TECHNISCHE UNIVERSITÄT WIEN
Vienna University of Technology

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

DIPLOMARBEIT

Finite-size Security Proof for Discrete-Modulated CV-QKD Protocols

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Technische Mathematik

eingereicht von

Dipl.-Ing. Florian KANITSCHAR, BSc, BSc

Matrikelnummer: 01425971

ausgeführt am
Institute for Quantum Computing an der University of Waterloo
und an der Technischen Universität Wien

unter der Anleitung von
Prof. Dr. Norbert Lütkenhaus,

Wien, am 15.10.2022

Florian Kanitschar

Norbert Lütkenhaus

Statement of contributions

This thesis, including the underlying data and results, are effectively my own, apart from my supervisor Norbert Lütkenhaus' advice and suggestions. Besides that, I want to acknowledge the following contributions to my thesis.

With the permission of my co-authors Ian George, Jie Lin, Twesh Upadhyaya and Norbert Lütkenhaus, large parts of Chapters 4 and 5, which present the finite-size security proof and the results of our numerical simulations, as well as of Appendices A, B and C, where we provide detailed proofs and derivations for statements in the main part, are taken from a preliminary version of the manuscript

[55] **F. Kanitschar**, I. George, J. Lin, T. Upadhyaya, and N. Lütkenhaus. Finite-Size Security for Discrete-Modulated Continuous-Variable Quantum Key Distribution Protocols. Manuscript forthcoming (2022)

representing our common work that is going to be published soon. Hence, these sections report the results of our common research. I am the first author of this document and wrote the vast majority of the text, hence these lines represent my own words.

The code used to generate the numerical results builds up upon the code for the numerical framework by the OQCT group at the Institute for Quantum Computing at the University of Waterloo. The particular version of the code I based my developments on was provided by Twesh Upadhyaya.

Besides that, during my work in the OQCT group at the Institute for Quantum Computing at the University of Waterloo, I contributed to the publication

[65] M Liu, **F. Kanitschar**, A. Arquand, and E. Y.-Z. Tan. Lipschitz continuity of quantum-classical conditional entropies with respect to angular distance, and related properties of angular distance. arXiv:2210.04874 [quant-ph] (2022)

authored by Michael Liu and co-authored by Amir Arquand and Ernest Tan and me. However, since this work is not directly related to the main topic of the present thesis, it is not covered therein.

Abstract

In Quantum Key Distribution (QKD) two remote parties aim to establish an information-theoretically secret key based on the laws of quantum mechanics. In contrast to frequently used classical encryption schemes, QKD is forward-secure, i.e., keys that are secure when they are generated cannot be reconstructed in the future, and do not rely on assumptions about the computational power of an eavesdropper or the existence of efficient algorithms for solving complex mathematical problems. Therefore, QKD allows secret communication even in the presence of scalable quantum computers. To perform quantum key distribution it requires a physical implementation, a protocol describing the steps both parties have to conduct and a security proof - which means finding a lower bound on the secure key rate, given a model of the practical implementation and some reasonable assumptions. For a long time, one of these assumptions was that the communicating parties can exchange infinitely long keys. This, of course, is an idealisation and does not hold true in the real world.

In this work, we analyse the security of a general discretely modulated continuous-variable quantum key distribution (DM CV-QKD) protocol in the finite-size regime. We use Renner's finite-size security proof framework [85] to establish composable security against i.i.d. collective attacks. CV-QKD protocols rely on measuring continuous quantities like the position and momentum of quantum states that live in infinite-dimensional Hilbert spaces. Therefore, one of the major challenges for finite-size security proofs for DM CV-QKD protocols is handling these infinite-dimensional systems properly. We introduce and prove a new noise-robust energy testing theorem that helps to bound the weight of the exchanged signals outside a finite-dimensional cutoff space and apply the dimension reduction method [105] to rigorously take the impact of this cutoff on the secure key rate into account. Although this energy test is an integral part of our security argument, we highlight that it is an interesting result on its own that might turn out to be useful in various contexts of quantum computation and communication. After extending Renner's framework to infinite-dimensional side-information, we finally apply a numerical security proof framework [19, 110] to calculate tight lower bounds on the secure key rate for different theoretically interesting and practically relevant scenarios.

The present security proof's flexible structure allows taking adaptations according to the experimentalist's and user's demands into account. For example, in contrast to many existing proof techniques, our method can take postselection into

account and does not rely on a particular physical model (e.g., of the detector or the channel), which makes it a useful tool for everyone working with practical QKD systems. This work presents another important step forward, towards the widespread deployment of practical (DM) CV-QKD systems, which will be essential for secure communication in the future.

Key words: Quantum Key Distribution, Quantum Cryptography, Quantum Communication, Continuous-Variable QKD, Security Proof, Composability, Finite-Size

Kurzfassung

Quantenschlüsselverteilung - kurz QKD für *Quantum Key Distribution* - ist ein Verfahren bei dem zwei Parteien einen informationstheoretisch sicheren Schlüssel, basierend lediglich auf den Gesetzen der Quantenmechanik, erzeugen. Der große Vorteil gegenüber gängigen Verschlüsselungsverfahren ist, dass QKD vorwärts gerichtet sicher (engl. *forward secure*) ist. Das bedeutet Schlüssel, die zum Zeitpunkt der Erzeugung sicher waren, können auch in der Zukunft nicht rekonstruiert werden. Außerdem ist die Sicherheit eines durch QKD erzeugten Schlüssels nicht abhängig von Annahmen über die Rechenleistung von Angreifern oder die Existenz effektiver Algorithmen für die Lösung schwieriger mathematischer Probleme und ermöglicht daher selbst in der Gegenwart skalierbarer Quantencomputer geheime Kommuniaktion.

Neben einer physischen Umsetzung und einem QKD Protokoll ist ein sogenannter Sicherheitsbeweis, die Ermittlung einer unteren Schranke an die garantiert sichere Schlüsselrate im Rahmen eines realistischen Modells des gesamten Systems und weiterer sinnvoller Annahmen, essenziell für die praktische Implementierung eines QKD Systems. Für lange Zeit war eine dieser Annahmen, dass die beiden kommunizierenden Parteien unendlich viele Signale austauschen können. Selbstverständlich ist dies eine theoretische Idealisierung, die in der Realität nie erreicht werden kann.

Im Rahmen der vorliegenden Arbeit analysieren wir die Sicherheit eines allgemeinen diskret modulierten Quantenverschlüsselungsprotokolls mit kontinuierlichen Variablen (DM CV-QKD, engl. für *Discretely Modulated Continuous-Variable QKD*) im Regime endlich langer Schlüssel, dem sogenanten *finite-size regime*. Wir beweisen die Sicherheit gegen sogenannte *i.i.d. collective attacks*, d.h. unter der Annahme eines identisch und gleichverteiltem Angriffs bei anschließender gemeinsamer Messung aller eingesetzten Hilfszustände durch den Angreifer, aufbauend auf Renners finite-size Sicherheitsbeweis-Framework [85]. Der verwendete Sicherheitsbegriff ist modular (engl. *composable*), das bedeutet das Sicherheitsversprechen des Protokolls bleibt aufrecht, auch wenn es als Subprotokoll eines beliebigen größeren Protokolls eingesetzt wird, dessen andere Bestandteile ebenfalls modular sicher sind. CV-QKD Protokolle, wie ihr Name bereits impliziert, verlangen die Messung von kontinuierlichen Größen wie Ort und Impuls von Quantenzuständen in unendlichdimensionalen Hilberträumen. Eine besondere Schwierigkeit bei der Analyse von DM CV-QKD Protokollen stellt daher die korrekte Behandlung

dieser unendlichdimensionalen Systeme dar, da - im Gegensatz zu vielen gaußmodulierten CV-QKD Protokollen - keine Symmetrien ausgenützt werden können, um die effektive Dimension zu verkleinern. Wir beweisen ein Theorem, das - vorausgesetzt eine experimentell leicht zu überprüfende Bedingung ist erfüllt - das Gewicht der analysierten Zustände außerhalb eines endlichdimensionalen Unterraums (ein s.g. *cutoff space*) beschränkt. Dieser sogenannte Energy Test ist für sich ein interessantes Resultat dieser Arbeit und kann auch für Anwendungen außerhalb des gegenständlichen Sicherheitsbeweises relevant sein. Anschließend wenden wir die *dimension reduction method* [105], ein Verfahren zur rigorosen Behandlung des Fehlers bei der Einschränkung auf endlichdimensionale Unterräume, an und erweitern Renners Rahmenwerk auf Systeme mit unendlichdimensionale Nebeninformation. Schließlich berechnen wir scharfe untere Schranken an die garantiert sichere Schlüsselrate mithilfe einer numerischen Sicherheitsbeweismethode [19, 110] für verschiedene theoretisch interessante und praktisch relevante Szenarien.
Die flexible Struktur des gegenständlichen Sicherheitsbeweises erlaubt einfache Anpassungen auf experimentelle und praktische Bedürfnisse von Experimentatoren und Anwendern. Beispielsweise ist, im Gegensatz zu zahlreichen anderen Beweismethoden, Postselection möglich, das die Performance von Protokollen merklich steigern kann. Außerdem ist es relativ einfach möglich verschiedene physikalische Modelle - etwa des Kanals oder des Detektors - zu berücksichtigen. Die vorliegende Arbeit präsentiert somit einen wichtigen technischen Fortschritt bei finite-size Sicherheitsbeweisen for DM CV-QKD Protokolle und leistet somit einen wichtigen Beitrag für die zukünftige Verbreitung von Kommunikationssystemen zum sicheren und geheimen Nachrichtenaustausch.

Schlagwörter: Quantenschlüsselverteilung, Quantenkryptographie, Quantenkommunikation, QKD mit kontinuierlichen Variablen, Sicherheitsbeweis, Composability, Finite-Size

Acknowledgements

I want to dedicate these lines to all people that supported me in accomplishing this thesis.

First and foremost I want to thank my advisor Prof. Dr. Norbert Lütkenhaus for giving me the outstanding opportunity to do my research for the present thesis in his group, in particular for his patience and endurance to make my stay in Waterloo possible even though at some points organisational challenges with my visa and working permit and a pandemic made it look almost impossible. I owe him a great debt of gratitude for sharing his insight and his unique view on quantum communication, for motivating me to become better every day and for his very principled approach to doing research. I am very grateful for the opportunity to experience and learn those and many more lessons first hand. Furthermore, I want to thank him for his cheerful, kind and human way of supervising and for his patience and understanding in all aspects.

Thanks to my collaborators and co-authors Ian George, Jie Lin and Twesh Upadhyaya for their contributions to our common research. Ian, thank you so much for sharing your insight on finite-key analysis, pointing out invisible connections, and for patiently answering all my questions. Jie, thank you very much for your guidance, for always having a good suggestion in mind and for pushing me to look at every detail. Twesh, thank you a lot for having time to discuss while finishing your own thesis, for providing code for and explanations about your dimension reduction method.

Many thanks to my colleagues and friends in the research group. Alex, Amir, Devashish, Ernest, Evan, Jack, Lars, Michael, Mikka, Scott, Shlok and Srijita, thank you for welcoming me so warmly to the group, for countless unforgettable lunch and cookie times, for many fun afternoons, evenings and nights. You made my time in Waterloo unforgettable!

Special thanks go to Devashish Tupkary, Jack Burniston, Lars Kamin and Shlok Nahar for many helpful whiteboard discussions and thanks to Jack for being our always helpful and patient coding and tech support. My thanks go as well to Ernest Tan, who constantly disentangled our confusion and patiently answered

our questions, not only in the reading group.

Thanks to David Wörgötter, Lars Kamin and Karabee Batta for proofreading early versions of my thesis. David, thank you very much for spotting even tiny details, in particular in the background section and for your beneficial feedback. Lars, special thanks for squeezing reading over my thesis in your tough timetable, for analysing my lines through your QKD glasses and for your very valuable comments. Karabee, thank so much you for your precious feedback on my thesis, for improving my English, for having an eye for details and for the artistic and humorous illustration of alternative occurrences of Gaussian waves.

I want to thank my friends and fellow students at TU Wien who accompanied me through the last years, including countless afternoons and evenings working on assignment problems or studying together, as well as many fun free-time activities. In particular, I want to mention Tobias Forster, who always had an open ear and encouraging words and became a true friend over the course of our common studies.

Last but not least I want to express my sincere gratitude to my parents, Gerda and Johann Kanitschar. Thank you for your support in so many ways, your confidence, your understanding and your love, making my studies, including this thesis, possible.

Contents

1. Introduction

The transmission of secret messages between two legitimate parties has been an integral task in human societies since the first ancient empires formed, and has gained even more importance in the digital world we live in nowadays, where almost every aspect of people's daily life - the exchange of confidential text messages, accessing user accounts, controlling medical devices, digital signatures, or electronic payments - is heavily reliant on protecting vulnerable data from third parties. Pioneers like Claude Shannon introduced the field of classical cryptography during the early and mid-20th century. He proved [94] that the so-called One-Time-Pad, a primitive to encrypt messages, is secure (if every key is used only once) and optimal (which means that there is no cryptographic protocol which uses a shorter key and is provable secure). However, the main drawback of the One-Time-Pad is that it requires the key to be of the same length as the message to be encrypted. Therefore, nowadays classical encryption schemes use different methods that rely on certain assumptions about the computational resources of adversaries and the difficulty of a mathematical problem. One of the most prominent examples is the Rivest-Shamir-Adleman (RSA) public encryption scheme, which relies on the computational hardness of prime-factorisation, i.e., the assumption that there is no efficient algorithm to factorise large numbers. This, however, is not a proven fact and therefore there is no guarantee that no efficient algorithm exists and can be found in the future. This imposes a severe security threat, once an efficient algorithm has been found, not only for current messages but even for past communication, which can be decrypted, given someone recorded and stored the communication transcripts. In 1994 Peter Shor discovered an efficient factoring algorithm for quantum computers, a new concept of computation based on quantum mechanics, envisioned by Nobel Prize laureate Richard Feynman about a decade earlier. His discovery did not only impose a sincere threat to nowadays encryption schemes, but also pushed the young field of Quantum Information Theory to work both on the development of quantum computers, which are expected to tackle difficult computational problems classical computers fail to solve, and new, quantum-safe, encryption methods.
Post Quantum Cryptography [7] aims to replace the commonly used mathematical problems (integer prime-factorisation, discrete logarithm and elliptic-curve discrete logarithm) in public-key algorithms by tasks that are not known to be easily solvable by quantum computers. While Post Quantum Cryptography only requires

software changes, it continues the race between cryptographers and code-breakers, as it cannot be proven that no efficient algorithm for the new problem can be found. Therefore, the cryptographic algorithm needs to be replaced constantly, as soon as new quantum algorithms are discovered. In contrast, Quantum Key Distribution (QKD) aims to establish a provable information-theoretically secure key, relying solely on the laws of quantum mechanics without imposing any assumptions on the computational power of adversaries. Furthermore, thanks to the nature of quantum mechanics [113], Quantum Key Distribution is safe against future progress in quantum hacking, as in contrast to classical schemes, an adversary cannot record and store all information exchanged during the key-generation process. This property is called forward-security. Since QKD involves a physical process rather than a mathematical problem, it demands new devices and infrastructure and therefore is a hardware solution, which requires more expensive adaptations than Post Quantum Cryptography.

1.1. Quantum Key Distribution

Quantum Key Distribution was first envisioned by Charles Bennett and Gilles Brassard in 1984 when they showcased their famous BB84 protocol [6] and independently discovered by Arthur Ekert [27] in 1991 when he introduced his E91 protocol. The setting of QKD is the following. Two distant parties, commonly called Alice and Bob, want to establish a secret shared key. They are connected by two channels - an authenticated classical channel and a quantum channel, which can be wiretapped by an eavesdropper known as Eve. Useful implementations of QKD protocols require a practical implementation and an information-theoretic security proof taking the limitations and shortcomings of realistic devices sufficiently into account.
QKD protocols can be divided into two protocol families, based on the detection technology used in implementations, Discrete-Variable (DV) and Continuous-Variable (CV) protocols. As the name suggests, DV protocols like BB84, B92 and E91 [5, 6, 27] use discrete physical properties of photons, like their polarization and rely on single-photon sources and single-photon detectors. Continuous-Variable protocols were introduced in 1999 by Timothy Ralph [84] and independently in 2000 by Mark Hillery [48] and encode information into the quadratures and phase of the quantum electromagnetic field, employing lasers and heterodyne detectors to transmit information. Based on the modulation scheme, one can further distinguish between Gaussian Modulated (GM) CV-QKD protocols [16, 44, 45, 67] and Discretely Modulated (DM) CV-QKD protocols [47, 49, 112]. On the one hand, Continuous-Variable protocols use mature and noise-resilient hardware which is very similar to state-of-the-art telecommunication infrastructure, hence have a

head start when it comes to future large-scale implementations. On the other hand, DV protocols currently achieve higher transmission distances than CV protocols, hence enjoying a performance advantage.

Security proofs for DV protocols [95] are more mature than those for CV protocols, while CV security analyses usually take place in infinite-dimensional Hilbert spaces, making security statements more challenging. In contrast to DM protocols, GM CV-QKD protocols show a high symmetry, which can be exploited to ease security proofs [62]. However, this symmetry is broken in real-world applications, opening security gaps. Comprehensive reviews about Quantum Key Distribution can be found in [24, 81, 90].

In the present thesis, we focus on DM CV-QKD protocols and aim to close one of the remaining open questions in DM CV-QKD security analyses - proving the security in the finite-size regime. In order to make use of the law of large numbers and to ease the analysis, so far many DM CV-QKD security proofs [22, 38, 64] have assumed that Alice and Bob exchange infinitely many signals to establish their secret key. This is known as security in the asymptotic limit. While this is a handy idealisation for theoretical considerations, exchanging an infinite number of signals is impossible in practical implementations, since at some finite point in time Alice and Bob need to know the length of their secret key in order to encrypt messages. This gap between security analysis and implementation was first closed by Renner [85] in his PhD thesis, by analysing the finite-size security within his ϵ-security framework. However, it is not straightforward to apply this framework to a generic DM CV-QKD protocol. In general, proving the security of a given QKD protocol means to lower-bound the achievable secure key rate within the used physical model. This lower bound can be achieved either by analytical or numerical security proofs. While analytical security proofs for CV-QKD protocols are often very technical and not very flexible regarding changes in the protocol structure or the physical model, numerical security proofs enjoy this flexibility at the cost of high computational demands and numerical imprecision.

So far, only a few DM CV-QKD finite-key analyses are available. Furrer et.al. [33, 34] proved security against general attacks for a protocol employing entangled states and digitalised homodyne detection using an argument based on an entropic uncertainty relation. However, their key rates do not converge against the known asymptotic limit bounds for large block sizes. Matsuura et.al. [69] present a finite-size security proof of a special two-state protocol using coherent states. Their security proof method does not seem to be easily generalisable to a broader protocol class and their key rates do not converge to the asymptotic bounds as the number of rounds goes to infinity. A recent work done by Lupo and Ouyang [68] presents a security analysis against collective i.i.d. attacks, exploiting the limitations of realistic detectors. Even though their key rates converge towards the asymptotic

bound (given by [22], which is known to be loose for a low number of signal states), the obtained key rates and the achievable range are rather low.
We introduce a general DM CV-QKD protocol and analyse its security against i.i.d. collective attacks in the finite-size regime. Therefore, we develop and apply a so-called energy test, rigorously extend Renner's ϵ-security framework [85] to infinite-dimensional side-information and apply a recent numerical security proof framework [19, 110] to calculate tight lower bounds on the secure key rate. Our analysis includes both untrusted, ideal and trusted, non-ideal detectors, hence is capable of taking realistic settings into account. The obtained finite-size key rates converge to the asymptotic limit (given by [64, 105], which is believed to be tight). Therefore, even though, due to the different assumptions in [68], a direct comparison is difficult, both our key rate and our maximal achievable transmission distance can be considered superior to the results in [68].

1.2. Structure of the Thesis

The present thesis is structured as follows. This brief introduction to the field of Quantum Key Distribution is succeeded by Chapter 2, where we review the mathematics required to follow the present thesis, as well as background on quantum information theory and quantum optics that builds the physical backbone of this work. In Section 2.1 we introduce mathematical quantities required to embed quantum theory in the mathematical framework of Hilbert spaces and to describe quantum states as positive operators acting on Hilbert spaces. Then, in Section 2.2 we introduce quantum states, formalise the physical measurement process mathematically and explain how the evolution of quantum states can be described with so-called quantum channels, which are completely positive, trace-preserving maps. Furthermore, we discuss how to measure similarity between quantum states. Another essential task in this thesis is quantifying information. In Section 2.3 we review several entropic quantities like the classical Shannon entropy and its quantum mechanical counterpart, the von Neumann entropy, followed by smooth min- and max-entropies, which will turn out to be essential for the finite-size analysis of quantum key distribution protocols. We conclude this chapter by a brief overview of quantum optics in Section 2.4, beginning with harmonic oscillators and coherent states, leading over to the mathematical description of optical instruments that are used for practical implementations of QKD and a short review about conic programming in Section 2.5.
Chapter 3 aims to give an introduction to Quantum Key Distribution and to introduce notions that are required to follow the security proof in the main part of the thesis. We begin with defining the basic setting of QKD and its advantages over classical cryptography in Section 3.1. Based on that we introduce a generic

QKD protocol to illustrate the process of generating a secret key. In Section 3.3 we elaborate on the process of proving security of QKD protocols. We begin with the discussion of different eavesdropping strategies which classify the power we allow a potential adversary to have and lead over to the notion of asymptotic and finite-size security. Finally, we discuss composability, which turns out to be the right security concept for cryptographic schemes. However, as perfect security can never be achieved in real-world applications, we have to allow small deviations from ideal devices and protocols which leads us to the concept of epsilon security. In Section 3.4 we review the numerical security proof framework we use in this work. First, we explain how this numerical approach provides a tight lower bound on the achievable secure key rate using a two-step process and we show how the framework is applied to DM CV-QKD protocols. However, although dealing with infinite-dimensional Hilbert spaces, at this point we still need to assume to perform our calculations in a finite-dimensional subspace to make the problem computationally feasible. We then address this issue by reviewing the dimension reduction method which rigorously explains how this so-called photon-number cutoff can be removed at the cost of introducing a small correction term to the key rate. Then, we explain how this framework can be extended to take imperfect detectors into account.

