DIPLOMARBEIT

Postselection Strategies for CV-QKD Protocols with Phase-Shift Keying Modulation

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Technische Physik

eingereicht von

Florian KANITSCHAR, BSc, BSc

Matrikelnummer 01425971

unter der Anleitung von
Univ.Doz. Dipl.-Ing. Dr.techn. Martin SUDA,
Dipl.-Ing. Dr.techn. Christoph PACHER

ausgeführt am
Atominstitut der Technischen Universität Wien
in Zusammenarbeit mit AIT Austrian Institute of Technology

Wien, am 15.07.2021

Florian Kanitschar   Martin Suda   Christoph Pacher

Statement of contributions

This thesis, including the underlying data and results, are effectively my own, beyond the advisement from my supervisors Christoph Pacher and Martin Suda. I want to acknowledge the following contributions to my thesis.

- The present thesis builds upon two 'pre-diploma project works' I conducted during my physics studies at AIT Austrian Institute of Technology. The aim of these projects is to introduce students to their future diploma-research project. Therefore, for my diploma thesis, I use knowledge I gained when conducting these projects. Although I programmed a simulator in Python while working on my projects, the code used for the present diploma thesis is new, as we decided to change the platform (MATLAB instead of Python). Furthermore, for the present thesis, I focussed on increasing the numerical accuracy and lowering the computation time and I included additional features like the non-ideal trusted detector scenario, other protocol variants and additional postselection strategies.
- In Section 6.1, I perform a theoretical key rate calculation for a QPSK protocol on a noiseless channel, where I generalised the method from [19]. Similar considerations have been carried out in my project thesis for a rotated QPSK protocol. Although there is some similarity to the calculations I carried out for the project thesis (as both generalise an idea from [19]), the derived expressions are slightly different. They are essential for the validation of the method in Chapter 7 and give the idea for the theoretical calculation for the 8PSK protocol in Section 6.2.
- With the permission of my co-author and supervisor Christoph Pacher, the results for the QPSK protocol in Chapter 7 as well as whole Chapter 8 are taken from our paper [23], which reports the results for four-state protocols of my thesis under the advisement of my supervisor. I am the first author of this paper, hence I wrote the majority of the text and carried out the calculations that led to the results presented in the paper. The plots for the QPSK protocol in Chapter 7, all plots in Chapter 8 and the sketches in Chapter 2.1 were produced by me and were published in our paper [23] first. Furthermore, analytical results for the region operators and for the Fock

representation of first- and second moment observables in Section 4.2 (for the ideal untrusted detector) and in Section 4.3 (for the non-ideal trusted detector), including the corresponding calculations in the Appendix (A.4, A.5 and A.6), were first published in our paper [23] but found during my work for the present diploma thesis.

- Furthermore, with the permission of my co-author and supervisor Christoph Pacher, the results for the 8PSK protocol in Chapter 7 and the whole Chapter 9 are taken from our paper [24], where we report the results for eight-state protocols obtained within the frame of my thesis under the advisement of my supervisor. I wrote the majority of this paper and carried out the calculations that led to the results presented there. The plots for the 8PSK protocol in Chapter 7 and all plots in Chapter 9 as well as the sketches in Section 2.2 were produced by me and were published first in our paper [24].

Abstract

Quantum Key Distribution, or short QKD, aims to establish a secure key without making any additional assumptions about the abilities or computational power of an adversary who is only limited by the laws of nature. The process of finding a mathematical expression for, or at least a lower bound on, the secure key rate of some QKD protocol, given relevant system parameters, is called security proof. In this thesis, we use a recent numerical security proof technique to examine different postselection strategies for continuous-variable quantum key distribution (CV-QKD) protocols with quadrature phase-shift keying modulation and four or eight signal states. CV-QKD protocols use coherent states to encode information and measure the field-quadrature components by homodyne or heterodyne detection. The basic idea of the used numerical security proof technique is to solve the key rate finding problem in a two-step process. In the first step, the problem is solved approximately, using a numerical algorithm, which yields an upper bound on the secure key rate. This is followed by step two, where the obtained upper bound is converted into a lower bound, using a sequence of theorems and taking numerical errors into account. Postselection aims to increase the secure key rate by removing those parts of the key, where a potential adversary might have gained more information than the communicating parties. The investigations are carried out both for the untrusted ideal and the trusted non-ideal detector scenario and we provide novel analytical results for the operators related to the postselection map.

For four-state protocols, we demonstrate that a new *cross-shaped* postselection strategy outperforms the state-of-the-art *radial* postselection scheme clearly in regions of medium to high transmission distances and medium to high values of noise and performs comparable to a more complicated *radial&angular* scheme. As the error-correction phase is a known bottleneck for many real QKD systems, we examined the secure key rate when a large fraction of the raw key is removed by postselection. We observe that a smart choice of the postselection strategy can increase the key rate while lowering the raw key rate, hence the computational effort in the error-correction phase. One can think this even further: For cross-shaped postselection we showed that the secure key rate is roughly 80% of the secure key rate without postselection when only 20% of the raw key passes the postselection. For high noise levels this can be increased even further. The cross-shaped postselection strategy can easily be implemented in the data processing of both new and existing CV-QKD systems, hence can increase the achievable secure key rate significantly. Furthermore, we examined the radial&angular postselection strategy which combines the advantages of the radial postselection scheme for low transmission distances and those of the cross-shaped postselection scheme for medium and high transmission distances on the cost of higher complexity.

Additionally, we examine an eight-state phase-shift keying protocol and compare the obtained key rates to the key rates for the four-state protocol and investigate a radial postselection scheme. We observe that the 8PSK protocol yields higher secure key rates and reaches higher maximal achievable transmission distances than a QPSK protocol with a comparable postselection strategy, in particular for medium to high values of excess noise. Furthermore, we explore the relation between the achievable secure key rate and the probability to pass the postselection phase for various noise-levels and two different practically relevant reconciliation efficiencies. This leads to similar strategies as found for the QPSK protocols to reduce the raw key rate significantly while decreasing the secure key rate only moderately. For very high values of excess noise, the raw key rate can be increased further compared to the key rate achieved without performing postselection while removing a large fraction of the raw key rate.

Kurzfassung

Das Ziel von Quantenschlüsselverteilung, abgekürzt QKD (engl. für Quantum Key Distribution), ist die Erzeugung eines informationstheoretisch sicheren Schlüssels. Der Sicherheitsbegriff soll dabei ohne zusätzliche Annahmen über die Rechenleistung eines Angreifers, der einzig von physikalischen Gesetzen, nicht aber von technischen Aspekten (wie beispielsweise der zur Verfügung stehenden Rechenleistung) limitiert ist, auskommen. Das Finden eines auf Systemparametern basierenden mathematischen Ausdrucks für die sichere Schlüsselrate, oder zumindest einer unteren Schranke an selbige, wird Sicherheitsbeweis genannt. In der vorliegenden Arbeit verwenden wir einen numerischen Sicherheitsbeweisansatz, um verschiedene Postselectionstrategien für Protokolle mit kontinuierlichen Variablen (kurz: CV-QKD für Continuous-Variable QKD) mit Phasenumtastungsmodulation (phase-shift keying modulation - PSK) und vier oder acht Signalzuständen zu untersuchen. Die verwendete Sicherheitsbeweismethode verfolgt einen zweistufigen Ansatz. Im ersten Schritt wird das Problem der Schlüsselratenberechnung approximativ durch Anwenden eines numerischen Algorithmus gelöst. Dies liefert eine obere Schranke an die garantiert sichere Schlüsselrate. Im zweiten Schritt wird, ausgehend von der berechneten obere Schranke und unter Zuhilfenahme einer Reihe von Theoremen, eine untere Schranke ermittelt, wobei auch numerische Ungenauigkeiten berücksichtigt werden. Durch Postselection kann die Schlüsselrate durch Entfernen von jenen Teilen des Schlüssels, über die ein möglicher Angreifer mehr Information gewonnen haben könnte als die kommunizierenden Parteien, erhöht werden. Im Rahmen dieser Diplomarbeit werden die entsprechenden Berechnungen sowohl für den idealen, nicht vertrauenswürdigen, als auch für den nicht idealen, vertrauenswürdigen Detektor durchgeführt. Außerdem werden neue analytische Ausdrücke für Operatoren vorgestellt, die für die Beschreibung der Postselection-Abbildung benötigt werden.

Wir zeigen in der vorliegenden Arbeit, dass eine neue kreuzförmige Postselectionstrategie die bereits bekannte radiale Postselectionstrategie bei mittleren bis hohen Transmissionsdistanzen und mittleren bis hohen Rauschwerten deutlich übertrifft und vergleichbare Schlüsselraten wie ein ebenfalls bereits bekanntes Schema mit radialer und winkelförmiger Postselection liefert. Die Fehlerkorrektur ist rechenaufwändig und daher ein bekannter Engpass in vielen QKD-Implementierungen. Deshalb untersuchen wir zusätzlich die Änderung der garantiert sicheren Schlüsselrate, wenn große Teile des Rohschlüssels mittels Postselection entfernt werden. Wir zeigen, dass eine kluge Wahl der Postselectionstrategie die sichere Schlüsselrate nur geringfügig senkt oder gar erhöhen kann, während der Rohschlüssel signifikant reduziert wird. Dies verringert den Rechenaufwand der Fehlerkorrektur deutlich. Beispielsweise beobachten wir, dass für kreuzförmige Postselection 80% des Rohschlüssels entfernt werden kann, während die sichere Schlüsselrate immer noch 80% der sicheren Schlüsselrate ohne Postselection beträgt. Für höhere Rauschwerte kann dieses Ergebnis sogar noch verbessert werden. Die in dieser Arbeit vorgeschlagene kreuzförmige Postselectionstrategie kann problemlos in die Datenverarbeitungsroutinen von neuen, als auch von bereits bestehenden CV-QKD Systemen integriert werden. Zusätzlich untersuchen wir im Rahmen dieser Arbeit Postseletion in radiale Richtung und in Winkelrichtung, welche die Vorteile der radialen Postselection für kurze Distanzen mit jenen der kreuzförmigen Postselection für mittlere bis hohe Übertragungslängen vereint, dabei jedoch von zwei Postselectionparametern abhängt.

Außerdem betrachten wir ein Protokoll mit Phasenumtastung und acht Signalzuständen für mehrere Rauschwerte und verschiedene Werte für die Effektivität der Fehlerkorrektur und vergleichen die dafür berechneten Schlüsselraten mit jenen von Vierzustandsprotokollen. Wir beobachten, dass das untersuchte 8PSK Protokoll deutlich höhere Schlüsselraten liefert und, insbesondere bei mittleren bis starken Rauschwerten, höhere Übertragungsreichweiten ermöglicht als ein QPSK Protkoll mit gleicher Postselectionstrategie. Außerdem untersuchen wir den Einfluss von radialer Postselection und ermitteln den Zusammenhang zwischen der sicheren Schlüsselrate und der Wahrscheinlichkeit, dass ein Signal im Rahmen des Postprocessings nicht aussortiert wird. Diese Überlegung führt zu ähnlichen Postselectionstrategien, wie wir bereits für Protokolle mit vier Zuständen vorgeschlagen haben und kann, insbesondere für sehr hohe Rauschwerte, dafür verwendet werden den Rohschlüssel signifikant zu verkleinern, während der garantiert sichere Schlüssel nicht wesentlich abnimmt oder gar erhöht wird.

Acknowledgements

I dedicate these lines to all those people who supported me in accomplishing this thesis, starting with my supervisors Christoph Pacher and Martin Suda, to whom I owe great debt of gratitude. Christoph, thank you for introducing me into the world of quantum communication, for your infectious enthusiasm about QKD and the quantum world in general, for uncountable beneficial discussions about various questions in physics and mathematics that came up during working on my thesis, and for your excellent guidance, encouragement and patient supervision. Martin, thank you for sharing your deep knowledge about quantum physics with me, for your valuable input regarding our paper, your quick and helpful replies, and your cheerful and kind supervision. Furthermore, I want to thank the AIT Austrian Institute of Technology for the opportunity to carry out this thesis.

I also want to thank my friends and fellow students Tobias Forster and David Wörgötter for proofreading early versions of my thesis, for having an eye for details and their valuable comments and feedback. My special thanks go to Karabee Batta for proofreading my thesis, her precious feedback, for the beautiful illustration of the key finding problem with the Heisenberg Hedgehogs and for improving my English skills in the most awesome way.

Thanks to all my friends and fellow students who accompanied me through my studies, including countless afternoons, nights and weekends solving exercises together. Thank you for all the fun we had in our learning-breaks and for enjoying our free evenings together - you made my time at university unforgettable! In particular, I want to thank you, Tobi, for your honest interest in my work, for your encouragement, for always having an open ear and for being a true friend, not only for the time working on the present thesis but for the years of my studies.

Finally, I want to express my sincere gratitude to my parents, Gerda and Johann Kanitschar. Thank you for everything! Without your support and confidence, my studies, including this thesis, would not have been possible.

Contents

1. Introduction **1**
1.1. An introduction to secure quantum communication 1
1.2. Notational agreements 5
1.3. Preliminaries 6
1.3.1. Quantum mechanics 7
1.3.2. Quantum Optics 10
1.3.3. Information theory and quantum information theory 11

2. Description of the objective protocols **17**
2.1. Examined four-state protocols 18
2.2. Examined eight-state protocols 22

3. Description of the security proof approach **27**
3.1. Finding an expression for the secret key rate 27
3.2. Description of step 1 30
3.3. Description of step 2 32

4. Formulation of the relevant optimisation problem **35**
4.1. Physical model 35
4.1.1. Model of the preparation and measurement process 35
4.1.2. Channel model 36
4.2. The ideal, untrusted detector scenario 36
4.2.1. Objective function for the ideal, untrusted detector scenario 36
4.2.2. Specifying the domain of optimisation for the ideal, untrusted detector scenario 39
4.3. Trusted detector approach 41
4.3.1. Objective function for the non-ideal, trusted detector scenario 44
4.3.2. Specifying the domain of optimisation for the non-ideal, trusted detector scenario 46
4.4. Error correction and postprocessing 48

5. Implementation **51**
5.1. Calculation of a feasible starting value 51
5.1.1. Using a channel model 51

5.1.2. Solving a semi-definite program 54
5.2. Calculation of the conditioned probabilities 54
5.3. Remarks on the implementation 56

6. Theoretical calculations 59
6.1. Theoretical calculation for four-state protocols 59
6.1.1. Calculation of the Holevo quantity 60
6.1.2. Calculating the mutual information and finding the secure key rate 64
6.2. Theoretical calculation for eight-state protocols 65
6.2.1. Calculation of the Holevo quantity 66
6.2.2. Calculating the mutual information and finding the secure key rate 68

7. Validation of the implementation 71
7.1. Choice of the cutoff number 74

8. Results for four-state protocols 77
8.1. Postselection strategies for untrusted detectors 77
8.1.1. Cross-shaped postselection 77
8.1.2. Comparison of postselection strategies 82
8.1.3. Influence of the probability to pass the postselection step on the secure key rate 84
8.2. Postselection strategies for trusted detectors 86
8.2.1. Cross-shaped postselection 87
8.2.2. Comparison of postselection strategies 88

9. Results for eight-state protocols 95
9.1. Finding the optimal coherent state amplitude 95
9.2. Secret key rates for 8PSK protocols 96
9.3. Influence of the probability to pass the postselection 99
9.4. Conclusion and discussion of the 8PSK examinations 103

10. Summary and outlook 105
10.1. Outlook 107

A. Appendix i
A.1. Used symbols i
A.2. Used variables iv
A.3. Used abbreviations and terms vii
A.4. Explicit calculation of region operators for the untrusted noise scenario ix
A.4.1. Calculation for radial and angular postselection ix

A.4.2. Calculation for cross-shaped postselection x

A.5. Calculations for the trusted detector scenario xii

A.5.1. Calculation for radial&angular postselection with trusted detector xiii

A.5.2. Calculation for cross-shaped postselection with trusted detector xiv

A.6. Representation of the first- and second-moment observables in the number basis xvii

A.7. Transforming a matrix-valued constraint xix

A.8. Constraining by experimental data xxi

A.8.1. Expectation values for the ideal untrusted detector xxii

A.8.2. Expectation values for the non-ideal trusted detector xxiv

Bibliography xxvii

1. Introduction

Before we start with the introduction, we give an overview of the structure of the present thesis. In the first chapter, we introduce the reader to secure quantum communication (Section 1.1), clarify the notation we are going to use throughout the thesis (Section 1.2), and present the necessary background in quantum physics, mathematics, and (quantum-) information theory (Section 1.3) that is required to understand the thesis. In Chapter 2, we introduce the used protocols and the examined postselection strategies. In Section 3, we summarise the used security proof method, which can be explained as a two-step process. That is followed by the formulation of the minimisation problem both for the ideal untrusted and the non-ideal trusted detector scenario in Chapter 4. Furthermore, we give novel analytical expressions necessary for the postprocessing procedure. In Chapter 5, we explain aspects of the implementation, like two different ways to find a feasible starting value for the optimisation algorithm (Section 5.1) and the calculation of conditional probabilities (Section 5.2) that are essential for the postprocessing procedures. In Chapter 6, we carry out key rate calculations for noiseless channels for the used QPSK (Section 6.1) and 8PSK (Section 6.2) protocol. These calculations are used in Chapter 7 to validate our implementation. In Chapter 8, we examine postselection strategies for the QPSK protocol in the ideal untrusted (Section 8.1) and non-ideal trusted (Section 8.2) scenario and discuss our results. In Chapter 9, we elaborate on our results for the eight-state protocol. Finally, in Chapter 10 we summarise our findings, put it into context and give a brief outlook about possible future goals. Lengthy calculations that are not essential to follow the arguments of the thesis were moved to the appendix.

1.1. An introduction to secure quantum communication

Secret communication has been a demand of humanity since ancient times, as early evidences of special hieroglyphs in ancient Egypt show. While schemes like that or the more famous medieval Alphabetum Kaldeorum based their secrecy on the usage of different symbols or letters that were not known by everybody, both would not be considered as valid encryption schemes nowadays, as their secrecy relies on the knowledge of the encryption-method. In modern times, encryption schemes became more sophisticated when mathematical tools were used to construct and examine cryptographic schemes. Claude Shannon, one of the pioneers in that field set the basis in his seminal work *Communication theory of secrecy systems* [40] and proved the security and the optimality of the so-called One-Time Pad. In this encryption scheme, the sender and the recipient share some random secret key k (where we assume k to be the binary representation of that key). The sender encrypts the message m (again, we assume that m is the binary representation of the message) by adding the message and the key bitwise, $m \oplus k$, and sends the message to the recipient, who encrypts the message by bitwise adding the key to what he received, $(m \oplus k) \oplus k = m \oplus (k \oplus k) = m$. Shannon showed that the One-Time Pad is secure if each key is used only once (which explains the name) and that this scheme is optimal, meaning that there is no encryption scheme which is provable secure and uses a shorter key.

The last line already highlights one of the main issues of the One-Time Pad, namely that the key has to be of equal length as the message. Many of nowadays encryption schemes like RSA (named after Ron Rivest, Adi Shamir, and Leonard Adleman) [38] use keys that are much shorter than the message, but are not provable secure. The integrity of messages relies on hard-to-solve mathematical problems that can be solved easily using a so-called trapdoor-function if some additional information is known. An example would be to find the prime-factorisation of some large number $n \in \mathbb{N}$, $n = r \cdot s$, for $r, s \in \mathbb{P}$. Providing that n is very large, this is a computationally very expensive task, while, for example, it is easy to find r by simple division if s is known. Modern encryption-schemes are designed in a way such that even the most powerful computers are expected to calculate for years or even longer to solve the problem, while the recipient, who knows the key (e.g., one of the two factors in the prime factorisation), can easily decipher the message. Hence, nowadays ciphering-techniques rely on assumptions about the computational power of a hypothetical adversary. Recent advancements in classical computation, number theory, and quantum computation, like Peter Shor's discovery [41, 42] that large numbers can be factorised efficiently once quantum computers are available, threaten nowadays encryption-schemes. In response to these developments, we require a new method of secure communication.

One attempt is post-quantum cryptography [4], which aims to use mathematical problems where no efficient quantum algorithm is known. An alternative method to achieve data-encryption relying only on fundamental laws of quantum mechanics, is Quantum Key Distribution (QKD). The security of quantum key distribution is based on very fundamental principles of quantum mechanics, namely that measurements modify the quantum state of the system to be measured or, equivalently, that non-orthogonal quantum states cannot be discriminated with certainty. Alternatively, one can employ the no-cloning theorem by Wootters and Zurek [56] which states that Eve cannot own a perfect copy of the states Alice and Bob exchange. Therefore, the notion of security is only based on physical properties but not on any assumptions (like about the computational power of an adversary) that may or may not hold. The basic setting of quantum key distribution is the following one.

Alice and Bob, two distant parties who want to establish secure communication, are connected by a quantum channel that can be read out and manipulated by an eavesdropper, called Eve, who is only limited by the laws of physics. In particular, we assume that she has access to a quantum computer and can store quantum states for an arbitrarily long time. Additionally, the communicating parties are linked by an authenticated classical channel where they can make public announcements. An adversary can listen to the classical channel but cannot manipulate the bits there. The communicating parties are equipped with devices required to prepare quantum states and to perform quantum measurements.

The first QKD protocol was published by Charles Bennett and Gilles Brassard [3] in 1984 and thus is named BB84. In their protocol, they assume that Alice is equipped with a single-photon source and that she is able to control the polarisation of the photons she sends to Bob. In more detail, she randomly chooses to polarise her photon either in horizontal (H), vertical (V), or diagonal (± 45)-direction, where H and $+45$ encode the bit value '0' and V and -45 encode the bit value '1'. One observes that the two bases (H,V) and $(+45, -45)$ are non-orthogonal. So, as Bob does not know the basis Alice chose to encode her bit, he has a 50%-chance of choosing the same basis as Alice used for preparation. Suppose Eve tried to do some polarisation-measurement before she forwards the photon to Bob. As she does not know either which basis Alice had chosen, she has also a 50%-chance of selecting the wrong basis. If, for example, Eve measures in (H,V), but Alice prepared her photon in $(+45, -45)$ the photon's polarisation state collapses with equal probability to H or V. When Bob performs his measurement in the $(+45, -45)$-basis the polarisation state collapses back either to $+45$ or -45 with equal probability. Hence, in total, there is a 50% chance for a bit-flip if Eve performed a measurement. After performing N rounds of key generation, Alice and Bob announce the bases they have used in every single round via the classical channel and remove all rounds, where they have used not the same basis. This is called 'sifting-phase' and ends up with Alice and Bob holding a list of approximately $\frac{N}{2}$ bits. Then, they reveal a random subset of their remaining bits to estimate the error rate to learn about the information Eve might have gained about their key. Alice and Bob perform classical privacy-amplification and error correction steps to reduce Eve's information about the key and decide whether they can keep or have to omit it (for the case that Eve gained too much information).

Bennett and Brassard's protocol uses on discretely polarised photons, hence is part of the family of discrete-variable quantum key distribution (DV-QKD) protocols, and relies on single-photon sources and single-photon detectors. Therefore, the achievable secure key rates are limited by the detector-deadtime. In contrast, continuous-variable quantum key distribution (CV-QKD) protocols require the measurement of the field quadratures of light, hence continuous amplitudes, with homodyne- or heterodyne-detectors. Therefore, photon counters are replaced by faster and more efficient photo-diodes, which are widely used for nowadays telecommunication networks, and single single-photon sources are replaced by lasers. The family of CV-QKD protocols divides into Discrete-Modulated- (DM-) CV-QKD and Gaussian-Modulated- (GM-) CV-QKD protocols. In DM-CV-QKD protocols (squeezed) coherent states are displaced by some fixed constant from the origin, while in GM-CV-QKD protocols, the states are displaced following a Gaussian distribution. An early example for a Discrete-Modulated CV-QKD protocol goes back to Ralph [37], while an early example for a Gaussian-modulated CV-QKD protocol was proposed by Grangier and Grosshans [18]. In this work, we are going to focus on DM-CV-QKD protocols.

To guarantee that the generated key is indeed secure, one has to calculate or at least find lower bounds on the achievable secure key rate, which is called security proof. In 2000, John Preskill and Peter Shor proved the security of the BB84 protocol [43]. Analytical attempts for CV-QKD protocols are often very technical, hold true only under some assumptions about the power of the eavesdropping attacks, and cannot be generalised easily to other protocols. Contrarily, numerical attempts are more flexible regarding changes in the protocol structure and can be adapted to a broader family of protocols more easily but suffer from finite-precision errors due to numerical evaluations. Furthermore, we cannot expect that numerical optimisations reach the optimum exactly and we cannot handle infinite-dimensional Hilbert spaces, which describe the state-spaces of continuous-variable protocols. Recently, a powerful, computationally efficient framework [6, 55] was published that includes estimates for the aforementioned numerical issues in the secure key rate calculation. The obtained key rates are expected to be tight, although this security proof approach considers the relevant key rate finding problem in a truncated space. This so-called photon-number cutoff assumption was removed recently in [51].

Comprehensive reviews about quantum key distribution, both for discrete- and continuous-variable schemes, experimental realisations and security proofs can be found in [10, 36, 39].

1.2. Notational agreements

The fundamental paper for this work is [29]. Therefore, the present thesis sticks close to the notation used in that work. We summarise the most important notation as below:

During the entire thesis, we use Dirac's BraKet notation, where $|.\rangle$ is called a 'ket' and denotes a vector in some (in general: complex) vector space. Physically, kets represent states in quantum systems. The counterpart of a ket is called are 'bra', denoted by $\langle .|$, and describes a linear form. That is a linear map assigning every vector some complex number, hence linear forms act on vectors and assign them complex numbers. This is denoted by a vertical bar, $\langle .|.\rangle$. A more detailed explanation of the Dirac notation can be found in many introductory quantum mechanics books (e.g., [17]). Furthermore, during the entire thesis, we denote operators by hats. For example, the operator corresponding to some quantity A is denoted by $\hat{A}$.
Coherent states were discovered by Erwin Schrödinger when he conducted his work on the quantum mechanical harmonic oscillator. They describe a (quantum-) particle moving in the potential of a harmonic oscillator having constant position and momentum uncertainty. In 1963, Roy Glauber explained laser modes using coherent states, hence used them to describe the quantised electromagnetic field. Coherent states represent Gaussian states with minimal uncertainty, where the uncertainty is distributed equally between the spatial and momentum quadrature. Since continuous-variable quantum key distribution employs lasers to generate signals, we are going to use coherent states extensively. Coherent states have applications in various sub-fields of quantum mechanics and quantum optics, hence are subject to almost every introductory quantum mechanics book (see, for example, [17]). Therefore, we are not going to introduce them in 'full fashion' here. We denote coherent states by Greek letters, e.g., $\alpha \in \mathbb{C}$, representing complex numbers. Coherent states are overcomplete, which means that they are not linearly independent, hence cannot form a basis (but are a generator).

In the present work, we deal with a numerical security proof method, thus need a basis to describe quantum states such that computers can easily represent them. Therefore, we use bosonic Fock states (named after the Soviet physicist Vladimir Fock), sometimes also called number states. We denote Fock states by $|n\rangle$, where

n (or, in general, some Latin letter) is a natural number and corresponds to the n-th eigenstate of the Hamilton operator describing our physical system. One can introduce the so-called creation and annihilation operators by their action on number states. The raising-operator is defined by $\hat{a}^\dagger |n\rangle := \sqrt{n+1}\,|n+1\rangle$, while its counterpart, the lowering operator, is given by $\hat{a}\,|n\rangle := \sqrt{n}\,|n-1\rangle$. Due to their action on number states they are called 'ladder operators'. Note that we defined these operators using natural units, where they obey the commutation relation $[\hat{a}, \hat{a}^\dagger] = 1$. One can find a very clearly structured table explaining the conversion of quantum mechanical quantities between different unit systems in [25]. The ladder operators are linked to the quadrature operators by $\hat{a}^\dagger = \frac{1}{\sqrt{2}}(\hat{q} - i\hat{p})$ and $\hat{a} = \frac{1}{\sqrt{2}}(\hat{q} + i\hat{p})$. Furthermore, it is convenient to define the operator $\hat{n} := \hat{a}^\dagger \hat{a}$, which is called number operator, as $\hat{n}\,|n\rangle = n\,|n\rangle$ holds. Hence, the n-th eigenvalue of the number operator is the occupation number n, which motivates the name. Finally, we state that coherent states can be represented in the Fock basis as $|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$.

In the Schrödinger picture, one uses either the position or the momentum space to describe a quantum mechanical state. Contrary, the phase-space formulation of quantum mechanics uses both the position and momentum variables simultaneously. In phase-space, we can describe quantum states by quasiprobability distributions instead of state vectors or density matrices. The field-quadratures are commonly called q and p and the corresponding field-quadrature operators are denoted by $\hat{q}$ and $\hat{p}$ respectively. The expectation value of a coherent state $|\alpha\rangle$ is linked with its expectation values for position and momentum (q and p) by the relation $\alpha = q + ip$.

Coherent states are eigenstates of the annihilation operator, $\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle$. This can be derived easily, inserting the Fock representation of the coherent state and using the properties listed above. Alternatively, one can create a coherent state from the vacuum using the displacement-operator $\hat{D} := e^{\alpha\hat{a}^\dagger - \bar{\alpha}\hat{a}}$. Analogously to the creation of an arbitrary number state from the vacuum by applying the creation operator multiple times (and performing some renormalisation) $|n\rangle = \frac{(\hat{a}^\dagger)^n}{\sqrt{n!}}\,|0\rangle$, one can create a coherent state by $|\alpha\rangle = \hat{D}(\alpha)\,|0\rangle$.

1.3. Preliminaries

In this section, we introduce important concepts and give definitions that we are going to use throughout this thesis. We start with definitions from basic quantum mechanics, proceed with a brief discussion of quasiprobability distributions in quantum optics and move on to notions and definitions from information theory and quantum information theory.

1.3.1. Quantum mechanics

Quantum mechanical states can be described by density operators. We give a formal definition following [33, Chapter 2.4].

Definition 1.1 ***(Density Operator)***
Let $\mathcal{H}$ be a Hilbert space and $\mathcal{I}$ a finite index set. A density operator for a quantum system, given by the states $\{|\psi_i\rangle\}_{i\in\mathcal{I}} \subseteq \mathcal{H}$, which are occupied with corresponding probabilities $\{p_i\}_{i\in\mathcal{I}}$, where $\forall i \in \mathcal{I}: \;\; 0 \leqslant p_i \leqslant 1$, is defined by

$$\hat{\rho} := \sum_{i\in I} p_i \left|\psi_i\right\rangle\left\langle\psi_i\right| . \tag{1.1}$$

We denote the set of all density operators associated with a Hilbert space $\mathcal{H}$ by $\mathcal{D}(\mathcal{H})$.

A density operator is characterised by the following properties [33, Chapter 2.4].

Theorem 1.2 ***(Properties of Density Operators)***
A density operator $\hat{\rho} : \mathcal{H} \to \mathcal{H}$, as defined in Definition 1.1, has the following properties:

(i) $\hat{\rho}^\dagger = \hat{\rho}$ *(hermiticity)*

(ii) $\forall \left|\psi\right\rangle \in \mathcal{H} : \left\langle\psi\right| \hat{\rho} \left|\psi\right\rangle \geqslant 0$ *(non-negativity, positive semi-definiteness)*

(iii) $Tr[\hat{\rho}] = 1$.

The most general way to describe the interaction of quantum states is by so-called quantum operations [33, Chapter 8.2.4].

Definition 1.3 ***(Quantum Operation)***
Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be finite-dimensional Hilbert spaces.
A quantum operation $\mathcal{E} : \mathcal{D}(\mathcal{H}_1) \to \mathcal{D}(\mathcal{H}_2)$ is a map from the set of density operators of the input space $\mathcal{H}_1$ to the set of density operators of the output space $\mathcal{H}_2$, with the following three axiomatic properties:

(i) *For the trace holds $\forall \hat{\rho} \in \mathcal{D}(\mathcal{H}): \;\; 0 \leqslant Tr[\mathcal{E}(\hat{\rho})] \leqslant 1$.*

(ii) *A quantum operation $\mathcal{E}$ is a convex linear map on the set of density operators. It holds $\forall \hat{\rho} \in \mathcal{D}(\mathcal{H}): \;\; \mathcal{E}(\sum_{i\in\mathcal{I}} p_i\hat{\rho}_i) = \sum_{i\in\mathcal{I}} p_i\mathcal{E}(\hat{\rho}_i)$ with $(p_i)_{i\in\mathcal{I}} \in [0,1]$, satisfying $\sum_{i\in\mathcal{I}} p_i = 1$. By $\mathcal{I}$, we denote a finite index set.*

(iii) A quantum operation $\mathcal{E}$ is a completely positive map. That is, if $\mathcal{E}$ maps density operators of system $\mathcal{H}_1$ to density operators of system $\mathcal{H}_2$, then for all operators A that are non-negative, $\mathcal{E}(A)$ has to be non-negative, too. We denote the set of completely positive maps between Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ by $CP(\mathcal{H}_1, \mathcal{H}_2)$.

In quantum information and quantum communication it is common to use quantum channels to model quantum processes. A quantum channel can be defined as follows [52].

Definition 1.4 ***(Quantum Channel)***
Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be finite dimensional Hilbert spaces over $\mathbb{C}$. A quantum channel is a linear map $\Phi : L(\mathcal{H}_1) \to L(\mathcal{H}_2)$ satisfying that Φ is trace preserving and completely positive, i.e.

1. $\forall X \in L(\mathcal{H}): \ Tr[\Phi(X)] = Tr[X]$

2. $\forall X \in L(\mathcal{H}): X \geqslant 0 \ \Rightarrow \ \Phi(X) \geqslant 0.$

According to this definition, a quantum channel is a completely positive trace preserving (CPTP) map. In other words, a quantum channel is a trace preserving quantum operation. There are several ways representing quantum channels, such as the Choi-representation and the Stinespring-representation. Another convenient way of representing quantum channels goes back to Karl Kraus (not to be confused with the famous eponymous writer!) and reads as follows [52, Chapter 2.2.2].

Definition 1.5 ***(Kraus representation)***
Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be finite dimensional Hilbert spaces over $\mathbb{C}$ and $\mathcal{I}$ a finite set. Consider the collections $\{A_i : \ i \in \mathcal{I}\}$ and $\{B_i : \ i \in \mathcal{I}\}$ of operators drawn from the space $L(\mathcal{H}_1, \mathcal{H}_2)$. We define a linear map $\Phi : \ L(\mathcal{H}) \to L(\mathcal{H})$ by

$$\Phi : \ X \mapsto \Phi(X) := \sum_{i \in \mathcal{I}} A_i X B_i^\dagger \tag{1.2}$$

and call this representation Kraus representation.

One can find a Kraus representation for every linear map, but the obtained map is, in general, not unique [52, Chapter 2.2.2].

Another very important concept for this thesis and in quantum mechanics in general is the quantum mechanical measurement. A formal definition goes back to John von Neuman and is given in [48].

Definition 1.6 ***(Quantum Mechanical Measurement)***
A measurement within a physical system, described by a finite-dimensional Hilbert space $\mathcal{H}$, is represented by a self-adjoint operator $\hat{O} : \mathcal{H} \to \mathcal{H}$. We call this quantity an observable. The possible measurement results are given by the eigenvalues λ_i of the operator $\hat{O}$, where $i \in \mathcal{I}$ for a suitable index set $\mathcal{I}$. The probability of measuring the eigenvalue λ_i is given by $Tr[\rho \hat{P}_i]$, where $\hat{P}_i$ is the (orthogonal) projector on the eigenspace, corresponding to λ_i, and ρ is the density operator of the measured state.

Alternatively, every quantum measurement can be viewed as a box, taking a quantum state and outputting a classical variable and a post-measurement state, conditioned on the classical variable. In some experiments it happens that the post-measurement state is not available any more. For example, think of the Stern-Gerlach experiment, where the particle hits a screen, leaving back some spatial coordinate (the classical variable) but being inaccessible for further measurement. Mathematically spoken, the post-measurement state is traced out. This notion is contained in the following definition [52, Chapter 2.3].

Definition 1.7 ***(Quantum Measurement)***
Let $\mathcal{H}$ be a finite dimensional Hilbert space and denote by $Pos(\mathcal{H})$ the set of positive semi-definite operators on $\mathcal{H}$. Let $\mathcal{I}$ be a finite set. A quantum measurement is a function of the form

$$\mu : \mathcal{I} \to Pos(\mathcal{H}), \tag{1.3}$$

satisfying $\sum_{i \in \mathcal{I}} \mu(i) = \mathbb{1}_{\mathcal{H}}$.

This is known as positive operator-valued measure (POVM).

As we operate on a Hilbert space, we need to define some inner product. Therefore, we define the Hilbert-Schmidt inner product [33].

Definition 1.8 ***(Hilbert-Schmidt inner product)***
Let $\mathcal{H}$ be a Hilbert space. A linear, bounded operator with a finite Hilbert-Schmidt norm $\|A\|_{HS} := \sqrt{Tr\,(A^\dagger A)}$ is called Hilbert-Schmidt operator.
The map $\langle .,. \rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{R}, (A,B) \mapsto \langle A, B \rangle_{HS} := Tr\left(A^\dagger B\right)$, that correlates two Hilbert-Schmidt operators A and B with a real number, is called Hilbert-Schmidt inner product.
If it is clear that we mean the Hilber-Schmidt inner product, we omit the sub-index HS.

This is a generalisation of the Frobenius inner product for infinite-dimensional vector spaces.

1.3.2. Quantum Optics

In this thesis, we will use two quasiprobability functions from quantum optics for calculations. We give their definitions and useful statements, following [45] and start by introducing the Wigner function, named after the Austrian-Hungarian physicist Eugene Wigner.

Definition 1.9 ***(Wigner function)***
The Wigner quasiprobability distribution, or short Wigner function, of some quantum state with density operator $\hat{\rho}$ is defined by

$$W(q,p) = \frac{1}{2\pi\hbar}\int_{-\infty}^{\infty} \langle q - \frac{y}{2}|\hat{\rho}|q + \frac{y}{2}\rangle e^{\frac{iyp}{\hbar}}\, dy. \tag{1.4}$$

It can be used to calculate the expectation value of an operator $\hat{A}$ as follows [45]

$$\langle \hat{A}\rangle = \mathrm{Tr}\left[\hat{\rho}\hat{A}\right] = \int\int A(x,p)W(x,p)\, dx\, dp. \tag{1.5}$$

Another quasiprobability distribution is the Q function, or Husimi Q-function. It is obtained by smoothing the Wigner function by a Gaussian distribution

Definition 1.10 ***(Q-function)***
The Q-function of some quantum state with density operator $\hat{\rho}$ is defined by

$$Q(x,p) = \int dq' \int dp' W(q',p') e^{-\frac{(q-q')^2+(p-p')^2}{\gamma}}, \tag{1.6}$$

where $\gamma > 0$.

In the remainder of this work, we are going to use $\gamma = 1$. Note that the exponential term next to the Wigner function is, up to a factor of π, the Wigner function of a coherent state with amplitude $\alpha = \frac{q+ip}{\sqrt{2}}$. Therefore, the Q-function can be interpreted [27] as the probability of finding the coherent state $|\alpha\rangle$ in the state $\hat{\rho}$,

$$Q(q,p) = \frac{1}{\pi}\langle \alpha|\hat{\rho}|\alpha\rangle. \tag{1.7}$$

The expectation value of an anti-normally ordered operator $\hat{A} = \hat{a}^k\hat{a}^{\dagger l}$ in terms of creation and annihilation operators is given by [27]

$$\langle \hat{a}^k\hat{a}^{\dagger l}\rangle = \int dq \int dp\; Q(q,p)\alpha^k\bar{\alpha}^l. \tag{1.8}$$

1.3.3. Information theory and quantum information theory

In this section, we list important definitions from (quantum-)information theory where one essential task is to store information. An abstraction of a (quantum-) storage is called register. Besides for memorising a finite amount of information, registers can be used for modelling discretely changing physical systems or systems where we are not interested in the way it changes but only in the initial and final state. Therefore, registers are perfectly suited to describe the transmission of information between two parties. A formal definition reads as follows [52, Definition 2.1].

Definition 1.11 ***(Register)***
A register X is either one of the following two objects:

1. *An alphabet Σ (so, a finite set). This is called a simple register.*
2. *An n-tuple $X = (Y_1, ..., Y_n)$, where $n \in \mathbb{N}$ and $Y_1, ..., Y_n$ are registers. We call this type of register a compound register.*

Next, we define the classical state set of a register [52, Definition 2.3].

Definition 1.12 ***(Classical state set of a register)***
The classical state set of a register X is determined as follows:

1. *If $X = \Sigma$ is a simple register, the classical state set of X is Σ.*
2. *If $X = (Y_1, ..., Y_n)$ is a compound register, the classical state set of X is the Cartesian product $\Sigma_1 \times ... \times \Sigma_n$, where Σ_k denotes the classical state set associated with a register Y_k for $k \in \{1, 2, ..., n\}$.*

One might want to store both classical and quantum states in a register. In what follows, we point out the differences, following an illustrative example, given in [52, Chapter 2.1.1]. Consider the compound register $X = (Y_1, ..., Y_n)$ with classical state set $\Sigma = \Sigma_1 \times ... \times \Sigma_n$, where $\Sigma_1, ..., \Sigma_n$ are the classical state sets of the registers $Y_1, ..., Y_n$. Suppose, we obtain a classical state $x = (y_1, ..., y_n)$ of the register X. Then, the classical state of Y_k is determined unambiguously by y_k for all $k \in \{1, 2, ..., n\}$. Contrariwise, if we hold the states y_k from Y_k the state of X is determined by $x = (y_1, ..., y_n)$. An entirely different behaviour is shown by probabilistic states, as defined in [52, Chapter 2.1.2].

Definition 1.13 ***(Probabilistic State)***
A probabilistic state of a register X refers to a probability distribution P over the classical state set Σ of that register. A probabilistic state of X is identified with a probability vector $p \in \mathcal{P}(\Sigma)$. For a given classical state $a \in \Sigma$, the probability that a is attained is given by $p(a)$.

Probabilistic states and quantum states are not exactly the same, since quantum states are represented by density operators instead of probability vectors. Nevertheless, in a mathematical sense, one can identify both notions [52, Chapter 2.1.2].

One of Claude Shannon's seminal works deals with the task of quantifying the amount of information associated with a certain state of interest. For classical information theory, he introduced the concept of entropy. Entropy measures how much information one gains once he learns the value of some random variable. Often, it is referred to as some 'uncertainty measure' of a certain state. Exactly speaking, the entropy is the expected information content of the random variable associated with the considered state. We start by defining the classical Shannon entropy of a random variable [54, Definition 10.1.1].

Definition 1.14 ***(Classical (Shannon) Entropy)***
Let X be a discrete random variable with probability distribution $p_X(x)$. The entropy of X is given by

$$H(X) := -\sum_x p_X(x)\log_2(p_X(x)). \tag{1.9}$$

As we require $\lim_{x\to 0} x\log_2(x) = 0$, $H(X)$ is well-defined. A special case of the Shannon entropy is the binary entropy, measuring the information content of a binary random variable, i.e., a random variable that can occupy only one out of two states (e.g., a coin that is flipped) [54, Definition 10.1.2].

Definition 1.15 ***(Binary Entropy)***
The binary entropy of $p \in [0,1]$ is given by

$$h(p) = -p\log_2(p) - (1-p)\log_2(1-p). \tag{1.10}$$

Next, we consider a situation playing a central role in quantum communication. Assume two parties hold variables X and Y, which share some correlations. One might ask how the information content of X is related to the information content of the other random variable Y (or vice-versa). For example, both random variables can be linked such that X and Y always have the same value. Then, we would not be surprised at all learning the state of X if we already know Y. Contrarily, consider two random variables X and Y having no correlations at all. Even if we learn the value of Y the value of the random variable X still is a mystery, so the information content of X has not changed from our perspective. Alternatively, we still experience the same surprise when learning the value of X as we had experienced when learning about X before knowing Y. The joint entropy and the conditional entropy will be useful when dealing with such situations. They are defined as follows [54, Definition 10.3.1 and Defintion 10.2.1]:

Definition 1.16 ***(Joint Entropy)***
Let X and Y be discrete random variables with joint probability distribution $p_{X,Y}(x,y)$. The joint entropy $H(X,Y)$ of X and Y is given by

$$H(X,Y) := -\sum_{x,y} p_{X,Y}(x,y)\log_2(p_{X,Y}(x,y)). \tag{1.11}$$

Definition 1.17 ***Conditional Entropy***
Let X and Y be discrete random variables with joint probability distribution $p_{X,Y}(x,y)$. The conditional entropy $H(X|Y)$ of X conditioned on Y is known is given by

$$H(X|Y) := -\sum_{x,y} p_{X,Y}(x,y)\log_2(p_{X|Y}(x|y)). \tag{1.12}$$

They are related to each other by

$$H(X,Y) = H(X|Y) + H(Y) = H(Y|X) + H(X), \tag{1.13}$$

as can be derived readily.
Another important quantity that will be handy when dealing with correlated random variables is the mutual information. It measures how much information the random variables X and Y have in common and is given by [33, Chapter 11.2.3].

