $\Delta T_{\text{sync}} = \text{const}$ for both protocols. For the computation of the secure key rate we assume a non-binary LDPC reconciliation with an efficiency of $\beta_{\text{EC}} = 0.9 = \text{const}$ [EMMM11, MEM12].

We have to take the additional N_{pe} tuples into account which are needed to estimate the protocol parameter d_0. Note that we have seen in Section 5.4.2.2 that the key rate is optimised for $q_X^{\text{key},(1)} = 1$. We set $N_{\text{key}}^{(1)} = 10^8$, assume $N_{\text{pe}} = 3 \cdot 10^7$ [GHD+14] and evaluate the runtime analysis of the asymmetric protocol by assuming N_{pe} correlated measurements in the phase quadrature which are all used to estimate the protocol parameter d_0 ($q_X^{\text{key},(1)} = 1$). That is

$$\begin{aligned} N_P^{(1)} &= N_{\text{pe}} = 3 \cdot 10^7 \\ &= N_{\text{tot}}^{(1)} \cdot \left(q_P^{(1)}\right)^2 = N_{\text{tot}}^{(1)} \cdot \left(1 - q_X^{(1)}\right)^2 \end{aligned}$$

which is the first boundary condition for this analysis. We furthermore fix the number of synchronised amplitude measurements of Alice and Bob which are all used to generated the raw key to be

$$\begin{aligned} N_X^{(1)} &= N_{\text{key}}^{(1)} = 10^8 \\ &= N_{\text{tot}}^{(1)} \cdot \left(q_X^{(1)}\right)^2 \end{aligned}$$

which is the second boundary condition. Note, that we do not have to take additional measurements for the parameter estimation in this quadrature into account because the parameter estimation only requires amplitude measurement tuples in this case.

[9] The number in parenthesis denotes the protocol under consideration. (1) represents the asymmetric protocol and (2) it's symmetric variant.

The weights with switching are

$$\begin{aligned}\widetilde{q}_X^{(1)} &= 0.444\\ \widetilde{q}_P^{(1)} &= 0.243\\ \widetilde{q}_{\text{sw}}^{(1)} &= 0.313.\end{aligned}$$

Let us raise the analysis to the level of two participants where each chose his measurement basis independently by the weights above. We know that in this case

$$N_{\text{key}}^{(1)} = N \cdot \left(\widetilde{q}_X^{(1)}\right)^2 = 10^8 = \text{const.}$$

Obeying this boundary condition we arrive at $N = 5.087 \cdot 10^8$ ($T_{\text{run}} = 5.087 \cdot 10^8 \cdot \Delta T_{\text{sync}}$) which is the total amount of time steps (runtime) of the system.

(2) Symmetric protocol:
Having all the necessary information to compute the secure key rate of the asymmetric protocol we now focus on the parameters of the symmetric variant. The basic parameters for one participant are in this case

$$\begin{aligned}q_X^{(2)} &= 0.5\\ q_P^{(2)} &= 0.5\\ T_{\text{run}} &= 5.087 \cdot 10^8 \cdot \Delta T_{\text{sync}}\end{aligned}$$

which allows us to directly compute the weights with switching by the runtime analysis. We find

$$\begin{aligned}\widetilde{q}_X^{(2)} &= \frac{1}{3}\\ \widetilde{q}_P^{(2)} &= \frac{1}{3}\\ \widetilde{q}_{\text{sw}}^{(2)} &= \frac{1}{3}\end{aligned}$$

and compute

$$N_{\text{key}}^{(2)} = N \cdot \left[\left(\widetilde{q}_X^{(2)}\right)^2 + \left(\widetilde{q}_P^{(2)}\right)^2\right] - N_{\text{pe}} = 0.830 \cdot 10^8$$

where the $N_{\text{pe}} = 3 \cdot 10^7$ tuples are used for the parameter estimation of d_0.

Key rates:
Having determined the total runtime T_{run} of the setups performing the asymmetric and symmetric CV-QKD protocol, we can start with the computations of the corresponding secure key rates $k_{\text{sec}}^{(i)}$ as a function of $N_{\text{key}}^{(i)}$.

Following the security analysis as described in Section 5.3.2 we find for the asymmetric protocol

$$\begin{aligned} q_X^{\text{key},(1)} &= 1 \\ k_{\text{sec}}^{(1)} &= 0.8917 \text{ Bit} \\ N_{\text{key}}^{(1)} &= 10^8 \\ |K_{\text{sec}}^{(1)}| &= 0.8917 \cdot 10^8 = 89.17 \text{ MBit} \end{aligned} \tag{5.23}$$

and for its symmetric variant

$$\begin{aligned} q_X^{\text{key},(2)} &= 0.5 \\ k_{\text{sec}}^{(2)} &= 0.7919 \text{ Bit} \\ N_{\text{key}}^{(2)} &= 0.8305 \cdot 10^8 \\ |K_{\text{sec}}^{(2)}| &= 0.6577 \cdot 10^8 = 65.77 \text{ MBit.} \end{aligned} \tag{5.24}$$

The key generated within T_{run} of the system is, for the asymmetric protocol, approximately $R_{1,2} = 1.356$ times larger than in case of its symmetric variant. We discuss the results in further detail in the next section.

5.4.2.4. Discussion

We showed in Section 5.4.2.3 a simulation by comparing the asymmetric protocol with its symmetric counterpart. We started by assuming for the asymmetric protocol $N_{\text{pe}} = 3 \cdot 10^7$ simultaneous measurements in the amplitude and $N_{\text{key}} = 10^8$ simultaneous measurements in the phase quadrature and found a total number of synchronised time steps of $N = 5.087 \cdot 10^8 \cdot \Delta T_{\text{sync}}$. We chose these values, because they are experimentally feasible.

We have shown that the asymmetric protocol which provides security against coherent attacks has two key benefits when being compared with its symmetric variant:

Key rate:
In the case of asymmetric states, the asymmetric protocol can optimise the secure key rate of the setup as a function of q_X^{key} for constant N_{key}. If the state is highly symmetric, the key rate cannot be significantly optimised by q_X^{key} any more like it is the case of the s-class state used in this simulations. The secure key is maximised when being generated from the amplitude quadrature $q_X^{\text{key}} = 1$.

Switching processes:
As asymmetric protocols always minimise the number of switching processes $\tilde{q}_{sw}$, more N_{key} samples can be used for key generation per runtime T_{run} of the setup which increases $|K_{AB}|$. The additional key generation samples increase the key rate k_{sec} of the setups as it saturates above $10^{10} > N_{\text{key}}$.

The reason for the small ratio[10] between the protocols is that the weights of the asymmetric protocol with switching are similar to the weights of the symmetric protocol. This is a direct consequence of the $N_{\text{pe}} = 3 \cdot 10^7$ tuples which are used to estimate the protocol parameter, the number of key generation samples $N_{\text{key}} = 10^8$ and the protocol strategy.

S-class states achieve higher key rates than their v-class variants with equal input squeezing. Although the key rate of such states depends only weakly on q_X^{key}, fewer switching processes still increase $|K_{AB}|$ and k_{sec} generated in one run of the setup T_{run}, i.e. the time the experiment is assumed to be stable at minimum. The simulations of our asymmetric CV-QKD protocol as presented in this section, perform better than their symmetric variant.

The ratio between the symmetric and the asymmetric CV-QKD protocols $R_{1,2} = 1.356$ will increase if $N > 5.087 \cdot 10^8$ while maintaining $N_{\text{pe}} = 3 \cdot 10^7$ which puts additional constraints on the experimental realisation because the longer the runtime T_{run} of the setup has to be, the more accurate it has to be set up. We chose the above values due to experimental feasibility and for the reason of good comparability with the other protocols presented in this thesis.

[10] The reader may compare these results with the simulation of the protocols providing security against collective attacks in Section 5.4.1.3.

5.5. Analysis of Experimental Realisations

In this section we discuss experimental setups assuming a remote Bob and analyse them theoretically using the asymmetric CV-QKD protocols presented above. We use the covariance matrices of the two table-top experiments (v-class state from Equation 5.12 and s-class state from Equation 5.13) as a starting point and extend the knowledge to situations which have not been experimentally realised yet.

We focus in this chapter explicitly on non-table-top experiments with Alice, holding the lab, and Bob being remote. Hence the state which is sent to Bob experiences some interactions with the medium in which it propagates, which is modelled by Gaussian damping (see Section 3.4.3) and phase noise (see Section 3.4.6). It follows, that the local distributions of Alice and Bob are different, which has to be taken into account during the key generation. We circumvent this problem of the key generation by scaling the outcomes of Alice and Bob as described in Section 6.3.7.1.

At first we emphasise an experimental solution to the problem of phase noise in Bob's fibre when executing the protocol providing security against collective attacks. In Section 5.5.2 we discuss the propagation through a fibre and show results for the collective and the coherent protocol.

5.5.1. Phase Noise

In this section we emphasise an way to experimentally circumvent the problem of phase noise which is described in [Gni14] when executing the CV-QKD protocol providing security against collective attacks. First we shortly remind the reader of the effect of phase noise as described in Section 3.4.6 and then we describe its importance in the case of the protocol providing security against collective attacks.

Certain effects between the light fields of the signal and the local oscillator can induce a time-dependent mismatch in the relative phase between them. The mismatch could be influenced by, for example, pressure on the fibre in use for the distribution of the signal.

The problem is that phase noise renders Bob's state to be non-Gaussian as already shown in Section 3.11. This problem has a special meaning as we have to assume that the state can be fully described by a covariance matrix (Gaussian state) when executing the collective CV-QKD protocol. If this as-

sumption is not fulfilled, the CV-QKD protocol providing security against collective attacks is compromised[11]. The problem is that there exists no information theoretical analysis of phase noise for finitely many measurements. But there exist experimental solutions to this problem one of which we will we describe now.

We encode the signal beam and the local oscillator in orthogonal polarisations which allows these two to propagate through the same space-time domain to circumvent the problem of phase noise. Note that the signal beam is already polarised by the composition of the source of the squeezed states as described in Section 3.4.1. In contrary the local oscillator is prepared in the orthogonal polarisation using a polarisation filter. The two light fields are now sent through the same space time domain (the fibre).

Note that the time-dependent disturbance imprint no longer results in phase-noise, as the phase-difference between the signal and the local oscillator is maintained. In this setup phase noise changes the polarisations of both beams identically.

The signal and the local oscillator are distinguished at the receiver. We refer to [Gni14] for the details of the experimental realisation. Note that the additional experimental complexity leads to Gaussian damping. In this sense, we circumvent phase-noise by the cost of more Gaussian damping. We will not go into further details at this point, as it was only our aim to emphasise the experimental solution.

5.5.2. Remote Bob (Fibre)

We discuss in this section a setup which uses a fibre (see Section 3.4.3) to send the signal from Alice to Bob. As we use entangled fields of light with a wavelength of 1550 nm to distribute the raw keys we can use standard-telecommunication fibres which have an absorption-minimum for this wavelength. This allows us to directly use existing telecommunication architecture. We are interested in the maximum achievable distance at which a secure key can be generated from the setup.

We focus for the computation of the secure key on the asymmetric CV-QKD protocols providing security against collective or coherent attacks as described

[11] Note that phase noise is naturally considered in the protocol providing security against coherent attacks, as it allows for all effects (and attacks) which are possible by quantum mechanics.

during this chapter. Note that the asymmetric protocol assuming coherent attacks is only applicable in a setting with direct reconciliation. The secure key rates as shown in the Figures 5.15 and 5.16 are computed by assuming two coupling processes and propagation through a fibre in between, as described in Section 3.4.4.

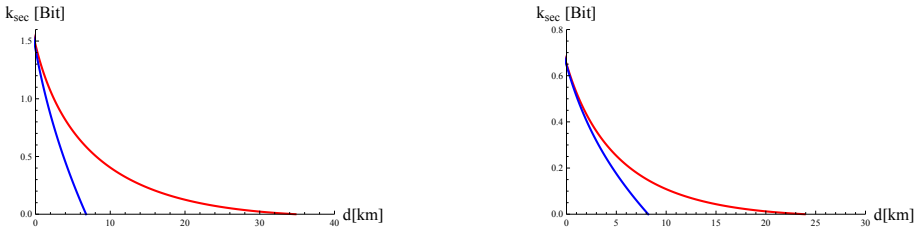

Figure 5.15.: The two plots show the key rate of the asymmetric protocol providing security against collective attacks as a function of the distance in d[km] at Bob's side for direct (red) and reverse (blue) reconciliation, $q_X^{\text{key}} = 1$ and $N_{\text{key}} = 10^8$. The picture on the right is generated by assuming the v-class and the left picture assuming the s-class state. The additional parameters for the computation of the key rates are taken from Table B.2.

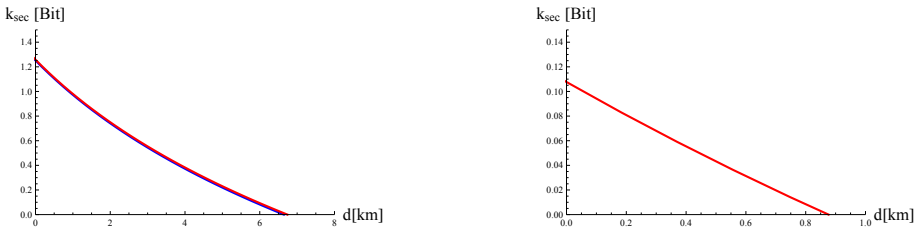

Figure 5.16.: The plot shows the key rate of the asymmetric protocol providing security against coherent attacks as a function of the distance d[km] at Bob's side for direct reconciliation, $q_X^{\text{key}} = 1$ and $N_{\text{key}} = 10^{10}$. The blue curve shows the key rate when the key is generated from the phase quadrature and the red one for the amplitude quadrature respectively. The picture on the left is generated by assuming the s-class state and the picture on the right assuming the v-class state. The additional parameters for the computation of the key rates are taken from Table B.3.

The CV-QKD protocol providing security against coherent attacks allows at the most for 6.5 km propagation in fibre for $N_{\text{key}} = 10^{10}$ key generation samples. This is experimentally very involved as $N \geq N_{\text{key}}$ time steps can easily exceed the stable runtime of the experiments under consideration. Note that this protocol provides higher security than the protocol which is secure against collective attacks and is thus less resilient to noise which is the reason for these circumstances. Furthermore, it can only be used in combination with direct reconciliation which again decreases the secure key rate. This can be seen when comparing the results of this protocol with the graph where the collective key rate is plotted for direct and reverse reconciliation.

The collective protocol with reverse reconciliation performs better than its variant with direct reconciliation allowing for a propagation through at the most 33 km of fibre. Remember that the collective protocol requires the state to be Gaussian which might not be the case as we already discussed in Section 3.4.6. We emphasised in Section 5.5.1 a work-around to this problem which maintains the Gaussianity of the bipartite state even when phase noise is present in the fibre at the cost of a higher Gaussian damping. Note again that the protocol providing security against coherent attacks considers all attacks that are allowed by quantum mechanics and does not require the state to be Gaussian. Hence the security of the protocol can not be compromised by phase noise but its key rate is, of course, reduced by this effect.

5.6. Discussion and Outlook

We rewrote the symmetric CV-QKD protocols providing security against collective and coherent attacks of Dr. F. Furrer [FFB+14] to allow for asymmetric basis choice and combined them in this chapter with a full runtime analysis of the setups. We showed, that the key is always best generated from only one quadrature (i.e. the quadrature providing a higher secure key rate) if $\beta_{\text{EC}} = \text{const}$ which is an idealised assumption. In Appendix A.2 we combined the asymmetric protocols with a more realistic model of a reconciliation scheme with $\beta_{\text{EC}} \neq \text{const}$ and show that it is sometimes better to generate the key from a mixture of the basis. A proper model of the reconciliation scheme used to correct the errors should always be applied when analysing the performance of QKD protocols. We discuss a new reconciliation scheme which is designed for the CV-QKD protocols which we discussed in this chapter in the next chapter 6.

Asymmetric protocols allow to generate a secure key in parameters ranges

where a symmetric CV-QKD protocol can not generate a key at all. They additionally allow to optimise the amount of key generation samples N_{key} in one run T_{run} of the experiment which increases the key rate due to the finite size effects of the security analysis. The simulations showed that the asymmetric CV-QKD protocols of family F^2_{2,T_M,T_S} optimised $|K_{\text{sec}}|$ (and k_{sec}) significantly.

Note especially, that the proposed runtime analysis of QKD-protocols represents furthermore a good certification method which can be used to compare different experimental realisations theoretically.

The performance of the runtime protocols of the family F^2_{2,T_M,T_S} in experiment depends heavily on T_M and T_S. It is possible to arrive at $T_S \approx 0$ by using two detectors together with a perfect redirection of the state which would call for additional technical resources. But even in this case, asymmetric protocols are, for certain parameter regions, superior to comparable symmetric protocols with perfect switching as shown in Section 5.3.3. We thus propose to implement experimental realisations which allow for a runtime protocol of family F^2_{2,T_M,T_S} and suggest to combine it with an asymmetric QKD protocol.

We showed that a local urban fibre-based QKD architecture is possible. Optimising the asymmetric coherent or collective protocol using the runtime analysis and s-class states allows for distances up to 33 km when using the collective protocol and 6.5 km when using the coherent protocol which is sufficient for an urban QKD network. If we compare these results with the distances which are possible using certain DV-QKD setups like, for example, satellite-based BB84 QKD [BMSH$^+$13] or free-space BB84 QKD [UTSM$^+$07] (144 km) we see that DV-QKD performs still better than the CV-QKD (asymmetric) protocols we analysed in this thesis.

Note that there is progress in the field of CV-QKD which we did not cover in this thesis. Dr. F. Furrer developed a CV-QKD protocol which is secure against coherent attacks under reverse reconciliation which allows for a maximum distance of 16 km in a fibre. The maximum distance of CV-QKD setups can be improved by inventing new security proof techniques and highly efficient reconciliation methods. We will discuss an efficient reconciliation scheme which is especially designed for the CV-QKD protocols which we analyse in this thesis in the next chapter.

6. Key Generation

6.1. Overview and Contributions

First we discuss an experiment in which a key secure against collective attacks was generated using standard binary LDPC reconciliation in Section 6.2. We use this example to motivate our new hybrid reconciliation procedure which we describe in this chapter from Section 6.3 onwards. Note that similar ideas (sliced reconciliation) have already been proposed for binary-LDPC [VACC06].

The structure of the new hybrid reconciliation scheme is specially designed for the Gaussian QKD protocols which are described in Chapter 5. This chapter is thus a contribution to the generation of an actual finite secure key. We show how the characteristics of the Gaussian regime can be exploited to increase the efficiency of standard reconciliation schemes.

The new hybrid reconciliation algorithm we propose is based on one-way communication and is divided into two steps. The first step exploits the Gaussian character of the errors and the second step corrects the errors left by the first step as explained in Section 6.3.1. We provide a basic analytic description and a full numerical simulation of the analysis of the first step in the following sections. This allows us to analyse the communication cost of the second step, by assuming non-binary LDPC reconciliation, as a function of the results of the first step as we show in Section 6.3.5. We continue in Section 6.3.6 by explaining the usage of the new hybrid reconciliation in an experiment where a key was generated which is secure against coherent attacks.

The chapter concludes with a detailed technical analysis of the characteristics of the hybrid reconciliation in Section 6.3.7 and a discussion.

6.2. Motivation

We discuss an experiment in which we used binary reconciliation to generate a key which is secure against collective attacks. Note that the key generation

protocol is the same for the protocol providing security against coherent attacks. We use this example to introduce the notation of this chapter, to explain the key generation in more detail and to motivate the hybrid reconciliation we propose in this chapter.

6.2.1. Experiment Secure Against Collective Attacks

We start with an experiment which was realised as part of the collaboration *Crypto on Campus* [Ebe13]. An s-class state was used in that experiment to extract a secure key using the symmetric CV-QKD protocol which provides security against collective attacks. We shortly review the CV-QKD protocol as explained in Section 4.5 and especially focus on the key generation (see Section 4.4) and the reconciliation (as described in Section 4.7). Note that the runtime setup of the experiment is member of $F^2_{2,T_{MS}}$ as explained in Section 5.3.1.

We begin with the basics of the table top experiment from which the raw key was generated. The two sources emitted squeezed states with $\mathrm{sqz}_1 = 10.3$ dB, $\mathrm{asqz}_1 = 14.9$ dB and $\mathrm{sqz}_2 = 10.9$ dB, $\mathrm{asqz}_2 = 15.3$ dB (see Section 3.4.1). The covariance matrix, as measured in the experiment by homodyne detection, reads[1]

$$\gamma_{AB} = \left(\begin{array}{cc|cc} 19.696 & (0) & -19.678 & (0) \\ (0) & 23.311 & (0) & 23.708 \\ \hline -19.678 & (0) & 19.817 & (0) \\ (0) & 23.708 & (0) & 24.314 \end{array}\right).$$

The important characteristics of the state are given in Table B.1. The remaining parameters of the symmetric protocol secure against collective attacks are given in Table B.5.

To generate a secure key from the setup, we have to perform classical post processing. As the experiment was realised on one table (table-top experiment) we chose to use direct reconciliation to correct the errors in Bob's raw key. Note again that we used standard binary LDPC to correct the errors in the raw keys of Alice and Bob after mapping their partitioned samples to the bit sequences. In other words, we corrected the errors on the level of $\mathrm{Bit}[\mathrm{Bin}[K_{AB}]]$. We used a key generation alphabet of size $|\mathcal{GF}(2^d)| = |\chi_{\mathrm{KG}}| = 2^d$ with $d = 6$ such that it can later be easily mapped to χ_{Bit}.

[1] The values in parenthesis were not determined. We refer to [Ebe13] for further information about how the covariance matrix was reconstructed.

We know that Alice's and Bob's synchronised key generation samples $K_{AB} = \{\{x_{A,i}, x_{B,i}\}\}$ stem from them both measuring the amplitude or the phase quadrature of the beam via homodyne detection with weight $q_X^{\text{key}} = 0.5$ ($q_P^{\text{key}} = 0.5$). We recall here shortly the key generation grid

$$G_{\text{KG}} = \{I_1, I_2, \ldots, I_{64}\} = \{\{-\alpha, -\alpha+\delta\}, \ldots, \{\alpha-\delta, \alpha\}\}$$

which is defined by the spacing δ and the cut-off parameter α. The size of the key generation alphabet induced by the grid is chosen to be $|\chi_{\text{KG}}| = 2 \cdot \alpha/\delta$. We write the partitioned correlated samples as $\text{Bin}[K_A]$ ($\text{Bin}[K_B]$) denoting Alice's (Bob's) raw key.