Chapter 4 is the core part of the thesis, where we present the main results of this work. We start by reviewing the current state of security proofs for DM CV-QKD protocols in Section 4.1. In Section 4.2 we point out a crucial point for (numerical) finite-size security proofs - estimating the maximal energy of photons considered in the analysis. Procedures that make statistical statements about the maximum energy in the considered rounds of quantum signals are called energy test. We review existing energy tests and point out why they are not suitable for the finite-size security analysis of general DM CV-QKD protocols with our numerical proof method. Based on this overview, we formulate requirements for a suitable energy test. In Section 4.3 we describe the general DM CV-QKD protocol we analyse in this work. Finally, in Section 4.4 we present the main result of the present thesis. We state our new energy test and prove composable security against i.i.d. collective attacks in the finite-size regime for a general DM CV-QKD protocol. This section focuses on a clear presentation of the proof, postponing technical proof steps and lengthy calculations to the appendix.

In Chapter 5, we calculate numerical secure key rates for a four-state phase-shift keying protocol. After a brief discussion of the choice of the weight in Section 5.2 and details about the implementation in Section 5.3, we state our numerical results in Section 5.4. We present numerical key rate curves both for the untrusted, ideal detector scenario and the trusted, non-ideal detector scenario and show that secure key rates can be obtained up to 100km transmission distance under experimentally viable conditions. Finally, we give a brief summary and conclusion in Chapter 6.

Many detailed proofs and calculations are given in the Appendices. In Appendix A, we prove our noise-robust energy testing theorem. In Appendix B.1 we give proofs for technical lemmas and theorems that are used in the security proof of our main theorem. In Appendix B.2 we generalise Renner's asymptotic equipartition property to infinite-dimensional side-information. In Appendix C we derive the finite-dimensional optimisation problem we solve numerically to lower-bound the finite-size key rate.

2. Background

In this chapter, we review the mathematics used throughout the thesis and give some necessary background on quantum information theory, quantum optics and convex optimisation, required to describe and analyse quantum key distribution (protocols). At the same time, we introduce some common notions and give definitions used throughout the whole thesis.

2.1. Mathematical preliminaries

> Quantum phenomena do not occur in a Hilbert space. They occur in a laboratory.
>
> *Asher Peres* [78, p. 373]

We begin by introducing the basic mathematical structure behind quantum mechanics and quantum information theory. We assume that readers are familiar with basic linear algebra, calculus and functional analysis, as it can be found in every introductory book on those topics. A review of the most essential mathematical background required to follow the present thesis is, for example, given in [108, Sections 1.1 and 1.2]. The definitions provided in this section are general and can be found in many books on functional analysis (see, for example, [54, 89]).

The mathematical formulation of quantum mechanics takes place in Hilbert spaces, so quantum mechanical objects and operations are represented by objects 'living' in or acting on Hilbert spaces. Many concepts that come with Hilbert spaces, like dual spaces, orthogonality and unitary operators play a crucial role in quantum theory. Therefore, we start with the following definitions.

Definition 2.1.1: Hilbert Space

*A **Hilbert space** $\mathcal{H}$ is a real or complex vector space equipped with an inner product $\langle \cdot, \cdot \rangle$ that is a complete normed space (i.e., a Banach space) with respect to the distance measure induced by its inner product, $||\cdot|| := \sqrt{\langle \cdot, \cdot \rangle}$. A Hilbert space $\mathcal{H}$ is called **separable** if it contains a countable, dense subset.*

Inner products are assumed to be conjugate linear in the first argument and linear in the second argument, which is known as *physicist's convention*. In the present thesis, we consider only separable Hilbert spaces over $\mathbb{C}$. Since every norm $|| \cdot ||$ induces a metric d_M via $d_M(x, y) := ||x - y||$, separable Hilbert spaces are metric spaces and we can presume that all Hilbert spaces in the present thesis have a countable basis. Next, we define the dual space of a Hilbert space.

Definition 2.1.2: Dual Space

*The **dual space** $\mathcal{H}^*$ of a Hilbert space $\mathcal{H}$ is the set of all linear maps from $\mathcal{H}$ to $\mathbb{C}$.*

Following the convention in quantum information theory, we use Dirac's BraKet notation throughout the whole thesis. States, i.e., vectors in $\mathcal{H}$, are denoted by a descriptive symbol or letter between a vertical line and a right angle bracket called *ket*, $|\cdot\rangle$. Linear forms, i.e., elements of the dual space $\mathcal{H}^*$, are denoted by a descriptive symbol or letter between a left angle bracket and a vertical line called *bra*, $\langle\cdot|$. The action of the bra $\langle\Phi|$ on the ket $|\Psi\rangle$ is then given by $\langle\Phi|\Psi\rangle$. Mathematically, the Riesz-Fréchet representation theorem (see, for example, [54, Theorem 9.16]) allows us to identify a Hilbert space with its topological dual space (in more detail it states that a Hilbert space and its dual space are isometrically isomorphic). Hence, for every ket $|\Phi\rangle$ we find a unique bra, and we are allowed to denote the inner product by $\langle\Phi|\Psi\rangle$. We are going to use this notation for the inner product on many occasions in the rest of this thesis.

2.1.1. Operator Theory

> At the moment physics is again terribly confused. In any case, it is too difficult for me, and I wish I had been a movie comedian or something of the sort and had never heard of physics.
>
> *Wolfgang Pauli (1924)* [17, p. 114]

The introductory quote, where later Nobel prize laureate Wolfgang Pauli refers to his struggles with the formulation of quantum theory at this time, highlights the unsatisfactory state of quantum theory in its early days. Even after Schrödinger showed the equivalence of his wave mechanics with Heisenberg's matrix mechanics, the general formalism of quantum mechanics still relied on mathematically ill-defined objects like the Dirac delta function [107]. It required the genius of John von Neumann to recognise that the theory of Hilbert spaces and linear operators acting upon them provides a very natural way of describing quantum mechanics [73] and it was as well von Neumann who generalised operator theory to unbounded observables [74], which resulted in a framework able to meet the requirements of quantum mechanics. Therefore, in the present section, we review those parts of operator theory that will be relevant to this work.

Operators are mathematical objects that map vectors from one Hilbert space to another one. As quantum mechanics is a linear theory, our focus will be on linear operators. Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be two Hilbert spaces. We denote the vector space of linear operators from $\mathcal{H}_A$ to $\mathcal{H}_B$ by $\mathrm{L}(\mathcal{H}_A, \mathcal{H}_B)$. If $\mathcal{H}_A = \mathcal{H}_B =: \mathcal{H}$, we simply write $\mathrm{L}(\mathcal{H})$. In what follows, we characterise subsets of the space of linear operators. We start by defining the operator norm.

Definition 2.1.3: Operator Norm

The operator norm of an operator $A : \mathcal{H}_A \to \mathcal{H}_B$ is defined as

$$||A||_\infty := \sup_{\Psi \in \mathcal{H}_A : ||\Psi|| \leqslant 1} ||A\Psi||_{\mathcal{H}_B}.$$

This allows us to define a subset of the set of linear operators, characterised by having finite operator norm.

Definition 2.1.4: Bounded Operators

Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be separable Hilbert spaces.
The ***set of bounded operators*** *$\mathcal{B}(\mathcal{H}_A, \mathcal{H}_B)$ is defined by*

$$\mathcal{B}(\mathcal{H}_A, \mathcal{H}_B) := \{A \in \mathrm{L}(\mathcal{H}_A, \mathcal{H}_B) \ : \ ||A||_\infty < \infty\}$$

If $\mathcal{H}_A = \mathcal{H}_B =: \mathcal{H}$ we simply write $\mathcal{B}(\mathcal{H})$ to denote bounded operators on $\mathcal{H}$.

For every bounded operator $A \in \mathcal{B}(\mathcal{H})$, we can associate its adjoint operator $A^\dagger$ satisfying

$$\forall\, |\Phi\rangle, |\Psi\rangle \in \mathcal{H} : \ \langle \Phi | A\Psi \rangle = \langle A^\dagger \Phi | \Psi \rangle .$$

Operators that are equal to their own adjoint play a special role in quantum mechanics.

Definition 2.1.5: Hermitian Operators

A bounded operator $H \in \mathcal{B}(\mathcal{H})$ is called ***Hermitian*** *or* ***self-adjoint*** *if $H^\dagger = H$.*
We denote the set of Hermitian operators on $\mathcal{H}$ by $Herm(\mathcal{H})$.

An operator H is Hermitian if and only if $\forall\, |\psi\rangle \in \mathcal{H} : \ \langle \Psi | H | \Psi \rangle \in \mathbb{R}$. Another interesting subset is the set of positive operators.

Definition 2.1.6: Positive Semi-Definite Operators

A bounded operator $P \in \mathcal{B}(\mathcal{H})$ is called ***positive semi-definite****, $P \geqslant 0$, if*

$$\forall\, |\Phi\rangle \in \mathcal{H} : \ \langle \Phi | P | \Phi \rangle \geqslant 0.$$

We denote the set of ***positive semi-definite*** *or* ***non-negative*** *operators on $\mathcal{H}$ by $Pos(\mathcal{H})$.*

We have the following alternative characterisations of positive semi-definite operators. An operator P is positive semi-definite if and only if P is Hermitian and $\mathrm{spec}(P) \subseteq \mathbb{R}_0^+$. Alternatively, P is positive semi-definite if and only if there exists $X \in \mathcal{B}(\mathcal{H})$ such that $P = X^\dagger X$.

Definition 2.1.7: Normal Operators

A linear operator $N \in \mathrm{L}(\mathcal{H})$ is called ***normal*** *if $NN^\dagger = N^\dagger N$.*

Note that every Hermitian operator is normal. In many contexts we want to apply functions $f : \mathbb{C} \to \mathbb{C}$ to Hermitian operators. The spectral theorem allows us to extend scalar-valued functions naturally to normal operators. For example, we may extend the square-root, $\sqrt{H}$, or the logarithm, $\log(H)$ for $H \in \mathrm{Herm}(\mathcal{H})$.

Recall that for arbitrary $X \in \mathcal{B}(\mathcal{H})$ $X^\dagger X$ is not only self-adjoint but also positive, hence has only non-negative eigenvalues. Therefore, $\sqrt{X^\dagger X}$ is well-defined and can be used to define the absolute value of the operator X, $|X| := \sqrt{X^\dagger X}$.

Definition 2.1.8: Trace

Let $\mathcal{H}$ be a separable Hilbert space and $A \in \mathrm{Herm}(\mathcal{H}) \cap \mathrm{Pos}(\mathcal{H})$. Let $(\phi_i)_{i\in\mathcal{I}}$ be an orthonormal basis of $\mathcal{H}$.
The ***trace*** *of A, denoted by $\mathrm{Tr}[A]$, is defined by*

$$\mathrm{Tr}[A] := \sum_i \langle \phi_i | A | \phi_i \rangle .$$

The trace is independent of the choice of the particular orthonormal basis. Since A is Hermitian, according to the spectral theorem for Hermitian operators, there exists an orthonormal basis of eigenvectors of A. By choosing this orthonormal basis, we see that the trace is equal to the sum of all eigenvalues of A.

Now we are ready to introduce a family of norms called Schatten p-norms that include many of the most common norms in quantum information theory as special cases.

Definition 2.1.9: Schatten p-norm

Let $\mathcal{H}$ be a Hilbert space, $A \in \mathrm{L}(\mathcal{H})$ and $p \in [0, \infty)$. The ***Schatten p-norm*** *of A is given by*

$$||A||_p := \left(\mathrm{Tr}\left[|A|^p\right]\right)^{\frac{1}{p}} .$$

Interesting special cases include the trace-norm $||\cdot||_1$, the Hilbert-Schmidt norm $||\cdot||_2$ and the operator norm $||\cdot||_\infty$. Schatten p-norms satisfy Hölder's inequality.

Theorem 2.1.10: Hölder's inequality

For $A, B \in \mathrm{L}(\mathcal{H})$ $p, q \in [1, \infty)$ with $\frac{1}{p} + \frac{1}{q} = 1$

$$|\langle A, B\rangle| \leqslant ||A||_p ||B||_q. \tag{2.1}$$

Note that the inner product between two bounded operators $A, B \in L(\mathcal{H})$ acting on a separable Hilbert space $\mathcal{H}$ is understood as

$$\langle A, B\rangle := \mathrm{Tr}\left[A^\dagger B\right]. \tag{2.2}$$

A special role in quantum information play operators with finite Schatten 1-norm, so-called trace-class operators.

Definition 2.1.11: Trace Class Operators

*Let $A \in \mathrm{L}(\mathcal{H})$. The operator A is said to be in **trace class** if $||A||_1 < \infty$. We denote the set of all trace class operators over $\mathcal{H}$ by $\mathcal{T}(\mathcal{H})$.*
By $\mathcal{T}_1(\mathcal{H})$ we denote all trace class operators with Schatten 1-norm $\leqslant 1$ and by adding the superscript $+$, $\mathcal{T}^+(\mathcal{H})$, we denote positive trace class operators.

Having introduced trace class operators allows us to give a alternative definition for the set of positive operators, $\mathrm{Pos}(\mathcal{H}) = \mathrm{cone}(\mathcal{T}^+)$ (see Definition 2.5.44).
We proceed by informally defining isometries and unitary operators. The identity operator $\mathbb{1}_\mathcal{H}$ on $\mathcal{H}$ maps vectors $|\Psi\rangle \in \mathcal{H}$ to themselves, $\mathbb{1}_\mathcal{H}|\Psi\rangle = |\Psi\rangle$. A bounded operator $U \in \mathcal{B}(\mathcal{H}_A, \mathcal{H}_B)$ is called an **isometry** if $U^\dagger U = \mathbb{1}_{\mathcal{H}_A}$. If additionally $UU^\dagger = \mathbb{1}_{\mathcal{H}_B}$ holds, U is a **unitary operator**.

Another commonly used type of linear operators, that does not even require an inner product, are projection operators, or short projections.

Definition 2.1.12: Projection Operators

*A **projection** on a vector space V is a linear operator $P : V \to V$ such that $P^2 = P$.*
If the vector space V is equipped with an inner product, we can define orthogonal projections by requiring additionally that $P = P^\dagger$.

On many occasions, for example, if we want to perform numerical calculations, we have to represent finite-dimensional operators as matrices. By fixing bases $\{|\phi\rangle_i\}_{i\in\mathcal{I}_1}$ of $\mathcal{H}_A$ and $\{|\psi\rangle_i\}_{i\in\mathcal{I}_2}$ of $\mathcal{H}_B$ we can associate a linear operator $A \in$

$\mathrm{L}(\mathcal{H}_A, \mathcal{H}_B)$ with its representation matrix M_A,

$$M_A := \sum_{i \in \mathcal{I}_1, j \in \mathcal{I}_2} \langle \psi_j | A | \phi_i \rangle .$$

Multipartite systems

The formalism we have summarised so far only allows us to describe states living in the same Hilbert space. Therefore, the next step is to formalise the mathematical description of objects living in different quantum systems. The tensor product is a tool to combine multiple Hilbert spaces to a new Hilbert space.

Definition 2.1.13: Tensor Product

Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be two Hilbert spaces over $\mathcal{C}$ and let $\langle \cdot | \cdot \rangle_{\mathcal{H}_A}$ and $\langle \cdot | \cdot \rangle_{\mathcal{H}_B}$ be their corresponding inner products.
*The **tensor product** of $\mathcal{H}_A$ and $\mathcal{H}_B$, denoted by $\mathcal{H}_A \otimes \mathcal{H}_B$, is defined via a bilinear map*

$$\mathcal{H}_A \times \mathcal{H}_B \to \mathcal{H}_A \otimes \mathcal{H}_B, \ (\Phi, \Psi) \mapsto \Phi \otimes \Psi$$

that maps every pair $(\Phi, \Psi) \in \mathcal{H}_A \times \mathcal{H}_B$ uniquely to an element $\Phi \otimes \Psi$ in $\mathcal{H}_A \otimes \mathcal{H}_B$. By pointwise definition of the vector space operations it becomes a vector space and

$$\langle \Phi \otimes \Psi | \omega \otimes \sigma \rangle_{\mathcal{H}_A \otimes \mathcal{H}_B} := \langle \Phi | \omega \rangle_{\mathcal{H}_A} \langle \Psi | \sigma \rangle_{\mathcal{H}_B}$$

defines an inner product which turns $\mathcal{H}_A \otimes \mathcal{H}_B$ into a Hilbert space.

This definition for bipartite systems can be extended inductively to multipartite systems. The n-fold tensor product of the same Hilbert space $\mathcal{H}$ is denoted by $\mathcal{H}^{\otimes n}$.
In the context of quantum mechanics, one often might want to apply the trace only on one part of a composite system. This is done by the partial trace operation.

Definition 2.1.14: Partial Trace

*Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be separable Hilbert spaces. The **partial trace** over $\mathcal{H}_B$ is the unique linear operator $Tr_{\mathcal{H}_B} : \mathrm{L}(\mathcal{H}_A \otimes \mathcal{H}_B) \to \mathrm{L}(\mathcal{H}_A)$ such that*

$$\forall X \in \mathrm{L}(\mathcal{H}_A) \ \forall Y \in \mathrm{L}(\mathcal{H}_B) : \ Tr_{\mathcal{H}_B}(X \otimes Y) = \mathrm{Tr}[X] Y.$$

To ease notation, usually we write Tr_A instead of $\mathrm{Tr}_{\mathcal{H}_A}$.

Linear Maps

So far, we have dealt with linear operators, which map vectors living in one Hilbert space to vectors in another (or the same) Hilbert space. Therefore, the next step is to talk about linear maps of the form $\mathcal{E} : \mathrm{L}(\mathcal{H}_A) \to \mathrm{L}(\mathcal{H}_B)$ that map linear operators over $\mathcal{H}_A$ to linear operators over $\mathcal{H}_B$. We denote the set of all such operators by $\mathrm{T}(\mathcal{H}_A, \mathcal{H}_B)$ and if $\mathcal{H}_A = \mathcal{H}_B =: \mathcal{H}$ we write $\mathrm{T}(\mathcal{H})$. In what follows we specify important special classes of linear maps.

Definition 2.1.15: Special classes of linear maps

Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be separable Hilbert spaces. A linear map $\mathcal{E} \in \mathrm{T}(\mathcal{H}_A, \mathcal{H}_B)$ is called

1. ***positive*** *if $\forall P \in Pos(\mathcal{H}_A) : \mathcal{E}(P) \in \mathrm{Pos}(\mathcal{H}_B)$*
2. ***completely positive*** *(CP) if for every Hilbert space $\mathcal{H}$ the map $\mathcal{E} \otimes \mathbb{1}_{\mathrm{L}(\mathcal{H})}$ is positive*
3. ***trace preserving*** *(TP) if $\forall X \in L(\mathcal{H}_A, \mathcal{H}_B) : \mathrm{Tr}\left[\mathcal{E}(X)\right] = \mathrm{Tr}\left[X\right]$*
4. ***trace non-increasing*** *(TNI) if $\forall X \in L(\mathcal{H}_A, \mathcal{H}_B) : \mathrm{Tr}\left[\mathcal{E}(X)\right] \leqslant \mathrm{Tr}\left[X\right]$*

An important class of maps will be completely positive trace preserving (CPTP) and completely positive trace non-increasing maps. It remains to define the dual map or adjoint map.

Definition 2.1.16: Dual Map (Adjoint Map)

*Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be separable Hilbert spaces and let $\mathcal{E} \in T(\mathcal{H}_A, \mathcal{H}_B)$. The **dual map** or **adjoint map** $\mathcal{E}^\dagger \in \mathrm{T}(\mathcal{H}_B, \mathcal{H}_A)$ is defined by*

$$\forall X \in \mathrm{L}(\mathcal{H}_A)\ \forall Y \in \mathrm{L}(\mathcal{H}_B) : \ \langle \mathcal{E}(X), Y \rangle = \langle X, \mathcal{E}^\dagger(Y) \rangle.$$

2.2. Quantum Theory

> It seems hard to sneak a look at God's cards. But that he plays dice is something that I cannot believe for a single moment.
>
> *Albert Einstein* [25, p. 68]

After having set the mathematical scaffolding in the previous chapter, we can now bring quantum theory to life. The definition and statements given in this section are widely known and can be found in many introductory books on quantum mechanics and quantum information theory. If not mentioned otherwise, we loosely follow the texts in [75, 109]. A quantum mechanical state describes our knowledge about a physical system at a given time. Based on physical insights, we require a quantum state to be a positive, Hermitian, trace-class operator with trace equal to one. We describe quantum states with so-called density operators, usually denoted by Greek letters.

Definition 2.2.17: Density Operator

Let $\mathcal{H}$ be a separable Hilbert space. We denote the set of ***density operators*** *by*

$$\mathcal{D}(\mathcal{H}) := \{\rho \in \mathrm{Pos}(\mathcal{H}) : \ ||\rho||_1 = 1\}\,.$$

Note that since non-negativity implies Hermiticity, we do not have to require Hermiticity separately. Sometimes, we want to work with subnormalised states. The set of subnormalised density operators is given by

$$\mathcal{D}_{\leqslant}(\mathcal{H}) := \{\rho \in \mathrm{Pos}(\mathcal{H}) : \ ||\rho||_1 \leqslant 1\}\,.$$

The possibly most prominent quantum states are **pure states**, which can be described by a single vector $|\Psi\rangle \in \mathcal{H}$ and its density matrix is given by $\rho = |\Psi\rangle\langle\Psi|$. For that reason, we sometimes call the state $|\Psi\rangle$ although technically we refer to the corresponding density operator. We denote the set of pure states on $\mathcal{H}$ by $\mathcal{S}_1(\mathcal{H})$. However, general quantum states are not necessarily pure but are given as a probabilistic mixture of pure states.