Definition 1.18 ***(Mutual Information)***
Let X and Y be discrete random variables with joint probability distribution $p_{X,Y}(x,y)$. The mutual information $I(X:Y)$ of X and Y is given by

$$I(X:Y) := H(X) + H(Y) - H(X,Y). \tag{1.14}$$

Obviously, it might occur that three or even more random variables are correlated in some way, hence we require the mentioned quantities for more than two random variables. We introduced the entropies and the mutual information for two random variables to explain the basic concept, but they can be generalised to n random variables in a natural way. Having this said, we proceed with the quantum equivalents of the classical quantities. The quantum version of the entropy named after John von Neumann is a generalisation of the Shannon entropy and takes into account that quantum states are described by density operators rather than probability distributions. It is defined as follows [54, Definition 11.1.1].

Definition 1.19 ***(Quantum (von Neumann) Entropy)***
Let $\mathcal{H}$ be a finite dimensional Hilbert space. Suppose a quantum system A is prepared in a state $\rho_A \in \mathcal{D}(\mathcal{H}_A)$. Then the quantum entropy $S(A)$ of the state ρ_A is defined as

$$S(A) := -Tr[\rho_A \log_2(\rho_A)]\,. \tag{1.15}$$

We note that some authors denote the quantum entropy by $H(\rho_A)$, where H generally stands for entropy, and the density operator indicates that we deal with a quantum state. All classical quantities from above can be generalised to the quantum case in a natural way [54], for example, the joint quantum entropy of the state ρ_{AB}, common to the systems A and B reads

$$S(A, B) := -\mathrm{Tr}\left[\rho_{AB} \log_2(\rho_{AB})\right] \tag{1.16}$$

and the conditional quantum entropy of those states reads

$$S(A|B) := S(A, B) - S(B). \tag{1.17}$$

The quantum relative entropy D plays a central role in the present thesis. It measures the distinguishability of two quantum states and is defined as follows [54, Definition 11.8.2].

Definition 1.20 ***(Quantum Relative Entropy)***
Let $\mathcal{H}$ be a finite-dimensional Hilbert space. The quantum relative entropy $D(\rho||\sigma)$ between a density operator $\rho \in \mathcal{D}(\mathcal{H})$ and a non-negative, linear operator σ (so essentially a density operator up to trace one) is defined as

$$D(\rho||\sigma) := \begin{cases} Tr\left[\rho \log(\rho)\right] - Tr\left[\rho \log(\sigma)\right] & , \textit{if } supp(\rho) \subseteq supp(\sigma) \\ \infty & , \textit{otherwise}, \end{cases} \tag{1.18}$$

where $supp(A) := \{|\psi\rangle \in \mathcal{H} : A|\psi\rangle \neq 0\}$.

In general, the maximisation of the mutual information of a state, held by two parties, is a non-trivial task. This situation is central to quantum communication as one aims to choose an ideal measurement to maximise the information between the communication parties. A brief description of the underlying problem is given in [54, Chapter 11.6.1]. Suppose Alice prepares an ensemble of classical states ρ_x following some probability distribution, i.e., every state ρ_x is prepared with probability p_x for $x \in \{0, 1, ..., n\}$, $\mathcal{E} := \{\rho_x, p_x\}$. Afterwards, she hands this ensemble to Bob without telling him the classical index x of the prepared symbol. Therefore, as Bob does not have any knowledge about the classical index, Bob's density operator is given by the mixture $\rho_B = \sum_x p_x \rho_x$. Since he wants to determine the classical index x, Bob is looking for the optimal measurement he can do to maximise the information about Alice's state X. Mathematically spoken, Bob wants to maximise the mutual information between his and Alice's state, which is a difficult task.
A theorem addressing this particular situation was given by Alexander Holevo [33, Theorem 12.1].

Theorem 1.21 ***(Holevo's theorem)***
Suppose Alice prepares a state ρ_x where $x \in \{0, 1, ..., n\}$ with probabilities $p_0, p_1, ..., p_n$. Bob performs a POVM, given by $\{E_y\} = \{E_0, E_1, ..., E_m\}$ with measurement outcome Y. Then the mutual information between Alice's and Bob's state is bounded by

$$I(X : Y) \leqslant \chi(\rho_B) := S(\rho_B) - \sum_x p_x S(\rho_x), \tag{1.19}$$

where χ is called the Holevo information or Holevo quantity and $\rho_B = \sum_x p_x \rho_x$ is the state Bob receives.

2. Description of the objective protocols

In this section, we introduce the protocols that are examined in what follows. We are going to deal with four- and eight state prepare-and-measure (P&M) phase-shift-keying protocols of the same type as 'Protocol 2' in [29]. Thus, we use the same formulation of the postprocessing steps as in [29] and try to stick close to the notation of that paper. The basic setting of quantum communication is the same for all examined protocols, independently of the number of signal-states and the chosen postselection strategy and reads as follows.

Alice and Bob, two distant parties who want to create secure communication, are connected by two channels. The first channel is a quantum channel, and the second one is an authenticated classical channel. An eavesdropper, commonly called Eve, is assumed to be only limited by the laws of physics, hence can manipulate all signals that are sent over the quantum channel. In particular, she may store quantum states and perform measurements at any time. Furthermore, Eve can listen to the communication via the classical channel, but she cannot manipulate the exchanged classical signals. In order to establish secure communication, Alice prepares a coherent state $|\psi_x\rangle$ from some set of states (whose cardinality depends on the chosen protocol) according to some probability p_x. This state is sent to Bob using the quantum channel, who performs heterodyne measurements after receiving his share. Then, Alice and Bob use the classical channel to exchange information to establish a secret key and to find out how much information Eve might have gained. As Alice prepares some states and Bob performs measurements, we deal with a prepare-and-measure protocol. Nevertheless, the source replacement scheme [7, 11] allows us to translate this into the entanglement-based scheme (and vice-versa). Therefore, we are free to switch between both schemes and may choose those scheme that is more convenient for the mathematical description. So, for example, if Alice prepares states $\{|\psi_x\rangle\}_x$ according to some probability distribution $\{p_x\}_x$, the corresponding formulation in the entanglement-based scheme would be $|\Psi\rangle_{AA'} = \sum_x \sqrt{p_x}|x\rangle_A|\psi_x\rangle_{A'}$. Here, we notated by A the register which is kept by Alice and by A' the register that is sent to Bob. Furthermore, we use B to label Bob's and E to denote Eve's register.

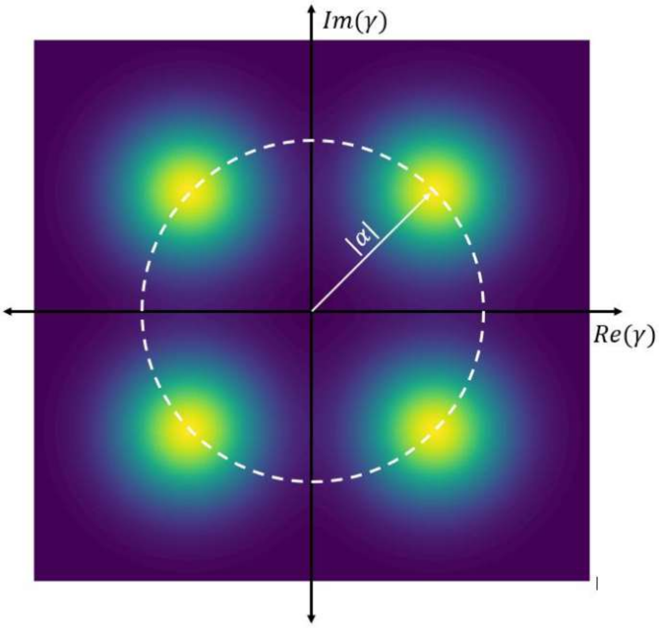


Figure 2.1.: Illustration of the arrangement of the prepared coherent states in the phase space. $|\alpha|$ is the coherent state amplitude.

2.1. Examined four-state protocols

In contrast to [29], we rotated the signal-states by $\pi/4$ in the p-q-plane such that they are not located on the axes but on the diagonals, which is in accordance with the arrangement of the signal states in classical QPSK-schemes. In the first part of this thesis, we investigate the influence of different postselection strategies on the key-rate of four-state protocols. So, the main difference between the examined protocols will occur in 4) of the following description.

Let $N \in \mathbb{N}$ be the block size of the raw key.

1) In each round, $n \leqslant N$ Alice prepares one out of four coherent states $|\Psi_n\rangle \in \{||\alpha|e^{i\frac{\pi}{4}}\rangle, ||\alpha|e^{i\frac{3\pi}{4}}\rangle, ||\alpha|e^{i\frac{5\pi}{4}}\rangle, ||\alpha|e^{i\frac{7\pi}{4}}\rangle\}$, where the coherent state-amplitude $|\alpha| > 0$ is chosen arbitrarily but fixed, according to some probability distribution. For example, for the present thesis, we chose the uniform distribution. The first state $||\alpha|e^{\frac{\pi}{4}}\rangle$ is associated with the symbol $x_n = 0$, the second one with the symbol $x_n = 1$, and so on. This phase is called **state preparation**.

After preparing one of these states, Alice sends it to Bob using the quantum channel.

2) When Bob receives the state, he performs heterodyne measurement, described by the POVM $\{E_\gamma = \frac{1}{\pi}|\gamma\rangle\langle\gamma| \ : \gamma \in \mathbb{C}\}$, and obtains some complex number y_n. That is called the **measurement phase**.

3) Next, Alice and Bob agree to choose some small, random subset $\mathcal{I}_{\text{Test}} \subset \{n \in \mathbb{N} \ : \ n \leqslant N\}$ and reveal the corresponding symbols x_l and measurement results y_l for $l \in \mathcal{I}_{\text{Test}}$ using the classical channel to perform **parameter estimation**, i.e., they determine the amount of information Eve might have gained about the key. The remaining rounds $\mathcal{I}_{\text{key}} := \{n \in \mathbb{N} \ : \ n \leqslant N\} \backslash \mathcal{I}_{\text{test}}$ will be used for key generation. For simplicity, we assume that $\mathcal{I}_{\text{key}}$ contains the first $m := |\mathcal{I}_{\text{key}}|$ rounds that can be used for key-generation (this can be assumed without loss of generality, as we always find some bijective map that reorders the set). After this step, Alice holds a key string $\mathbf{X} := (x_1, ..., x_m)$.

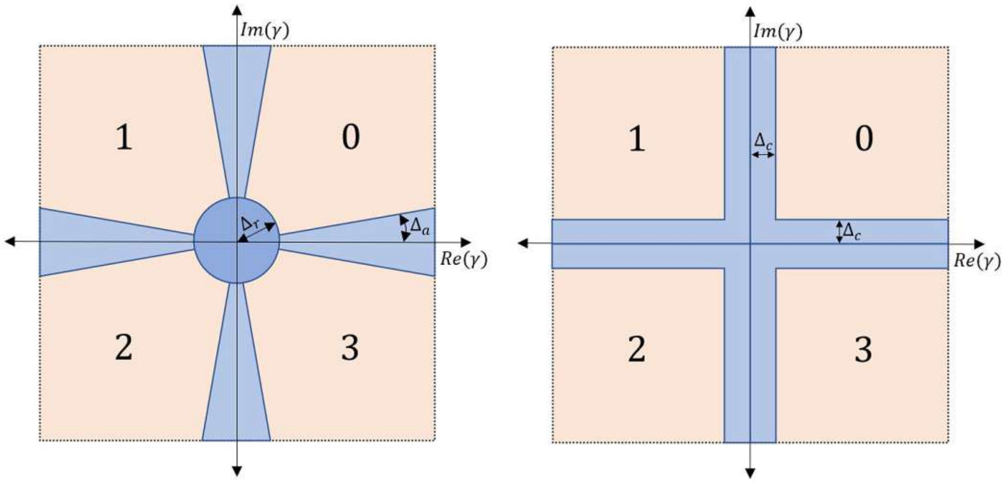
4) Now we perform a reverse reconciliation keymap to obtain Bob's key string $\mathbf{Z} = (z_j)_{j \in \mathcal{I}_{\text{key}}}$, where Bob's measurement outcomes y_l for rounds $l \in \mathcal{I}_{\text{key}}$ are assigned to some element in the set $\{0, 1, 2, 3, \perp\}$. The keymap differs, depending on the chosen postselection strategy.

   i) **Radial postselection (rPS):** Fix some $0 \leqslant \Delta_r \in \mathbb{R}$ and determine Bob's key string according to the following rule:

$$z_j = \begin{cases} 0 & \arg(y_j) \in \left[0, \frac{\pi}{2}\right) \wedge |y_j| \geqslant \Delta_r, \\ 1 & \arg(y_j) \in \left[\frac{\pi}{2}, \pi\right) \wedge |y_j| \geqslant \Delta_r, \\ 2 & \arg(y_j) \in \left[\pi, \frac{3\pi}{2}\right) \wedge |y_j| \geqslant \Delta_r, \\ 3 & \arg(y_j) \in \left[\frac{3\pi}{2}, 2\pi\right) \wedge |y_j| \geqslant \Delta_r, \\ \perp & \text{otherwise.} \end{cases} \tag{2.1}$$

   ii) **Radial and angular postselection (raPS):** Fix some $0 \leqslant \Delta_r \in \mathbb{R}$ and $0 \leqslant \Delta_a \in \mathbb{R}$ and determine Bob's key string according to the following rule:

$$z_j = \begin{cases} 0 & \arg(y_j) \in \left[\Delta_a, \frac{\pi}{2} - \Delta_a\right) \wedge |y_j| \geqslant \Delta_r, \\ 1 & \arg(y_j) \in \left[\frac{\pi}{2} + \Delta_a, \pi - \Delta_a\right) \wedge |y_j| \geqslant \Delta_r, \\ 2 & \arg(y_j) \in \left[\pi + \Delta_a, \frac{3\pi}{2} - \Delta_a\right) \wedge |y_j| \geqslant \Delta_r, \\ 3 & \arg(y_j) \in \left[\frac{3\pi}{2} + \Delta_a, 2\pi - \Delta_a\right) \wedge |y_j| \geqslant \Delta_r, \\ \perp & \text{otherwise.} \end{cases} \tag{2.2}$$



(a) Sketch for radial- (rPS) and radial&angular (raPS) postselection

(b) Sketch for cross postselection (cPS).

Figure 2.2.: (a) Keymap for radial- (rPS) and radial&angular postselection (raPS). Bob's measurement outcomes $\gamma \in \mathbb{C}$, lying in one of the blue-shaded areas are postselected, i.e., they are assigned to the symbol $\perp$. The remaining outcomes are assigned to the bit-values that are associated with numbers written in the quadrants. Δ_r is the radial- and Δ_a is the angular postselection parameter. (b) Keymap for cross postselection (cPS). Bob's measurement outcomes $\gamma \in \mathbb{C}$ lying in one of the blue-shaded areas are postselected, i.e., they are assigned to the symbol $\perp$. The remaining outcomes are assigned to the bit-values that are associated with the quadrants. In principle, one could choose different postselection parameters for real- and imaginary direction, but for symmetry reasons, we expect that both have to be chosen equally to maximize the key rate. Therefore, Δ_c is the postselection parameter for both directions.

iii) **Cross Postselection (cPS):** Fix some $0 \leqslant \Delta_c \in \mathbb{R}$ and determine Bob's key string according to the following rule:

$$z_j = \begin{cases} 0 & \Re(y_j) \in [\Delta_c, \infty) \wedge \Im(y_k) \in [\Delta_c, \infty)\,, \\ 1 & \Re(y_j) \in (-\infty, \Delta_c] \wedge \Im(y_k) \in [\Delta_c, \infty)\,, \\ 2 & \Re(y_j) \in (-\infty, -\Delta_c] \wedge \Im(y_k) \in (-\infty, -\Delta_c]\,, \\ 3 & \Re(y_j) \in [\Delta_c, \infty) \wedge \Im(y_k) \in (-\infty, -\Delta_c]\,, \\ \perp & \text{otherwise.} \end{cases} \tag{2.3}$$

Note that all three postselection strategies coincide for $\Delta_r = \Delta_a = \Delta_c = 0$, which is the case without any postselection, and that rPS is a special case of raPS for $\Delta_a = 0$.

5) Finally, Alice and Bob perform classical **error correction and privacy amplification** algorithms to generate a secret key. In what follows, we briefly discuss these terms, following [26]. The technique, where one party sends information on its share on the key to the other one, which corrects its bit-string according to the other's data, is called one-way information reconciliation. Obviously, one-way error correction can be carried out in two different ways; either Bob corrects his key string according to Alice's instructions which is called direct reconciliation, or Alice corrects her key string according to Bob's data which is called reverse reconciliation. Since direct reconciliation is limited to total transmittances > 0.5 (otherwise, Eve potentially has more information about Alice's data than Bob), we focus on reverse reconciliation, where no such limitation exists. The efficiency of the used routine $0 < \beta < 1$ is called reconciliation efficiency. After that, Alice and Bob confirm their key, using a family of almost universal hash functions to upper-bound the probability that the error correction has failed. If the hash-values are different, they omit the key and restart the key generation process. Finally, Alice and Bob aim to reduce Eve's knowledge about their shared key as much as possible. That is called privacy amplification and, for example, can be done by a seeded randomness extractor algorithm.

Using the definitions of the postselection maps, we define the following subsets of the phase space ($\mathbb{C}$)

$$\begin{aligned} A_0^{\text{ra}} &:= \left\{ z \in \mathbb{C} : \arg(z) \in \left[\Delta_a, \frac{\pi}{2} - \Delta_a\right) \wedge |z| \geqslant \Delta_r \right\}, \\ A_1^{\text{ra}} &:= \left\{ z \in \mathbb{C} : \arg(z) \in \left[\frac{\pi}{2} + \Delta_a, \pi - \Delta_a\right) \wedge |z| \geqslant \Delta_r \right\}, \\ A_2^{\text{ra}} &:= \left\{ z \in \mathbb{C} : \arg(z) \in \left[\pi + \Delta_a, \frac{3\pi}{2} - \Delta_a\right) \wedge |z| \geqslant \Delta_r \right\}, \\ A_3^{\text{ra}} &:= \left\{ z \in \mathbb{C} : \arg(z) \in \left[\frac{3\pi}{2} + \Delta_a, 2\pi - \Delta_a\right) \wedge |z| \geqslant \Delta_r \right\}, \end{aligned} \tag{2.4}$$

and

$$
\begin{aligned}
A_0^{\mathrm{c}} &:= \{z \in \mathbb{C} : \Re(z) \geqslant \Delta_c \wedge \Im(z) \geqslant \Delta_c\}\,, \\
A_1^{\mathrm{c}} &:= \{z \in \mathbb{C} : \Re(z) \leqslant -\Delta_c \wedge \Im(z) \geqslant \Delta_c\}\,, \\
A_2^{\mathrm{c}} &:= \{z \in \mathbb{C} : \Re(z) \leqslant -\Delta_c \wedge \Im(z) \leqslant -\Delta_c\}\,, \\
A_3^{\mathrm{c}} &:= \{z \in \mathbb{C} : \Re(z) \geqslant \Delta_c \wedge \Im(z) \leqslant -\Delta_c\}\,.
\end{aligned}
\tag{2.5}
$$

for the radial&angular and the cross-shaped postselection scheme, respectively. The chosen postselection is indicated by the superscript (ra for radial&angular and c for cross-shaped). Note that one obtains the sets for the radial postselection scheme from the sets referring to the radial&angular scheme by setting $\Delta_a = 0$.

2.2. Examined eight-state protocols

In addition to the four-state protocols, we examine generalisations to eight signal states, which are arranged in the phase space as depicted in Figure 2.3. These eight-state protocols differ from the four state protocols only in the number of signal states and, consequently, the postselection scheme. Therefore, it is sufficient to replace 1) and 4) in the protocol description in the previous section. The corresponding key map is sketched in Figure 2.3.

1*) In each round, $n \leqslant N$ Alice prepares one out of eight coherent states $|\Psi_n\rangle \in \{||\alpha|\rangle, ||\alpha|e^{i\frac{\pi}{4}}\rangle, i|\alpha|\rangle, ||\alpha|e^{i\frac{3\pi}{4}}, -|\alpha|\rangle, ||\alpha|e^{i\frac{5\pi}{4}}, -i|\alpha|\rangle, ||\alpha|e^{i\frac{7\pi}{4}}\rangle\}$, where the coherent state-amplitude $|\alpha| > 0$ is chosen arbitrary but fixed, according to some probability distribution. For example, in the present work, we chose the uniform distribution. The first state $|\alpha|e^{\frac{\pi}{4}}\rangle$ is associated with the symbol $x_k = 0$, the second one with the symbol $x_k = 1$, and so on. This phase is called **state preparation**. After preparing one of these states, Alice sends it to Bob using the quantum channel.

4*) We perform a reverse reconciliation keymap to obtain Bob's key string $\mathbf{Z} = (z_j)_{j\in\mathcal{I}_{\text{key}}}$, where Bob's measurement outcomes y_l for rounds $l \in \mathcal{I}_{\text{key}}$ are assigned to some element in the set $\{0, 1, 2, 3, 5, 6, 7, \perp\}$. The keymap differs, depending on the chosen postselection strategy.

i) **Radial postselection (rPS):** Fix some $0 \leqslant \Delta_r \in \mathbb{R}$ and determine

Bob's key string according to the following rule:

$$z_j = \begin{cases} 0 & \arg(y_j) \in \left[-\frac{\pi}{8}, \frac{\pi}{8}\right) \wedge |y_j| \geqslant \Delta_r, \\ 1 & \arg(y_j) \in \left[\frac{\pi}{8}, \frac{3\pi}{8}\right) \wedge |y_j| \geqslant \Delta_r, \\ 2 & \arg(y_j) \in \left[\frac{3\pi}{8}, \frac{5\pi}{8}\right) \wedge |y_j| \geqslant \Delta_r, \\ 3 & \arg(y_j) \in \left[\frac{5\pi}{8}, \frac{7\pi}{8}\right) \wedge |y_j| \geqslant \Delta_r, \\ 4 & \arg(y_j) \in \left[\frac{7\pi}{8}, \frac{9\pi}{8}\right) \wedge |y_j| \geqslant \Delta_r, \\ 5 & \arg(y_j) \in \left[\frac{9\pi}{8}, \frac{11\pi}{8}\right) \wedge |y_j| \geqslant \Delta_r, \\ 6 & \arg(y_j) \in \left[\frac{11\pi}{8}, \frac{13\pi}{8}\right) \wedge |y_j| \geqslant \Delta_r, \\ 7 & \arg(y_j) \in \left[\frac{13\pi}{8}, \frac{15\pi}{8}\right) \wedge |y_j| \geqslant \Delta_r, \\ \perp & \text{otherwise.} \end{cases} \tag{2.6}$$

ii) **Radial and angular postselection (raPS)** Fix some $0 \leqslant \Delta_r \in \mathbb{R}$ and $0 \leqslant \Delta_a \in \mathbb{R}$ and determine Bob's key string according to the following rule.

$$z_j = \begin{cases} 0 & \arg(y_j) \in \left[-\frac{\pi}{8} + \Delta_a, \frac{\pi}{8} - \Delta_a\right) \wedge |y_j| \geqslant \Delta_r, \\ 1 & \arg(y_j) \in \left[\frac{\pi}{8} + \Delta_a, \frac{3\pi}{8} - \Delta_a\right) \wedge |y_j| \geqslant \Delta_r, \\ 2 & \arg(y_j) \in \left[\frac{3\pi}{8} + \Delta_a, \frac{5\pi}{8} - \Delta_a\right) \wedge |y_j| \geqslant \Delta_r, \\ 3 & \arg(y_j) \in \left[\frac{5\pi}{8} + \Delta_a, \frac{7\pi}{8} - \Delta_a\right) \wedge |y_j| \geqslant \Delta_r, \\ 4 & \arg(y_j) \in \left[\frac{7\pi}{8} + \Delta_a, \frac{9\pi}{8} - \Delta_a\right) \wedge |y_j| \geqslant \Delta_r, \\ 5 & \arg(y_j) \in \left[\frac{9\pi}{8} + \Delta_a, \frac{11\pi}{8} - \Delta_a\right) \wedge |y_j| \geqslant \Delta_r, \\ 6 & \arg(y_j) \in \left[\frac{11\pi}{8} + \Delta_a, \frac{13\pi}{8} - \Delta_a\right) \wedge |y_j| \geqslant \Delta_r, \\ 7 & \arg(y_j) \in \left[\frac{13\pi}{8} + \Delta_a, \frac{15\pi}{8} - \Delta_a\right) \wedge |y_j| \geqslant \Delta_r, \\ \perp & \text{otherwise} \end{cases} \tag{2.7}$$

Using these definitions for the postselection maps, we define the following subsets of the phase space ($\mathbb{C}$)

$$\begin{aligned}
A_0^{\text{ra}} &:= \left\{z \in \mathbb{C} : \arg(z) \in \left[-\frac{\pi}{8} + \Delta_a, \frac{\pi}{8} - \Delta_a\right) \wedge |z| \geqslant \Delta_r\right\}, \\
A_1^{\text{ra}} &:= \left\{z \in \mathbb{C} : \arg(z) \in \left[\frac{\pi}{8} + \Delta_a, \frac{3\pi}{8} - \Delta_a\right) \wedge |z| \geqslant \Delta_r\right\}, \\
A_2^{\text{ra}} &:= \left\{z \in \mathbb{C} : \arg(z) \in \left[\frac{3\pi}{8} + \Delta_a, \frac{5\pi}{8} - \Delta_a\right) \wedge |z| \geqslant \Delta_r\right\}, \\
A_3^{\text{ra}} &:= \left\{z \in \mathbb{C} : \arg(z) \in \left[\frac{5\pi}{8} + \Delta_a, \frac{7\pi}{8} - \Delta_a\right) \wedge |z| \geqslant \Delta_r\right\}, \\
A_4^{\text{ra}} &:= \left\{z \in \mathbb{C} : \arg(z) \in \left[\frac{7\pi}{8} + \Delta_a, \frac{9\pi}{8} - \Delta_a\right) \wedge |z| \geqslant \Delta_r\right\}, \\
A_5^{\text{ra}} &:= \left\{z \in \mathbb{C} : \arg(z) \in \left[\frac{9\pi}{8} + \Delta_a, \frac{11\pi}{8} - \Delta_a\right) \wedge |z| \geqslant \Delta_r\right\}, \\
A_6^{\text{ra}} &:= \left\{z \in \mathbb{C} : \arg(z) \in \left[\frac{11\pi}{8} + \Delta_a, \frac{13\pi}{8} - \Delta_a\right) \wedge |z| \geqslant \Delta_r\right\}, \\
A_7^{\text{ra}} &:= \left\{z \in \mathbb{C} : \arg(z) \in \left[\frac{13\pi}{8} + \Delta_a, \frac{15\pi}{8} - \Delta_a\right) \wedge |z| \geqslant \Delta_r\right\}
\end{aligned} \tag{2.8}$$

for the radial&angular postselection scheme, as indicated by the superscript. Note that one obtains the sets for the radial postselection scheme from the sets referring to the radial&angular scheme by setting $\Delta_a = 0$, hence we do not define separate sets for the radial postselection scheme.

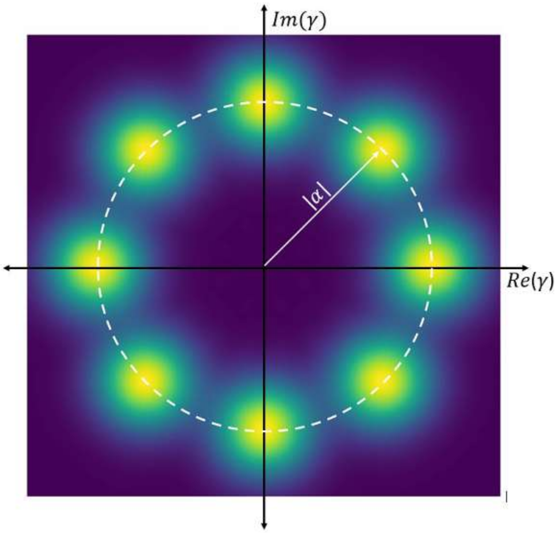


Figure 2.3.: Illustration of the arrangement of the prepared coherent states for eight-state protocols in the phase space. $|\alpha|$ is the chosen coherent state amplitude.

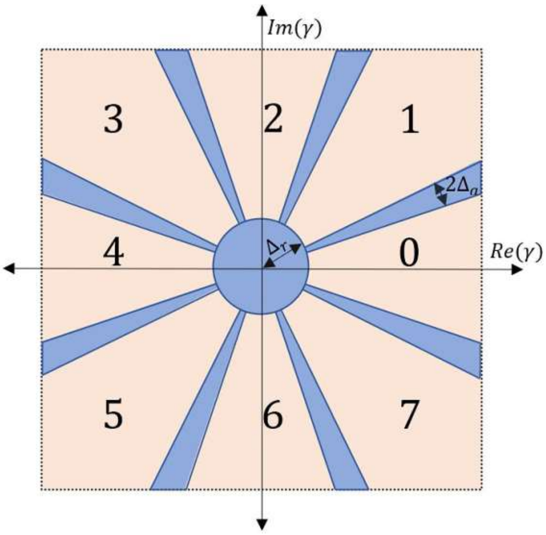


Figure 2.4.: Sketch of the keymap for radial (rPS) and radial&angular postselection (raPS) for eight-state protocols. Bob's measurement outcomes $\gamma \in \mathbb{C}$ lying in one of the blue-shaded areas are postselected, i.e., they are assigned to the symbol $\perp$. The remaining outcomes are assigned to the bit-values that are associated with numbers written in the quadrants. Δ_r is the radial- and Δ_a is the angular postselection parameter.

3. Description of the security proof approach

The security proof framework used within this thesis was introduced in [6, 55] and a model for the postprocessing steps was published in [29]. In this chapter, we give a brief summary of the security proof approach following those sources. For the sake of uniformity we stick close to the notation of [29, 55]. We denote Alice's finite-dimensional Hilbert space by $\mathcal{H}_A$, the infinite-dimensional Hilbert space describing Bob's state space by $\mathcal{H}_B$ and their joint state space by $\mathcal{H}_{AB}$.

3.1. Finding an expression for the secret key rate

The goal of every security proof not only for discrete modulated CV-QKD protocols is to find or lower-bound the achievable secure key rate, assuming collective attacks. In the present thesis, we are interested in the secret key generation rate, i.e. the average amount of secret information per transmitted signal, commonly called (secure or secret) key rate. Here, we try to motivate the mathematical key rate finding problem for the present protocol-types, starting with considerations regarding the error correction phase, where Alice and Bob try to synchronise their key strings. The mutual information between Alice and Bob gives the amount of information one of both has to reveal to correct the differences between the key strings,

$$I(A:B) = H(A) + H(B) - H(AB) = H(A) - H(A|B), \tag{3.1}$$

where we used the corresponding definitions of the mutual information and the joint entropy, given in Chapter 1. The last expression has a nice interpretation. It tells us that the amount of information that has to be revealed is equal to Bob's uncertainty about Alice's raw key (or vice-versa, Alice's uncertainty about Bob's raw key).

Next, we deal with the privacy amplification phase, where Alice and Bob aim to destroy as much of Eve's information about their bit strings as possible. Depending on whose bit string Eve gained less information about, they have to destroy at least $\min(I_{EA}, I_{EB})$ bits of information, where I_{EA} denotes the amount of information Eve gained about Alice's bit string and I_{EB} denotes the amount of information

Eve gained about Bob's bit string. Unfortunately, we do not know much about either I_{EA} and I_{EB}. For the case of reverse reconciliation, which is when Bob keeps his bit string and Alice adapts her, the Devetak-Winter theorem [9] states

$$R \geqslant I(A:B) - I(B:E). \tag{3.2}$$

As the second term in this expression is difficult to calculate, we use Holevo's theorem (Theorem 1.21) to upper-bound Eve's knowledge on the key, hence lower-bound the key rate by

$$R \geqslant I(A:B) - \chi(B:E), \tag{3.3}$$

where χ is the Holevo quantity.

After taking into account that not all rounds pass the postselection phase, we obtain for the secure key rate in the asymptotic limit

$$R^{\infty} = p_{\text{pass}} \left(I(A:B) - \max_{\text{Eve}} \chi(B:E) \right), \tag{3.4}$$

where p_{pass} is the probability of passing the postselection phase. According to [55], this expression can be reformulated further to

$$R^{\infty} = \min_{\rho_{AB} \in \mathcal{S}} f(\rho_{AB}) - p_{pass}\delta_{EC}, \tag{3.5}$$

where $f(\rho_{AB}) = D\left(\mathcal{G}\left(\rho_{AB}\right) || \mathcal{Z}\left(\mathcal{G}\left(\rho_{AB}\right)\right)\right)$. Note that p_{pass} is implicitly included in f. The set $\mathcal{S}$, a subset of $\text{Pos}(\mathcal{H}_{AB})$, is the feasible set of the optimisation and is given by a set of linear constraints,

$$\mathcal{S} := \{\rho \in \text{Pos}(\mathcal{H}_{AB}) \mid \forall i \in I: \ \text{Tr}\left[\Gamma_i \rho\right] = \gamma_i\}. \tag{3.6}$$

By $I \subset \mathbb{N}$ we denote some finite subset of the natural numbers. The Hermitian operators $\Gamma_i \in \text{Herm}(\mathcal{H}_{AB})$ represent (quantum-)measurements and the $\gamma_i \in \mathbb{R}$ are measurement results. Both will be specified later based on the physical model. By D, we denote the quantum relative entropy (see Definition 1.20), $\mathcal{G}$ is a completely positive trace non-increasing map, and $\mathcal{Z}$ is a pinching quantum channel. In particular, both $\mathcal{G}$ and $\mathcal{Z}$ are linear maps that depend on the chosen protocol and postselection strategy and will be specified later. Finally, δ_{EC} is a parameter depending on the performed post-processing and error correction routines and p_{pass} is the probability to pass the postselection phase.

A physical interpretation of this minimisation problem can be as follows. By solving the present optimisation problem, we search the worst-case density operator which yields the lowest secure key rate and is still compatible with the constraints, which are given by physical requirements. This means that we search for the secure key rate Alice and Bob can achieve when Eve performs an optimal eavesdropping attack.

Using Lindblad's theorem [30] and the linearity of the maps $\mathcal{G}$ and $\mathcal{Z}$ it was shown that the target function f is convex. Furthermore, f is continuous and bounded from below and it was shown that the present optimisation problem attains its minimum and that every local minimum is already a global minimum. Additionally, the admissible set $\mathcal{S}$ is convex. Thus, we deal with an infinite-dimensional convex minimisation problem with linear constraints and the additional requirement that all admissible ρ are positive semi-definite. Hence, we face a semi-definite program over an infinite-dimensional separable Hilbert space which is spanned by the basis of Fock states $\{|n\rangle : \ n \in \mathbb{N}_0\}$.

When we try to solve this optimisation problem, we face two issues. First, the problem lives in an infinite-dimensional Hilbert space and second the objective function is highly non-linear. Therefore, in order to make this problem computationally feasible, we approximate the infinite-dimensional Hilbert space by a finite dimensional one. Following the so-called photon-number cutoff assumption in [29], the infinite-dimensional space is approximated by the finite-dimensional space spanned by the first $N_c + 1 \in \mathbb{N}_0$ Fock states, $\mathcal{H}_B^{N_c} := \{|n\rangle : \ 0 \leqslant n \leqslant N_c\}$, where N_c is called the photon cutoff number. For the finite-dimensional minimisation problem it is an easy exercise to show that it still obeys the same properties as the finite-dimensional problem. In fact, the proof of most of the properties that required some work in the infinite-dimensional case turn out to be quite obvious in the finite-dimensional case.

Contrary to many other minimisation problems, here it is not sufficient to find an almost optimal value, as this would give us merely an upper bound on the secure key rate. Therefore, it is not tolerable to solve this problem numerically and approximatively and use the numerical solution for key rate calculation. In response to this issue, the method introduced in [55] divides the problem into a two-step process. In the first step, an algorithm is applied to solve the problem approximately, i.e., to find an eavesdropping attack which is close to optimal. In the second step, this upper bound is converted into a lower bound combining a linearisation based on the result of the first step and the duality-theory for semi-definite programs. Finally, numerical errors like constraint violations are taken into account by using a relaxation theorem, which relates changes in the feasible set to changes in the minimum of the objective function.

3.2. Description of step 1

As elaborated in the previous section, the minimisation problem (3.5) is a semi-definite program (SDP) with convex domain of optimisation $\mathcal{S}$. In particular, the target-function attains its global minimum and every local minimum is already a global minimum. Hence, it is judicious to perform a numerical minimisation because we can expect to find some ρ_{AB} at least close to the global minimum, without getting stuck at any local minimum.

Therefore, our goal for the first step is to find a close to optimal attack, so a density matrix $\rho_{AB} \in \mathcal{S}$ that is close to the minimiser $\rho_{min} \in \mathcal{S}$ of the objective function. As already mentioned, our target function f is highly non-linear, hence we cannot apply an SDP solver directly. One can solve continuous, convex and non-linear minimisation problems numerically, using some iterative algorithm. As we deal with a constrained problem we either need an algorithm that does not leave the feasible set or we require some projection that brings us back into the feasible set after every iteration. The Frank-Wolfe algorithm [13] is guaranteed not to leave the feasible set, in contrast to rivalling methods like gradient descent. Therefore, we use a modified version of that algorithm, where we then have to solve a linearised problem, yielding a descent direction. Then, we perform a line-search towards the obtained descent direction in order to speed up the problem.

The original Frank-Wolfe algorithm reads as follows [13]:

Algorithm 3.1 ***(Frank-Wolfe Algorithm)***

```
Choose $x^{(0)} \in \mathcal{S}$
for $k = 1$ to $k_{max}$ do
    Compute $s := \arg\min \langle s, \nabla f(x^{(k)}) \rangle$
    Set $\gamma := \frac{2}{k+2}$
    Update $x^{(k+1)} := (1-\gamma)x^{(k)} + \gamma s$
end for
```

It is essential for the algorithm to begin with a feasible starting point $x^{(0)} \in \mathcal{S}$. In Section 5.1 we describe how such a feasible starting point can be found for the present problem.

According to [22], the iterates of the Frank-Wolfe algorithm satisfy

$$f(x^{(k)}) - f(x^*) \leqslant \mathcal{O}\left(\frac{1}{k}\right), \tag{3.7}$$

where x^* is the (unknown) optimal solution. In practical applications, this algorithm can be improved significantly by replacing the step width $\gamma = \frac{2}{k+2}$ by a line-search in direction of the steepest descent. Then, we do not know the exact convergence rate of the algorithm any more, but as the minimum in the descent direction obtained by line-search is always smaller or equal than the value of the objective function obtained using the step width of the original Frank-Wolfe algorithm, we know that we are going to expect at least the convergence rate mentioned above.

In the present problem, we consider the objective function

$$f(\rho) := D\left(\mathcal{G}(\rho)||\mathcal{G}\left(\mathcal{Z}(\rho)\right)\right). \tag{3.8}$$

Taylor's theorem yields for $\sigma, \rho \in \mathcal{S}$, $\Delta\rho := \sigma - \rho$

$$f(\sigma) = f(\rho) + \langle \Delta\rho, \nabla f(\rho)\rangle + \mathcal{O}\left(|\Delta\rho|^2\right). \tag{3.9}$$

Observe that the first term on the right-hand side is constant. We assume the quadratic term in the Taylor expansion being negligible, so we minimise the linearised problem $\langle \Delta\rho, \nabla f(\rho)\rangle = \mathrm{Tr}\left[(\Delta\rho)^\top \nabla f(\rho)\right]$ instead of the non-linear function f. Then, similarly to [55], we may apply the following modified Frank-Wolfe algorithm 3.1.

Algorithm 3.2 ***(Frank-Wolfe Algorithm for the present problem)***

```
Choose $\epsilon_{FW} > 0$ and $\rho^{(0)} \in \mathcal{S}$
for $k = 1$ to $k_{max}$ do
    Compute $\Delta\rho := arg\ min\ Tr\left[(\Delta\rho)^\top \nabla f(\rho^{(k)})\right]$ subject to $\Delta\rho + \rho^{(k)} \in \mathcal{S}$
    if $Tr\left[(\Delta\rho)^\top \nabla f(\rho^{(k)})\right] < \varepsilon$ then
        return $\rho^{(i)}$
    else
        Find $\lambda \in (0,1)$ such that $\lambda := argmin f(\rho^{(k)} + \lambda\ \Delta\rho)$
        Update $\rho^{(k+1)} := \rho^{(k)} + \lambda\Delta\rho$
    end if
end for
```

The additional stopping-criterion in Algorithm 3.2, $\mathrm{Tr}\left[(\Delta\rho)^\top \nabla f(\rho^{(k)})\right] < \epsilon_{FW}$, exits the loop once we are close to the minimum. This trace is exactly the inner product between $\Delta\rho$ and $\nabla f(\rho^{(k)})$, meaning that we stop if the descent direction $\Delta\rho$ and $\nabla f(\rho^{(k)})$ are almost orthogonal. This is necessary because we cannot expect the gradient to vanish at the optimal value for constrained optimisation problems. Therefore, we stop the modified Frank-Wolfe algorithm if the descent direction $\Delta\rho$ that we obtain from the minimisation problem is (almost) tangent to an equipotential line, meaning that following this direction does not decrease the value of the objective function significantly. For numerical reasons, we do not require the inner product to be exactly zero but smaller than some small ϵ_{FW}, indicating that we are close to the optimum.

As the objective function f is matrix-valued, we have to specify how we define the gradient of the map f at some ρ. Following [55], we define

$$\nabla f(\rho) := \sum_{k,j} d_{jk} \left|j\right\rangle\left\langle k\right|, \quad d_{jk} := \left.\frac{\partial f(\sigma)}{\partial \sigma_{jk}}\right|_{\sigma=\rho}, \quad \sigma_{jk} := \left\langle j\right| \sigma \left|k\right\rangle. \tag{3.10}$$

Inserting for f the present objective function $f(\rho) = D(\mathcal{G}(\rho)||\mathcal{Z}(\mathcal{G}(\rho)))$ and calculainge the gradient following the rules given in [35], we yield

$$\left[\nabla f(\rho)\right]^T = \mathcal{G}^\dagger \left(\log_2\left(\mathcal{G}(\rho)\right)\right) - \mathcal{G}^\dagger \left(\log_2\left(\mathcal{Z}(\mathcal{G}(\rho))\right)\right). \tag{3.11}$$

This gradient does not necessarily exist over the whole feasible set S. Following [55], we introduce a small perturbation, mapping $\mathcal{G}(\rho)$ to its interior. For $0 < \tilde{\epsilon} < 1$ we define

$$\mathcal{D}_{\tilde{\epsilon}}(\rho) := (1-\tilde{\epsilon})\rho + \tilde{\epsilon}\tau, \tag{3.12}$$

where $\tau = \frac{1}{d'}\mathbb{1}$ is the maximally mixed state, and d' is the dimension of $\mathcal{G}(\rho)$. Therefore, we finally define a perturbed map

$$\mathcal{G}_{\tilde{\epsilon}}(\rho) := \left(\mathcal{D}_{\tilde{\epsilon}} \circ \mathcal{G}\right)(\rho). \tag{3.13}$$

According [55, Lemma 1], the gradient of the perturbed function

$$f_{\tilde{\epsilon}}(\rho) := D\left(\mathcal{G}_{\tilde{\epsilon}}(\rho)||\mathcal{Z}(\mathcal{G}_{\tilde{\epsilon}}(\rho))\right) \tag{3.14}$$

exists for all $\rho \geqslant 0$. Similarly to the gradient for the unperturbed map, we calculate the gradient of the perturbed function, following the rules given in [35]. In the rest of this paper, we always replace $\mathcal{G}(\rho)$ by the perturbed map $\mathcal{G}_{\epsilon}(\rho)$ without stating this explicitly.

Summing up, Algorithm (3.2) yields a density matrix, which is close to optimal. Thus, the value $f(\rho_{step1})$ serves as an upper bound on the key rate, where the upper bound on the key rate is close to the secure key rate, if ρ_{step1} is close to the minimiser of the present problem, ρ^*.

3.3. Description of step 2

In the second step, we aim to convert the upper bound, obtained in step 1, into a lower bound on the secure key rate. The description of step 2 follows [55], where the reader finds proofs for the theorems. Starting from the result in step one, we are going to sketch the basic idea of the second step.