Let us write the mapping from Alice's and Bob's partitioned synchronised measurement samples

$$\{I_i\}_j = \text{Bin}[\{K_A\}_j] \in \chi_{\text{KG}} \quad \forall j \in \{1, 2, ..., N_{\text{key}}\}$$
$$\{I_k\}_j = \text{Bin}[\{K_B\}_j] \in \chi_{\text{KG}} \quad \forall j \in \{1, 2, ..., N_{\text{key}}\}$$

to the bit sequences

$$\left\{\chi_i^{\text{Bit}}\right\}_j = \text{Bit}\left[\{I_i\}_j\right] \in \chi_{\text{Bit}} \quad \forall j \in \{1, 2, ..., N_{\text{key}}\}$$
$$\left\{\chi_k^{\text{Bit}}\right\}_j = \text{Bit}\left[\{I_k\}_j\right] \in \chi_{\text{Bit}} \quad \forall j \in \{1, 2, ..., N_{\text{key}}\}$$

with $i, k \in \{1, 2, ..., |\chi_{\text{KG}}|\}$. The mapping must fulfill the following restriction to be optimal:

Hamming distance:
If Alice and Bob measure in neighbouring partitions $\{I_i\}_j$ and $\{I_{k=i+1}\}_j$, the distance between their alphabet elements should be equal to the Hamming distance of the corresponding bit sequences $\left\{\chi_i^{\text{Bit}}\right\}_j$ and $\left\{\chi_{i+1}^{\text{Bit}}\right\}_j$:

$$\left|\text{mod}_2\left[\chi_i^{\text{Bit}} + \chi_{i+1}^{\text{Bit}}\right]\right| \stackrel{!}{=} \left|I_i - I_{i+1}\right| = 1 \quad \forall_{i \in \{1,2,...,|\chi_{\text{KG}}|-1\}}.$$

This minimises the bit error rate (BER) of the resulting raw keys of Alice and Bob. This restriction is important as the number of bits disclosed within the reconciliation step is proportional to the BER. By minimising the BER we minimise the communication cost of the binary LDPC reconciliation. The

restriction is fulfilled by using the so called Gray code construction [Gra53] over $\mathcal{GF}(2^d)$.

We present here a typical Gray code of dimension $d = 2$

$$\chi_{\text{Bit}} = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$$

which fulfils the restriction discussed above (see Figure 6.1). Remember that during the process of the key generation Bob's raw key inherits the errors which stem from the Gaussian correlation function as is described in Section 4.4.1.

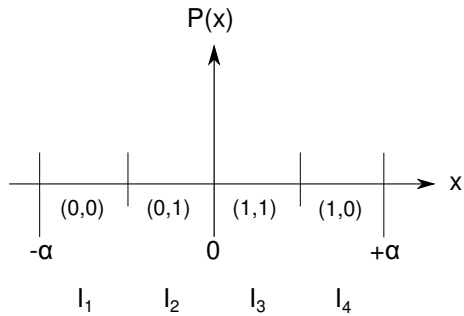

Figure 6.1.: A Gray code construction for $\mathcal{GF}(2^2)$ in phase space. The BER is minimised with respect to the alphabet samples which are measured by Alice and Bob.

For the experiment we chose $d = 6$ and found a positive secure key by omitting the alphabet elements of Alice and Bob via post selection of the partitions 27, 29, 31, 33, 35 and 37 as described in Section 4.3. This decreased the BER to a level where the amount of disclosed bits during the reconciliation was small enough to allow for a positive secure key after privacy amplification.

Although a larger key generation alphabet $|\chi_{\text{KG}}|$ would lead to a smaller spacing $\delta = 2 \cdot \alpha / |\chi_{\text{KG}}|$ and thus to a higher potential secure key rate k_{pot}, the resulting additional errors in the raw key would require too many additional bits to be disclosed during the binary reconciliation, resulting in a secure key rate of zero for $d > 6$. This effect follows directly from the usage of binary LDPC reconciliation, which has the disadvantage that it operates bit-wise on

possibly correlated bits. In this setup $d = 6$ bits are generated from one measurement. In this sense binary reconciliation does not make use of the correlation between the six bits of one measurement which renders its performance less efficient for increasing $|\chi_{\mathrm{KG}}|$. Note that this is not the case when using non-binary reconciliation which operates directly on the key generation alphabet instead as we will show later.

The software for the classical post processing (i.e. the reconciliation) of the raw keys of Alice $\mathrm{Bit}[\mathrm{Bin}[K_A]]$ and Bob $\mathrm{Bit}[\mathrm{Bin}[K_B]]$ was written by Dr. C. Pacher from the *Austrian Institute of Technology*. The size of the raw key is $|K_A| = |K_B| = 1.15 \cdot 10^8$ with a reduction rate of $k_{\mathrm{sec}} = k_{\mathrm{pot}} - \ell_{\mathrm{EC}}\left(N_{\mathrm{key}}\right)/N_{\mathrm{key}} = 0.102$ Bit (during privacy amplification) resulting in

$$|K_{\mathrm{sec}}^{\mathrm{Bit}}| = 11.948 \text{ MBit}$$

which is equal to ≈ 1.494 MByte secure key which could be extracted from the experimental outcomes.

The efficiency of the binary LDPC used to reconcile the raw key is $\beta_{\mathrm{EC}} = 0.964$ when normalised to the analytic estimation of binary reconciliation. But when we compare the result to perfect non-binary reconciliation the implementation has an efficiency of only $\beta_{\mathrm{EC}} = 0.440$. This indicates that a non-binary reconciliation on the level of χ_{KG} with efficiency $\beta_{\mathrm{EC}} = 0.9$ would disclose less information $\ell_{\mathrm{EC}}\left(N_{\mathrm{key}}\right)$, which would increase the secure key rate $k_{\mathrm{sec}} = k_{\mathrm{pot}} - \ell_{\mathrm{EC}}\left(N_{\mathrm{key}}\right)/N_{\mathrm{key}}$ significantly.

6.3. Hybrid Reconciliation

Analysing the key generation described in Section 6.2.1 for possible optimisations we learned that many problems can be solved by just using non-binary-LDPC reconciliation on $\mathrm{Bin}[K_{AB}]$ instead of $\mathrm{Bit}[\mathrm{Bin}[K_{AB}]]$. This means that the partitioned measurement samples should ideally be corrected before they are mapped to their bit sequences. This decreases the communication cost within the classical reconciliation drastically.

The motivation of the new hybrid reconciliation we propose in this chapter is to increase the efficiency and decrease the computational complexity of the reconciliation scheme [DF07] by exploiting the Gaussian character of the errors in the partitioned outcomes of Alice and Bob. We introduce two independent steps to achieve this task. This is why we refer to this reconciliation scheme as *hybrid reconciliation*.

6.3.1. General Description

Here we sketch the hybrid reconciliation protocol which is customised for the CV-QKD protocols of Section 5.4. We do not have to make any assumptions about the security level (collective or coherent) as the key generation is the same in both cases as described in Section 4.4. We detail the two steps of the hybrid reconciliation in this section.

The idea of the first step of the hybrid reconciliation scheme is to exploit the fact that the outcomes of Alice and Bob are strongly correlated in the sense that if Bob measures some value $x_{B,i}$, Alice's conditioned state is described by Equation 4.7. Bob uses this knowledge about the conditioned state and his outcome to estimate Alice's raw key element. A second reconciliation step is needed if this estimation does not correct all the errors between Alice and Bob's partitioned raw key elements.

We describe the two steps of the hybrid reconciliation by focusing on one quadrature alone. The other quadrature can implemented analogously.

6.3.1.1. Step 1

We have knowledge about the *origin of noise* (see Section 4.4.1) due to which Bob's key elements differ from the reference (Alice). As Alice represents the reference in direct reconciliation, she sends Bob some information about her outcome. Bob uses this information in the estimation of the first step to reconcile his raw key element using his knowledge about the origin of noise (conditional probability) and his actual measurement outcome. As the noise is described by a Gaussian distribution around Bob's measurement outcome, different partitions have different probabilities to be measured by Alice according to her conditional state (see Figure 6.2). Note that this is, at this level, a function of only the distance of their (partitioned) measurement samples. The size of the key generation alphabet used for the partitioning is $|\chi_{\mathrm{KG}}|$. We now introduce two additional alphabets χ_1 and χ_2 such that

$$|\chi_{\mathrm{KG}}| = |\chi_1| \cdot |\chi_2|.$$

We combine the alphabets such that $\chi_1 = \{1, 2, ...|\chi_1|\}$ represents a coarse graining of χ_{KG} with $\chi_2 = \{1, 2, ...|\chi_2|\}$ enumerating the different elements of χ_{KG} lying in every of those coarse grained partitions as explained in Figure 6.3.

We can now write every partitioned measurement outcome of Alice and Bob in $\mathrm{Bin}[K_{AB}]$ as

$$\{\mathrm{Bin}[K_A]\}_i = \alpha_{A,i} + (\beta_{A,i} - 1) \cdot |\chi_2|$$
$$\{\mathrm{Bin}[K_B]\}_i = \alpha_{B,i} + (\beta_{B,i} - 1) \cdot |\chi_2|$$

with $\alpha_{j,i} \in \chi_2$ and $\beta_{j,i} \in \chi_1$.

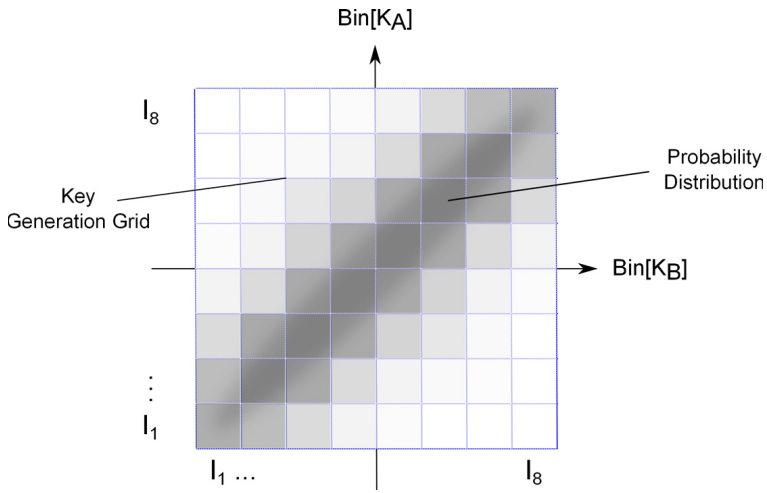

Figure 6.2.: This figure shows all combinations of Alice's and Bob's partitioned alphabet elements $\mathrm{Bin}[K_{AB}]$. The probability of measuring a specific combination is coded in the levels of grey of the corresponding box (the darker, the more probable).

For this decomposition Alice and Bob both do the following computations

$$\alpha_{j,i} = \mathrm{mod}_{|\chi_2|}\left[\{\mathrm{Bin}[K_j]\}_i\right] \in \chi_2$$
$$\beta_{j,i} = \frac{\{\mathrm{Bin}[K_j]\}_i - \mathrm{mod}_{|\chi_2|}\left[\{\mathrm{Bin}[K_j]\}_i\right]}{|\chi_2|} + 1 \in \chi_1$$

with $j \in \{A, B\}$ for all $i \in \{1, 2, ..., N_{\mathrm{key}}\}$ samples.

The main ingredient of our idea is that Alice communicates every $\alpha_{A,i}$ subsequently to Bob over the authenticated classical channel. As this is one way

classical communication, the first step of the hybrid reconciliation fulfils the requirements of direct reconciliation. Bob corrects his noisy variable $\beta_{B,i}$ sample-wise using the following maximum likelihood estimator

$$\widetilde{\beta}_{B,i} = \max_{\beta_{B,i}} \left[\mathcal{P}\left(\beta_{B,i} | \alpha_{A,i}, \alpha_{B,i}, \beta_{B,i}\right) \right], \tag{6.1}$$

which exploits the knowledge of the conditional Gaussian distribution function. Finally Bob replaces his $\alpha_{B,i}$ by setting $\alpha_{B,i} = \alpha_{A,i}$. Note that the estimator is especially designed to correct all the noise in $\alpha_{j,i}$ and to use the knowledge about the origin of noise (conditional probability) to additionally correct some noise in $\beta_{j,i}$. We discuss two maximum likelihood estimators (the simple and the extended estimator) in Section 6.3.3.

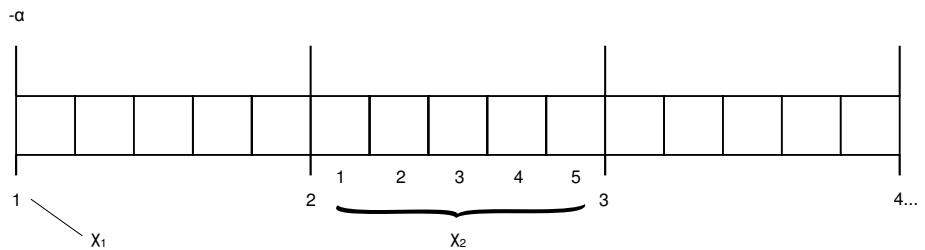

Figure 6.3.: The hybrid reconciliation ansatz. In this example the key generation grid G_{KG} is divided into two other grids which correspond to the alphabets χ_1 and χ_2. The specific arrangement allows for a unique description of Alice's and Bob's outcome as linear function of the elements of the two additional alphabets.

We rewrite Bob's partitioned measurement outcomes after the first step as

$$\{\mathrm{Bin}[K_B]\}_i = \alpha_{A,i} + \left(\widetilde{\beta}_{B,i} - 1\right) \cdot |\chi_2|$$

where $\widetilde{\beta}_{B,i} \in \chi_1$ is the last noisy variable left in this decomposition. Note, that the first step of the hybrid reconciliation is not affected by the finite amount of samples generated in one run of the setup, as it operates sample-wise on the single partitioned outcomes of Alice and Bob by construction. Its efficiency is thus not influenced by finite-size effects.

In principle Alice and Bob could correct all their errors by only performing this first step of the hybrid reconciliation using very large $|\chi_2| \to |\chi_{\mathrm{KG}}|$. But

the communication cost of $\log_2\{|\chi_2|\}$ bits per sample would render this step to be very inefficient in this case. In most of the realistic QKD setups they cannot do this because too many bits would have to be communicated, exceeding the potential secure key rate k_{pot}. They are hence left with reduced but non-vanishing noise in $\widetilde{\beta}_{B,i}$ and thus $\text{Bin}[K_B]$ has to be furthermore corrected in a second step.

Note that, during the first step of the hybrid reconciliation, the size of all the involved alphabets is arbitrary up to $|\chi_{\text{KG}}| = |\chi_1| \cdot |\chi_2|$ which is an extension of the idea of sliced reconciliation as described in [VACC06], where only Galois fields and binary LDPC were analysed[2].

6.3.1.2. Step 2

The noise in χ_1 which remains after the first step can, in principle, be corrected by some arbitrary one-way reconciliation scheme. We propose the usage of non-binary LDPC algorithms as usually $|\chi_1| > 2$. We analyse the noise remaining after the first step in the next sections and use the Shannon entropy to estimate the communication cost of the second step analytically as described in Section 4.7.4.

6.3.2. Analytic Description

A full analytic description of the first step of the new hybrid reconciliation scheme, as detailed in Section 6.3.3, is complicated. We implemented the first step instead in a numerical simulation which we explain in Section 6.3.4 and use this analytic description to compare the numerical simulation with two steps with non-binary LDPC reconciliation in one step and furthermore to validate the simulation results whenever possible.

We focus again on outcomes of only one of the two possible measurement quadratures, say the amplitude measurement X, in this analytic description of the first step of the hybrid reconciliation. The phase quadrature can be analogously implemented if needed.

We start with the probability distribution function of Alice's measurement outcome $x_{A,i}$ conditioned on Bob's outcome $x_{B,i}$. Recall that the bivariate probability function (Wigner function, see Section 3.2.1) describing Alice's

[2] The variable $\beta \in \chi_1$ is, in sliced reconciliation terminology, denoted as *most significant information* and $\alpha \in \chi_2$ is called the *least significant information*.

and Bob's synchronised measurement samples is

$$\begin{aligned}\mathcal{P}(x_{A,i}, x_{B,i}) &= \mathcal{W}_\rho\left(\gamma_{AB}^X\right) \\ &= \frac{1}{(2\pi)^n\sqrt{\det\left(\gamma_{AB}^X\right)}}\exp\left[-\frac{1}{2}\vec{\xi}^T(\gamma_{AB}^X)^{-1}\vec{\xi}\right],\end{aligned} \tag{6.2}$$

where

$$\gamma_{AB}^X = \begin{pmatrix} \lambda_A & C_X \\ C_X & \lambda_B \end{pmatrix}$$

is the covariance matrix describing Alice's and Bob's synchronised amplitude measurements. Bob knows the joint probability density (see Equation 6.2) and his measurement outcome $x_{B,i}$. The conditional probability function is normally distributed by

$$\mathcal{P}(x_{A,i}|x_{B,i}) = \mathcal{N}(\mu_C(x_{B,i}), \lambda_{A|B})$$

with (conditional) mean and variance

$$\begin{aligned}\mu_C(x_{B,i}) &:= E(x_{A,i}|x_{B,i}) = x_{B,i}\frac{C_X}{\lambda_B}, \\ \lambda_{A|B} &:= V(x_{A,i}|x_{B,i}) = \frac{\lambda_A\lambda_B - C_X^2}{\lambda_B}.\end{aligned} \tag{6.3}$$

Notice especially that the conditional variance $\lambda_{A|B}$ is constant and does not depend on the value of the measurement result $x_{B,i}$ as already explained in Section 4.4.1.

We combine the conditional probability density in the following with the key generation grid. We describe the probability of Alice's measurement outcome $x_{A,i}$ lying in $I_k = \text{Bin}\left[x_{A,i}\right]$ conditioned on Bob's outcome $x_{B,i}$. The conditional probability that Alice's measurement is in interval I_k given Bob's measurement result $x_{B,i}$ is described by[3]

[3] The cumulative distribution function $F_X(x) = p(X \le x)$ of the normal distribution $\mathcal{N}(\mu,\sigma^2)$ is $F(x;\mu,\sigma) = \Phi\left(\frac{x-\mu}{\sigma}\right) = \frac{1}{2}\left[1+\text{Erf}\left(\frac{x-\mu}{\sqrt{2\sigma^2}}\right)\right]$ and $\int_a^b \mathcal{P}(K_A|K_B)dx_{A,i} = F(b;\mu_C,\lambda_{B|A}) - F(a;\mu_C,\lambda_{B|A})$ (see [BSMM00]).

$$\mathcal{P}(\mathrm{Bin}\left[x_{A,i}\right]_k|x_{B,i}) = \int_{I_k} \mathcal{P}(x_{A,i}|x_{B,i})dx_{A,i} \tag{6.4}$$
$$= \frac{1}{2}\mathrm{Erf}\left(\frac{x_{k+1}(I_{k+1}) - \mu_C(x_{B,i})}{\sqrt{2\lambda_{A|B}}}\right) - \frac{1}{2}\mathrm{Erf}\left(\frac{x_k(I_k) - \mu_C(x_{B,i})}{\sqrt{2\lambda_{A|B}}}\right).$$

Note that if the marginal distributions of Alice and Bob have variances $\lambda_A \neq \lambda_B$, two different key generation grids are needed to achieve optimal correlation between their raw keys. We choose to maintain one grid G_{KG} for both and scale Bob's outcomes such that $\lambda_A = \lambda_B$ instead. In reverse reconciliation Alice's outcomes would be scaled. We discuss the process of scaling in Section 6.3.7.1 in wider detail.

6.3.3. Estimators

We explain in this section two different estimators which are possible in the first step of the hybrid reconciliation. The choice of estimator depends on $|\chi_2|$ being either equal or odd. If $|\chi_2|$ is large enough, the two estimators saturate to the same results as we will show later in Section 6.3.4.

Let us now explain the two estimators:

Extended estimator (even $|\chi_2|$):
In the case where $|\chi_2|$ is even, the estimator could produce two minima of equal probability for different $I_k \in \chi_1$. In this case Bob sends Alice a signal with the request of repeating the first step of the hybrid reconciliation on a broader grid of size $|\tilde{\chi}_1| = 1/2 \cdot |\chi_1|$ and larger $|\chi_3| = 2 \cdot |\chi_2|$. This avoids in most cases two maxima of the estimator and allows Bob to successfully reconcile with the position of Alice in χ_1 with higher probability. This process can be repeated iteratively until Bob no longer finds two maxima any more. One can show that already one repetition is enough to achieve optimal efficiency. The extended estimator is depicted in Figure 6.4.

Simple estimator (odd $|\chi_2|$):
Another idea of avoiding two minima of same probability is by assuming $|\chi_2|$ is odd. The simple estimator is depicted in Figure 6.5.

If the partitioned outcomes are already perfectly correlated the estimators have no effect by their construction. Note, that we disclose $\log_2(|\chi_2|)$ bits for each sample of Alice and Bob during the first reconciliation step even when

their outcomes are already perfectly correlated $I_k^A = I_k^B$. But as the estimator is especially designed for the *origin of errors* (see Section 4.4.1) and for the requirements of the CV-QKD protocols we discuss in this thesis, it has very high efficiency for the appropriate choice of its parameter range (i.e. large $|\chi_{\mathrm{KG}}|$) as we will show later in Section 6.3.6. The noise in Bob's raw key is completely reduced to $\beta_{B,i} \in \chi_1$ after the first step.

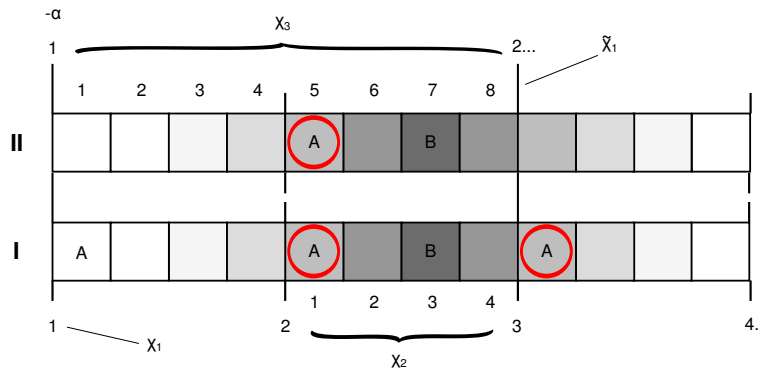

Figure 6.4.: Extended estimator: This figure explains the maximum likelihood estimator of the first step of the hybrid reconciliation when $|\chi_2|$ is even. Alice communicates her position $\alpha_{A,i}$ in the grid χ_2 and Bob computes the distances between his position and Alice's possible outcomes and chooses the one with minimal distance (highest probability). Two equal probabilities (red circles) as outcome of the estimator are possible in this situation. In the first and already optimal iteration of the extended estimator (II), Alice sends her position in a broader grid of size $|\chi_3| = 2 * |\chi_2|$ and Bob recomputes his probabilities. The probabilities for the I_k are correct with a higher probability (red circle).

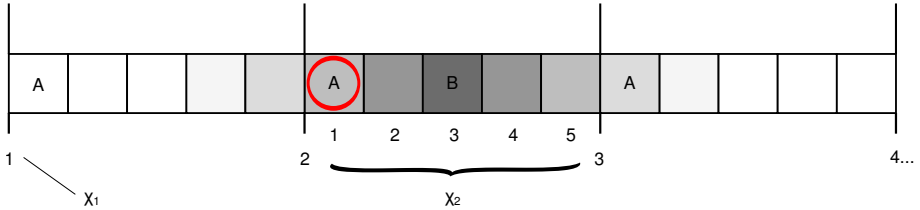

Figure 6.5.: Simple estimator: This figure explains the maximum likelihood estimator of the first step of the hybrid reconciliation when $|\chi_2|$ is odd. Alice communicates her position $\alpha_{A,i}$ in the grid χ_2. Bob computes the distances between his position and Alice's element of χ_2 in the different grid χ_1 and chooses the element of χ_1 which provides a minimal distance (maximal probability, red circle).