Definition 2.2.18: Mixed State

Let $\{|\Psi_1\rangle, ..., |\Psi_n\rangle\}$ *be an ensemble of pure states in a separable Hilbert space* $\mathcal{H}$ *and let* $\{p_1, ..., p_n\}$ *be a collection of non-negative real numbers such that* $\sum_{i=1}^{n} p_i = 1$*. Then, a* ***mixed state*** *is represented by the following density operator*

$$\rho = \sum_{i=1}^{n} p_i \, |\Psi_i\rangle\langle\Psi_i| \, .$$

For a given mixed state $\rho_A \in \mathcal{D}(\mathcal{H}_A)$, it is always possible to find another Hilbert space $\mathcal{H}_E$, $\dim(\mathcal{H}_A) \leqslant \dim(\mathcal{H}_E)$, and a pure state $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_E$ in this larger Hilbert space such that the marginal of this pure state is ρ_A,

$$\rho_A = \mathrm{Tr}_E \left[|\Psi\rangle\langle\Psi| \right] . \tag{2.3}$$

The state $|\Psi\rangle$ is called purification of ρ_A.

2.2.1. Entanglement

> Entanglement is not one but rather the characteristic trait of quantum mechanics.
>
> *Erwin Schrödinger* [93, p. 555]

Next, we turn our focus to probably the most peculiar property of quantum mechanics: entanglement. Entanglement occurs when two or more quantum systems interact in a way such that the quantum state of each system cannot be described independently of the state of the other systems. This is not restricted to spatial proximity but includes systems that are separated by large distances, which led to Einstein's famous quote, calling entanglement 'spukhafte Fernwirkung'- 'spooky action at a distance'. In fact, entanglement is one mechanism that enables to do quantum communication. Therefore, we require a mathematical way of describing entanglement. For simplicity, we describe entanglement between two quantum systems. The ideas given here can be generalised straightforwardly to multiple quantum systems. Consider two separable Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$. To ease notation, we call the quantum systems associated with those Hilbert spaces A and B. A state $\rho_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ is called a bipartite state. One interesting family of bipartite states are entangled states.

Definition 2.2.19: Separable States - Entangled States

Let $\rho_{AB} \in \mathcal{D}(\mathcal{H}_{AB})$ be a bipartite state over the Hilbert space $\mathcal{H}_{AB} := \mathcal{H}_A \otimes \mathcal{H}_B$.
The state ρ is called ***separable****, if there exist ensembles $\{\rho_A^{(i)}\}_{i\in\mathcal{I}} \subseteq \mathcal{D}(\mathcal{H}_A)$ and $\{\rho_A^{(B)}\}_{i\in\mathcal{I}} \subseteq \mathcal{D}(\mathcal{H}_B)$ and a set of non-negative real numbers $\{p_i\}_{i\in\mathcal{I}}$, $\sum_{i\in\mathcal{I}} p_i = 1$ such that*

$$\rho_{AB} = \sum_{i\in\mathcal{I}} p_i \left(\rho_A^{(i)} \otimes \rho_B^{(i)}\right).$$

If ρ_{AB} is not separable, it is called ***entangled****.*

We have a special name for separable states with exactly one non-zero coefficient p_i. States of the form $\rho_A \otimes \rho_B$ are called **product states**.
A special subset of separable states is the set of so-called classical-quantum states, which play an important role in quantum key distribution.

Definition 2.2.20: Classical-Quantum States

Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be two separable Hilbert spaces and $\rho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$. The density operator ρ_{AB} is called a ***classical-quantum state*** *if there exists an orthonormal basis $\{|\phi_i\rangle\}_{i\in\mathcal{I}}$ of $\mathcal{H}_A$ and an ensemble of non-negative real numbers $\{p_i\}_{i\in\mathcal{I}}$ with $\sum_{i\in\mathcal{I}} p_i = 1$, as well as an ensemble of density matrices $\{\rho_E^{(i)}\} \subseteq \mathcal{D}(\mathcal{H}_B)$ such that*

$$\rho_{AB} = \sum_{i\in\mathcal{I}} p_i \ |\phi_i\rangle\langle\phi_i| \otimes \rho_B^{(i)}.$$

2.2.2. Measurements

> Observations not only disturb what is to be measured, they produce it.
>
> Pascual Jordan [52, p. 161]

We interact and gain information from quantum systems by performing measurements. According to the third postulate of quantum mechanics, quantum measurements are described by a set of measurement operators $\{\Gamma_i\}_{i\in\mathcal{I}}$, where the index i corresponds to the measurement outcome in the experiment. Within the frame of this work, we view measurement as a process, where a quantum state enters our

measurement device and we obtain a measurement outcome as a result. In particular, we are not interested in the post-measurement state of our quantum system. This notion is captured by positive operator-valued measures. The explanations in this subsection follow [102].

Definition 2.2.21: Positive Operator-Valued Measure (1)

Let $\mathcal{H}$ be a separable Hilbert space. A ***positive operator-valued measure (POVM)*** *on a measurable space $(\Omega, \mathcal{A})$ is a map $\mu : \mathcal{A} \to \mathcal{B}(\mathcal{H})$ satisfying*

- $\forall A \in \mathcal{A} : \ \mu(A) \geqslant 0$
- $\mu(\Omega) = \mathbb{1}_{\mathcal{H}}$
- *μ is σ-additive, i.e., for every sequence of pairwise disjoint sets $(A_i)_{i\in\mathbb{N}} \subseteq \mathcal{A}$:*

$$\mu\left(\bigcup_{i\in\mathbb{N}} A_i\right) = \sum_{i\in\mathbb{N}} \mu(A_i).$$

The series converges in the weak operator topology.

In the context of quantum information, it is very common to call the set of bounded linear operators $\{\Gamma_s\}_{s\in\mathcal{S}} = \{\mu(A_s)\}_{s\in\mathcal{S}}$, for $(A_s)_{s\in\mathcal{S}}$, POVMs. Therefore, we also give an alternative, less formal, definition, which turns out to be more practical for the present work [109, Definition 4.2.1].

Definition 2.2.22: Positive Operator-Valued Measure (2)

Let $\mathcal{H}$ be a separable Hilbert space and $\mathcal{S}$ some set. A ***positive operator-valued measure (POVM)*** *is a set $\{\Gamma_s\}_{s\in\mathcal{S}}$ of operators that satisfy non-negativity and completeness:*

- $\forall s \in \mathcal{S} : \ \Gamma_s \geqslant 0$
- $\sum_{s\in\mathcal{S}} \Gamma_s = \mathbb{1}_{\mathcal{H}}$

According to Born's rule, the probability for obtaining the outcome s if the considered quantum state is described by the density operator ρ is given by $\mathrm{Prob}(s) = \mathrm{Tr}\left[\Gamma_s \rho\right]$. We see that the two required properties non-negativity and completeness then correspond to the requirement that probabilities have to be non-negative and need to sum to one. We remark that POVMs are not restricted to discrete index sets $\mathcal{S}$. Then, in the completeness condition, the sum is replaced by a suitable

integral. This will be the case for measurements of continuous quantities in the present work.
Next, we discuss observables, i.e., physical quantities that can be measured. Every observable O of a quantum system described by a Hilbert space $\mathcal{H}$ is associated with a linear operator $\hat{O} \in \mathrm{L}(\mathcal{H})$[1]. Eigenvalues of $\hat{O}$ are associated with possible measurement outcomes and therefore, in particular, real numbers. Hence, observables are Hermitian operators $\mathrm{Obs}(\mathcal{H}) \subset \mathrm{Herm}(\mathcal{H})$.

Definition 2.2.23: Observable

Let $\mathcal{H}$ be a separable Hilbert space. A quantum mechanical ***observable*** *of a quantum system described by the Hilbert space $\mathcal{H}$ is a self-adjoint linear operator $\hat{O} \in Herm(\mathcal{H})$.*

The expected value of an observable is denoted by $\langle \hat{O} \rangle_\rho = \mathrm{Tr}\left[\hat{O}\rho\right]$, where the underlying state is indicated as a subscript. Sometimes, if the underlying state is clear from the context, the subscript is omitted. As we will see later, observables can be unbounded, in that case, $\langle \hat{O} \rangle$ might be undefined.
Observables are included in the concept of POVM measurements. We obtain observables as the special case where all POVM operators are projection operators (so, we face the special case of a projection-valued measure) on the sample space $\Omega = \mathbb{R}$. Then, in general, we obtain the operator $\hat{O}$ associated with the observable O by $\hat{O} = \int_{\mathbb{R}} \mu(x)\, \mathrm{d}\lambda(x)$.
In the discrete case, using the simplified definition of POVMs, the observable associated with some projective measurement $\{\Gamma_s\}_{s\in\mathcal{S}}$ yielding the measurement results $\{\gamma_s\}_{s\in\mathcal{S}}$ gives rise to the observable $\hat{O} = \sum_{s\in\mathcal{S}} \gamma_s \Gamma_s$. Note that Γ_s is the projector on the eigenspace of $\hat{O}$ corresponding to the eigenvalue γ_s.
In contrast to classical physics, in quantum mechanics, not all observables can be measured simultaneously. Mathematically, this is expressed by the commutator, $[\hat{A}, \hat{B}] := \hat{A}\hat{B} - \hat{B}\hat{A}$. Observables that cannot be measured at the same time, do not commute, $[\hat{A}, \hat{B}] \neq 0$.

[1] Note that we emphasise the difference between the observable and the operator associated with the observable by adding a $\hat{\cdot}$ when we refer to the operator.

2.2.3. Quantum Channels

> Quantum channels are all encompassing. (...) From this perspective, one could argue that there really is just a single underlying postulate of quantum physics, that everything we consider in the theory is just a quantum channel of some sort.
>
> Mark Wilde [109, p. 160]

It remains to describe the evolution of quantum states. The present subsection follows the text [109, Chapter 4.4], where we refer the interested reader for more details (in particular, to see why quantum channels can capture not only the idea of the evolution of states but also concepts like quantum measurements and discarding quantum systems, as indicated by the introductory quote). We picture the process of the evolution of quantum states as a black box where we input a density matrix and obtain another density matrix as output. Now suppose that one prepares one out of two quantum states $\rho, \sigma \in \mathcal{D}(\mathcal{H}_A)$ according to some probability distribution. For example, assume ρ is prepared with probability $0 < p < 1$ and σ with probability $1 - p$ and then the evolution $\mathcal{E}$ is applied. The state then reads $\mathcal{E}(p\rho+(1-p)\sigma)$. Suppose this experiment is repeated multiple times and afterwards we are given all the states and are allowed to perform measurements. In a first scenario, we measure the state $\mathcal{E}(p\rho + (1-p)\sigma)$ directly and record how often we obtained $\mathcal{E}(\rho)$ and $\mathcal{E}(\sigma)$. In a second scenario, we are told in which rounds which state was prepared, so for a fraction p of our measurements we conclude that we obtained $\mathcal{E}(\rho)$, while for a fraction $1-p$ we conclude that we obtained $\mathcal{E}(\sigma)$. For consistency reasons, we expect the observed statistics to coincide in both scenarios. Therefore, we require a quantum evolution to be linear. Putting all this together, we can define the mathematical description of a quantum evolution: a quantum channel.

Definition 2.2.24: Quantum Channel

A quantum evolution is described by a ***quantum channel****, which is a linear, completely positive, trace preserving (CPTP) map.*

Sometimes, we want to work with sub-normalised states, so we do not require the output to have trace equal to one. Then, quantum evolutions can be described as well by **completely positive trace non-increasing (CPTNI) maps**. A useful

way to characterise quantum channels is the so-called Kraus representation.

Theorem 2.2.25: Kraus Representation

Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be separable Hilbert spaces and let $\mathcal{E}: \mathrm{L}(\mathcal{H}_A) \to \mathrm{L}(\mathcal{H}_B)$. Then, the map $\mathcal{E}$ is linear, completely positive and trace-preserving if and only if there exist $K_i \in \mathrm{L}(\mathcal{H}_A, \mathcal{H}_B)$ for $i \in \{0, ..., d-1\}$ such that

$$\forall X \in \mathrm{L}(\mathcal{H}_A): \ \mathcal{E}(X) = \sum_{i=0}^{d-1} K_i X K_i^\dagger$$

*with $\sum_{i=0}^{d-1} K_i^\dagger K_i = \mathbb{1}_{\mathcal{H}_A}$ and $d \leqslant \dim(\mathcal{H}_A)\dim(\mathcal{H}_B)$. The operators K_i are called **Kraus operators** and this representation of a quantum channel is called **Kraus representation**.*

Quantum channels and their Kraus representation will play an important role in the present thesis.

2.2.4. Distance Measures

> The idea of distinguishing probability distributions is slippery business.
>
> Christopher Fuchs [30, p. 12]

In many contexts, we have to quantify the distance between probability distributions or density operators. In what follows, we introduce the distance measures used in the present thesis, following [109, Chapter 9]. We begin with the trace distance, which is (up to a scaling factor) the distance measure introduced by the Schatten 1-norm.

Definition 2.2.26: Trace-Distance

*Let P and Q be positive operators. The **trace-distance** between P and Q is defined as*

$$\Delta(P, Q) := \frac{1}{2}||P - Q||_1. \tag{2.4}$$

Note that by including the factor $\frac{1}{2}$, we defined the so-called normalised trace-distance, as then for density matrices $\rho, \sigma \in \mathcal{D}(\mathcal{H})$ we have $0 \leqslant \Delta(\rho, \sigma) \leqslant 1$. The lower bound is attained if $\rho = \sigma$ and the upper bound follows from the triangle-inequality $\frac{1}{2}||\rho - \sigma||_1 \leqslant \frac{1}{2}\left(||\rho||_1 + ||\sigma||_1\right) = 1$. The significance of this normalisation

will become clear later on when we give the trace distance an operational meaning.

However, the trace distance has one technical issue. To illustrate that, suppose we hold two density operators $\rho_{AB}, \sigma_{AB} \in \mathcal{D}(A \otimes B)$ and let $\rho_A := \mathrm{Tr}_B(\rho_{AB})$ and $\sigma_A := \mathrm{Tr}_B(\sigma_{AB})$ be their marginals. Assume further, we know that $||\rho_A - \sigma_A||_1 \leqslant \epsilon$. Then, the trace norm doesn't allow us to conclude anything about how similar ρ_{AB} and σ_{AB} are. To close this gap (on the cost of losing the nice operational interpretation) we introduce the purified distance. However, this requires some preparation.

The closeness of two states can as well be measured by the fidelity. In the easiest case, the pure-state fidelity determines the squared overlap between two pure states $|\Psi\rangle$ and $|\Phi\rangle$, $|\langle\Psi|\Phi\rangle|^2$. It obeys values between zero and one and tells us how likely the state $|\Psi\rangle$ would pass a test for being the state $|\Phi\rangle$ (or vice-versa). We see that if $|\Psi\rangle = |\Phi\rangle$ the pure-state fidelity is equal to 1, so it is not directly a distance measure. Let us next define fidelity for general quantum states as a generalised measure of their overlap.

Definition 2.2.27: Fidelity

Let $\mathcal{H}$ be a separable Hilbert space and $\rho, \sigma \in \mathcal{D}(\mathcal{H})$.
*The **fidelity** between ρ and σ is defined as*

$$F(\rho, \sigma) := \left(\mathrm{Tr}\left[\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right]\right)^2.$$

Note that, unfortunately, there are two slightly different definitions of fidelity in quantum information literature. While some authors omit the square, we follow those who define fidelity with a square. However, this is not a problem as long as we consistently stick to one of both conventions.

Even though fidelity is not directly a distance measure, as mentioned earlier, it can be used to define distance measures, like the angular distance $A(\rho, \sigma) := \arccos\left(\sqrt{F(\rho, \sigma)}\right)$ [39].

In the present work, we will rely on a generalised form of fidelity to include sub-normalised states. Based on the observation that we can think of sub-normalised states as normalised states on a larger Hilbert space [100], we define

Definition 2.2.28: Generalised Fidelity

Let $\mathcal{H}$ be a separable Hilbert space and $\rho, \sigma \in \mathcal{D}_{\leqslant}(\mathcal{H})$. By $\mathcal{H}' \supseteq \mathcal{H}$ we denote that a Hilbert space $\mathcal{H}$ is embedded in another Hilbert space $\mathcal{H}'$. Let Π be the corresponding projector onto $\mathcal{H}$.
*The **generalised Fidelity** between ρ and σ is*

$$F_*(\rho, \sigma) := \sup_{\mathcal{H}':\ \mathcal{H}' \supseteq \mathcal{H}} \sup_{\substack{\bar{\rho}, \bar{\sigma} \in \mathcal{D}(\mathcal{H}') \\ \Pi\bar{\rho}\Pi = \rho,\ \Pi\bar{\sigma}\Pi = \sigma}} F(\bar{\rho}, \bar{\sigma}).$$

As shown in [100, Lemma 3] $F_*(\rho, \sigma)$ reduces to $F(\rho, \sigma)$ if ρ or σ is normalised. Based on the fidelity, we now can define the so-called purified distance [39, 100].

Definition 2.2.29: Purified Distance

*Let $\mathcal{H}$ be a separable Hilbert space and $\rho, \sigma \in \mathcal{D}(\mathcal{H})$. The **purified distance** between ρ and σ is defined as*

$$\mathcal{P}(\rho, \sigma) := \sqrt{1 - F_*(\rho, \sigma)}.$$

It can be shown that the purified distance is a metric [100, Lemma 5]. The purified distance can be thought of as the minimum trace-distance between purifications of the states ρ and σ [100]. Therefore, the trace-distance is always upper-bounded by the purified distance. This, in fact, is the mathematical statement of the lower Fuchs-van de Graaf inequalities, which relate the purified distance and the trace-distance [31],

$$\Delta(\rho, \sigma) \leqslant \mathcal{P}(\rho, \sigma) \leqslant \sqrt{2\Delta(\rho, \sigma)}. \tag{2.5}$$

2.3. Quantum Information Theory

> I argue that quantum mechanics is fundamentally a theory about the representation and manipulation of information, not a theory about the mechanics of nonclassical waves or particles.
>
> Jeffrey Bub [13]

Both classical and quantum information theory deal with storing and quantifying information. In this section, we review the information-theoretic concepts that are

relevant to the present thesis, following the texts [75, 108, 109].
Registers are a mathematical model of physical devices, used to memorise information. In this context, the term **alphabet** refers to a finite, non-empty (index-)set. Alphabets usually are denoted by capital Greek letters. Elements of alphabets are called **symbols**. We give an abstract definition of a register [108, Definition 2.1].

Definition 2.3.30: Register

*A **register** X is either one of the following two objects:*

- *an alphabet Σ (simple register)*
- *an n-tuple $X = (Y_1, ..., Y_n)$, where $n \in \mathbb{N}^+$ and $Y_1, ..., Y_n$ are registers (compound register).*

It turns out that classical information-theoretic tasks, which are based on random variables and probability distributions, are special cases of quantum mechanical problems, where we hold quantum states represented by density matrices. For example, we can write a classical probability distribution into the diagonal entries of a matrix, hence probability distributions can be seen as a subset of density matrices.

2.3.1. Entropic Quantities

> Von Neumann told me, 'You should call it entropy, for two reasons. In the first place your uncertainty function has been used in statistical mechanics under that name, so it already has a name. In the second place, and more important, no one really knows what entropy really is, so in a debate you will always have the advantage.'
>
> *Claude Shannon* [101]

One of the central tasks both in classical and quantum information theory is to quantify information. We begin with reviewing ways to measure information in the classical case and introduce the generalised quantities afterwards. Since bits are the basic carriers of information in modern information theory, we quantify

information in bits.
Probability density functions $p_X(x)$ of a random variable X tell us how likely we observe the realisation $X = x$ of our random variable. If we are certain about the outcome of our random variable, for example, if $p_X(x_1) = 1$, we are not surprised at all to find x_1 when reading out X and do not learn anything new. Conversely, our surprise when obtaining a particular realisation is high, if all realisations are equally likely. Therefore, information content of a random variable measures the surprise when learning the outcome of a random experiment, $i(x) := -\log_2(p_X(x))$. However, the information content only quantifies the surprise of a particular realisation and hence does not characterise the whole random variable. Therefore, we introduce the entropy which is the expected information content of a random variable.

Definition 2.3.31: Shannon Entropy

*Let X be a discrete random variable with associated probability distribution $p_X(x)$. The **classical entropy** or **Shannon entropy** of X is defined as*

$$H(X) := -\sum_x p_X(x) \log_2(p_X(x)),$$

where we use the convention $0 \cdot \log_2(0) = 0$.

A special case of the Shannon entropy is the **binary entropy** for Bernoulli random variables X with $p_X(0) = p$ and $p_X(1) = 1 - p$ for $p \in [0, 1]$, denoted by

$$h(p) = -p \log_2(p) - (1 - p) \log_2(1 - p). \tag{2.6}$$

Assume we hold two random variables X and Y that are somehow correlated. How are the information contents of those two random variables related to each other? An important quantity to answer this question is the joint entropy.

Definition 2.3.32: Joint Entropy

*Let X and Y be discrete random variables with joint probability distribution $p_{X,Y}(x, y)$. The **joint entropy** of X and Y is defined as*

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

Next, suppose we already possess the random variable Y. How much uncertainty do we still have about X given our side information due to knowing Y? This notion is captured by the conditional entropy.

Definition 2.3.33: Conditional Entropy

Let X and Y be discrete random variables with joint probability distribution $p_{X,Y}(x,y)$. The ***conditional entropy*** *of X conditioned on Y is known is defined as*

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

A brief calculation shows that the three entropic quantities we introduced are related to each other by

$$H(X,Y) = H(X|Y) + H(Y) = H(Y|X) + H(X). \tag{2.7}$$

Finally, we want to measure how much information the random variables X and Y have in common.

Definition 2.3.34: Mutual Information

Let X and Y be discrete random variables with joint probability distribution $p_{X,Y}(x,y)$. The ***mutual information*** *of X and Y is defined as*

$$I(X:Y) := H(X) + H(Y) - H(X,Y). \tag{2.8}$$

We introduced the joint entropy, the conditional entropy and the mutual information for two correlated random variables. However, they can be generalised naturally to n random variables.
The quantum version of the classical entropy was discovered by John von Neumann (interestingly, even before Claude Shannon introduced the classical entropy, as the quote at the beginning of the section indicates). Since density operators describe quantum states, we expect an entropic measure to be a function of the density matrix. Furthermore, as classical probability distributions are included as a special case in the density operator formalism, we expect the quantum entropies to coincide with their classical equivalents in this special case.