The basic idea of step 2 is to underestimate the secure key rate, combining SDP-duality theory and some linearisation, starting from the value we obtained from step 1, followed by considering numerical imprecisions. A sketch of the idea can be found in 3.1.

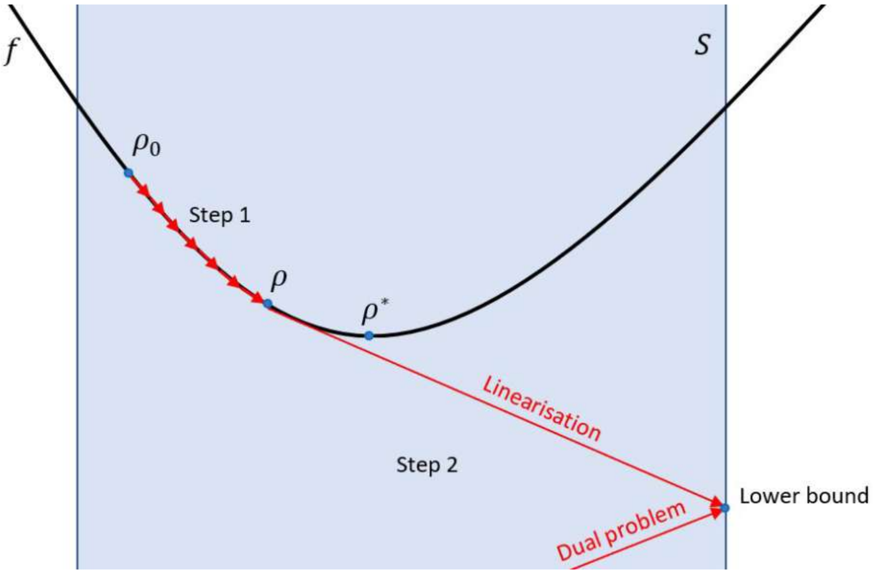


Figure 3.1.: Sketch of step 2

Consider the first-order Taylor expansion of our objective function around ρ, the result of step 1, and omit the terms of higher order,

$$T_1(\sigma) = f(\rho) + \mathrm{Tr}\left[(\sigma - \rho)^\top \nabla f(\rho)\right]. \tag{3.15}$$

As the objective function is convex, we know that the first-order Taylor expansion is always below the function,

$$\forall \sigma \in \mathcal{S}: \ f(\sigma) \geqslant T_1(\sigma). \tag{3.16}$$

Following our previous notation, we denote the minimiser of f by ρ^*. Then, we have

$$\begin{aligned} f(\rho^*) &\geqslant T_1(\rho^*) \\ &= f(\rho) + \mathrm{Tr}\left[(\rho^* - \rho)^\top \nabla f(\rho)\right] \\ &= f(\rho) + \min_{\tau \in \mathcal{S}} \mathrm{Tr}\left[(\tau - \rho)^\top \nabla f(\rho)\right] \\ &= f(\rho) - \mathrm{Tr}\left[\rho^\top \nabla f(\rho)\right] + \min_{\tau \in \mathcal{S}} \mathrm{Tr}\left[\tau^\top \nabla f(\rho)\right]. \end{aligned}$$

In the line step, we used that f is convex. For the second equality, we inserted the Taylor expansion from above and in the third line, we used that ρ^* is assumed to be the minimiser of f. In the last line, we just pulled out all terms of the minimisation that do not depend on τ.
The first two terms in the last line are known since we insert $\rho = \rho_{\text{start 1}}$, the result of step 1. The remaining minimisation problem is a semi-definite program with linear objective function and constraints similarly to those of the problem occurring in step 1. According to SDP duality theory, every semi-definite minimisation problem has a dual maximisation problem and the maximum of the dual problem is lower or equal to the minimum of the primal problem [5]. According to [55] strong duality holds, meaning that the solutions of both of the problems are equal, so one can replace the minimisation problem by the corresponding dual problem. Furthermore, for a reliable security proof, one has to take numerical errors like those due to finite precision and differences between the exact constraints and their computer representations into account. Let us denote the computer representations of the operators occurring in the constraints and the corresponding right-hand sides by tildes, so $\tilde{\Gamma}_i$ is the computer representation of the operator Γ and $\tilde{\gamma}$ is the computer representation of γ. If all constraints are satisfied up to some small number $\epsilon' > 0$,

$$\forall i \in I : \left|\mathrm{Tr}\left[\tilde{\Gamma}\rho - \tilde{\gamma}\right]\right| \leqslant \epsilon', \tag{3.17}$$

the following theorem holds [55].

Theorem 3.3 *Let* $\rho \in \left\{\rho \in \mathcal{H}_+^{N_c} \ : \ \left|Tr\left[\tilde{\Gamma}_i\rho - \tilde{\gamma}_i\right]\right| \leqslant \epsilon'\right\}$ *where* $\epsilon' > 0$ *and* $0 < \epsilon \leqslant \frac{1}{e(dim(\mathcal{G}(\rho))-1)}$. *Then*

$$\min_{\rho\in\mathcal{S}} f(\rho) \geqslant \beta_{\epsilon\epsilon'}(\rho) - \zeta_\epsilon, \tag{3.18}$$

where $\zeta_\epsilon := 2\epsilon(dim(\mathcal{G}(\rho)) - 1)\log\left(\frac{dim(\mathcal{G}(\rho))}{\epsilon(dim(\mathcal{G}(\rho))-1)}\right)$ *and*

$$\beta_{\epsilon,\epsilon'}(\sigma) := f_\epsilon(\sigma) - Tr\left[\sigma^\top \nabla f_\epsilon(\sigma)\right] + \max\left(\vec{y}, \vec{z} \in \tilde{\mathcal{S}}_\epsilon^*(\rho)\left(\vec{\tilde{\gamma}} \cdot \vec{y} - \epsilon' \sum_{i=1}^{|I|}\right)\right. . \tag{3.19}$$

The set $\tilde{\mathcal{S}}_\epsilon^*(\sigma)$ *is given by*

$$\tilde{\mathcal{S}}_\epsilon^*(\rho) := \left\{(\vec{y}, \vec{z}) \in (\mathbb{R}^{|I|}, \mathbb{R}^{|I|}) \ \middle|\ -\vec{z} \leqslant \vec{y} \leqslant \vec{z},\ \sum_{i=1}^{|I|} y_i\tilde{\Gamma}_i^\top \leqslant \nabla f_\epsilon(\sigma)\right\}. \tag{3.20}$$

A rigorous proof of that statement can be found in [55].

4. Formulation of the relevant optimisation problem

After summarising the security proof approach in the previous chapter, we have to find the relevant optimisation problem for the examined protocols. First, we discuss the physical model of the preparation process and the model for the quantum channel connecting Alice and Bob, followed by a discussion of Bob's measurements.

4.1. Physical model

We begin by explaining the physical model of the secret key generation process and the model for the quantum channel. This section follows [29]. Readers can refer to it for details.

4.1.1. Model of the preparation and measurement process

According to the protocol descriptions in Chapter 2, Alice prepares some quantum state and sends it to Bob, who performs measurements. Hence, we deal with prepare-and-measure schemes. Thanks to the source-replacement-scheme [12], this can be translated into an entanglement-based scheme, where Alice creates some entangled state, keeping one share while sending the share to Bob. This translation between the two schemes can be done in both directions, so that we may choose the description which is more comfortable to us in certain stages of the mathematical treatment. In the present case, the mathematical analysis in the entanglement-based schemes is more advantageous. So, Alice prepares one out of N_{St} states $|\phi_x\rangle$, where N_{St} is either 4 or 8 (depending on the protocol), with probability p_x, where $x \in \{0, 1, ..., N_{\mathrm{St}} - 1\}$. According to the protocols we examine in this thesis, $|\phi_x\rangle = |\alpha e^{i\phi_x}\rangle$ is one out of four or eight coherent states. Thus, Alice prepares the following bipartite state

$$|\Psi\rangle_{AA'} := \sum_{x=0}^{N_{\mathrm{St}}-1} \sqrt{p_x}\, |x\rangle_A \, |\phi_x\rangle_{A'} \,. \tag{4.1}$$

Here A denotes a register corresponding to Alice's system, while A' denotes Alice's output register. Furthermore, by B we denote Bob's quantum register. Alice keeps the classical state $|x\rangle$ and sends $|\phi_x\rangle_{A'}$ to Bob via the quantum channel, modelled by a completely positive, trace-preserving map $\mathcal{E}_{A'\to B}$. Then, Alice's and Bob's common state is given by the following density operator,

$$\rho_{AB} = (\mathbb{1}_A \otimes \mathcal{E}_{A'\to B}) \left(|\Psi\rangle\langle\Psi|_{AA'} \right). \tag{4.2}$$

Next, Alice performs a measurement, described by a positive operator valued measure (POVM), $M_A = \{|x\rangle\langle x|, x \in \{0, 1, ..., N_{\mathrm{St}} - 1\}\}$ to assign the state she sends to Bob. Thus, depending on Alice's measurement, Bob receives the state

$$\rho_B^x = \frac{1}{p_x} \mathrm{Tr}_A \left[\rho_{AB} \left(|x\rangle\langle x|_A \otimes \mathbb{1}_B \right) \right]. \tag{4.3}$$

Finally, Bob does his measurements on register B.

4.1.2. Channel model

We model the quantum channel connecting Alice and Bob as phase-invariant Gaussian channel with transmittance η_t and excess noise ξ, where the excess noise is defined by $\xi := \frac{(\Delta q_{obs})^2}{(\Delta q_{vac})^2} - 1$ with q_{vac} and q_{obs} being the q quadrature of the vacuum state and the measured quadrature for the signal state, respectively. The same can be formulated using the p-quadrature, as we assume q and p having the same variance in the present protocols. A short calculation yields for coherent states $(\Delta q)^2 = \langle \hat{q}^2 \rangle - \langle \hat{q} \rangle^2 = \frac{1}{2}$.

This model states that if Alice prepares a coherent state $|\alpha\rangle$ that passes a quantum channel, Bob receives a displaced thermal state centered at $\sqrt{\eta_t}\alpha$ with variance $\frac{1}{2}(1+\xi)$ for each quadrature. By ξ, we refer to the excess noise when Alice measures $(\Delta q_{obs})^2$ at A', and we denote it by δ when Bob measures $(\Delta q_{obs})^2 \in \{0, 1, 2, 3\}$. In the whole thesis we measure the noise in shot-noise units (see, for example [25] for comparison of different units).

4.2. The ideal, untrusted detector scenario

First, we are going to assume that Bob can perform ideal heterodyne detection, i.e., measurement of the q and p quadratures of the coherent state without any losses.

4.2.1. Objective function for the ideal, untrusted detector scenario

Following the postprocessing framework of [29], the objective function f is given in terms of the quantum relative entropy and two maps, $\mathcal{G}$ and $\mathcal{Z}$, which model postprocessing steps. The postprocessing map $\mathcal{G}(\sigma) := K\sigma K^\dagger$ is a quantum channel, given by its Kraus representation, where the Kraus operators read as follows

$$K := \sum_{z=0}^{N_{\mathrm{St}}-1} |z\rangle_R \otimes \mathbb{1}_A \otimes \left(\sqrt{R_z}\right)_B . \tag{4.4}$$

Recall that A and B denote Alice's and Bob's registers, respectively. Furthermore, R is some additional classical register. By $(R_z)_{z\in\{0,\ldots,N_{\mathrm{St}}-1\}}$ we denote the so-called region operators, which are determined by the POVM describing Bob's measurements and the actual key map of the chosen protocol. If E_y denotes the POVM of Bob's measurements, the region operators are given by

$$R_z := \int_{\mathcal{A}_z} E_y \, d^2y, \tag{4.5}$$

where $\mathcal{A}_z$ is the set corresponding to the symbol z in the chosen key map.

If we assume that Bob performs ideal heterodyne detection, the POVM reads $\{E_\gamma = \frac{1}{\pi} |\gamma\rangle\langle\gamma| \ : \ \gamma \in \mathbb{C}\}$ [49]. Then the measurement operators, called region operators, for the protocols introduced in Chapter 2 corresponding to the symbol $z = k$, $k \in \{0, 1, \ldots, N_{\mathrm{St}} - 1\}$ are defined by

$$R_z^{\mathrm{ra}} := \int_{A_z^{\mathrm{ra}}} E_\gamma \, d^2\gamma = \frac{1}{\pi} \int_{A_z^{\mathrm{ra}}} |\gamma\rangle\langle\gamma| \, d^2\gamma, \tag{4.6}$$

$$R_z^{\mathrm{c}} := \int_{A_z^{\mathrm{c}}} E_\gamma \, d^2\gamma = \frac{1}{\pi} \int_{A_z^{\mathrm{c}}} |\gamma\rangle\langle\gamma| \, d^2\gamma. \tag{4.7}$$

As outlined in Chapter 3, we need to approximate the infinite-dimensional Hilbert space by a problem living in a finite-dimensional Fock space. Therefore, we express the region operators in the number-basis,

$$R_z^{\mathrm{ra}} = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} \langle n|R_z^{\mathrm{ra}}|m\rangle |n\rangle\langle m|, \tag{4.8}$$

$$R_z^{\mathrm{c}} = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} \langle n|R_z^{\mathrm{c}}|m\rangle |n\rangle\langle m|, \tag{4.9}$$

and replace the upper limit of the sum by the cutoff number N_c, to approximate the infinite-dimensional region operators by their finite-dimensional counterparts.

It is shown in Appendix A.4 that the coefficients for four-state protocols for the radial&angular and the cross-shaped scheme have the form

$$\langle n|R_z^{\mathrm{ra}}|m\rangle = \begin{cases} \frac{\Gamma\left(n+1,\Delta_r^2\right)}{2\pi(n!)}\left[\frac{\pi}{2}-2\Delta_a\right] & n=m \\ \frac{\Gamma\left(\frac{m+n}{2}+1,\Delta_r^2\right)}{\pi(m-n)\sqrt{n!}\sqrt{m!}}e^{-i(m-n)\left(z+\frac{1}{2}\right)\frac{\pi}{2}}\sin\left[\left(\frac{\pi}{4}-\Delta_a\right)(m-n)\right] & n\neq m, \end{cases} \tag{4.10}$$

$$\langle n|R_z^{\mathrm{c}}|m\rangle = \begin{cases} \frac{1}{4\pi(n!)}\sum\limits_{j=0}^{n}\binom{n}{j}\Gamma\left(j+\frac{1}{2},\Delta_c^2\right)\Gamma\left(n-j+\frac{1}{2},\Delta_c^2\right) & n=m \\ \frac{\sum\limits_{j=0}^{n}\sum\limits_{k=0}^{m}\binom{n}{j}\binom{m}{k}\Gamma\left(\frac{j+k+1}{2},\Delta_c^2\right)\Gamma\left(\frac{n+m-j-k+1}{2},\Delta_c^2\right)D_{j,k,m,n}^{(z)}}{4\pi\sqrt{n!}\sqrt{m!}} & n\neq m, \end{cases} \tag{4.11}$$

where

$$D_{j,k,m,n}^{(z)} = i^{n-m+k-j}\cdot\begin{cases} 1 & z=0 \\ (-1)^{k-j} & z=1 \\ (-1)^{n-m} & z=2 \\ (-1)^{n-m+k-j} & z=3 \end{cases}. \tag{4.12}$$

These analytical expressions for the region operators were published by the author in [23]. Note that the region operators for the radial postselection scheme are included in the result for the radial&angular postselection scheme and can be obtained by setting $\Delta_a = 0$. These results are consistent with the numerical solutions of the occurring integrals with MATLAB™, version R2020a, and additionally have been cross-checked with Wolfram Mathematica™, version 11.1.1.

For the eight-state protocol, the key map for the radial&angular scheme is very similar to the four-state case, as only the angular part differs. Therefore, we obtain by using the corresponding sets A_k^{ra} for eight-state protocols and, carrying out a similar calculation

$$\langle n|R_z^{\mathrm{ra}}|m\rangle = \begin{cases} \frac{\Gamma\left(n+1,\Delta_r^2\right)}{\pi(n!)}\left[\frac{\pi}{8}-\Delta_a\right] & n=m \\ \frac{\Gamma\left(\frac{m+n}{2}+1,\Delta_r^2\right)}{\pi(m-n)\sqrt{n!}\sqrt{m!}}e^{i(m-n)z\frac{\pi}{2}}\sin\left[\left(\frac{\pi}{8}-\Delta_a\right)(m-n)\right] & n\neq m. \end{cases} \tag{4.13}$$

We note that this expression was published by the author in [24].

Furthermore, $\mathcal{Z}$, a pinching quantum channel, is given by

$$\mathcal{Z}(\sigma) := \sum_{j=0}^{N_{\mathrm{St}}-1}\left(|j\rangle\langle j|_R\otimes\mathbb{1}_{AB}\right)\sigma\left(|j\rangle\langle j|_R\otimes\mathbb{1}_{AB}\right). \tag{4.14}$$

Thus, we have specified the objective function f completely and it remains to specify the domain of optimisation.

4.2.2. Specifying the domain of optimisation for the ideal, untrusted detector scenario

In the present optimisation problem, we search for Eve's optimal attack, i.e., the density matrix with the minimal key rate, which is still compatible with some constraints. In this section, we are going to describe the constraints in more detail. First, all density matrices in the feasible set $S \subseteq \mathcal{D}(\mathcal{H})$, where $\mathcal{D}(\mathcal{H})$ denotes the set of all density matrices on the Hilbert space $\mathcal{H}$, have to be consistent with Bob's measurement results. Denote by $\hat{q} = \frac{1}{\sqrt{2}}\left(\hat{a}^\dagger + \hat{a}\right)$ and $\hat{p} = \frac{i}{\sqrt{2}}\left(\hat{a}^\dagger + \hat{a}\right)$ the quadrature operators and define $\hat{n} := \frac{1}{2}\left(\hat{q}^2 + \hat{p}^2 - 1\right)$ and $\hat{d} := \hat{q}^2 - \hat{p}^2$. Note that $\hat{n}$ is the number operator, satisfying $\hat{n}\,|n\rangle = n\,|n\rangle$. Alternatively, one can use the second-moment observables directly, as $\hat{n}$ and $\hat{d}$ are just linear combinations of the second-moment operators $\hat{q}^2$ and $\hat{p}^2$.

We obtain expectation values of the first two moments of the quadrature operators by Bob's measurements. Thus, we know the mean photon number and the expectation value of the operator $\hat{d}$. Hence, we find the following set of constraints due to Bob's measurement results,

$$\begin{aligned}
\mathrm{Tr}\left[\rho_{AB}\left(|x\rangle\langle x|_A \otimes \hat{q}_B\right)\right] &= p_x\langle\hat{q}\rangle_x, \\
\mathrm{Tr}\left[\rho_{AB}\left(|x\rangle\langle x|_A \otimes \hat{p}_B\right)\right] &= p_x\langle\hat{p}\rangle_x, \\
\mathrm{Tr}\left[\rho_{AB}\left(|x\rangle\langle x|_A \otimes \hat{n}_B\right)\right] &= p_x\langle\hat{n}\rangle_x, \\
\mathrm{Tr}\left[\rho_{AB}\left(|x\rangle\langle x|_A \otimes \hat{d}_B\right)\right] &= p_x\langle\hat{d}\rangle_x,
\end{aligned}$$

where $x \in \{0, 1, ..., N_{\mathrm{St}} - 1\}$, which makes up a total of 16 constraints for four-state protocols and a total of 32 constraints for eight-state protocols. By $\langle\hat{q}\rangle_x, \langle\hat{p}\rangle_x, \langle\hat{n}\rangle_x$ and $\langle\hat{d}\rangle_x$, we denote the expectation values of the corresponding operators for the conditional state ρ_B^x. Using the channel model (see Section 4.1.2), one obtains

$$\langle\hat{q}\rangle_x = \sqrt{2\eta_t}\,\Re(\alpha_x), \tag{4.15}$$

$$\langle\hat{p}\rangle_x = \sqrt{2\eta_t}\,\Im(\alpha_x), \tag{4.16}$$

$$\langle\hat{n}\rangle_x = \eta|\alpha_x|^2 + \frac{\eta_t\xi}{2}, \tag{4.17}$$

$$\langle\hat{d}\rangle_x = \eta\left(\alpha_x^2 + (\alpha_x^*)^2\right), \tag{4.18}$$

as shown in Appendix A.8.1

Second, Eve cannot modify Alice's system A, since Eve has access to the quantum channel, but not to Alice's lab. Therefore, her attack maps A' to B, leaving Alice's register A unchanged. Consequently, following [55], we add the constraint

$$\rho_A = \mathrm{Tr}_B\left[\rho_{AB}\right]. \tag{4.19}$$

By using the bipartite state given in (4.1), we calculate $\rho_A = \mathrm{Tr}_{A'}\left[\rho_{AB}\right]$ (as the quantum channel, which maps from A' to B is a trace-preserving map we may trace over A' instead of B) and find

$$\rho_A = \sum_{x,y=0}^{N_{\mathrm{St}}-1} \sqrt{p_x p_y} \left\langle \phi_y | \phi_x \right\rangle |x\rangle\langle y|_A \,. \tag{4.20}$$

This constraint is still matrix-valued, and we need to transform this constraint into a set of scalar-valued constraints to proceed. This is done by a technique called state-tomography. Here, we choose a basis out of measurement operators for Alice's system to convert the matrix-valued constraint into a set of 16 (for four-state protocols) or 64 (for eight-state protocols) scalar valued constraints. For the sake of consistency, the corresponding considerations can be found in the appendix, Chapter A.7, where we transform this matrix-valued constraint into a set of 16 (for four-state protocols) or 64 (for eight-state protocols) scalar-valued constraints. This leaves us back with a total of $M = 32$ (for four-state protocols) or $M = 96$ (for eight-state protocols) constraints of the form $\mathrm{Tr}\left[\rho_{AB}\Gamma_i\right] = \gamma_i$.

Finally, we have to take into account that ρ_{AB} is a density operator, hence being positive semi-definite, Hermitian, and having trace equal to one. It is well known that positive semi-definiteness implies hermiticity, so we do not need to take the latter into account separately. The condition for positive semi-definiteness was already considered earlier by requiring that the feasible set has to be a subset of the set of all density operators. Making this requirement explicit, we have $\rho_{AB} \geqslant 0$. In contrast to [29], we do not require the trace equal to one condition explicitly. This is because we 'disassembled' the matrix-valued constraint into a set of scalar-valued constraints, using state tomography. It turns out that together with the constraints from Bob's measurements, this set is sufficient to linear-combine the trace-equal-to-one constraint with satisfying numerical accuracy. As for numerical reasons, it is beneficial to avoid almost linearly-dependent conditions in the problem-formulation, we chose to omit this condition.

Summing up, we face the following optimisation problem

$$\text{minimise } D\left(\mathcal{G}(\rho_{AB}) || \mathcal{Z}(\mathcal{G}(\rho_{AB}))\right) \tag{4.21}$$

subject to:

$$\begin{aligned}
&\mathrm{Tr}\left[\rho_{AB}\left(|x\rangle\langle x|_A \otimes \hat{q}_B\right)\right] = p_x\sqrt{2\eta_t}\;\Re(\alpha_x),\\
&\mathrm{Tr}\left[\rho_{AB}\left(|x\rangle\langle x|_A \otimes \hat{p}_B\right)\right] = p_x\sqrt{2\eta_t}\;\Im(\alpha_x),\\
&\mathrm{Tr}\left[\rho_{AB}\left(|x\rangle\langle x|_A \otimes \hat{n}_B\right)\right] = p_x\left(\eta_t|\alpha_x|^2 + \frac{\eta_t\xi}{2}\right),\\
&\mathrm{Tr}\left[\rho_{AB}\left(|x\rangle\langle x|_A \otimes \hat{d}_B\right)\right] = p_x\eta_t\left(\alpha_x^2 + (\alpha_x^*)^2\right),\\
&\mathrm{Tr}_B\left[\rho_{AB}\right] = \sum_{i,j=0}^{N_{\mathrm{St}}-1}\sqrt{p_i p_j}\,\langle\phi_j|\phi_i\rangle\,|i\rangle\langle j|_A\,,\\
&\rho_{AB} \geqslant 0.
\end{aligned}$$

Therefore, the feasible set reads

$$\mathcal{S} := \{\rho \geqslant 0 \mid \mathrm{Tr}\left[\rho\Gamma_i\right] = \gamma_i \ \forall i \in \{1,2,...,M\}\} \subseteq \mathcal{D}(\mathcal{H}_{AB}), \tag{4.22}$$

where Γ_i and γ_i are given by the constraints above.

4.3. Trusted detector approach

Up to now, we assumed that Bob performs his measurements using ideal homodyne detectors, which is not true in a realistic setting. So, the secret key rates we obtained when we solve the semi-definite program (4.21) are too optimistic for experimental realisations. On the other hand, in the previous model, we considered the excess noise ξ but no noise due to the detector. Typically, experimentalists who want to include the detector noise in their considerations add this noise to the channel noise and take secret key rates calculated with ξ equal to the sum of those noises. This is quite pessimistic, as this scenario dedicates all noise to Eve. One may assume that Eve has no access to Bob's lab, hence cannot take advantage of the electronic noise in his detectors. In other words, the detector is assumed to be trusted. In [28] the present numerical security proof framework is extended to the trusted detector scenario. In what follows, we summarise the changes and adaptations that are necessary to include the trusted detector, following [28].

A heterodyne detector consists out of two homodyne detectors and a 50:50 beam splitter that divides the incoming light into two equal parts, where each of these beams is led to one of the homodyne detectors. Let each of the realistic homodyne detectors have detector efficiencies η_1, $\eta_2 \leqslant 1$ and electronic noise levels of ν_1 and ν_2, where we measure the electronic noise in shot noise units, just as the excess noise. The quantum optical model for realistic heterodyne detectors by Lodewyck

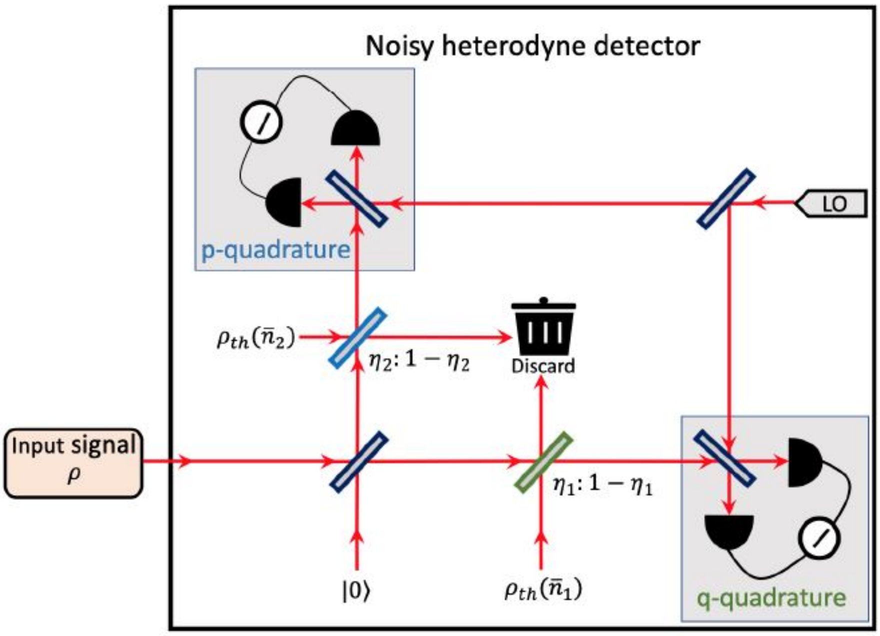


Figure 4.1.: Sketch for the physical model of an imperfect, noisy heterodyne detector. The figure was taken from [28].

[31] includes this quantities by adding two additional beam splitters with transmissions of η_1 and η_2 (hence, reflectances of $1-\eta_1$ and $1-\eta_2$), one for each homodyne detector, where the signals are mixed with a thermal state. The thermal states have mean photon numbers of $\bar{n}_j = \frac{\nu_j}{2(1-\eta_j)}$, $j \in \{1,2\}$ which, after being mixed with the signal state, models the effect of electronic noise due to the detector. Then, ideal homodyne detectors are used to measure the q and p quadrature. A sketch for this model can be found in Figure 4.1.

One has to find the POVM $\{G_y \ : \ y \in \mathbb{C}\}$ corresponding to this noisy heterodyne detector. We know that for every measurement outcome $y \in \mathbb{C}$ the POVM can be used to express the probability for that particular outcome, $P(y) = \mathrm{Tr}\,[\rho G_y]$. Alternatively, one can obtain the same probability using Wigner functions [27]

$$P(y) = \pi \int W_\rho(\gamma) W_{G_y}(\gamma)\, d^2\gamma, \tag{4.23}$$

where $W_\rho(\gamma)$ is the Wigner function of the signal state and $W_{G_y}(\gamma)$ is the Wigner function of the operator G_y, respectively. Knowing the Wigner functions of the vacuum state [27]

$$W_{|0\rangle}(\gamma) = \frac{2}{\pi} e^{-2|\gamma|^2}, \tag{4.24}$$

the displaced thermal state [27]

$$W_{\hat{D}(\alpha)\rho_{th}(\bar{n})\hat{D}^{\dagger}(\alpha)}(\gamma) = \frac{2}{\pi}\frac{1}{1+2\bar{n}}e^{-\frac{2|\gamma-\alpha|^2}{1+2\bar{n}}}, \tag{4.25}$$

the homodyne q and p quadrature measurements [28]

$$W_{H_{\Re(y)}}(\gamma) = \delta\left(\Re(\alpha) - \frac{\Re(y)}{\sqrt{2}}\right), \tag{4.26}$$

$$W_{H_{\Im(y)}}(\gamma) = \delta\left(\Im(\alpha) - \frac{\Im(y)}{\sqrt{2}}\right), \tag{4.27}$$

and the transformation rule for Wigner functions under a beam splitter transformation [27]

$$W_{\text{out}}(\beta,\gamma) = W_{\text{in}}\left(\sqrt{\eta}\beta + \sqrt{1-\eta}\gamma, \sqrt{1-\eta}\beta - \sqrt{\eta}\gamma\right), \tag{4.28}$$

one can calculate the probability $P(y)$ as follows. Let us call the state which is measured by the ideal detectors, i.e., after passing the beam splitter network, ρ_{end} and the corresponding Wigner function W_{end}. This state is unknown, but we know the Wigner functions of the homodyne measurements and the Wigner functions of the states that are mixed by the beam splitter network. Therefore, we start with the generalised overlap formula for $P(y)$ and perform inverse beam splitter transformations,

$$P(y) = \pi^4 \int d^2\alpha \int d^2\beta \int d^2\gamma \int d^2\omega \; W_{\text{end}}(\alpha,\beta,\gamma,\omega)\frac{1}{\pi^2}W_{H_{\Re(y)}}(\alpha)W_{H_{\Im(y)}}(\beta).$$

Considering the action of the beam splitter network yields

$$\begin{aligned} P(y) = \pi^2 \int d^2\alpha \; W_{\rho}(\alpha) \int d^2\beta \; W_{|0\rangle}(\beta) & \\ \times \int d^2\gamma \; W_{\rho_{th}(\bar{n}_1)}(\gamma) W_{H_{\Re(y)}} & \left(\sqrt{\eta_1}\frac{\alpha+\beta}{\sqrt{2}} + \sqrt{1-\eta_1}\gamma\right) \\ \times \int d^2\omega \; W_{\rho_{th}(\bar{n}_2)}(\omega) W_{H_{\Im(y)}} & \left(\sqrt{\eta_2}\frac{\alpha-\beta}{\sqrt{2}} - \sqrt{1-\eta_2}\omega\right). \end{aligned}$$

Integration over all variables except α and rearranging the expressions leaves us back with the Wigner function of ρ and some remaining Wigner function, which, using $P(y) = \text{Tr}\left[\rho G_y\right] = \int d^2\alpha W_\rho W_{G_y}(\alpha)$, can be identified as $W_{G_y}(\alpha)$,

$$W_{G_y}(\alpha) = \frac{2}{\sqrt{\eta_1\eta_2}\pi^2}\frac{e^{\frac{-2\left(\frac{\Re(y)}{\sqrt{\eta_1}}-\Re(\alpha)\right)^2}{1+\frac{2(1-\eta_1)(1+2\bar{n}_1)}{\eta_1}}+\frac{-2\left(\frac{\Im(y)}{\sqrt{\eta_2}}-\Im(\alpha)\right)^2}{1+\frac{2(1-\eta_2)(1+2\bar{n}_2)}{\eta_2}}}}{\sqrt{1+\frac{2(1-\eta_1)(1+2\bar{n}_1)}{\eta_1}}\sqrt{1+\frac{2(1-\eta_2)(1+2\bar{n}_2)}{\eta_2}}}. \tag{4.29}$$

Inserting $\bar{n}_j = \frac{\nu_j}{2(1-\eta_j)}$, $j \in \{1, 2\}$ and simplifying leads to

$$W_{G_y}(\alpha) = \frac{2}{\sqrt{\eta_1\eta_2}\pi^2} \frac{e^{\frac{-2\left(\Re(\alpha) - \frac{\Re(y)}{\sqrt{\eta_1}}\right)^2}{1+\frac{2(1-\eta_1+\nu_1)}{\eta_1}}}}{\sqrt{1 + \frac{2(1-\eta_1+\nu_1))}{\eta_1}}} \frac{e^{\frac{-2\left(\Im(\alpha) - \frac{\Im(y)}{\sqrt{\eta_2}}\right)^2}{1+\frac{2(1-\eta_2+\nu_2)}{\eta_2}}}}{\sqrt{1 + \frac{2(1-\eta_2+\nu_2)}{\eta_2}}}. \tag{4.30}$$

In what follows, we assume $\eta_d := \eta_1 = \eta_2$ and $\nu_{el} = \nu_1 = \nu_2$ to simplify the calculations. Although we cannot expect to hold two identical detectors, we can choose η_d to be the minimum of η_1 and η_2 and ν_{el} to be the maximum of ν_1 and ν_2. Then, the secret key rate we obtain with these parameters is a lower bound for the real system. Consequently, we obtain the following simplified Wigner function

$$W_{G_y}(\alpha) = \frac{2}{\eta_d\pi^2} \frac{e^{\frac{-2\left|\alpha - \frac{y}{\sqrt{\eta_d}}\right|^2}{1+\frac{2(1-\eta_d+\nu_{el})}{\eta_d}}}}{1 + \frac{2(1-\eta_d+\nu_{el})}{\eta_d}}. \tag{4.31}$$

This is, up to a prefactor, the Wigner function of a displaced thermal state. So, correcting this prefactor, we finally obtain

$$G_y = \frac{1}{\eta_d\pi} \hat{D}\left(\frac{y}{\sqrt{\eta_d}}\right) \rho_{th}\left(\frac{1-\eta_d+\nu_{el}}{\eta_d}\right) \hat{D}^\dagger\left(\frac{y}{\sqrt{\eta_d}}\right). \tag{4.32}$$

4.3.1. Objective function for the non-ideal, trusted detector scenario

Similarly to the ideal, untrusted detector, we need to specify the maps $\mathcal{G}$ and $\mathcal{Z}$ to find the objective function of the key rate finding problem. While $\mathcal{Z}$ does not change, as the classical steps described by that map remain unchanged, the map $\mathcal{G} = K\sigma K^\dagger$ changes, as the corresponding Kraus operator K depends on the region operators R_z (see equation 4.4),

$$K := \sum_{z=0}^{N_{\mathrm{St}}-1} |z\rangle_R \otimes \mathbb{1}_A \otimes \left(\sqrt{R_z}\right)_B.$$

Recall that A and B denote Alice's and Bob's registers and that R is some additional classical register. These region operators $(R_z)_{z\in\{0,1,\ldots,N_{\mathrm{St}}-1\}}$ are given in terms of the POVM describing Bob's measurements, which changed, compared to the ideal heterodyne detector and depend on the key map of the chosen protocol (see equation 4.5),

$$R_z := \int_{\mathcal{A}_z} E_y \, d^2y,$$

where $\mathcal{A}_z$ is the set corresponding to the symbol z in the chosen key map. Therefore, we insert the POVM $\{G_y \ : \ y \in \mathbb{C}\}$, describing the non-ideal, trusted detector, derived in the previous section and obtain

$$R_z^{\text{ra, tr}} := \int_{A_z^{\text{ra}}} G_\gamma \, d^2\gamma, \tag{4.33}$$

$$R_z^{\text{c, tr}} := \int_{A_z^{\text{c}}} G_\gamma \, d^2\gamma. \tag{4.34}$$

As outlined in Chapter 3, we need to approximate the infinite-dimensional Hilbert space by a problem living in a finite-dimensional Fock space. Therefore, we express the region operators in the number-basis,

$$R_z^{\text{ra, tr}} = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} \langle n | R_z^{\text{ra, tr}} | m \rangle |n\rangle\langle m|, \tag{4.35}$$

$$R_z^{\text{c, tr}} = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} \langle n | R_z^{\text{c, tr}} | m \rangle |n\rangle\langle m|. \tag{4.36}$$

For numerical treatment, we replace the upper limit of the sum by the cutoff number N_c, hence approximate the infinite-dimensional region operators by their finite-dimensional counterparts. It is shown in Appendix A.5 that the coefficients for the radial&angular and the cross-shaped scheme have the form

$$\langle n | R_z^{\text{ra, tr}} | m \rangle =$$
$$\begin{cases} C_{n,n} \left[\frac{\pi}{4} - \Delta_a\right] \sum\limits_{j=0}^{n} \binom{n}{n-j} \frac{\Gamma(j+1, a\Delta_r^2)}{a^{j+1} b^j j!} & n = m \\ \frac{C_{n,m}}{(m-n) a^{\frac{m-n}{2}}} e^{-i(m-n)\left(z+\frac{1}{2}\right)\frac{\pi}{2}} \sin\left[(m-n)\left(\frac{\pi}{4} - \Delta_a\right)\right] \sum\limits_{j=0}^{n} \binom{m}{n-j} \frac{\Gamma\left(j+1+\frac{m-n}{2}, a\Delta_r^2\right)}{a^{j+1} b^j j!} & n < m \\ \overline{\langle m | R_z^{\text{ra, tr}} | n \rangle} & n > m \end{cases} \tag{4.37}$$

$$\langle n | R_z^{\text{c, tr}} | m \rangle =$$
$$\begin{cases} C_{n,n} \sum\limits_{j=0}^{n} \frac{\binom{n}{n-j}}{a^{j+1} b^j j!} \sum\limits_{k=0}^{j} \binom{j}{k} \Gamma\left(k + \frac{1}{2}, a\Delta_c^2\right) \Gamma\left(j - k + \frac{1}{2}, a\Delta_c^2\right) & n = m \\ \frac{C_{n,m}}{4a^{\frac{m-n}{2}}} \sum\limits_{j=0}^{n} \frac{\binom{m}{n-j}}{a^{j+1} b^j j!} \sum\limits_{k=0}^{m-n} \binom{m-n}{k} D_{k,m,n}^{(z)} \sum\limits_{l=0}^{j} \binom{j}{l} \Gamma\left(l + \frac{k+1}{2}, a\Delta_c^2\right) \Gamma\left(j - l + \frac{m-n-k+1}{2}, a\Delta_c^2\right) & n < m \\ \overline{\langle m | R_z^{\text{c, tr}} | n \rangle} & n > m \end{cases} \tag{4.38}$$

where $C_{n,m} := \frac{1}{\pi\eta_d^{\frac{m-n}{2}+1}}\sqrt{\frac{n!}{m!}}\frac{\overline{n}_d^n}{(1+\overline{n}_d)^{m+1}}$, $a := \frac{1}{\eta_d(1+\overline{n}_d)}$ and $b := \eta_d\overline{n}_d(1+\overline{n}_d)$ and

$$D_{k,m,n}^{(z)} = i^{m-n-k} \cdot \begin{cases} (-1)^{m-n-k} & z=0 \\ (-1)^{m-n} & z=1 \\ (-1)^k & z=2 \\ 1 & z=3 \end{cases} . \tag{4.39}$$

These analytical expressions for the region operators were published by the author in [23]. Furthermore, we note that [28] derives an expression for the case with only radial postselection, relying on Taylor series expansion. In contrast, our result for the radial&angular-case is more general, as it additionally includes angular postselection and since our result does not require Taylor series coefficients. To the best of our knowledge, our result for the cross-shaped postselection scheme is novel. Both results have been validated with numerical solutions of the occurring integrals with MATLAB™, version R2020a and the analytical derivations have been cross-checked with Wolfram Mathematica™, version 11.1.1.

Thus, the objective function f of the key rate finding problem for the non-ideal, trusted detector was specified completely.

4.3.2. Specifying the domain of optimisation for the non-ideal, trusted detector scenario

It remains to specify the domain of optimisation for the non-ideal, trusted detector scenario, hence the explicit form of the constraints due to Bob's measurements. In contrast to the ideal, untrusted detector case, we do not define operators $\hat{n}$ and $\hat{d}$, but utilise the second-moment observables directly. To distinguish the operators for the trusted detector scenario from those for the untrusted detector, we follow the notation from [28] and call the first-moment observables $\hat{F}_Q$ and $\hat{F}_P$ and the second-moment observables $\hat{S}_Q$ and $\hat{S}_P$. They are defined as

$$\hat{F}_Q = \int \frac{y^* + y}{\sqrt{2}} G_y \, d^2y, \tag{4.40}$$

$$\hat{F}_P = \int i\frac{y^* - y}{\sqrt{2}} G_y \, d^2y, \tag{4.41}$$

$$\hat{S}_Q = \int \left(\frac{y^* + y}{\sqrt{2}}\right)^2 G_y \, d^2y, \tag{4.42}$$

$$\hat{S}_P = \int \left(i\frac{y^* - y}{\sqrt{2}}\right)^2 G_y \, d^2y. \tag{4.43}$$

While the representation of the operators for the ideal, untrusted case in the number basis was straightforward, now we have to derive expressions for the first- and second-moment operators for the non-ideal trusted in the number basis,

$$\hat{F}_Q = \sum_{n=0}^{\infty}\sum_{m=0}^{\infty} \langle n|\hat{F}_Q|m\rangle \;|n\rangle\langle m| \tag{4.44}$$

$$\hat{F}_P = \sum_{n=0}^{\infty}\sum_{m=0}^{\infty} \langle n|\hat{F}_P|m\rangle \;|n\rangle\langle m| \tag{4.45}$$

$$\hat{S}_Q = \sum_{n=0}^{\infty}\sum_{m=0}^{\infty} \langle n|\hat{S}_Q|m\rangle \;|n\rangle\langle m| \tag{4.46}$$

$$\hat{S}_P = \sum_{n=0}^{\infty}\sum_{m=0}^{\infty} \langle n|\hat{S}_P|m\rangle \;|n\rangle\langle m|\,. \tag{4.47}$$

The matrix elements with respect to the Fock basis are derived in Appendix A.6 and read

$$\langle n|\hat{F}_P|n+1\rangle = i\frac{\pi C_{n,n+1}}{\sqrt{2}} \sum_{j=0}^{n} \binom{n+1}{n-j} \frac{j+1}{a^{j+2}b^j} = i\langle n|\hat{F}_Q|n+1\rangle, \tag{4.48}$$

and $\langle n|\hat{F}_Q|m\rangle = 0 = \langle n|\hat{F}_P|m\rangle$ if $m \neq n \pm 1$. Furthermore

$$\langle n|\hat{S}_Q|n\rangle = -\langle n|\hat{S}_P|n\rangle = \pi C_{n,n} \sum_{j=0}^{n} \binom{n}{n-j} \frac{j+1}{a^{j+2}b^j}, \tag{4.49}$$

$$\langle n|\hat{S}_Q|n+2\rangle = -\langle n|\hat{S}_P|n+2\rangle = \pi C_{n,n+2} \sum_{j=0}^{n} \binom{n+2}{n-j} \frac{(j+2)(j+1)}{a^{j+3}b^j}, \tag{4.50}$$

and $\langle n|\hat{S}_Q|m\rangle = \langle n|\hat{S}_P|m\rangle = 0$ otherwise. Note that these operators are Hermitian, hence we only give elements with $n \leqslant m$, as one obtains the missing elements by complex conjugation. These analytical expressions for the first- and second-moment observables were published by the author in [23]. Furthermore, we note that [28] derives alternative expressions relying on Taylor series coefficients.