6.3.4. Simulation

We implemented the full numerical simulation of the first step of the reconciliation in Mathematica and used the simplified analysis which is described in Section 6.3.2 to verify the results for certain sets of parameters. We assume non-binary LDPC reconciliation in the second step and use the results of the first step to describe the communication cost of the non-binary LDPC reconciliation analytically.

The key generation and the partitioning is discussed in detail in the Sections 4.3 and 4.4. We drop the assumption $|\chi_{\mathrm{KG}}| = 2^d$, hence allowing for key generation alphabets of arbitrary size as long as $|\chi_{\mathrm{KG}}| = |\chi_1| \cdot |\chi_2|$ and focus on only one quadrature.

The simulation starts by generating $N_{\mathrm{key}} = |K_{AB}|$ correlated raw key measurements $\{K_{AB}\}_i = \{x_{A,i}, x_{B,i}\}$ for Alice and Bob from the Wigner distribution function according to γ^X_{AB}. After partitioning the correlated measurement samples, Alice and Bob hold each a raw key with $\mathrm{Bin}[K_A] \neq \mathrm{Bin}[K_B]$ consisting of elements of the key generation alphabet χ_{KG}. We now rewrite every raw key element as linear combination of the elements of $\alpha_{k,i} \in \chi_2$ and $\beta_{k,i} \in \chi_1$ with $k \in \{A, B\}$ as explained in Section 6.3.1.1. Alice communicates $\alpha_{A,i}$ over an authenticated classical channel to Bob who performs the first step of the hybrid reconciliation using one of the maximum likelihood estimators which are described in Section 6.3.3. The question of which maximum likelihood estimator is to be used depends on $|\chi_2|$.

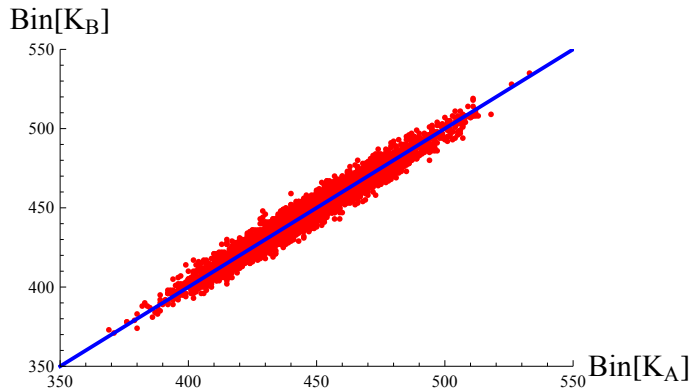

Figure 6.6.: The partitioned synchronised outcomes $\mathrm{Bin}[K_{AB}]$ of Alice and Bob for $|\chi_{\mathrm{KG}}| = |\chi_1| \cdot |\chi_2| = 2^7 \cdot 7 = 896$. The thick blue line denotes the perfectly correlated samples. All the other points represent samples which are less correlated (red). The task of the hybrid reconciliation is to correct all outcomes to lie on the blue line. For this figure we used only $N_{\mathrm{key}} = 5000$ samples for the purpose of presentation.

In this section we analyse the behaviour of the hybrid reconciliation as a function of $|\chi_2| \in \{1, 2, ...50\}$ and fix $\alpha = 45$ and $|\chi_1| = 2^7 = 128$ if not otherwise noted. The size of the key generation alphabet is now $|\chi_{\mathrm{KG}}| = 2^7 \cdot |\chi_2|$ and the spacing scales with $\delta\left(|\chi_2|\right) = 2^{-6} \cdot \alpha / |\chi_2|$. We assume an efficiency of $\beta_2 = 0.9$ of the non-binary LDPC in the optimal second step with one iteration when the estimator (see Equation 6.1) produced two equal maxima.

In the simulation we use the following covariance matrix describing the bipartite state of Alice and Bob as an example

$$\gamma_{AB} = \left(\begin{array}{cc|cc} 5.06 & 0.01 & 4.95 & 0 \\ 0.01 & 5.06 & 0 & -4.95 \\ \hline 4.95 & 0 & 5.06 & 0.01 \\ 0 & -4.95 & 0.01 & 5.06 \end{array}\right)$$

which reflects a proper scaling of the samples and use only the amplitude measurements for the key generation. A full collection of the parameters of the simulation is given in Table B.6. We chose the parameters and the covariance matrix as they allow us to discuss the different effects of the estimators

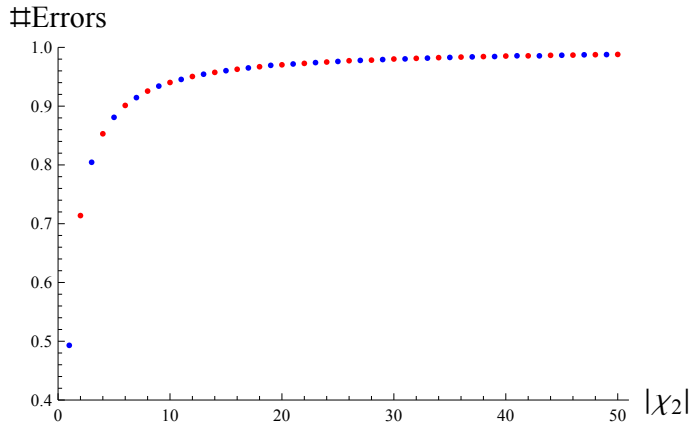

Figure 6.7.: The number of imperfectly correlated measurement samples (#Errors) of the raw key samples as a function of $|\chi_2|$ normalised to N_{key}. The values of #Errors are colour coded for χ_2 odd (even). One can see that already for small $|\chi_2|$ many samples are imperfectly correlated. For increasing $|\chi_2| \to \infty$ the number of errors tends to unity as the spacing $\delta\left(|\chi_2|\right) \to 0$.

as we will show later.

Raw key generation:
Let us at first focus on the partitioned measurement samples of Alice and Bob before the reconciliation. The partitioned and synchronised bit sequences $\text{Bin}[K_{AB}]$ of Alice and Bob are plotted in Figure 6.6 for $|\chi_{\text{KG}}| = 2^7 \cdot 7 = 896$. The simulation shows that under these circumstances already $\approx 91\%$ of the partitioned samples are imperfectly correlated.

We can find this value in Figure 6.7 where we plot the number of synchronised samples that are imperfectly correlated as a function of $|\chi_2|$. The amount of samples which are imperfectly correlated saturates to unity for $|\chi_{\text{KG}}| \to \infty$. Very high alphabet error rates are typical for key generation of the CV-QKD protocols that we discuss in this thesis.

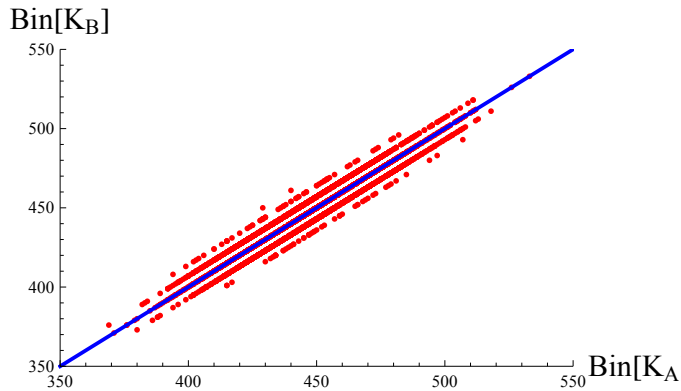

Figure 6.8.: The partitioned synchronised outcomes $\mathrm{Bin}[K_{AB}]$ of Alice and Bob for $|\chi_{\mathrm{KG}}| = |\chi_1| \cdot |\chi_2| = 2^7 \cdot 7 = 896$ and $\alpha = 45$ after the first step of the hybrid reconciliation. The thick blue line denotes the perfectly correlated samples, all the other points represent samples which are less correlated (red). The outcome of the first step of the hybrid reconciliation is that the noise is reduced to χ_1 which is reflected by the parallel lines with distance $|\chi_2| \cdot \delta\left(|\chi_2|\right)$ to the next neighbouring line. This graph shows that there is still some noise left in χ_1. For this figure we used only $N_{\mathrm{key}} = 5000$ samples for the purpose of illustration.

First step: Let us now focus on the results of the different estimators of the first step of the hybrid reconciliation. Figure 6.8 shows the results of the first step on the partitioned and synchronised samples of Alice and Bob. The noise (the errors between Alice's and Bob's raw keys) is reduced to $\beta_{B,i} \in \chi_1$ as denoted by the parallel lines. Note that the parallel lines always have a distance of $|\chi_2| \cdot \delta\left(|\chi_2|\right)$ to the next neighbouring line. This behaviour is independent of the estimator which is used in the first step.

Figure 6.9 shows the number of the imperfectly correlated samples of Alice and Bob by comparing the simple estimator with the extended estimator whenever possible ($|\chi_2|$ even). In this simulation the extended estimator performs always better than the simple estimator, especially for small $|\chi_2|$. The performance of the simple estimator increases with $|\chi_2|$ and saturates to a constant value for $\delta\left(|\chi_2|\right) \to 0$.

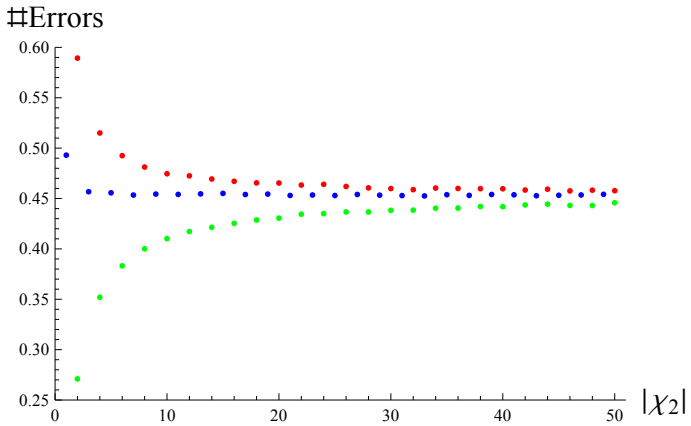

Figure 6.9.: The number of imperfectly correlated samples of Alice and Bob (#Errors) as a function of $|\chi_2|$ after the first step of the hybrid reconciliation. The values are colour coded for χ_2 odd; even, using the simple estimator; even, using the extended estimator. Note that in the case of $|\chi_2| = 1$ no information is sent during the first step which leaves the #Errors unchanged (compare with Figures 6.7 and 6.11).

Let us discuss the communication cost of the first step $\ell_{\mathrm{EC},1}/N_{\mathrm{key}}$ as a function of $|\chi_2|$, as shown in Figure 6.10. The communication costs of the simple estimator are given by $\log_2\lceil|\chi_2|\rceil$. In this simulation the extended estimator has a better performance at a price of higher communication costs $\log_2\lceil k\cdot|\chi_2|\rceil = \log_2\lceil|\chi_3|\rceil$ with $k = 2$ (i.e. one iteration, if needed). The alphabet χ_3 denotes here the larger grid which is described in Figure 6.3 and used during the first and only iteration in the simulation. As $\chi_2 \subset \chi_3$ and $|\chi_3| = 2\cdot|\chi_2|$ Eve learns only one bit more when the iteration is executed. The communication costs of all estimators coincide for increasing $|\chi_2|$, the differences are hence only significant for small $|\chi_2|$.

As expected, the first step of the hybrid reconciliation reduces this value significantly but a second step is needed to reconcile the noise in χ_1.

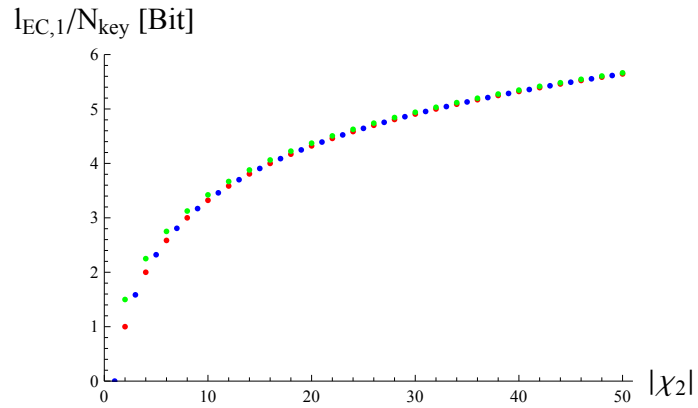

Figure 6.10.: We see here the communication cost $\ell_{\mathrm{EC},1}/N_{\mathrm{key}}$ of the first step as a function of $|\chi_2|$. The values of $\ell_{\mathrm{EC},1}/N_{\mathrm{key}}$ are colour coded for χ_2 odd; even, using the simple estimator; even, using the extended estimator. The communication costs of the extended estimator are, as expected, always higher than those of the simple estimator, especially for small $|\chi_2|$. This comes from the fact that the extended estimator allows for iterations on a larger alphabet than $|\chi_2|$ thereby disclosing more information. The communication costs of the simple estimator are, in contrast, always $\log_2\left[|\chi_2|\right]$.

Second step: We assume non-binary LDPC reconciliation to correct the remaining errors in Alice' and Bob's raw key's $\mathrm{Bin}[K_{AB}]$. The communication cost of the reconciliation operating only on χ_1 in the second step is computed according to Section 4.7.4. We compute the weights with which each of the parallel lines as sketched in Figure 6.8 appear which allows us to estimate the communication cost of the second step. We chose the efficiency of the second step of non-binary LDPC reconciliation to be $\beta_2 = 0.9$. All synchronised samples of Alice and Bob are fully correlated at the end of the hybrid reconciliation, i.e. after passing both steps[4].

Figure 6.11 shows the communication costs $\ell_{\mathrm{EC},2}/N_{\mathrm{key}}$ of the second step as

[4] Real-life implementations of reconciliation schemes sometimes still result in different raw keys for Alice and Bob. This is checked in the confirmation procedure as explained in Section 4.3. Real-life implementations thus result in identical raw keys of Alice and Bob with a probability $1-\varepsilon_{\mathrm{FER}} < 1$ where FER denotes the amount of frames (parts of the raw key's) of Alice and Bob that can not be successfully reconciled. We discuss this in Section 6.3.7.

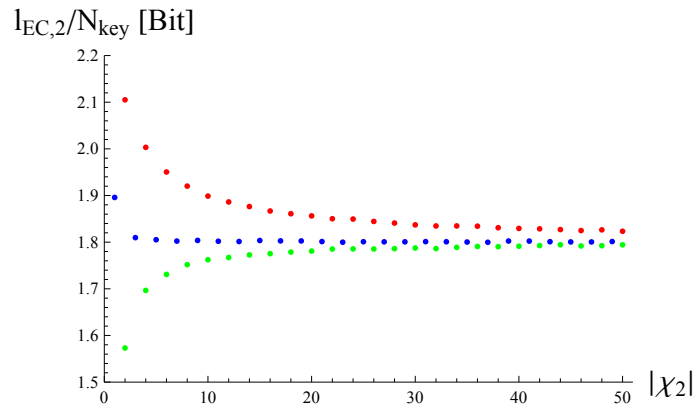

Figure 6.11.: The communication costs of the second step $\ell_{\mathrm{EC},2}/N_{\mathrm{key}}$ assuming non-binary LDPC with an efficiency $\beta_2 = 0.9$ operating on χ_1 as a function of $|\chi_2|$. The values of $\ell_{\mathrm{EC},2}/N_{\mathrm{key}}$ are colour coded for χ_2 odd; even, using the simple estimator; even, using the extended estimator. Note that the simple estimator operating on even $|\chi_2|$ generates the highest $\ell_{\mathrm{EC},2}/N_{\mathrm{key}}$ due to the possible uncertainty of two maxima in the estimator (see Section 6.3.3).

a function of $|\chi_2|$ for the simple and the extended estimator. We see that the communication cost of the simple estimator for even $|\chi_2|$ is the highest due to the possible two maxima. Its communication cost for odd $|\chi_2|$ saturates very quickly at ≈ 1.8 Bit and is more optimal due to the avoidance of two maxima of the estimator. Note that the saturation value itself is a function of α and γ^X_{AB}. The extended estimator left less errors in the raw key which minimises its communication costs in second step.

Let us focus on the total communication cost of the hybrid reconciliation as a function of $|\chi_2|$, which is presented in Figure 6.12. One can see that the communication costs show the largest differences for small $|\chi_2|$. This effect becomes less significant for increasing χ_{KG} which makes sense as this increases the resolution of the key generation grid during the simulation, which renders two maxima of the estimator less probable. Note that even $|\chi_2|$ still produce slightly higher communication costs when using the simple estimator. In this simulation all the estimators saturate to a common value for large enough $|\chi_2| \geq 2^5 = 32$. This means that even the simple estimator alone suffices,in this simulation, for large enough $|\chi_2|$.

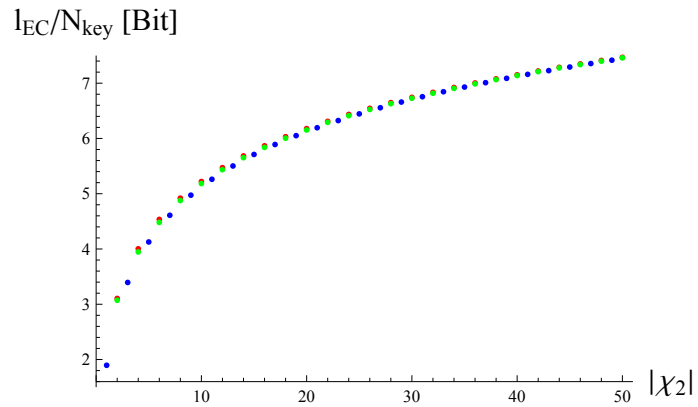

Figure 6.12.: The communication cost of the hybrid reconciliation as a function of $|\chi_2|$. The values of $\ell_{\mathrm{EC},2}/N_{\mathrm{key}}$ are colour coded for χ_2 odd; even, using the simple estimator; even, using the extended estimator. One can see that the hybrid reconciliation has a better performance when operating on even $|\chi_2|$ using the simple estimator.

6.3.5. Results

Here we summarise and discuss the results of Section 6.3.4, where we analyse the impact of the extended and the simple estimator on the hybrid reconciliation as a function of $|\chi_2|$ for $\alpha = 45$ and $|\chi_{\mathrm{KG}}| = |\chi_2| \cdot 2^7$, showing that the difference between the two different estimators becomes insignificant for large enough $|\chi_2| \geq 2^5$.

We compare in Figure 6.13 the communication cost of perfect non-binary LDPC with $\beta_{\mathrm{EC}} = 1$ in one step (see Section 6.3.2) with the results of the simulation which we presented in Section 6.3.4 in terms of the efficiency $\beta_{\mathrm{EC}}(|\chi_2|)$ of the hybrid reconciliation as a function of $|\chi_2|$. The efficiency of the hybrid reconciliation is surprisingly high, as the simulation was primarily designed for the purpose of a good illustration of the effect of the estimators, and saturates for large $|\chi_2|$ to $\beta_{\mathrm{EC}} \approx 0.95$. The differences between the estimators are most apparent for small $|\chi_2|$ and vanish for large $|\chi_2|$. For even $|\chi_2|$ the extended estimator performs slightly better than the simple estimator. Note that we used only one iteration when two maxima occurred in the extended estimator. More iterations should increase the efficiency of the hybrid reconciliation a little bit further.

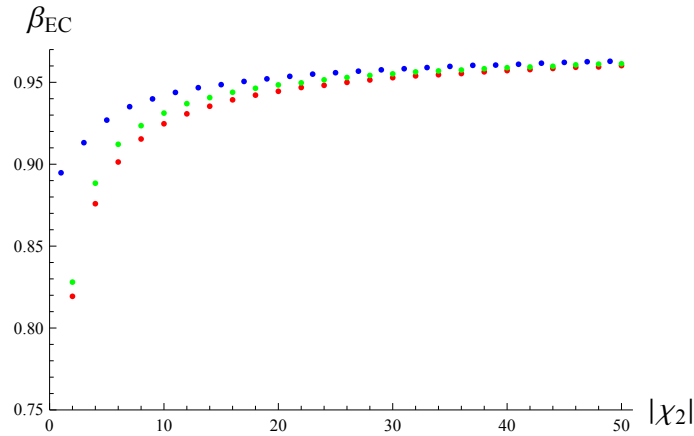

Figure 6.13.: This figure compares the communication cost of the hybrid reconciliation with the analytic outcomes for perfect non-binary LDPC as a function of $|\chi_2|$. The values of β_{EC} are colour coded for χ_2 odd; even, using the simple estimator; even, using the extended estimator. For $|\chi_2| \geq 5$ the hybrid reconciliation achieves already an efficiency of $\beta_{\mathrm{EC}} \geq 0.9$ and saturates for $|\chi_2| \to 50$ to $\beta_{\mathrm{EC}} \approx 0.95$. Note that in the case of $|\chi_2| = 1$ no information is sent during the first step and the errors are all corrected in the second step with an efficiency of $\beta_2 = 0.9$, as reflected in this graph (the small deviation from $\beta_2 \neq \beta_{\mathrm{EC}} = 0.9$ is a numerical artefact).

It can be shown that the first step of the hybrid reconciliation operates very close to the Shannon limit with an efficiency of $\beta_1 \approx 0.97$. This is a little bit counter intuitive as during the first step Alice communicates $\ell_{\mathrm{EC},1}/N_{\mathrm{key}}$ bits for every sample even when the partitioned outcome of Bob is already perfectly correlated. This can be explained as the number of imperfectly correlated partitioned samples of Alice and Bob is very large throughout the whole simulation and saturates to unity for decreasing spacing $\delta\left(|\chi_2|\right) \to 0$. It follows that almost no samples of Alice and Bob are perfectly correlated after partitioning which is the reason for the high efficiency of the first step.

Note that the efficiency of the hybrid reconciliation is small for $|\chi_2| = 2$. This comes from the fact that, when Alice's element of χ_2 does not coincide with Bob's, the estimator always produces two minima, as the distance between

their elements is maximally 1. We suggest allowing for larger possible distance between Alice's and Bob's elements $|\chi_2| > 2$, together with the extended estimator if needed or, even better, the simple estimator. This increases the efficiency of the hybrid reconciliation. But as the key generation grids are normally chosen such that $\chi_{\mathrm{KG}} = \mathcal{GF}\left(2^d\right)$ in order to simplify the mapping to the bit sequences of length d after reconciliation, we propose using the extended estimator with multi-level iterations in this case. Note that the difference between the estimators becomes less significant for larger $|\chi_2|$ and $|\chi_{\mathrm{KG}}|$.

We use the hybrid reconciliation algorithm presented in Section 6.3.6 in a CV-QKD experiment providing security against coherent attacks and show again that large $|\chi_2|$ are almost optimal.