Definition 2.3.35: Von Neumann Entropy

Let $\mathcal{H}_A$ be a separable Hilbert space representing a quantum system A and let $\rho_A \in \mathcal{D}(\mathcal{H}_A)$. The ***von Neumann entropy*** *of ρ_A is defined as*

$$H(A)_\rho := -\mathrm{Tr}\left[\rho_A \log_2(\rho_A)\right].$$

The definition of the joint quantum entropy for a bipartite density operator $\rho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ follows straightforwardly.

Definition 2.3.36: Joint Quantum Entropy

Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be separable Hilbert spaces representing a quantum system A and B and let $\rho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$. The ***joint quantum entropy*** *of ρ_{AB} is defined as*

$$H(AB)_\rho := -\mathrm{Tr}\left[\rho_{AB} \log_2(\rho_{AB})\right].$$

Based on the classical relation between joint entropy and conditional entropy, we define the conditional quantum entropy as follows.

Definition 2.3.37: Conditional Quantum Entropy

Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be separable Hilbert spaces representing a quantum system A and B and let $\rho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$. The ***conditional quantum entropy*** *$H(A|B)_\rho$ of ρ_{AB} is defined as*

$$H(A|B)_\rho := H(AB)_\rho - H(B)_\rho. \tag{2.9}$$

The quantum mutual information is defined analogously to the classical case.

Definition 2.3.38: Quantum Mutual Information

Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be separable Hilbert spaces representing quantum systems A and B and let $\rho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$. The ***quantum mutual information*** *of the bipartite state ρ_{AB} is defined as*

$$I(A:B)_\rho := H(A)_\rho + H(B)_\rho - H(A,B)_\rho.$$

Finally, we introduce another entropic quantity which will play an important role in quantum key distribution - the quantum relative entropy. It measures how distinguishable two quantum states ρ and σ are and can be used to re-express other entropies.

Definition 2.3.39: Quantum Relative Entropy

Let $\mathcal{H}$ be a separable Hilbert space and $\rho \in \mathcal{D}(\mathcal{H})$ and $\sigma \in Pos(\mathcal{H})$. The ***quantum relative entropy*** *between ρ and σ is given by*

$$D(\rho||\sigma) := \begin{cases} \mathrm{Tr}\left[\rho \log_2(\rho)\right] - \mathrm{Tr}\left[\rho \log_2(\sigma)\right] & , \text{ if } supp(\sigma) \subseteq supp(\rho) \\ \infty & , \text{ otherwise,} \end{cases}$$

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

For example, one can express the conditional entropy in terms of the quantum relative entropy,

$$H(A|B)_\rho = -\min_{\sigma_B} D(\rho_{AB}||\mathbb{1}_A \otimes \sigma_B). \tag{2.10}$$

The importance of both the Shannon and the von Neumann entropy arises from their relation to certain information-theoretic tasks. For example, according to Shannon's famous formula, classical entropy is used to express the capacity of a communication channel. For the sake of another example, assume we want to encode some information into a quantum state ρ. The von Neumann entropy quantifies the maximal number of qubits required to store the information. However, these characterisations only work if we are allowed to repeat the process infinitely many times, i.e., in an asymptotic setting. Additionally, Shannon assumed a memoryless channel and for encoding example, we require a source emitting independently and identically distributed states. This leads us to (smooth) min- and max entropies, which were introduced in [85] to quantify information in tasks with finitely many repetitions.

Smooth min- and max-Entropy

We are going to introduce the smooth min- and max-entropy following the text [99]. We start by giving the basic definitions and try to give an interpretation afterwards. We begin with the min- and max-entropy.

Definition 2.3.40: Min-Entropy

Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be separable Hilbert spaces and $\rho_{AB} \in \mathcal{D}_\leqslant(\mathcal{H}_A \otimes \mathcal{H}_B)$ as well as $\sigma_B \in \mathcal{D}_\leqslant(\mathcal{H}_B)$.

*The **min-entropy of ρ_{AB} relative to σ_B** is defined as*

$$H_{min}(\rho_{AB}||\sigma_B) := -\log_2 \inf\{\lambda \in \mathbb{R} : \ \lambda \mathbb{1}_A \otimes \sigma_B \geqslant \rho_{AB}\}.$$

*The **min-entropy A conditioned on B of the state ρ_{AB}** is*

$$H_{min}(A|B)_\rho := \sup_{\sigma_B \in \mathcal{D}_\leqslant(\mathcal{H}_B)} H_{min}(\rho_{AB}||\sigma_B).$$

The min-entropy gives the maximum amount of uniform randomness that can be extracted guaranteed from A given B.

Definition 2.3.41: Max-Entopy

Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be separable Hilbert spaces and $\rho_{AB} \in \mathcal{D}_{\leqslant}(\mathcal{H}_A \otimes \mathcal{H}_B)$ as well as $\sigma_B \in \mathcal{D}_{\leqslant}(\mathcal{H}_B)$.
The ***max-entropy of*** *A* ***conditioned on*** *B* ***of the state*** *ρ_{AB} is*

$$H_{max}(A|B)_\rho := \sup_{\sigma \in \mathcal{D}_{\leqslant}(\mathcal{H}_B)} \log_2 \left(F(\rho_{AB}, \mathbb{1}_A \otimes \sigma_B) \right).$$

The max-entropy quantifies the maximum amount register A can be compressed without failure, given B. While in the classical case the min- and the max-entropy seem to be rather unrelated, in the quantum case there appears an interesting relation. Let $\mathcal{H}_A, \mathcal{H}_B, \mathcal{H}_C$ be separable Hilbert spaces. For a pure state $\rho \in \mathcal{S}_1(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$ we have

$$H_{\max}(A|B)_\rho = -H_{\min}(A|C)_\rho. \tag{2.11}$$

This tells us, the more B knows about A, the less C can know about A. This connection is a beautiful example of a quantum phenomenon that is not possible in the classical world.

However, the min- and max-entropy have one major drawback. They can change significantly if the considered quantum state changes only slightly under the trace norm. In Chapter 3.2 of Renner's thesis [85] one can find a classical example illustrating this fact for the max-entropy. This highlights that we might want to have a smoothed version of the min- and max-entropy, being the maximum or minimum over all states close to the considered state. This leads to the smooth min- and smooth max-entropy. We measure closeness either in terms of the trace distance, or the purified distance. Let us define the ϵ-balls around some state ρ,

$$\mathcal{B}^\epsilon_{\mathrm{TD}}(\rho) := \{\tilde{\rho} \in \mathrm{Pos}(\mathcal{H}_A \otimes \mathcal{H}_B) : \mathrm{Tr}\left[\rho\right] \geqslant \mathrm{Tr}\left[\tilde{\rho}\right] \wedge ||\rho - \tilde{\rho}||_1 \leqslant \mathrm{Tr}\left[\rho\right] \epsilon\}, \tag{2.12}$$

$$\mathcal{B}^\epsilon_{\mathrm{PD}}(\rho) := \{\tilde{\rho} \in \mathcal{D}_{\leqslant}(\mathcal{H}_A \otimes \mathcal{H}_B) : \ \mathcal{P}(\rho, \tilde{\rho}) \leqslant \epsilon\}, \tag{2.13}$$

where the subscript denotes the used distance measure.

Definition 2.3.42: Smooth min- and max-entropy

Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be separable Hilbert spaces and $\rho \in \mathcal{D}_{\leqslant}\mathcal{H}_A \otimes \mathcal{H}_B)$ and $\sigma_B \in \mathcal{D}_{\leqslant}(\mathcal{H}_B)$.
The ***smooth min-entropy of*** *A* ***conditioned on*** *B* ***of the state*** *ρ_{AB} is defined as*

$$H_{min}^{\epsilon}(A|B)_{\rho} := \sup_{\overline{\rho}_{AB} \in \mathcal{B}^{\epsilon}(\rho_{AB})} H_{min}(A|B)_{\overline{\rho}}.$$

The ***ϵ-smooth max-entropy of*** *A* ***conditioned on*** *B* ***of the state*** *ρ_{AB} is defined as*

$$H_{max}^{\epsilon}(A|B)_{\rho} := \inf_{\overline{\rho}_{AB} \in \mathcal{B}^{\epsilon}(\rho_{AB})} H_{max}(A|B)_{\overline{\rho}}.$$

In case the smoothing is done in the trace-distance, we denote this by adding (TD) to the subscript and for purified distance, we add (PD).

As we already noted, for i.i.d. states in the asymptotic case, we do not need min- or max-entropies to quantify information-theoretic tasks. The asymptotic equipartition property shows that in the asymptotic limit we recover the von Neumann entropy. The following result is taken from [87, Corollary 3.3.7] and we apply a correction noted in [35, p. 17] and is stated for finite-dimensional Hilbert spaces.

Theorem 2.3.43: Asymptotic Equipartition Property

Let $\rho_{XB} \in \mathcal{D}(\mathcal{H}_X \otimes \mathcal{H}_{\mathcal{B}})$ be a classical-quantum state and let the dimension of $\mathcal{H}_X \otimes \mathcal{H}_B$ be finite.

Then, for $\epsilon \geqslant 0$

$$\frac{1}{n} H_{min}^{\epsilon}(X^{\otimes n}|B^{\otimes n})_{\rho} \geqslant H(XB)_{\rho} - H(B)_{\rho} - \delta,$$

where $\delta := (2\log_2(rank(\rho_X) + 3)\sqrt{\frac{\log_2\left(\frac{2}{\epsilon}\right)}{n}}$.

This is the so-called direct part of the AEP, which is used frequently in the key rate analysis of quantum key distribution protocols. We will see later that a very similar statement holds for infinite-dimensional Hilbert space $\mathcal{H}_B$ as well.

In [99] Corollaries 6.2 and 6.3 they show that even in the fully quantum case, for

$\rho_{A^nB^n} = \rho_{AB}^{\otimes n}$ and $0 \leqslant \epsilon \leqslant 1$, we obtain

$$\lim_{n\to\infty} \frac{1}{n} H_{\min}^{\epsilon}(A^n|B^n)_\rho = H(A|B)_\rho$$
$$\lim_{n\to\infty} \frac{1}{n} H_{\max}^{\epsilon}(A^n|B^n)_\rho = H(A|B)_\rho,$$

i.e., in the asymptotic limit, we recover the von Neumann entropy.

2.4. Quantum Optics

The statements made by quantum information theory refer to generic quantum systems with certain properties but are not exclusive to particular implementations. However, for practical reasons, quantum key distribution is usually realised by quantum optical implementations. Thus, we need to give a brief review of basic concepts in quantum optics, following the texts [37, 61, 92].

The theoretical description of quantum optical phenomena is based on the quantisation of the electromagnetic field. From field theory, we know that an **(optical) mode** in some systems like an optical fibre or a cavity is a solution to Maxwell's equations for some fixed frequency. It can be shown that an optical mode can be described mathematically by the solutions to a quantum mechanical harmonic oscillator. Therefore, in quantum key distribution, it suffices to build up upon the theory of quantum mechanical harmonic oscillators rather than working directly with field theory. For a detailed derivation of the algebraic method to describe the quantum mechanical harmonic oscillator, we refer the interested reader to [43, Chapter 2.3].
We proceed with a review of the theory, relevant to the present thesis. In contrast to the classical harmonic oscillator, the energy levels of the quantum harmonic oscillator are - nomen est omen - quantised. We number the energy levels by natural numbers n, beginning with 0 for the lowest possible energy - the vacuum energy, which is greater than zero. Going up or down one energy level adds or annihilates one photon of energy $\hbar\omega$, so the energy levels are separated by equidistant gaps. We denote the quantum state associated with n photons by $|n\rangle$. Inspired by the equidistantly spaced energies, we introduce so-called ladder-operators $\hat{a}$ - the **creation-operator** and $\hat{a}^\dagger$ the **annihilation-operator**, which add or subtract one photon,

$$\hat{a}\,|n\rangle = \sqrt{n}\,|n-1\rangle \tag{2.14}$$
$$\hat{a}^\dagger\,|n\rangle = \sqrt{n+1}\,|n+1\rangle\,. \tag{2.15}$$

For the vacuum-state, so if $n = 0$, we have $\hat{a}\,|0\rangle = |0\rangle$. The states $\{|n\rangle\}_{n=0}^{\infty}$ are called **Fock states** and form a basis of the Hilbert space we use to describe the quantum mechanical harmonic oscillator. From Eq. (2.14) and (2.15), we observe

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

We just showed that $|n\rangle$ is the eigenstate of the operator $\hat{a}^\dagger\hat{a}$ with eigenvalue n. This motivates the definition of the **photon number operator** $\hat{n} := \hat{a}^\dagger\hat{a}$. Furthermore, we note that the ladder operators obey the commutation relation $[\hat{a}, \hat{a}^\dagger] = \mathbb{1}$. Note that we chose natural units, i.e. we set $\hbar = 1$. Since different authors follow different conventions, we direct the reader to [60, Appendix F] for a well-structured table converting quantities used in quantum optics between different unit systems.
The field quadrature operators $\hat{q}$ and $\hat{p}$, within the frame of canonical quantisation the operators corresponding to the classical quantities position and momentum, can be expressed in terms of the ladder operators as

$$\hat{q} = \frac{1}{\sqrt{2}}(\hat{a}^\dagger + \hat{a}) \tag{2.16}$$

$$\hat{p} = \frac{i}{\sqrt{2}}(\hat{a}^\dagger - \hat{a}). \tag{2.17}$$

They obey the commutation relation $[\hat{q}, \hat{p}] = i$.
Besides Fock states, another important class of states are **coherent states**, denoted by $|\alpha\rangle$ where $\alpha \in \mathbb{C}$. Coherent states describe laser pulses, hence can be created easily in experiments and therefore play a prominent role in quantum key distribution. Mathematically, coherent states are eigenstates of the annihilation operator, $\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle$ and can easily be represented as a Poissonian distribution of Fock states

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}\,|n\rangle\,. \tag{2.18}$$

Note that the coherent state $|0\rangle$ is equal to the vacuum state. Mathematically, we can create coherent states from the vacuum using the **displacement operator**,

$$\hat{D}(\alpha) := e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}, \tag{2.19}$$

where α^* denotes the complex conjugate of α. Starting from a vacuum state $|0\rangle$, we obtain a coherent state via $|\alpha\rangle = \hat{D}(\alpha)\,|0\rangle$. More generally, applied to an arbitrary coherent state $|\alpha\rangle$, we obtain $\hat{D}(\beta)\,|\alpha\rangle = e^{i\mathrm{Im}(\beta\alpha^*)}\,|\alpha+\beta\rangle$. We can as well displace arbitrary states or even operators. We denote operators displaced by β as $\hat{A}_\beta := \hat{D}(\beta)\hat{A}\hat{D}(\beta)^\dagger$ and we use the short notation $|n\rangle_\beta := \hat{D}(\beta)\,|n\rangle$ to denote

a displaced number state. Note that one can see directly from the definition that $\hat{D}(\alpha)^\dagger = \hat{D}(-\alpha)$.
The name of the displacement operator refers to its action on states in the phase space. In quantum optics, the phase space is used to visualise single-mode quantum states in terms of quasi-probability distributions. In contrast to the Schrödinger picture, where either position q or momentum p are used to parameterise the wave function, in the phase-space formalism position and momentum occur equitably.
Another important class of states are **thermal states**. They can be represented as a thermal distribution of Fock states

$$\rho_{\text{th}} = \frac{1}{1+\overline{n}} \sum_{n=0}^{\infty} \left(\frac{\overline{n}}{(1+\overline{n})} \right)^n |n\rangle\langle n| \,, \tag{2.20}$$

where $\overline{n}$ denotes the mean photon number, i.e., $\text{Tr}\left[\rho_{\text{th}} \hat{n}\right] = \overline{n}$.

2.4.1. Optical Instruments

In order to perform quantum key distribution, we require optical devices to manipulate and detect light. The most prominent component is a **beamsplitter**. A symmetric beam splitter is a device with two inputs and two outputs characterised by its transmittance t and its reflectance r, where both are linked to each other via the equation $t^2 + r^2 = 1$. While a more in-depth discussion can be found, for example, in [37, Chapter 6.2], we only state the most important result. A symmetric beam splitter transforms the annihilation operators corresponding to the input modes, labelled by 0 and 1 as follows

$$\begin{pmatrix} \hat{a}_2 \\ \hat{a}_3 \end{pmatrix} = \begin{pmatrix} t & ir \\ ir & t \end{pmatrix} \begin{pmatrix} \hat{a}_0 \\ \hat{a}_1 \end{pmatrix}, \tag{2.21}$$

where the output modes are labelled as 2 and 3. The factor of i next to the reflectance r arises from the fact that for beam splitters built as a single dielectric layer, the reflected and the transmitted beam differ in phase by $\frac{\pi}{2}$.
Note that in the quantum case the beam splitter is always a two-input, two-output device, even though we (actively) send light only in one mode, as the other mode contains at least the vacuum state.
Even though we have already covered the theoretical description of measurements in quantum mechanics in Section 2.2.2, it remains to specify, how measurements in QKD protocols analysed within the frame of the present thesis, are conducted. For protocols with continuous variables, we mostly perform homodyne and heterodyne measurements. The idea is to mix the signal with a strong laser, called the local oscillator, which serves as a phase reference. We begin with the description of **homodyne detection**, following [37, Chapter 7.3].

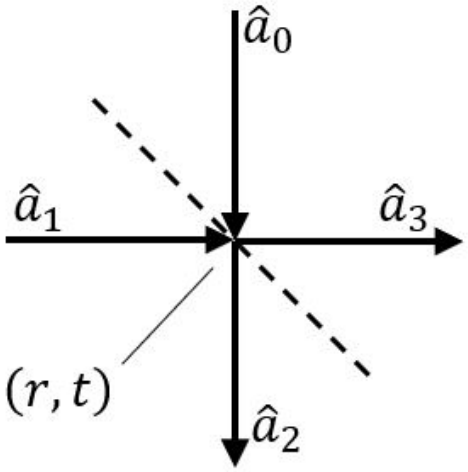

Figure 2.1.: Schematic of a quantum mechanical beamsplitter.

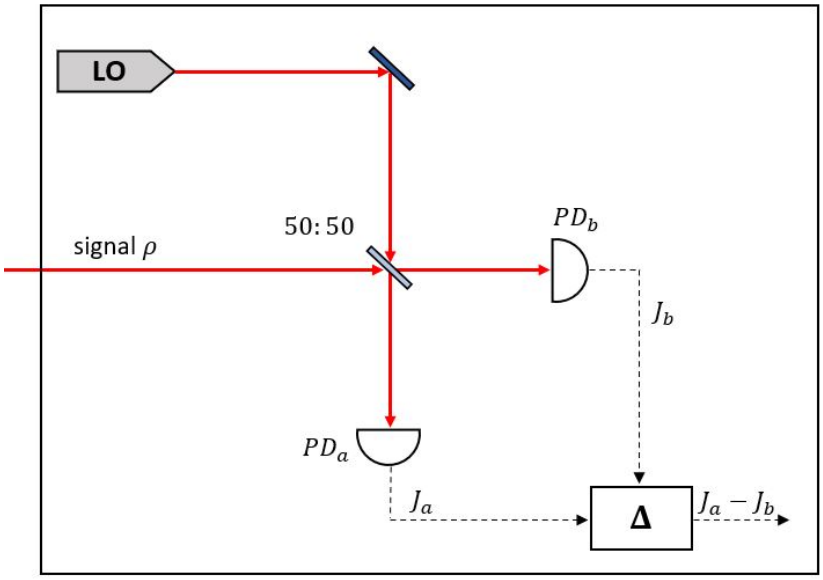

Figure 2.2.: Schematic of a homodyne detector. LO denotes the local oscillator and PD_a and PD_b are photodiodes. The box labelled with Δ subtracts the photocurrents J_a and J_b.

Consider the constellation illustrated in Figure 2.2. The main components of a homodyne detector are two photodiodes and a 50:50 beam splitter. We apply the signal we want to measure to mode 0 of the beamsplitter, while mode 1 contains the coherent laser light from the local oscillator. Following the beamsplitter relation in Eq. (2.21), we obtain the annihilation operators of the output modes 2 and 3 of the beam splitter

$$\hat{a}_2 = \frac{1}{\sqrt{2}}\left(\hat{a}_0 + i\hat{a}_1\right)$$
$$\hat{a}_3 = \frac{1}{\sqrt{2}}\left(\hat{a}_1 + i\hat{a}_0\right).$$

At the outputs, we place photodiodes, which measure the intensities $J_a \propto \langle \hat{a}_2^\dagger \hat{a}_2 \rangle$ and $J_b \propto \langle \hat{a}_3^\dagger \hat{a}_3 \rangle$. The photodiodes output electric currents J_a and J_b which are proportional to the incident intensity. Thus, we can easily build the difference between the currents from the photodiodes a and b, hence between the measured intensities,

$$\langle \hat{n}_{ab} \rangle := J_a - J_b \propto \langle \hat{a}_0^\dagger \hat{a}_1 - \hat{a}_0 \hat{a}_1^\dagger \rangle.$$

Note that we inserted the expressions for $\hat{a}_2$ and $\hat{a}_2$ from above. Assuming that the reference beam in mode 1 is a coherent state with amplitude β and that it has the same frequency as our signal, one obtains

$$\langle \hat{n}_{ab} \rangle \propto |\beta| \langle \hat{X}(\theta) \rangle, \tag{2.22}$$

where

$$\hat{X}(\theta) := \frac{1}{\sqrt{2}}\left(\hat{a}_0 e^{-i\theta} + \hat{a}_0^\dagger e^{i\theta}\right) \tag{2.23}$$

is the field quadrature operator at the angle θ. Note that for $\theta = 0$ we obtain $\hat{q}$ and for $\theta = \frac{\pi}{2}$ we obtain $\hat{p}$. Hence, by choosing the phase difference θ between the signal and the reference beam properly, we can measure either the q- or the p-quadrature.