The expectation values of these operators are derived in Appendix A.8.2 and read

$$\langle \hat{F}_Q\rangle_x = \sqrt{2\eta_d\eta}\;\Re(\alpha_x), \tag{4.51}$$

$$\langle \hat{F}_P\rangle_x = \sqrt{2\eta_d\eta}\;\Im(\alpha_x), \tag{4.52}$$

$$\langle \hat{S}_Q\rangle_x = 2\eta_d\eta\left(\Re(\alpha_x)\right)^2 + 1 + \frac{1}{2}\eta_d\eta\xi + \nu_{el}, \tag{4.53}$$

$$\langle \hat{S}_P\rangle_x = 2\eta_d\eta\left(\Im(\alpha_x)\right)^2 + 1 + \frac{1}{2}\eta_d\eta\xi + \nu_{el}. \tag{4.54}$$

These expressions coincide with the expectation values given in [28].

The Matrix-valued constraint, obtained by tracing out Bob's system, is the same as in the ideal, trusted detector scenario and can be disassembled into a set of scalar valued constraints as described in Appendix A.7.

Summing up, we face the following optimisation problem

$$\text{minimise } D\left(\mathcal{G}(\rho_{AB})||\mathcal{Z}(\mathcal{G}(\rho_{AB}))\right) \tag{4.55}$$

subject to:

$$\begin{aligned}
&\mathrm{Tr}\left[\rho_{AB}\left(|x\rangle\langle x|_A \otimes \left(\hat{F}_Q\right)_B\right)\right] = p_x\sqrt{2\eta_d\eta}\ \Re(\alpha_x),\\
&\mathrm{Tr}\left[\rho_{AB}\left(|x\rangle\langle x|_A \otimes \left(\hat{F}_P\right)_B\right)\right] = p_x\sqrt{2\eta_d\eta}\ \Im(\alpha_x),\\
&\mathrm{Tr}\left[\rho_{AB}\left(|x\rangle\langle x|_A \otimes \left(\hat{S}_Q\right)_B\right)\right] = p_x\left(2\eta_d\eta\left(\Re(\alpha_x)\right)^2 + 1 + \frac{1}{2}\eta_d\eta\xi + \nu_{el}\right),\\
&\mathrm{Tr}\left[\rho_{AB}\left(|x\rangle\langle x|_A \otimes \left(\hat{S}_P\right)_B\right)\right] = p_x\left(2\eta_d\eta\left(\Im(\alpha_x)\right)^2 + 1 + \frac{1}{2}\eta_d\eta\xi + \nu_{el}\right),\\
&\mathrm{Tr}_B\left[\rho_{AB}\right] = \sum_{i,j=0}^{N_{\mathrm{St}}-1}\sqrt{p_ip_j}\,\langle\phi_j|\phi_i\rangle\,|i\rangle\langle j|_A\\
&\rho_{AB} \geqslant 0.
\end{aligned}$$

4.4. Error correction and postprocessing

It remains to find expressions for the terms δ_{EC} and p_{pass}, which are related to the error correction and postprocessing phases. By construction, the probability that Bob obtains the symbol $z = k$ conditioned that Alice has prepared the state $x = l$ is obtained by building the trace of the product of the region operator associated with the symbol k and the density matrix of the state Bob receives if Alice sends the state associated with the symbol l,

$$P(z = k|x = l) = \mathrm{Tr}\left[\rho_b^l R_k\right]. \tag{4.56}$$

Hereby, Bob's state is given by

$$\rho_B^l = \frac{1}{p_l}\mathrm{Tr}_A\left[\rho_{AB}\left(|l\rangle\langle l| \otimes \mathbb{1}_B\right)\right], \tag{4.57}$$

where $(p_l)_{l\in\{0,1,\dots,N_{\mathrm{St}}-1\}}$ is the probability that Alice prepares the state l. This probability can be used to calculate the probability that a signal passes the post-selection phase,

$$p_{\mathrm{pass}} = \sum_{l=0}^{N_{\mathrm{St}}-1} \sum_{k=0}^{N_{\mathrm{St}}-1} p_l P(z = k|x = l). \tag{4.58}$$

Furthermore, we need to find an expression for the information leakage per signal, δ_{EC}. In what follows, we denote the reconciliation efficiency by β and consider reverse reconciliation. In that case, Bob sends additional information to Alice such that she can guess Bob's values. The information flow goes in the opposite direction than the quantum signals which explains the naming of reverse reconciliation. For error correction at the Slepian-Wolfe limit [44], we have

$$\delta_{EC} = H(\mathbf{Z}|\mathbf{X}) = H(\mathbf{Z}) - I(\mathbf{X} : \mathbf{Z}), \tag{4.59}$$

where $H(\mathbf{Z})$ is the von Neumann entropy of the string $\mathbf{Z}$, $H(\mathbf{Z}|\mathbf{X})$ is the conditioned von Neumann entropy, and $I(\mathbf{Z}; \mathbf{X})$ denotes the mutual information between the bit-strings $\mathbf{Z}$ and $\mathbf{X}$. As we cannot assume to perform error correction exactly at the Slepian-Wolfe limit, but with reconciliation efficiency β, we replace the mutual information between the bit-strings $\mathbf{Z}$ and $\mathbf{X}$ by $\beta I(\mathbf{X} : \mathbf{Z})$ and express the mutual information in terms of entropies

$$I(\mathbf{X} : \mathbf{Z}) = H(\mathbf{X}) + H(\mathbf{Z}) - H(\mathbf{X}, \mathbf{Z}) = H(\mathbf{Z}) - H(\mathbf{Z}|\mathbf{X}). \tag{4.60}$$

Then, we obtain

$$\delta_{EC} = (1 - \beta)H(\mathbf{Z}) + \beta H(\mathbf{Z}|\mathbf{X}). \tag{4.61}$$

These entropies can be calculated using the probabilities from equation (4.56) and the law of total probability.

5. Implementation

In the previous sections, we described the numerical security proof method and formulated the present key rate finding problem by specifying the objective function and the domain of optimisation depending on the chosen protocol both for the trusted and untrusted detector scenario. In this section, we explain important details of the remaining steps and the implementation in more detail.

5.1. Calculation of a feasible starting value

We discuss two different approaches to find feasible starting values for the Frank-Wolfe algorithm, which is a prerequisite to obtain reasonable solutions. The first approach simulates the quantum channel connecting Alice and Bob to find a feasible starting value, while the second one solves a semi-definite program.

5.1.1. Using a channel model

In Section 4.1.2, we agreed to model the quantum channel as Gaussian channel, which is a standard model to describe the noisy evolution of quantum states. According to [20], Gaussian channels map Gaussian states to Gaussian states and are determined by their action on the first and second statistical moments. Let us denote by $\hat{x} := (\hat{q}, \hat{p})^\top$, by $\bar{x} := \langle \hat{x} \rangle$ the mean value of the q- and p-quadrature of a Gaussian state, and by V is the covariance matrix $V_{ij} := \frac{1}{2} \langle \{ \hat{x}_i - \langle x_i \rangle, \hat{x}_j - \langle \hat{x}_j \rangle \} \rangle$ of a Gaussian state, where $\{.,.\}$ is the anti-commutator. Then, following [53], an arbitrary Gaussian channel maps the Gaussian state $\rho(\bar{x}, V)$ to another Gaussian state with mean $T\bar{x} + d$ and covariance matrix $TVT^\top + N$, where $d \in \mathbb{R}^2$ is some displacement vector and $N, T \in \mathbb{R}^{2\times 2}$ satisfy the conditions $N = N^\top \geqslant 0$ and $\det(N) \geqslant (\det(T) - 1)^2$.

According to [53], there is an even more simple description for Gaussian loss channels. They can be described by a beam splitter transformation with transmittance η_t, where the signal is mixed with a thermal state with mean photon number $\bar{n} = \frac{1}{2}\eta_t \xi$. We use this to find a feasible starting value ρ_0 for the present optimisation problem.

Following the physical model in Section 4.1.1, Alice prepares a bipartite state $|\Psi\rangle_{AA'} := \sum_{x=0}^{N_{\mathrm{St}}-1} \sqrt{p_x}\, |x\rangle_A\, |\phi_x\rangle_{A'}$, where the share in register A' is sent to Bob via the quantum channel $\mathcal{E}_{A'\to B}$,

$$\rho_{AB} = \sum_{x,y=0}^{N_{\mathrm{St}}-1} \sqrt{p_x p_y}\, |x\rangle\langle y|^A \otimes \mathcal{E}_{A'\to B}\left(|\alpha_x\rangle\langle\alpha_y|^{A'}\right). \tag{5.1}$$

Our task now is to describe the state Bob receives, $\mathcal{E}_{A'\to B}\left(|\alpha_x\rangle\langle\alpha_y|^{A'}\right)$, in the number basis. From what was said above, we know that the quantum channel can be described by a beam splitter transformation, where we mix the state that is sent by Alice,

$$|\alpha_x\rangle\langle\alpha_y|^{A'} = \sum_{k,l=0}^{\infty} e^{-\frac{|\alpha_x|^2+|\alpha_y|^2}{2}} \frac{(\alpha_x)^k}{\sqrt{k!}} \frac{(\alpha_y^*)^l}{\sqrt{l!}}\, |k\rangle\langle l| =: \sum_{k,l=0}^{\infty} \rho_{k,l}^{A'}(x,y)\, |k\rangle\langle l| \tag{5.2}$$

with a thermal state with mean photon number $\bar{n} = \frac{1}{2}\eta_t\xi$

$$\rho^{th} = \sum_{n,m=0}^{\infty} \frac{\bar{n}^n}{(1+\bar{n})^{n+1}} \delta_{n,m}\, |m\rangle\langle n| =: \sum_{n,m=0}^{\infty} \rho_{m,n}^{th}\, |m\rangle\langle n| \tag{5.3}$$

at a beam splitter. Note that we defined $\rho_{k,l}^{A'}(x,y)$ and $\rho_{m,n}^{th}$ by the right-hand sides of the last equalities. For the following beamsplitter calculations, we denote the input ports by 1 and 2 and the output ports by $1'$ and $2'$. So, we consider the two-mode state

$$\rho^{in}(x,y) = \rho^{A'} \otimes \rho^{th} = \sum_{k,l=0}^{\infty} \sum_{m,n=0}^{\infty} \rho_{k,l}^{A'}(x,y)\rho_{m,n}^{th}\, |k,m\rangle\langle l,n|^{1,2}. \tag{5.4}$$

In the Schrödinger picture, we obtain the output of the beam splitter transformation by

$$\rho^{out}(x,y) = \hat{U}_B \rho^{in}(x,y) \hat{U}_b^\dagger = \sum_{k,l=0}^{\infty} \sum_{m,n=0}^{\infty} \rho_{k,l}^{A'}(x,y)\rho_{m,n}^{th} \hat{U}_B\, |k,m\rangle\langle l,n|^{1,2}\, \hat{U}_b^\dagger, \tag{5.5}$$

where $\hat{U}_B$ is the matrix for the beam splitter transformation.

We have

$$\begin{aligned} |k,m\rangle' := \hat{U}_B\, |k,m\rangle &= \frac{1}{\sqrt{k!}\sqrt{m!}} \hat{U}_B \left(\hat{a}_1^\dagger\right)^k \left(\hat{a}_2^\dagger\right)^m |0,0\rangle \\ &= \frac{1}{\sqrt{k!}\sqrt{m!}} \hat{U}_B \left(\hat{a}_1^\dagger\right)^k \left(\hat{a}_2^\dagger\right)^m \hat{U}_B^\dagger\, |0,0\rangle. \end{aligned}$$

For the last equality we used $\hat{U}_B^\dagger |0,0\rangle = |0,0\rangle$. Next, we express the primed creation operators, i.e., operators corresponding to the right side of the beam splitter, by the non-primed ones,

$$\begin{pmatrix} \hat{a}_1^{'} \\ \hat{a}_2^{'} \end{pmatrix} = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} \cdot \begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \end{pmatrix} \Rightarrow \begin{pmatrix} \hat{a}_1^{'\dagger} \\ \hat{a}_2^{'\dagger} \end{pmatrix} = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}^\dagger \cdot \begin{pmatrix} (\hat{a}_1)^\dagger \\ (\hat{a}_2)^\dagger \end{pmatrix}. \tag{5.6}$$

Then, we obtain

$$\begin{aligned} &|k,m\rangle^{'} \\ &= \frac{1}{\sqrt{k!}\sqrt{m!}} \left(B_{11}\hat{a}_1^{'\dagger} + B_{21}\hat{a}_2^{'\dagger}\right)^k \left(B_{12}\left(\hat{a}_1^{'}\right)^\dagger + B_{22}\left(\hat{a}_2^{'}\right)^\dagger\right)^l |0,0\rangle \\ &= \frac{1}{\sqrt{k!}\sqrt{m!}} \sum_{p,q=0}^{k,m} \binom{k}{p}\binom{m}{q} B_{11}^p B_{21}^{k-p} B_{12}^q B_{22}^{m-q} \left(\hat{a}_1^{'\dagger}\right)^p \left(\hat{a}_2^{'\dagger}\right)^{k-p} \left(\hat{a}_1^{'\dagger}\right)^q \left(\hat{a}_2^{'\dagger}\right)^{m-q} |0,0\rangle \\ &= \frac{1}{\sqrt{k!}\sqrt{m!}} \sum_{p,q=0}^{k,m} \binom{k}{p}\binom{m}{q} B_{11}^p B_{21}^{k-p} B_{12}^q B_{22}^{m-q} \sqrt{(p+q)!} \\ &\qquad \cdot \sqrt{(k+m-p-q)!}\, |p+q, k+m-p-q\rangle\,. \end{aligned}$$

We consider a beam splitter with transmittance η_t and reflection $1-\eta_t$, so we have $B_{11} = \eta_t = B_{22}$ and -$B_{12} = (1-\eta_t) = B_{21}$. Therefore, we find

$$\begin{aligned} |k,m\rangle^{'} = \frac{1}{\sqrt{k!}\sqrt{m!}} \sum_{p,q=0}^{k,m} \binom{k}{p}\binom{m}{q} \eta_t^{m+p-q}(1-\eta_t)^{k+q-p}(-1)^{k-p} \\ \cdot \sqrt{(p+q)!}\sqrt{(k+m-p-q)!}\, |p+q, k+m-p-q\rangle\,. \end{aligned} \tag{5.7}$$

Inserting this into equation (5.5) yields

$$\begin{aligned} \rho^{out}(x,y) = \sum_{k,l,m,n=0}^{\infty} \sum_{p,q,r,s=0}^{k,m,l,n} C_{k,l,m,n}^{p,q,r,s}\, \rho_{k,l}^{A'}(x,y)\rho_{m,n}^{th} \eta_t^{m+n+p-q+r-s}(1-\eta_t)^{k+l+q-p+s-r} \\ \cdot (-1)^{k+l-r-p}\, |p+q\rangle\langle r+s|^{1'} \otimes |k+m-p-q\rangle\langle l+n-r-s|^{2'} \end{aligned} \tag{5.8}$$

where

$$C_{k,l,m,n}^{p,q,r,s} := \frac{\binom{k}{p}\binom{m}{q}\binom{l}{r}\binom{n}{s}\sqrt{(p+q)!}\sqrt{(k+m-p-q)!}\sqrt{(r+s)!}\sqrt{(n+l-r-s)!}}{\sqrt{k!}\sqrt{m!}\sqrt{l!}\sqrt{n!}}. \tag{5.9}$$

Finally, we have to trace out mode $2'$, as we are only interested in the mode that is transmitted to Bob.

$$\rho_{\text{Start}} = \text{Tr}_{2'}\left[\rho^{out}(x,y)\right]. \tag{5.10}$$

In order to make the problem computationally feasible, we replace the upper limits ∞ in the sums over k, l, m and n by the cutoff number N_c.

5.1.2. Solving a semi-definite program

Alternatively, one can calculate a feasible starting value by solving a semi-definite program similar to the key rate finding problem, but where we set the objective function $f = 1$. Hence, we look only for a feasible starting value. Consequently, we have to solve the following semi-definite program to obtain a feasible starting value ρ_{Start}.

$$\text{minimise } 1 \tag{5.11}$$

subject to:

$$\begin{aligned}
\operatorname{Tr}\left[\rho_{AB}\left(|x\rangle\langle x|_A \otimes \hat{q}_B\right)\right] &= p_x \langle \hat{q} \rangle_x, \\
\operatorname{Tr}\left[\rho_{AB}\left(|x\rangle\langle x|_A \otimes \hat{p}_B\right)\right] &= p_x \langle \hat{p} \rangle_x, \\
\operatorname{Tr}\left[\rho_{AB}\left(|x\rangle\langle x|_A \otimes \hat{n}_B\right)\right] &= p_x \langle \hat{n} \rangle_x, \\
\operatorname{Tr}\left[\rho_{AB}\left(|x\rangle\langle x|_A \otimes \hat{d}_B\right)\right] &= p_x \langle \hat{d} \rangle_x, \\
\operatorname{Tr}_B\left[\rho_{AB}\right] &= \sum_{i,j=0}^{N_{\text{St}}-1} \sqrt{p_i p_j}\, \langle \phi_j | \phi_i \rangle\, |i\rangle\langle j|_A\,, \\
\rho_{AB} &\geqslant 0.
\end{aligned}$$

As the objective function is constant, this problem can be solved directly using some SDP solver without the necessity to linearise or apply the Frank-Wolfe algorithm. This attempt is (computationally) faster than the channel model approach, but due to numerical errors and solver imprecisions, sometimes the SDP-attempt returns density matrices with small negative eigenvalues, in particular for 'exotic' parameter regimes like very low ξ or high L.

5.2. Calculation of the conditioned probabilities

In this section, we give an expression for the probability that Bob measures $y \in \mathbb{C}$ given that Alice sent the state associated with the symbol x. According to the channel model (see Section 4.1.2) Bob receives a displaced thermal state. We obtain the wanted probability by tracing the product of the POVM operator associated with the outcome y with the density matrix Bob receives. In what follows, we are going to calculate this probability for the non-ideal trusted detector, because one obtains the corresponding probability for the ideal untrusted detector by setting $\eta_d = 1$ and $\nu_{el} = 0$. We use (4.23) to relate the conditioned probability to an integral over Wigner functions

$$P(y|x) = \mathrm{Tr}\left[\rho_B^x G_y\right] = \pi \int W_{\rho_B^x}(\gamma) W_{G_y}(\gamma)\, d^2\gamma, \tag{5.12}$$

where G_y is the POVM of the non-ideal trusted detector. Using equation (4.25), we find for the Wigner function of Bob's state

$$W_{\rho_B^x}(\gamma) = W_{\hat{D}(\sqrt{\eta}\alpha)\rho_{th}(\frac{\eta_t\xi}{2})\hat{D}^\dagger(\sqrt{\eta}\alpha)}(\gamma) = \frac{1}{\pi}\frac{1}{\frac{1}{2}(1+\eta_t\xi)} e^{-\frac{|\gamma-\sqrt{\eta}\alpha|^2}{\frac{1}{2}(1+\eta_t\xi)}}. \tag{5.13}$$

In combination with the Wigner function of the POVM G_y, given in equation (4.31), we obtain

$$\begin{aligned}
P(y|x) &= \pi \frac{1}{\pi\frac{1}{2}\left(1+\eta_t\xi\right)} \frac{2}{\eta_d \pi^2 \left(1 + \frac{2(1-\eta_d+\nu_{el}}{\eta_d}\right)} \int d^2\gamma e^{-\frac{\left|\gamma-\sqrt{\eta_t}\alpha_x\right|^2}{\frac{1}{2}(1+\eta_t\xi)}} e^{-\frac{2\left|\gamma-\frac{y}{\sqrt{\eta_d}}\right|^2}{\left(1+\frac{2(1-\eta_d+\nu_{el})}{\eta_d}\right)}} \\
&= C \int d\Re(\gamma) d\Im(\gamma) e^{-\frac{\left(\Re(\gamma)-\sqrt{\eta_t}\Re(\alpha_x)\right)^2+\left(\Im(\gamma)-\sqrt{\eta_t}\Im(\alpha_x)\right)}{\frac{1}{2}(1+\eta_t\xi)}} \int e^{-\frac{2\left(\Re(\gamma)-\frac{\Re(y)}{\eta_d}\right)^2+2\left(\Im(\gamma)-\frac{\Im(y)}{\eta_d}\right)^2}{\left(1+\frac{2(1-\eta_d+\nu_{el})}{\eta_d}\right)}} \\
&= C \int d\Re(\gamma) e^{-\frac{\left(\Re(\gamma)-\sqrt{\eta_t}\Re(\alpha_x)\right)^2}{\frac{1}{2}(1+\eta_t\xi)}} e^{-\frac{2\left(\Re(\gamma)-\frac{\Re(y)}{\eta_d}\right)^2}{\left(1+\frac{2(1-\eta_d+\nu_{el})}{\eta_d}\right)}} \\
&\qquad \cdot \int d\Im(\gamma) e^{-\frac{\left(\Im(\gamma)-\sqrt{\eta_t}\Im(\alpha_x)\right)}{\frac{1}{2}(1+\eta_t\xi)}} e^{-\frac{2\left(\Im(\gamma)-\frac{\Im(y)}{\eta_d}\right)^2}{\left(1+\frac{2(1-\eta_d+\nu_{el})}{\eta_d}\right)}}
\end{aligned}$$

where

$$C := \frac{4}{(1+\eta_t\xi)\left(1+\frac{2(1-\eta_d+\nu_{el})}{\eta_d}\right)\eta_d\pi^2}. \tag{5.14}$$

To ease the notation, we introduce the abbreviations $a_1 := \eta_t\xi$, $a_2 := \frac{2(1-\eta_d+\nu_{el})}{\eta_d}$. We observe that the integral over the real part has the same form as the integral over the imaginary part. Therefore, we consider only the integral over the real part, starting by rearranging the exponent of the integrand,

$$\begin{aligned}
&\frac{\left(\Re(\gamma)-\sqrt{\eta_t}\Re(\alpha_x)\right)^2}{\frac{1}{2}(1+a_1)}+\frac{\left(\Re(\gamma)-\frac{\Re(\alpha_x)}{\sqrt{\eta_d}}\right)^2}{\frac{1}{2}(1+a_2)}\\
&=\frac{2(2+a_1+a_2)}{(1+a_1)(1+a_2)}\left(\Re(\gamma)-\frac{\sqrt{\eta_t\eta_d}(1+a_2)\Re(\alpha_x)+(1+a_1)\Re(y)}{\eta_d(2+a_1+a_2)}\right)^2\\
&\qquad\qquad+\frac{2}{\eta_d(2+a_1+a_2)}\left(\Re(\alpha_x)\sqrt{\eta_t\eta_d}-\Re(y)\right)^2.
\end{aligned}$$

Then we arrive at

$$\int d\Re(\gamma)e^{-\frac{\left(\Re(\gamma)-\sqrt{\eta_t}\Re(\alpha_x)\right)^2}{\frac{1}{2}(1+\eta_t\xi)}}e^{-\frac{2\left(\Re(\gamma)-\frac{\Re(y)}{\eta_d}\right)^2}{\left(1+\frac{2(1-\eta_d+\nu_{el})}{\eta_d}\right)}}=\sqrt{\frac{\pi(1+a_1)(1+a_2)}{2(2+a_1+a_2)}}e^{-\frac{2\left(\sqrt{\eta_t\eta_d}\Re(\alpha_x)-\Re(y)\right)^2}{(2+a_1+a_2)\eta_d}}.$$

We obtain the solution for the integral over the imaginary part by replacing $\Re$ by $\Im$. Reinserting C, a_1 and a_2 and simplifying yields

$$P(y|x)=\frac{1}{\pi\left(1+\frac{1}{2}\eta_d\eta_t\xi+\nu_{el}\right)}e^{-\frac{\left|\sqrt{\eta_t\eta_d}\alpha_x-y\right|^2}{1+\frac{1}{2}\eta_d\eta_t\xi+\nu_{el}}}. \tag{5.15}$$

This result coincides with the conditional probability reported in [28]. If we set $\eta_d=1$ and $\nu_{el}=0$ we obtain the corresponding probability for the ideal untrusted detector

$$P(y|x)=\frac{1}{\pi\left(1+\frac{1}{2}\eta_t\xi\right)}e^{-\frac{\left|\sqrt{\eta_t}\alpha_x-y\right|^2}{1+\frac{1}{2}\eta_t\xi}}, \tag{5.16}$$

which matches with the value reported in [29].

5.3. Remarks on the implementation

In this work, we introduced protocols without fixing the sampling distribution. In the remainder of this thesis, we fix the sampling distribution to be the uniform distribution, $\forall j\in\{0,1,2,3\}:\ p_j=\frac{1}{4}$, which is expected to yield the highest key rates due to symmetry reasons. If not mentioned otherwise, we chose the photon cutoff number to $N_c=12$ for four-state protocols and $N_c=14$ for eight-state protocols. This turned out to be a good compromise between accuracy and computational requirements for many parameter-choices (see discussion in Section 7.1). Hence, the representation in the Fock basis of all operators is replaced by a truncated operator, i.e., we replaced the upper bound of the occurring sums by N_c. Furthermore, the maximum number of Frank-Wolfe iterations was chosen to be between

$N_{FW} = 10$ and $N_{FW} = 200$, depending on the choice of system parameters like the excess noise and the transmission distance. The threshold for the Frank-Wolfe algorithm ϵ_{FW} was chosen to be 10^{-7} and the perturbation $\tilde{\epsilon}$ was set to 10^{-11}. The transmittance was chosen to be $-0.2dB/km$ which is about 95.5% per kilometer, following $\eta = 10^{-0.02L}$. In the whole thesis, we chose a reconciliation efficiency of $\beta = 0.95$, if not mentioned otherwise. This is a realistic value as low-density parity-check (LDPC) codes with efficiencies up to $\beta = 0.95$ for the binary channel exist for relevant values of the error rate. Furthermore, we note that all sources of noise like the excess noise ξ and the electronic noise ν_{el} are measured in shot noise units.

The coding for the numerical security proof was carried out in MATLAB™R2020a and we used CVX [16, 15] to model the linear semi-definite programs. We employed both the MOSEK solver [2] and SDPT3 [47, 50] to dispense the semi-definite programs, while we mainly used MOSEK for the QPSK protocols and SDPT3 for the 8PSK examinations. Furthermore, it turned out that the line-search appearing in the modified Frank-Wolfe algorithm can be solved efficiently using the bisection method.

6. Theoretical calculations

In this chapter, we calculate secure key rates for four- and eight-state PSK protocols in the absence of noise and without postselection, where analytical results are known. Therefore, we generalise a security proof attempt presented in [19], to four- and eight-state protocols. The obtained secure key rates in this ideal case are used to validate our numerical method in the following chapter.

6.1. Theoretical calculation for four-state protocols

We begin with the four-state protocol (see Chapter 2). Note that similar results for a non-rotated QPSK protocol, based on [19], can be found in the appendix of [29]. We assume a noiseless channel, i.e., $\xi = 0$. According to the protocol description, Alice prepares one of the states $|\alpha_x\rangle$ with $\alpha_x \in \left\{|\alpha|e^{\frac{1i\pi}{4}}, |\alpha|e^{\frac{3i\pi}{4}}, |\alpha|e^{\frac{5i\pi}{4}}, |\alpha|e^{\frac{7i\pi}{4}}\right\}$ for $|\alpha| \in \mathbb{R}^+$ with equal probability $P(x = i) = \frac{1}{4}$ for $i \in \{0, 1, 2, 3\}$. According to [19], for a noiseless channel, it is sufficient to consider the generalised beam-splitter-attack, i.e., for a quantum channel with transmission $\eta > 0$, Bob receives one of the states

$$\left\{|\sqrt{\eta}|\alpha|e^{\frac{1i\pi}{4}}\rangle, |\sqrt{\eta}|\alpha|e^{\frac{3i\pi}{4}}\rangle,\ |\sqrt{\eta}|\alpha|e^{\frac{5i\pi}{4}}\rangle, |\sqrt{\eta}|\alpha|e^{\frac{7i\pi}{4}}\rangle\right\},$$

while Eve is assumed to hold one of the states

$$\left\{|\sqrt{1-\eta}|\alpha|e^{\frac{1i\pi}{4}}\rangle, |\sqrt{1-\eta}|\alpha|e^{\frac{3i\pi}{4}}\rangle, |\sqrt{1-\eta}|\alpha|e^{\frac{5i\pi}{4}}\rangle, |\sqrt{1-\eta}|\alpha|e^{\frac{7i\pi}{4}}\rangle\right\}.$$

So, Bob and Eve share the state $|\sqrt{\eta}\alpha_x\rangle_B \otimes |\sqrt{1-\eta}\alpha_x\rangle_E$, $x \in \{0, 1, 2, 3\}$. Hence, given that Alice sent the state corresponding to the symbol $x \in \{0, 1, 2, 3\}$, Eve holds

$$|\epsilon_x\rangle = |\sqrt{1-\eta}\alpha_x\rangle.$$

In the present protocol, we use reverse reconciliation, i.e., Alice corrects her bit string according to the information she receives from Bob. We use the Devetak-Winter formula [9] and evaluate

$$R^\infty = \beta I(A : B) - \chi(B : E). \tag{6.1}$$

Therefore, we have to calculate $I(A:B)$ and $\chi(B:E)$ and we start with the Holevo quantity.

6.1.1. Calculation of the Holevo quantity

Given that Alice sent the state corresponding to the symbol $x \in \{0,1,2,3\}$, Eve's states are

$$|\epsilon_0\rangle = e^{-\frac{|\sqrt{1-\eta}\alpha|^2}{2}} |\sqrt{1-\eta}\alpha_0\rangle = e^{-\frac{|\sqrt{1-\eta}\alpha|^2}{2}} \sum_{k=0}^{\infty} \frac{\left(\sqrt{1-\eta}|\alpha|e^{\frac{1i\pi}{4}}\right)^k}{\sqrt{k!}} |k\rangle, \tag{6.2}$$

$$|\epsilon_1\rangle = e^{-\frac{|\sqrt{1-\eta}\alpha|^2}{2}} |\sqrt{1-\eta}\alpha_1\rangle = e^{-\frac{|\sqrt{1-\eta}\alpha|^2}{2}} \sum_{k=0}^{\infty} \frac{\left(\sqrt{1-\eta}|\alpha|e^{\frac{3i\pi}{4}}\right)^k}{\sqrt{k!}} |k\rangle, \tag{6.3}$$

$$|\epsilon_2\rangle = e^{-\frac{|\sqrt{1-\eta}\alpha|^2}{2}} |\sqrt{1-\eta}\alpha_2\rangle = e^{-\frac{|\sqrt{1-\eta}\alpha|^2}{2}} \sum_{k=0}^{\infty} \frac{\left(\sqrt{1-\eta}|\alpha|e^{\frac{5i\pi}{4}}\right)^k}{\sqrt{k!}} |k\rangle, \tag{6.4}$$

$$|\epsilon_3\rangle = e^{-\frac{|\sqrt{1-\eta}\alpha|^2}{2}} |\sqrt{1-\eta}\alpha_3\rangle = e^{-\frac{|\sqrt{1-\eta}\alpha|^2}{2}} \sum_{k=0}^{\infty} \frac{\left(\sqrt{1-\eta}|\alpha|e^{\frac{7i\pi}{4}}\right)^k}{\sqrt{k!}} |k\rangle. \tag{6.5}$$

We want to describe Eve's system by an orthonormal set, $\{|e_0\rangle, |e_1\rangle, |e_2\rangle, |e_3\rangle\}$. It is an easy exercise to show that the states $|\epsilon_x\rangle$ are not orthonormal. We divide $\mathbb{N}_0$ into congruence classes of $0,1,2,3 \pmod 4$ and try to form basis vectors only by using number states that are in the same congruence class. Thus, we define

$$|\tilde{e}_0\rangle = \sum_{n=0}^{\infty} \frac{(\sqrt{1-\eta}|\alpha|)^{4n}}{\sqrt{(4n)!}} (-1)^n |4n\rangle, \tag{6.6}$$

$$|\tilde{e}_1\rangle = \sum_{n=0}^{\infty} \frac{(\sqrt{1-\eta}|\alpha|)^{4n+1}}{\sqrt{(4n+1)!}} (-1)^n |4n+1\rangle, \tag{6.7}$$

$$|\tilde{e}_2\rangle = \sum_{n=0}^{\infty} \frac{(\sqrt{1-\eta}|\alpha|)^{4n+2}}{\sqrt{(4n+2)!}} (-1)^n |4n+2\rangle, \tag{6.8}$$

$$|\tilde{e}_3\rangle = \sum_{n=0}^{\infty} \frac{(\sqrt{1-\eta}|\alpha|)^{4n+3}}{\sqrt{(4n+3)!}} (-1)^n |4n+3\rangle. \tag{6.9}$$

These vectors are pairwise orthogonal. Now we express $|\epsilon_x\rangle$ for $x \in \{0, 1, 2, 3\}$ as follows:

$$
\begin{aligned}
e^{\frac{|\sqrt{1-\eta}\alpha|^2}{2}} \left|\epsilon_0\right\rangle &= 1\left|\tilde{e}_0\right\rangle + e^{\frac{1i\pi}{4}}\left|\tilde{e}_1\right\rangle + e^{\frac{2i\pi}{4}}\left|\tilde{e}_2\right\rangle + e^{\frac{3i\pi}{4}}\left|\tilde{e}_3\right\rangle,\\
e^{\frac{|\sqrt{1-\eta}\alpha|^2}{2}} \left|\epsilon_1\right\rangle &= 1\left|\tilde{e}_0\right\rangle + e^{\frac{3i\pi}{4}}\left|\tilde{e}_1\right\rangle + e^{\frac{6i\pi}{4}}\left|\tilde{e}_2\right\rangle + e^{\frac{9i\pi}{4}}\left|\tilde{e}_3\right\rangle,\\
e^{\frac{|\sqrt{1-\eta}\alpha|^2}{2}} \left|\epsilon_2\right\rangle &= 1\left|\tilde{e}_0\right\rangle + e^{\frac{5i\pi}{4}}\left|\tilde{e}_1\right\rangle + e^{\frac{10i\pi}{4}}\left|\tilde{e}_2\right\rangle + e^{\frac{15i\pi}{4}}\left|\tilde{e}_3\right\rangle,\\
e^{\frac{|\sqrt{1-\eta}\alpha|^2}{2}} \left|\epsilon_4\right\rangle &= 1\left|\tilde{e}_0\right\rangle + e^{\frac{7i\pi}{4}}\left|\tilde{e}_1\right\rangle + e^{\frac{14i\pi}{4}}\left|\tilde{e}_2\right\rangle + e^{\frac{21i\pi}{4}}\left|\tilde{e}_3\right\rangle.
\end{aligned}
$$

It remains to normalise the orthonormal state vectors $|\tilde{e}_x\rangle$, $x \in \{0, 1, 2, 3\}$.

$$
\begin{aligned}
\langle \tilde{e}_0 | \tilde{e}_0 \rangle &= \sum_{n=0}^{\infty}\sum_{m=0}^{\infty} \frac{(\sqrt{1-\eta}|\alpha|e^{-\frac{1i\pi}{4}})^{4m}}{\sqrt{(4m)!}}(-1)^m \frac{(\sqrt{1-\eta}|\alpha|e^{+\frac{1i\pi}{4}})^{4n}}{\sqrt{(4n)!}}(-1)^n \langle 4m|4n\rangle\\
&= \sum_{n=0}^{\infty}\sum_{m=0}^{\infty} \frac{(\sqrt{1-\eta}|\alpha|e^{-\frac{1i\pi}{4}})^{4m}}{\sqrt{(4m)!}} \frac{(\sqrt{1-\eta}|\alpha|e^{\frac{1i\pi}{4}})^{4n}}{\sqrt{(4n)!}}(-1)^{m+n}\delta_{4m,4n}\\
&= \sum_{n=0}^{\infty} \frac{((1-\eta)|\alpha|^2)^{4n}}{(4n)!}\\
&= \frac{1}{2}\left(\sum_{n=0}^{\infty} \frac{((1-\eta)|\alpha|^2)^{2n}}{(2n)!} + \sum_{n=0}^{\infty}(-1)^n \frac{((1-\eta)|\alpha|^2)^{2n}}{(2n)!}\right)\\
&= \frac{\cosh((1-\eta)|\alpha|^2) + \cos((1-\eta)|\alpha|^2)}{2}.
\end{aligned}
$$

Similarly, we obtain

$$
\begin{aligned}
\langle \tilde{e_1} | \tilde{e_1} \rangle &= \frac{\sinh((1-\eta)|\alpha|^2) + \sin((1-\eta)|\alpha|^2)}{2},\\
\langle \tilde{e_2} | \tilde{e_2} \rangle &= \frac{\cosh((1-\eta)|\alpha|^2) - \cos((1-\eta)|\alpha|^2)}{2},\\
\langle \tilde{e_3} | \tilde{e_3} \rangle &= \frac{\sinh((1-\eta)|\alpha|^2) - \sin((1-\eta)|\alpha|^2)}{2}.
\end{aligned}
$$

Finally, the orthonormal system reads

$$|e_0\rangle = \frac{\sqrt{2}}{\sqrt{\cosh((1-\eta)|\alpha|^2) + \cos((1-\eta)|\alpha|^2)}} \sum_{n=0}^{\infty} \frac{((1-\eta)|\alpha|)^{4n}}{(4n)!}(-1)^n \, |4n\rangle \,, \tag{6.10}$$

$$|e_1\rangle = \frac{\sqrt{2}}{\sqrt{\sinh((1-\eta)|\alpha|^2) + \sin((1-\eta)|\alpha|^2)}} \sum_{n=0}^{\infty} \frac{((1-\eta)|\alpha|)^{4n+1}}{(4n+1)!}(-1)^n \, |4n+1\rangle \,, \tag{6.11}$$

$$|e_2\rangle = \frac{\sqrt{2}}{\sqrt{\cosh((1-\eta)|\alpha|^2) - \cos((1-\eta)|\alpha|^2)}} \sum_{n=0}^{\infty} \frac{((1-\eta)|\alpha|)^{4n+2}}{(4n+2)!}(-1)^n \, |4n+2\rangle \,, \tag{6.12}$$

$$|e_3\rangle = \frac{\sqrt{2}}{\sqrt{\sinh((1-\eta)|\alpha|^2) - \sin((1-\eta)|\alpha|^2)}} \sum_{n=0}^{\infty} \frac{((1-\eta)|\alpha|)^{4n+3}}{(4n+3)!}(-1)^n \, |4n+3\rangle \,. \tag{6.13}$$

After defining

$$c_0 := e^{-\frac{|\sqrt{1-\eta}\alpha|^2}{2}} \frac{\sqrt{\cosh((1-\eta)|\alpha|^2) + \cos((1-\eta)|\alpha|^2)}}{\sqrt{2}}, \tag{6.14}$$

$$c_1 := e^{-\frac{|\sqrt{1-\eta}\alpha|^2}{2}} \frac{\sqrt{\sinh((1-\eta)|\alpha|^2) + \sin((1-\eta)|\alpha|^2)}}{\sqrt{2}}, \tag{6.15}$$

$$c_2 := e^{-\frac{|\sqrt{1-\eta}\alpha|^2}{2}} \frac{\sqrt{\cosh((1-\eta)|\alpha|^2) - \cos((1-\eta)|\alpha|^2)}}{\sqrt{2}}, \tag{6.16}$$

$$c_3 := e^{-\frac{|\sqrt{1-\eta}\alpha|^2}{2}} \frac{\sqrt{\sinh((1-\eta)|\alpha|^2) - \sin((1-\eta)|\alpha|^2)}}{\sqrt{2}}, \tag{6.17}$$

we obtain the following representations for Eve's states in terms of our orthonormal basis,

$$\begin{aligned}
|\epsilon_0\rangle &= c_0 \, |e_0\rangle + c_1 e^{\frac{1i\pi}{4}} \, |e_1\rangle + c_2 e^{\frac{2i\pi}{4}} \, |e_2\rangle + c_3 e^{\frac{3i\pi}{4}} \, |e_3\rangle \,, \\
|\epsilon_1\rangle &= c_0 \, |e_0\rangle + c_1 e^{\frac{3i\pi}{4}} \, |e_1\rangle + c_2 e^{\frac{6i\pi}{4}} \, |e_2\rangle + c_3 e^{\frac{9i\pi}{4}} \, |e_3\rangle \,, \\
|\epsilon_2\rangle &= c_0 \, |e_0\rangle + c_1 e^{\frac{5i\pi}{4}} \, |e_1\rangle + c_2 e^{\frac{10i\pi}{4}} \, |e_2\rangle + c_3 e^{\frac{15i\pi}{4}} \, |e_3\rangle \,, \\
|\epsilon_3\rangle &= c_0 \, |e_0\rangle + c_1 e^{\frac{7i\pi}{4}} \, |e_1\rangle + c_2 e^{\frac{14i\pi}{4}} \, |e_2\rangle + c_3 e^{\frac{21i\pi}{4}} \, |e_3\rangle \,.
\end{aligned}$$

We proceed by describing Eve's states, depending on the result of Bob's measurement,

$$\rho_{E,j} = \sum_{i=0}^{3} P(x=i|z=j) \, |\epsilon_i\rangle\langle\epsilon_i| \,, \tag{6.18}$$

where $j \in \{0,1,2,3\}$. First, we rewrite the conditional probability $P(x=i|z=j)$ as

$$P(x=i|z=j) = \frac{P(x=i,z=j)}{P(z=j)}. \tag{6.19}$$

Recall that according to the protocol definition, Alice sends every state with equal probability, $\forall i \in \{0,1,2,3\}: \ P(x=i) = \frac{1}{4}$. By symmetry, the probability that Bob measures one of the states $\{0,1,2,3\}$ is equal too, $\forall j \in \{0,1,2,3\}: \ P(z=j) = \frac{1}{4}$. In what follows, we use the short-notation $P(i,j) := P(x=i,z=j)$. Then, we obtain for $j \in \{0,1,2,3\}$ the following density matrices:

$$\begin{aligned}
\rho_{E,j} &= \sum_{i=0}^{3} \frac{P(i,j)}{P(z=j)} |\epsilon_i\rangle\langle\epsilon_i| \\
&= \frac{1}{P(z=j)} \left[P(0,j) \begin{pmatrix} |c_0|^2 & c_0\overline{c_1}e^{-\frac{1i\pi}{4}} & c_0\overline{c_2}e^{-\frac{2i\pi}{4}} & c_0\overline{c_3}e^{-\frac{3i\pi}{4}} \\ c_1\overline{c_0}e^{\frac{1i\pi}{4}} & |c_1|^2 & c_1\overline{c_2}e^{-\frac{1i\pi}{4}} & c_1\overline{c_3}e^{-\frac{2i\pi}{4}} \\ c_2\overline{c_0}e^{\frac{2i\pi}{4}} & c_2\overline{c_1}e^{\frac{1i\pi}{4}} & |c_2|^2 & c_2\overline{c_3}e^{-\frac{1i\pi}{4}} \\ c_3\overline{c_0}e^{\frac{3i\pi}{4}} & c_3\overline{c_1}e^{\frac{2i\pi}{4}} & c_3\overline{c_2}e^{\frac{1i\pi}{4}} & |c_3|^2 \end{pmatrix} \right. \\
&\quad + P(1,j) \begin{pmatrix} |c_0|^2 & c_0\overline{c_1}e^{-\frac{3i\pi}{4}} & c_0\overline{c_2}e^{-\frac{6i\pi}{4}} & c_0\overline{c_3}e^{-\frac{9i\pi}{4}} \\ c_1\overline{c_0}e^{\frac{3i\pi}{4}} & |c_1|^2 & c_1\overline{c_2}e^{-\frac{3i\pi}{4}} & c_1\overline{c_3}e^{-\frac{6i\pi}{4}} \\ c_2\overline{c_0}e^{\frac{6i\pi}{4}} & c_2\overline{c_1}e^{\frac{3i\pi}{4}} & |c_2|^2 & c_2\overline{c_3}e^{-\frac{3i\pi}{4}} \\ c_3\overline{c_0}e^{\frac{9i\pi}{4}} & c_3\overline{c_1}e^{\frac{6i\pi}{4}} & c_3\overline{c_2}e^{\frac{3i\pi}{4}} & |c_3|^2 \end{pmatrix} \\
&\quad + P(2,j) \begin{pmatrix} |c_0|^2 & c_0\overline{c_1}e^{-\frac{5i\pi}{4}} & c_0\overline{c_2}e^{-\frac{10i\pi}{4}} & c_0\overline{c_3}e^{-\frac{15i\pi}{4}} \\ c_1\overline{c_0}e^{\frac{5i\pi}{4}} & |c_1|^2 & c_1\overline{c_2}e^{-\frac{5i\pi}{4}} & c_1\overline{c_3}e^{-\frac{10i\pi}{4}} \\ c_2\overline{c_0}e^{\frac{10i\pi}{4}} & c_2\overline{c_1}e^{\frac{5i\pi}{4}} & |c_2|^2 & c_2\overline{c_3}e^{-\frac{5i\pi}{4}} \\ c_3\overline{c_0}e^{\frac{15i\pi}{4}} & c_3\overline{c_1}e^{\frac{10i\pi}{4}} & c_3\overline{c_2}e^{\frac{5i\pi}{4}} & |c_3|^2 \end{pmatrix} \\
&\quad \left. + \ P(3,j) \begin{pmatrix} |c_0|^2 & c_0\overline{c_1}e^{-\frac{7i\pi}{4}} & c_0\overline{c_2}e^{-\frac{14i\pi}{4}} & c_0\overline{c_3}e^{-\frac{21i\pi}{4}} \\ c_1\overline{c_0}e^{\frac{7i\pi}{4}} & |c_1|^2 & c_1\overline{c_2}e^{-\frac{7i\pi}{4}} & c_1\overline{c_3}e^{-\frac{14i\pi}{4}} \\ c_2\overline{c_0}e^{\frac{14i\pi}{4}} & c_2\overline{c_1}e^{\frac{7i\pi}{4}} & |c_2|^2 & c_2\overline{c_3}e^{-\frac{7i\pi}{4}} \\ c_3\overline{c_0}e^{\frac{21i\pi}{4}} & c_3\overline{c_1}e^{\frac{14i\pi}{4}} & c_3\overline{c_2}e^{\frac{7i\pi}{4}} & |c_3|^2 \end{pmatrix} \right].
\end{aligned}$$

Eve's mixed state is given by

$$\begin{aligned}\rho_E &= \sum_{j=0}^{3} P(z=j)\rho_{E,j} = \sum_{j=0}^{4} P(z=j)\frac{1}{P(z=j)}\sum_{i=0}^{3} P(i,j)\,|\epsilon_i\rangle\langle\epsilon_i| \\ &= \sum_{i=0}^{3}\sum_{j=0}^{3} P(i,j)\,|\epsilon_i\rangle\langle\epsilon_i| \overset{(1)}{=} \sum_{i=0}^{3} P(x=i)\,|\epsilon_i\rangle\langle\epsilon_i| \\ &= \frac{1}{4}\sum_{i=0}^{3}|\epsilon_i\rangle\langle\epsilon_i|\,.\end{aligned}$$

For (1), we inserted the definition of the marginal distribution and for the last equality, we used that Alice prepares all states with equal probability. Therefore, we obtain Eve's density matrix with respect to the chosen orthonormal basis by adding the matrices from above and dividing the result by four,

$$\rho_E = \begin{pmatrix} |c_0|^2 & 0 & 0 & 0 \\ 0 & |c_1|^2 & 0 & 0 \\ 0 & 0 & |c_2|^2 & 0 \\ 0 & 0 & 0 & |c_3|^2 \end{pmatrix}. \tag{6.20}$$

It can be seen easily that the off-diagonal entries vanish, because we add complex numbers that are spread on the unit-circle regularly. Then, the von Neumann entropy of ρ_e can be calculated directly, exploiting the diagonal form,

$$H(\rho_E) = -\mathrm{Tr}\left[\rho_E \log_2(\rho_E)\right] = -2\sum_{i=0}^{3}|c_i|^2\log_2(|c_i|). \tag{6.21}$$

The entropies $H(\rho_j)$ for $j \in \{0,1,2,3\}$ do not have such a nice form, hence are calculated directly, without further simplifications.
Now we can calculate the Holevo quantity,

$$\chi(B:E) = H(\rho_E) - \sum_{j=0}^{3} P(z=j)H(\rho_{E,j}). \tag{6.22}$$

6.1.2. Calculating the mutual information and finding the secure key rate

The mutual information can be calculated as follows. We start from equation (1.14),

$$I(A:B) = H(\rho_A) + H(\rho_B) - H(\rho_A,\rho_B),$$

where the von Neumann entropies $H(\rho_A)$ and $H(\rho_B)$ are equal to 2. This is because we transmit two bits of information within one signal, i.e., the surprise when one learns about Alice's state (or vice-versa), is 2 bits. We evaluate $H(\rho_A, \rho_B)$ directly by using the definition,

$$\begin{aligned} H(\rho_A, \rho_B) &= -\sum_{i=0}^{3}\sum_{j=0}^{3} P(x=i, z=j)\log_2(P(i,j)) \\ &= -\sum_{i=0}^{3}\sum_{j=0}^{3} P(z=j|x=i)P(x=i)\log_2(P(j|i)P(x=i)). \end{aligned}$$

Note that we used the definition of the conditioned probability for the second equality, $P(B|A) = \frac{P(B\cap A)}{P(A)}$.