6.3.6. Experiment Secure Against Coherent Attacks

The experiment we present in this section was realised as part of the collaboration *Crypto on Campus*. The symmetric CV-QKD protocol providing security against coherent attacks (see Section 4.6) was used to generate the secure key [GHD+14]. The hybrid reconciliation scheme which is presented in this section was implemented by Dr. C. Pacher from the *Austrian Institute of Technology* and used to correct the errors between Alice's and Bob's raw key in direct reconciliation. Note the runtime protocol of the experiment is member of $F^2_{2,T_{MS}}$ as explained in Section 5.3.1.

Remember that in the past experimental implementations of QKD protocols providing security against coherent attacks required single photon preparation and detection, as QKD systems using amplitude and phase modulations failed to provide the same security standard. We present here the first implementation of a QKD protocol using amplitude and phase modulations of an optical field (s-class state). The experimental setup is explained in Section 3.3 and the parameters of the CV-QKD protocol (see Section 4.3) are shown in Table B.7.

Remember especially that the CV-QKD protocol requires very large key generation alphabets $|\chi_{\mathrm{KG}}|$ to maximise the potential key k_{pot} of the setup. The size we chose for this experiment was $|\chi_{\mathrm{KG}}| = |\mathcal{GF}\left(2^{12}\right)| = 2^{12}$. The hybrid reconciliation achieved an efficiency of about $\beta_{\mathrm{EC}} \approx 95\%$ with $|\chi_1| = |\mathcal{GF}\left(2^5\right)| = 2^5$ (most significant information) and $|\chi_2| = |\mathcal{GF}\left(2^7\right)| = 2^7$ (least significant information). As $|\chi_2| = 2^7$ we only used the simple estimator during the rec-

onciliation. We chose the size of all alphabets such that they can be identified with Galois fields which simplifies the mapping to the bit sequences after reconciliation.

In this table-top experiment we generated about

$$\approx 97 \text{ MBit}$$

secure key from $k_{\text{sec}} = 1.14$ Bit, $N_{\text{key}} = 0.85 \cdot 10^8 = |K_{AB}|$ ($N_{\text{tot}} = 2x10^8 = |M_{AB}|$, $N_{\text{pe}} = 1.15 \cdot 10^8$) synchronised samples using the hybrid reconciliation. This is more than 1 bit per sample in the raw key and, thus, exceeds the theoretical bound for QKD protocols using single photons.

6.3.7. Characteristics

The promising results of hybrid reconciliation in the CV-QKD experiment providing security against coherent attacks and the simulation motivated the technical analysis we present in this section. The software was implemented by Dr. Jesus Martinez Mateo from the *Universidad Politecnica de Madrid*. The collaboration provided a full analysis of the characteristics of the hybrid reconciliation scheme (see [PMD+14]) which we present in the following sections.

We again focus on only one quadrature, say the amplitude, and begin in Section 6.3.7.1 with a detailed description of the process of scaling Alice's and Bob's measurement outcomes. We show that all covariance matrices can be brought into a form where the local variances of Alice's and Bob's outcomes are $\lambda_A = \lambda_B = 1$, whereby the covariance is described by a parameter $\rho \in [0,1]$. We use the scaling of the outcomes in this technical analysis for the purpose of a more general presentation.

We continue in Section 6.3.7.3 with a description of the simulation and show the results in the Sections 6.3.7.4 and 6.3.7.5. The results are discussed and compared to other reconciliation schemes in Section 6.3.7.6.

6.3.7.1. Scaling

We explain in this section two different methods of scaling Alice's and Bob's outcomes. The asymmetry between Alice's and Bob's marginal probability density functions is described by their local variances λ_A and λ_B. As Alice always holds the sources and Bob is probably remote we usually have $\lambda_A > \lambda_B$. Assuming the key generation grids of Alice and Bob to be $G_{\text{KG}}^A = G_{\text{KG}}^B$, it can

happen that, although Alice's and Bob's measurement samples are perfectly correlated, their corresponding partitioned measurement outcomes are different as described in Section 4.4.1.

We propose rescaling the measurement outcomes, such that $\lambda_A = \lambda_B$, to circumvent the above mentioned problem while maintaining one key generation grid G_{KG}. Note that the scaling of the measurement outcomes only affects the raw key generation and not the secure key analysis. In direct reconciliation only Alice's outcomes conditioned on Eve are relevant for the security analysis, which allows us to rescale Bob's outcomes (in reverse reconciliation Alice's outcomes are scaled).

We furthermore extend the idea of scaling to the situation where the variances of the marginals of Alice and Bob are $\lambda_A = \lambda_B = 1$ with covariance (correlation coefficient) $\rho \in [0,1]$ and show that every covariance matrix can be brought into this form. We use this description in the technical analysis of the characteristics of the hybrid reconciliation. Note that the key generation grid is not maintained when using this method of scaling the outcomes. The key generation grid (and all affiliated parameters) have to be scaled accordingly too.

1) Scaling to $\lambda_A = \lambda_B$:
We start with the covariance matrix of a general bipartite Gaussian state

$$\gamma_{AB}^{X} = \begin{pmatrix} \lambda_A & C_X \\ C_X & \lambda_B \end{pmatrix}.$$

The scaling we propose here can be used in all the CV-QKD protocols we discuss in this thesis because the marginal Gaussian distributions needed to fulfill the task can always be estimated from the outcomes which are disclosed during parameter estimation and those which are sorted out during sifting. Assuming direct reconciliation we locally scale Bob's outcomes by

$$\widetilde{K}_B = \frac{\sqrt{\lambda_A}}{\sqrt{\lambda_B}} \cdot K_B$$

where K_B are Bob's outcomes that are later used in key generation. In case of reverse reconciliation we scale Alice's outcomes by

$$\widetilde{K}_A = \frac{\sqrt{\lambda_B}}{\sqrt{\lambda_A}} \cdot K_A.$$

Having rescaled the measurement outcomes for the key generation by the above factors, the covariance matrix (direct reconciliation) becomes

$$\gamma^X_{1,AB} = \begin{pmatrix} \lambda & \widetilde{C}_X \\ \widetilde{C}_X & \lambda \end{pmatrix}.$$

Note that the key generation grid is maintained in this method of scaling, as only the outcomes of one participant (in direct reconciliation Bob's and in reverse reconciliation Alice's) are scaled. The key generation grid is left unchanged because we scale only the outcomes of the participant who does not appear in the security analysis. Hence this scaling is the method of choice when performing CV-QKD experiments using the protocols we discussed in Chapter 5.

2) Scaling to $\lambda_A = \lambda_B = 1$:
We will show, that every Gaussian covariance matrix describing bipartite quadrature measurements can be brought into the form

$$\widetilde{\gamma}^X_{AB} = \begin{pmatrix} 1 & \rho \\ \rho & 1 \end{pmatrix}. \tag{6.5}$$

This representation also allows for equal key generation grids G_{KG} on Alice's and Bob's side, although G_{KG} has to be scaled in addition to the outcomes. This allows us to describe the hybrid reconciliation scheme in a simpler fashion, as the only free parameter left in the representation of the bipartite Gaussian state is the correlation coefficient $\rho \in [0,1]$.

Let us describe the scaling on the level of the corresponding estimated covariance matrix, which is in general

$$\gamma^X_{AB} = \begin{pmatrix} \lambda_A & C_X = \rho\sqrt{\lambda_A}\sqrt{\lambda_B} \\ C_X = \rho\sqrt{\lambda_A}\sqrt{\lambda_B} & \lambda_B \end{pmatrix}$$

where $\rho \in [0,1]$ measures the strength of the correlation between Alice's and Bob's outcomes (correlation coefficient). We assume direct reconciliation and first rescale Bob's entries locally such that his marginal distribution is equal to Alice's. The operator describing this on the level of covariance matrices is

$$U_1 = \begin{pmatrix} 1 & 0 \\ 0 & \frac{\sqrt{\lambda_A}}{\sqrt{\lambda_B}} \end{pmatrix}$$

which results in

$$\begin{aligned}\gamma^X_{1,AB} &= U_1 \cdot \gamma^X_{AB} \cdot U_1^T \\ &= \begin{pmatrix} \lambda_A & \rho\lambda_A \\ \rho\lambda_A & \lambda_A \end{pmatrix}.\end{aligned}$$

In the second step we rescale Alice's and Bob's equal marginal distributions by

$$U_2 = \begin{pmatrix} \frac{1}{\sqrt{\lambda_A}} & 0 \\ 0 & \frac{1}{\sqrt{\lambda_A}} \end{pmatrix}$$

which results in

$$\begin{aligned}\gamma^X_{2,AB} &= U_2 \cdot \gamma^X_{1,AB} \cdot U_2^T \\ &= \begin{pmatrix} 1 & \rho \\ \rho & 1 \end{pmatrix}.\end{aligned}$$

The only free parameter in this representation is the correlation coefficient $\rho \in [0,1]$. In realistic setups $\rho < 1$ because of finite squeezing of the sources, as explained in Section 3.4.1. The correlation coefficient can only reach $\rho = 1$ in the case of infinite squeezing of the sources, but $\rho < 1$ always, since the generation of infinite squeezing requires infinite energy.

We use this representation furthermore to measure the strength of the correlations between Alice and Bob in terms of $\rho \in [0,1]$. The proposed method of scaling the outcomes can in this sense also be used for the characterisation of Gaussian bipartite states.

6.3.7.2. Signal to Noise Ratio

We use the correlation coefficient ρ for a general description of the Gaussian state when analysing the technical details of the hybrid reconciliation in Section 6.3.7.3. But the parameter which is commonly used in the field is the signal to noise ratio (SNR) in decibel. The bijective mapping from ρ to the SNR is described as

$$\mathrm{SNR}(\rho) = \frac{\rho^2}{1-\rho^2}.$$

The SNR in decibel is

$$\mathrm{SNR}[\mathrm{dB}] = 10 \cdot \log_{10}\left[\mathrm{SNR}(\rho)\right].$$

Figure 6.14 shows the SNR in decibel [dB] as a function of ρ.

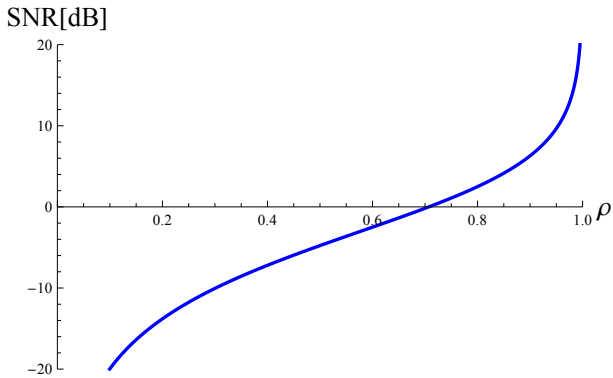

Figure 6.14.: The SNR in decibel as a function of the correlation coefficient ρ.

We focus in the following section on $\rho \geq 0.7$ because the hybrid reconciliation is especially designed for high signal to noise ratios (SNR$[dB] > 0$).

6.3.7.3. Simulations

In this section we describe the basic setup of the simulations which are used to fully analyse the hybrid reconciliation. Both steps have been fully implemented. The first step has been realised using the simple estimator as we will focus on large enough χ_2 and ρ. As the first step has already been discussed in wide detail we focus in this Section on the second step. We use regular and irregular non-binary LDPC in the second step[5]. The basics of non-binary LDPC are introduced in Section 4.7.3.

The simulations were performed to analyse the performance and the efficiency of the hybrid reconciliation algorithm using regular and irregular non-binary LDPC codes over finite (Galois) fields of order 2^{d_1}, denoted by $\chi_1 = \mathcal{GF}(2^{d_1})$, in the second step. These codes are used for reconciling the frames (i.e. the raw keys of Alice and Bob) $\{x, y\}_i \in K_A \times K_B = K_{AB}$ belonging to two continuous random and correlated variables, denoted by X and Y with

[5] A LDPC matrix is regular if the number of ones is constant for every row and constant for every column. Irregular LDPC matrices do not fulfill these restriction.

$i \in \{1, ..., N_{\text{key}}\}$. The correlated variables are assumed to follow the bivariate normal distribution which describes the correlation between Alice's and Bob's measurement tuples as shown in Section 6.3.7.1. We set $n = N_{\text{key}}$ for the purpose of illustration.

The non-binary LDPC decoding over $\chi_1 = \mathcal{GF}(2^{d_1})$ was performed by using a sum-product (belief propagation based) algorithm, as the one described in [BD03, DF07], with a maximum of 50 decoding iterations (i.e. the syndrome of a frame is calculated and verified after each decoding iteration and the algorithm stops whenever the syndrome is validated or when the maximum number of iterations is reached).

Note that while the order of the Galois field used for decoding is 2^{d_1}, $d = d_1 + d_2$ bits are used to identify each partition of the reconciliation interval $[-\alpha_{\text{EC}}, +\alpha_{\text{EC}}]$, where d_2 is the number of less significant bits per symbol which are disclosed in the first step of the hybrid reconciliation[6] which corresponds to a rate of $R = 0$ of this step[7]. Thus, the number of partitions (quantised values) is given by $|\chi_{\text{KG}}| = 2^{d_1+d_2} = 2^d$.

Good families of irregular non-binary LDPC codes for decoding over different Galois fields, and adapted to the current reconciliation scheme, were optimised using a differential evolution algorithm as the one described in [SS00]. Parity-check matrices for regular and irregular non-binary LDPC codes were constructed using the progressive edge-growth algorithm described in [HEA05]. As in [HEA05] we constructed a binary LDPC matrix and then replaced every entry with value one with a random variable which is chosen uniformly from $\{1, 2, ...2^{d_1-1}\}$.

6.3.7.4. Performance

Initially, the Figures 6.15 to 6.17 show the performance of regular non-binary LDPC codes for different number of partitions of the reconciliation interval. In addition we show as horizontal top-axis the SNR in decibel (dB). The performance is calculated as frame error rate (FER), i.e. the ratio of frames that cannot be reconciled, and it is shown as a function of the correlation coefficient ρ between X and Y, or equivalently the signal-to-noise ratio (SNR). The frames that can not reconciled by non-binary LDPC are reconciled by open

[6] The cut-off parameter α of the CV-QKD protocols as discussed in Chapter 5 does not necessarily have to be the same as in the reconciliation process. All the tuples that lie outside of $[-\alpha_{\text{EC}}, +\alpha_{\text{EC}}]$ are completely disclosed to avoid post selection. This allows to optimise the hybrid reconciliation by differentiating between α and α_{EC}.

[7] The coding rate R denotes the amount of disclosed bits via $\ell_{EC} = (1-\text{R}) \cdot n$.

communication over the authenticated channel. The reason is, that the CV-QKD protocol providing security against coherent attacks does not allow for post selection as explained in Section 4.6.

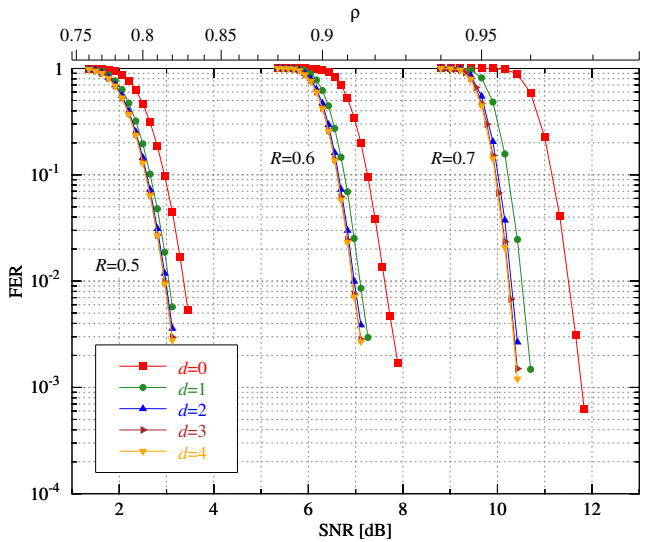

Figure 6.15.: Frame error rate of non-binary LDPC decoding over $\mathcal{GF}(2^5 = 32)$ for different coding rates R, from left to right in the figure R $= 0.5$, R $= 0.6$, and R $= 0.7$. The frame length is $n = 10^3$ and the interval half width is $\alpha_{\mathrm{EC}} = 8$. The FER is shown as a function of the SNR (bottom axis) and the correlation coefficient ρ (top axis).

Figure 6.15 shows the performance as a function of the SNR in decibels (dB). The correlation coefficient ρ between the frames which are to be reconciled is also depicted in the figure. The order of the Galois field used for decoding is $2^5 = 32$, and a short frame length of $n = 10^3$ symbols was considered for practical issues, i.e. lower computational complexity. As shown, $|\chi_2| = 2^{d_2} = 2^3$ (brown curve) is large enough to achieve the near optimal performance even for different coding (information) rates.

The Figure 6.16 also shows the performance for different number of partitions of the reconciliation interval, but now comparing non-binary LDPC decoding over different Galois fields. As previously, simulations were performed using regular and short frame length non-binary LDPC codes, of $n =$

10^3 symbols, and $\alpha_{\mathrm{EC}} = 8$. As shown, the best performance is achieved as in Figure 6.15 when $|\chi_2| = 2^{d_2} \geq 2^3$. Although the performance of only one coding rate is shown, $\mathrm{R} = 0.7$, several coding rates for each Galois field were also simulated to confirm this behaviour.

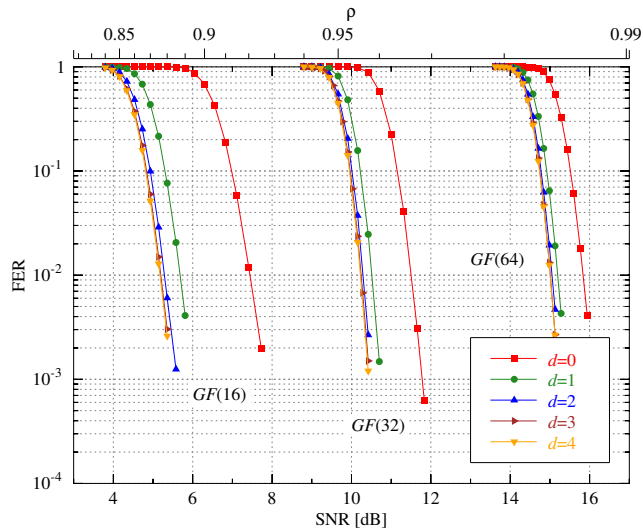

Figure 6.16.: Frame error rate of non-binary LDPC decoding over $\mathcal{GF}(2^4 = 16)$, $\mathcal{GF}(2^5 = 32)$, and $\mathcal{GF}(2^6 = 64)$ and coding rate $\mathrm{R} = 0.7$. The frame length is $n = 10^3$ and the interval half width is $\alpha_{\mathrm{EC}} = 8$. The FER is shown as a function of the SNR (bottom axis) and the correlation coefficient ρ (top axis).

This d_2 value has been empirically shown to be near optimal for different Galois fields, coding rates, frame lengths, and reconciliation interval half widths. Therefore, hereinafter $d_2 \geq 3$ is considered to compute the performance and reconciliation efficiency.

Figure 6.17 shows how the performance improves, and thus the reconciliation efficiency (labelled as β) too, as the frame length increases. In the figure, the FER is shown as a function of the SNR. Simulations were carried out using regular non-binary LDPC codes and decoding over $\chi_1 = \mathcal{GF}(2^5 = 32)$, with common parameters: coding rate, $\mathrm{R} = 0.7$, reconciliation interval half width, $\alpha_{\mathrm{EC}} = 8$, and number of less significant bits disclosed per symbol, $d_2 = 3$. The performance was then computed and compared for several frame lengths.

The reconciliation efficiency for all the frame lengths considered is also depicted (solid black dots) and labelled in the figure. As shown, these efficiencies are calculated for a constant FER value of $\varepsilon_{\text{FER}} = 10^{-1}$, it means that the efficiency is calculated using an estimate (empirically computed) of the highest correlation coefficient for which a frame can be reconciled with a success rate of $1-\varepsilon_{\text{FER}}$ (i.e. 90%).

Note that throughout this technical analysis a significantly high FER value of $\varepsilon_{\text{FER}} = 10^{-1}$ was considered in order to compare our results with those other published in the literature [JKJL11, JKJL13].

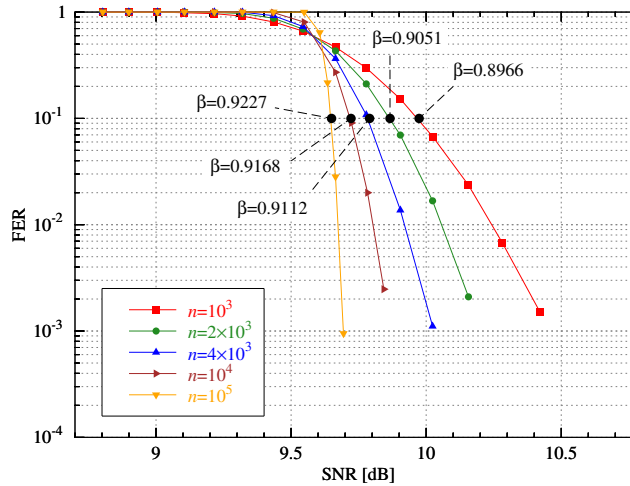

Figure 6.17.: Frame error rate and efficiency for different frame lengths, $n = 10^3$ symbols (red curve), $n = 2 \cdot 10^3$ (green), $n = 4 \cdot 10^3$ (blue), $n = 10^4$ (brown) and $n = 10^5$ (orange). The coding rate is $R = 0.7$ and the interval half width is $\alpha_{\text{EC}} = 8$ together with $d_2 = 3$. The FER is shown as a function of the SNR (bottom axis).

6.3.7.5. Efficiency

Figure 6.18 shows the reconciliation efficiency[8] β as a function of the SNR for non-binary LDPC decoding over different Galois fields. The efficiency using a

[8] Note that the over-all efficiency when additionally including the frame error rate is given by $\widetilde{\beta} = (1-\varepsilon_{\text{FER}}) \cdot \beta$.

frame length of $n = 10^3$ symbols (solid line) is also compared for larger frame lengths, $n = 10^4$ symbols (dashed line), and $n = 10^5$ symbols (dotted line).

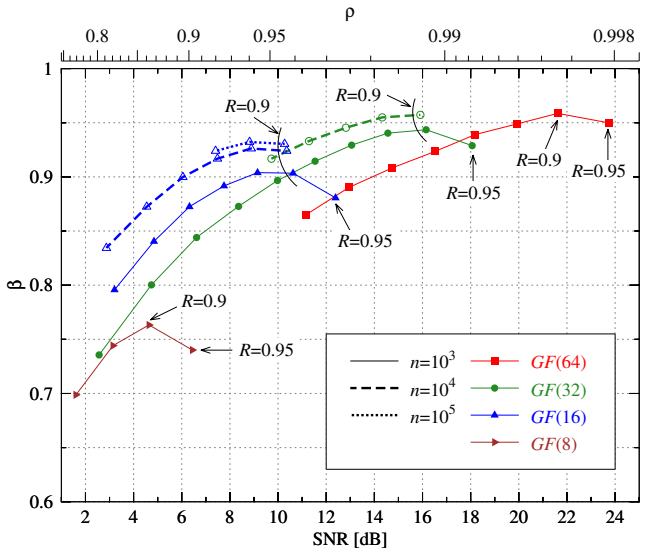

Figure 6.18.: Reconciliation efficiency of non-binary LDPC decoding over different Galois fields, $\chi_1 = \mathcal{GF}(8)$ (brown curve), $\mathcal{GF}(2^4 = 16)$ (blue), $\mathcal{GF}(2^5 = 32)$ (green), and $\mathcal{GF}(2^6 = 64)$ (red), and several coding rates and frame lengths. The efficiency is shown as a function of the SNR (bottom axis) and the correlation coefficient ρ (top axis). The coding rate of two consecutive points on each curve differs by 0.05.