Unfortunately, homodyne detection allows us only to measure one of the quadratures at the same time. **Heterodyne detection** overcomes this issue at the cost of by 3dB lowered signal intensity. To perform heterodyne detection, we combine two homodyne detectors and an additional 50:50 beam splitter, which divides the signal into two parts, halving the intensity. Note that even though we do not actively apply any signal to the second input of this beamsplitter, our input is mixed with the vacuum state there, in accordance with the description of the quantum mechanical beamsplitter. In our sketch in Figure 2.3, we indicate the vacuum state by $|0\rangle$. As the reflected mode of a beamsplitter naturally experiences a phase shift

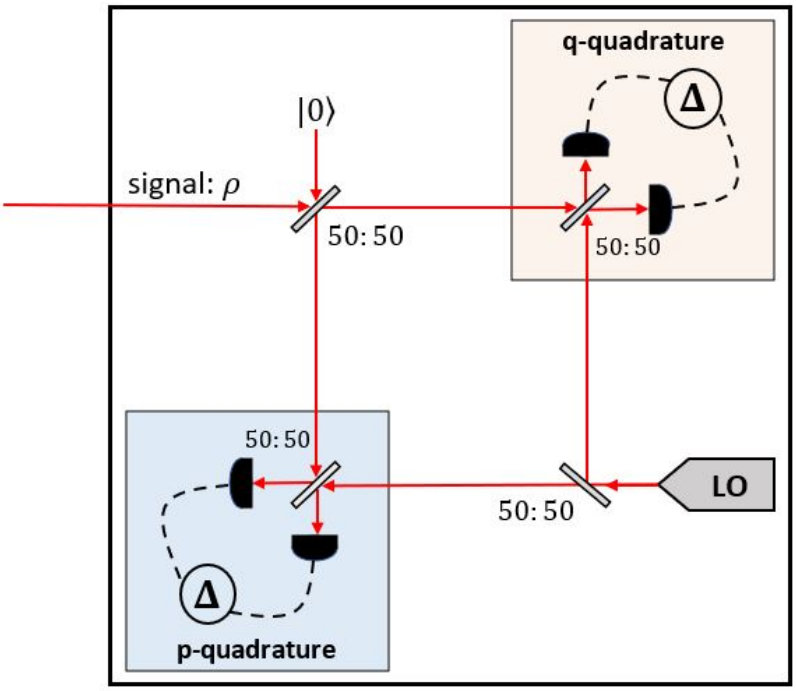

Figure 2.3.: Schematic of a heterodyne detector. LO denotes the local oscillator and the two boxes represent homodyne measurements which measure the q and p quadrature.

by $\frac{\pi}{2}$, we can measure the q- and the p-quadrature at the same time. The POVM of an ideal heterodyne detector reads [103]

$$E_y = \frac{1}{\pi} |y\rangle\langle y| \,. \tag{2.24}$$

2.5. Conic Programming

In this section, we summarise the theoretical background required to understand conic linear programming, following [40]. A standard text about convex optimisation is the book by Boyd and Vandenberghe [9]. We refer the reader to this work for more details.

2.5.1. Preliminaries

Definition 2.5.44: (Convex) Cone

A subset C of a vector space V over an ordered field F is called ***cone (linear cone)*** *if*

$$\forall x \in C,\ \forall \alpha \in F, \alpha > 0 :\ \alpha x \in C.$$

A cone is then a convex cone if

$$\forall \alpha, \beta \in F,\ \alpha, \beta > 0\ \forall x, y \in C :\ \alpha x + \beta y \in C. \tag{2.25}$$

Note that for a cone C we have C is convex $\Leftrightarrow C + C \subseteq C$. As we have defined a cone, we are now ready to define the dual of a cone.

Definition 2.5.45: Dual Cone

Let V be a vector space equipped with an inner product and $C \subseteq V$. The ***dual cone to*** *C is defined to be the set*

$$C^* := \{v \in V^* \mid \forall w \in C :\ \langle w, v \rangle \geqslant 0\}. \tag{2.26}$$

The cone of our main interest will be the closed convex cone of $n \times n$ Hermitian, positive semi-definite matrices.

2.5.2. Conic Programming and the Standard Form of SDPs

Consider $\mathcal{H}_A$ and $\mathcal{H}_B$, two separable Hilbert spaces and let $\mathcal{N} : \mathrm{L}(\mathcal{H}_A) \to \mathrm{L}(\mathcal{H}_B)$ be a linear map. Furthermore, denote by $\mathcal{K}_A \subseteq \mathrm{L}(\mathcal{H}_A)$ and $\mathcal{K}_A \subseteq \mathrm{L}(\mathcal{H}_B)$ two convex cones and let $H_A \in \mathrm{L}(\mathcal{H}_A)$ and $H_A \in \mathrm{L}(\mathcal{H}_B)$ be two arbitrary but fixed Hermitian matrices. A conic linear program is defined as follows:

(P) Primal problem:

$$\begin{aligned} &\alpha := \inf \langle X, H_A \rangle_{\mathcal{H}_A} \\ \text{s.t.} \\ &\mathcal{N}(X) - H_B \in \mathcal{K}_B \\ &X \in \mathcal{K}_A \end{aligned}$$

(D) Dual problem:

$$\begin{aligned} &\beta := \sup \langle Y, H_B \rangle_{\mathcal{H}_B} \\ \text{s.t.} \\ &H_A - \mathcal{N}^*(X) \in \mathcal{K}_A^* \\ &Y \in \mathcal{K}_B^* \end{aligned}$$

The difference between α, the primal solution and β, the dual solution, is called duality gap. Weak duality guarantees that for any primal feasible X and dual feasible Y we have $\alpha \geqslant \beta$, so the duality gap is always non-negative. Under certain conditions, we have even equality between the solution of the primal and the dual problem, which is called strong duality. A sufficient condition for strong duality is the so-called Slater's condition:
If there exists a primal feasible $X_0 \in \text{int}(\mathcal{K}_A)$ such that $\mathcal{N}(X_0) - H_B \in \text{int}(\mathcal{K}_B)$ and if there exists an optimal primal solution, then $\alpha = \beta$, so there is no duality gap.

In what follows, we focus on the cone of Hermitian, positive semi-definite matrices, as this will be the relevant cone in the present work. The subfield of convex optimisation which deals with the optimisation over the positive semi-definite cone is called semi-definite programming. The standard form for semi-definite programs reads as follows [108].

Definition 2.5.46: Standard Form for SDPs

Let $\mathcal{H}_A, \mathcal{H}_B$ be separable Hilbert spaces and $\Psi \in \mathrm{L}(\mathcal{H}_A, \mathcal{H}_B)$ a Hermitian-preserving map. Let $A \in Herm(\mathcal{H}_A)$ and $B \in Herm(\mathcal{H}_B)$.
*A **semi-definite program in standard form** is a triple (Ψ, A, B) with the following optimisation problems*

(P) Primal problem:

$$\begin{aligned} & \alpha := \min \langle A, X \rangle_{\mathcal{H}_A} \\ s.t. & \\ & \Psi(X) = B \\ & X \in Pos(\mathcal{H}_A) \end{aligned}$$

(D) Dual problem:

$$\begin{aligned} & \beta := \max \langle B, Y \rangle_{\mathcal{H}_B} \\ s.t. & \\ & A \succcurlyeq \Psi^*(Y) \\ & Y \in Herm(\mathcal{H}_B). \end{aligned}$$

The set

$$\mathcal{A} := \{X \in \mathrm{Pos}(\mathcal{H}_A) \mid \Psi(X) = B\}$$

is called the **primal feasible set**, while

$$\mathcal{B} := \{Y \in \mathrm{Herm}(\mathcal{H}_B) \mid A \succcurlyeq \Psi^*(X)\}$$

is called the **dual feasible set**.

3. Introduction to Quantum Key Distribution

> God had meant photons to travel rather than to stay put! This was the insight that made us think of using a quantum channel to transmit confidential information.
>
> *Gilles Brassard* [10]

The aim of this chapter is to give an overview of quantum key distribution and all notions required to follow the security proof in the main part of the present thesis. We begin by clearly defining the setting of quantum key distribution, followed by the definition of security and by reviewing the differences between asymptotic security analyses and finite-size security. In the second part of this chapter, we give an overview of the numerical security proof method we use in this work to obtain a tight lower bound on the secure key rate, including the dimension reduction method and the non-ideal detector with trusted detector noise extension.

3.1. Basic Setting of Quantum Key Distribution

Consider two remote, honest parties called Alice and Bob. They are connected via both an untrusted quantum channel and an authenticated public channel. There are several techniques known for how to authenticate a classical message. However, since this is a well-known classical process, for our purposes it suffices to know that given some small pre-shared secret key, Alice and Bob can authenticate their channel. Therefore, technically, we are dealing with a key-growing routine. An eavesdropper, commonly called Eve, can manipulate the quantum channels in any way that is permitted by the laws of physics and can read but not tamper with messages exchanged via the classical channel. With only classical techniques, it is impossible for Alice and Bob to establish a shared secret key in this setting, where Eve's only limitations are the laws of physics. However, thanks to the peculiar nature of quantum mechanics, this task turns out to be feasible with a

more advanced technique called quantum key distribution, or short QKD. One way of explaining this advantage of the quantum world is the no-cloning theorem [113], which is solely based on the very fundamental linear nature of quantum mechanics. The no-cloning theorem makes it impossible for Eve to distinguish non-orthogonal states with certainty without introducing errors that then can be detected by Alice and Bob. Notice that in the whole scenario, we did not put any constraints on the computational resources of the eavesdropper, i.e, quantum key distribution aims for information-theoretical security rather than relying on assumptions about the computational power like in classical cryptography. The second and even more striking advantage of QKD is perfect forward security. This means that QKD-keys at any future point in time are as secret as they have been when they were generated. Note that this is opposite to classical cryptography, where an increase in computational power immediately leads to a decline in secrecy, as information can be copied and stored for an arbitrarily long time and may be encrypted once the computational capacities suffice.

3.2. QKD Protocol

A QKD protocol is a publicly known list of instructions Alice and Bob follow to establish a secret key and is usually subdivided into a quantum phase and a classical phase. In the quantum phase, the quantum states are distributed via the quantum channel and measured, while in the classical phase the measured data is processed to decorrelate an eavesdropper's correlations and via communication over the classical channel the bit-strings of the communicating parties are error-corrected. While there exist protocols that involve trusted and untrusted third parties, we focus on the case, where only Alice and Bob perform protocol steps. Furthermore, in the sub-class of QKD protocols we consider in the present thesis, Alice's and Bob's (measurement) devices are assumed to be fully characterised and trusted and their labs are assumed to be inaccessible to Eve. This is called device-dependent QKD. However, we note that there exist QKD protocol families with weaker assumptions like measurement-device independent quantum key distribution (MDI-QKD) [11, 66], where measurement devices do not have to be trusted or even device-independent quantum key distribution (DI-QKD) (see [83] for a review), where monitoring violations of Bell-inequalities allows Alice and Bob to establish a secret key without trusting any devices. Clearly, in general, keys generated under weaker assumptions are shorter than keys generated in the device-dependent scenario.

We differentiate between two big classes of protocols, **entanglement-based (EB) protocols** and **prepare-and-measure (P&M) protocols**. In entanglement-based protocols both Alice and Bob receive one share of a bipartite state and

then each of them performs measurements on the received state. In prepare-and-measure protocols, Alice holds a quantum source, prepares a quantum state and sends the prepared state to Bob via the quantum channel, while keeping a (classical) record of the prepared state. It turns out that both families are equivalent thanks to the source-replacement scheme [21, 28], which allows to translate entanglement-based protocols into prepare-and-measure protocols and vice-versa. The idea is that both implementations turn out to be indistinguishable for everyone outside of Alice's lab, and hence can be considered equivalent. This happens to be very useful in security analyses as one can switch between both descriptions, depending on which formulation is more convenient for theoretical analysis. However, we want to emphasise that source replacement does not change the physical implementation of the protocol, as it is only a theoretical concept to ease certain arguments in the security proof.
Next, let us describe the steps of a generic prepare-and-measure protocol.

1.) **State Preparation** — Alice prepares one out of $N_{\mathrm{St}} \in \mathbb{N}$ quantum states $\{|\phi_0\rangle, ..., |\phi_{N_{\mathrm{St}}-1}\rangle\}$ according to some probability distribution $\{p_0, ..., p_{N_{\mathrm{St}}-1}\}$ in her lab and sends it to Bob via the quantum channel. She keeps track of the state she prepared in a classical register.

2.) **Measurement** — Bob receives the states and measures them with a POVM $\{P_B^i\}_{i\in\mathcal{I}}$. Afterwards, he holds a classical random variable representing his measurement results.

Steps 1 and 2 are repeated N times. After N rounds Alice and Bob hold two correlated random variables representing their raw data.

3.) **Public Announcement and Sifting** — Alice and Bob agree to perform testing on a random subset of m rounds. For these rounds, Alice announces publicly which state she prepared and Bob announced his measurement results. This allows them to calculate some statistical quantities they use to decide if they have to abort the protocol or not. In case they conclude that Eve might have gained too much information about their quantum states, they stop. This phase is often (misleadingly) called parameter estimation, implying that we determine channel parameters like channel transmission and noise. We note that in particular in the finite-size regime, this naming is inaccurate, as we do not estimate 'real' quantities (which are never accessible) but calculate statistical quantities and compare them with predefined acceptance sets. Therefore, in the present thesis, we coin the term **acceptance testing**.

   Additionally, some protocols allow for sifting. This means that Alice and Bob communicate to agree to discard particular rounds and to keep others

(for example, in protocols with basis choice, they might only want to proceed with rounds where they chose the same bases).

4.) **Key Map** — If they decided to proceed, one party performs a key map, based on the publicly announced data and their own private information. The key map assigns every round that is left after the testing and sifting procedure a symbol in the set $\{0, ..., N_{\text{Symb}} - 1, \perp\}$ in case of a N_{Symb}-ary key map. Assigning $\perp$ to some of the rounds and announcing it publicly allows performing postselection. Mathematically, a key map is a function

$$g : \ S_1^{\text{public}} \times S_2^{\text{public}} \times S_2^{\text{private}} \to \{0, ..., N_{\text{Symb}} - 1, \perp\},$$

where '2' labels the party that performs the key map. Motivated by the direction of the information flow (with or reverse to the quantum signals), in case Alice does the key map it is called direct reconciliation, while Bob performing the key map is referred to as reverse reconciliation.

5.) **Error Correction (EC)** — Alice and Bob use the classical channel to get their data to agree with the key established by the party who performed the key map. Thereby, they unavoidably reveal some information about their key.

6.) **Privacy Amplification (PA)** — In the privacy amplification step, Alice and Bob determine the maximal length of their final key while still being secure and then randomly choose a member of the family of two-universal hash-functions and apply it to their shared bit-string. Eventually, they obtain the final secret shared key of length ℓ.

Without performing postselection, for CV-QKD with direct reconciliation, a secure key cannot be created if the efficiency of the quantum channel falls below 50% as Eve can mimic the losses by inserting a beam splitter [45]. Then, in case the losses exceed 50% Eve holds a larger share of the state than Bob, hence can extract more information than him. However, as shown in [96] this issue can be resolved by performing postselection. In the present thesis, we focus on reverse reconciliation, where Eve has to guess Bob's key that is based on his measurement results rather than the state Alice prepared. Reverse reconciliation is known to have a better performance for CV-QKD protocols, in particular for higher transmission distances. We note that postselection can be applied in the case of reverse reconciliation as well (see, for example, [56, 64]). However, our proof method is applicable both to direct and reverse reconciliation.

3.3. Security Analysis of QKD Protocols

Once Alice and Bob agreed on a certain QKD protocol, they require a physical implementation capable of performing all required protocol steps as well as a security proof, determining if they are able to distil secret key (and how much) with their chosen protocol. In the present thesis, we focus on the security proof and consider the details of the physical implementation only up to a degree that is necessary for the security proof. By security proof, we mean a theoretical assessment of the protocol, whose output is a lower bound on the achievable secure key rate (the number of secure key bits divided by the total number of signals sent) of a certain QKD protocol, given some system parameters like the channel noise, the channel transmittance or the detection efficiency and under some mathematical description of the involved devices. While the goal of every security analysis is to prove security without any assumptions or restrictions on Eve's abilities, it can be favourable to first prove security under some assumptions, simplifying the security proof significantly, and lifting the proof to a more general case afterwards.

3.3.1. Eavesdropping Strategies

The following considerations refer to the prepare-and-measure picture and follow [90]. In general, Eve can attach an ancilla state to the signal that leaves Alice's lab and let them interact via some unitary transformation. By measuring her ancilla state after the interaction, Eve hopes to gain some information about the state Alice prepared. Depending on how Eve's ancillae are prepared, how long Eve can wait to do her measurements (i.e., depending on if she has a quantum memory), and the way she has to perform her measurement, we distinguish three different classes of attacks, starting with the weakest.

- **Individual attacks:** Eve's ancilla states interact with each of Alice's quantum signals individually and independently from others, following the same strategy. This does not mean that she has to perform the same action in every round but can include probabilistic strategies. Eve has to measure her states before Alice and Bob start their classical postprocessing.
- **Collective attacks:** Again, Eve attacks each round of quantum signals independently from each other, hence Alice's, Bob's and Eve's common state can be assumed to have tensor-product structure $\rho_{ABE}^{N} = \sigma_{ABE}^{\otimes N}$, where σ_{ABE} is some single-round state. In contrast to individual attacks, Eve is allowed to keep her ancilla states in a quantum memory until Alice and Bob have finished their postprocessing routine. Then, she may perform a collective measurement on all of her ancilla states based on what she learnt from Alice's and Bob's communication over the classical channel.

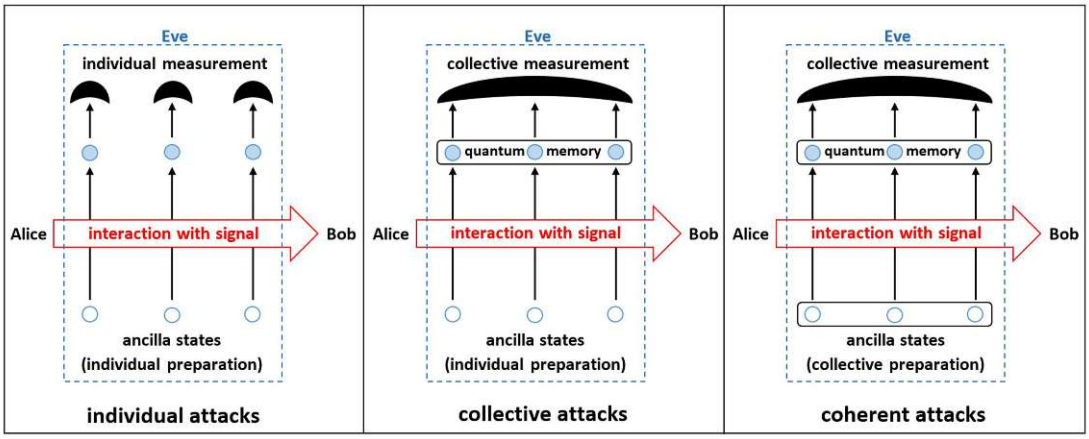

Figure 3.1.: Schematic sketch of the three classes of eavesdropping strategies.

- **Coherent attacks:** Coherent attacks represent the most general class of attacks. Eve does not have to interact with every round independently from each other. She may prepare one large ancilla state and let it interact with each of the rounds via some joint unitary operation. Afterwards, she can store her ancilla state in a quantum memory and measure at some time, in particular after Alice and Bob have finished their postprocessing routine. In her collective measurement Eve can use the knowledge she gained from listening to the communication during the classical phase.

Individual attacks turned out to be unjustifiably unrestrictive, leading to overly optimistic key rates. In contrast, for many classes of protocols, there exist techniques that allow us to relate key rates against collective attacks to key rates against coherent attacks, like the quantum de Finetti theorem [86], the postselection technique [18] or the (generalised) entropy accumulation theorem [26, 70], stating that collective attacks are optimal up to some non-leading order correction terms. Hence, in many cases, it is reasonable to simplify the analysis by assuming collective attacks as a first step and lifting the security statement to general attacks afterwards.

3.3.2. Asymptotic vs. Finite-Size Security

In practical settings, Alice and Bob exchange a finite amount of $N \in \mathbb{N}$ signals in the quantum phase (steps 1 and 2) before they proceed with the classical phase (steps 3 to 6) of the protocol. However, from the perspective of security analysis, it is much easier to assume that the number of exchanged signals $N \to \infty$. Security proofs relying on this assumption are called asymptotic security proofs.

The asymptotic secure key rate against i.i.d. collective attacks is given by the Devetak-Winter formula [23]

$$R_\infty \geqslant I(X:Z) - I(Z:E), \tag{3.1}$$

where X and Z denote Alice's and Bob's bit strings, respectively and E denotes Eve's knowledge, including all knowledge she gained from listening to Alice's and Bob's classical communication. In general, Eve's information about Bob's key string is difficult to calculate. The Holevo quantity $\chi(Z:E)$ gives an upper bound on Eve's accessible information $I(Z:E)$. It is given by

$$\chi(Z:E') = H(\rho_{E'}) - \sum_z p(z) H(\rho_{E'|z}), \tag{3.2}$$

where H denotes the von Neumann entropy, the sum is over Bob's classical alphabet distributed according to probability $p(z)$, $\rho_{E'|z}$ is Eve's conditional ancilla state and $\rho_{E'} = \sum_z p(z)\rho_{E'|z}$ is Eve's marginal state. Note that our formulation assumes reverse reconciliation. For direct reconciliation, replace the quantities referring to Bob with those corresponding to Alice.
While the asymptotic limit is a convenient simplification to ease the theoretical analysis, it is an idealisation that can never be achieved in practical settings. Therefore, the ultimate goal is to prove security for a finite number of rounds N, i.e., to prove security in the finite-size regime. To take finite-size effects into account, we have to modify the key rate formula in Eq. (3.1) by subtracting a finite-size correction term $c(N,\epsilon)$,

$$R_{\text{fin}} \geqslant I(X:Y) - I(Y:E) - c(N,\epsilon). \tag{3.3}$$

Besides the number of transmitted quantum signals N, the finite-size correction term depends on $\epsilon > 0$ which takes the failure probabilities of subprotocol steps into account. This epsilon is closely linked to the idea of composability, which will be discussed in Section 3.3.3. For ϵ small enough but non-zero and $N \to \infty$, the correction term should converge to zero, $c(N,\epsilon) \overset{n\to\infty}{\to} 0$, i.e. Eq. (3.3) converges to Eq. (3.1), $R_\infty = \lim_{N\to\infty} R_{\text{fin}}(N)$.
In the finite-size regime, we are usually interested in the achievable key length ℓ as well. Note that the finite-size key rate R_{fin} is related to the key length via

$$R_{\text{fin}} = \frac{\ell}{N}.$$

3.3.3. Composability

Cryptographic keys are generated to encrypt messages and are therefore used as part of a larger protocol. For example, the obtained secret key can be used as

an input for the one-time pad to enable secure communication. Therefore, it is essential that the security of subprotocols can be used to argue that a larger cryptographic scheme is secure. This is called **composable security**. In the present subsection, we summarise the idea of composability, following [81, Chapter II] and [82].