Finally, we insert our results into equation (6.1) and obtain a lower bound on the key rate.

6.2. Theoretical calculation for eight-state protocols

We proceed similarly for the eight-state protocol (see Chapter 2) and generalise the attempt in [19] to eight states. Again we consider a noiseless channel, $\xi = 0$. According to the protocol description, Alice prepares one of the states $|\alpha_x\rangle$ with

$$\alpha_x \in \left\{|\alpha|e^{\frac{0i\pi}{4}}, |\alpha|e^{\frac{1i\pi}{4}}, |\alpha|e^{\frac{2i\pi}{4}}, |\alpha|e^{\frac{3i\pi}{4}}, |\alpha|e^{\frac{4i\pi}{4}}, |\alpha|e^{\frac{5i\pi}{4}}, |\alpha|e^{\frac{6i\pi}{4}}, |\alpha|e^{\frac{7i\pi}{4}}\right\}$$

with equal probability $P(x=i) = \frac{1}{8}$ for $i \in \{0, 1, ..., 7\}$. Considering the generalised beam-splitter-attack for a quantum channel with transmission $\eta > 0$, Bob receives $|\sqrt{\eta}\alpha_x\rangle$, while Eve holds $|\sqrt{1-\eta}\alpha_x\rangle$ for $x \in \{0, 1, ..., 7\}$. Similarly to the previous section, we introduce the short notation

$$|\epsilon_x\rangle = |\sqrt{1-\eta}\alpha_x\rangle\,.$$

The secret key rate in the asymptotic limit is given by the Devetak-Winter formula (here for reverse reconciliation),

$$R^{\infty} = \eta I(A:B) - \chi(B:E).$$

In what follows, we discuss how to calculate the mutual information between Alice and Bob and the Holevo quantity, starting with the Holevo quantity.

6.2.1. Calculation of the Holevo quantity

Given that Alice sent the state corresponding to the symbol $x \in \{0, 1, ..., 7\}$, Eve's states have the form

$$\left|\epsilon_x\right\rangle = e^{-\frac{|\sqrt{1-\eta}\alpha_x|^2}{2}} \left|\sqrt{1-\eta}\alpha_x\right\rangle = e^{-\frac{|\sqrt{1-\eta}\alpha_x|^2}{2}} \sum_{k=0}^{\infty} \frac{\left(\sqrt{1-\eta}\alpha_x\right)^k}{\sqrt{k!}} \left|k\right\rangle . \tag{6.23}$$

As we need to calculate the entropy of Eve's state, it would be beneficial to describe Eve's state by an orthonormal basis

$$\{\left|e_0\right\rangle, \left|e_1\right\rangle, \left|e_2\right\rangle, \left|e_3\right\rangle, \left|e_4\right\rangle, \left|e_5\right\rangle, \left|e_6\right\rangle, \left|e_7\right\rangle\} .$$

Therefore, we use a similar idea as in the previous section and divide $\mathbb{N}_0$ into eight congruence classes of $0, 1, ..., 7 \pmod 8$, where each basis vector should consist of all Fock states with numbers in one congruence class. This means we consider a set of eight vectors of the form

$$\left|\tilde{e}_x\right\rangle = \sum_{n=0}^{\infty} \frac{\left(\sqrt{1-\eta}\alpha_x\right)^{8n+x}}{\sqrt{(8n+x)!}} \left|8n+x\right\rangle \tag{6.24}$$

for $x \in \{0, ..., 7\}$. Per construction, these vectors are pairwise orthogonal, $\left\langle \tilde{e}_i, \tilde{e}_j \right\rangle = 0$ if $i \neq j$. Eve's states can be expressed in terms of the basis vectors as follows

$$\left|\epsilon_x\right\rangle = e^{-\frac{|\sqrt{1-\eta}\alpha_x|^2}{2}} \sum_{l=0}^{7} \left(e^{\frac{xi\pi}{4}}\right)^l \left|\tilde{e}_l\right\rangle . \tag{6.25}$$

It remains to normalise the basis states. To ease the following calculations, we introduce the short-notation $\gamma := (1-\eta)|\alpha|^2$. Then, we derive the first basis vector

$$\begin{aligned}
&\left\langle \tilde{e}_0 \middle| \tilde{e}_0 \right\rangle \\
&= \sum_{n=0}^{\infty} \frac{\gamma^{8n}}{(8n)!} = \frac{1}{2}\left[\sum_{n=0}^{\infty} \frac{\gamma^{4n}}{(4n)!} + \sum_{n=0}^{\infty} (-1)^n \frac{\gamma^{4n}}{(4n)!}\right] \\
&= \frac{1}{4}\left[\sum_{n=0}^{\infty} \frac{\gamma^{2n}}{(2n)!} + \sum_{n=0}^{\infty} (-1)^n \frac{\gamma^{2n}}{(2n)!}\right] + \frac{1}{4}\left[\sum_{n=0}^{\infty} (-i)^n \frac{\gamma^{2n}}{(2n)!} + \sum_{n=0}^{\infty} i^n \frac{\gamma^{2n}}{(2n)!}\right] \\
&= \frac{1}{4}\left[\sum_{n=0}^{\infty} \frac{\gamma^{2n}}{(2n)!} + \sum_{n=0}^{\infty} (-1)^n \frac{\gamma^{2n}}{(2n)!}\right] + \frac{1}{4}\left[\sum_{n=0}^{\infty} (-1)^n \frac{\left(e^{\frac{i\pi}{4}}\gamma\right)^{2n}}{(2n)!} + \sum_{n=0}^{\infty} \frac{\left(e^{\frac{i\pi}{4}}\gamma\right)^{2n}}{(2n)!}\right] \\
&= \frac{1}{4}\left[\cosh(\gamma) + \cos(\gamma) + \cos\left(e^{\frac{i\pi}{4}}\gamma\right) + \cosh\left(e^{\frac{i\pi}{4}}\gamma\right)\right] .
\end{aligned}$$

Similarly, we obtain for the other basis vectors

$$
\begin{aligned}
\langle \tilde{e}_1|\tilde{e}_1\rangle &= \frac{1}{4}\left[\sinh(\gamma) + \sin(\gamma) + e^{-\frac{i\pi}{4}}\sin\left(e^{\frac{i\pi}{4}}\gamma\right) + e^{-\frac{i\pi}{4}}\sinh\left(e^{\frac{i\pi}{4}}\gamma\right)\right],\\
\langle \tilde{e}_2|\tilde{e}_2\rangle &= \frac{1}{4}\left[\cosh(\gamma) - \cos(\gamma) + i\cos\left(e^{\frac{i\pi}{4}}\gamma\right) - i\cosh\left(e^{\frac{i\pi}{4}}\gamma\right)\right],\\
\langle \tilde{e}_3|\tilde{e}_3\rangle &= \frac{1}{4}\left[\sinh(\gamma) - \sin(\gamma) + ie^{-\frac{i\pi}{4}}\sin\left(e^{\frac{i\pi}{4}}\gamma\right) - ie^{-\frac{i\pi}{4}}\sinh\left(e^{\frac{i\pi}{4}}\gamma\right)\right],\\
\langle \tilde{e}_4|\tilde{e}_4\rangle &= \frac{1}{4}\left[\cosh(\gamma) + \cos(\gamma) - \cos\left(e^{\frac{i\pi}{4}}\gamma\right) - \cosh\left(e^{\frac{i\pi}{4}}\gamma\right)\right],\\
\langle \tilde{e}_5|\tilde{e}_5\rangle &= \frac{1}{4}\left[\sinh(\gamma) + \sin(\gamma) - e^{-\frac{i\pi}{4}}\sin\left(e^{\frac{i\pi}{4}}\gamma\right) - e^{-\frac{i\pi}{4}}\sinh\left(e^{\frac{i\pi}{4}}\gamma\right)\right],\\
\langle \tilde{e}_6|\tilde{e}_6\rangle &= \frac{1}{4}\left[\cosh(\gamma) - \cos(\gamma) - i\cos\left(e^{\frac{i\pi}{4}}\gamma\right) + i\cosh\left(e^{\frac{i\pi}{4}}\gamma\right)\right],\\
\langle \tilde{e}_7|\tilde{e}_7\rangle &= \frac{1}{4}\left[\sinh(\gamma) - \sin(\gamma) - ie^{-\frac{i\pi}{4}}\sin\left(e^{\frac{i\pi}{4}}\gamma\right) + ie^{-\frac{i\pi}{4}}\sinh\left(e^{\frac{i\pi}{4}}\gamma\right)\right].
\end{aligned}
$$

Hence, the orthonormal basis vectors read

$$
|e_l\rangle = \frac{1}{\sqrt{\langle \tilde{e}_l|\tilde{e}_l\rangle}}\,|\tilde{e}_l\rangle\,. \tag{6.26}
$$

Finally, we express Eve's states in terms of the orthonormal basis vectors,

$$
|\epsilon_x\rangle = \sum_{l=0}^{7} c_l \left(e^{\frac{xi\pi}{4}}\right)^l |e_l\rangle\,, \tag{6.27}
$$

where

$$
c_l := e^{-\frac{(\sqrt{1-\eta}\alpha_x)^2}{2}}\sqrt{\langle \tilde{e}_l|\tilde{e}_l\rangle}.
$$

Eve's state, depending on Bob's measurement result $z = j \in \{0, 1, ..., 7\}$ reads

$$
\rho_{E,j} = \sum_{i=0}^{7} P(x = i|z = j)\,|\epsilon_i\rangle\langle\epsilon_i|\,, \tag{6.28}
$$

where the conditional probability can be rewritten by

$$
P(x = i|z = j) = \frac{P(x = i, z = j)}{P(z = j)}. \tag{6.29}
$$

Then, we obtain Eve's mixed state by

$$\begin{aligned}\rho_E &= \sum_{j=0}^{7} P(z=j)\rho_{E,j} = \sum_{j=0}^{7} P(z=j) \sum_{i=0}^{7} \frac{P(x=i,z=j)}{P(z=j)} \left|\epsilon_i\right\rangle\left\langle\epsilon_i\right| \\ &= \sum_{j=0}^{7}\sum_{i=0}^{7} P(x=i,z=j) \left|\epsilon_i\right\rangle\left\langle\epsilon_i\right| = \sum_{i=0}^{7} P(x=i) \left|\epsilon_i\right\rangle\left\langle\epsilon_i\right| \\ &= \frac{1}{8}\sum_{i=0}^{7} \left|\epsilon_i\right\rangle\left\langle\epsilon_i\right| .\end{aligned}$$

For the last equality, we inserted that Alice sends each state with equal probability, $\forall i \in \{0, ..., 7\} : P(x=i) = \frac{1}{8}$. One observes the diagonal structures of the conditioned states $\rho_{E,j}$ as well as ρ_E. This will turn out to be advantageous for the calculation of the von Neumann entropies.

Next, we use equation (6.27) to find an explicit matrix representation for ρ_E. Obviously, we obtain for the diagonal terms $(\left|\epsilon_i\right\rangle\left\langle\epsilon_i\right|)_{kk} = |c_k|^2$. So, after summation over i, we have $8|c_k|^2$ and the pre-factor 8 cancels with the $\frac{1}{8}$ in front of the sum. The off-diagonal terms add up to zero, as the additional exponential factors $e^{\frac{i\pi}{4}(k-l)x}$ occurring in the expression $(\left|\epsilon_i\right\rangle\left\langle\epsilon_i\right|)_{kl} = c_k\bar{c}_l \sum_{x=0}^{7} e^{\frac{i\pi}{4}(k-l)x}$ are spread on the unit-circle equally. Thus, we have

$$\rho_E = \mathrm{diag}\left(|c_0|^2, |c_1|^2, |c_2|^2, |c_3|^2, |c_4|^2, |c_5|^2, |c_6|^2, |c_7|^2\right) . \tag{6.30}$$

The von Neumann entropy of Eve's state reads,

$$H(\rho_E) = -\mathrm{Tr}\left[\rho_e \log_2(\rho_E)\right] = -2\sum_{i=0}^{7} |c_i|^2 \log_2(|c_i|).$$

The entropies $H(\rho_j)$ for $j \in \{0, 1, ..., 7\}$ do not have such a nice form, as not all probabilities $P(x=i, z=j)$ have the same value, hence we proceed without any further simplification.

Nevertheless, we can calculate the Holevo quantity,

$$\chi(B:E) = H(\rho_E) - \sum_{j=0}^{7} P(z=j)H(\rho_{E,j}). \tag{6.31}$$

6.2.2. Calculating the mutual information and finding the secure key rate

We obtain the mutual information from equation (1.14),

$$I(A:B) = H(\rho_A) + H(\rho_B) - H(\rho_A, \rho_B),$$

where the von Neumann entropies $H(\rho_A)$ and $H(\rho_B)$ are equal to 4. This is because we transmit four bits of information within one signal, i.e., the surprise when Bob learns Alice's state (or vice-versa), is 4 bits. We evaluate $H(\rho_A, \rho_B)$ directly by using the definition,

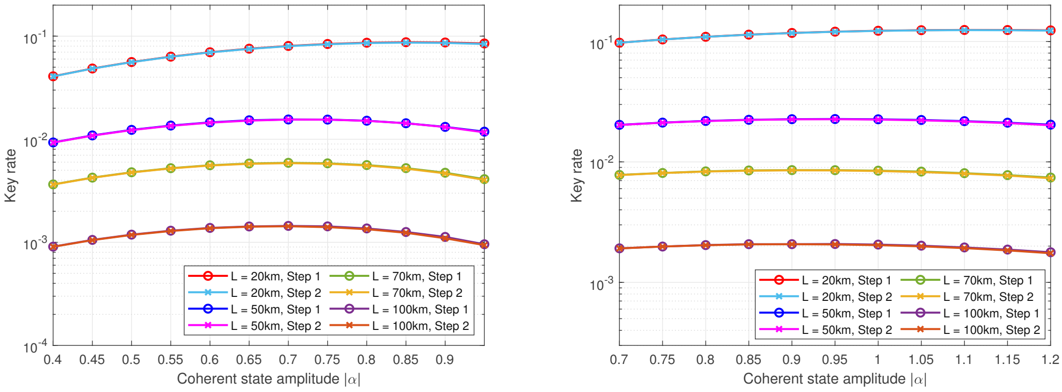
$$\begin{aligned} H(\rho_A, \rho_B) &= -\sum_{i=0}^{7}\sum_{j=0}^{7} P(x=i, z=j)\log_2(P(i,j)) \\ &= -\sum_{i=0}^{7}\sum_{j=0}^{7} P(z=j|x=i)P(x=i)\log_2(P(z=j|x=i)P(x=i)). \end{aligned}$$

Note that we used the definition of the conditioned probability for the second equality, $P(B|A) = \frac{P(B\cap A)}{P(A)}$.

Finally, we insert our results into equation (6.1) and obtain a lower bound on the key rate.

7. Validation of the implementation

Before we come to the results of this thesis, we validate our implementation by comparing our numerical results with the results from the analytical calculation for the noiseless channel without postselection carried out in the previous chapter. In the whole chapter we set the reconciliation efficiency to $\beta = 0.95$ and consider the case of reverse reconciliation. For the sake of numerical stability, we use $\xi = 10^{-5}$ for our numerical calculations instead of $\xi = 0$. We perform the validation both for the four-state (QPSK) and the eight-state (8PSK) protocol.



(a) QPSK protocol

(b) 8PSK protocol

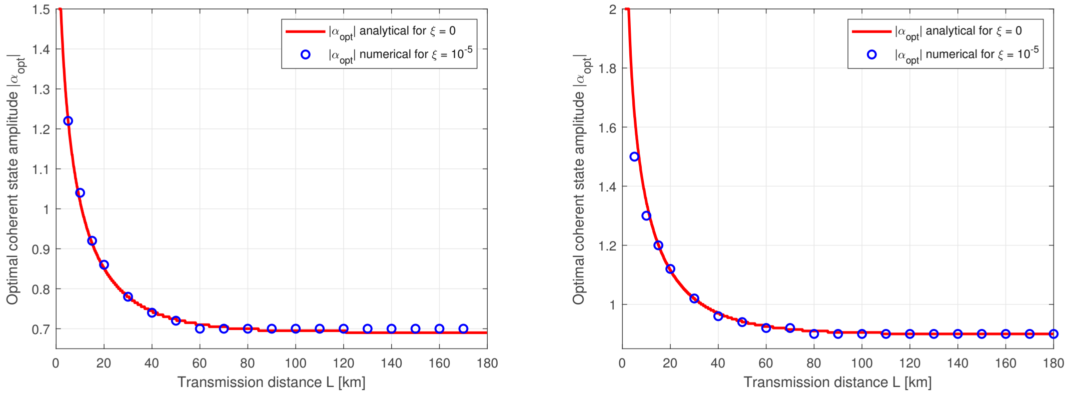
Figure 7.1.: Secure key rate vs. coherent state amplitude $|\alpha|$ for a noiseless channel (to achieve numerical stability we used $\xi = 10^{-5}$) for various transmission distances. The photon cutoff number was chosen to be $N_c = 12$ for the QPSK protocol and $N_c = 14$ for the 8PSK protocol.

First, we examine the dependency of the secure key rate on the coherent state amplitude $|\alpha|$ for various transmission distances L. We chose the cutoff number to be $N_c = 12$ for the QPSK protocol and $N_c = 14$ for the 8PSK protocol. The 8PSK protocol requires a higher cutoff number since (as we will see in what follows) it involves higher coherent state amplitudes $|\alpha|$ than the QPSK protocol, hence requires higher cutoffs to represent the occurring cohrerent states with negligible error. This is because states with higher coherent state amplitude have a greater displacement from the origin, hence require Fock states with higher occupation number to be described accurately. For our numerical examinations, we chose a step size of $\Delta_{|\alpha|} = 0.05$. In Figure 7.1, we display the achieved secure key rates over the coherent state amplitude for different transmission distances, where the results for the QPSK protocol are shown in Figure 7.1a and the results for the 8PSK protocol in Figure 7.1b.

For the QPSK protocol (see Figure 7.1a), one reads out a maximal secure key rate of $|\alpha| = 0.86$ for $L = 20$km, a maximal secure key rate of $|\alpha| = 0.72$ and $|\alpha| = 0.75$ for $L = 50$km, and a maximal secure key rate of $|\alpha| = 0.70$ for $L = 70$km as well as for $L = 100$km. Similarly, one finds for the 8PSK protocol (see Figure 7.1b) a maximal secure key rate of about $|\alpha| = 1.10$ for $L = 20$km, a maximal secure key rate of about $|\alpha| = 0.95$ for $L = 50$km, and a maximal secure key rate of about $|\alpha| = 0.90$ for $L = 70$km and $L = 100$km. Note that the obtained curves are smooth and the gap between the first and the second step is very small, indicating only a small gap between the obtained upper and lower bound on the secure key rate. Furthermore, observe that the maximal secure key rate for $L = 100$km is about one tenth of the maximal secure key rate for $L = 50$km, both for the QPSK and the 8PSK protocol, exactly as expected for a channel with losses of 0.2db/km.

Similar examinations were conducted for various transmission distances. For all examined transmission lengths, we found an excellent accordance between predictions and the theoretical values. This can be seen in Figure 7.2, where we plotted the optimal coherent state amplitude according to the theoretical model (red line) and the values for the numerical optimum (blue dots) both for the QPSK protocol (Figure 7.2a) and the 8PSK protocol (Figure 7.2b). The analytical curve was obtained by searching the optimum over the key rates obtained by using eq. (6.1) and the considerations in the previous chapter with a fine-grained search in steps of $\Delta_{|\alpha|} = 0.02$ and $\Delta_L = 0.1$km.

Second, we consider the secure key rates for the noiseless channel and for transmission distances up to 180km. In Figure 7.3, we compare the analytical prediction according to eq. (6.1) and the considerations in the previous chapter with our numerical results for $\xi = 10^{-5}$, where we plot both the result for the first and the second step. The underlying data for the QPSK protocol (Figure 7.3a) was calculated with $N_c = 12$ and for the 8PSK protocol (Figure 7.3b) we used $N_c = 14$. Furthermore, we plot the absolute difference between the first and the second step and the relative (secondary y-axis) differences between the second steps and the theoretical prediction. One observes that the gap between the first and the sec-



(a) QPSK protocol

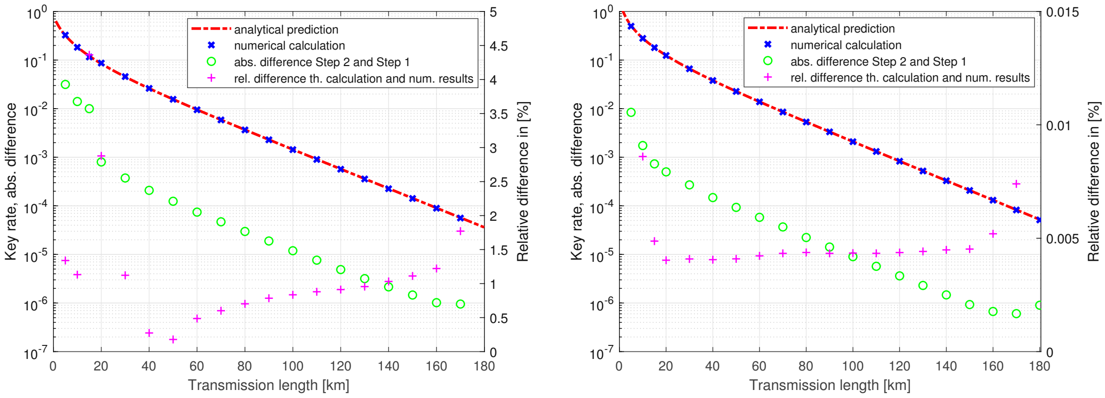
(b) 8PSK protocol

Figure 7.2.: Optimal analytical $|\alpha|$ for different transmission lengths L and for $\xi = 0$, found by fine-grained search in steps of $\Delta_{|\alpha|} = 0.005$ (red line) and optimal coherent state amplitudes obtained by numerical calculations and fine-grained search in steps of $\Delta_{|\alpha|} = 0.02$ (blue dots). The investigation shows that optimal coherent state amplitudes obtained by numerical calculation match perfectly with the analytical prediction.

ond step is a few magnitudes lower than the key rate which indicates satisfying results. The relative difference between our lower bound and the numerical results are lower than 1.5%, except for three outliers at 15km, 20km and 170km. These deviations are due to numerical instabilities of the algorithm for low excess-noise.

Similarly, for the 8PSK protocol, the absolute gap between the first and the second step is a few magnitudes lower than the calculated lower bounds. Focussing on transmission lengths between 15km and 160km, the differences between the first and the second step are smaller than 0.5%. The relative differences between the theoretical prediction and our numerical lower bounds on the secure key rate for the 8PSK protocol are lower than 0.01% for distances between 10km and 170km and are higher only for 5km and 180km, which underlines the excellent accuracy of our implementation.

Hence, we obtain satisfying results, demonstrating the reliability of our code. Furthermore, according to our data, the 8PSK protocol yields significantly higher key rates than the QPSK protocol, which meets the expectations.



(a) QPSK protocol (b) 8PSK protocol

Figure 7.3.: Comparison between key rates for theoretical prediction and numerical results for the lower bound on the secure key rate (almost) without noise and without postselection. The left y-axis shows the secure key rate in log-scale, as well as the absolute difference between step 1 and step 2, and the right y-axis the relative difference between the theoretical prediction and the obtained lower bound in %. The displayed secure key rates are obtained by optimizing over $|\alpha|$.

7.1. Choice of the cutoff number

Finally, we comment on the chosen photon cutoff number N_c. We carry out our examinations for the four-state protocol to keep the computational effort low, but we expect comparable results for the eight-state protocol for similar $|\alpha|$. Recall that the photon-number cutoff assumption [29], allows us to truncate Bob's infinite-dimensional Hilbert space $\mathcal{H}_B = \{|n\rangle \ : \ n \in \mathbb{N}_0\}$, spanned by the number states, after the first $N_c + 1$ basis vectors. Therefore, we need to choose N_c large enough such that the error due to the cutoff is negligible, but as small as possible to keep the computational effort low, as the problem size increases with increasing N_c. To find the optimal cutoff number N_c we examined the change in the secure key rate for different N_c for various transmission distances and postselection patterns. In Figure 7.4, we plot the secure key rates over the cutoff number N_c for fixed reconciliation efficiency $\beta = 0.95$ and fixed excess-noise $\xi = 0.01$ for the present four-state protocol for different transmission distances and postselection parameters. One observes that the secret key rates stay approximately constant for $N_c \geqslant 12$ for all examined parameter sets. For $N_c \geqslant 12$, the secure key rates change by less than 0.5% between neighbouring points on the same curve, and by less than 0.2% for $N_c \geqslant 14$. We note that this small variations are mainly caused by the differences between the first and the second step of our key rate finding procedure. The deviations between the first steps are smaller than 0.01% for $N_c \geqslant 12$. Therefore, $N_c = 12$ turned out to be sufficiently accurate for four-state protocols, while still yielding computationally feasible optimisation tasks. Since eight-state protocols involve slightly higher coherent state amplitudes $|\alpha|$, we used $N_c = 14$ for eight-state examinations.

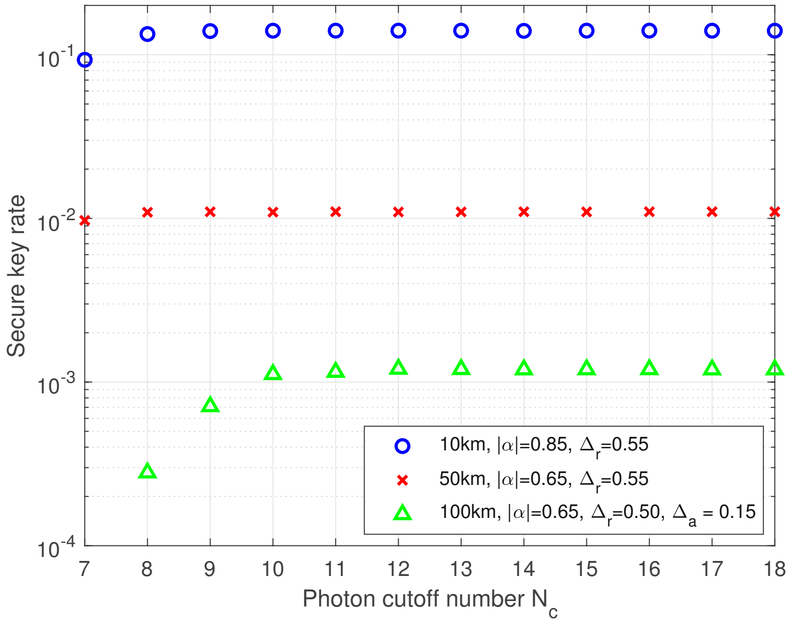


Figure 7.4.: Secure key rate versus chosen cutoff-number N_c for three different distances and choices of postselection parameter. For all three curves, we set $\beta = 0.95$ and $\xi = 0.01$ and the results refer to the four-state protocol.

8. Results for four-state protocols

In this chapter, we present the results and findings for the four-state protocol, both for the untrusted ideal and the trusted non-ideal detector, obtained within the frame of the present thesis. The following chapter was published by the author in [23], where it makes up sections VI and VII.

8.1. Postselection strategies for untrusted detectors

In this section, we are going to present our numerical results and findings for the untrusted ideal detector scenario. Recall that in the whole thesis, we work with a reconciliation-efficiency of $\beta = 0.95$ if not mentioned otherwise and measure the excess noise ξ in shot noise units.

8.1.1. Cross-shaped postselection

The basic idea of introducing postselection is to increase the secure key rate by discarding noisy data, where Eve could have gained more information about the key than Alice and Bob did. Performing no postselection at all gives Eve an advantage if the signal is noisy, while on the other hand, postselecting too much (or even all signals) does not leave back enough data to generate a secret key. Therefore, we expect that there is some sweet spot where Alice and Bob can take an optimal advantage. According to our cross-shaped scheme (see Chapter 2), we expect that Eve can benefit most from noisy signals with quadratures close to the axis, where little noise suffices to convert one symbol into another one, i.e., where bit-flips are likely. In the cross-shaped postselection strategy, we determine the ratio of signals that are discarded by varying the postselection parameter Δ_c. Hence, an important task will be to determine the optimal choice of Δ_c depending on the chosen $|\alpha|$ for every transmission length L.

Optimal coherent state amplitude

Before we investigate Δ_c, we enquire about the influence of $|\alpha|$ on the secure key rate, as the optimal choice of Δ_c might heavily depend on the chosen $|\alpha|$. In Figure 8.1, we investigate the optimal choice of the coherent state amplitude $|\alpha|$ for different values of ξ via coarse-grained search in steps of size 0.05 in the interval $|\alpha| \in [0.4, 1.2]$ and for lengths between 5km and 180km in the absence of postselection and compare our findings with the analytical curve for optimal $|\alpha|$ in the noiseless case. Our results show that the optimal coherent state amplitude in noisy channels is still close to the result for the noiseless case and the values for $20, 50, 80$ and 100km match with the values reported by [29] for a similar protocol with rotated signal states. Furthermore, we observe that there are only minor differences between the found optimal values for different values of excess noise. Therefore, it is sufficient to search around $|\alpha_{opt}|$, obtained from the noiseless case, which will be useful for the following examinations.

Key rates for different transmission distances and noise levels

In Figures 8.2a and 8.2b, we plot the first and second step of the secure key rate calculation versus the postselection parameter Δ_c for $\xi = 0.01$ (Fig. 8.2a) and $\xi = 0.02$ (Fig. 8.2b) for fixed distances $L = 50$km (solid lines) and $L = 100$km (dashed lines) on logarithmic scale. Note that the differences between the curves representing the first step and those representing the second step in each of the plots are very small, indicating small gaps between the calculated upper and lower bounds, hence tight bounds on the secure key rates.

One observes a very different behaviour of the curves for $L = 50$km and $L = 100$km for both values of excess noise. First, we investigate $\xi = 0.01$, depicted in Figure 8.2a, beginning with the curves with solid lines, representing a transmission distance of 50km. The curve for $|\alpha| = 0.75$ does not show a maximum in the interior of the interval $[0, 0.55]$ at all but attains its maximum at $\Delta_c = 0$, which means no postselection at all. If we raise $|\alpha|$ to 0.90, the curve is still flat in the interval $[0, 0.25]$ but starts forming a maximum around $\Delta_c = 0.25$. Increasing $|\alpha|$ to 1.00, leads to a distinct maximum at $\Delta_c = 0.35$. Therefore, the maximal secure key rate does not move from $\Delta_c = 0$ to higher values slowly when increasing $|\alpha|$ but changes rapidly from zero to some value in the middle of the interval.

We do not observe 'flat' secure key rate curves without a pronounced maximum for $L = 100$km. The corresponding curves are represented by dashed lines in Figure 8.2a. Here, already the curve for $|\alpha| = 0.75$ shows a distinct maximum, as well as

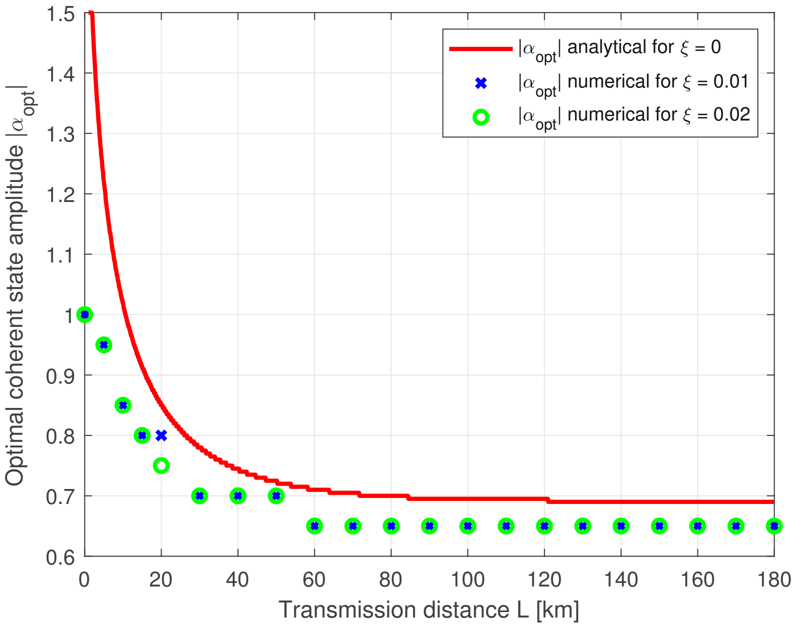
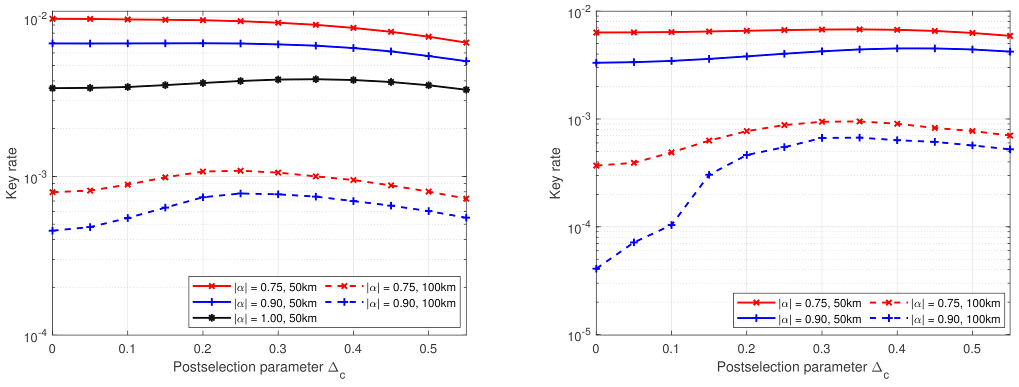


Figure 8.1.: Optimal $|\alpha|$ for different transmission lengths L and for $\xi = 0$, found by fine-grained search in steps of $\Delta_{|\alpha|} = 0.005$ (red line). Furthermore, we plotted the optimal $|\alpha|$ for $\xi = 0.01$ and $\xi = 0.02$, obtained by numerical calculations and coarse grained search (with a step-size of $\Delta_{|\alpha|} = 0.05$). As expected, the optimal coherent state amplitude for noisy channels is very close to the analytically calculated coherent state amplitude in the noiseless case with only minor differences between the optimal choice of $|\alpha|$ for different values of excess noise.



(a) $\xi = 0.01$

(b) $\xi = 0.02$

Figure 8.2.: Secure key rate vs. Δ_c for $L = 50$km (solid lines) and $L = 100$km (dashed lines) and various $|\alpha|$. We chose the photon cutoff number $N_c = 12$.

the curve for $|\alpha| = 0.90$, indicating that Alice and Bob can increase their secure key rate by removing parts of their raw key for both choices of $|\alpha|$.

In Figure 8.2b, we increased ξ to 0.02. One observes a distinct optimum apart from $\Delta_c = 0$ for all curves in this plot, in particular for those with $|\alpha| = 0.75$ where we have not observed any maximum for $\xi = 0.01$. Note that the logarithmic scale suppresses the maximum of the curve for $|\alpha| = 0.75$, although in a linear plot one already observes a distinct maximum at $\Delta_c = 0.35$. Therefore, we see that for increased excess noise ξ we require postselection to obtain the maximal secure key rate. That is, in accordance with our expectations, as additional noise gives Eve an advantage, hence requires Alice and Bob to remove parts of the signal. The curves for $L = 100$km do not change significantly, as they already had a distinct maximum for $\xi = 0.01$. Thus, increased excess noise requires postselection for all examined values of $|\alpha|$ for fixed transmission length L.

We observe that the differences between the secure key rate for $\Delta_c = 0$ and the secure key rate for the optimal choice of Δ_c differ significantly for various values of excess noise and several transmission distances. For example, the difference between the maximal secure key rate and that at $\Delta_c = 0$ for $\xi = 0.02$ and $|\alpha| = 0.75$ at $L = 50$km is about 5%, while the difference at $L = 100$km is about 240%. That highlights the increasing role of postselection for higher transmission distances. We observe a similar behaviour when we optimise over Δ_c for the plot of the maximal achievable secure key rate versus transmission length.

Next, we compare the decrease of the maximal secure key rates for fixed $|\alpha|$ and L and different values of ξ. The maximal secure key rate for $|\alpha| = 0.75$ and $L = 50$km for $\xi = 0.01$ is about 10×10^{-3}, where the corresponding curve for $\xi = 0.02$ attains a maximum secure key rate of about 6.8×10^{-3}. So, the optimal secure key rate drops by a factor of about 1.5. Similarly, we find a factor of about 1.5 when we compare the maximal secure key rates for $|\alpha| = 0.90$. In contrast, if we compare the corresponding curves for $L = 100$km, we find for $|\alpha| = 0.75$ maximal secure key rates of 11×10^{-4} and 9.5×10^{-4}. Thus, the factor drops to approximately 1.15, similarly as for $|\alpha| = 0.90$. Therefore, postselection reduces the relative difference between secure key rates for low and high noise with ascending transmission length L. That can be explained as follows. For $L = 50$km, the optimal secure key rates for $\xi = 0.01$ are obtained (almost) without postselection, while higher values of excess noise, such as $\xi = 0.02$, require Bob to perform postselection (with postselection parameters around $\Delta_c = 0.35$). In contrast, for $L = 100$km Bob has to perform postselection for both values of ξ to obtain the maximal secure key rate and it turned out that the optimal values for the postselection parameters ($\Delta_c = 0.25$ for $\xi = 0.01$ versus $\Delta_c = 0.35$ for $\xi = 0.02$) differ less than for $L = 50$km. Therefore, the reduction of the raw key rate due to postselection is smaller for $L = 100$km compared to $L = 50$km, leading to a smaller difference between the corresponding secure key rates. Thus, we expect the curves for the secure key rate for different values of excess noise to approach closer to each other for higher distances (of course, providing that the parameters allow the calculation of secure key rates at all). This observation underlines the advantage of performing postselection for higher values of excess noise.

Both curves for 100km in Figure 8.2a show a distinct maximum around $\Delta_c = 0.25$ while the curves for $|\alpha| = 1.0$ and $|\alpha| = 0.95$ for $L = 50$km show only a comparably weak maximum around $\Delta_c = 0.30$, and the curve for $|\alpha| = 0.75$ is monotonically decreasing, i.e., attains its global maximum for $\Delta_c = 0$. That supports our observation that for transmission distances of 50km and lower the optimal postselection parameter for the optimal choice of $|\alpha|$, i.e., the parameter-set yielding the highest secure key rate, is $\Delta_c = 0$.

We conclude with a remark about the choices of $|\alpha|$ in Figures 8.2a and 8.2b. The coherent state amplitude $|\alpha| = 0.75$ is close to the optimal value for a transmission length of 50km, according to the theoretical calculations. As can be seen in Figure 8.1, the optimal choice for $|\alpha|$ raises rapidly if one lowers the transmission distances. Hence, the coherent state amplitude has to be adapted accordingly, in order to achieve the maximal secure key rate. Therefore, we additionally examined $|\alpha| = 0.90$, which can be a sound compromise, yielding high secure key rates for most of the relevant transmission lengths.

8.1.2. Comparison of postselection strategies

Now, after confirming the advantageous effect of postselection on the secure key rate and getting an idea of the magnitude for different scenarios, we are going to examine the three postselection strategies introduced in Chapter 2. In the whole section, we fix the excess noise to $\xi = 0.01$. First, we compare the cross-shaped postselection scheme with the radial scheme.

Cross-shaped vs. radial postselection

In the previous section, we learned that cross-shaped postselection does not outperform the secure key rates obtained without postselection for a transmission length of 50km. It turns out that the same applies to distances lower than 50km and that the outperformance starts at about 70km. Accordingly, for transmission lengths below 70km, the optimal values for the parameter of the cross-shaped postselection turn out to be 0 for values below 60km and differs from 0 for $L = 60$km and higher. Therefore, we cannot expect the cross-shaped scheme to outperform the radial scheme in this region as for the radial scheme, for consistency reasons, the secure key rate for the choice $\Delta_r = 0$ is equal to the one for the cross-shaped postselection scheme with $\Delta_c = 0$. Furthermore, the secure key rate for that choice of Δ_r is a lower bound on the maximal achievable secure key rate for the radial postselection scheme, i.e., the maximal secure key rate for transmission lengths lower than 70km cannot be smaller. Therefore, for the first region, the main question will be whether, and if yes, how much the radial postselection scheme performs better. In the second region, where transmission lengths are greater than 60km, we cannot draw similar conclusions in advance.
Figure 8.3 illustrates that both postselection strategies perform very similarly for transmission distances up to 70km, as expected. A more detailed analysis shows that the radial strategy outperforms the cross-shaped strategy by about 8% in this region. That is because it turned out that the optimal choice for Δ_r, indeed, is greater than zero. Contrarily, for distances higher than 70km, one observes a definite outperformance of the cross-shaped postselection strategy, compared with the radial strategy, yielding an increase in secure key rate by a factor of up to 5/3. This can be seen in Figure 8.3, where the relative difference between the cross-shaped and the radial scheme turns from negative to positive. We note that, again, we observed a rapid change in the optimal value for the postselection parameter Δ_c, being 0 for $L = 50$km and being 0.25 for $L = 60$km. This can be explained, similarly to Section 8.1.1, by the development of a maximum apart from $\Delta_c = 0$.