Note that results of non-binary LDPC decoding over $\mathcal{GF}(2^6 = 64)$ for larger frame lengths were not computed, and the largest frame length was only considered for $\mathcal{GF}(2^4 = 16)$. Simulations were carried out using regular non-binary LDPC codes, $d_2 = 3$ for the number of disclosed bits per symbols, and the reconciliation interval half width $\alpha_{\mathrm{EC}} = 8$. The efficiency was calculated in all the cases estimating the highest SNR for which a sequence can be reconciled with a frame error rate of $\varepsilon_{\mathrm{FER}} = 10^{-1}$. Several coding rates were used to empirically estimate the expected reconciliation efficiency in a range of SNR. Therefore, each point in the curves corresponds to the efficiency computed using a particular coding rate (some of them labelled in the figure).

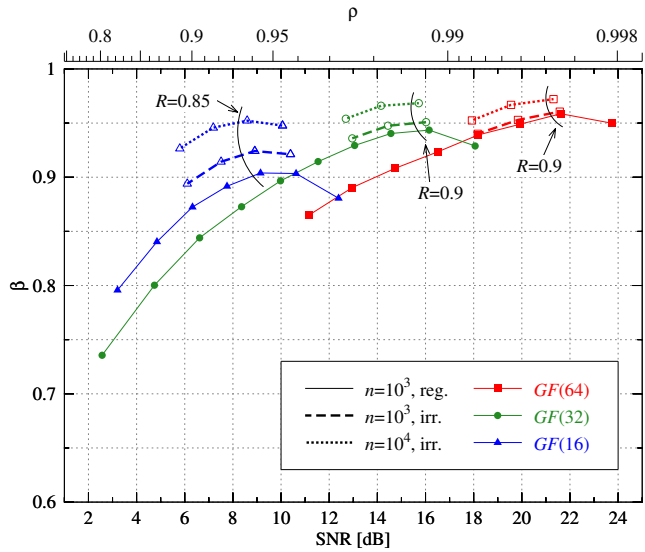

Figure 6.19.: Reconciliation efficiency with regular and irregular non-binary LDPC codes. The efficiency is shown as a function of the SNR (bottom axis) and the correlation coefficient ρ (top axis). The coding rate of two consecutive points on each curve differs by 0.05.

Figure 6.19 shows how the reconciliation efficiency improves as the frame length increases and using irregular non-binary LDPC codes. Results of Figure 6.18 with regular codes are here compared, thus, as previously, new simulations were computed for several frame lengths and coding rates but using common parameters: $d_2 = 3$, $\alpha_{\mathrm{EC}} = 8$, and $\varepsilon_{\mathrm{FER}} = 10^{-1}$. As expected and shown, better irregular codes can be designed for lower Galois field orders, and efficiency values above 0.95 can be achieved for non-binary LDPC decoding over $\chi_1 = \mathcal{GF}(2^4 = 16)$, $\mathcal{GF}(2^5 = 32)$ and $\mathcal{GF}(2^6 = 64)$ using irregular codes and frame lengths of $n = 10^4$ symbols.

Figure 6.20 shows the reconciliation efficiency as a function of the SNR for different sizes of the reconciliation interval half (α_{EC}). Increasing α_{EC} values (half of the interval width) were considered for a constant coding rate R . We then compared the reconciliation efficiency of several coding rates over different Galois field, although Figure 6.20 only shows the efficiency of irregular non-binary LDPC codes for decoding over $\chi_1 = \mathcal{GF}(2^4 = 16)$, $\mathcal{GF}(2^5 = 32)$, and

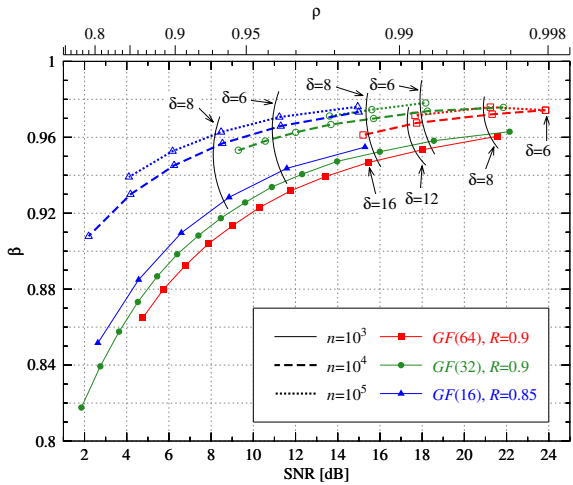

Figure 6.20.: Reconciliation efficiency for non-binary LDPC decoding over different Galois fields varying the interval width of a fixed-rate code. The values of the polynomials which generate the LDPC matrices are given in Table B. The efficiency is shown as a function of the SNR (bottom axis) and the correlation coefficient ρ (top axis).

$\mathcal{GF}(2^6 = 64)$, with coding rates R $= 0.85$, R $= 0.9$, and R $= 0.9$, respectively. In this case, the number of partitions of the reconciliation interval remain constant to 2^9, such that the number of disclosed bits differs for each Galois field, i.e. $d_2 = 5$, 4, and 3 for decoding over $\mathcal{GF}(2^4 = 16)$, $\mathcal{GF}(2^5 = 32)$, and $\mathcal{GF}(2^6 = 64)$, respectively. The smallest interval width (i.e. $\alpha_{\mathrm{EC}} = 4$ and $\alpha_{\mathrm{EC}} = 6$) are labelled in the figure. Note that the interval width of two consecutive points on a curve differs by 2 or 4. Finally, we conclude that the best efficiency is obtained varying the interval width α_{EC} of a fixed-rate code depending on the SNR. As shown, the efficiency considering a frame length of $n = 10^4$ bits is over 0.9 in the range from 2 dB to 24 dB.

6.3.7.6. Discussion

Non-binary LDPC codes are originally proposed for improving the reconciliation efficiency of discrete variables in QKD by Kasai *et al.* [KMS10]. However, we originally propose here the use of non-binary LDPC codes for reconciling continuous variables in the context of secret-key agreement. Note that the use of non-binary codes is the straightforward way to reconcile quantised

values (i.e. the quantisation of a continuous set of values).

Table 6.1 summarises the best efficiency values reported in the literature (to the best knowledge of the author) regarding to the reconciliation of continuous variables in QKD. In the table, three different information reconciliation techniques are compared for a range of SNR with the results obtained here: (1) sliced error correction (SEC) originally proposed by Cardinal *et al.* in [CVA03, VACC06] (using turbo codes) and later improved in [JKJL13, JEKJ14] (using LDPC and polar codes), (2) multilevel coding and multi stage decoding (MLC/MSD) using LDPC codes [BTMM06], and (3) multidimensional reconciliation (MD) [LAB$^+$08b, LAB$^+$08a, JKJL11]. In the table, two values are shown for the non-binary reconciliation scheme proposed here, the former corresponds to the estimated efficiency using a maximum of 50 decoding iterations, while in the latter simulations were performed increasing the maximum number of decoding iterations to 200.

SNR [dB]	ρ	β_{SEC}	β_{SEC}	β_{MLC}	β_{MD}	$\beta_{\text{non-binary}}$
4.8	0.866	79%	94.1%	88.7%	90%	94.3%−95.2%
7.0	0.913	-	94.4%	-	-	95.7%−96.5%
8.5	0.935	84%	-	90.9%	-	96.3%−97.0%
11.8	0.968	92%	95.8%	92.2%	-	97.1%−97.7%
14.9	0.984	-	-	-	-	97.6%−98.2%
n (bits)		$2\cdot10^5$	2^{20}	$2\cdot10^5$		$4\cdot10^5$
Refs.		[BTMM06]	[JEKJ14]	[BTMM06]	[LAB$^+$08b] [LAB$^+$08a]	[PMD$^+$14]

Table 6.1.: The efficiency of the hybrid reconciliation compared to other realisations.

6.4. Outlook and Discussion

In this chapter we presented a novel non-binary hybrid reconciliation scheme which is especially designed for the CV-QKD protocols as presented in Chapter 5. The hybrid reconciliation is parted in two steps. The first step uses the knowledge about the conditional probability function which describes the correlated samples of Alice and Bob by disclosing the d_2 less significant bits over an authenticated classical channel. The second step uses non-binary

LDPC codes to correct the remaining errors in the d_1 most significant bits. Note that the maximum of the size of the key generation alphabet $|\chi_{\mathrm{KG}}|$ is given by the resolution of the homodyne detectors which are used to measure the bipartite state.

The first step is not influenced by finite-size effects as it operates on the level of single tuples. Note furthermore that the computational complexity of the first step is very low. We have shown that this step operates very close to the Shannon-limit if the parameter of the reconciliation scheme are chosen properly. The noise in the raw keys of Alice $\mathrm{Bin}[K_A]$ and Bob $\mathrm{Bin}[K_B]$ is after this step reduced to the alphabet χ_1.

The noise in the alphabet χ_1 is corrected in the second step using non-binary LDPC reconciliation. The size of the alphabet $2^{d_1} = |\chi_1| < |\chi_{\mathrm{KG}}| = 2^d$ which reduces the computational complexity of the second step significantly [DF07] thus accelerating the runtime of the whole process.

The hybrid reconciliation has been successfully used in an experiment in which a key secure against coherent attacks has been generated with an reconciliation efficiency of $\approx 95\%$. We presented a technical analysis of the hybrid reconciliation and found a maximum of the reconciliation efficiency of $\approx 98\%$. Note that the hybrid reconciliation is applicable in direct as well as in reverse reconciliation.

The performance of the hybrid reconciliation scheme may be increased by using another estimator which does not operate on the partitioned raw keys $\mathrm{Bin}[K_{AB}]$ but on the measurement outcomes K_{AB} itself. This has the benefit that two maxima of equal probability are unlikely but it also increases, as a drawback, the computational complexity of the first step.

We presented a method of scaling covariance matrices which allows us to describe all possible covariance matrix by only one free parameter ρ which we call the correlation coefficient. Let us revisit the two covariance matrices which we extensively used in Chapter 5 and which are characterised in Table B.1. Table 6.4 shows the efficiency of the hybrid reconciliation β as a function of ρ for the amplitude (phase) sub-space of the two covariance matrices.

	V-class	S-class
β_X	≈ 0.93	≈ 0.97
β_P	≈ 0.98	≈ 0.98

We combine the hybrid reconciliation with the CV-QKD protocols which we discuss in Section 5 in the technical Appendix A.2.

Summing up we have proposed a new hybrid reconciliation algorithm which is well suited for the needs of the CV-QKD protocols we presented in Chapter 5. The feasibility of the reconciliation scheme has been shown in an experiment and in a technical analysis.

7. Conclusion

In the introductory chapters we provided a clear connection between the theoretical tools used in this thesis and their realisation in an experiment. We used these tools to stick as closely as possible to experimental realisations of the new security protocols and reconciliation schemes we propose in this thesis.

In **Chapter 5** we started with the question: How much key can be generated in one run of a quantum key distribution experiment? The question was motivated by the fact that experiments are always performed for a finite time, which we call the runtime of the system. In our runtime analysis we included the time needed to perform a measurement and the time needed to switch the basis between the measurements. We focused mainly on a setup with two measurements and two participants. We showed that QKD protocols that allow for a non-uniform choice of the measurement basis (asymmetric QKD protocols) can outperform QKD protocols that assume a uniform choice of the basis (symmetric QKD protocols).

This motivated us to introduce asymmetric CV-QKD protocols that provide security against collective and coherent attacks by extending the CV-QKD protocols of F. Furrer *et al.* [FFB+14] to allow for a non-uniform choice of the involved bases. We compared the two new protocols with their symmetric variants in simulations based on experiments that were carried out by Prof. Dr. R. Schnabel's group. We found that the new asymmetric CV-QKD protocols outperformed the symmetric protocols significantly.

The runtime analysis we used to motivate the asymmetric CV-QKD protocols proved to be a good tool for comparing different QKD protocols and experimental realisations. It can furthermore be extended to setups with more than two participants and measurements. It would be interesting to compare, for example, the prepare and measure DV-QKD BB84 protocol, the entanglement based DV-QKD E91 protocol and the prepare and measure CV-QKD protocol using Gaussian modulated states with our new asymmetric protocols on the basis of standard experimental technology.

In **Chapter 6** we discussed the key generation of the asymmetric CV-QKD protocols providing security against collective and coherent attacks. We described an experiment in which an actual secure key was generated using the CV-QKD protocol providing security against collective attacks together with binary LDPC reconciliation[1]. The binary LDPC reconciliation proved to be unsuitable for the CV-QKD protocols we discussed in this thesis.

This motivated us to develop a new non-binary reconciliation scheme which is specifically designed for the CV-QKD protocols we discussed in this thesis. The hybrid reconciliation which we propose is divided into two steps. The first step uses the knowledge of the conditional Gaussian probability function describing the correlation between Alice's and Bob's measurement tuples in an estimator. We showed in a simulation of the hybrid reconciliation scheme that this first step does not suffice to correct all errors between Alice's and Bob's raw keys. We introduced a second step which uses non-binary LDPC to correct the remaining errors. This hybrid reconciliation scheme has been successfully used in an experiment in which an actual key, secure against coherent attacks, was generated[2].

We provided a full technical analysis of the hybrid reconciliation scheme[3] and found a maximum value for the efficiency of $\beta = 0.98$. The hybrid reconciliation scheme is, furthermore, very efficient over a wide range of the signal to noise ratio. Hence we propose implementing the hybrid reconciliation in other CV-QKD protocols that use Gaussian states to distribute the raw keys.

[1] The software was implemented by Dr. C. Pacher of the *Austrian Institute of Technology*.
[2] The software was implemented by Dr. C. Pacher of the *Austrian Institute of Technology*.
[3] The software was implemented by Dr. Jesus Martinez Mateo from the *Universidad Politecnica de Madrid*.

A. Appendix

A.1. Runtime Analysis for Three Bases

Here we present the runtime analysis, as discussed in Chapter 5, for three basis (X, $Q_{\pi/4}$ and P) and combine it with the asymmetric CV-QKD protocol providing security against collective attacks[1].

We lift the runtime analysis presented in Section 5.4.1.3 to the runtime family F^2_{3,T_M,T_S} which describes two parties with three measurement basis and switching processes. We combine the runtime analysis later with the asymmetric CV-QKD protocol providing security against collective attacks and close with a discussion.

Runtime analysis:
We look at first at the transitions [Fel57] which are represented by their weights $q_{1,2}$, $q_{2,1}$, $q_{1,3}$, $q_{3,1}$, $q_{2,3}$ and $q_{3,2}$ of one participant, since the weights $q_{1,1}$, $q_{2,2}$ and $q_{3,3}$ correspond to the cases where no switching occurs. We can identify the weight of the switching processes by

$$\begin{aligned} q_{\text{sw}} &= \sum_{i\neq j} q_{i,j} \\ &= q_1q_2 + q_2q_1 + q_1q_3 + q_3q_1 + q_2q_3 + q_3q_2 \\ &= 2\cdot q_1q_2 + 2\cdot q_1q_3 + 2\cdot q_2q_3 \\ &= 2\cdot\left[q_1q_2 + \left(q_1+q_2\right)\cdot\left(1-q_1-q_2\right)\right] \end{aligned} \tag{A.1}$$

where we inserted $q_3 = \left(1-q_1-q_2\right)$.

Together with the Equations 5.3 and 5.4 we can identify the weight of the switching processes $\tilde{q}_{\text{sw}}$ and the renormalised weights $\tilde{q}_1$, $\tilde{q}_2$ and $\tilde{q}_3$ by

$$\tilde{q}_i = q_i \frac{1}{1+q_{\text{sw}}} \tag{A.2}$$

[1] Note, that we only focus on the collective protocol in this section as the coherent protocol does not call for the third basis $Q_{\pi/4}$.

with $i \in \{1,2,3\}$. The Figure A.1 illustrates the weight of the switching processes $\tilde{q}_{\text{sw}}$ as a function of q_1 and q_2.

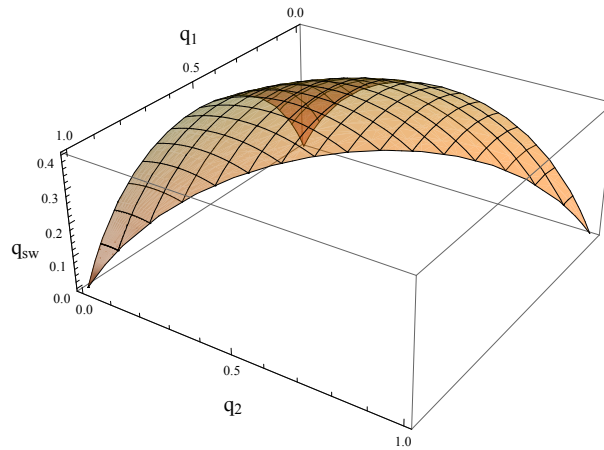

Figure A.1.: This figure illustrates the weight of $\tilde{q}_{\text{sw}}$ as a function of q_1 and q_2. Note that $q_3 = 1 - q_1 - q_2$ which confines the plot to the range $q_1 \in [0,1]$ and $q_2 \in [0, 1-q_1]$. The maximum of the weight of the switching processes $\tilde{q}_{\text{sw}} = 0.4$ is found at $q_1 = q_2 = q_3 = 1/3$.

A.1.1. Simulations

We restrict ourselves, for the reason of comparability, to as close as possible to the simulations which are presented in Section 5.4.1.3 and use the same covariance matrix describing an v-class state as follows

$$\gamma_{AB} = \left(\begin{array}{cc|cc} 0.541 & 0.135 & 0.459 & -0.095 \\ 0.135 & 24.633 & -0.037 & -23.293 \\ \hline 0.459 & -0.037 & 0.548 & 0.264 \\ -0.095 & -23.293 & 0.264 & 23.840 \end{array}\right).$$

We use the parameters presented in Table B.4 in the following simulations and know from Section 5.4.1.2 that the key is at best generated from the amplitude quadrature $q_X^{\text{key}} = 1$.

Let us now compare the performance of the asymmetric CV-QKD protocol

providing security against collective attacks with its symmetric variant in the following. We focus on CV-QKD runtime protocols of family F^2_{3,T_M,T_S}. The results of this computation are shown in Table B.11.

We again fix $\Delta T_{\text{sync}} = 1$ for the rest of the discussion and identify the weight of the amplitude (phase) quadrature $q_X = q_1$ ($q_P = q_2$) and the weight of the $Q_{\pi/4}$ quadrature $q_{\pi/4} = q_3$. Following the simulation explained in Section 5.4.1.3, at least $5 \cdot 10^6$ correlated tuples of any combination of X and P were assumed for the parameter estimation. We now include the $Q_{\pi/4}$ in the simulation to simulate a full tomography of the Gaussian state. Hence every participant has additionally to measure $5 \cdot 10^6$ outcomes in the $Q_{\pi/4}$ quadrature. Note that, in contrast to the amplitude and phase quadrature, the measurements in the $Q_{\pi/4}$ quadrature do not have to be correlated as explained in Section 3.5.

Asymmetric protocol:
We analyse the asymmetric protocol in this paragraph and generate the key from the amplitude quadrature assuming $N^{(1)}_{\text{key}} = 10^8$ correlated measurements of Alice and Bob in that quadrature.

The boundary conditions[2] for the computation of the q_i in the case of the asymmetric protocol allowing for F^2_{3,T_M,T_S} are

$$\begin{aligned} N^{(1)}_{\pi/4} &= 5 \cdot 10^6 = N \cdot \widetilde{q}^{(1)}_{\pi/4} \\ N^{(1)}_{P} &= 5 \cdot 10^6 = N \cdot \left(\widetilde{q}^{(1)}_{P}\right)^2 \\ N^{(1)}_{X} &= 10^8 + 5 \cdot 10^6 = N \cdot \left(\widetilde{q}^{(1)}_{X}\right)^2 \end{aligned}$$

where we use Equation A.2 to describe the $\widetilde{q}^{(1)}_X$.

We solve this system and find

$$\begin{aligned} q^{(1)}_P &= 0.174 \\ q^{(1)}_{\pi/4} &= 0.024 \\ q^{(1)}_X &= 0.802. \end{aligned}$$

[2] The number in parenthesis denotes the protocol under consideration. (1) represents the asymmetric protocol and (2) its symmetric variant.

The amount of time steps needed to satisfy the boundary conditions is $N = 2.953 \cdot 10^8$.

Taking the switching processes of the setup into consideration we arrive at

$$\begin{aligned}\widetilde{q}_P^{(1)} &= 0.132\\ \widetilde{q}_{\pi/4}^{(1)} &= 0.017\\ \widetilde{q}_X^{(1)} &= 0.605\\ \widetilde{q}_{\mathrm{sw}}^{(1)} &= 0.246.\end{aligned}$$

Symmetric protocol:
We use the same covariance matrix as in the analysis of the symmetric protocol and fix the number of time steps to be $N = 2.953 \cdot 10^8 = \text{const}$.

Remember that we distinguish asymmetric protocols ($q_X \neq q_P$) from symmetric protocols ($q_X = q_P$) by the weight of the bases which are used to generate the raw key. Note again that the $Q_{\pi/4}$ quadrature is only used for the parameter estimation which allows us to set $q_{\pi/4}^{(2)} \neq q_X^{(2)} = q_P^{(2)}$ even in the case of a symmetric CV-QKD protocol.

The boundary conditions for the computation of the weights are

$$\begin{aligned}\widetilde{q}_X^{(2)} &= \widetilde{q}_P^{(2)}\\ \widetilde{q}_{\pi/4}^{(2)} &= 5 \cdot 10^6 \cdot N\end{aligned} \tag{A.3}$$

We solve the system under the assumption of these runtime boundaries and find

$$\begin{aligned}q_X^{(2)} &= 0.487\\ q_{\pi/4}^{(2)} &= 0.026\\ q_P^{(2)} &= 0.487\end{aligned}$$

thereby maintaining $q_X^{(2)} = q_P^{(2)}$ during the key generation process, as is required by a symmetric protocol. Using the runtime analysis, we arrive at the following weights with switching processes

$$\begin{aligned}
\widetilde{q}_X^{(2)} &= 0.319 \\
\widetilde{q}_{\pi/4}^{(2)} &= 0.017 \\
\widetilde{q}_P^{(2)} &= 0.319 \\
\widetilde{q}_{\text{sw}}^{(2)} &= 0.345 \\
N_{\text{key}}^{(2)} &= \left[\left(\widetilde{q}_X^{(2)}\right)^2 + \left(\widetilde{q}_P^{(2)}\right)^2\right] \cdot N - 10^7 = 4.842 \cdot 10^8
\end{aligned}$$

where the $10^7 = 2 \cdot 5 \cdot 10^6$ account for the samples needed for the parameter estimation of the two quadratures. Note especially that $\widetilde{q}_{\pi/4}^{(2)} = \widetilde{q}_{\pi/4}^{(1)}$ as expected.