Early security proofs like the BB84 security proof by Shor and Preskill [95] based their proof on a non-composable security definition, which was shown to be insecure when combined in a larger framework [59]. Composability goes back to developments in classical cryptography where it was proposed independently by Canetti [14, 15] and Pfitzmann and Waidner [80]. It was applied to the quantum case briefly after [3, 4, 104]. The composability notion for quantum key distribution we present in this section goes back to Renner and König [85, 87].

In contrast to previous security definitions, which considered the information gathered by an adversary, composable security compares an ideal system with the real protocol and quantifies how well they can be told apart from each other. This is known as the real-world ideal-world paradigm. An adversary is therefore seen as a distinguisher that has all abilities of the original adversary and is able to simulate any protocol that ran before the examined cryptographic protocol. He can choose the inputs of the protocol (so, the outputs of previously run protocols) and obtain all outputs that are not private to Alice or Bob while being allowed to tamper with the communication channels similar to the original adversary. The distinguisher then has access to two black boxes, the ideal and the real implementation and has to decide which one is the real protocol. Then, a real system is called secure if it is indistinguishable from the ideal protocol, i.e., if the probability of choosing the right one is not better than randomly guessing. Let us call the ideal protocol $\mathcal{F}_0$ and the real protocol $\mathcal{F}_1$ and assume a distinguisher $\mathcal{D}$ is given both the output x of the ideal and of the real protocol with probability $p = \frac{1}{2}$. The output of the distinguisher is a guess $g \in \{0, 1\}$, where $c = 0$ or $c = 1$ indicate which protocol he believes the output he received came from. Then, the distinguishability is defined as [85, Proposition 2.1.1]

$$d(\mathcal{F}_0, \mathcal{F}_1) := \max_{\mathcal{D}} \left[2 \left(\Pr[g = c] - \frac{1}{2} \right) \right]. \tag{3.4}$$

It can be shown that the trace distance is exactly the right measure to capture the notion of distinguishability,

$$\frac{1}{2} \left|\left| \rho_x^{(0)} - \rho_x^{(1)} \right|\right|_1 = d(\mathcal{F}_0, \mathcal{F}_1). \tag{3.5}$$

In a real implementation, we cannot expect to achieve perfect security, therefore we have to weaken our security definition to make it practical. This is captured

by ϵ-security. A real implementation is ϵ-secure if its distinguishability from the ideal protocol is less than ϵ.
According to the security notion introduced by Renner and König [87] for QKD protocols, the key of the real system is compared to a random and uniformly distributed key that is completely uncorrelated to the eavesdropper's system E,

$$\rho^{\text{ideal}}_{K_A K_B E} = \frac{1}{N} \sum_{x=0}^{N-1} |x\rangle\langle x| \otimes |x\rangle\langle x| \otimes \rho_E. \tag{3.6}$$

So, a perfect QKD protocol outputs a key with the following properties

1. $K_A = K_B$,
2. K_B is uniformly distributed,
3. Eve does not have any knowledge about K_B.

The density matrix corresponding to the successful execution of the real implementation reads

$$\rho^{\text{real}}_{K_A K_B E} = \sum_{x,y=0}^{N-1} P(x,y)\, |x\rangle\langle x| \otimes |y\rangle\langle y| \otimes \rho_E^{x,y}. \tag{3.7}$$

Let us use the symbol $\perp$ to denote the abortion of the protocol and $p(\perp)$ the corresponding abort-probability. Then, the states taking the probability that the protocol aborts into account, read

$$\sigma^{\text{ideal}}_{ABE} = p(\perp)\, |\perp\rangle\langle\perp| \otimes |\perp\rangle\langle\perp| \otimes \rho_E^{\perp} + (1 - p(\perp))\rho^{\text{ideal}}_{ABE}, \tag{3.8}$$

$$\sigma^{\text{real}}_{ABE} = p(\perp)\, |\perp\rangle\langle\perp| \otimes |\perp\rangle\langle\perp| \otimes \rho_E^{\perp} + (1 - p(\perp))\rho^{\text{real}}_{ABE}. \tag{3.9}$$

The protocol is trivially secure if it aborts. Therefore, the security definition for a QKD protocol is

$$\frac{1}{2} \left|\left|\rho^{\text{ideal}}_{K_A K_B E} - \rho^{\text{real}}_{K_A K_B E}\right|\right|_1 \leqslant \frac{\epsilon}{1 - p(\perp)}. \tag{3.10}$$

If we introduce the state

$$\rho_{UUE'} := \frac{1}{N} \sum_{x=0}^{N-1} |x\rangle\langle x| \otimes |x\rangle\langle x| \otimes \rho_E^x \tag{3.11}$$

and apply the triangle inequality, we can split the security condition into two parts,

$$\begin{aligned} &\frac{1}{2} \left|\left|\rho^{\text{ideal}}_{K_A K_B E} - \rho^{\text{real}}_{K_A K_B E}\right|\right|_1 \\ \leqslant &\frac{1}{2} \left|\left|\rho^{\text{ideal}}_{K_A K_B E} - \rho_{UUE}\right|\right|_1 + \frac{1}{2} \left|\left|\rho_{UUE} - \rho^{\text{real}}_{K_A K_B E}\right|\right|_1 \\ < &\frac{\epsilon_{\text{sec}} + \epsilon_{\text{cor}}}{1 - p(\perp)}. \end{aligned}$$

The first part,

$$(1 - p(\perp))\, \Delta(\rho^{\text{ideal}}_{K_A K_B E}, \rho_{UUE}) < \epsilon_{\text{sec}}, \tag{3.12}$$

is called secrecy condition, which bounds the joint probability of not aborting and the private information is known to Eve, while the second part,

$$(1 - p(\perp))\, \Delta(\rho_{UUE}, \rho^{\text{real}}_{K_A K_B E}) = (1 - p(\perp))\, \Pr\left[K_A \neq K_B\right] < \epsilon_{\text{sec}}, \tag{3.13}$$

is called correctness condition, which bounds the joint probability of not aborting and Alice and Bob not sharing the same key. This shows that if a protocol is ϵ_{sec}-secret and ϵ_{cor}-correct then it is $\epsilon := \epsilon_{\text{sec}} + \epsilon_{\text{cor}}$ secure.
We have already noted that a protocol that aborts all the time is trivially secure. However, we want a practically useful protocol to execute successfully most of the time when the adversary behaves honestly. This is called robustness. In more detail, let q be a parameter quantifying the introduced noise (if the adversary is passive). Then, the probability of a key being generated is a function of q and for every q the probability that the protocol aborts is δ, the robustness of the protocol [82, Section 4.4]

3.4. Numerical Security Proof Framework

In the present thesis, we use the numerical security proof framework introduced in [19, 110] which was applied to calculate tight secure key rates in the asymptotic limit for DM CV-QKD protocols in [64]. In contrast to analytical security proofs which are often very technical, introduce looseness in the obtained lower bounds and are rather inflexible regarding changes in the protocol structure, numerical security proofs do not have those drawbacks on the cost of suffering from finite numerical precision and high computational complexity. In the upcoming section, we review the numerical security proof method for DM CV-QKD protocols in the asymptotic limit, following [19, 110] for the general idea and [64] for the application to DM CV-QKD protocols.

3.4.1. Asymptotic Numerical Security Proof Framework

Consider the entanglement-based version of the generic QKD protocol we described in Section 3.2 under the assumption that Alice and Bob exchange infinitely many rounds of signals. We denote the measurements Alice and Bob perform on system A and B to obtain their raw key strings by Z_A and Z_B. Let the corresponding POVM elements be $\{Z_A^i\}_{i\in\mathcal{I}}$ and $\{Z_B^j\}_{j\in}$. The Devetak-Winter formula [23] for the case of reverse reconciliation,

$$R_\infty \geqslant I(Z_A : Z_B) - I(Z_B : E)$$

can be reformulated using the definition of the mutual information in Eq. (2.8) and the entropy relations in Eq. (2.7) and Eq. (2.9). We obtain

$$R_\infty \geqslant H(Z_B|E)_\rho - H(Z_B|Z_A)_\rho. \tag{3.14}$$

If we denote the tripartite density operator shared between Alice, Bob and Eve by ρ_{ABE}, the density operators related to the von Neumann entropies in the key rate formula read

$$\rho_{Z_A Z_B} = \sum_{\substack{i\in\mathcal{I}\\ j\in\mathcal{J}}} \mathrm{Tr}\left[\left(Z_A^i \otimes Z_B^j\right)\rho_{AB}\right] |i\rangle\langle i| \otimes |j\rangle\langle j|\,, \tag{3.15}$$

$$\rho_{Z_B E} = \sum_{j\in\mathcal{J}} |j\rangle\langle j| \otimes \mathrm{Tr}\left[\left(Z_B^j \otimes \mathbb{1}_E\right)\rho_{BE}\right]. \tag{3.16}$$

The source-replacement scheme [21, 28] allows us to describe prepare-and-measure protocols in the entanglement-based picture, hence Alice effectively prepares

$$|\Psi\rangle_{AA'} = \sum_{x\in\mathcal{N}_{\mathrm{St}}} \sqrt{p_x}\,|x\rangle_A\,|\phi_x\rangle_{A'}\,, \tag{3.17}$$

where we introduced the short notation $\mathcal{N}_{\mathrm{St}} := \{0, ..., N_{\mathrm{St}}-1\}$ and where A' denotes the register that is sent to Bob via the quantum channel. In this picture, Alice chooses the state she prepared, using the local POVM $Z_A := \{|x\rangle\langle x|\}_{x\in\mathcal{N}_{\mathrm{St}}}$ on her register A. Describing the quantum channel connecting Alice and Bob by the CPTP map $\mathcal{E}_{A'\to B}$, the bipartite state upon Bob receiving his share reads

$$\rho_{AB} = \left(\mathrm{id}_A \otimes \mathcal{E}_{A'\to B}\right)\left(|\Psi\rangle\langle\Psi|_{AA'}\right). \tag{3.18}$$

Then, depending on Alice's measurement $|x\rangle\langle x|$, Bob receives

$$\rho_B^x = \frac{1}{p_x}\mathrm{Tr}_A\left[\left(|x\rangle\langle x| \otimes \mathbb{1}_B\right)\rho_{AB}\right]. \tag{3.19}$$

We can use this formulation to determine constraints on Alice's and Bob's bipartite state which helps us to specify the set over which the optimisation in Eq. (3.23) is performed.

It is reasonable to assume that Eve does not have access to Alice's lab (strong lab wall assumption), hence Eve cannot modify Alice's part of the state as it never leaves her laboratory. Therefore, Alice's share of the state is fixed,

$$\rho_A = \mathrm{Tr}_B\left[\rho_{AB}\right] = \sum_{x,x'\in\mathcal{N}_{\mathrm{St}}} \sqrt{p_x p_{x'}}\,\langle\phi_x|\phi_{x'}\rangle\,|x\rangle\langle x|_A\,. \tag{3.20}$$

Bob's state travels through the quantum channel, which is under Eve's control before he receives it. Therefore, Bob's share of their joint state ρ_{AB} is unknown

and he has to perform local measurements to constrain the set of possible density operators. We denote the set of performed measurements by $\{\Gamma_k\}_{k\in\{0,\dots,M-1\}}$ for $M \in \mathbb{N}$, where the Γ_k's are Hermitian operators and the corresponding expected values by $\gamma_k := \langle\Gamma_k\rangle = \mathrm{Tr}\left[\Gamma_k \rho_{AB}\right]$. In addition, we require that ρ_{AB} represents a valid quantum state, i.e., $\rho \geqslant 0$ and $\mathrm{Tr}\left[\rho\right] = 1$. The trace constraint can be included in the first set of constraints by setting $\Gamma_M := \mathbb{1}_B$.
These constraints make up the set, defining all possible density matrices

$$\mathcal{S}_\infty := \{\rho_{AB} \geqslant 0 : \ \rho_A = \mathrm{Tr}_B\left[\rho_{AB}\right], \ \forall k \in \{0,\dots,M\} : \ \mathrm{Tr}\left[\Gamma_k \rho_{AB}\right] = \gamma_k\}. \quad (3.21)$$

Eve's system is assumed to purify ρ_{AB} as this gives her the most information about ρ_{AB}. In general, the set $\mathcal{S}_\infty$ is non-trivial and contains many density operators. Since we are looking for a lower bound on the secure key rate, we have to find the state ρ_{AB} in $\mathcal{S}_\infty$ which minimises Eq. (3.14), i.e., the state which gives Eve the most information about ρ_{AB}, while still being compatible with the constraints imposed by $\mathcal{S}_\infty$. Therefore, we obtain

$$R_\infty \geqslant \min_{\rho_{AB}\in\mathcal{S}_\infty} \left[H(Z_B|E)_\rho - H(Z_B|Z_A)_\rho\right]. \quad (3.22)$$

To ease the notation, we drop the subscript AB if it is clear from the context. It is shown in [110, Section 4] that Eq. (3.22) can be reformulated to

$$R_\infty \geqslant \min_{\rho\in\mathcal{S}_\infty} D\left(\mathcal{G}(\rho)||\mathcal{Z}(\mathcal{G}(\rho))\right) - p_{\mathrm{pass}}\delta^{\mathrm{EC}}_{\mathrm{leak}}, \quad (3.23)$$

where $D(\rho||\sigma)$ is the quantum relative entropy, $\mathcal{G}$ is a completely positive map describing postprocessing steps, $\mathcal{Z}$ is a completely positive trace-preserving map used to read out the result of the key map (see [64] for a more detailed explanation of the maps $\mathcal{G}$ and $\mathcal{Z}$) and p_{pass} is the probability of passing the sifting procedure (including postselection, see steps 3.) and 4.) of the generic protocol in Section 3.2). Furthermore, by $\delta^{\mathrm{EC}}_{\mathrm{leak}}$, we denote the information-leakage in the information reconciliation procedure. Thanks to the joint convexity of the quantum relative entropy and the linearity of the maps $\mathcal{G}$ and $\mathcal{Z}$ the objective function $f(\rho) := D\left(\mathcal{G}(\rho)||\mathcal{Z}(\mathcal{G}(\rho))\right)$ is convex. As the constraints in Eq. (3.21) are linear, we conclude that the optimisation problem

$$\alpha := \min_{\rho\in\mathcal{S}_\infty} f(\rho) \quad (3.24)$$

is a convex optimisation problem. In more detail, we face a semidefinite program (SDP) with a convex, non-linear objective function. While, in general, there is not much hope in solving this optimisation analytically, there exist numerical methods to solve problems of that structure numerically. However, numerical methods cannot be expected to find the exact minimum, but only yield solutions close to

the actual optimum. Since this is not a reliable lower bound for our key rate finding problem, i.e., the obtained key rates would not guarantee security, we require a more sophisticated method. The numerical security proof method established in [19, 110] tackles the problem using a two-step procedure. In the first step, the authors solve the optimisation problem approximately, finding a density matrix representing a close-to-optimal eavesdropping attack. Therefore, the output of step 1 gives only an upper bound on the secure key rate. In the second step, the result from step 1 is converted into a lower bound, combining a linearisation of the problem, based on the intermediate solution of step 1, with duality theory for semidefinite programs.
Since we deal with linearisations of the objective function f, we require the gradient of f at some point ρ. The gradient of the (matrix-valued) map f at some point ρ can be defined in the standard basis $\{|k\rangle\}$

$$\nabla f(\rho) := \sum_{k,j} c_{jk} \, |j\rangle\langle k| \, , \quad c_{jk} := \left. \frac{\partial f(\sigma)}{\partial \sigma_{jk}} \right|_{\sigma=\rho} , \quad \sigma_{jk} := \langle j| \, \sigma \, |k\rangle \, . \tag{3.25}$$

If we insert $f(\rho) = D(\mathcal{G}(\rho)||\mathcal{Z}(\mathcal{G}(\rho)))$, following the rules given in [79], we derive for the gradient

$$|\nabla f(\rho)|^T = \mathcal{G}^\dagger \left(\log_2 \left(\mathcal{G}(\rho) \right) \right) - \mathcal{G}^\dagger \left(\log_2 \left(\mathcal{Z}(\mathcal{G}(\rho)) \right) \right) . \tag{3.26}$$

However, the gradient might not exist over the whole range of the feasible set. Therefore, the authors in [110] introduce a small perturbation $\tilde{\epsilon} > 0$ that maps $\mathcal{G}(\rho)$ to its interior. For τ, the maximally mixed state in the output space of $\mathcal{G}$, we define

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

This ensures that the eigenvalues of ρ are non-zero. Then, using the perturbed map

$$\mathcal{G}_{\tilde{\epsilon}}(\rho) := \left(\mathcal{D}_{\tilde{\epsilon}} \circ \mathcal{G} \right) (\rho) \tag{3.27}$$

they show in [110, Lemma 1] that the gradient of

$$f_{\tilde{\epsilon}}(\rho) := D \left(\mathcal{G}_{\tilde{\epsilon}}(\rho) || \mathcal{Z}(\mathcal{G}_{\tilde{\epsilon}}(\rho)) \right) \tag{3.28}$$

exists for all $\rho \geqslant 0$. Hence, in what follows, we frequently replace f by its perturbed version $f_{\tilde{\epsilon}}$ without stating this explicitly.
Since the objective function is highly non-linear, step 1 is solved iteratively. One well-suited method for this task is the Frank-Wolfe algorithm [29], which is an iterative first-order optimisation algorithm for constrained, convex optimisation problems. It is known for staying within the feasible set and therefore we do not require a projection that brings us back after every iteration (in contrast to alternative methods like the gradient descent algorithm). The guaranteed convergence

of the Frank-Wolfe algorithm is only $\mathcal{O}\left(\frac{1}{k}\right)$ [51], where k is the number of iterations. Therefore, we replace the update rule for the step width with a line-search in the found descent direction. Furthermore, since the solution of a semidefinite program in every iteration is computationally costly, we introduce an additional stopping criterion to avoid the execution of iterations that do not lead to significant improvements. This leads to the following modified Frank-Wolfe algorithm [110].