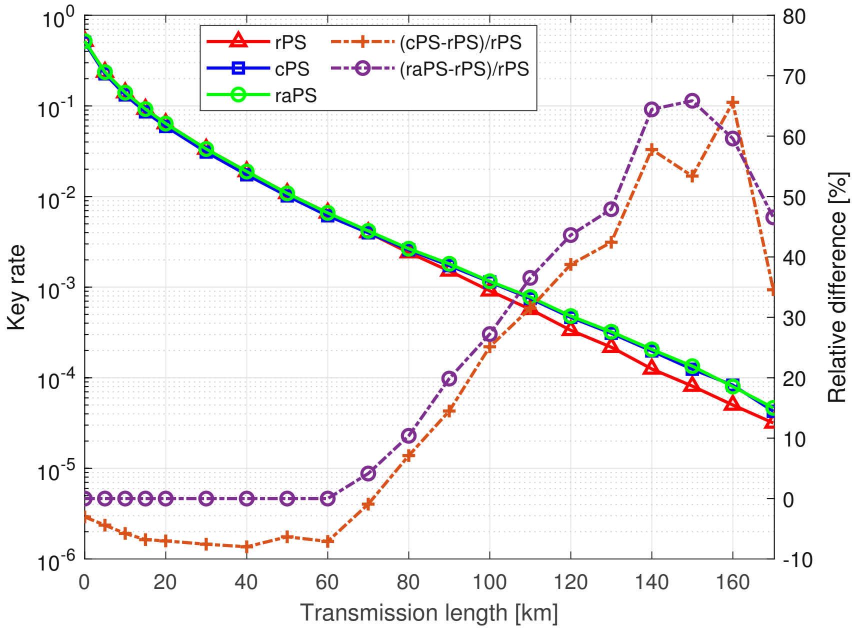


Figure 8.3.: Secure key rates for the untrusted detector for radial, cross-shaped, and radial&angular postselection for $\xi = 0.01$. The secure key rates were optimised via coarse-grained search over $|\alpha|$ and Δ_r, Δ_c or Δ_r and Δ_a, respectively (depending on postselection strategy). The parameter $|\alpha|$ was varied in steps of 0.05 in the interval $|\alpha| \in [0.4, 1.2]$ and the postselection parameters were varied in steps of 0.025 in the intervals $\Delta_c \in [0, 0.45]$, $\Delta_r \in [0, 0.55]$ and $\Delta_a \in [0, 0.35]$. We plotted relative differences (right y-axis) between the secure key rates, obtained with different postselection strategies.

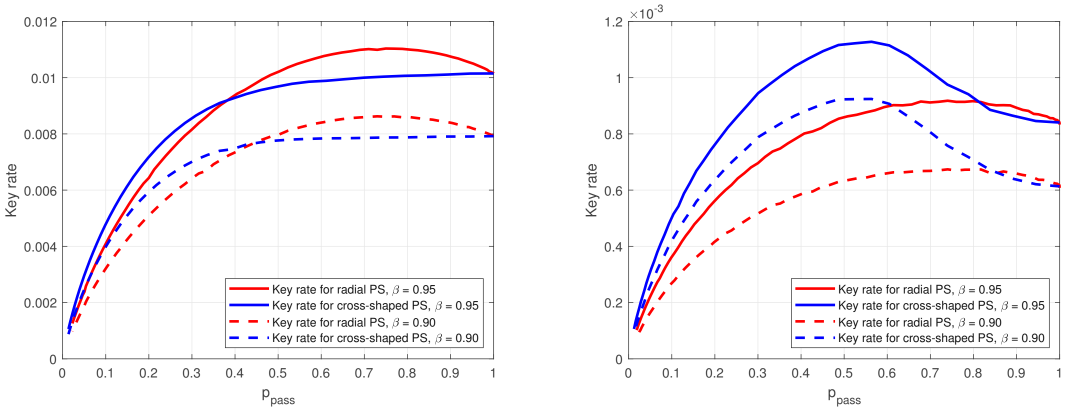
Radial&angular postselection

The comparison between the radial and the cross-shaped postselection scheme confirms the initial presumption that measurement results close to the axis but apart from the origin tend to be faulty. On the other hand, the cross-shaped postselection scheme performs slightly worse for low transmission distances. While the cross-shaped scheme is the simplest and computationally most efficient scheme, one might aim to maximise the secure key rate. An alternative scheme that has the potential to combine the advantages of both the radial and the cross-shaped scheme is the third scheme, introduced in Chapter 2 with radial&angular postselection. Figure 8.3 shows that the radial&angular scheme performs very similar to the cross-shaped postselection scheme for distances higher than 60km and yields the same secure key rates as the radial postselection scheme for transmission distances lower or equal to 60km. In particular, our research shows that the optimal choice for the angular postselection parameter Δ_a differed from 0 only for transmission lengths higher than 60km.

Note that the difference between the radial&angular and the radial scheme in Figure 8.3 for lengths of 70km and lower is 0. Therefore, the curve corresponding to the relative difference drops to zero at 70km. This is because for distances lower than 70km, the optimal choice for the angular postselection parameter is $\Delta_a = 0$. Summing up, the radial&angular scheme succeeds over the whole examined interval between 0 and 180km. Our result is opposed to [29], where they state that angular postselection has no significant effect on the secure key rate. According to our examination, this is only true for low transmission lengths, but does not hold for medium and high distances. According to the examinations for the noiseless channel, one can expect a negative impact of regions in the phase-space, lying close to the axes. If we add (untrusted) noise, we do not expect a positive impact on the secure key rate. In particular, we anticipate a higher error rate for measurement results close to the axes, which are the boundaries between regions, associated with different key values. Hence, we assume that omitting results close to the axes has a positive impact on the secure key rate, which is in accordance with our numerical results.

8.1.3. Influence of the probability to pass the postselection step on the secure key rate

Next, we are going to have a more detailed view on the cross-shaped and the circular postselection. Therefore, we fix $|\alpha| = 0.7$ and compare both postselection strategies for $L = 50$km, where the radial scheme has the edge over the cross-shaped postselection scheme, and for $L = 100$km, where the cross-shaped strategy



(a) $L = 50\text{km}$

(b) $L = 100\text{km}$

Figure 8.4.: Secure key rates versus probability to pass the postselection phase for radial and cross-shaped postselection schemes for $|\alpha| = 0.7$. The excess noise was set to $\xi = 0.01$ and we plot curves for $\beta = 0.95$ and $\beta = 0.90$. The curves were obtained varying the postselection parameters Δ_r and Δ_c in the intervals $\Delta_r \in [0, 2]$ and $\Delta_c \in [0, 1.125]$ with step-sizes of 0.025

has an advantage concerning maximising secure key rates. In Figures 8.4a and 8.4b, we plotted the achievable secure key rates over p_{pass}, which is the probability of passing the postselection phase for two different values for the reconciliation efficiency, $\beta = 0.90$ and $\beta = 0.95$. Note that $1 - p_{\text{pass}}$ is the fraction of signals which is removed by the postselection, and hence is not fed into the error correction and privacy amplification routines.

For $L = 50\text{km}$ (see Figure 8.4a), we find that the radial postselection scheme achieves greater secure key rates, which confirms our earlier results. The curve representing the radial scheme attains its maximum at $p_{\text{pass}} = 0.75$, while the curve representing the cross-shaped scheme increases monotonically, obtaining its maximum at $p_{\text{pass}} = 1$. This coincides with our previous results, stating that the optimal choice for low transmission distances is $\Delta_c = 0$. Furthermore, we observe that for passing probabilities lower than 37.5%, the cross-shaped scheme yields greater secure key rates than the radial scheme.

For $L = 100\text{km}$ (see Figure 8.4b), we observe a totally different behaviour. Here, the cross-shaped postselection scheme outperforms the radial scheme in the interval $[0, 0.8]$ very clearly and attains a much higher maximum than the radial scheme. Again, this is in accordance with our earlier results. Furthermore, we observe that the maximum of the cross-postselection scheme is attained at $p_{\text{pass}} = 0.55$, while the (much lower) maximum of the radial scheme is attained at $p_{\text{pass}} = 0.8$. Therefore, using the cross-shaped postselection strategy, the secure key rates are increased by about 35%, while simultaneously the raw key is reduced by almost 50%. That reduces the data required to undergo classical error correction and privacy amplification steps considerably and is a clear advantage for the cross-shaped postselection scheme, as the computations for those steps often are bottlenecks in practical systems. For reference, in [28] they report for the radial postselection scheme at $L = 75$km to reduce the raw key by $20-30\%$ while increasing the secure key rate by $5-8\%$, which highlights the advantage of the cross-shaped scheme over the radial scheme.

One can think this idea even further. If one aims to reduce the raw key drastically, for example, by 65% or even more, the cross-shaped scheme yields higher secure key rates both for lengths of 50km and 100km. Therefore, if one aims to remove 80% of the raw key, for $L = 50$km the secure key rate drops merely by about 20%, compared to the case without postselection. For 100km, the secure key rate is almost the same as without postselection, if one reduces the raw key by 80%.

Summing up, the cross-shaped postselection strategy performs slightly worse than the radial strategy for low distances but shows a distinct outperformance for higher transmission distances. The cross-shaped scheme yields higher secure key rates than the radial scheme if one chooses low passing probabilities. The observed effects do not depend on the reconciliation efficiency β. Additionally, the cross-shaped postselection strategy is easy to implement in real-world systems, as heterodyne detectors directly measure the p- and q-quadrature. Therefore, the cross-shaped postselection can be applied directly to the measurement results without any further computations.

8.2. Postselection strategies for trusted detectors

In this section, we examine the three different postselection strategies in the trusted noise scenario. For the whole chapter, we used $\eta_d = 0.72$ and $\nu_{el} = 0.04$, which coincide with the early stage data of a practical CV-QKD system currently built at AIT.

It turns out that the optimal choice of the coherent state amplitude $|\alpha|$, depending on the transmission length L, in the trusted detector scenario is identical to the values obtained for the untrusted detector scenario, given in Figure 8.1. Therefore, we proceed by examining the cross-shaped postselection scheme for the trusted detector scenario.

We begin by examining the cross-shaped scheme, followed by a comparison with other postselection strategies.

8.2.1. Cross-shaped postselection

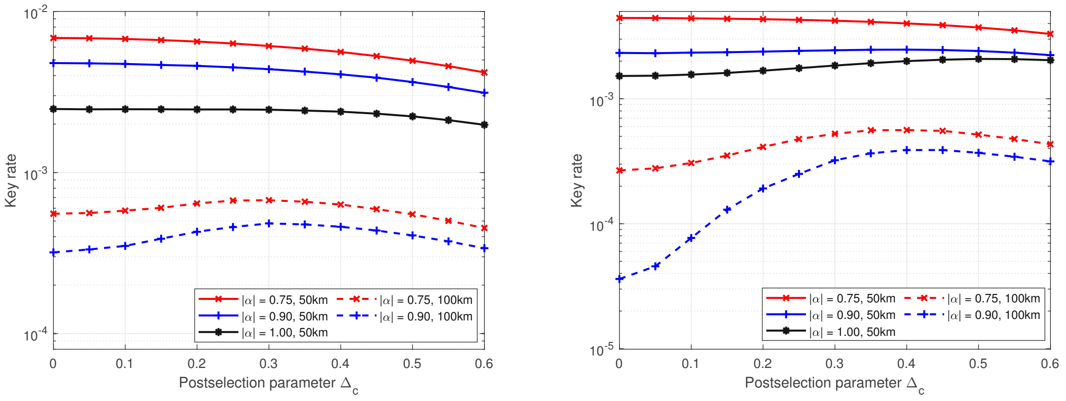
Similar to the preceding sections, we are interested in the secure key rates as a function of the postselection parameter Δ_c for fixed transmission lengths L and values of excess noise ξ. Recall that we measure both the excess noise and the electronic noise in shot noise units and fix the reconciliation efficiency β to 0.95 for the whole section.

For the sake of consistency, we chose to investigate the secure key rates for transmission distances of $L = 50$km and $L = 100$km with excess noise $\xi = 0.01$ and $\xi = 0.02$, which are the same values as in the investigation of the untrusted detector scenario. In addition to the excess noise, we have trusted electronic noise, so the curves investigated in this section have a higher total noise compared to those we examined in the untrusted scenario. Furthermore, now we consider non-ideal detectors. Therefore, we expect lower secure key rates than in the previous section.

With one little exception, the curves in this section show very small gaps between the first and the second step of the secure key rate calculation, indicating that the bounds on the secure key rates are tight.

For $L = 50$km, we observe a very similar behaviour as in the previous chapter (see solid lines in Figures 8.5a and 8.5b). The curves for $\xi = 0.01$ do not show a distinct maximum at all, so the maximal secure key rate is attained for $\Delta_c = 0$, which means no postselection. If we increase the excess noise to $\xi = 0.02$, we see that the curve for $|\alpha| = 0.90$ forms a maximum, but the curve for $|\alpha| = 0.75$, which, is the (theoretical) optimal value for the coherent state amplitude for a transmission distance of $L = 50$km, does not. Afresh, we conclude that the optimal choice of Δ_c does not grow slowly from $\Delta_c = 0$ to larger values, but changes rapidly from zero to values around $\Delta_c = 0.4$, when the maximum starts to shape. So, when searching for the optimal value of Δ_c, one has to be careful and needs to examine the whole interval for every transmission distance, and not only values of Δ_c that are close to the optima for neighbouring values of L, as 'flat' secure key rate curves without distinct maximum start to form a distinct maximum within a small interval.

For $L = 100$km, the curves show pronounced maxima for both choices of $|\alpha|$, where



(a) $\xi = 0.01$

(b) $\xi = 0.02$

Figure 8.5.: Secure key rate vs. Δ_c for $L = 50$km (solid lines) and $L = 100$km (dashed lines) and various $|\alpha|$ in trusted detector scenario. Chosen detector parameters $\eta_d = 0.72$, $\nu_{el} = 0.04$.

we observe that increasing ξ shifts the maximum to the right, i.e., the maximal secure key rates are obtained with higher values of the postselection parameter Δ_c. This is in accordance with our observations in the untrusted detector scenario and with the notion that higher noise requires more postselection.

In general, these results are in accordance with our expectations, as we did not suppose significant impact of the trusted detector assumption on the qualitative behaviour of the secure key rate curves. Hence, all considerations carried out in section 8.1.1 stay valid for the trusted detector scenario.

8.2.2. Comparison of postselection strategies

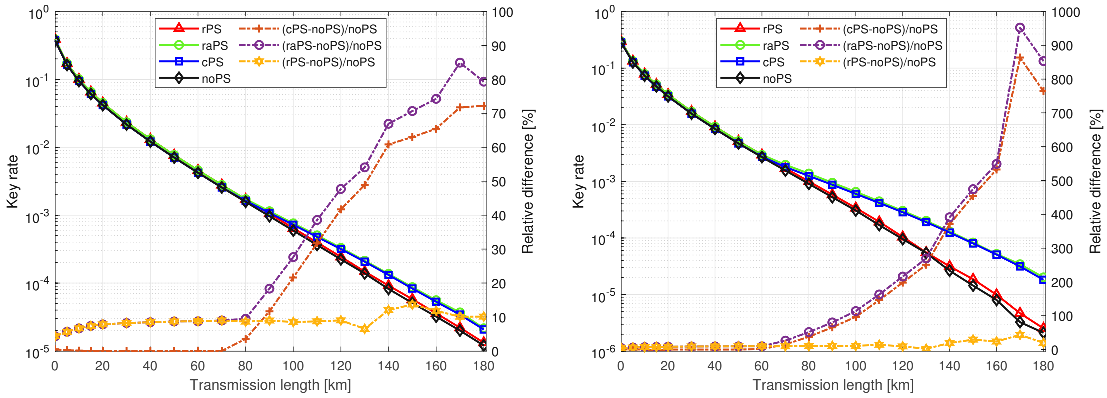
Finally, we are going to examine the effect of the three different postselection strategies on the secure key rates. Therefore, we investigated $\xi = 0.01$ and $\xi = 0.02$ and optimized the secure key rate over the coherent state amplitude $|\alpha|$ and the postselection parameter Δ_c using coarse-grained search in steps of 0.05 for $|\alpha| \in [0.4, 1.2]$ and in steps of 0.025 for the postselection parameters $\Delta_c \in [0, 0.45]$, $\Delta_r \in [0, 0.55]$ and $\Delta_a \in [0, 0.35]$.

Key rates for low values of excess noise ($\xi = 0.01$)

For $\xi = 0.01$ we compare the radial, the cross-shaped and the radial&angular postselection schemes (see Figure 8.6a) and plot both the obtained secure key rates as well as the relative differences of the radial, the cross-shaped and the radial&angular scheme compared to the secure key rates obtained without postselection. The radial postselection scheme yields slightly higher secure key rates than the cross-shaped scheme for transmission lengths $L \leqslant 80$km. The outperformance in this region is smaller than 10%, as indicated by the difference between the corresponding dot-dashed curves in Figure 8.6a. For transmission distances greater or equal than 80km, the cross-shaped postselection scheme starts outperforming the radial scheme by up to 60%, where the advantage raises with increasing transmission length. We note that the cross-shaped postselection strategy starts outperforming the radial scheme around 80km, indicated by the crossing of the dot-dashed brown and the dot-dashed yellow curve in Figure 8.6a.

Summing up, for distances lower or equal to 80km the cross-shaped scheme in the trusted detector scenario performs slightly worse than the radial postselection scheme but has a clear advantage (up to almost 60%) for higher transmission distances. According to our examination, the secure key rates obtained with radial postselection for $\xi = 0.01$ are up to 13% (dot-dashed yellow curve in Figure 8.6a) higher than those without any postselection. Contrarily, the cross-shaped postselection strategy shows an improvement of about 70% compared to the case where we do not perform postselection at all (dot-dashed brown curve in Figure 8.6a). As the choice $\Delta_c = 0$ includes the case without postselection, the secure key rate obtained using the cross-shaped postselection scheme is always an upper bound for the secure key rates obtained without postselection. Furthermore, the comparison between the radial and the cross-shaped scheme in section 8.1.2 for the untrusted detector scenario stays valid. In particular, the cross-shaped postselection scheme yields higher secure key rates than the radial postselection scheme if one decides to cut out large parts of the raw key, reducing the amount of data to be processed in the error correction phase.

The radial&angular postselection scheme combines the advantages of the other two schemes. Ithas the same performance as the radial scheme for low transmission distances, as the optimisation shows that for transmission lengths lower than 80km the optimal choice for the angular postselection parameter Δ_p is zero. Therefore, the dot-dashed purple curve, representing the relative difference of the secure key rates obtained using the radial&angular postselection scheme with the secure key rates obtained without postselection, in Figure 8.6a, overlaps with the dot-dashed yellow curve representing the corresponding relative difference for the radial post-



(a) $\xi = 0.01$, $N_{FW} = 30$

(b) $\xi = 0.02$, $N_{FW} = 150$

Figure 8.6.: Secure key rate vs. transmission length L for different postselection schemes and with detector parameters $\eta_d = 0.72$ and $\nu_{el} = 0.04$. The secure key rates were optimised via coarse-grained search over $|\alpha|$ and Δ_r, Δ_c or Δ_r and Δ_a (depending on the postselection strategy). $|\alpha|$ was varied in steps of 0.05 in the interval $|\alpha| \in [0.4, 1.2]$ and the postselection parameters were varied in steps of 0.025 in the interval $[0, 0.55]$. Furthermore, we plotted relative (dot-dashed lines) differences between the key rates obtained with radial postselection, cross-shaped postselection and radial&angular postselection, where the reference is the secure key rate obtained without postselection. The right y-axis depicts the relative differences.

selecton strategy. For higher transmission distances the radial&angular scheme has a clear advantage of up to 70% over the radial scheme and performs comparable to the cross-shaped postselection scheme, as shown by the violet dashed line in Figure 8.6a. The advantage over the secure key rates obtained by radial postselection grows with raising L and is slightly greater than the advantage of the secure key rates obtained by cross-shaped postselection over those obtained by radial postselection. The advantage over the secure key rates calculated without any postselection is up to 85%, as displayed by the dot-dashed purple curve in Figure 8.6a.

Key rates for medium values of excess noise ($\xi = 0.02$)

We observe qualitatively similar results for $\xi = 0.02$, but find that the difference between the radial scheme and the other schemes intensifies (see Figure 8.6b). Note that we had to increase the number of Frank-Wolfe iterations to $N_{FW} = 150$ as for $N_{FW} = 30$ we observed large gaps between the results of the first and the second step, indicating that the algorithm terminated reaching the iteration limit. Again, the cross-shaped and the radial&angular scheme are clearly ahead the radial postselection scheme. As visualised by the dot-dashed purple and brown lines in Figure 8.6b, the outperformances of the cross-shaped and the radial&angular postselection scheme, compared to the radial scheme or the case without any postselection is apparent. In concrete numbers, one observes an increase in the secure key rate of up to outstanding 900% comparing the cross-shaped or the radial&angular postselection strategy with the case without postselection and an increase of up to 700% compared with radial postselection. So, the secure key rate can be increased by a factor of up to 9 when choosing an optimised postselection strategy, compared to no postselection. For $\xi = 0.02$ the ratio between the secure key rates obtained with radial postselection and those obtained without any postselection is up to 23%, according to our investigation (dot-dashed yellow curve in Figure 8.6b). Therefore the increase in the secure key rate for the radial postselection strategy compared to the secure key rate obtained without postselection is comparably small.

The differences between the cross-shaped and the radial&angular scheme are small, with little advantage for the radial&angular scheme. Furthermore, note that the distances where the cross-shaped and the radial&angular postselection strategies start outperforming the radial scheme are now around 70km, i.e., were shifted to the left compared to the plot for $\xi = 0.01$. This means both the cross-shaped and the radial&angular postselection scheme start outperforming the radial scheme earlier, i.e., at lower transmission distances. This meets our expectations, as more noise increases the demand for postselection already at lower distances. We expect

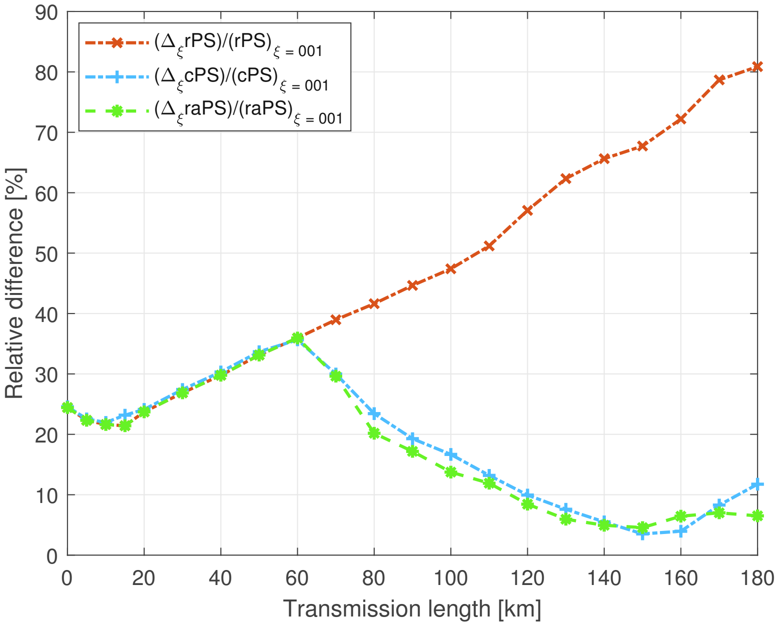


Figure 8.7.: Relative differences between the secure key rates for excess noise $\xi = 0.01$ and $\xi = 0.02$ using various postselection strategies in the trusted detector scenario. Here Δ_ξxPS is a short notation for the difference between the secure key rates obtained for $\xi = 0.01$ and $\xi = 0.02$ using the postselection strategy 'x', where $\mathrm{x} \in \{\mathrm{r}, \mathrm{c}, \mathrm{ra}\}$. Furthermore, $(\mathrm{xPS})_{\xi=0.01}$ denotes the secure key rate obtained with 'x' postselection for $\xi = 0.01$. The same applies for $(\mathrm{xPS})_{\xi=0.02}$ with excess noise $\xi = 0.02$.

that this shift to lower distances proceeds, if one increases the excess noise further.

Sensitivity of the key rate on the noise level

When comparing the results for $\xi = 0.01$ and $\xi = 0.02$ one observes another interesting behaviour of the three different postselection strategies. In Figure 8.7, we plot the relative differences between the obtained secure key rates for fixed postselection strategies but different values of excess noise.

While, following our expectations, the secure key rates for higher values of excess noise are lower, the gap between the secure key rates behaves differently for different postselection strategies. The relative difference between the secure key rates for $\xi = 0.01$ and $\xi = 0.02$ when using the radial strategy raises with increasing transmission distance, being maximal for the highest examined values of L, reaching a relative difference of about 80%. In contrast, the relative difference between the secure key rates for $\xi = 0.01$ and $\xi = 0.02$ for the cross-shaped and the radial&angular postselection strategy increase up to $L = 60$km reaching a relative difference of about 35% and decrease for higher distances, ending up at relative differences lower than 10%. Note that the calculated cPS and raPS secure key rates for $L < 60$km are less than or equal to the secure key rates obtained using the radial postselection strategy. Recall that we found out that the optimal choice for the angular postselection parameter in the radial&angular postselection strategy differs from zero only for distances greater than 60km. Similarly, recall that the cross-shaped scheme outperforms the radial postselection strategy for distances greater than 60km. This explains the bend in the relative differences in Figure 8.7 at 60km. Therefore, the decrease in the relative difference between the secure key rates for $\xi = 0.01$ and $\xi = 0.02$ for the cross-shaped postselection strategy and the radial&angular scheme for distances higher than 60km are evidently linked with the postselection of measurement results with low absolute q or p value, which takes place in those strategies, but not in the radial scheme. As higher values of excess noise result in higher probabilities for bit-flips, it is understandable that omitting measurement results that lie close to the axes (hence have a higher chance of being detected in the wrong sector) increases the secure key rate. This explains the clear and distinct outperformances compared to the radial postselection strategy. Hence, choosing a proper postselection routine can lower the negative influence of high excess noise on the secure key rates, especially for high transmission distances, considerably.

Resumé for the trusted dectector scenario

For the trusted detector scenario, the key rate obtained with the radial&angular strategy yields the highest secure key rates for all examined values of excess noise and transmission length. The latter performs merely slightly worse and outperforms the radial postselection clearly.The outperformance of the cross-shaped and the radial& angular postselection schemes compared to the radial scheme for higher transmission distances can be explained by the postselection of measurement results close to the borders of the key map. For channels without noise a similar behaviour has can be observed for noiseless channels, based on a security proof given in [46]. As the scenario of no postselection is included in every of the mentioned schemes by choosing all corresponding postselection parameters equal to zero, it is evident that all secure key rates obtained with postselection are upper bounds on the secure key rates without postselection.

In contrast, if one aims to reduce the computational effort of the postprocessing steps, one may choose the cross-shaped postselection strategy without a significant drop in the secure key rate.

9. Results for eight-state protocols

In this chapter, we present the results and findings for the eight-state protocol, where, due to increasing computational effort compared to the four-state variants, we chose to investigate only the untrusted detector scenario. Nevertheless, similar to the results in the previous chapter for four-state protocols, we expect comparable results for the trusted detector scenario. We conduct the examination for eight-state protocols very similarly to the examinations for four-state protocols, but, for symmetry reasons, we cannot implement a cross-shaped postselection strategy for eight-state protocols. Therefore, we focus our efforts on the investigation of the radial&angular scheme, but go into more detail regarding different noise-levels. This chapter was published by the author in [24], where it makes up the 'Results' part of the paper.

9.1. Finding the optimal coherent state amplitude

First, we have to find the optimal choice for coherent state amplitude $|\alpha|$, which might differ from the theoretical prediction for the loss-only channel (see Figure 7.2b). Therefore, we carry out a coarse-grained search in steps of size 0.05 in the interval $|\alpha| \in [0.75, 1.60]$, where the interval is chosen slightly bigger than the relevant range for $|\alpha|$ according to the theoretical prediction. We investigated lengths between 5km and 180km and excess-noise levels of $\xi = 0.01$ and $\xi = 0.02$, while we do not perform any postselection. In Figure 9.1 we plot the results of the coarse-grained search and give the theoretical prediction according to Section 6.2 as reference-curve. As expected, the optimal coherent state amplitude for noisy channels is slightly lower than those for a loss-only channel, but is still close to the theoretical prediction. We observe that the optimal choice for the coherent state amplitude decreases with increasing transmission distance, hence with increasing losses. This is in accordance with our expectations, as for high losses Eve receives a much stronger signal than Bob, whose signal has to pass the whole optical fibre, while Eve is assumed to extract Alice's signal right after leaving her lab. Hence, the amplitude has to be small for high transmission distances to keep Eve's advantage as small as possible. Based on our observations, it turns out that it is

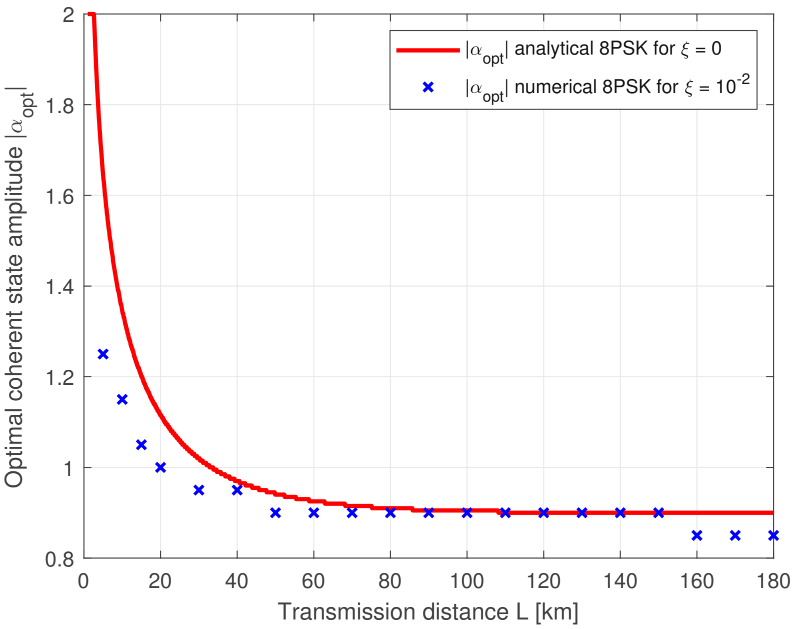


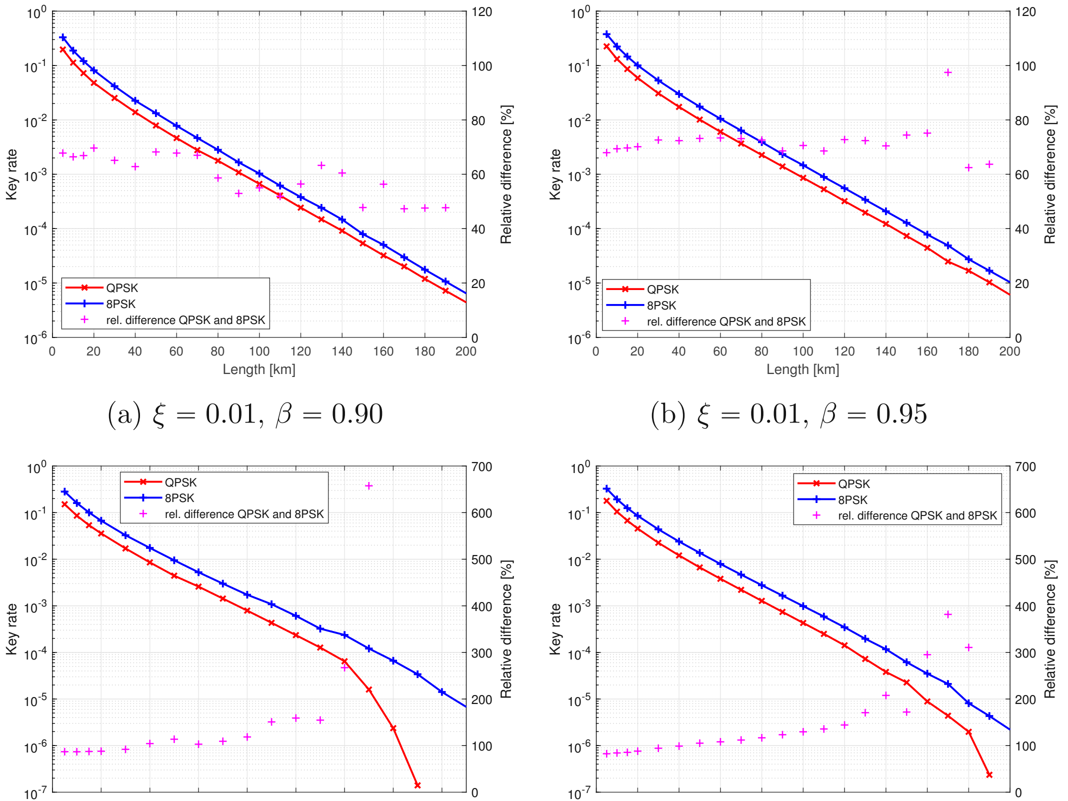
Figure 9.1.: Optimal choice of the coherent state amplitude $|\alpha|$ for $\xi > 0$ obtained by coarse-grained search compared to predicted optimal choice for loss-only channel. As our results for $\xi = 0.01$ and $\xi = 0.02$ do not differ significantly, we plot only the data points for $\xi = 0.01$.

sufficient to search $|\alpha_{\mathrm{opt}}|$ around the theoretical prediction. Furthermore, we note that the found optimal $|\alpha|$ does not differ significantly for all examined values of excess noise. In general, we notice that the optimal coherent state amplitude is higher than the corresponding value for QPSK protocols (see 8). We will use these optimal values for the coherent state amplitude for all calculations in the present chapter, if not stated otherwise.

9.2. Secret key rates for 8PSK protocols

Next, we examine the achievable secret key rates, using the optimal values for the coherent state amplitude from the previous section. First, we give the obtained secret key rates for transmission lengths up to 200km and various values of excess-noise without any postselection and compare the results to the achieved key rates for the QPSK protocol without postselection. In Figure 9.2, we show the obtained secure key rates for $\xi = 0.01$ and $\xi = 0.02$ and reconciliation efficiencies of $\beta = 0.90$ and $\beta = 0.95$ for both protocols and plot the relative difference between the key rates on the secondary y-axis. For $\xi = 0.01$, one observes an outperformance of the 8PSK protocol compared to the QPSK protocol of about 40 to 70% if the reconciliation efficiency is chosen to be $\beta = 0.90$ and of about 70 to 80% for $\beta = 0.95$, where the relative difference shows only a little dependency on the transmission distance. For $\xi = 0.02$, we obtained higher relative differences of about 100% for transmission distances up to 110km for both values of reconciliation efficiency β. For higher transmission lengths, the relative difference increases notably as the higher noise level causes a significant drop in the secure key rate for the QPSK protocol. We note that for transmission distances of 140km and higher the gap between step 1 and step 2 increases slightly for the eight-state protocol, while the gap remains small for the four-state protocol, except for the regions where the key rates drop steeply. This is due to numerics and may be improved. As step 2 serves as a lower bound on the key rate, this decreases the bound for the 8PSK protocol. Therefore, we expect even a slightly higher outperformance (i.e., a higher relative difference) for transmission distances greater than 140km if the gap can be narrowed down.

Finally, we examine the influence of postselection on the secure key rate. By construction, postselection omits some fraction of the measurement results. It is expected to contribute significantly to the overall key rate, in particular for high transmission distances, where the signal losses are high, hence Eve has a much stronger signal than Bob. This is because Eve is assumed to grab her share of the signal before it enters the quantum channel, hence her signal has not experienced any losses or noise, while Bob's signal did. Therefore, the communicating parties try to reduce Eve's information about the key by lowering the signal amplitude and using postselection to reduce parts of the key, where Eve might have gained more information than the communicating parties. Additionally, we expect postselection also to be advantageous in order to mitigate Eve's edge due to the channel noise. While postselection is expected to have a positive influence on the key rate, obviously, choosing the postselection-areas too large results in a decrease in the secure key rate, as parts of the key that could have been used to generate a secret key were omitted. Therefore, one can expect to find some sweet-spot, where the secret key rate can be increased maximally. Note that the case without postselection is included in every postselection scheme by setting the postselection parameter $\Delta = 0$. As the calculations for eight-state protocols involve solving very high-dimensional semi-definite programs, hence are computationally very expensive, we chose to focus on the investigation of influence of the radial postselection parameter Δ_r on the key rate. Therefore, we perform coarse-grained search and vary Δ_r with step-sizes of 0.05 in the interval $\Delta_r \in [0, 0.65]$ which turned out to be sufficient to find the maximal secret key rate. In Figure 9.3, we plotted



(a) $\xi = 0.01$, $\beta = 0.90$

(b) $\xi = 0.01$, $\beta = 0.95$

(c) $\xi = 0.02$, $\beta = 0.90$

(d) $\xi = 0.02$, $\beta = 0.95$

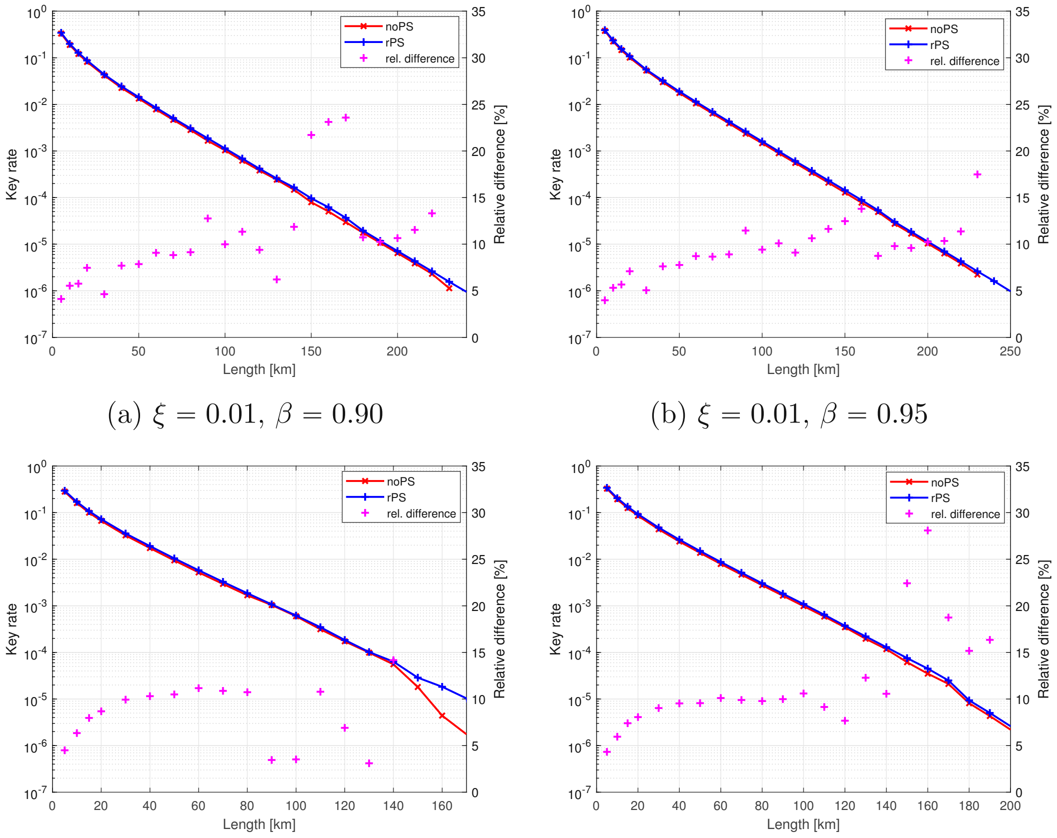
Figure 9.2.: Comparison of the obtained secure key rates for QPSK and 8PSK protocol without performing postselection for two different values of $\xi \in \{0.01, 0.02\}$ and $\beta \in \{0.90, 0.95\}$. The secondary y-axis shows the relative difference between the second steps of the secure key rate, calculated for the 8PSK and the QPSK protocol. Missing data points correspond to data point where the calculation for the protocol without any postselection did not lead to positive key rates after the second step.

both the result without postselection and with radial postselection for transmission distances up to 250km (in steps of 10km) for excess-noise levels of $\xi = 0.01$ and $\xi = 0.02$. The secondary y-axis shows the relative difference between both curves. For $\xi = 0.01$ and $\beta = 0.95$ we observe relative differences of about 5% for very low transmission distances and up to 14% for high transmission lengths, while the relative outperformance starts at 5% for low transmission distances and goes up to 25% for medium to high transmission distances for $\beta = 0.90$. We see qualitatively similar results for $\xi = 0.02$. As expected, based on our findings for four-state protocols, radial postselection increases the secure key rate for all transmission distances, as the case without postselection is included in the radial postselection scheme by setting $\Delta_r = 0$. Furthermore, we observe an increasing impact on the secure key rate for high transmission distances, and higher values of excess noise. We note that the exact value of the relative outperformance is influenced by the gap between step 1 and step 2, in particular for higher transmission distances. Therefore, we expect that numerical improvements would lead to smoother absolute- and relative difference curves.

9.3. Influence of the probability to pass the postselection

In the previous section, we showed that one can increase the secure key rate of eight-state phase-shift keying protocols by applying radial postselection, and we investigated the magnitude of the increase in key rate. Besides maximising the secure key rate, experimentalists might aim to reduce the raw key to reduce the effort of the error-correction phase, which is known to be computationally expensive. Therefore, it can be interesting to examine the relation between the achievable secure key rate and the probability to pass the postselection phase p_{pass} (or, alternatively, the probability of being postselected $1 - p_{\text{pass}}$) in order to know either the reduction in raw key for some fixed (for example, the maximal) key rate or to know the key rate for some given raw key reduction.

Therefore, we fixed $L = 50$km and $|\alpha| = 0.90$ (which, according to Figure 9.1, is the optimal value for 50km) and varied the radial postselection parameter Δ_r in the interval $[0, 2.15]$ with a step-size of 0.05. We investigated four different values of excess-noise, $\xi \in \{0.01, 0.02, 0.03, 0.04\}$, and two different values for the reconciliation efficiency, $\beta = 0.90$ and $\beta = 0.95$, which are the relevant values for many QKD systems. We note that $\beta = 0.95$ can be achieved with low-density parity-check codes. We plot our results in Figure 9.4, where Figure 9.4a shows the secure key rates for $\beta = 0.90$ and Figure 9.4b shows the results for $\beta = 0.95$. As



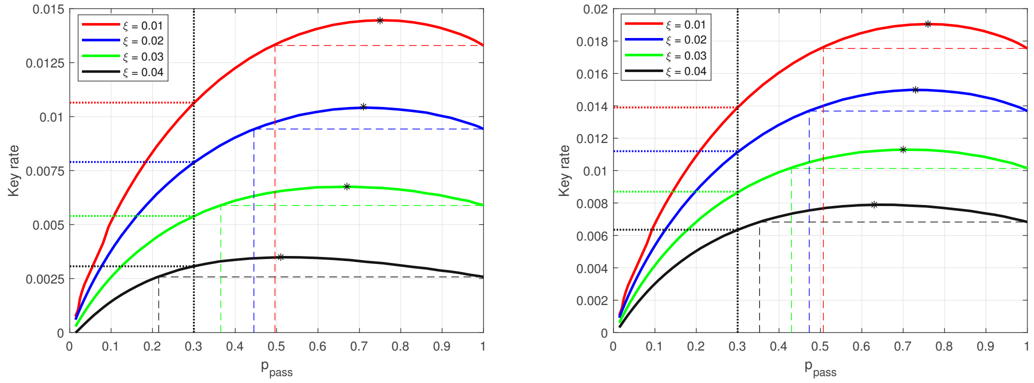
(a) $\xi = 0.01,\ \beta = 0.90$

(b) $\xi = 0.01,\ \beta = 0.95$

(c) $\xi = 0.02,\ \beta = 0.90$

(d) $\xi = 0.02,\ \beta = 0.95$

Figure 9.3.: Comparison of secure key rates for transmission distances up to 250km between an 8PSK protocol without postselection and with radial postselection for $\xi \in \{0.01, 0.02\}$ and $\beta \in \{0.90, 0.95\}$. The secondary y-axis displays the relative difference between the key rates obtained with radial postselection and without postselection. Missing data points correspond to data point where the calculation for the protocol without any postselection did not lead to positive key rates after the second step.