Key rates:
We can now compute the key rates of the two protocols on the basis of their amount of key generation samples, $N_{\text{key}}^{(1)} = 10^8$ and $N_{\text{key}}^{(2)} = 4.842 \cdot 10^8$.

Following the security analysis as described in Section 5.4.1 we find for the asymmetric protocol

$$\begin{aligned}
q_X^{\text{key},(1)} &= 1 \\
k_{\text{sec}}^{(1)} &= 0.789 \text{ Bit} \\
N_{\text{key}}^{(1)} &= 10^8 \\
|K_{\text{sec}}^{(1)}| &= 0.789 \cdot 10^8 = 78.94 \text{ MBit}
\end{aligned} \tag{A.4}$$

and for its symmetric variant

$$\begin{aligned}
q_X^{\text{key},(2)} &= 0.5 \\
k_{\text{sec}}^{(2)} &= 0.593 \text{ Bit} \\
N_{\text{key}}^{(2)} &= 0.484 \cdot 10^8 \\
|K_{\text{sec}}^{(2)}| &= 0.287 \cdot 10^8 = 28.71 \text{ MBit.}
\end{aligned} \tag{A.5}$$

The common parameter used to compare the two protocols is $T_{\text{run}} = 2.869 \cdot 10^8 \cdot \Delta T_{\text{sync}}$ ($N = 2.869 \cdot 10^8$). The key generated within T_{run} of the system for the asymmetric protocol is approximately $R_{1,2} = 2.750$ times larger than in case of its symmetric variant. Note here that we analysed CV-QKD protocols of family F^2_{3,T_M,T_S} by including the $Q_{\pi/4}$ quadrature in the computations.

The ratio between the asymmetric and the symmetric CV-QKD protocol which we analysed in Section 5.4.1.3 (see Equations 5.14 and 5.15) for the runtime family F^2_{2,T_M,T_S} was $R_{1,2} = 2.777$. Including the $Q_{\pi/4}$ quadrature in the analysis we presented above did not lower the ratio much, as expected. The reason is, that no simultaneous measurements of Alice and Bob in that quadrature are needed. One should note, that we found $N = 2.869 \cdot 10^8$ times steps in the above analysis which is more than we found in the analysis we presented in Section 5.4.1.3 ($N = 2.609 \cdot 10^8$) but still experimentally feasible.

We showed, that asymmetric CV-QKD protocols remain superior when compared with their symmetric variant even when the $Q_{\pi/4}$ quadrature is included.

A.2. Keyrates with Hybrid Reconciliation

In this section we combine the results of the CV-QKD protocols providing security against coherent attacks (see Section 5.4.2.2) and collective attacks (see Section 5.4.1.2) with the results of the simulations of the hybrid reconciliation from Section 6.3.7.6. Note especially that the choice of a specific q_X^{key} has an effect on the efficiency β_{EC} of the hybrid reconciliation as shown in Table 6.1 which is something we did not include in the CV-QKD simulations in Chapter 5 up to now. It is our aim to combine the computation of the secure rates as a function of q_X^{key} by considering the specific efficiency of the reconciliation protocol in use[3]. We again use the v-class and the s-class state (see Table B.1).

Remember that we discuss asymmetric CV-QKD protocols in this thesis which allows for a computation of the corresponding key rates as a function of $q_X^{\text{key}} \in [0,1]$, which describes the weights of the basis used for the key generation. This means that we have at first to establish the connection between the mixture of the amplitude and the phase sub-spaces and the correlation coefficient ρ. We later use the results which are given in Table 6.1 to estimate $\beta_{\text{EC}}\left(q_X^{\text{key}}, \rho\right)$ which allows us to compute $\ell(\beta_{\text{EC}})$. We finally compute the key rate considering the hybrid reconciliation as a function of q_X^{key}.

Mixture of states:
Let us start by describing the mixture of the amplitude γ^X_{AB} and the phase γ^P_{AB} phase sub-spaces as a function of q_X^{key}. We use the same technique as

[3] Note that we do not take the frame error rate into account.

in Section 3.4.3 and write it as a convex combination of the two according covariance matrices by

$$\gamma_{AB}^{q_X^{\text{key}}} = q_X^{\text{key}} \cdot \gamma_{AB}^{X} + \left(1 - q_X^{\text{key}}\right) \cdot \gamma_{AB}^{P}.$$

We furthermore use the scaling method which we propose in Section 6.3.7.1 to compute the correlation strength $\rho\left(\gamma_{AB}^{q_X^{\text{key}}}\right)$ as a function of q_X^{key}.

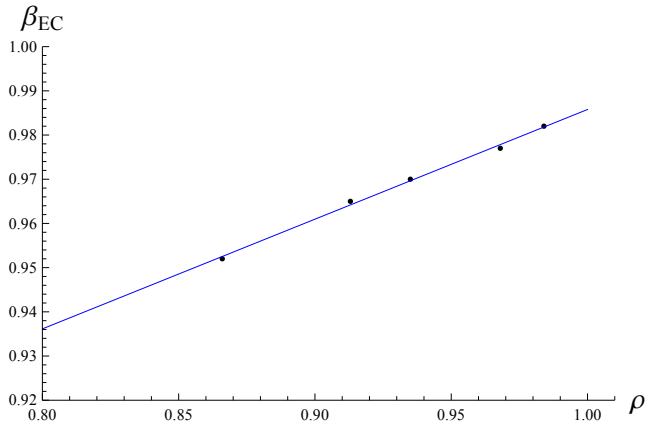

Figure A.2.: The efficiency β_{EC} as a function of the correlation strength ρ. The black points denote the numerical results of the simulations of the hybrid reconciliation. The blue line represents the estimated continuous linear function used to describe $\beta_{\text{EC}}(\rho)$ for $\rho \in [0.8, 1]$. The hybrid reconciliation we present in this thesis operates at best for $\rho \to 1$.

Hybrid reconciliation:
We connect now $\rho\left(\gamma_{AB}^{q_X^{\text{key}}}\right)$ with the efficiency $\beta_{\text{EC}}(\rho)$ of the hybrid reconciliation. We use the best results of the simulations of the hybrid reconciliation which are shown in Table 6.1 to estimate an continuous function which describes $\beta_{\text{EC}}(\rho)$. One can see in Figure A.2 that the following linear function suffices to approximately describe

$$\beta_{\text{EC}}(\rho) = 0.737 + 0.248 \cdot \rho \quad \forall \rho \in [0.8, 1].$$

Reconciliation efficiency:
Let us now compute the reconciliation efficiency $\beta_{\mathrm{EC}}\left(q_X^{\mathrm{key}}\right)$ for the v-class and the s-class state as a function of q_X^{key}. The Figures A.3 show the results of these computations assuming the hybrid reconciliation.

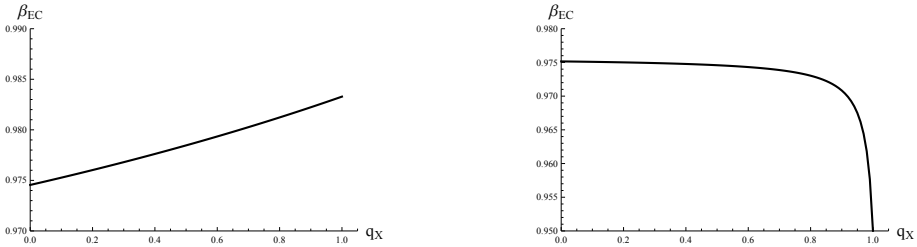

Figure A.3.: The reconciliation efficiency $\beta_{\mathrm{EC}}\left(q_X^{\mathrm{key}}\right)$ for the s-class (left figure) and the v-class (right figure) state as a function of q_X^{key}. We assume a perfect tomography of the states.

We can now include the estimation of the efficiency of the hybrid reconciliation $\beta_{\mathrm{EC}}\left(\gamma_{AB}^{q_X^{\mathrm{key}}}\right)$ as a function of q_X^{key} in the computation of the secure key rates by

$$k_{\mathrm{sec}}\left(q_X^{\mathrm{key}}\right) = k_{\mathrm{pot}}\left(q_X^{\mathrm{key}}\right) - \ell\left(\beta_{\mathrm{EC}}(q_X^{\mathrm{key}})\right).$$

Key rate of collective protocol:
The Figures A.4 show the secure key rates of the CV-QKD protocols providing security against collective attacks for the v-class and the s-class state as function of N_{key}.

Key rate of coherent protocol:
Figure A.5 shows the secure key rates of the CV-QKD protocols providing security against coherent attacks for the v-class and the s-class state as function of N_{key}.

We discuss the results in Section A.2.1.

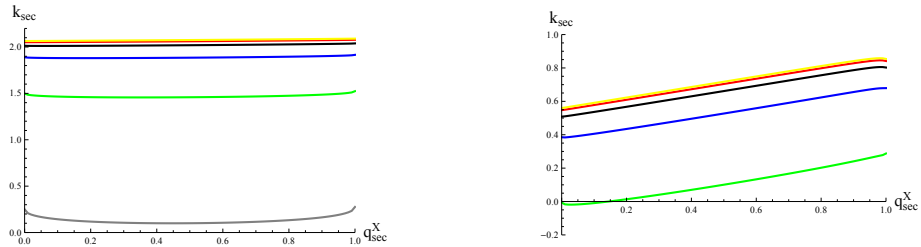

Figure A.4.: The key rate of the CV-QKD protocol providing security against collective attacks assuming an s-class state (left figure) and an v-class state (right figure) for six different values of $N_{\text{key}} \in \{10^9, 10^8, 10^7, 10^6, 10^5, 10^4\}$ (yellow, red, black, blue, green, grey) as a function of q_X^{key}. The maximum of the secure key rate for $N_{\text{key}} = 10^9$ is in case of the the s-class state $k_{\text{sec}} = 2.090$ Bit with $q_X^{\text{key}} = 1$. Note especially that the maximum of the secure key rate for $N_{\text{key}} = 10^9$ is in case of the the v-class state $k_{\text{sec}} = 0.858$ with $q_X^{\text{key}} = 0.98$.

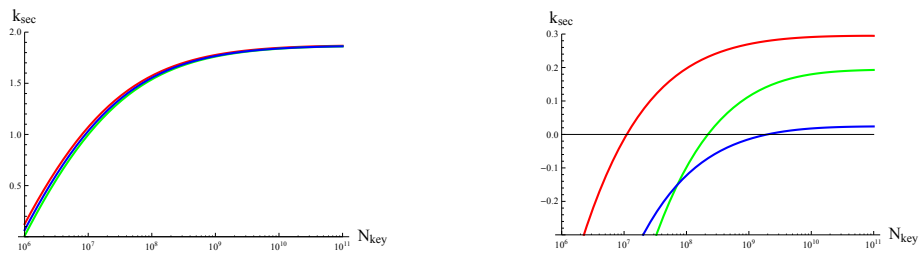

Figure A.5.: The key rate of the CV-QKD protocol providing security against collective attacks assuming an s-class state (left figure) and an v-class state (right figure) as a function of N_{key} and $q_X \in \{0, 0.5, 1\}$ (green, blue, red). The key rates saturate for $N_{\text{key}} > 10^9$. The maximum of the secure key rate for $N_{\text{key}} = 10^{10}$ is in case of the the s-class state $k_{\text{sec}} = 1.846$ Bit for $q_X^{\text{key}} = 1$ and in the case of the v-class state $k_{\text{sec}} = 0.294$ Bit for $q_X = 1$.

A.2.1. Discussion

In this Section we discuss the results of using the hybrid reconciliation in the new asymmetric CV-QKD protocols.

The efficiency of the hybrid reconciliation is for $\rho \in [0.8, 1]$ better than the efficiency we assume in Chapter 5 and in Table B.1 ($\beta_{\mathrm{EC}} = 0.9 = \mathrm{const}$). It follows that all the secure key rates we present in Section A.2 are higher when compared to the former results. Let us discuss the different cases in more detail:

V-class / Collective:
It is now possible to generate a secure key for $N_{\mathrm{key}} = 10^5$ using the symmetric CV-QKD protocol (see Section 5.4.1.2). Note that the key rate is maximised ($k_{\mathrm{sec}}^{q_X^{\mathrm{key}}} = 0.858$ Bit) for $q_X^{\mathrm{key}} = 0.98$ for $N_{\mathrm{key}} = 10^9$ which is different to the former results where the key rate was maximised for either $q_X^{\mathrm{key}} = 1$ or $q_X^{\mathrm{key}} = 0$. The reason is that the efficiency of the hybrid reconciliation decreases for $q_X^{\mathrm{key}} \to 1$. Remember that we assumed $\beta_{\mathrm{EC}} = \mathrm{const}$ in the former computations. This shows that it might not always be optimal to generate the key from one quadrature alone.

S-class / Collective:
Note that that the efficiency of the hybrid reconciliation is, in contrast to the v-class state, almost constant for all q_X^{key}. It follows that the characteristics of the key rate as a function of q_X^{key} is almost maintained while the key rate is increased by a constant factor. The key rate is maximised ($k_{\mathrm{sec}}^X = 2.090$ Bit) with $q_X^{\mathrm{key}} = 1$ for $N_{\mathrm{key}} = 10^9$. Note that it is now possible to generate a secure key for $N_{\mathrm{key}} = 10^4$.

V-class / Coherent:
It is now possible to generate a secure key when exercising the symmetric CV-QKD protocol as all key rates are increased when using the hybrid reconciliation in the classical post processing. The key rates become positive for smaller N_{key} for the same reason. The key rate is maximised ($k_{\mathrm{sec}}^X = 0.294$ Bit) for $N_{key} > 10^9$ when using the amplitude quadrature to generate the key.

S-class / Coherent:
The key rate is again almost constant for all q_X^{key}. It is maximised ($k_{\mathrm{sec}}^X = 1.846$ Bit) for $q_X^{\mathrm{key}} = 1$ and $N_{\mathrm{key}} > 10^9$. Remember that the maximum key rate when using polarisation-based QKD like BB84 [BB84] and E91 [Eke91] is one bit per measurement tuple. We can generate nearly 2 bit per correlated and simultaneous measurement of Alice and Bob.

We have shown that real-life implementations do, in general, not provide $\beta_{\mathrm{EC}} = \text{const}$. It is hence important to implement a model of a real-life reconciliation in the analysis of QKD setups. This leads sometimes to the case that the key generation using only one measurement quadrature $q_X^{\mathrm{key}} \in [0,1]$ might not always be the optimal choice.

A.3. Entropies

As the security proofs of Dr. F. Furrer and its extensions presented in this thesis in Chapter 5, heavily rely on the use of entropies, we will briefly review some basics of this topic in this section. Entropies are additionally used to analytically describe the optimal amount of the information disclosed in several reconciliation protocols (see Chapter 6). A good introduction into quantum information and quantum computation is presented in [NC00]. In [WPGP+12] a more general introduction in quantum information with Gaussian systems is provided. Note that this section is only meant as a remainder and does thus not contain anything new.

A.3.1. Shannon Entropy

We mainly use the Shannon entropy to describe the entropy between Alice's and Bob's raw keys in Chapter 6. For this task we first define the Shannon entropy of a random variable and secondly the conditional entropy between the raw keys of the two participants. Following Shannon's coding theorem [Sha48] one can find an approximately optimal protocol which corrects the errors between the raw keys thereby disclosing as little information as possible, which is given by the Shannon limit.

Let us start with one identically and independently distributed random variable X where we describe the realisations x of the random variable X by a finite alphabet χ_X with $x \in \chi_X$. The probabilities of the realisations x can be written in terms of probability mass $\mathcal{P}_X(x)$ whereby

$$\sum_{x \in \chi_X} \mathcal{P}_X(x) = 1.$$

The evaluation of a Gaussian system by the Shannon entropy is especially simple, as Gaussian systems can always be described by a classical distribution (the Gaussian function). We are now ready to define the Shannon en-

tropy by

$$\mathrm{S}(X) := -\sum_{x \in \chi_X} \mathcal{P}_X(x) \cdot \log_2[\mathcal{P}_X(x)].$$

Note that we define $0 \cdot \log(0) = 0$. For $|\chi_X| = 2$ and $\mathcal{P}_X(x_2) = 1 - \mathcal{P}_X(x_1)$ this gives rise to

$$\mathrm{S}(X) = -\mathcal{P}_X(x_1)\log_2[\mathcal{P}_X(x_1)] - (1-\mathcal{P}_X(x_1)) \cdot \log_2[1-\mathcal{P}_X(x_1)],$$

the binary entropy as shown in Figure A.6.

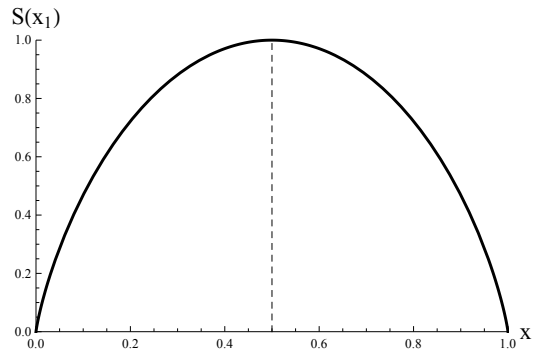

Figure A.6.: The entropy of a binary channel. It is a concave function being symmetric around $\mathcal{P}_X(x_1) = 0.5$.

A.3.1.1. Conditional Entropy

We now focus on the entropy of Alice's raw key conditioned on Bob's outcomes. For this task we introduce two alphabets χ_X and χ_Y for the two random variables X and Y. Let us assume that the realisations $x \in \chi_X$ are chosen i.i.d. from some classical distribution $\mathcal{P}_X(x)$. We furthermore assume that the probabilities of the realisations $y \in \chi_Y$ depend on x and write $\mathcal{P}_Y(y) = \mathcal{P}_{Y|X}(y|x)$. We define the conditional entropy by

$$\mathrm{S}(Y|X) := -\sum_{x \in \chi_X} \sum_{y \in \chi_Y} \mathcal{P}_X(x)\mathcal{P}_{Y|X}(y|x) \cdot \log_2\left[\mathcal{P}_{Y|X}(y|x)\right] \tag{A.6}$$

and identify

$$\mathcal{P}_{X,Y}(x,y) = \mathcal{P}_X(x)\mathcal{P}_{Y|X}(y|x) \tag{A.7}$$

as the joint probability. We rewrite for a particular realisation

$$\begin{aligned}\mathrm{S}(Y|X) &= -\sum_{x\in\chi_X}\sum_{y\in\chi_Y}\mathcal{P}_{X,Y}(x,y)\cdot\log_2\left[\mathcal{P}_{X,Y}(x,y)\right] \\ &\quad+\sum_{x\in\chi_X}\mathcal{P}_X(x)\cdot\log_2\left[\mathcal{P}_X(x)\right] \\ &= \mathrm{S}(Y,X)-\mathrm{S}(X),\end{aligned}$$

where we defined the joint entropy $\mathrm{S}(Y,X)$. Note, that the Shannon entropy assumes perfect tomography of the probabilities with which certain elements appear in their raw keys which is only possible if the raw keys are of infinite length.

A.3.1.2. Mutual Information

We ask for an entropic measure of the capability of Alice to predict Bob's outcome after her measurement or vice versa. We again start by introducing two alphabets χ_X and χ_Y whereby the realisations $x\in\chi_X$ are chosen i.i.d. from some classic distribution $\mathcal{P}_X(x)$ and assume that the probabilities of the realisations $y\in\chi_Y$ depend on x. The marginals of the distributions are

$$\begin{aligned}\mathcal{P}_X(x) &= \sum_{y\in\chi_Y}\mathcal{P}_{X,Y}(x,y) \\ \mathcal{P}_Y(y) &= \sum_{x\in\chi_X}\mathcal{P}_{X,Y}(x,y)\end{aligned}$$

and rewrite Equation A.7 to

$$\mathcal{P}_{X|Y}(x,y)=\frac{\mathcal{P}_{X,Y}(x,y)}{\mathcal{P}_Y(y)},$$

which is the conditional distribution. If the two realisations x and y are independent, the joint distribution $\mathcal{P}_{X|Y}(x|y)$ simplifies to $\mathcal{P}_X(x)\cdot\mathcal{P}_Y(y)$. As the distributions are in this case independent from one another we can use this to define the mutual information by

$$\begin{aligned}\mathrm{I}(X:Y) &= \sum_{x\in\chi_X}\sum_{y\in\chi_Y}\mathcal{P}_{X,Y}(x,y)\cdot\log_2\left[\frac{\mathcal{P}_{X,Y}(x,y)}{\mathcal{P}_X(x)\cdot\mathcal{P}_Y(y)}\right] \\ &= \mathrm{S}(X)-\mathrm{S}(X|Y) \\ &= \mathrm{S}(X)+\mathrm{S}(Y)-\mathrm{S}(X,Y).\end{aligned}$$

A.3.2. Von Neumann Entropy

The von Neumann entropy is a natural extension of the Shannon entropy to the quantum setting. We use it mainly to compute the secure key rates of the CV-QKD setup. We define the von Neumann entropy of a quantum mechanical system described by a density matrix ρ by

$$\mathrm{H}\left(\rho\right) = -\mathrm{tr}\left[\rho \log_2 \rho\right].$$

This equation can be further evaluated if we assume, that ρ is written in the eigen-basis

$$\rho = \sum_i \mathcal{P}_i \cdot |i\rangle\langle i|$$

where $\mathcal{P}_i$ is the normalised probability of measuring the state in the i'th eigen basis (realisation). It follows

$$\mathrm{H}\left(\rho\right) = -\sum_i \mathcal{P}_i \cdot \log_2 [\mathcal{P}_i]$$

where the connection to the Shannon entropy (up to some constant) is more obvious. The von Neumann entropy is normalised to the entropy of pure states. If we, for example, choose $\mathcal{P}_1 = 1$ and $\mathcal{P}_i = 0, \forall_{i>1}$ we see that $\mathrm{H}\left(\rho\right) = 0$. The evaluation of a Gaussian system by the von Neumann entropy is especially simple, as Gaussian systems can always be described by the covariance matrix.

A.3.3. (Smooth) Min-Max Entropies

The (smooth) min-max entropies are mainly used in the security proofs which we present in Chapter 5. One speciality of these entropies is that they describe the information that is transferred in one shot (one synchronised measurement) of Alice and Bob. In contrast to von-Neumann and Shannon entropies, which describe the transferred information only in the limit of infinitely many synchronised measurements, we can describe the information between Alice and Bob for finitely many samples N_{key} , which is more realistic.