Algorithm 3.4.1: Modified Frank-Wolfe Algorithm

Choose $\delta_{\mathrm{FW}} > 0$, $i_{\max} \in \mathbb{N}$ and $\rho^{(0)} \in \mathcal{S}_\infty$
for $i = 1$ **to** $i_{\max}$ **do**
  Compute $\Delta\rho := \arg\min \mathrm{Tr}\left[(\Delta\rho)^\top \nabla f(\rho^{(i)})\right]$ subject to $\Delta\rho + \rho^{(i)} \in \mathcal{S}_\infty$
  if $\mathrm{Tr}\left[(\Delta\rho)^\top \nabla f(\rho^{(i)})\right] < \delta_{\mathrm{FW}}$ **then**
    return $\rho^{(i)}$
  else
    Find $\lambda \in (0,1)$ such that $\lambda := \mathrm{argmin} f(\rho^{(i)} + \lambda\, \Delta\rho)$
    Update $\rho^{(i+1)} := \rho^{(i)} + \lambda\Delta\rho$
  end if
end for

Let us call the output of this algorithm $\rho_{\text{Step 1}}$, which gives rise to an upper bound on the secure key rate. It remains to convert this into a lower bound. Since the objective function is convex, the hyperplane defined via the gradient of f at $\rho_{\text{Step 1}}$ lies underneath the graph of f, $\forall\sigma \in \mathcal{S}_\infty$:

$$f(\sigma) \geqslant f(\rho_{\text{Step 1}}) + \mathrm{Tr}\left[(\sigma - \rho_{\text{Step 1}})^\top \nabla f(\rho_{\text{Step 1}})\right].$$

This holds, in particular for the minimiser $\rho^* \in \mathcal{S}_\infty$. Therefore, one deduces

$$\begin{aligned} f(\rho^*) &\geqslant f(\rho_{\text{Step 1}}) + \mathrm{Tr}\left[(\rho^* - \rho_{\text{Step 1}})^\top \nabla f(\rho_{\text{Step 1}})\right] \\ &\geqslant f(\rho_{\text{Step 1}}) + \min_{\sigma\in\mathcal{S}_\infty} \mathrm{Tr}\left[(\sigma - \rho_{\text{Step 1}})^\top \nabla f(\rho_{\text{Step 1}})\right]. \end{aligned}$$

As $\rho_{\text{Step 1}}^\top \nabla f(\rho_{\text{Step 1}})$ is constant with respect to the minimisation, lower-bounding our original optimisation problem reduces to solving

$$\min_{\sigma\in\mathcal{S}_\infty} \mathrm{Tr}\left[\sigma^\top \nabla f(\rho_{\text{Step1}})\right]. \tag{3.29}$$

The authors in [110] show that the dual of this linearised problem reads

$$\max_{\vec{y}\in\mathcal{S}_\infty^*(\rho_{\text{Step 1}})} \vec{\gamma}\cdot\vec{y}, \tag{3.30}$$

where

$$\mathcal{S}^*_\infty(\rho_{\text{Step 1}}) := \left\{ \vec{y} \in \mathbb{R}^{M+1} : \sum_{i=0}^{M} y_i \Gamma_i \leqslant \nabla f(\rho_{\text{Step 1}}) \right\} \tag{3.31}$$

and $\gamma_i := \langle \Gamma_i \rangle$. Weak duality then implies that the solution of the dual is a lower bound for the solution of the primal problem. This leads to Theorem 2 in [110], which states that for any attack $\rho_{\text{Step 1}} \in \mathcal{S}_\infty$,

$$\alpha \geqslant \beta_{\tilde{\epsilon}}(\rho_{\text{Step 1}}) := f_{\tilde{\epsilon}}(\rho_{\text{Step 1}}) - \text{Tr}\left[\rho_{\text{Step 1}} \nabla f_{\tilde{\epsilon}}(\rho_{\text{Step 1}})\right] + \max_{\vec{y} \in \mathcal{S}^*_\infty} \vec{\gamma} \cdot \vec{y} - \zeta_{\tilde{\epsilon}}, \tag{3.32}$$

with $\zeta_{\tilde{\epsilon}} := 2\tilde{\epsilon}(d'-1) \ln\left(\frac{d'}{\tilde{\epsilon}(d'-1)}\right)$ and $d' := \dim(\mathcal{G}(\rho_{\text{Step 1}})$. The last correction term takes the price into account we pay for using the perturbed objective function $f_{\tilde{\epsilon}}$. Therefore, in step 2 it remains to solve the maximisation in Eq. (3.32). This summarises the basic idea of the numerical security proof method.
However, so far we have ignored numerical errors inherent to computer representations of analytical quantities. So, it is not possible to find elements that are completely in $\mathcal{S}_\infty$. Let us denote the computer representations of Γ_i and γ_i by $\tilde{\Gamma}_i$ and $\tilde{\gamma}_i$. The authors in [110] construct a relaxed set

$$\tilde{\mathcal{S}}^{\epsilon'}_\infty := \{\rho \in \mathcal{D}(\mathcal{H}) : \ \forall i, \ |\text{Tr}\left[\tilde{\Gamma}_i\right] - \tilde{\gamma}_i| \leqslant \epsilon'\}, \tag{3.33}$$

where ϵ' is some small quantity that upper-bounds the constraint violations, that contains $\mathcal{S}_\infty$ and derive a relaxed lower bound,

$$\begin{aligned} \alpha \geqslant \beta_{\tilde{\epsilon},\epsilon'} :=& f_{\tilde{\epsilon}}(\rho_{\text{Step 1}}) - \text{Tr}\left[\rho^\top_{\text{Step 1}} \nabla f_{\tilde{\epsilon}}(\rho_{\text{Step 1}})\right] \\ &+ \max_{(\vec{y},\vec{z}) \in \tilde{\mathcal{S}}^{*,\tilde{\epsilon}}_\infty(\rho_{\text{Step 1}})} \left(\vec{\tilde{\gamma}} \cdot \vec{y} - \epsilon' \sum_{i=0}^{M} z_i \right) - \zeta_{\tilde{\epsilon}}, \end{aligned} \tag{3.34}$$

where

$$\begin{aligned} &\tilde{\mathcal{S}}^{*,\tilde{\epsilon}}_\infty(\rho_{\text{Step 1}}) \\ &:= \left\{ (\vec{y},\vec{z}) \in (\mathbb{R}^{M+1}, \mathbb{R}^{M+1}) : \ -\vec{z} \leqslant \vec{y} \leqslant \vec{z}, \ \sum_{i=0}^{M} y_i \tilde{\Gamma}_i^\top \leqslant \nabla f_{\tilde{\epsilon}}(\rho_{\text{Step 1}}) \right\}. \end{aligned} \tag{3.35}$$

It is argued in [110, Section 3.4] that the obtained lower bounds are tight, provided that $\tilde{\epsilon}$ and ϵ' are small and $\rho_{\text{Step 1}}$ is close to the optimum.

3.4.2. DM CV-QKD Optimisation Problem

In the present thesis, we are concerned with continuous-variable QKD protocols and focus on protocols where Bob performs heterodyne detection (see Section 2.4).

However, the technique can easily be adapted to homodyne detection as well (see, for example, 'Protocol 1' in [64]). This subsection follows [64] ('Protocol 2') for the formulation of the optimisation problem. In both cases, Bob measures the first and second moments of the quadrature operators $\hat{q}$ and $\hat{p}$. Based on the measurement outcomes, he can calculate the derived quantities $\hat{n} = \frac{1}{2}\left(\hat{q}^2 + \hat{p}^2 - 1\right)$ and $\hat{d} = \hat{q}^2 - \hat{p}^2$, where $\hat{n}$ is the photon number operator introduced in Section 2.4. We use these measurement results to constrain the bipartite state ρ_{AB} and obtain the following optimisation problem

$$\begin{aligned}
&\min\ D\left(\mathcal{G}(\rho_{AB}) || \mathcal{Z}\left(\mathcal{G}(\rho_{AB})\right)\right) \\
&\text{s.t.} \\
&\qquad \mathrm{Tr}_B\left[\rho_{AB}\right] = \rho_A, \\
&\qquad \mathrm{Tr}\left[\rho_{AB}\right] = 1, \\
&\qquad \mathrm{Tr}\left[\left(|x\rangle\langle x| \otimes \hat{q}\right)\rho_{AB}\right] = p_x \langle \hat{q} \rangle_x, \\
&\qquad \mathrm{Tr}\left[\left(|x\rangle\langle x| \otimes \hat{p}\right)\rho_{AB}\right] = p_x \langle \hat{p} \rangle_x, \\
&\qquad \mathrm{Tr}\left[\left(|x\rangle\langle x| \otimes \hat{n}\right)\rho_{AB}\right] = p_x \langle \hat{n} \rangle_x, \\
&\qquad \mathrm{Tr}\left[\left(|x\rangle\langle x| \otimes \hat{d}\right)\rho_{AB}\right] = p_x \langle \hat{d} \rangle_x, \\
&\qquad \rho_{AB} \geqslant 0,
\end{aligned} \tag{3.36}$$

where $x \in \mathcal{N}_{\mathrm{St}}$, $\rho_A = \sum_{x,x' \in \mathcal{N}_{\mathrm{St}}} \sqrt{p_x p_{x'}} \langle \phi_x | \phi_{x'} \rangle |x\rangle\langle x|_A$ and $\langle \hat{q} \rangle_x$, $\langle \hat{p} \rangle_x$, $\langle \hat{n} \rangle_x$ and $\langle \hat{d} \rangle_x$ are the expected values of Bob's measurement operators for the conditional state ρ_B^x. It remains to specify the maps $\mathcal{G}$ and $\mathcal{Z}$ occurring in the objective function. We describe the postprocessing maps in terms of Kraus operators, $\mathcal{G}(\rho) = K \rho K^\dagger$. In case of reverse reconciliation, we use the following Kraus operator

$$K = \sum_{z \in \mathcal{N}_{\mathrm{St}}} |z\rangle_R \otimes \mathbb{1}_A \otimes \left(\sqrt{R_B^z}\right)_B, \tag{3.37}$$

where R is a classical register. The operators R_B^z coarse-grain Bob's heterodyne measurement results to regions in the phase space that are associated with the key map. The so-called region operators are defined as

$$R_B^z := \frac{1}{\pi} \int_{\Delta_r}^{\infty} \int_{\frac{2j-1}{N_{\mathrm{St}}}\pi}^{\frac{2j+1}{N_{\mathrm{St}}}\pi} r |re^{i\phi}\rangle\langle re^{i\phi}|\, d\phi\, dr, \tag{3.38}$$

for $z \in \mathcal{N}_{\mathrm{St}}$, where Δ_r denotes the (radial) postselection parameter. They arise from integrating the POVM elements for heterodyne detection from Eq. (2.24) over wedge-shaped regions in phase space. The pinching quantum channel $\mathcal{Z}$ is defined as

$$\mathcal{Z}(\rho) = \sum_{j \in \mathcal{N}_{\mathrm{St}}} \left(|j\rangle\langle j|_R \otimes \mathbb{1}_{AB}\right) \rho \left(|j\rangle\langle j|_R \otimes \mathbb{1}_{AB}\right). \tag{3.39}$$

Note that this description already uses the simplified postprocessing map. For a detailed derivation, we refer interested readers to [64, Appendix A].

Photon-number cutoff assumption

The optimisation in Eq. (3.23) involves Alice's and Bob's bipartite states $\rho_{AB} \in \mathcal{S}_\infty$. Therefore, the dimension of the optimisation problem depends on the dimension of Alice's and Bob's Hilbert space. In the present thesis, we are concerned with continuous-variable protocols. While the dimension of Alice's system is determined by the number of different signal states she prepares, so in particular finite, the dimension of Bob's Hilbert space is infinite and so is the dimension of Alice's and Bob's bipartite system. However, as we want to employ computers to calculate secure key rates, we require a finite-dimensional description of the problem. Motivated by the Poissonian distribution of the photon number in coherent states, one can argue that high photon-number states are unlikely to be populated. This leads to the photon-number cutoff assumption, which imposes that Bob's system is sufficiently well described by a finite-dimensional Hilbert space $\mathcal{H}_B = \text{span}\{|0\rangle, ..., |n_c\rangle\}$, where $n_c \in \mathbb{N}$ s the so-called photon cutoff number. Following the photon-number cutoff assumption, we replace ρ_B by $\Pi^{n_c}\rho_B\Pi^{n_c}$, where $\Pi^{n_c} := \sum_{n=0}^{n_c} |n\rangle\langle n|$ and adapt all operators on Bob's side in the same way. However, for a valid security proof, this assumption needs to be removed. This is done rigorously by the dimension reduction method, which we are going to discuss in the next section.

3.4.3. Dimension Reduction Method

In this section, we review the dimension reduction method first presented in [105]. The idea is to rigorously treat the photon-number cutoff by connecting the original infinite-dimensional optimisation problem to a suitably chosen finite-dimensional optimisation problem that is numerically evaluated under some reasonable requirements on the objective function f. The method gives a tight lower bound on the infinite-dimensional optimisation problem based on the result of the finite-dimensional optimisation problem and a penalty term, that takes the cutoff into account.

We choose $\mathcal{H}_{\text{fin}}$ to be any finite-dimensional subspace of the original infinite-dimensional Hilbert space $\mathcal{H}_\infty := \mathcal{H}_A \otimes \mathcal{H}_B$. Let Π be the corresponding projection onto $\mathcal{H}_{\text{fin}}$. Furthermore, choose $\mathcal{S}_{\text{fin}}$ to be a nonempty convex subset of $\mathcal{D}_{\leqslant}(\mathcal{H}_{\text{fin}})$ such that $\Pi\mathcal{S}_\infty\Pi \subseteq \mathcal{S}_{\text{fin}}$. Our goal is to relate the infinite-dimensional optimisation

$$\min_{\rho \in \mathcal{S}_\infty} f(\rho) \tag{3.40}$$

to the finite-dimensional problem

$$\min_{\rho \in \mathcal{S}_{\text{fin}}} f(\rho). \tag{3.41}$$

Let $\rho_\infty \in \mathcal{S}_\infty$ be the density operator achieving the optimum in Eq. (3.40). Note that for continuous f and compact $\mathcal{S}_\infty$ such a ρ_∞ exists. Furthermore, let $\rho_{\text{fin}} \in \mathcal{S}_{\text{fin}}$ be the density matrix achieving the optimum in the finite-dimensional optimisation, given in Eq. (3.41) and introduce $\rho_\Pi := \Pi\rho_\infty\Pi$, which is the projection of the optimum of the infinite-dimensional optimisation problem onto the finite-dimensional subspace. The relation between the optimal values of the optimisations in Eq. (3.40) and Eq. (3.41) is established via two inequalities. By construction ρ_Π lies within the finite-dimensional feasible set $\mathcal{S}_{\text{fin}}$. Since ρ_{fin} attains the minimum of f in $\mathcal{S}_{\text{fin}}$, we have

$$f(\rho_\Pi) \geqslant f(\rho_{\text{fin}}). \tag{3.42}$$

For the second inequality, we require f to satisfy a certain condition, which turns out to be satisfied by the objective function of the key rate finding problem.

Definition 3.4.2: Uniformly Close to Decreasing under Projection

Let $\mathcal{H}$ be a separable Hilbert space. A function $f : \mathcal{D}_{\leqslant}(\mathcal{H}) \to \mathbb{R}$ is called ***uniformly close to decreasing under projection (UCDUP)*** *on a set $\mathcal{S} \subseteq \mathcal{D}_{\leqslant}(\mathcal{H})$ with correction term $\Delta(w)$ if*

$$\forall \rho \in \mathcal{S} : \; F(\rho, \Pi\rho\Pi) \geqslant \operatorname{Tr}[\rho] - w \Rightarrow f(\Pi\rho\Pi) - f(\rho) \leqslant \Delta(w), \tag{3.43}$$

where Π is a projection onto a subspace of $\mathcal{H}$.

Note that UCDUP is a slightly weaker condition than uniform continuity.
Requiring f to be UCDUP on $\mathcal{S}_\infty$, Ref. [105] shows that

$$f(\rho_\Pi) - \Delta(w) \leqslant f(\rho_\infty) \tag{3.44}$$

holds. Combining inequalities (3.42) and (3.44) leads to the main theorem of the dimension reduction method ([105, Theorem 1]) where we used the improved correction term from [106, Theorem 2]. For more details, we refer the interested reader to the original paper.

Theorem 3.4.3: Dimension Reduction

Let $\mathcal{H}$ be a separable Hilbert space and Π the projection onto some finite-dimensional subspace $\mathcal{H}_{fin}$ of $\mathcal{H}$ as well as $\Pi^{\perp}$ the projection onto $(\mathcal{H}_{fin})^{\perp}$. Let $\rho_{\infty} \in \mathcal{D}_{\leqslant}(\mathcal{H})$ and $\rho_{fin} \in \mathcal{D}_{\leqslant}(\mathcal{H}_{fin})$.
If $f : \mathcal{D}_{\leqslant}(\mathcal{H}) \to \mathbb{R}$ is uniformly close to decreasing under projection, then

$$f(\rho_{fin}) - \Delta(w) \leqslant f(\rho_{\infty}),$$

where

$$\Delta(w) := \sqrt{w}\log_2(|Z|) + (1+\sqrt{w})h\left(\frac{\sqrt{w}}{1+\sqrt{w}}\right). \tag{3.45}$$

Here, $|Z|$ denotes the dimension of the key map and $h(\cdot)$ is the binary entropy.

The size of the correction term $\Delta(w)$ is a function of the weight w which depends on the size of the chosen finite-dimensional Hilbert space $\mathcal{H}_{\text{fin}}$, hence on the chosen cutoff space $\mathcal{H}_{n_c}$. Hence, we are looking for a subspace where we expect the weight to be small. The authors in [105] show that for the present DM CV-QKD key rate optimisation problem, a particularly good choice is a subspace spanned by displaced Fock states $|n_\gamma\rangle = \hat{D}(\gamma)|n\rangle$, where the displacement is linked to the states that Alice prepares. The projection for the i^{th} state is then $\Pi := \sum_{n=0}^{n_c} |n_{\beta_i}\rangle\langle n_{\beta_i}|$, where $\{\beta_i\}_{i\in\mathcal{N}_{\text{St}}}$ is chosen according to $\sqrt{\eta}\alpha_i$, where $i \in \mathcal{N}_{\text{St}}$.

Next, we give an interpretation of the quantity w and a brief motivation for naming it weight. Using Winter's Gentle Measurement Lemma [111], the UCDUP condition can be written as

$$F(\rho, \Pi\rho\Pi) = \text{Tr}\left[\rho\Pi\right] \geqslant \text{Tr}\left[\rho\right] - w \tag{3.46}$$

since Π is a projection. This implies

$$\text{Tr}\left[(\mathbb{1} - \Pi)\rho\right] \leqslant w, \tag{3.47}$$

so w is an upper bound for the weight of the state ρ outside the finite-dimensional space $\mathcal{H}_{\text{fin}}$.

It remains to state the finite-dimensional optimisation problem we have to solve. For a derivation, we refer the interested reader to [105].

$$
\begin{aligned}
&\min\ f(\rho_{\text{fin}}) \\
&\text{s.t.} \\
&\quad ||\text{Tr}_B\left[\rho_{\text{fin}}\right] - \rho_A||_1 \leqslant 2\sqrt{w} \\
&\quad 1 - w \leqslant \text{Tr}\left[\rho_{\text{fin}}\right] \leqslant 1, \\
&\quad \text{Tr}\left[\left(|x\rangle\langle x| \otimes \hat{n}_{\beta_x}\right)\rho_{\text{fin}}\right] \leqslant p_x\langle\hat{n}_{\beta_x}\rangle, \\
&\quad \text{Tr}\left[\left(|x\rangle\langle x| \otimes \hat{n}^2_{\beta_x}\right)\rho_{\text{fin}}\right] \leqslant p_x\langle\hat{n}^2_{\beta_x}\rangle, \\
&\quad \rho_{\text{fin}} \in \text{Pos}\left(\mathcal{H}_{\text{fin}}\right),
\end{aligned}
\tag{3.48}
$$

where $x \in \mathcal{N}_{\text{St}}$, $\rho_A = \sum_{x,x' \in \mathcal{N}_{\text{St}}} \sqrt{p_x p_{x'}}\langle\phi_x|\phi_{x'}\rangle\,|x\rangle\langle x|_A$ and $\langle\hat{n}_{\beta_x}\rangle$ and $\langle\hat{n}^2_{\beta_x}\rangle$ are the expected values of the displaced number operator and the squared displaced number operator, respectively.

3.4.4. Trusted Detector Noise and Nonideal Detectors

So far, we assumed that Bob's detectors have 100% detection efficiency and that all observed noise is excess noise, hence under Eve's control. In realistic implementations detectors are not perfect, but have detection efficiency $\eta_d \in (0, 1)$ and electronic noise $\nu_{\text{el}} > 0$. If parts of the noise can be traced back to Bob's detectors, one might decide to trust this part of the total noise, as the detectors are located in Bob's lab. Hence, it is reasonable to assume the electronic noise is not under Eve's control. The authors in [63] generalise the present method to this more realistic scenario. We review their ideas and the necessary changes briefly.

The noisy, nonideal heterodyne detector is described, following the detector model by Lodewyck [67]. The idea is to introduce two additional beamsplitters with transmittances η_1 and η_2 matching to the efficiencies of the real homodyne detectors that are placed after the initial $50:50$ beam splitter that divides the input signal into two equal shares. At each of the additional beamsplitters, signal is mixed with a thermal state with mean photon number $\overline{n}_i = \frac{\nu_i}{2(1-\eta_i)}$, $i \in \{1, 2\}$ such that the matching electronic noise is added to the outputs. Finally, two ideal homodyne detectors measure the resulting states. A sketch of the situation can be found in Figure 3.2. For simplicity, we assume it what follows that $\eta_1 = \eta_2 =: \eta_d$ and $\nu_1 = \nu_2 =: \nu_{\text{el}}$.

As the detector model is different now, several quantities change. First, we need to replace the ideal detector POVM elements $E_y = \frac{1}{\pi}|y\rangle\langle y|$ by

$$
G_y = \frac{1}{\eta_d \pi}\hat{D}\left(\frac{y}{\sqrt{\eta_d}}\right)\rho_{\text{th}}\left(\frac{1 - \eta_d + \nu_{\text{el}}}{\eta_d}\right)\hat{D}^\dagger\left(\frac{y}{\sqrt{\eta_d}}\right), \tag{3.49}
$$

as derived in [63]. This leads to modified region operators $R^z_B = \int_{y \in \mathcal{A}_z} G_y\ d^2y$, where $\mathcal{A}_z$ denotes the region in phase space the operator corresponds to. The map

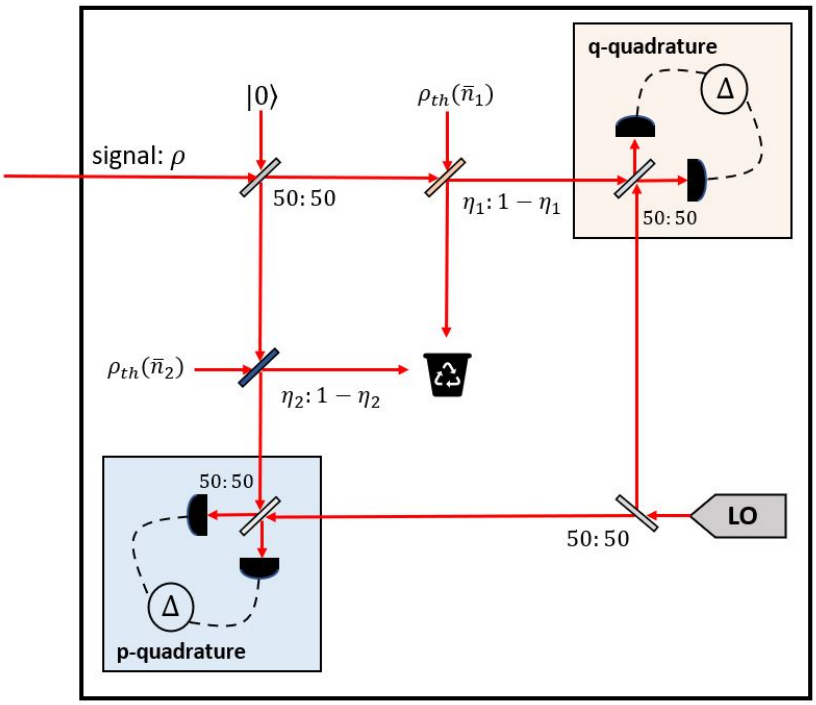

Figure 3.2.: Schematic of the trusted, nonideal detector model. The incident signal is mixed with the vacuum state at a 50:50 beamsplitter. The output signals pass another beamsplitter with transmission η_1 and η_1, where they are mixed with thermal states. Finally, the q and q quadratures are measured by ideal homodyne detectors.