(a) $\beta = 0.90$

(b) $\beta = 0.95$

Figure 9.4.: Secure key rate versus the probability to pass the postselection phase p_{pass} for radial postselection and for four different values of excess noise. The underlying data was calculated varying the postselection parameter Δ_r in the interval $[0, 2.15]$ with a step size of 0.025.

the gap between the first and the second step turned out to be very small, we plot only our results for the second step, as that serves as lower bound on the secure key rate. We note that the achieved maximal key rates for $\xi = 0.01$ and $\xi = 0.02$ coincide with those reported for $L = 50\text{km}$ in the previous section.

We start with a discussion of Figure 9.4b, where the reconciliation efficiency is $\beta = 0.95$. We observe that the maxima are shifted to the left for increasing excess-noise, meaning that a higher noise-level requires more postselection to obtain the maximal key rate, which meets with our expectations. For example, the maximum for $\xi = 0.01$ (red curve) is attained at $p_{\text{pass}} = 0.76$ while the maximum for $\xi = 0.04$ (black curve) is attained at $p_{\text{pass}} = 0.63$. For $\xi = 0.01$ the secure key rate obtained without postselection ($p_{\text{pass}} = 1$) is equal to the secure key rate for $p_{\text{pass}} = 0.51$. So, one can achieve the same secure key rate as without performing postselection, while almost halving the data that has to be error-corrected. This effect intensifies for increasing noise-levels, as for $\xi = 0.02$ the secure key rate for $p_{\text{pass}} = 0.47$ is equal to the secure key rate without performing postselection and for $\xi = 0.03$ we find even $p_{\text{pass}} = 0.43$. Finally, for $\xi = 0.04$ one obtains $p_{\text{pass}} = 0.34$.

The curves for $\beta = 0.90$ in Figure 9.4a show a similar behaviour, but are lower and flatter than those for $\beta = 0.95$. This results in a even more clear advantage with respect to postselection. For example, for $\xi = 0.01$ (red curve) the point, where the secure key rate is equal to the secure key rate without performing postselection, is at $p_{\text{pass}} = 0.50$, so shifted to the left, compared to the curve for $\beta = 0.95$. We make

	p_{pass} (at max. key rate)		p_{pass} (same key rate as noPS)	
ξ	$\beta = 0.90$	$\beta = 0.95$	$\beta = 0.90$	$\beta = 0.95$
0.01	0.75	0.76	0.50	0.51
0.02	0.71	0.73	0.44	0.47
0.03	0.67	0.70	0.36	0.43
0.04	0.51	0.63	0.21	0.34

Table 9.1.: Summary of results for secure key rate vs. probability to pass the postselection for two different values of β and four different values of excess noise. The second and third column show the value of p_{pass}, when obtaining the maximal secure key rate. In the last two columns, one finds the value for p_{pass} where the key rate has the same value as one obtains without performing postselection. So, one is left with exactly the share of the raw key given in the corresponding cell, while obtaining the same secure key rate as without performing postselection at all.

	Change in secure key rate	
ξ	$\beta = 0.90$	$\beta = 0.95$
0.01	-20%	-21%
0.02	-16%	-19%
0.03	-8%	-14%
0.04	$+19\%$	-8%

Table 9.2.: Change in the secure key rate when omitting 70% of the raw key compared to the secure key rate obtained without performing postselection for two different values of β and four different values of excess noise.

similar observations for $\xi = 0.02$ (blue curve), where the corresponding point can be found at about $p_{\text{pass}} = 0.44$, for $\xi = 0.03$, where the point is at $p_{\text{pass}} = 0.36$, as well as for $\xi = 0.04$, where at $p_{\text{pass}} = 0.21$ one has the same secure key rate as without performing postselection.
Contrarily, if we choose to omit 70% of the raw key, the secure key rate for $\xi = 0.03$ drops only slightly and for $\xi = 0.04$, we observe even an increase in the secure key rate of about 19%. For $\xi = 0.02$ we observe a drop of about 16% and for $\xi = 0.01$ the drop makes up about 20%.

9.4. Conclusion and discussion of the 8PSK examinations

We investigated the achievable secure key rates for the proposed 8PSK protocol, using a recent numerical security proof technique, and showed that it yields about $70-80\%$ higher key rates than a QPSK protocol with a comparable protocol structure. With the present method for calculating secure key rates, we were able to calculate secure key rates up to 250km (for excess-noise of $\xi = 0.01$), which is about 25% higher than for the QPSK protocol. Therefore, eight-state phase-shift keying protocols increase both the achievable secure key rate and the achievable range of continuous-variable quantum key distribution systems with phase-shift keying modulation. We showed that radial postselection can increase the secure key rate up to 14% compared with no postselection. Finally, we investigated the relation between secure key rates and the probability to pass the postselection, which is equal to the fraction of symbols of the raw key that have to be error-corrected. Error-correction is a computationally expensive task and therefore a known bottleneck for many practical implementations of QKD systems. We showed how radial postselection for 8PSK protocols can reduce the raw key significantly by $50-80\%$, depending on the level of excess-noise and the reconciliation efficiency, yielding the same secure key rate as one obtains without performing postselection at all. This addresses the computational issues of the error-correction phase directly by reducing the data for the error-correction phase, and can be implemented easily both in new and existing CV-QKD systems.

10. Summary and outlook

In this thesis, we used a recent numerical method to calculate secure key rates of continuous-variable quantum key distribution protocols to investigate different four- and eight-state phase-shift keying protocols, defined in Chapter 2, under the untrusted ideal and the trusted non-ideal detector scenario. The security proof method is summarised in Chapter 3 and the key rate finding problem, which is known to have the form of a semi-definite program, both for the untrusted ideal and the trusted non-ideal detector scenario, including the physical model of the system and the description of the error-correction and postselection phase, is formulated in Chapter 4. There, we state purely analytical expressions for operators relevant for the problem formulation, like the region operators (operators associated to the key map of the chosen postselection strategy) for various protocols and for both scenarios. The corresponding derivations are given in the appendix. In Chapter 5, we discuss details of the implementation of the security proof method, like two ways of calculating a feasible starting value for the present optimisation problem. The first method utilises a model for a Gaussian channel to determine a possible state on Bob's side and the second method solves another semi-definite program with trivial objective function. In Chapter 6, we adapt a security proof attempt to calculate secure key rates for the examined four- and eight-state protocols for the special case of a noiseless channel. The obtained secure key rates serve to validate our implementation in Chapter 7. There, we show that our code yields very satisfying and plausible results matching excellently with the reference data.

In Chapter 8, we investigate postselection strategies for four-state phase-shift keying protocols. This chapter of the present thesis was published separately in [23]. In the first part, we focus on postselection strategies for untrusted detectors. We examine a new, cross-shaped, postselection strategy, compare it to strategies with radial and radial&angular postselection and show that both the cross-shaped and radial&angular postselection schemes show a clear outperformance compared to the radial scheme. While the radial&angular scheme performs slightly better than the cross-shaped postselection scheme, the cross-shaped scheme is easier to implement and uses directly the output of the measurement devices without requiring any additional calculations. Furthermore, we examined the influence of the probability to pass the postselection phase on the secure key rate. We compared the cross-shaped scheme with the radial scheme and showed that postselection can

be used to address a serious issue of practical implementations of QKD systems, namely that the error-correction phase is computationally expensive and therefore a known bottleneck for many implementations. Postselection can be used to reduce the raw key (and therefore the data that has to be error-corrected) while increasing the secure key rate. One can think about this idea even further: One may reduce the raw key considerably, for example by 70% while the secure key rate does not drop significantly, compared to the secure key rates obtained without performing postselection at all. As the implementation of a suitable postselection strategy does not require any additional hardware, but only small software-adaptations, this idea can be used to address the issues related to the error-correction phase as well as to increase the achievable transmission distances, both in new and in existing QKD systems.
Furthermore, we carried out examinations for the mentioned postselection strategies for trusted detectors and showed that both cross-shaped and radial&angular postselection show a clear outperformance compared to radial postselection and no postselection, in particular for high transmission distances and higher noise-levels.
In Chapter 9, we investigated an eight-state phase shift keying protocol for different noise-levels and two different practically relevant values for the reconciliation efficiency. First, we compared the achievable secure key rates for the 8PSK protocol with the secure key rates obtained for the four state protocol in the no-postselection scnario, and observed a clear outperformance for all examined values for the excess-noise and all examined values for the reconciliation efficiency. Furthermore, we observed that, using the present security proof approach, one achieves considerably higher transmission distances with the 8PSK protocol than with the QPSK protocol. For low values of excess noise and high reconciliation efficiencies we achieved secure key rates up to 230km even without performing postselection. All key rates and maximal transmission distances could be improved, using radial postselection. Finally, we examined the relation between the obtained secure key rates and the probability to pass the postselection phase for the 8PSK protocol with radial postselection for excess-noise levels of $\xi = 0.01 - 0.04$ and for two different practically relevant values of reconciliation efficiency. It turned out that, similar to QPSK protocols, postselection for 8PSK protocols can be used to reduce the raw key significantly, while reducing the secure key rate only moderately, or even increase the secure key rate. This effect increases with raising noise level.

Summing up, in the present thesis we investigated various phase-shift keying protocols and examined the influence of postselection on the secret key rate and the raw key and provides both analytical expressions to improve the accuracy and to speed up the calculation of secure key rates and strategies to increase the secure key rate and the maximal achievable transmission length while reducing the computational effort for the error-correction phase. Nevertheless, there are several interesting paths for further investigation.

10.1. Outlook

First, the increasing gap between step 1 and step 2 for the 8PSK protocol or some of the non-smooth curves in Chapter 8 showed, there is still potential for numerical improvements of the algorithm. A detailed analysis of the mathematical structure of the present key rate finding problem was published very recently [21]. They use facial reduction to develop an efficient and more accurate algorithm for the present problem. It would be interesting to examine the numerical improvements obtained with that method and apply it to our postselection investigations.
Second, the security proof approach used in the present thesis relies on the photon-number cutoff assumption, where we assume that only Fock states up to a certain population number contribute significantly to the key rate. While this assumption seems to be valid, as empirical experiments showed that an increased cutoff number does not change the obtained secure key rates significantly, it is still somehow unsatisfying from a mathematical point of view. It was shown recently [51] that the cutoff assumption can be justified ('removed') by analytical means.
Third, we use a security proof approach for key rates in the asymptotic limit. Therefore, the obvious next step is to aim for finite key rates. Recently it was shown that the numerical security proof approach we use in the present thesis, in principle, can be extended to the finite key regime [14], although the obtained key rates are not tight yet.
Finally, the dimension of the key rate finding problem increases quadratically with the number of states. Therefore, the computation time increases at least quadratically, which sets a limit on the maximal number of signal states. Using the present implementation, we think it would be possible to calculate secure key rates for up to 16 signal states, although the corresponding calculations for single data points are expected to run for days. Calculating key rates for 64 states, or even more, seems to be out of range. A completely different attempt [8] is capable of dealing with considerably higher number of states, but cannot handle postselection. It would be interesting to compare both attempts for a higher number of signal states. As huge parts of our total computation time come from parts of the code that are not under our control (e.g., the SDP solver) or use already fast standard algorithms (Gram-Schmidt orthonormalisation, line-search), we do not expect that numerical improvements lead to a significant speed-up. Therefore, we think that an accurate analysis of the key rate finding problem and the use of symmetries might be a promising way to reduce the problem size.

This brief overview about very recent developments in the field of CV-QKD security proofs in general, and developments directly related to the numerical method we use in this thesis, as well as the plethora of interesting follow-up questions and directions, show the timeliness of the present topic and give a tiny insight on the research currently carried out all over the globe. As the mentioned findings were published within the last few months, to date it was not possible to include all those developments and improvements in our code. Nevertheless, we do not expect significant qualitative changes in our propositions due to these developments. Therefore, we hope that the present thesis and its findings contribute to developing the field of quantum key distribution and offers ways for experimentalists to improve the secure key rate of their QKD systems without requiring additional hardware components.

A. Appendix

A.1. Used symbols

In what follows, we list the symbols that are used in this thesis.

$\mathbb{N}$ denotes the set of natural numbers without 0.

$\mathbb{N}_0$ denotes the set of natural numbers including 0.

$\mathbb{R}$ denotes the set of real numbers.

$\mathbb{R}^+$ denotes the set of positive real numbers.

$\mathbb{C}$ denotes the set of complex numbers.

$\mathcal{H}$ denotes a finite dimensional Hilbert space (over $\mathbb{C}$).

$L(\mathcal{H}_1, \mathcal{H}_2)$ denotes the set of all linear operators, mapping from Hilbert space $\mathcal{H}_1$ to the Hilbert space $\mathcal{H}_2$.

$L(\mathcal{H})$ is a short notation for $L(\mathcal{H}, \mathcal{H})$.

$\mathrm{CP}(\mathcal{H}_1, \mathcal{H}_2)$ denotes the set of all completely positive operators, mapping from Hilbert space $\mathcal{H}_1$ to the Hilbert space $\mathcal{H}_2$.

$\mathrm{CP}(\mathcal{H})$ is a short notation for $\mathrm{CP}(\mathcal{H}, \mathcal{H})$.

$\mathrm{CPTP}(\mathcal{H}_1, \mathcal{H}_2)$ denotes the set of all completely positive, trace preserving operators, mapping a Hilbert space $\mathcal{H}_1$ to another Hilbert space $\mathcal{H}_2$.

$\mathrm{CPTP}(\mathcal{H})$ is a short notation for $\mathrm{CPTP}(\mathcal{H}, \mathcal{H})$.

$\mathrm{Pos}(\mathcal{H})$ is the set of all positive semi-definite operators on a Hilbert space $\mathcal{H}$.

$\mathrm{Herm}(\mathcal{H})$ is the set of all Hermitian operators on a Hilbert space $\mathcal{H}$, i.e., we have $\forall A \in \mathrm{Herm}(\mathcal{H}) : \; A^\dagger = A$.

Σ is an alphabet, i.e., a finite set.

$\mathcal{P}(\Sigma)$ is the set of all probability vectors over an alphabet Σ. This implies that all entries in $p \in \mathcal{P}(\Sigma)$ add up to one.

$\mathcal{D}(\mathcal{H})$ denotes the set of density operators on a Hilbert space $\mathcal{H}$ (see Definition 1.1).

$.^\top$ denotes the transpose of a matrix.

$\bar{.}$ denotes the complex conjugate, see also $.^*$, which is used interchangeably if $\bar{.}$ might be confused with other mathematical symbols, like the average.

$.^*$ denotes the complex conjugate, see also $\bar{.}$, which is used interchangeably.

$.^\dagger$ denotes the hermitian adjoint of an operator $\hat{O} : \mathcal{H}_1 \to \mathcal{H}_2$ between two Hilbert spaces $\mathcal{H}_1, \mathcal{H}_2$. The hermitian adjoint $\hat{O}^\dagger$ is defined by $\langle \hat{O}u, v\rangle_{\mathcal{H}_2} = \langle u, \hat{O}^\dagger v\rangle_{\mathcal{H}_1}$, where $\langle ., .\rangle_{\mathcal{H}_i}$ is the scalar-product of the Hilbert space $\mathcal{H}_i$. If A is a matrix, $A^\dagger = \bar{A}^\top$ holds.

$\geqslant$ denotes, if applied to operators, the non-negativity of this operator. If it is applied to a matrix, it denotes the positive semi-definiteness of this matrix. So for an operator $\hat{A}$, we mean by $\hat{A} \geqslant 0$ that $\hat{A}$ is non-negative and for a matrix M, we mean by $M \geqslant 0$, that M is positive semi-definite.

$\otimes$ denotes the tensor product, i.e., a bilinear function $\otimes : \mathcal{H}^A \times \mathcal{H}^B \to \mathcal{H}^A \otimes \mathcal{H}^B$ with $\dim(\mathcal{H}^A \otimes \mathcal{H}^B) = \dim(\mathcal{H}^A)\dim(\mathcal{H}^B)$.

$\Re(.)$ denotes the real part x of a complex number $z = x + iy \in \mathbb{C}$.

$\Im(.)$ denotes the imaginary part y of a complex number $z = x + iy \in \mathbb{C}$.

$\mathbb{1}_X$ is the identity operator on the space X.

$|.\rangle$ denotes a vector in a Hilbert space $\mathcal{H}$ in Dirac's BraKet notation.

$\langle .|$ denotes a linear-form of a Hilbert space $\mathcal{H}$ (so a member of $\mathcal{H}'$) in Dirac's BraKet notation.

$\langle .|.\rangle$ is defined by $\langle \psi|\phi\rangle := \langle \psi, \phi\rangle_{\mathcal{H}}$ and maps from $\mathcal{H}' \times \mathcal{H}$ to $\mathbb{C}$.

$|.\rangle\langle .|$ is a map from $\mathcal{H}$ to $\mathcal{H}$ and is defined by $|\psi\rangle\langle\phi|\sigma\rangle := \langle\phi|\sigma\rangle\,|\psi\rangle$.

$\langle . \rangle_x$ denotes the expectation value of an operator $\hat{O}$ in the state (associated with) x. For mixed states we describe the state by a density operator ρ. So $\langle \hat{O}\rangle_\rho := Tr(\rho\hat{O})$.

$e^{\cdot}$ denotes the exponential function. If $e^{\cdot}$ is applied on a matrix or an operator A, we mean $e^A := \sum_{n=0}^{\infty} \frac{A^n}{n!}$. This is well-defined for matrices and bounded operators A.

$\log_b(.)$ denotes the logarithm with base b. If $\log_b$ is applied on a matrix, we mean by $\log_b(A)$ the matrix that satisfies $b^{\log_b(A)} = A$. The logarithm of a diagonalisable matrix $M = T^{-1}DT$ reads as follows: $\log_b(M) = T^{-1}\log_b(D)T$.

$\langle .,. \rangle$ denotes a scalar product. If applied to vectors, we mean the ordinary Euclidean scalar product and if applied to matrices, we mean the Hilbert-Schmidt scalar product (see Definition 1.8).

$\mathrm{Tr}\,[M]$ denotes the trace of a matrix M.

$P(x, y)$ denotes the joint probability of events x and y.

$P(x|y)$ denotes the conditional probability of events x and y. So, $P(x|y)$ gives the probability that the event x takes place if we know that y happened.

A.2. Used variables

In what follows, we list the symbols that are used in this thesis.

α_x denotes the complex amplitude of the coherent state labelled by x.

β is the reconciliation efficiency, i.e., the efficiency of the classical error correction phase.

$\hat{d}$ denotes a second order quadrature operator (see Section 4.2.2).

$D(\rho||\sigma)$ is the quantum relative entropy between the density matrix ρ and the non-negative linear operator σ (see Definition 1.20).

Δ_a is the angular postselection parameter (see Chapter 2).

Δ_c is the postselection parameter of the cross-shaped scheme (see Chapter 2).

Δ_r is the radial postselection parameter (see Chapter 2).

δ_{EC} is the information leakage (see Section 4.4).

$\mathcal{E}_{A'\rightarrow B}$ denotes the map, modelling the quantum channel between Alice and Bob.

E_y POVM of ideal heterodyne measurement.

ϵ_{FW} is the threshold for the modified Frank-Wolfe algorithm (see Section 3.2).

$\tilde{\epsilon}$ is the perturbation introduced to guarantee differentiability of the objective function (see Section 3.3).

η is the transmittance of the quantum channel. In the present thesis, we chose $\eta = 10^{-0.02L}$. This corresponds to a loss of -0.2dB/km which is a common value for state-of-the-art optical fibres. Equivalently, one can say that only about 95.5% of the light pass an optical fibre with 1km length.

η_t is the transmittance of the optical channel, see η. If there is no danger of confusion, we omit the subscript.

η_d is the detector-efficiency.

$\hat{F}_P$ is the first-order p-quadrature operator for the trusted detector scenario (see Section 4.3.2).

$\hat{F}_Q$ is the first-order q-quadrature operator for the trusted detector scenario (see Section 4.3.2).

$\mathcal{G}$ is a completely positive trace non-increasing map used to formulate the objective function (see Chapter 4).

$\hat{\Gamma}_i$ denotes the i-th measurement operator that is used to define the feasible set $\mathcal{S}$ (see Chapter 4).

γ_i denotes the right hand-side of the i-th constraint required to define the feasible set $\mathcal{S}$ (see Chapter 4).

$H(X)$ denotes the Shannon entropy of the random variable X (see Definition 1.14).

$I(A:B)$ denotes the mutual information, i.e., the information shared by A and B (see Definition 1.18).

I_{AB} denotes the mutual information, see $I(A:B)$.

denotes the transmission distance, measured in km.

$\hat{n}$ denotes the number operator (see Section 4.2.2).

N_c is the photon cutoff number (see Section 3.1).

N_{FW} is the maximum number of Frank-Wolfe iterations (see Section 3.2).

N_{St} denotes the number of states of a certain protocol (see Chapter 2).

ν_{el} is the electronic noise (of some detector) measured in shot-noise units.

$\hat{p}$ denotes the momentum-operator (see Section 4.2.2).

p_i denotes the probability that the signal, associated with the symbol i, is generated (see Chapter 2).

p_{pass} is the probability that a signal passes the postselection phase (see Section 4.4).

$\hat{q}$ denotes the spatial quadrature operator (see Section 4.2.2).

R denotes the secret key rate.

R^{∞} denotes the secret key rate in the asymptotic limit (i.e., for the assumption of infinitely long keys).

R_z^{c} is the region operator, corresponding to the region labelled by the symbol z, for the cross-shaped postselection strategy in the untrusted ideal detector scenario (see 4.2).

R_z^{ra} is the region operator, corresponding to the region labelled by the symbol z, for the radial&angular postselection strategy in the untrusted ideal detector scenario (see 4.2).

$R_z^{\text{c, tr}}$ is the region operator, corresponding to the region labelled by the symbol z, for the cross-shaped postselection strategy in the trusted non-ideal detector scenario (see 4.3).

$R_z^{\text{ra, tr}}$ is the region operator, corresponding to the region labelled by the symbol z, for the radial&angular postselection strategy in the trusted non-ideal detector scenario (see 4.3).

ρ denotes a general density matrix.

ρ_A denotes a density matrix, referring to Alice's system A.

ρ_B denotes a density matrix, referring to Bob's system B.

ρ_{AB} denotes a density matrix, referring to Alice's and Bob's joint system AB.

$S(A)$ denotes the von Neumann entropy contained in the quantum system A (see Definition 1.19).

$\mathcal{S}$ is the feasible set of the conducted optimisation (see Chapter 4).

$\hat{S}_P$ is the second-order p-quadrature operator for the trusted detector scenario (see Section 4.3.2).

$\hat{S}_Q$ is the second-order q-quadrature operator for the trusted detector scenario (see Section 4.3.2).

ξ is the excess noise, measured in shot-noise units.

$\mathcal{Z}$ is a pinching quantum channel used to formulate the objective function (see Chapter 4).

A.3. Used abbreviations and terms

In what follows, we list abbreviations and terms that are used in this thesis.

8PSK stands for 8-state Phase-Shift Keying and is a modulation pattern, where eight coherent states with same state amplitude but different phase are prepared.

Direct Reconciliation The sender of the quantum states (Alice) sends classical information to Bob, who corrects his bit-string according to Alice's instructions. As the classical information-flow is in the same direction as the flow of quantum-signals, one calls it *direct* reconciliation.

Error Correction is a method to perform information reconciliation.

Homodyne Detection is a method to measure one quadrature-component of a light-signal. The signal is superposed with a local oscillator at a 50:50 beamsplitter and the intensity is measured with proportional detectors and the difference between the measured photo-currents is a measure for the quadrature component.

Heterodyne Detection is a method to measure two quadrature-components of a light-signal simultaneously. Therefore, it combines a beam-splitter and two heterodyne detectors.

Information Reconciliation is a process, where Alice and Bob start with partially uncorrelated bit-strings and end up with two perfectly correlated bit-strings while some information is leaked on the classical channel.

Postprocessing is the process of extracting a shorter secret key from the raw key.

Postselection is the process of omitting parts of the measurement results in order to increase the secure key rate or to reduce the raw key.

POVM stands for Positive Operator-Valued Measure (see Definition 1.7).

QKD stands for Quantum Key Distribution.

Privacy Amplification is a procedure to destroy Eve's knowledge about the secret key shared between Alice and Bob.

QPSK stands for Quadrature Phase-Shift Keying and is a modulation pattern, where four coherent states with same state amplitude but different phase are prepared.

Raw Key is the bit-string shared between Alice and Bob after they completed the transmission process, but before performing classical steps, etc.

Reverse Reconciliation The recipient of the quantum states (Bob) sends classical information to the sender (Alice), who corrects her bit-string according to Bob's instructions. As the classical information-flow is in the opposite direction as the flow of quantum-signals, one calls it *reverse* reconciliation.

Security Proof is a theoretical process, where one has to calculate or lower-bound the achievable secure key rate of some QKD protocol, based on system parameters.

Secure Key Rate refers to those fraction of the transmitted signals that can be used to encrypt messages.

Trusted Detector describes here a detector, where Bob can trust (parts of) the noise, i.e. he assumes that the trusted parts of the noise are not under Eve's control.

A.4. Explicit calculation of region operators for the untrusted noise scenario

The calculations given in this section were conducted by the author within the frame of the present thesis and have been published in [23] by the author, where it makes up Appendix A and B.

We present the explicit calculations leading to to the matrix representations of the region operators with respect to the Fock basis, as stated in section 4.2.1. Both for the calculation of the radial&angular and the cross-shaped postselection strategy, the projection of a coherent state with amplitude $|\alpha|$ and phase θ on a number state

$$\left\langle |\alpha| e^{i\theta} \middle| \, n \right\rangle = e^{-\frac{|\alpha|^2}{2}} \frac{|\alpha|^n e^{-in\theta}}{\sqrt{n!}}, \tag{A.1}$$

or, in Cartesian coordinates, $|\alpha| e^{i\theta} = x + iy$,

$$\langle x + iy | n \rangle = e^{-\frac{x^2+y^2}{2}} \frac{(x-iy)^n}{\sqrt{n!}} \tag{A.2}$$

will be useful. This relation is obtained readily by expressing the coherent state in the number basis and applying the inner product with $|n\rangle$.

Before we start with the calculation, we derive an integral that occurs multiple times in the following derivations. For $p > 0$ and $k > 0$ we have

$$\int_{\Delta}^{\infty} \gamma^p e^{-k\gamma^2} \, d\gamma = \frac{1}{2k^{\frac{p+1}{2}}} \Gamma\left(\frac{p+1}{2}, k\Delta^2\right). \tag{A.3}$$

This can be seen as follows. Using the substitution $z := k\gamma^2$ we derive

$$\int_{\Delta}^{\infty} \gamma^p e^{-k\gamma^2} \, d\gamma = \frac{1}{2k^{\frac{p+1}{2}}} \int_{k\Delta^2}^{\infty} z^{\frac{p-1}{2}} e^{-z} \, dz = \frac{1}{2k^{\frac{p+1}{2}}} \int_{k\Delta^2}^{\infty} z^{\frac{p+1}{2}-1} e^{-z} \, dz.$$

According to the definition of the incomplete gamma function, the integral in the last line is equal to $\Gamma\left(\frac{p+1}{2}, k\Delta^2\right)$.

A.4.1. Calculation for radial and angular postselection

We start with the expression for the region operators given in equation (4.6) and insert the definition of the sets A_0^{ra}, A_1^{ra}, A_2^{ra} and A_3^{ra} from (2.4),

$$R_z^{\mathrm{ra}} = \frac{1}{\pi} \int_{\Delta_r}^{\infty} \int_{\frac{\pi}{2}z+\Delta_a}^{\frac{\pi}{2}(z+1)-\Delta_a} \gamma |\gamma e^{i\theta}\rangle\langle\gamma e^{i\theta}| \, \mathrm{d}\theta \, \mathrm{d}\gamma. \tag{A.4}$$

Note that we transformed the integral to polar coordinates, which explains the additional γ coming from the Jacobi-determinant. By using the completeness relation, $\mathbb{1} = \sum_n |n\rangle\langle n|$, twice, we obtain

$$\begin{aligned} R_z^{\text{ra}} &= \frac{1}{\pi} \int_{\Delta_r}^{\infty} \int_{\frac{z\pi}{2}+\Delta_a}^{\frac{(z+1)\pi}{2}-\Delta_a} \sum_{n,m} |n\rangle\langle m|\gamma\langle n|\gamma e^{i\theta}\rangle\langle\gamma e^{i\theta}|m\rangle \, \mathrm{d}\theta \, \mathrm{d}\gamma \\ &= \frac{1}{\pi} \sum_{n,m} |n\rangle\langle m| \int_{\Delta_r}^{\infty} \frac{\gamma^{n+m+1} e^{-\gamma^2}}{\sqrt{m!\, n!}} \, d\gamma \int_{\frac{z\pi}{2}+\Delta_a}^{\frac{(z+1)\pi}{2}-\Delta_a} e^{i\theta(n-m)} \, d\theta. \end{aligned}$$

The radial integral can be expressed by the incomplete gamma function $\Gamma(x, a)$ using the integral given in eq. (A.3).

$$\int_{\Delta_r}^{\infty} \frac{\gamma^{n+m+1} e^{-\gamma^2}}{\sqrt{m!\, n!}} \, d\gamma = \frac{1}{2\sqrt{m!\, n!}} \Gamma\left(\frac{m+n}{2} + 1, \Delta_r^2\right).$$

If $m = n$, the angular integral simplifies to $\frac{\pi}{2} - 2\Delta_a$. For the case $m \neq n$ we obtain $\frac{2}{m-n} e^{-i(m-n)\left(z+\frac{1}{2}\right)\frac{\pi}{2}} \sin\left[\left(\frac{\pi}{4} - \Delta_a\right)(m-n)\right]$.

In conclusion, we have

$$\begin{aligned} R_z^{\text{ra}} := \frac{1}{\pi} \sum_n \sum_m & \frac{\Gamma(\frac{m+n}{2} + 1, \Delta_r^2)}{\sqrt{m!\, n!}} |n\rangle\langle m| \\ & \cdot \begin{cases} \frac{\pi}{4} - \Delta_a & m = n \\ \frac{1}{m-n} e^{-i(m-n)\left(z+\frac{1}{2}\right)\frac{\pi}{2}} \sin\left[\left(\frac{\pi}{4} - \Delta_a\right)(m-n)\right] & n \neq m \end{cases} . \end{aligned} \tag{A.5}$$

A.4.2. Calculation for cross-shaped postselection

We start by using the definition of the region operators in equation (4.7) and the sets $A_0^{\text{c}}, A_1^{\text{c}}, A_2^{\text{c}}$ and A_3^{c} from equation (2.5),

$$\begin{aligned} R_0^{\text{c}} &= \frac{1}{\pi} \int_{\Delta_c}^{\infty} \int_{\Delta_c}^{\infty} |x+iy\rangle\langle x+iy| \, \mathrm{d}y \, \mathrm{d}x, \\ R_1^{\text{c}} &= \frac{1}{\pi} \int_{-\infty}^{-\Delta_c} \int_{\Delta_c}^{\infty} |x+iy\rangle\langle x+iy| \, \mathrm{d}y \, \mathrm{d}x, \\ R_2^{\text{c}} &= \frac{1}{\pi} \int_{-\infty}^{-\Delta_c} \int_{-\infty}^{-\Delta_c} |x+iy\rangle\langle x+iy| \, \mathrm{d}y \, \mathrm{d}x, \\ R_3^{\text{c}} &= \frac{1}{\pi} \int_{\Delta_c}^{\infty} \int_{-\infty}^{-\Delta_c} |x+iy\rangle\langle x+iy| \, \mathrm{d}y \, \mathrm{d}x. \end{aligned}$$

All integrals have the same form and differ only by the boundaries of the occurring integrals. Hence, we derive only the expression for R_0^c and argue to obtain the remaining integrals. We start by using the completeness relation, $\mathbb{1} = \sum_n |n\rangle\langle n|$, twice and obtain

$$\begin{aligned} R_0^{\mathrm{c}} &= \frac{1}{\pi}\sum_{n,m} |n\rangle\langle m| \int_{\Delta_c}^{\infty}\int_{\Delta_c}^{\infty} \langle n|x+iy\rangle\langle x+iy|m\rangle \,\mathrm{d}y\,\mathrm{d}x \\ &= \frac{1}{\pi}\sum_{n,m} \frac{|n\rangle\langle m|}{\sqrt{n!}\sqrt{m!}} \int_{\Delta_c}^{\infty}\int_{\Delta_c}^{\infty} e^{-(x^2+y^2)}(x+iy)^n(x-iy)^m \,\mathrm{d}y\,\mathrm{d}x. \end{aligned}$$

For $m = n$ we find

$$\begin{aligned} \int_{\Delta_c}^{\infty}\int_{\Delta_c}^{\infty} e^{-(x^2+y^2)}(x^2+y^2)^n \,\mathrm{d}y\,\mathrm{d}x &= \sum_{k=0}^{n}\binom{n}{k}\int_{\Delta_c}^{\infty} e^{-x^2}x^{2k}\,\mathrm{d}x \int_{\Delta_c}^{\infty} e^{-y^2}y^{2(n-k)}\,\mathrm{d}y \\ &= \frac{1}{4}\sum_{k=0}^{n}\binom{n}{k}\Gamma\left(k+\frac{1}{2},\Delta_c^2\right)\Gamma\left(n-k+\frac{1}{2},\Delta_c^2\right). \end{aligned}$$

Where we used eq. (A.3) to express the occurring integrals by the incomplete gamma function.

For $m \neq n$ we deduce

$$\begin{aligned} &\int_{\Delta_c}^{\infty}\int_{\Delta_c}^{\infty} e^{-(x^2+y^2)}(x+iy)^n(x-iy)^m \,\mathrm{d}y\,\mathrm{d}x \\ &= \sum_{j=0}^{n}\sum_{k=0}^{m}\binom{n}{j}\binom{m}{k}\int_{\Delta_c}^{\infty} e^{-x^2}x^{j+k}\,\mathrm{d}x \int_{\Delta_c}^{\infty} e^{-y^2}y^{n+m-j-k}(-1)^{m-k}i^{n+m-j-k}\,\mathrm{d}y \\ &= \frac{1}{4}\sum_{j=0}^{n}\sum_{k=0}^{m}\binom{n}{j}\binom{m}{k}(-1)^{m-k}i^{n+m-j-k}\Gamma\left(\frac{j+k+1}{2},\Delta_c^2\right)\Gamma\left(\frac{n+m-j-k+1}{2},\Delta_c^2\right), \end{aligned}$$

where we used again eq. (A.3). Note that

$$(-1)^{m-k}i^{n+m-j-k} = i^{n+3m-j-3k} = i^{n-m+k-j}.$$

Including this in the expression for the region operator, we obtain

$$R_0^{\mathrm{c}} = \tag{A.6}$$

$$\sum_{n,m}\frac{|n\rangle\langle m|}{4\pi\sqrt{n!}\sqrt{m!}} \cdot \begin{cases} \sum_{j=0}^{n}\binom{n}{j}\Gamma\left(j+\frac{1}{2},\Delta_c^2\right)\Gamma\left(n-j+\frac{1}{2},\Delta_c^2\right) & n=m \\ \sum_{j=0}^{n}\sum_{k=0}^{m}\binom{n}{j}\binom{m}{k}\Gamma\left(\frac{j+k+1}{2},\Delta_c^2\right)\Gamma\left(\frac{n+m-j-k+1}{2},\Delta_c^2\right)i^{n-m+k-j} & n\neq m. \end{cases} \tag{A.7}$$

We observe that the integral for the case $m = n$ consists only of squares of x and y, hence this part is not sensitive to sign-changes and therefore equal for all four operators $R^c_z, \ z = 0, 1, 2, 3$.

For $m \neq n$, when we calculate R^c_1, we face an integral of the same form as we do for R^c_0 once we substitute $x \mapsto -\tilde{x}$. This leads to

$$\int_{-\infty}^{-\Delta_c} e^{-x^2} x^{j+k} \, \mathrm{d}x = (-1)^{j+k} \int_{\Delta_c}^{\infty} e^{-\tilde{x}^2} \tilde{x}^{j+k} \, \mathrm{d}\tilde{x}.$$

So, this substitution introduces a factor of $(-1)^{j+k}$ leaving the remaining expression unchanged. If we substitute $y \mapsto -\tilde{y}$, as required for the calculation of R^c_3, we find

$$\int_{-\infty}^{-\Delta_c} e^{-y^2} y^{n+m-j-k} \, \mathrm{d}y = (-1)^{n+m-j-k} \int_{\Delta_c}^{\infty} e^{-\tilde{y}^2} \tilde{y}^{n+m-j-k} \, \mathrm{d}\tilde{y}.$$

Here, we obtain a factor of $(-1)^{n+m-j-k}$. Finally, the calculation for R^c_2 requires two substitutions, namely $x \mapsto -\tilde{x}$ and $y \to -\tilde{y}$, which introduces a factor of $(-1)^{j+k}(-1)^{m+n-j-k}$. Let us denote the power of -1 that occurs in the expression for the region operator z by $D^{(z)}_{j,k,m,n}$. According to the consideration above, we find

$$\begin{aligned}
\tilde{D}^{(0)}_{j,k,m,n} &= 1, \\
\tilde{D}^{(1)}_{j,k,m,n} &= (-1)^{j+k} = (-1)^{k-j}, \\
\tilde{D}^{(2)}_{j,k,m,n} &= (-1)^{j+k}(-1)^{m+n-j-k} = (-1)^{m+n} = (-1)^{n-m}, \\
\tilde{D}^{(3)}_{j,k,m,n} &= (-1)^{m+n-j-k} = (-1)^{n-m+k-j}.
\end{aligned}$$

To include the power of i in this factor, we define $D^{(z)}_{j,k,m,n} := \tilde{D}^{(z)}_{j,k,m,n} \ i^{n+m-j-k}$. Therefore, we finally arrive at

$$R^c_z = \tag{A.8}$$

$$\sum_{n,m} \frac{|n\rangle\langle m|}{4\pi\sqrt{n!}\sqrt{m!}} \cdot \begin{cases} \sum\limits_{j=0}^{n} \binom{n}{j} \Gamma\left(j+\frac{1}{2}, \Delta_c^2\right) \Gamma\left(n-j+\frac{1}{2}, \Delta_c^2\right) & n = m \\ \sum\limits_{j=0}^{n} \sum\limits_{k=0}^{m} \binom{n}{j}\binom{m}{k} \Gamma\left(\frac{j+k+1}{2}, \Delta_c^2\right) \Gamma\left(\frac{n+m-j-k+1}{2}, \Delta_c^2\right) D^{(z)}_{j,k,m,n} & n \neq m. \end{cases} \tag{A.9}$$

A.5. Calculations for the trusted detector scenario

First we express the POVM Element, given in equation (4.32) in the number basis, where we use equations (6.13) and (6.14) in [32].

After defining $C_{n,m} := \frac{1}{\pi\eta_d^{\frac{m-n}{2}+1}}\sqrt{\frac{n!}{m!}}\frac{\overline{n}_d^n}{(1+\overline{n}_d)^{m+1}}$, $a := \frac{1}{\eta_d(1+\overline{n}_d)}$ and $b := \eta_d\overline{n}_d(1+\overline{n}_d)$, we obtain for $n \leqslant m$

$$\langle n|G_y|m\rangle = C_{n,m}e^{-a|y|^2}(y^*)^{m-n}L_n^{(m-n)}\left(-\frac{|y|^2}{b}\right), \tag{A.10}$$

where

$$L_k^\alpha(x) = \sum_{j=0}^{k}(-1)^j\binom{k+\alpha}{k-j}\frac{x^j}{j!} \tag{A.11}$$

is the generalized Laguerre polynomial of degree k and with parameter α [34].

A.5.1. Calculation for radial&angular postselection with trusted detector

We start with the expression for the region operators given in equation (4.6), where we replaced the POVM for the ideal homodyne detector by that for the nonideal, trusted detector, and inserted the definition of the sets A_0^{ra}, A_1^{ra}, A_2^{ra} and A_3^{ra} from equation (2.4),

$$\begin{aligned} R_z^{\text{ra, tr}} &= \int_{\Delta_r}^{\infty}\int_{\frac{\pi}{2}z+\Delta_a}^{\frac{\pi}{2}(z+1)-\Delta_a} \gamma\ G_{\gamma e^{i\theta}}\ \mathrm{d}\theta\ \mathrm{d}\gamma \\ &= \sum_{n=0}^{N_c}\sum_{m=0}^{N_c}|n\rangle\langle m|\int_{\Delta_r}^{\infty}\int_{\frac{\pi}{2}z+\Delta_a}^{\frac{\pi}{2}(z+1)-\Delta_a} \gamma\ \langle n|G_{\gamma e^{i\theta}}|m\rangle\, d\theta\, d\gamma. \end{aligned}$$

Inserting the expression for G_y from equation (A.10) yields

$$\begin{aligned} R_z^{\text{ra, tr}} = \sum_{n=0}^{N_c}\sum_{m=0}^{N_c}C_{n,m}|n\rangle\langle m|\int_{\Delta_r}^{\infty} e^{-a\gamma^2}\gamma^{m-n+1}L_n^{(m-n)}\left(-\frac{\gamma^2}{b}\right)\, d\gamma \\ \cdot\int_{\frac{\pi}{2}z+\Delta_a}^{\frac{\pi}{2}(z+1)-\Delta_a} e^{-i\theta(m-n)}\, d\theta. \end{aligned}$$

For $n = m$ the angular integral simplifies to $\frac{\pi}{2} - 2\Delta_a$ and the radial integral can be expressed as

$$\int_{\Delta_r}^{\infty} e^{-a\gamma^2}\gamma L_n^{(0)}\left(-\frac{\gamma^2}{b}\right)\, d\gamma = \sum_{j=0}^{n}\binom{n}{n-j}\frac{1}{b^j j!}\int_{\Delta_r}^{\infty}\gamma^{2j+1}e^{-a\gamma^2}\, d\gamma,$$

where we used the sum-representation (A.11) of the generalised Laguerre polynomials. Using eq. (A.3), we obtain

$$\langle n|R_z^{\text{ra, tr}}|n\rangle = \frac{C_{n,n}}{2}\left(\frac{\pi}{2} - 2\Delta_a\right)\sum_{j=0}^{n}\binom{n}{n-j}\frac{1}{a^{j+1}b^j j!}\Gamma\left(j+1, a\Delta_r^2\right).$$

For $n \neq m$, we obtain the angular integral

$$\frac{2}{(m-n)} e^{-i(m-n)\left(z+\frac{1}{2}\right)\frac{\pi}{2}} \sin\left[(m-n)\left(\frac{\pi}{4} - \Delta_a\right)\right]$$

and derive the radial integral

$$\begin{aligned} \int_{\Delta_r}^{\infty} e^{-a\gamma^2} \gamma^{m-n+1} L_n^{(m-n)}\left(-\frac{\gamma^2}{b}\right) d\gamma = \\ = \sum_{j=0}^{n} \binom{m}{n-j} \frac{1}{b^j j!} \int_{\Delta_r}^{\infty} \gamma^{2j+m-n+1} e^{-a\gamma^2} \, d\gamma \\ = \frac{1}{2} \sum_{j=0}^{n} \binom{m}{n-j} \frac{1}{a^{j+1+\frac{m-n}{2}} b^j j!} \Gamma\left(j+1+\frac{m-n}{2}, a\Delta_r^2\right). \end{aligned}$$

We do not need to calculate the matrix element for $m < n$ separately, as the region operator has to be Hermitian.