One drawback of the (smooth) min-max entropies is, that they are hard to estimate as they are basically a mathematical tool. As classical systems can always be described by a Hilbert space, the min-max entropies can also be used for classical systems. The (smooth) min-max entropies were introduced

in the Ph.D.-thesis of Prof. Dr. R. Renner [Ren05]. Good references for details of these entropies are [Tom12] for the finite-dimensional and [Fur12] for the infinite dimensional case.

We start with defining the mathematical background by focusing on our setup, in particular on continuous variables. Let $\mathcal{H}$ be an infinite-dimensional separable Hilbert space and $S(\mathcal{H})$ the corresponding state space with all positive semi-definite trace class operators with trace 1. As usual we focus on $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ where $\mathcal{H}_A$ and $\mathcal{H}_B$ denote the sub-systems of Alice and Bob. let $\omega_{AB} \in \mathcal{H}_{AB}$ denote the bipartite state of the two participants and $\omega_A \in \mathcal{H}_A$ ($\omega_B \in \mathcal{H}_B$) the corresponding reduced states after measurement of the other participant, respectively.

We define the min-entropy of A conditioned on B for $\omega_{AB} \in S(\mathcal{H}_{AB})$ as

$$H_{\min}(A|B) = \sup_{\sigma_B \in S(B)} \left[sup \left\{ \lambda \in \mathbb{R} | \omega_{AB} \leq 2^{-\lambda} \mathbb{1}_A \otimes \sigma_B \right\} \right].$$

The min-entropy of a classical-quantum state ω_{XB} can be understood as the optimal guessing probability of the classical variable X conditioned on the quantum sub-system B. We refer to [KRS09] for a more detailed interpretation of the operational meaning of the min-entropy.

We now define the smoothed min-max entropies from the definition of the min entropy. To this end we focus on two states $\omega, \rho \in S(\mathcal{H}_{AB})$ and define the purified distance as

$$f(\omega, \rho) = \sqrt{1 - F(\omega, \rho)}$$

with

$$F(\omega, \rho) = \mathrm{tr}\left[|\sqrt{\omega}\sqrt{\rho}| \right] + \sqrt{(1 - \mathrm{tr}[\omega]) \cdot \left(1 - \mathrm{tr}\left[\rho\right]\right)}$$

being the generalised fidelity. We can now define the smoothed min-entropy of Alice being conditioned on Bob for $\omega_{AB} \in S(\mathcal{H}_{AB})$ as

$$H^{\epsilon}_{\min}(A|B) = sup \left[H_{\min}(A|B)_{\widetilde{\omega}_{AB}} \right]$$

with $\epsilon \geq 0$. The supremum is taken over-all $\widetilde{\omega}_{AB} \in S(\mathcal{H}_{AB})$ with $f(\widetilde{\omega}_{AB}, \omega_{AB}) \leq \epsilon$ which denotes the states $\widetilde{\omega}_{AB}$ lying in some ϵ-ball around ω_{AB}. In this sense the entropies are smoothed. We consider now an arbitrary purification ω_{ABC} of ω_{AB} and define the smoothed max-entropy of Alice conditioned on Bob by

$$H^{\epsilon}_{\max}(A|B)_{\omega_{ABC}} = -H^{\epsilon}_{\min}(A|B)_{\omega_{ABC}}.$$

Note that this equation is known as the duality relation between the smooth min / max entropies.

B. List of Tables

State	V-class	S-class
[3.6]: γ_{AB}	$\left(\begin{array}{cc\|cc} 0.541 & 0.135 & 0.459 & -0.095 \\ 0.135 & 24.633 & -0.037 & -23.293 \\ \hline 0.459 & -0.037 & 0.548 & 0.264 \\ -0.095 & -23.293 & 0.264 & 23.840 \end{array}\right)$	$\left(\begin{array}{cc\|cc} 19.696 & (0) & -19.678 & (0) \\ (0) & 23.311 & (0) & 23.708 \\ \hline -19.678 & (0) & 19.817 & (0) \\ (0) & 23.708 & (0) & 24.314 \end{array}\right)$
[3.21]: sqz_1	11.1 dB	10.3 dB
[3.21]: asqz_1	16.6 dB	14.9 dB
[3.21]: sqz_2	0 dB	10.9 dB
[3.21]: asqz_2	0 dB	15.3 dB
[4.8]: $\lambda^X_{A\|B}$	0.156	0.156
[4.8]: $\lambda^P_{A\|B}$	0.158	0.156
[4.8]: $\lambda^X_{B\|A}$	1.874	0.193
[4.8]: $\lambda^P_{B\|A}$	1.814	0.202
[6.5]: ρ^X	0.842	0.996
[6.5]: ρ^P	0.961	0.995
[4.10]: d_0^X	$32.992 \cdot \delta$	$31.596 \cdot \delta$
[4.10]: d_0^P	$109.451 \cdot \delta$	$35.542 \cdot \delta$
[3.12]: $\mathcal{E}^v(\gamma_{AB})$	1.933	3.402
[3.10] $\mu(\rho)$:	0.553	0.261
[5.21]: $k^{X,\mathrm{coh}}_{\mathrm{pot}}$	9.370 Bit	9.429 Bit
[5.7]: l^X_{EC}	7.447 Bit	7.702 Bit
[5.21]: $k^{P,\mathrm{coh}}_{\mathrm{pot}}$	7.697 Bit	9.269 Bit
[5.7]: l^P_{EC}	9.318 Bit	7.868 Bit
[5.18]: $k^{\mathrm{sym,coh}}_{\mathrm{pot}}$	8.304 Bit	9.347 Bit
[5.7]: $l^{\mathrm{sym}}_{\mathrm{EC}}$	8.382 Bit	7.785 Bit
[5.9]: $k^{X,\mathrm{col}}_{\mathrm{pot}}$	5.874 Bit	7.179 Bit
[5.7]: l^X_{EC}	5.068 Bit	5.379 Bit
[5.9]: $k^{P,\mathrm{col}}_{\mathrm{pot}}$	7.457 Bit	7.339 Bit
[5.7]: l^{EC}_P	7.032 Bit	5.532 Bit
[5.9]: $k^{\mathrm{sym,col}}_{\mathrm{pot}}$	6.665 Bit	7.259 Bit
[5.7]: $l^{\mathrm{sym}}_{\mathrm{EC}}$	6.050 Bit	5.455 Bit

Table B.1.: A characterisation of the two states which are published in [EHD+13, Ebe13]. The references label the equations used to compute the values. The equations are evaluated assuming perfect tomography, $N_{\mathrm{key}} = 10^8$ ($N_{\mathrm{key}} = 10^{10}$) for collective (coherent) attacks and direct reconciliation. The missing parameters are found in Tab. B.2 and Tab. B.3.

Parameter	Value
Security level	Collective attacks
Protocol parameter	Covariance matrix γ_{AB}
Reconciliation	Non-binary LDPC with efficiency $\beta_{\mathrm{EC}} = 0.9$
N_{tot}	Result
N_{key}	Result
δ	$\delta_X = \delta_P = 0.05$
α	$\alpha_X = \alpha_P = 50$
$\lvert\chi_{\mathrm{KG}}\rvert$	2000
ϵ_S	10^{-16}
ϵ_C	10^{-16}
ϵ_{pe}	10^{-10}
k_{sec}	Result
Runtime protocol	F_2^2
q_X^{key}	Variable
$\tilde{q}_X$	Result
T_{run}	Result
ΔT_{sync}	1

Table B.2.: The parameters for the runtime simulation of the CV-QKD protocol (member of family F_2^2) providing security against collective attacks. An v-class state has been used in this simulation (see therefore Table B.1).

Parameter	Value
Security level	Coherent attacks
Protocol parameter	Hamming distance d_0
Reconciliation	Non-binary LDPC with efficiency $\beta_{\mathrm{EC}} = 0.9$
N_{tot}	Result
N_{key}	Result
δ	$\delta_X = \delta_P = 0.01$
α	$\alpha_X = \alpha_P = 70$
$\lvert\chi_{\mathrm{KG}}\rvert$	14000
ϵ_S	10^{-16}
ϵ_C	10^{-16}
ϵ_{pe}	10^{-10}
k_{sec}	Result
Runtime protocol	F_2^2
q_X^{key}	Variable
$\tilde{q}_X$	Result
T_{run}	Result
ΔT_{sync}	1

Table B.3.: The parameters for the runtime simulation of the CV-QKD protocol (member of family F_2^2) being secure against coherent attacks. An s-class state has been used in this simulation (see therefore Table B.1).

Parameter	Value
Security level	Collective attacks
Protocol parameter	Covariance matrix γ_{AB}
Reconciliation	Non-binary LDPC with efficiency $\beta_{\mathrm{EC}} = 0.9$
N_{tot}	Result
N_{key}	Result
δ	$\delta_X = \delta_P = 0.05$
α	$\alpha_X = \alpha_P = 50$
$\lvert\chi_{\mathrm{KG}}\rvert$	2000
ϵ_S	10^{-16}
ϵ_C	10^{-16}
ϵ_{pe}	10^{-10}
k_{sec}	Result
Runtime protocol	F_3^2
q_X^{key}	Variable
q_P^{key}	Variable
$\tilde{q}_X$	Result
$\tilde{q}_P$	Result
q_X	Variable
q_P	Variable
T_{run}	Result
ΔT_{sync}	1

Table B.4.: The parameters for the runtime simulation of the CV-QKD protocol (member of family F_3^2) being secure against collective attacks. An v-class state has been used in this simulation (see therefore Table B.1).

Parameter	Value
Security level	Collective attacks
Protocol parameter	Covariance matrix γ_{AB}
Reconciliation	Binary LDPC
N_{tot}	$2 \cdot 10^8$
N_{key}	$1.15 \cdot 10^8$
$\delta_X = \delta_P$	$\frac{2 \cdot 29.778}{64} \cdot 0.832$
α_X	26
α_P	29
$\lvert\chi_{\text{KG}}\rvert$	$64 = 2^6$
q_X^{key}	0.5
k_{sec}	0.102 Bit
ϵ_S	10^{-16}
ϵ_C	10^{-16}
ϵ_{pe}	10^{-10}

Table B.5.: The parameters for the experiment using the CV-QKD protocol (member of family $F^2_{2,T_{MS}}$) being secure against collective attacks. An s-class state has been used in this experiment (see Table B.1).

Parameter	Value
Security level	Not relevant
Protocol parameter	Covariance matrix γ_{AB}
N_{key}	$5 \cdot 10^5$
δ	Result
α_{EC}	45
$\lvert\chi_{\text{KG}}\rvert$	Result
q_X^{key}	1
DN	0.01
Reconciliation	Hybrid reconciliation
$\lvert\chi_1\rvert$	128
$\lvert\chi_2\rvert$	$\{1, 2, ...50\}$

Table B.6.: The parameters for the numerical simulation of the behaviour of the hybrid reconciliation. A theoretically generated s-class state with $\text{sqz}_{1,2} = 10$ and $\text{asqz}_{1,2} = 10$ has been used in this simulation (see Section 3.4.1).

Parameter	Value
Security level	Coherent attacks
Protocol parameter	Hamming distance d_0
Reconciliation	Non-binary LDPC ($\beta_{\mathrm{EC}} = 0.946$)
N_{tot}	$2 \cdot 10^8$
N_{key}	$0.85 \cdot 10^8$
$\delta_X = \delta_P$	0.0298
$\alpha_X = \alpha_P$	61.1
$\lvert\chi_{\mathrm{KG}}\rvert$	2^{12}
q_X^{key}	0.5
$\widetilde{q}_X$	0.5
ϵ_S	10^{-10}
ϵ_C	$2 \cdot 10^{-10}$
ϵ_{pe}	10^{-10}
k_{sec}	1.14 Bit

Table B.7.: The parameters for the experiment using the CV-QKD protocol (member of family $F^2_{2,T_{MS}}$) being secure against coherent attacks. An s-class state has been used in this experiment (see Table B.1).

Coeff. $\lambda(x)$	$GF(2^4 = 16)$ $R = 0.85$	$GF(2^5 = 32)$ $R = 0.9$	$GF(2^6 = 64)$ $R = 0.9$
λ_2	0.62755	0.67173	0.81173
λ_5	0	0	0.00710
λ_6	0.03896	0.00164	0
λ_7	0	0.00481	0
λ_8	0	0.01342	0.01004
λ_{10}	0.02497	0	0
λ_{11}	0.01158	0	0
λ_{14}	0.00598	0.02081	0
λ_{15}	0.03557	0	0.17113
λ_{16}	0	0.28759	0
λ_{17}	0.20497	0	0
λ_{19}	0.05042	0	0

Table B.8.: The generating polynomials which describe the ensemble of irregular codes which are used in Figure 6.20.

Parameter	Value
T_{run}	$2.609 \cdot 10^8 \cdot \Delta T_{\text{sync}}$
Asymmetric CV-QKD	
Measurement tuples	$\left(\begin{array}{cc\|cc} 166 & 0 & 105 & 23 \\ 0 & 36 & 23 & 5 \\ \hline 105 & 23 & 166 & 0 \\ 23 & 5 & 0 & 36 \end{array}\right)$
Parameter estimation	$\left(\begin{array}{cc\|cc} 66 & - & 5 & 23 \\ - & 36 & 23 & 5 \\ \hline 5 & 23 & 66 & - \\ 23 & 5 & - & 36 \end{array}\right)$
Key generation	$\left(\begin{array}{cc\|cc} 100 & - & 100 & - \\ - & - & - & - \\ \hline 100 & - & 100 & - \\ - & - & - & - \end{array}\right)$
q_X^{key}	1
k_{sec}	0.789 Bit
N_{key}	10^8
Symmetric CV-QKD	
Measurement tuples	$\left(\begin{array}{cc\|cc} 87 & 0 & 29 & 29 \\ 0 & 87 & 29 & 29 \\ \hline 29 & 29 & 87 & 0 \\ 29 & 29 & 0 & 87 \end{array}\right)$
Parameter estimation tuples	$\left(\begin{array}{cc\|cc} 63 & - & 5 & 29 \\ - & 63 & 29 & 5 \\ \hline 5 & 29 & 63 & - \\ 29 & 5 & - & 63 \end{array}\right)$
Key generation samples	$\left(\begin{array}{cc\|cc} 24 & - & 24 & - \\ - & 24 & - & 24 \\ \hline 24 & - & 24 & - \\ - & 24 & - & 24 \end{array}\right)$
q_X^{key}	0.5
k_{sec}	0.593 Bit
N_{key}	$0.479 \cdot 10^8$

Table B.9.: The results of the simulation considering two bases assuming collective attacks. This table shows the total number of measurements, the number of measurements used for parameter estimation and the key generation samples of the different combinations of the quadratures in units of 10^6. The '—' denotes the entries which are not needed / considered to fulfill the corresponding task.

Parameter	Value
T_{run}	$5.087 \cdot 10^8 \cdot \Delta T_{\text{sync}}$
Asymmetric CV-QKD	
Measurement tuples	$\left(\begin{array}{cc\|cc} 226 & 0 & 100 & 55 \\ 0 & 124 & 55 & 30 \\ \hline 100 & 55 & 226 & 0 \\ 55 & 30 & 0 & 124 \end{array}\right)$
Parameter estimation tuples	$\left(\begin{array}{cc\|cc} - & - & - & - \\ - & - & - & 30 \\ \hline - & - & - & - \\ - & 30 & - & - \end{array}\right)$
Key generation samples	$\left(\begin{array}{cc\|cc} - & - & 100 & - \\ - & - & - & - \\ \hline 100 & - & - & - \\ - & - & - & - \end{array}\right)$
q_X^{key}	1
k_{sec}	0.891 Bit
N_{key}	10^8
Symmetric CV-QKD	
Measurement tuples	$\left(\begin{array}{cc\|cc} 170 & 0 & 57 & 57 \\ 0 & 170 & 57 & 57 \\ \hline 57 & 57 & 170 & 0 \\ 57 & 57 & 0 & 170 \end{array}\right)$
Parameter estimation tuples	$\left(\begin{array}{cc\|cc} - & - & 15 & - \\ - & - & - & 15 \\ \hline 15 & - & - & - \\ - & 15 & - & - \end{array}\right)$
Key generation samples	$\left(\begin{array}{cc\|cc} 42 & - & 42 & - \\ - & 42 & - & 42 \\ \hline 42 & - & 42 & - \\ - & 42 & - & 42 \end{array}\right)$
q_X^{key}	0.5
k_{sec}	0.791 Bit
N_{key}	$0.830 \cdot 10^8$

Table B.10.: The results of the simulation considering two bases assuming coherent attacks. This table shows the total number of measurements, the number of measurements used for parameter estimation and the key generation samples of the different combinations of the quadratures in units of 10^6. The '—' denotes the entries which are not needed to fulfill the corresponding task.

Parameter	Value
T_{run}	$2.953 \cdot 10^8 \cdot \Delta T_{\text{sync}}$
Asymmetric CV-QKD	
Measurement tuples	$\left(\begin{array}{cc\|cc} 174 & 5 & 105 & 23 \\ 5 & 38 & 23 & 5 \\ \hline 105 & 23 & 174 & 5 \\ 23 & 5 & 5 & 38 \end{array}\right)$
Parameter estimation tuples	$\left(\begin{array}{cc\|cc} 74 & 5 & 5 & 23 \\ 5 & 38 & 23 & 5 \\ \hline 5 & 23 & 74 & 5 \\ 23 & 5 & 5 & 38 \end{array}\right)$
Key generation samples	$\left(\begin{array}{cc\|cc} 100 & - & 100 & - \\ - & - & - & - \\ \hline 100 & - & 100 & - \\ - & - & - & - \end{array}\right)$
q_X^{key}	1
k_{sec}	0.789 Bit
N_{key}	10^8
Symmetric CV-QKD	
Measurement tuples	$\left(\begin{array}{cc\|cc} 91 & 5 & 29 & 29 \\ 5 & 91 & 29 & 29 \\ \hline 29 & 29 & 91 & 5 \\ 29 & 29 & 5 & 91 \end{array}\right)$
Parameter estimation tuples	$\left(\begin{array}{cc\|cc} 67 & 5 & 5 & 29 \\ 5 & 67 & 29 & 5 \\ \hline 5 & 29 & 67 & 5 \\ 29 & 5 & 5 & 67 \end{array}\right)$
Key generation samples	$\left(\begin{array}{cc\|cc} 24 & - & 24 & - \\ - & 24 & - & 24 \\ \hline 24 & - & 24 & - \\ - & 24 & - & 24 \end{array}\right)$
q_X^{key}	0.5
k_{sec}	0.593 Bit
N_{key}	$0.484 \cdot 10^8$

Table B.11.: The results of the simulation considering three bases assuming collective attacks. This table shows the total number of measurements, the number of measurements used for parameter estimation and the key generation samples of the different combinations of the quadratures in units of 10^6. The '—' denotes the entries which are not needed to fulfill the corresponding task.

Danksagung

Nun möchte ich mich abschließend endlich bei all jenen bedanken, die mir bei meiner Promotion zur Seite gestanden haben.

Ich danke Prof. Dr. Reinhard Werner für die fachliche Unterstützung und darüber hinaus für die Gestaltungsmöglichkeiten bei der Ausübung meiner wissenschaftlichen Tätigkeit.

Ich danke Prof. Dr. Andreas Ruschhaupt für die freundliche Übernahme des Korreferats und die Betreuung meiner Diplomarbeit. Bei Herrn Prof. Dr. Haug bedanke ich mich für den Vorsitz der Prüfungskommission.

Im Laufe meiner Tätigkeit in der Arbeitsgruppe *Quanteninformation* habe ich viele Mitarbeiter besser kennengelernt und auch einige Freundschaften geschlossen. In diesem Sinne danke ich Dr. Torsten Franz, Dr. Fabian Furrer, Msc. Ash Milsted, Dipl.-Phys. Markus Otto, Dr. Sönke Schmidt und Msc. Leander Fiedler für die gute Zeit, die wir gemeinsam hatten und haben. An dieser Stelle danke ich auch der gesamten Arbeitsgruppe *Quanteninformation* für das angenehme Arbeitsklima und den freundlichen Umgang.

Für das Lektorat dieser Arbeit danke ich Dr. Ciara Morgan, Msc. Kais Abdelkhalek, Dipl. Phys. Fabian Transchel, Msc. Rene Schwonnek und Dr. Christoph Pacher.

Auf der fachlichen Seite danke ich ausserdem Prof. Dr. Roman Schnabel, Dr. Tobias Gehring und Dr. Jesus Martinez Mateo für die vielen guten Ideen und die erfolgreiche Zusammenarbeit.

Ausserdem danke ich Wiebke Möller und Birgit Ohlendorf für die Unterstützung in formalen Angelegenheiten und ein stets offenes Ohr.

Für langjährige Freundschaft und gute Zeiten danke ich Maria Cramm, Dominik Müller, Dominik Härke, Martin Adamczyk, Kathrin Goltz, Matthias Romaniuk, Jann Lengert, Arke Vogell, Marcin Zarzycki, Timo Ferber und Florian Gebert.

Insbesondere danke ich meiner Lebensgefährtin Monika Kotzian für die Unterstützung, die Liebe und die Geduld, die sie mir entgegen bringt. Außerdem danke ich ihrer Familie - Eva, Martina, Helmuth und Siglinde Kotzian für die vielen schönen Zeiten. Weiterhin danke ich meiner Familie (Sigrid Niehüser, Josef Duhme, Stefanie Schrader) für die Ablenkungen während des Verfassens dieser Doktorarbeit.

Diese Arbeit widme ich Karsten Niehüser.

Vielen Dank

Jörg Duhme

Bibliography

[Abb99] J. Abbate. *Inventing the Internet.* MIT University Press, 1999.

[Aea12] J. Abadien et al. A gravitational wave observatory operating beyond the quantum shot-noise limit. *Nat. Phys.*, 7(12):1745–2473, 2012.

[Aea13] J. Aasi et al. Enhanced sensitivity of the ligo gravitational wave detector by using squeezed states of light. *Nat. Phot.*, 7(8):613 – 619, June 2013.

[ANS+11] 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. *Opt. Lett.*, 36(17):3467–3469, 2011.

[BB84] C. H. Bennett and G. Brassard. Public key distribution and coin tossing. *Proceedings of IEEE*, 175:8, 1984.

[BBB+92] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5(1):3, 1992.

[BBCM95] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer. Generalized privacy amplification. *Information Theory, IEEE Transactions on*, 41(6):1915–1923, Nov 1995.

[BBR88] C. H. Bennett, G. Brassard, and J.-M. Robert. Privacy amplification by public discussion. *SIAM Journal on Computing*, 17(2):210, 1988.

[BCF+13] M. Berta, M. Christandl, F. Furrer, S. Scholz, and M. Tomamichel. Continuous variable entropic uncertainty relations in the presence of quantum memory. *arXiv:1308.4527*, pages 1–27, 2013.

[BD03] L. Barnault and D. Declercq. Fast decoding algorithm for LDPC over GF(2^q). In *ITW 2003, IEEE Information Theory Workshop*, pages 70–73, March 2003.

[BDP+10] G. Nocerino Buono, D. and, V. D'Auria, A. Porzio, S. Olivares, and M. G. A. Paris. Quantum characterization of bipartite gaussian states. *J. Opt. Soc. Am. B*, 27(6):A110–A118, Jun 2010.