In conclusion, we found for $R_z^{\text{ra, tr}} = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} \langle n | R_z^{\text{ra, tr}} | m \rangle |n\rangle\langle m|$ the matrix elements

$$\langle n | R_z^{\text{ra, tr}} | m \rangle = \begin{cases} C_{n,n} \left[\frac{\pi}{4} - \Delta_a\right] \sum\limits_{j=0}^{n} \binom{n}{n-j} \frac{\Gamma(j+1, a\Delta_r^2)}{a^{j+1} b^j j!} & n = m \\ \frac{C_{n,m}}{m-n} e^{-i(m-n)\left(z+\frac{1}{2}\right)\frac{\pi}{2}} \sin\left[(m-n)\left(\frac{\pi}{4} - \Delta_a\right)\right] \sum\limits_{j=0}^{n} \binom{m}{n-j} \frac{\Gamma\left(j+1+\frac{m-n}{2}, a\Delta_p^2\right)}{a^{j+1+\frac{m-n}{2}} b^j j!} & n < m \\ \overline{\langle m | R_z^{\text{ra, tr}} | n \rangle} & n > m \end{cases} . \tag{A.12}$$

A.5.2. Calculation for cross-shaped postselection with trusted detector

Similarly to the calculations for the untrusted scenario, we start by using the definition of the region operators in equation (4.7) and the sets A_0^c, A_1^c, A_2^c and A_3^c from equation (2.5),

$$\begin{aligned} R_0^{\text{c, tr}} &= \int_{\Delta_c}^{\infty} \int_{\Delta_c}^{\infty} G_{x+iy} \, \mathrm{d}y \, \mathrm{d}x, \\ R_1^{\text{c, tr}} &= \int_{-\infty}^{-\Delta_c} \int_{\Delta_c}^{\infty} G_{x+iy} \, \mathrm{d}y \, \mathrm{d}x, \\ R_2^{\text{c, tr}} &= \int_{-\infty}^{-\Delta_c} \int_{-\infty}^{-\Delta_c} G_{x+iy} \, \mathrm{d}y \, \mathrm{d}x, \\ R_3^{\text{c, tr}} &= \int_{\Delta_c}^{\infty} \int_{-\infty}^{-\Delta_c} G_{x+iy} \, \mathrm{d}y \, \mathrm{d}x. \end{aligned}$$

Again, all integrals have the same form and differ only by the boundaries of the occurring integrals. Hence, we derive only the expression for $R_0^{\text{c, tr}}$ and reason the changes to obtain the remaining integrals.

For $n \leqslant m$ we obtain

$$\begin{aligned}
R_0^{\text{c, tr}} &= \sum_{n,m} |n\rangle\langle m| \int_{\Delta_c}^{\infty} \int_{\Delta_c}^{\infty} \langle n|G_{x+iy}|m\rangle \, dy \, dx \\
&= \sum_{n,m} |n\rangle\langle m| C_{n,m} \int_{\Delta_c}^{\infty} \int_{\Delta_c}^{\infty} e^{-a(x^2+y^2)} (x-iy)^{m-n} L_n^{(m-n)} \left(-\frac{x^2+y^2}{b} \right) dy \, dx,
\end{aligned}$$

where we inserted the expression for G_y from equation (A.10) in the last line.

First, we treat the case $m = n$, where we have

$$\begin{aligned}
\langle n|R_0^{\text{c, tr}}|m\rangle &= C_{n,n} \int_{\Delta_c}^{\infty} \int_{\Delta_c}^{\infty} e^{-a(x^2+y^2)} L_n^{(0)} \left(-\frac{x^2+y^2}{b} \right) dy \, dx \\
&= C_{n,n} \sum_{j=0}^{n} \binom{n}{n-j} \frac{(-1)^j}{j!} \int_{\Delta_c}^{\infty} \int_{\Delta_c}^{\infty} e^{-a(x^2+y^2)} \frac{(x^2+y^2)^j}{b^j} (-1)^j \, dy \, dx \\
&= C_{n,n} \sum_{j=0}^{n} \binom{n}{n-j} \frac{1}{b^j j!} \sum_{k=0}^{j} \binom{j}{k} \int_{\Delta_c}^{\infty} e^{-ax^2} x^{2k} \, dx \int_{\Delta_c}^{\infty} e^{-ay^2} y^{2(j-k)} \, dy.
\end{aligned}$$

For the second equality we inserted the sum representation of the Laguerre polynomials (A.11) and for the third equality we used the binomial theorem to express $(x^2+y^2)^j$ as sum. Both the integrals over x and y are of the same form as discussed in eq. (A.3), therefore we obtain

$$\begin{aligned}
&\langle n|R_0^{\text{c, tr}}|n\rangle = \\
&C_{n,n} \sum_{j=0}^{n} \binom{n}{n-j} \frac{1}{b^j j!} \sum_{k=0}^{j} \binom{j}{k} \frac{1}{a^{j+1}} \Gamma\left(k+\frac{1}{2}, a\Delta_c^2\right) \Gamma\left(j-1+\frac{1}{2}, a\Delta_c^2\right).
\end{aligned} \tag{A.13}$$

Second, we deal with $n < m$. We have

$$
\begin{aligned}
\langle m|R_0^{\text{c, tr}}|n\rangle &= C_{n,m}\int_{\Delta_c}^{\infty}\int_{\Delta_c}^{\infty} e^{-a(x^2+y^2)} L_n^{(m-n)}\left(-\frac{x^2+y^2}{b}\right) dy\, dx \\
&= C_{n,m}\sum_{j=0}^{n}\binom{m}{n-j}\frac{1}{b^j j!}\int_{\Delta_c}^{\infty}\int_{\Delta_c}^{\infty} e^{-a(x^2+y^2)}(x-iy)^{m-n}(x^2+y^2)^j\, dy\, dx \\
&= C_{n,m}\sum_{j=0}^{n}\binom{m}{n-j}\frac{1}{b^j j!}\sum_{l=0}^{j}\binom{j}{l} \\
&\qquad \cdot\sum_{k=0}^{m-n}\binom{m-n}{k}(-i)^{n-m-k}\int_{\Delta_c}^{\infty} e^{-ax^2}x^{k+2l}\, dx\int_{\Delta_c}^{\infty} e^{-ay^2}y^{2j-2l+m-n-k}\, dy.
\end{aligned}
$$

For the second equality we inserted the sum representation of the Laguerre polynomials (A.11) and for the third equality we used the binomial theorem twice; first, to express $(x^2+y^2)^j$ as sum and second, to write $(x-iy)^{m-n}$ as a sum too. Again, the occurring integrals are of the form given in equation (A.3). Therefore, we obtain

$$
\begin{aligned}
&\langle m|R_0^{\text{c, tr}}|n\rangle \\
&= \frac{C_{n,m}}{4}\sum_{j=0}^{n}\frac{\binom{m}{n-j}}{b^j j!}\sum_{l=0}^{j}\binom{j}{l}\sum_{k=0}^{m-n}\binom{m-n}{k}\frac{(-1i)^{m-n-k}}{a^{j+1+\frac{m-n}{2}}} \\
&\qquad \cdot\Gamma\left(l+\frac{k+1}{2}, a\Delta_c^2\right)\Gamma\left(j-l+\frac{m-n-k+1}{2}, a\Delta_c^2\right).
\end{aligned}
$$

As the region operators have to be Hermitian, we do not need to calculate the matrix elements for $n > m$ separately. Summing up, we found for the region operator $R_0^{\text{c, tr}} = \sum_{n,m}|n\rangle\langle m|\langle n|R_0^{\text{c, tr}}|m\rangle$ the matrix elements

$$
\langle n|R_0^{\text{c, tr}}|m\rangle =
\begin{cases}
C_{n,n}\sum_{j=0}^{n}\frac{\binom{n}{n-j}}{b^j j!}\sum_{k=0}^{j}\binom{j}{k}\frac{1}{a^{j+1}}\Gamma\left(k+\frac{1}{2}, a\Delta_c^2\right)\Gamma\left(j-k+\frac{1}{2}, a\Delta_c^2\right) & n = m \\
\frac{C_{n,m}}{4}\sum_{j=0}^{n}\frac{\binom{m}{n-j}}{a^{j+1}b^j j!}\sum_{l=0}^{j}\binom{j}{l}\sum_{k=0}^{m-n}\binom{m-n}{k}\frac{\tilde{D}^{(0)}_{k,m,n}\Gamma\left(l+\frac{k+1}{2}, a\Delta_c^2\right)\Gamma\left(j-l+\frac{m-n-k+1}{2}, a\Delta_c^2\right)}{a^{\frac{m-n}{2}}} & n < m \\
\overline{\langle m|R_z^{\text{c, tr}}|n\rangle} & n > m
\end{cases}, \tag{A.14}
$$

where we set $\tilde{D}^{(0)}_{k,m,n} := (-1i)^{m-n-k}$. Similarly to the cross-shaped postselection in the untrusted scenario, we observe that the integral for $m = n$ contains only even powers of x and y. Hence, this part is not affected by sign-changes in the boundaries of the occurring integrals. In contrast, for $n < m$ we have odd powers of x and y, so we expect additional powers of -1 in the expressions for $\langle n|R_z^{\text{c, tr}}|m\rangle$, $z \in 1, 2, 3$ compared to $\langle n|R_0^{\text{c, tr}}|m\rangle$. By similar considerations as carried out in Section A.4, we obtain

$$\begin{aligned}\tilde{D}^{(0)}_{k,m,n} &= (-1)^{m-n-k},\\ \tilde{D}^{(1)}_{k,m,n} &= (-1)^{m-n}\\ \tilde{D}^{(2)}_{k,m,n} &= (-1)^{k},\\ \tilde{D}^{(3)}_{k,m,n} &= 1,\end{aligned}$$

where $\tilde{D}^{(z)}_{m,n,k}$ denotes the power of -1 that occurs in the expression for the region operator z. Note that we have already included the factor $(-1)^{m-n-k}$, which occurs in the expression for all z. We define $D^{(z)}_{m,n,k} := \tilde{D}^{(z)}_{m,n,k}\, i^{m-n-k}$ and obtain for $R_z^{\text{c, tr}} = \sum_{n,m} |n\rangle\langle m|\langle n|R_z^{\text{c, tr}}|m\rangle$ the representation with respect to the number basis

$$\langle n|R_z^{\text{c, tr}}|m\rangle = \begin{cases} C_{n,n}\sum\limits_{j=0}^{n}\frac{\binom{n}{n-j}}{a^{j+1}b^j j!}\sum\limits_{k=0}^{j}\binom{j}{k}\Gamma\left(k+\frac{1}{2}, a\Delta_c^2\right)\Gamma\left(j-k+\frac{1}{2}, a\Delta_c^2\right) & n = m\\ \frac{C_{n,m}}{4a^{\frac{m-n}{2}}}\sum\limits_{j=0}^{n}\frac{\binom{m}{n-j}}{a^{j+1}b^j j!}\sum\limits_{l=0}^{j}\binom{j}{l}\sum\limits_{k=0}^{m-n}\binom{m-n}{k}D^{(z)}_{k,m,n}\Gamma\left(l+\frac{k+1}{2}, a\Delta_c^2\right)\Gamma\left(j-l+\frac{m-n-k+1}{2}, a\Delta_c^2\right) & n < m\\ \overline{\langle m|R_z^{\text{c, tr}}|n\rangle} & n > m\end{cases}. \tag{A.15}$$

A.6. Representation of the first- and second-moment observables in the number basis

For the sake of completeness, we give explicit number-basis representations of the first- and second-moment observables, defined in equations (4.40-4.43). We note that [28] gives explicit representations in the appendix, too, which again depend on the coefficients of some Taylor expansion. In contrast to this, we give explicit expressions and solve the integrals similar to our calculations for the region operators in the preceding sections. In what follows, we give only expressions for $n \leqslant m$, as all operators need to be Hermitian, hence $\langle k|\hat{O}|l\rangle = \overline{\langle l|\hat{O}|k\rangle}$ gives the missing matrix elements.

We start with $\hat{F}_Q$, whose matrix elements with respect to the number basis are given by

$$\langle n|\hat{F}_Q|m\rangle = \frac{1}{\sqrt{2}}\int (y+y^*)\langle n|G_y|m\rangle$$

Choosing polar coordinates and inserting the expression for $G_{\gamma e^{i\theta}}$ from equation (A.10) leads to

$$\begin{aligned}\langle n|\hat{F}_Q|m\rangle &= \frac{C_{n,m}}{\sqrt{2}}\int_0^{2\pi}\left(e^{i\theta}+e^{-i\theta}\right)e^{-i\theta(m-n)}\,d\theta\int_0^\infty \gamma^{m-n+2}e^{-a\gamma^2}L_n^{(m-n)}\left(-\frac{\gamma^2}{b}\right)d\gamma\\ &= \frac{2\pi C_{n,m}}{\sqrt{2}}\delta_{m,n\pm1}\int_0^\infty \gamma^{m-n+2}e^{-a\gamma^2}L_n^{(m-n)}\left(-\frac{\gamma^2}{b}\right)d\gamma\\ &= \frac{2\pi C_{n,m}}{\sqrt{2}}\delta_{m,n\pm1}\sum_{j=0}^{n}\binom{m}{n-j}\frac{(-1)^j}{b^j j!}\int_0^\infty \gamma^{m-n+j+2}e^{-a\gamma^2}\,d\gamma.\end{aligned}$$

The remaining integral can be solved using (A.3) for the special case where $\Delta=0$. Therefore, we obtain

$$\langle n|\hat{F}_Q|n+1\rangle = \frac{\pi C_{n,n+1}}{\sqrt{2}}\sum_{j=0}^{n}\binom{n+1}{n-j}\frac{1}{a^{j+2}b^j j!}\Gamma(j+2) = \frac{\pi C_{n,n+1}}{\sqrt{2}}\sum_{j=0}^{n}\binom{n+1}{n-j}\frac{j+1}{a^{j+2}b^j} \tag{A.16}$$

and $\langle n|\hat{F}_Q|m\rangle = 0$ for $m \neq n\pm1$, where we used the definition of the gamma function. Similarly, starting from equation (4.41), we derive

$$\langle n|\hat{F}_P|n+1\rangle = i\frac{\pi C_{n,n+1}}{\sqrt{2}}\sum_{j=0}^{n}\binom{n+1}{n-j}\frac{j+1}{a^{j+2}b^j} = i\langle n|\hat{F}_Q|n+1\rangle \tag{A.17}$$

and $\langle n|\hat{F}_P|m\rangle = 0$ if $m \neq n\pm1$.

The matrix representations of the second-moment observables read

$$\langle n|\hat{S}_Q|n\rangle = -\langle n|\hat{S}_P|n\rangle = \pi C_{n,n}\sum_{j=0}^{n}\binom{n}{n-j}\frac{j+1}{a^{j+2}b^j}, \tag{A.18}$$

$$\langle n|\hat{S}_Q|n+2\rangle = -\langle n|\hat{S}_P|n+2\rangle = \pi C_{n,n+2}\sum_{j=0}^{n}\binom{n+2}{n-j}\frac{(j+2)(j+1)}{a^{j+3}b^j} \tag{A.19}$$

and $\langle n|\hat{S}_Q|m\rangle = \langle n|\hat{S}_P|m\rangle = 0$ otherwise.

A.7. Transforming a matrix-valued constraint

In this section, we discuss how we transform the matrix-valued constraint in the present optimisation problem into a set of scalar-valued constraints. According to Chapter 4 the matrix-valued constraint reads as

$$\rho_A = Tr_B\left(\rho_{AB}\right) = Tr_{A'}\left(|\Psi\rangle\langle\Psi|_{AA'}\right).$$

We translate this constraint into a set of scalar-valued constraints using a technique that is inspired by quantum state tomography (see, e.g., [1]). Our goal is to find an orthonormal basis $\hat{\Theta}_k$ of Alice's Hilbert space $\mathcal{H}_A$, where orthonormal is meant with respect to the Hilbert-Schmidt inner product (see 1.8). Then, we may decompose ρ_A as follows:

$$\rho_A = \sum_k \theta_k \cdot \hat{\Theta}_k \tag{A.20}$$

with $\theta_k := \langle \rho_A, \hat{\Theta}_k \rangle = Tr\left(\rho_A \cdot \hat{\Theta}_k\right)$.

The present protocols deal with four or eight signal states. Hence Alice's Hilbert space $\mathcal{H}_A$ is spanned by either 4×4 or $8 \times 8 = 4 \times 4 \times 4$ basis vectors. We want that the used operators are physical observables, hence we require the basis vectors to be Hermitian. We use the Pauli matrices

$$\sigma_0 := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$
$$\sigma_1 := \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$
$$\sigma_2 := \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},$$
$$\sigma_3 := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

that form a basis of the space of all 2×2 Hermitian matrices. Therefore, we define our orthonormal basis for four-state protocols by

$$\left\{\hat{\Theta}_k\right\}_k := \{\sigma_i \otimes \sigma_j \text{ for } i, j \in \{0, 1, 2, 3\}\}, \tag{A.21}$$

and the orthonormal basis for eight-state protocols by

$$\left\{\hat{\Theta}_k\right\}_k := \{\sigma_i \otimes \sigma_j \otimes \sigma_l \text{ for } i, j, l \in \{0, 1, 2, 3\}\}, \tag{A.22}$$

Obviously, $\hat{\Theta}_k$ is Hermitian for all k. One can readily check that they are hermitian and $\forall m, n \in \{0, 1, ..., N_{\text{St}} - 1\} : \langle \hat{\Theta}_m, \hat{\Theta}_n \rangle = \delta_{mn}$ holds (orthogonality is inherited from the Pauli matrices).

We hold now a set of orthonormal operators to fix Alice's density matrix ρ_A. Next, we define the corresponding set of measurement operators, acting on the whole Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$,

$$\left\{ \hat{\Theta}_k \otimes \mathbb{1}_B : k \in \{0, 1, ..., N_{\mathrm{St}} - 1\} \right\}$$

According to eq. (A.20), ρ_{AB} can be decomposed as

$$\rho_{AB} = \sum_{k=0}^{N_{\mathrm{St}}-1} \theta_k \cdot (\hat{\Theta}_k \otimes \mathbb{1}_B), \tag{A.23}$$

where $\theta_k = \langle \rho_{AB}, (\hat{\Theta}_k \otimes \mathbb{1}_B) \rangle = Tr\left(\rho_{AB}(\hat{\Theta}_k \otimes \mathbb{1}_B) \right)$. It remains to find expressions for θ_k, as we want to constrain the unknown ρ_{AB} rather than calculating θ_k from ρ_{AB}. According to the model of the preparation process (see Section 4.1.1), the state after preparation reads

$$|\Psi\rangle_{AA'} = \sum_{x=0}^{N_{\mathrm{St}-1}} \sqrt{p_x} \, |x\rangle_A \, |\phi_x\rangle_{A'} = \sum_{x=0}^{N_{\mathrm{St}}-1} \sqrt{p_x} e^{-\frac{|\beta_x|^2}{2}} \sum_{n=0}^{\infty} \frac{\beta_x^n}{\sqrt{n!}} \, |n\rangle \, |x\rangle_A \,, \tag{A.24}$$

where $\beta_x \in \mathbb{C}$ is the amplitude of the coherent state that is prepared by Alice. Then the share A' (in the entanglement-based picture) is sent to Bob, using a quantum channel $\mathcal{E}_{A' \to B}$. This channel is trace-preserving, therefore we may trace out A' instead of B, hence trace over AA' instead of AB.
The density matrix corresponding to the state $|\Psi\rangle_{AA'}$ reads

$$\rho_{AA'} = \sum_{x=0}^{N_{\mathrm{St}}-1} \sum_{y=0}^{N_{\mathrm{St}}-1} e^{-|\beta_x|^2 - |\beta_y|^2} \sqrt{p_x p_y} \, |x\rangle\langle y|_A \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} \frac{\beta_x^n (\overline{\beta_y})^m}{\sqrt{n!}\sqrt{m!}} \, |n\rangle\langle m|_B \,.$$

Let us denote the representation of $\hat{\Theta}_k$ with respect to the chosen basis by

$$\hat{\Theta}_k = \sum_{r=0}^{N_{\mathrm{St}}-1} \sum_{s=0}^{N_{\mathrm{St}}-1} d_{rs}^{(k)} \, |r\rangle\langle s|_A \,, \tag{A.25}$$

where $d_{rs}^{(k)} \in \mathbb{C}$. Note that we have $\sqrt{2} d_{rs}^{(k)} \in \{-1, 0, 1, -i, i\}$.
Then, we write $(\hat{\Theta}_k \otimes \mathbb{1}_B)$ as

$$(\hat{\Theta}_k \otimes \mathbb{1}_{A'}) = \sum_{r=0}^{N_{\mathrm{St}}-1} \sum_{s=0}^{N_{\mathrm{St}}-1} \sum_{p=0}^{\infty} \sum_{q=0}^{\infty} d_{rs}^{(k)} \delta_{pq} \, |r\rangle\langle s|_A \, |p\rangle\langle q|_B \,, \tag{A.26}$$

where δ_{pq} is the Kronecker delta.

Finally, we find

$$
\begin{aligned}
\theta_k &= \mathrm{Tr}\left[(\hat{\Theta}_k \otimes \mathbb{1}_{A'})\rho_{AA'}\right] \\
&= e^{-|\beta_x|^2}\mathrm{Tr}\left[\sum_{x,y=0}^{N_{\mathrm{St}}-1}\sum_{r,s=0}^{N_{\mathrm{St}}-1}\sqrt{p_x p_y}d_{rs}^{(k)}\,|r\rangle\langle s|x\rangle\langle y|_A\sum_{p,q=0}^{\infty}\sum_{n,m=0}^{\infty}\delta_{pq}\frac{\beta_x^n(\overline{\beta}_y)^m}{\sqrt{n!}\sqrt{m!}}\,|p\rangle\langle q|n\rangle\langle m|_B\right] \\
&= e^{-|\beta_x|^2}\mathrm{Tr}\left[\sum_{x,y=0}^{N_{\mathrm{St}}-1}\sum_{r=0}^{N_{\mathrm{St}}-1}\sqrt{p_x p_y}d_{rx}^{(k)}\,|r\rangle\langle y|_A\sum_{p=0}^{\infty}\sum_{m=0}^{\infty}\frac{\beta_x^p(\overline{\beta}_y)^m}{\sqrt{p!}\sqrt{m!}}\,|p\rangle\langle m|_B\right] \\
&= e^{-|\beta_x|^2}\left(\sum_{i=0}^{N_{\mathrm{St}}-1}\sum_{x,y=0}^{N_{\mathrm{St}}-1}\sum_{r=0}^{N_{\mathrm{St}}-1}\sqrt{p_x p_y}d_{rx}^{(k)}\,\langle i|r\rangle\langle y|i\rangle_A\sum_{j=0}^{\infty}\sum_{p=0}^{\infty}\sum_{m=0}^{\infty}\frac{\beta_x^p(\overline{\beta}_y)^m}{\sqrt{p!}\sqrt{m!}}\langle j|p\rangle\langle m|j\rangle_B\right) \\
&= e^{-|\beta_x|^2}\left(\sum_{x=0}^{N_{\mathrm{St}}-1}\sum_{y=0}^{N_{\mathrm{St}}-1}\sqrt{p_x p_y}d_{yx}^{(k)}\sum_{m=0}^{\infty}\frac{\beta_x^m(\overline{\beta}_y)^m}{m!}\right) \\
&= \sum_{x=0}^{N_{\mathrm{St}}-1}\sum_{y=0}^{N_{\mathrm{St}}-1}\sqrt{p_x p_y}d_{yx}^{(k)}\left(e^{-|\beta_x|^2}\sum_{m=0}^{\infty}\frac{|\beta_x|^{2m}}{m!}\right) \\
&= \sum_{x=0}^{N_{\mathrm{St}}-1}\sum_{y=0}^{N_{\mathrm{St}}-1}\sqrt{p_x p_y}d_{yx}^{(k)}e^{-|\beta_x|^2}e^{|\beta_x|^2} \\
&= \sum_{x=0}^{N_{\mathrm{St}}-1}\sum_{y=0}^{N_{\mathrm{St}}-1}\sqrt{p_x p_y}d_{yx}^{(k)},
\end{aligned}
$$

as expected.

A.8. Constraining by experimental data

In this section, we calculate the expectation values for the measurement results both for the ideal untrusted and the non-ideal trusted detector scenario.

A.8.1. Expectation values for the ideal untrusted detector

We begin with the expectation values for the ideal untrusted detector scenario. According to Section 4.2.2 (and [28]) the measurement operators are given by

$$\begin{aligned}
\hat{q} &= \frac{1}{\sqrt{2}}\left(\hat{a}^\dagger + \hat{a}\right), \\
\hat{p} &= \frac{i}{\sqrt{2}}\left(\hat{a}^\dagger - \hat{a}\right), \\
\hat{n} &= \frac{1}{2}\left(\hat{q}^2 + \hat{p}^2 - 1\right) = \hat{a}^\dagger\hat{a} = \hat{a}\hat{a}^\dagger - 1, \\
\hat{d} &= \hat{q}^2 - \hat{p}^2 = (\hat{a})^2 + \left(\hat{a}^\dagger\right)^2 .
\end{aligned}$$

Using equation (1.8) we can calculate the expectation value for anti-normally ordered operators by the Q-function. According to our channel model, Bob receives a displaced thermal state $\rho_B^x = \hat{D}(\sqrt{\eta_t}\alpha)\hat{\rho}_{th}\hat{D}^\dagger(\sqrt{\eta_t}\alpha)$ with mean photon number $\bar{n} = \frac{1}{2}\eta_t\xi$. The Q-function for Bob's state can be obtained by inserting this into equation (1.7),

$$Q_x(\gamma) = \frac{1}{\pi\left(1 + \frac{1}{2}\eta_t\xi\right)} e^{-\frac{|\gamma - \sqrt{\eta_t}\alpha_x|^2}{1+\frac{1}{2}\eta_t\xi}} . \tag{A.27}$$

Note that this coincides with the conditional probability in equation (5.16).

To ease the notation, we use γ_r and γ_i for $\Re(\gamma)$ and $\Im(\gamma)$ interchangeably and we introduce the abbreviations $\beta_x := \sqrt{\eta_t}\alpha_x$ and $\sigma^2 := 1 + \frac{1}{2}\eta_t\xi$. We need to calculate the following integrals

$$\langle\hat{q}\rangle_x = \int d^2\gamma \frac{(\bar{\gamma} + \gamma)}{\sqrt{2}} Q_x(\gamma) = \frac{\sqrt{2}}{\pi\left(1 + \frac{1}{2}\eta\xi\right)} \int d^2\gamma \; \gamma_r e^{-\frac{|\gamma - \sqrt{\eta}\alpha_x|^2}{1+\frac{1}{2}\eta\xi}} , \tag{A.28}$$

$$\langle\hat{p}\rangle_x = \int d^2\gamma \frac{i\left(\bar{\gamma} - \gamma\right)}{\sqrt{2}} Q_x(\gamma) = \frac{\sqrt{2}}{\pi\left(1 + \frac{1}{2}\eta\xi\right)} \int d^2\gamma \; \gamma_i e^{-\frac{|\gamma - \sqrt{\eta}\alpha_x|^2}{1+\frac{1}{2}\eta\xi}} , \tag{A.29}$$

$$\langle\hat{n}\rangle_x = \int d^2\gamma \left(|\gamma|^2 - 1\right) Q_x(\gamma) = \frac{1}{\pi\left(1 + \frac{1}{2}\eta\xi\right)} \int d^2\gamma \left(\gamma_r^2 + \gamma_i^2 - 1\right) e^{-\frac{|\gamma - \sqrt{\eta}\alpha_x|^2}{1+\frac{1}{2}\eta\xi}} , \tag{A.30}$$

$$\langle\hat{d}\rangle_x = \int d^2\gamma \left(\gamma^2 + \bar{\gamma}^2\right) Q_x(\gamma) = \frac{2}{\pi\left(1 + \frac{1}{2}\eta\xi\right)} \int d^2\gamma \left(\gamma_r^2 - \gamma_i^2\right) e^{-\frac{|\gamma - \sqrt{\eta}\alpha_x|^2}{1+\frac{1}{2}\eta\xi}} , \tag{A.31}$$

where $\gamma = \gamma_r + i\gamma_i$. We consider the following integrals.

$$\begin{aligned}
\int d^2\gamma\ \gamma_r e^{-\frac{|\gamma-\beta|^2}{\sigma^2}} &= \int_{-\infty}^{\infty} d\gamma_r \int_{-\infty}^{\infty} d\gamma_i\ \gamma_r e^{-\frac{(\gamma_r-\beta_r)^2}{\sigma^2}} e^{-\frac{(\gamma_i-\beta_i)^2}{\sigma^2}} \\
&\overset{(1)}{=} \sqrt{\pi}\sigma \int_{-\infty}^{\infty} d\gamma_r\ \gamma_r e^{-\frac{(\gamma_r-\beta_r)^2}{\sigma^2}} \\
&\overset{(2)}{=} \sqrt{\pi}\sigma \int_{-\infty}^{\infty} dz\ (z+\beta_r) e^{-\frac{z^2}{\sigma^2}} \\
&\overset{(3)}{=} \pi\sigma^2\beta_r
\end{aligned}$$

For (1) we used the Gaussian integral $\int_{-\infty}^{\infty} dx e^{-\frac{x^2}{\sigma^2}} = \sqrt{\pi}\sigma$, for (2) we substituted $z := \gamma_r - \beta_r$ and for (3) we noticed that $ze^{-\frac{z^2}{\sigma^2}}$ is an odd function that is integrated over a symmetric integral and used the Gaussian integral again. Similarly, we obtain

$$\int d^2\gamma\ \gamma_i e^{-\frac{|\gamma-\beta|^2}{\sigma^2}} = \pi\sigma^2\beta_i.$$

Next we consider

$$\begin{aligned}
\int d^2\gamma\ \gamma_r^2 e^{-\frac{|\gamma-\beta|^2}{\sigma^2}} &= \int_{-\infty}^{\infty} d\gamma_r \int_{-\infty}^{\infty} d\gamma_i\ \gamma_r^2 e^{-\frac{(\gamma_r-\beta_r)^2}{\sigma^2}} e^{-\frac{(\gamma_i-\beta_i)^2}{\sigma^2}} \\
&\overset{(1)}{=} \sqrt{\pi}\sigma \int_{-\infty}^{\infty} d\gamma_r\ \gamma_r^2 e^{-\frac{(\gamma_r-\beta_r)^2}{\sigma^2}} \\
&\overset{(2)}{=} \sqrt{\pi}\sigma \int_{-\infty}^{\infty} dz\ (z^2 + 2\beta_r z + \beta_r^2) e^{-\frac{z^2}{\sigma^2}} \\
&\overset{(3)}{=} \sqrt{\pi}\sigma \left(\sigma^3 \int_{-\infty}^{\infty} dx\ x^2 e^{-x^2} + \beta_r^2 \sqrt{\pi}\sigma \right) \\
&\overset{(4)}{=} \sqrt{\pi}\sigma \left(\sigma^3 \int_{-\infty}^{\infty} dx\ \frac{1}{2} \left[e^{-x^2} - \frac{d}{dx} \left(x e^{-x^2} \right) \right] + \beta_r^2 \sqrt{\pi}\sigma \right) \\
&\overset{(5)}{=} \sqrt{\pi}\sigma \left(\frac{1}{2}\sigma^3\sqrt{\pi} + \beta_r^2\sqrt{\pi}\sigma \right) \\
&= \frac{1}{2}\pi\sigma^4 + \pi\sigma^2\beta_r^2.
\end{aligned}$$

For (1) we used the Gaussian integral, for (2) we substituted $z = \gamma_r - \beta_r$, for (3) we recognised that the second part of the integral is an odd function that is integrated over a symmetric integral, hence vanishes. Furthermore, we substituted $x := \frac{z}{a}$. For (4) we used the inverse product rule to rewrite the integral and for

(5) we utilised that $\lim_{x\to\pm\infty} xe^{-x^2} = 0$. Similarly, we obtain

$$\int d^2\gamma\ \gamma_i^2 e^{-\frac{|\gamma-\beta|^2}{\sigma^2}} = \frac{1}{2}\pi\sigma^4 + \pi\sigma^2\beta_i^2.$$

Combining these results, we find

$$\langle\hat{q}\rangle_x = \sqrt{2\eta_t}\Re(\alpha_x), \tag{A.32}$$

$$\langle\hat{p}\rangle_x = \sqrt{2\eta_t}\Im(\alpha_x), \tag{A.33}$$

$$\langle\hat{n}\rangle_x = \eta|\alpha_x|^2 + \frac{1}{2}\eta_t\xi, \tag{A.34}$$

$$\langle\hat{d}\rangle_x = 2\eta_t\left(\Re(\alpha_x)^2 - \Im(\alpha_x)^2\right) = \eta_t\left(\alpha_x^2 + \overline{\alpha_x}^2\right). \tag{A.35}$$

These results coincide with those stated in [28].

A.8.2. Expectation values for the non-ideal trusted detector

We proceed with a the calculation of the expectation values in the trusted noise scenario. According to Section 4.3, the measurement operators for the trusted noise scenario are given by

$$\begin{aligned}
\hat{F}_Q &= \int \frac{y^* + y}{\sqrt{2}} G_y\, d^2y, \\
\hat{F}_P &= \int i\frac{y^* - y}{\sqrt{2}} G_y\, d^2y, \\
\hat{S}_Q &= \int \left(\frac{y^* + y}{\sqrt{2}}\right)^2 G_y\, d^2y, \\
\hat{S}_P &= \int \left(i\frac{y^* - y}{\sqrt{2}}\right)^2 G_y\, d^2y.
\end{aligned}$$

Similarly to the preceding section, we want to calculate the expectation values using the conditioned probability density function, found in Chapter 5. According to equation (5.15) the conditioned probability for the measurement results $y \in \mathbb{C}$ given that Alice prepared a state corresponding to the symbol x reads

$$P(y|x) = \frac{1}{\pi\left(1 + \frac{1}{2}\eta_d\eta_t\xi + \nu_{el}\right)} e^{-\frac{|\sqrt{\eta_t\eta_d}\alpha_x - y|^2}{1+\frac{1}{2}\eta_d\eta_t\xi+\nu_{el}}}.$$

Then, we obtain the expectation values by

$$\langle \hat{F}_Q \rangle_x = \int d^2\gamma \frac{\bar{\gamma}+\gamma}{\sqrt{2}} P(\gamma|x) = \frac{\sqrt{2}}{\pi\left(1+\frac{1}{2}\eta_d\eta_t\xi+\nu_{el}\right)} \int d^2\gamma \gamma_r e^{-\frac{|\sqrt{\eta_t\eta_d}\alpha_x - y|^2}{1+\frac{1}{2}\eta_d\eta_t\xi+\nu_{el}}} \tag{A.36}$$

$$\langle \hat{F}_P \rangle_x = \int d^2\gamma i\frac{\bar{\gamma}-\gamma}{\sqrt{2}} P(\gamma|x) = \frac{\sqrt{2}}{\pi\left(1+\frac{1}{2}\eta_d\eta_t\xi+\nu_{el}\right)} \int d^2\gamma \gamma_i e^{-\frac{|\sqrt{\eta_t\eta_d}\alpha_x - y|^2}{1+\frac{1}{2}\eta_d\eta_t\xi+\nu_{el}}} \tag{A.37}$$

$$\langle \hat{S}_Q \rangle_x = \int d^2\gamma \frac{(\bar{\gamma}-\gamma)^2}{2} P(\gamma|x) = \frac{2}{\pi\left(1+\frac{1}{2}\eta_d\eta_t\xi+\nu_{el}\right)} \int d^2\gamma \gamma_r^2 e^{-\frac{|\sqrt{\eta_t\eta_d}\alpha_x - y|^2}{1+\frac{1}{2}\eta_d\eta_t\xi+\nu_{el}}} \tag{A.38}$$

$$\langle \hat{S}_P \rangle_x = \int d^2\gamma \frac{i^2(\bar{\gamma}-\gamma)^2}{2} P(\gamma|x) = \frac{2}{\pi\left(1+\frac{1}{2}\eta_d\eta_t\xi+\nu_{el}\right)} \int d^2\gamma \gamma_i^2 e^{-\frac{|\sqrt{\eta_t\eta_d}\alpha_x - y|^2}{1+\frac{1}{2}\eta_d\eta_t\xi+\nu_{el}}}. \tag{A.39}$$

We face similar integrals as in the previous calculations for the untrusted detector. Now we have $\sigma^2 := 1+\frac{1}{2}\eta_d\eta_t\xi+\nu_{el}$ and $\beta_x := \sqrt{\eta_t\eta_d}\alpha_x$ and, consequently, the normalisation factor for the probability distribution changes. So, we can reuse the derivations from the previous sections and obtain

$$\langle \hat{F}_Q \rangle_x = \sqrt{2\eta_t\eta_d}\Re(\alpha_x), \tag{A.40}$$

$$\langle \hat{F}_P \rangle_x = \sqrt{2\eta_t\eta_d}\Im(\alpha_x), \tag{A.41}$$

$$\langle \hat{S}_Q \rangle_x = 2\eta_t\eta_d\Re(\alpha_x)^2 + 1 + \frac{1}{2}\eta_t\eta_d\xi + \nu_{el}, \tag{A.42}$$

$$\langle \hat{S}_P \rangle_x = 2\eta_t\eta_d\Im(\alpha_x)^2 + 1 + \frac{1}{2}\eta_t\eta_d\xi + \nu_{el}. \tag{A.43}$$

These results coincide with the expectation values given in [28].

Bibliography

[1] J. Altepeter, E. Jeffrey, and P. Kwiat. *Photonic State Tomography*, pages 105–159. Advances in Atomic, Molecular and Optical Physics. Dec. 2005.

[2] M. ApS. *The MOSEK optimization toolbox for MATLAB manual. Version 9.0.*, 2019.

[3] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, page 175, India, 1984.

[4] D. Bernstein. *Introduction to post-quantum cryptography*, pages 1–14. Springer, 01 2009.

[5] S. Boyd and L. Vandenberghe. *Convex Optimization*. Cambridge University Press, USA, 2004.

[6] P. J. Coles, E. M. Metodiev, and N. Lütkenhaus. Numerical approach for unstructured quantum key distribution. *Nature Communications*, 7:11712, May 2016.

[7] M. Curty, M. Lewenstein, and N. Lütkenhaus. Entanglement as a precondition for secure quantum key distribution. *Phys. Rev. Lett.*, 92:217903, May 2004.

[8] A. Denys, P. Brown, and A. Leverrier. Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation of coherent states. *arXiv:2103.13945 [quant-ph]*, 2021.

[9] I. Devetak and A. Winter. Distillation of secret key and entanglement from quantum states. *Proc.R.Soc.*, 461:207–235, Jan 2005.

[10] E. Diamanti and A. Leverrier. Distributing secret keys with quantum continuous variables: Principle, security and implementations. *Entropy*, 17(12):6072–6092, Aug 2015.

[11] A. Ferenczi and N. Lütkenhaus. Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning. *Phys. Rev. A*, 85:052310, May 2012.

[12] A. Ferenczi and N. Lütkenhaus. Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning. *Phys. Rev. A*, 85:052310, May 2012.

[13] M. Frank and P. Wolfe. An algorithm for quadratic programming. *Naval Research Logistics Quarterly*, 3(1-2):95–110, 1956.

[14] I. George, J. Lin, and N. Lütkenhaus. Numerical calculations of the finite key rate for general quantum key distribution protocols. *Physical Review Research*, 3(1), Mar 2021.

[15] M. Grant and S. Boyd. Graph implementations for nonsmooth convex programs. In V. Blondel, S. Boyd, and H. Kimura, editors, *Recent Advances in Learning and Control*, Lecture Notes in Control and Information Sciences, pages 95–110. Springer-Verlag Limited, 2008. `http://stanford.edu/~boyd/graph_dcp.html`.

[16] M. Grant and S. Boyd. CVX: Matlab software for disciplined convex programming, version 2.1. `http://cvxr.com/cvx`, Mar. 2014.

[17] D. Griffiths. *Introduction to Quantum Mechanics*. Cambridge University Press, 2017.

[18] F. Grosshans and P. Grangier. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.*, 88:057902, Jan 2002.

[19] M. Heid and N. Lütkenhaus. Efficiency of coherent-state quantum cryptography in the presence of loss: Influence of realistic error correction. *Phys. Rev. A*, 73:052316, May 2006.

[20] A. S. Holevo and R. F. Werner. Evaluating capacities of bosonic gaussian channels. *Phys. Rev. A*, 63:032312, Feb 2001.

[21] H. Hu, J. Im, J. Lin, N. Lütkenhaus, and H. Wolkowicz. Robust interior point method for quantum key distribution rate computation. *arXiv:2104.03847 [quant-ph]*, 2021.

[22] M. Jaggi. Revisiting Frank-Wolfe: Projection-free sparse convex optimization. In S. Dasgupta and D. McAllester, editors, *Proceedings of the 30th International Conference on Machine Learning*, volume 28-1 of *Proceedings of Machine Learning Research*, pages 427–435, Atlanta, Georgia, USA, 17–19 Jun 2013. PMLR.

[23] F. Kanitschar and C. Pacher. Postselection Strategies for Continuous-Variable Quantum Key Distribution Protocols with Quadrature Phase-Shift Keying Modulation. *arXiv:2104.09454v3 [quant-ph]*, 2021.

[24] F. Kanitschar and C. Pacher. Tight Secure Key Rates for CV-QKD with 8PSK Modulation. *arXiv:2107.06110 [quant-ph]*, 2021.

[25] F. Laudenbach, C. Pacher, and et.al. Continous-Variable Quantum Key Distribution with Gaussian Modulation - The Theory of Practical Implementations. *arXiv:1703.09278v3 [quant-ph]*, 2017.

[26] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel. Continuous-variable quantum key distribution with gaussian modulation-the theory of practical implementations. *Advanced Quantum Technologies*, 1(1):1800011, Jun 2018.

[27] U. Leonhardt. *Essential Quantum Optics: From Quantum Measurements to Black Holes*. Cambridge University Press, 2010.

[28] J. Lin and N. Lütkenhaus. Trusted detector noise analysis for discrete modulation schemes of continuous-variable quantum key distribution. *Physical Review Applied*, 14(6), Dec 2020.

[29] J. Lin, T. Upadhyaya, and N. Lütkenhaus. Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution. *Physical Review X*, 9(4), Dec 2019.

[30] G. Lindblad. Expectations and entropy inequalities for finite quantum systems. *Communications in Mathematical Physics*, 39:111–119, Jun 1974.

[31] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and et al. Quantum key distribution over25kmwith an all-fiber continuous-variable system. *Physical Review A*, 76(4), Oct 2007.

[32] B. R. Mollow and R. J. Glauber. Quantum theory of parametric amplification. i. *Phys. Rev.*, 160:1076–1096, Aug 1967.

[33] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, New York, NY, USA, 10th edition, 2011.

[34] K. Oldham, J. Myland, and J. Spanier. *The Laguerre Polynomials Ln(x)*, pages 209–216. Springer, New York, NY, 2008.

[35] K. Petersen and M. Pedersen. The Matrix Cookbook. `http://www2.imm.dtu.dk/pubdb/p.php?3274`, 2012.

[36] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, and et al. Advances in quantum cryptography. *Advances in Optics and Photonics*, 12(4):1012, Dec 2020.

[37] T. C. Ralph. Continuous variable quantum cryptography. *Phys. Rev. A*, 61:010303, Dec 1999.

[38] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, Feb. 1978.

[39] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81:1301–1350, Sep 2009.

[40] C. E. Shannon. Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4):656–715, 1949.

[41] P. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[42] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 299(5):1484–1509, Oct. 1997.

[43] P. W. Shor and J. Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441–444, Jul 2000.

[44] D. Slepian and J. Wolf. Noiseless coding of correlated information sources. *IEEE Transactions on Information Theory*, 19(4):471–480, 1973.

[45] M. Suda. *Quantum Interferometry in Phase Space: Theory and Applications.* Springer, 2006.

[46] D. Sych and G. Leuchs. Coherent state quantum key distribution with multi letter phase-shift keying. *New Journal of Physics*, 12(5):053019, may 2010.

[47] K. C. Toh, M. J. Todd, and R. H. Tütüncü. Sdpt3 — a matlab software package for semidefinite programming, version 1.3. *Optimization Methods and Software*, 11(1-4):545–581, 1999.

[48] P. Tombsi and O. Hirota. Quantum Measurement Problem and State Dual Representations. In *Quantum Communication, Computing and Measurement 3*, pages 151 – 154. Springer Science+Business Media New York, 2002.

[49] T. Tyc and B. C. Sanders. Operational formulation of homodyne detection. *Journal of Physics A: Mathematical and General*, 37(29):7341–7357, Jul 2004.

[50] R. H. Tütüncü, K. C. Toh, and M. J. Todd. Solving semidefinite-quadratic-linear programs using sdpt3. *Mathematical Programming*, 95(2):189–217, 2003.

[51] T. Upadhyaya, T. van Himbeeck, J. Lin, and N. Lütkenhaus. Dimension reduction in quantum key distribution for continuous- and discrete-variable protocols. *PRX Quantum*, 2(2), May 2021.

[52] J. Watrous. *The Theory of Quantum Information.* Cambridge University Press, 2018.

[53] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd. Gaussian quantum information. *Rev. Mod. Phys.*, 84:621–669, May 2012.

[54] M. M. Wilde. *Quantum Information Theory.* Cambridge University Press, USA, 1st edition, 2013.

[55] A. Winick, N. Lütkenhaus, and P. J. Coles. Reliable numerical key rates for quantum key distribution. *Quantum*, 2:77, Jul 2018.

[56] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 26:802–803, Oct 1982.