[BFS11] M. Berta, F. Furrer, and V. B. Scholz. The Smooth Entropy Formalism on von Neumann Algebras. *arXiv:1107.5460v1*, 2011.

[BH12] J. C. A. Barata and M. S. Hussein. The moore-penrose pseudoinverse. a tutorial review of the theory. *Braz. J. Phys.*, pages 146–165, 2012.

[BLMS00] G. Brassard, N. Lütkenhaus, T. Mor, and B. Sanders. Limitations on practical quantum cryptography. *Phys. Rev. Lett.*, 85:1330–1333, Aug 2000.

[BMSH+13] J. P. Bourgoin, E. Meyer-Scott, B. L. Higgins, B. Helou, C. Erven, H. Hübel, B. Kumar, D. Hudson, I. D'Souza, R. Girard, R. Laflamme, and T. Jennewein. A comprehensive design and performance analysis of low earth orbit satellite quantum communication. *New Journal of Physics*, 15(2):023006, 2013.

[BND+10] D. Buono, G. Nocerino, V. D'Auria, A. Porzio, S. Olivares, and M. G. A. Paris. Quantum characterization of bipartite gaussian states. *J. Opt. Soc. Am. B*, 27:A110–A118, 2010.

[Bru03] D. Bruß. *Quanteninformation*. Fischer Taschenbuch Verlag, 2003.

[BS93] G. Brassard and L. Salvail. Secret-key reconciliation by public discussion. In *Workshop on the theory and application of cryptographic techniques on Advances in cryptology*, volume 765, pages 410–423. Springer, 1993.

[BSMM00] I. N. Bronstein, K. A. Semendjajew, G. Musiol, and H. Mühling. *Taschenbuch der Mathematikt*. Verlag Harri Deutsch, 2000.

[BTMM06] M. Bloch, A. Thangaraj, S. W. McLaughlin, and J. M. Merolla. LDPC-based Gaussian key reconciliation. In *ITW 2006, IEEE Information Theory Workshop*, pages 116–120, March 2006.

[BvL05] S. L. Braunstein and P. van Loock. Quantum information with continuous variables. *Rev. Mod. Phys.*, 77:513–577, 2005.

[Can01] R. Canetti. Universal composable security: A new paradigm for cryptographic protocols. *Proceedings IEEE*, 42:136–145, 2001.

[CBMS13] A. Christ, B. Brecht, W. Mauerer, and S. Silberhorn. Theory of quantum frequency conversion and type-ii parametric down-conversion in the high-gain regime. *New Journal of Physics*, 15(5):053038, 2013.

[CKW00] V. Coffman, J. Kundu, and W. K. Wootters. Distributed entanglement. *Phys. Rev. A*, 61, 2000.

[CLA01] N. J. Cerf, M. Lévy, and G. Van Assche. Quantum distribution of Gaussian keys using squeezed states. *Phys. Rev. A*, 63:052311, 2001.

[CLS+04] J. Chiaverini, D. Leibfried, T. Schätz, M. D. Barrett, R. B. Blakestad, J. Britton, W. M. Itano, J. D. Jost, E. Knill, C. Langer, R. Ozeri, and D. J. Wineland. Realization of quantum error correction. *Nature*, 432:602–605, 2004.

[Col09] The Virgo Collaboration. Advanced virgo baseline desig, 2009. https://tds.ego-gw.it/ql/?c=6589.

[CPM+98] D. Cory, M. Price, W. Maas, E. Knill, R. Laflamme, W. Zurek, T. Havel, and S. Somaroo. Experimental quantum error correction. *Phys. Rev. Lett.*, 81:2152–2155, Sep 1998.

[CVA03] J. Cardinal and G. Van Assche. Construction of a shared secret key using continuous variables. In *ITW 2003, IEEE Information Theory Workshop*, pages 135–138, March 2003.

[CVDS07] S. Chelkowski, H. Vahlbruch, K. Danzmann, and R. Schnabel. Coherent control of broadband vacuum squeezing. *Phys. Rev. A*, 75:043814, Apr 2007.

[DF07] D. Declercq and M. Fossorier. Decoding algorithms for nonbinary LDPC codes over GF(q). *IEEE Transactions on Communications*, 55(4):633–643, April 2007.

[DFSW10a] J. Duhme, T. Franz, S. Schmidt, and R. F. Werner. Quanteninformationstheorie Teil 1: Grundlagen; Verschränkung - Schlüssel zur Quantenwelt. *Physik in unserer Zeit*, 41(5):236, 2010.

[DFSW10b] J. Duhme, T. Franz, S. Schmidt, and R.F. Werner. Quanteninformationstheorie Teil 2: Anwendungen; Geheime Nachrichten und schnelle Rechner. *Physik in unserer Zeit*, 41(6):292, 2010.

[DHF+07] J. DiGuglielmo, B. Hage, A. Franzen, J. Fiurasek, and R. Schnabel. Experimental characterization of gaussian quantum-communication channels. *Phys. Rev. A*, 76:012323, 2007.

[DiG10] J. DiGuglielmo. *On the Experimental Generation and Characterization of Entangled States of Light*. PhD thesis, Leibniz University Hannover, 2010.

[Ebe09] T. Eberle. Squeezed light enhanced fibre sagnac interferometer. Diplomarbeit, University of Heidelberg, 2009.

[Ebe13] T. Eberle. *Realization of Finite-Size Quantum Key Distribution based on Einstein-Podolsky-Rosen Entangled Light*. PhD thesis, Leibniz University Hannover, 2013.

[EHD+11] T. Eberle, V. Händchen, J. Duhme, T. Franz, R.F. Werner, and R. Schnabel. Strong Einstein-Podolsky-Rosen entanglement from a single squeezed light source. *Phys. Rev. A*, 83:052329, 2011.

[EHD+13] T. Eberle, V. Händchen, J. Duhme, T. Franz, F. Furrer, Schnabel R., and R.F. Werner. Gaussian entanglement for quantum key distribution from a single-mode squeezing source. *New Journal of Physics*, 15:053049, 2013.

[EHS13] T. Eberle, V. Händchen, and R. Schnabel. Stable control of 10 db two-mode squeezed vacuum states of light. *Opt. Express*, 21(9):11546–11553, May 2013.

[Eke91] A. K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663, 1991.

[EMLW09] C. Erven, X. Ma, R. Laflamme, and G. Weihs. Entangled quantum key distribution with a biased basis choice. *New Journal of Physics*, 11(4):045025, 2009.

[EMMM11] D. Elkouss, J. Martinez-Mateo, and V. Martin. Information reconcilliation for quantum key distribution. *Quantum Information and Computation*, 11:226–238, 2011.

[ESB+10] 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. *Phys. Rev. Lett.*, 104:251102, 2010.

[ESP02] J. Eisert, S. Scheel, and M. B. Plenio. Distilling gaussian states with gaussian operations is impossible. *Phys. Rev. Lett.*, 89:137903, 2002.

[FAR11] F. Furrer, J. Aberg, and R. Renner. Min- and max-entropy in infinite domensions. *Communications in Mathematical Physics*, 306:165–186, 2011.

[Fel57] W. Feller. *An introduction to probability theory and its applications*. Encyclopedia of Mathematics, 1957.

[FFB+14] F. Furrer, T. Franz, M. Berta, A. Leverrier, B. Scholz, V. M. Tomamichel, and F. Werner, R.˙ Erratum: Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks. *Phys. Rev. Lett.*, 112:019902, 2014.

[FFW11] T. Franz, F. Furrer, and R. F. Werner. Extremal quantum correlations and cryptographic security. *Phys. Rev. Lett.*, 106:250502, 2011.

[FHD+06] A. Franzen, B. Hage, J. DiGuglielmo, J. Fiurasek, and R. Schnabel. Experimental demonstration of continuous variable purification of squeezed states. *Phys. Rev. Lett.*, 97:150505, 2006.

[Fra13] T. Franz. *Quantum Correlations and Quantum Key Distribution*. PhD thesis, Leibniz University Hannover, 2013.

[Fur12] F. Furrer. *Security of Continuous-Variable Quantum Key Distribution and Aspects of Device-Independent Security*. PhD thesis, Leibniz University Hannover, 2012.

[Fur14] F. Furrer. Reverse-reconciliation continuous-variable quantum key distribution based on the uncertainty principle. *Phys. Rev. A*, 90:042325, Oct 2014.

[FWN+10] M. Fürst, H. Weier, S. Nauerth, D.G. Marangon, C. Kurtsiefer, and H. Weinfurter. High speed optical quantum random number generation. *Opt. Express*, 18(12):13029, 2010.

[Gal63] R. G. Gallager. *Low Density Parity Check Codes*. PhD thesis, M. I. T. Press, 1963.

[GC08] H. Grote and LIGO Scientific Collaboration. The status of geo 600. *Classical and Quantum Gravity*, 25(11):114043, 2008.

[GG02] F. Grosshans and P. Grangier. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.*, 88:057902, 2002.

[GHD+14] T. Gehring, V. Händchen, J. Duhme, F. Furrer, T. Franz, C. Pacher, R. F. Werner, and R. Schnabel. Arbitrary-attack-proof quantum key distribution without single photons. *ArXiV*, page 6, 2014.

[GK05] C. C. Gerry and P. L. Knight. *Introductory Quantum Optics*. Cambridge University Press, 2005.

[Gni14] J. Gniesmer. Verteilung nicht-klassischer zustände des lichts über eine glasfaser von 1 km länge. Masterarbeit, Leibniz University Hannover, 2014.

[GP01] D. Gottesman and J. Preskill. Secure quantum key distribution using squeezed states. *Phys. Rev. A*, 63:022309, 2001.

[Gra53] F. Gray. Pulse code communication, March 17 1953. US Patent 2,632,058.

[GtLSC10] M. H. Gregory and the LIGO Scientific Collaboration. Advanced ligo: the next generation of gravitational wave detectors. *Classical and Quantum Gravity*, 27(8):084006, 2010.

[Hae10] V. Haendchen. Verschränkte lichtfelder bei 1550 nm für faserbasierte quantenschlüsselverteilung. Diplomarbeit, Leibniz University Hannover, 2010.

[Hän10] E. Hänggi. *Device-independent quantum key distribution*. PhD thesis, ETH Zurich, 2010.

[HDF+08] B. Hage, J. DiGuglielmo, A. Franzen, J. Fiurasek, and R. Schnabel. Preparation of distilled and purified continuous-variable entangled states. *Nature Physics*, 4:915–918, 2008.

[HEA05] Xiao-Yu Hu, E. Eleftheriou, and D.-M. Arnold. Regular and irregular progressive edge-growth tanner graphs. *IEEE Transactions on Information Theory*, 51(1):386–398, January 2005.

[Hei27] W Heisenberg. Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik. *Zeitschrift für Physik*, page 26, 1927.

[HES+12] V. Händchen, 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.

[HOSW84] M. Hilery, R.F. O'Connell, M.O. Scully, and E.P. Wigner. Distribution functions in physics: fundamentals. *Physics Reports*, 106:121, 1984.

[Inf01] Federal Information. Announcing the advanced encryption standard (aes). *Processing Standards Publication 197*, 2001.

[JEKJ14] P. Jouguet, D. Elkouss, and S. Kunz-Jacques. High-bit-rate continuous-variable quantum key distribution. *Phys. Rev. A*, 90(4):042329, October 2014.

[JKJL11] P. Jouguet, S. Kunz-Jacques, and A. Leverrier. Long-distance continuous-variable quantum key distribution with a gaussian modulation. *Phys. Rev. A*, 84(6):062317, December 2011.

[JKJL13] P. Jouguet, S. Kunz-Jacques, and A. Leverrier. High performance error correction for quantum key distribution using polar codes. *Quantum Information & Computation*, 14(3&4):329–338, 2013.

[JW07] R. Johnson and D. Wichern. *Applied multivariate statistical analysis*. Pearson Prentice Hall, 2007. ISBN 978-0135143506.

[KMS10] K. Kasai, R. Matsumoto, and K. Sakaniwa. Information reconciliation for QKD with rate-compatible non-binary LDPC codes. In *2010 International Symposium on Information Theory and its Applications (ISITA)*, pages 922–927, October 2010.

[KRS09] R. Koenig, R. Renne, and C. Schaffner. The operational meaning of min- and max-entropy. *IEEE Trans. Inf. Th.*, page 11, 2009.

[KW10] J. Kiukas and R. F. Werner. Maximal violation of bell inequalities by position measurements. *J. Math. Phys.*, page 072105, 2010.

[LAB+08a] A. Leverrier, R. Alleaume, J. Boutros, G. Zemor, and P. Grangier. Multidimensional reconciliation for a continuous-variable quantum key distribution. *Phys. Rev. A*, 77(4):042325, April 2008.

[LAB+08b] A. Leverrier, R. Alleaume, J. Boutros, G. Zemor, and P. Grangier. Multidimensional reconciliation for continuous-variable quantum key distribution. In *ISIT 2008, IEEE International Symposium on Information Theory*, pages 1020–1024, July 2008.

[LGG10] A. Leverrier, F. Grosshans, and P. Grangier. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A*, 81:062343, 2010.

[LHA+01] A. I. Lvovsky, H. Hansen, T. Aichele, O. Benson, J. Mlynek, and S. Schiller. Quantum state reconstruction of the single-photon fock state. *Phys. Rev. Lett.*, 87:050402, 2001.

[Lou97] R. Loudon. *The Quantum Theory of Light*. Oxford Science Publications, 1997.

[LR38] E. H. Lieb and M. B. Ruskai. Proof of the strong subadditivity of quantum mechanical entropy. *Journ. Math. Phys.*, page 14, 1938.

[MAE+11] M. Mehmet, A. Ast, T. Eberle, S. Steinlechner, H. Vahlbruch, and R. Schnabel. Squeezed light at 1550 nm with a quantum noise reduction of 12.3 db. *Opt. Express*, 19(25):25763–25772, Dec 2011.

[MEM12] J. M. Mateo, D. Elkouss, and V. Martin. Blind reconciliation. *Quantum Information and Computation*, 12:0791–0812, 2012.

[MK04] D. J. C. Mac Kay. Information theory, interference, and learning algorithms. *Cambridge University Press*, 22:348–349, 2004.

[MMPP+15] J. Martinez-Mateo, C. Pacher, M. Peev, A. Ciurana, and V. Martin. Demystifying the information reconciliation protocol Cascade. *Quantum Information & Computation*, 15(5&6):453–477, May 2015. arXiv:1407.3257 [quant-ph].

[MN95] D. J. C. MacKay and R. M. Neal. Good codes based on very sparse matrices. *Cryptography and Coding*, 1025:100–111, 1995.

[Moy49] J.E Moyal. Quantum mechanics as a statistical theory. *Mathematical Proceedings of the Cambridge Philosophical Society*, 45:99124, 1949.

[MQR09] J. Müller-Quade and R. Renner. Composability in quantum cryptography. *New J. Phys.*, 11:085006, 2009.

[MW95] S. Mandel and E. Wolf. *Optical Coherence and Quantum Optics*. Cambridge University Press, 1995.

[NC00] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2000.

[NGA06] M. Navascues, F. Grosshans, and A. Acin. Optimality of gaussian attacks in continuous-variable quantum cryptography. *Phys. Rev. Lett.*, 97:190502, Nov 2006.

[Nol07] W. Nolting. *Grundkurs Theoretische Physik (Elektrodynamik)*. Springer Verlag, 2007.

[PAL+12] C. Pacher, A. Abidin, T. Lorünser, M. Peev, R. Ursin, A. Zeilinger, and J. A. Larsson. Attacks on quantum key distribution protocols that employ non-its authentication. *ArXiV:1209.0365*, 2012.

[Pen55] R. Penrose. A generalized inverse for matrices. *Cambridge Philosophical Society*, 51:406, 1955.

[Ple82] V. Pless. *Introduction to the Theory of Error-Correcting Codes*. John Wiley and Sons, 1982. ISBN 0-471-08684-3.

[PMD+14] C. Pacher, J. M. Mateo, J. Duhme, V. Händchen, T. Gehring, R. F. Werner, and R. Schnabel. Reconciliation for continuous-variable quantum key distribution using non-binary low density parity check codes. *To be published*, 2014.

[Ren05] R. Renner. *Security of Quantum Key Distribution*. PhD thesis, ETH Zurich, 2005.

[RS78] M. Reed and B. Simon. *Methods of Modern Mathematical Physics, Vol. I: Functional Analysis*. NewYork Academic Press, 1978.

[RSA78] R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21:120–126, 1978.

[SAA+10] C. Simon, M. Afzelius, J. Appel, A. Boyer de la Giroday, S. J. Dewhurst, N. Gisin, C. Y. Hu, F. Jelezko, S. Kröll, J. H. Müller, J. Nunn, E. S. Polzik, J. G. Rarity, H. De Riedmatten, W. Rosenfeld, A. J. Shields, N. Sköld, R. M. Stevenson, R. Thew, I. A. Walmsley, M. C. Weber, H. Weinfurter, J. Wrachtrup, and R. J. Young. Quantum memories. *The European Physical Journal D*, 58(1):1–22, 2010.

[Sai03] T. Saito. Thermal noise random pulse generator and random number generator, April 1 2003. US Patent 6,542,014.

[Sam12] A. Samblowski. *State Preparation for Quantum Information Science and Metrology*. PhD thesis, Leibniz University Hannover, 2012.

[SBPC+09] V. Scarani, H. B.-P., N. J. Cerf, M. Dusek, N. Lütkenhaus, and M.l Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81:1301–1350, 2009.

[Sch] Prof. Dr. R. Schnabel. http://www.qi.aei-hannover.de/.

[SFL+13] M. Suchara, E. Faruque, C. Lai, G. Paz, F. T. Chong, and J. Kubiatowicz. Comparing the overhead of topological and concatenated quantum error correction. *ArXiV*, page 17, 2013.

[Sha48] C. E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:623–656, 1948.

[Sho02] A. Shokrollahi. An introduction to low-density parity-check codes. In *Theoretical Aspects of Computer Science*, volume 2292 of *Lecture Notes in Computer Science*, pages 175–197. Springer Berlin Heidelberg, 2002.

[Sim00] R. Simon. Peres-Horodecki separability criterion for continuous variable systems. *Phys. Rev. Lett.*, 84:2726, 2000.

[Sin99] S. Singh. *Geheime Botschaften.* Carl Hanser Verlag, 1999.

[SIPDS04] A. Serafini, F. Illuminati, Matteo G. A. Paris, and S. De Siena. Entanglement and purity of two-mode gaussian states in noisy channels. *Phys. Rev. A*, 69:022318, 2004.

[SS00] A. Shokrollahi and R. Storn. Design of efficient erasure codes with differential evolution. In *Proceedings IEEE International Symposium on Information Theory*, pages 1–5, Sorrento, 2000. IEEE.

[Sti94] D. R. Stinson. Universal hashing and authentication codes. *Des. Codes Cryptography*, 4:369–380, 1994.

[SW71] D. Slepian and J. Wolf. Noiseless coding of correlated information sources. *IEEE Transactions on Information Theory*, 19:461, 1971.

[TCR10] M. Tomamichel, R. Colbeck, and R. Renner. Duality between smooth min- and max-entropies. *IEEE Transactions on Information Theory*, 56:4674, 2010.

[TLGR14] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner. Tight finite-key analysis for quantum cryptography. *Nature Communications*, page 11, 2014.

[Tom12] M. Tomamichel. *A Framework for Non-Asymptotic Quantum Information Theory*. PhD thesis, ETH Zürich, 2012.

[TYYF07] Y. Takeno, M. Yukawa, H. Yonezawa, and A. Furusawa. Observation of -9 db quadrature squeezing with improvement of phase stability in homodyne measurement. *Opt. Express*, 15:4321, 2007.

[UTSM+07] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Omer, M. AU Furst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger. A comprehensive design and performance analysis of low earth orbit satellite quantum communication. *Nat Phys*, 3(7):481 – 486, 2007.

[VACC06] G. Van Assche, J. Cardinal, and N. J. Cerf. Reconciliation of a quantum-distributed gaussian key. *IEEE Trans. Inf. Theor.*, 50(2):394–400, September 2006.

[Wer] Prof. Dr. R. F. Werner. https://www.itp.uni-hannover.de/Gruppen/quinfo/home.php.

[WFD13] R. F. Werner, T. Franz, and J. Duhme. Crypto on campus, 2008-2013. Lokales Exzellenzcluster (LU Hannover).

[Wie84] S. Wiesner. Conjugate coding. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, page 175, 1984. Originally written c. 1970 but unpublished.

[Wig32] E. Wigner. On the quantum correction for thermodynamic equilibrium. *Phys. Rev.*, 40:749, 1932.

[WM04] D.F. Walls and G.J. Milburn. *Quantum Optics*. Springer Berlin, 2004.

[WPGP+12] C. Weedbrook, S Pirandola, R. García-Patrón, N. Cerf, T.C. Ralph, J.H. Shapiro, and S. Lloyd. Gaussian quantum information. *Rev. Mod. Phys.*, 84:621, 2012.

[WSDH14] R. F. Werner, R. Schnabel, J. Duhme, and V. Händchen. Crypto on campus, 2013-2014. DFG, Fördernummer: WE 1240/20-1 (AOBJ 608317).

[WVO99] D. G. Welsch, W. Vogel, and T. Opatrny. Homodyne detection and quantum state reconstruction. *Progress in Optics*, 39:63–211, 1999.

[YHJ+13] C. Yuan, L. Hao, Y. Juan, L. Y. Hai, Z. Fei, W. Yu-Ping, R. Ji-Gang, L. Yu-Huai, P. Ge-Sheng, Tao Y., M. Xiongfeng, P. Cheng-Zhi, and P. Jian-Wei. Entanglement-based quantum key distribution with biased basis choice via free space. *Opt. Express*, 21(22):27260–27268, Nov 2013.

[YMHA07] T. Yuishi, Y. Mitsuyoshi, Y. Hidehiro, and F. Akira. Observation of -9 db quadrature squeezing with improvement of phasestability in homodyne measurement. *Opt. Express*, 15:4321–4327, 2007.

[ZWZ+13] W. Zhengchao, W. Weilong, Z. Zhen, G. Ming, M. Zhi, and M. Xiongfeng. Decoy-state quantum key distribution with biased basis choice. *Sci. Rep.*, 3, Aug 2013.

Curriculum Vitae

Full name:	Jörg Duhme
Date of birth:	1978-09-05
Place of birth:	Rheda-Wiedenbrück (Nordrhein-Westfalen)

Positions and Education

2009 - 2014	Leibniz University Hannover Institute for Theoretical Physics
2003 - 2009	Studies of Physics at the University of Braunschweig Degree: Physics Diploma
2000 - 2003	Abitur, Kolleg Braunschweig
1999 - 2000	Civilian Service
1997 - 1998	Scientific Assistant Physikalisch Technische Bundesanstalt Braunschweig Division 3. Explosion Control
1994 - 1997	Apprenticeship: Physics lab assistant (Physiklaborant) Physikalisch Technische Bundesanstalt Braunschweig
1992 - 1996	General Certificate of Secondary Education, Realschule Querum