$\mathcal{G}$, hence the objective function f, change correspondingly. Furthermore, the first- and second-moment observables become

$$\begin{aligned}
\hat{F}_Q &= \int_{\mathbb{C}} \frac{y^* + y}{\sqrt{2}} G_y \; d^2y, \\
\hat{F}_P &= \int_{\mathbb{C}} \frac{i\,(y^* - y)}{\sqrt{2}} G_y \; d^2y, \\
\hat{S}_Q &= \int_{\mathbb{C}} \frac{(y^* + y)^2}{2} G_y \; d^2y, \\
\hat{S}_P &= \int_{\mathbb{C}} \frac{-(y^* - y)^2}{2} G_y \; d^2y.
\end{aligned} \tag{3.50}$$

This leads to the following optimisation problem for trusted, nonideal detectors

$$\begin{aligned}
&\min \; f^{\text{noisy}}(\rho) \\
&\text{s.t.} \\
&\qquad \mathrm{Tr}_B\left[\rho_{AB}\right] = \rho_A, \\
&\qquad \mathrm{Tr}\left[\rho_{AB}\right] = 1, \\
&\qquad \mathrm{Tr}\left[\left(|x\rangle\langle x| \otimes \hat{F}_Q\right) \rho_{AB}\right] = p_x \langle \hat{F}_Q \rangle_x, \\
&\qquad \mathrm{Tr}\left[\left(|x\rangle\langle x| \otimes \hat{F}_P\right) \rho_{AB}\right] = p_x \langle \hat{F}_P \rangle_x, \\
&\qquad \mathrm{Tr}\left[\left(|x\rangle\langle x| \otimes \hat{S}_Q\right) \rho_{AB}\right] = p_x \langle \hat{S}_Q \rangle_x, \\
&\qquad \mathrm{Tr}\left[\left(|x\rangle\langle x| \otimes \hat{S}_P\right) \rho_{AB}\right] = p_x \langle \hat{S}_P \rangle_x, \\
&\qquad \rho_{AB} \geqslant 0,
\end{aligned} \tag{3.51}$$

where, again, $x \in \mathcal{N}_{\text{St}}$, $\rho_A = \sum_{x,x' \in \mathcal{N}_{\text{St}}} \sqrt{p_x p_{x'}} \langle \phi_x | \phi_{x'} \rangle \, |x\rangle\langle x|_A$ and $\langle \hat{n}_{\beta_x} \rangle$ and $\langle \hat{n}^2_{\beta_x} \rangle$ are the expected values of the displaced number operator and the squared displaced number operator, respectively.

Similarly, as we derived (3.51) from (3.36), we can modify the optimisation problem arising from the dimension reduction method (3.48). We give only a brief review, following [105, Section VI, D and Appendix D], for more details, we refer the interested reader to the original paper. It turns out that although Bob's observables $\left[\hat{n}_{\sqrt{\eta_d}\beta_x}\right]'$ and $\left[\hat{n}^2_{\sqrt{\eta_d}\beta_x}\right]$ in the noisy, trusted detector case are displaced by $\sqrt{\eta_d}\beta_x$, compared to only β_x in the ideal, untrusted detector case, $\hat{n}_{\beta_x}$ and $\hat{n}^2_{\beta_x}$, the new observables are related to the old ones by linear combinations. This means that based on his measurement results, Bob can recreate the expected values of the ideal observables. Let us denote these 'effective' expected values by $\langle \hat{n} \rangle^{\text{eff}}$ and

$\langle \hat{n}^2 \rangle^{\text{eff}}$. Then, as shown in [106, Section 5.3], the following relations hold

$$\langle \hat{n}_{\beta_x} \rangle^{\text{eff}} = \frac{\left\langle \left[\hat{n}_{\sqrt{\eta_d}\beta_x} \right]' \right\rangle - \nu_{\text{el}}}{\eta_d} \tag{3.52}$$

$$\langle \hat{n}^2_{\beta_x} \rangle^{\text{eff}} = \frac{1}{\eta_d^2} \left(\left\langle \left[\hat{n}^2_{\sqrt{\eta_d}\beta_x} \right]' \right\rangle - 2\nu_{\text{el}}^2 - \nu_{\text{el}} - (4\nu_{\text{el}} + 1 - \eta_d) \left(\left\langle \left[\hat{n}_{\sqrt{\eta_d}\beta_x} \right]' \right\rangle - \nu_{\text{el}} \right) \right), \tag{3.53}$$

for $x \in \mathcal{N}_{\text{St}}$. Therefore, if Bob calculates these effective quantities based on his measured results, only the objective function of the optimisation problem changes due to different POVM elements for noisy, trusted detectors, while the set of feasible states remains unchanged. The semidefinite program reads,

$$\begin{aligned} \min \; & f^{\text{noisy}}(\rho_{\text{fin}}) \\ \text{s.t.} \; & \\ & ||\text{Tr}_B \left[\rho_{\text{fin}}\right] - \rho_A||_1 \leqslant 2\sqrt{w} \\ & 1 - w \leqslant \text{Tr}\left[\rho_{\text{fin}}\right] \leqslant 1, \\ & \text{Tr}\left[\left(|x\rangle\langle x| \otimes \hat{n}_{\beta_x}\right) \rho_{\text{fin}}\right] \leqslant p_x \langle \hat{n}_{\beta_x} \rangle^{\text{eff}}, \\ & \text{Tr}\left[\left(|x\rangle\langle x| \otimes \hat{n}^2_{\beta_x}\right) \rho_{\text{fin}}\right] \leqslant p_x \langle \hat{n}^2_{\beta_x} \rangle^{\text{eff}}, \\ & \rho_{\text{fin}} \in \text{Pos}\left(\mathcal{H}_{\text{fin}}\right), \end{aligned} \tag{3.54}$$

where $x \in \mathcal{N}_{\text{St}}$, $\rho_A = \sum_{x,x' \in \mathcal{N}_{\text{St}}} \sqrt{p_x p_{x'}} \langle \phi_x | \phi_{x'} \rangle |x\rangle\langle x|_A$ and $\langle \hat{n}_{\beta_x} \rangle^{\text{eff}}$ and $\langle \hat{n}^2_{\beta_x} \rangle^{\text{eff}}$ are the effective expected values of the displaced number operator and the squared displaced number operator, as described above.

4. Finite-Size Security Analysis of DM CV-QKD Protocols

After having set the stage in the previous chapter, we are now almost ready to state the main result of this work. Large parts of this chapter, in particular Sections 4.3 and 4.4, are taken from the draft of our paper that is currently in preparation [55]. We begin this section with a brief overview of the current state of DM CV-QKD security proofs, followed by a discussion of so-called energy tests. Then, we introduce the protocol we analysed and finally present the finite-size security proof for DM CV-QKD protocols against i.i.d. collective attacks.

4.1. State of Security Proofs

We begin by reviewing the current state of security proofs for DM CV-QKD protocols. Although practically simpler, security proofs for discretely modulated CV-QKD protocols have been lagging behind proofs for protocols with Gaussian modulation for a long time, even though it is known that a practically useful security analysis needs to take the influence of finite constellations into account [53].

4.1.1. Asymptotic Security Proofs

Early asymptotic security proofs for DM CV-QKD protocols against collective attacks [47, 98] were restricted to idealised cases like channels without noise, but already allowed some flexibility regarding the number of different signal states used. Later, the first proofs for the more general case of noisy channels emerged [114], but only applied for binary modulation and used homodyne detection. Binary modulation schemes, however, are known to be limited, even for short distances [46, 88]. The proof idea from [114] was extended to three states in [12]. However, the attempt does not seem to be generalisable to an arbitrary number of states.
This leads us to more general security proofs against collective attacks in the asymptotic limit for lossy, noisy channels. We begin with analytical attempts. The proof by Denys et.al. [22] bounds the asymptotic secure key rate by analytically solving a semidefinite program for arbitrary modulation schemes. While the secure key rates for large constellations come close to key rates known from

Gaussian modulation but are loose for a low number of signal states. Furthermore, this proof approach does not allow postselection. Another security proof by Kaur et.al. [58] approximates an isotropic Gaussian probability distribution by finite-size constellations and applies entropic continuity bounds to quantify how well approximated the Gaussian modulation is by the finite constellation. By construction, this security proof is not suitable to determine secure key rates for small constellations.
Finally, we come to numerical security proofs against collective attacks in the asymptotic limit, which are more flexible than analytical approaches at the cost of high computational complexity. Ghorai et.al. [38] use Bob's measurements to minimise over all density matrices that are compatible with the covariance matrix determined based on Bob's results. The optimality of Gaussian attacks then gives a bound on the Holevo quantity, hence the secure key rate. The occurring semidefinite program has a linear objective function and is solved numerically. In contrast, the numerical security proof framework [19, 110] reformulates the Devetak-Winter formula in terms of the quantum relative entropy and formulates a semidefinite program constrained by Bob's observations and additional requirements on the density matrix arising from the source-replacement scheme with a nonlinear objective function. This SDP is solved in a two-step process, which results in a tight lower bound on the secure key rate. The framework has been applied to DM CV-QKD protocols [63, 64] both for homodyne and heterodyne detection and for untrusted, ideal as well as for trusted, nonideal detectors. While both mentioned numerical approaches initially relied on a photon-number cutoff assumption to handle infinite-dimensional systems, this was removed by [105] for the numerical framework in [19, 64, 110]. While both numerical frameworks allow postselection, the key rates obtained by [64] are clearly higher than those by [38]. Both attempts are in principle generalisable to a higher number of signal states (see, for example, [56, 57]) and also allow for different modulation patterns. However, with a growing number of signal states, the computational complexity increases rapidly, making the problems numerically very challenging.

4.1.2. Finite-Size Security Proofs

Next, we turn to security proofs in the practically relevant finite-size regime. One of the first finite-size security proofs for DM CV-QKD protocols is by Furrer et.al. [34] and analyses a protocol employing two-mode squeezed vacuum states and homodyne detection. The authors provide security statements both for collective and general attacks by exploiting the fact that in the case Alice and Bob both measured the same quadrature, Eve's knowledge about the complementary quadrature is small. This allows them to lower-bound the smooth min-entropy quantifying Eve's knowledge about Alice's outcome. Another approach by Fur-

rer [33] exploits the finite detection range of real detectors, adds an additional test measurement and employs an entropic uncertainty relation to obtain a lower bound on the secure key rate. Both attempts work only for a special protocol and give nonzero secure key rates only for very low transmission distances.

Papanastasiou et.al. [77] prove the composable finite-size security against Gaussian collective attacks for a protocol using phase-encoded coherent states and heterodyne detection. They allow for trusted thermal noise but no postselection and they need to introduce a photon number cutoff to make the problem computationally feasible. In the paper, they treat only the case of two and three signal states, which seems to be already computationally demanding. Therefore, it is not clear if this method can be used easily for higher constellations.

Matsuura et.al. [69] prove the general security of a binary phase-modulated CV-QKD protocol detection by estimating the fidelity of an optical pulse to a coherent state, where they use heterodyne detection for testing and homodyne detection for key generation rounds. Their analysis does not include trusted detector noise or postselection and does not seem to be generalisable to arbitrary constellations.

Another very recent approach by Lupo et.al. [68] builds up on the numerical framework by Ghorai et.al and proves composable security against i.i.d. collective attacks in the finite-size regime. The authors exploit the finite detection range of realistic heterodyne detectors to bound the maximal photon number of incoming signals. While they take the finite resolution of real detectors into account, their measurement devices have unit detection efficiency and they do not consider trusted noise or postselection. Similarly to [38] they solve linear SDPs to bound entries of the covariance matrix to obtain bounds on the Holevo information, hence on the secure key rate. They obtain secure key rates for a protocol with quaternary modulation that for a large number of signal states N converge against the asymptotic key rates reported by [22], which are known to be loose for a low number of states.

4.1.3. Résumé

This brief overview shows that security proofs for DM CV-QKD protocols are subject to active research. While there has been much progress over the last couple of years, in particular for proofs in the asymptotic limit, there is still no general finite-size security proof for general modulation patterns, including postselection and realistic detection devices available. In the asymptotic regime, the numerical framework [19, 64, 110] provides a very flexible tool to calculate tight secure key rates. This motivates us to extend this framework to the finite-size regime.

4.2. Energy Tests

To illustrate the need for one of the main contributions of this work, imagine the following situation. Alice sends $N < \infty$ quantum signals with low energy $\mathcal{E} = \frac{1}{N}$ to Bob via a quantum channel, while Eve might interfere with the signals. Bob receives the quantum states and decides to perform testing on $k \ll N$ randomly selected rounds. Now, assume Eve has replaced one of the signals by a state with energy $\mathcal{E} \gg \frac{1}{N}$. In most of the cases, Bob will test only those rounds, where Eve has not interfered with the signal and might conclude that the average energy of the states he receives is $\mathcal{E} = \frac{1}{N}$, while indeed the average energy is much higher. Thus, he underestimates both the average and the maximum energy horribly. Note that the energy of a harmonic oscillator (which is how we modelled laser pulses) and the photon number are related via $\mathcal{E}_n = \hbar\omega n$, hence underestimating the maximum energy is equivalent to underestimating the maximal photon number. This was not a problem for security proofs in the asymptotic limit as there the number of rounds used for testing was infinite as well, but turns out to be a critical aspect for finite-size security proofs, in particular for numerical approaches, which rely on having a maximal photon number. This situation highlights, why it requires some statistical statement about the maximal energy in the received pulses. Such statistical tests, aiming to estimate or bound the maximum energy (or, equivalently, the maximum number of photons) in a sequence of pulses, are called energy tests.

A couple of energy tests are known in the literature. The energy test by Renner and Cirac, presented in [86], uses the permutation invariance of the quantum output of most QKD protocols. The authors propose testing on a small subset of all rounds. Given the test was successful, except with some small probability, most of the remaining rounds live in a finite-dimensional Hilbert space. However, with this approach, we are left with some possibly infinite-dimensional systems. Unfortunately, it seems to be not possible to remove these infinite-dimensional systems later on during the security proof in the lack of a chain rule for smooth-min entropies removing infinite-dimensional registers. Hence, this energy test is not applicable in our case.

In contrast, another energy test by Leverrier, introduced in [62], performs testing on a small subset but results in a statistical energy bound on all remaining rounds. However, this energy test requires a very strong phase-space rotation symmetry, which is not satisfied by our protocol. Applying an additional symmetrisation step to our protocol, performing the test and undoing the symmetrisation afterwards again is not possible, as this artificial symmetrisation basically mixes all rounds with each other. Then, the test traces out $k \ll N$ rounds, hence 'destroys' some information that is needed to recreate $N - k$ non-symmetrised rounds. Besides that, even if it was possible, we expect the whole artificial symmetrisation procedure including performing its reverse operation, would require a large amount of

coordination between Alice and Bob, hence communication over the classical channel. This would lead to large overhead and make the protocol slow and impractical and potentially leaks information to Eve, lowering the key rate.
The energy test by Furrer [33] requires an additional beamsplitter which is used to extract a small fraction of every signal. This small part of the signal is then measured via a heterodyne detector. Besides the fact that an additional beamsplitter introduces additional losses, performing this energy test requires supplementary hardware like a second measurement setup and is therefore experimentally less favourable and less practical.
This motivates the development of an alternative energy test that does (a) not require additional hardware, (b) does not require high symmetry and (c) makes a probabilistic statement about all remaining systems after the testing.

4.3. General DM CV-QKD Protocol

In what follows, we describe the general discrete modulated CV-QKD protocol we consider in the present work, where $N_{\mathrm{St}} \in \mathbb{N}$ denotes the number of distinct signal states used in the protocol and Greek letters put in bra-ket notation refer to coherent states. We present the prepare-and-measure version of the protocol. Note that thanks to the source-replacement scheme [21, 28] this is equivalent to the entanglement-based version of the protocol and we are free to switch between both versions in case this eases the security analysis.

1 **State preparation**— Alice prepares one out of N_{St} possible coherent states $|\alpha\rangle$ with $\alpha \in \{\alpha_0, ..., \alpha_{N_{St}-1}\}$ in her lab with equal probability and sends it to Bob using the quantum channel. Alice associates every state with a symbol and keeps track of what she sent in a private register.

2 **Measurement**— Bob receives the signal and performs a heterodyne measurement to determine the quadratures of the received signal. This can be described by a positive operator-valued measure $\{E_\gamma = \frac{1}{\pi}|\gamma\rangle\langle\gamma| \ : \ \gamma \in \mathbb{C}\}$. After applying this POVM, Bob holds a complex number $y_k \in \mathbb{C}$ that is stored in his private register.

Steps 1 and 2 are repeated N times.

3 **Energy test**— After completing the state preparation and measurement phases, Bob performs an energy test on $k_{\mathrm{T}} \ll N$ rounds by using the measurement results related to these rounds. If for most of the tested signals, the heterodyne detection gave small measurement results, the test passes. This means that most of the weight of the transmitted signals lies within

a finite-dimensional Hilbert space, except with some small probability ϵ_{ET}. Otherwise, Alice and Bob abort the protocol. For details about the energy test, we refer to Section 4.2.

4 **Acceptance test** — If the energy test was successful, Bob discloses the data from the rounds he used for the energy test via the classical channel. This information is used by Alice and Bob to determine statistical estimators for their observables. If they lie within the acceptance set, Alice and Bob proceed, otherwise, they abort the protocol.

5 **Key map**— Bob performs a reverse reconciliation key map on the remaining $n := N - k_T$ rounds to determine the raw key string $\tilde{z}$. For this purpose, Bob's measurement outcomes are discretised to an element in the set $\{0, ..., N_{\mathrm{St}} - 1, \perp\}$, where symbols mapped to $\perp$ are discarded. By choosing a key map that discards results in certain regions of the phase space, Bob can perform postselection as described in [64].

6 **Error correction**— Alice and Bob publicly communicate over the classical channel to reconcile their raw keys $\tilde{x}$ and $\tilde{z}$. After the error correction phase, Alice and Bob share a common string except with a small probability ϵ_{EC}.

7 **Privacy amplification**— Finally, they apply a two-universal hash-function to their common string. Except with small probability ϵ_{PA}, in the end, Alice and Bob hold a secret key.

We note that step 4 is often called **parameter estimation**. However, we want to emphasise that in the finite-size regime we can never estimate any properties of the 'real' density matrix, but only determine some statistical quantities based on our observations. First, we define a so-called acceptance set, which can be imagined as a list of accepted observations. Based on our measurement results, we partition the set of all density matrices into two disjoint sets. The first one contains density matrices that lead to accepted statistics with probability less than ϵ_{AT}, i.e., the protocol aborts with high probability for those states. The second set is the complement of the first one and in what follows, we can restrict our security considerations to states lying in the latter set, called the 'feasible set'. Based on this construction, we restrict our analysis to states that are ϵ-secure with $\epsilon < \epsilon_{\mathrm{AT}}$. For a more detailed discussion of the idea of acceptance sets, we refer the reader to [36, Section II.B], where this notion is discussed for discrete-variable QKD.
While we present our security proof approach for an arbitrary number N_{St} of signal states, we demonstrate our numerical results for a quadrature phase-shift keying protocol with $N_{St} = 4$, where all four states are arranged equidistantly on a circle with radius $|\alpha|$, $\alpha_k \in \{|\alpha|, i|\alpha|, -|\alpha|, -i|\alpha|\}$, where i denotes the complex unit. In this case, the key map in step 5.) of the protocol description reads as follows

$$\tilde{z}_i = \begin{cases} 0, \text{ if } \frac{7\pi}{4} \leqslant \arg(y_i) < \frac{1\pi}{4} & \wedge\ |y_j| \geqslant \Delta_r, \\ 1, \text{ if } \frac{1\pi}{4} \leqslant \arg(y_i) < \frac{3\pi}{4} & \wedge\ |y_j| \geqslant \Delta_r, \\ 2, \text{ if } \frac{3\pi}{4} \leqslant \arg(y_i) < \frac{5\pi}{4} & \wedge\ |y_i| \geqslant \Delta_r, \\ 3, \text{ if } \frac{5\pi}{4} \leqslant \arg(y_i) < \frac{7\pi}{4} & \wedge\ |y_i| \geqslant \Delta_r, \\ \perp \text{ otherwise,} \end{cases} \tag{4.1}$$

where $\Delta_r \geqslant 0$ is the radial postselection parameter and $\arg(z)$ denotes the polar angle between the vector representing z and the positive q axis. We note that our method, of course, can take other postselection patterns into account as well.

4.4. Finite-Size Security Proof

4.4.1. High-level outline of the security proof

Before we go into the details of our security proof, we aim to give the big picture of our approach. For our proof, we assume i.i.d. collective attacks, this means Eve prepares a fresh ancilla state to interact with each round of the protocol in an identical manner and then stores them in a quantum memory. Once Alice and Bob have finally executed their protocol, she measures her quantum memory, containing all ancillae, collectively. In particular, this means that there are no correlations between different rounds and that we can treat all rounds equally.
Since Alice's quantum signals went through the quantum channel, which is under Eve's control, we do not know a-priori if there is a maximum photon number in the states Bob receives. Thus, we have to work with infinite-dimensional Hilbert spaces. To bound the maximum dimension, we perform an energy test (Theorem 4.4.1) by choosing a cutoff number n_c, a weight w and a testing parameter β_{test}. If the test passes, except with some small probability ϵ_{ET}, most of the weight of the sent states lies within the chosen cutoff space $\mathcal{H}^{n_c}$. In this case, we are dealing with bounded observables and we can use Hoeffding's inequality to perform a statistical test in the acceptance testing step (Theorem 4.4.2) and obtain bounds on the expectations. Mathematically, we distinguish between two scenarios for each of both tests. Either the test fails, meaning that with high probability the observed statistical quantity does not correspond to a state in our acceptance set. Otherwise, the test passes. Hence, after performing both the energy test and the acceptance test, we know that the actual state is $\epsilon_{\mathrm{ET}} + \epsilon_{\mathrm{AT}}$ close to the set we consider in our security analysis. Within Renner's finite-size framework [85], the next step is to handle blockwise post-processing and error correction and to apply the leftover hashing lemma, which tells us that if Alice and Bob apply a randomly chosen hash function from the family of two-universal hash functions, the output is secure as long as it is smaller than Eve's uncertainty about Alice's and Bob's

initial key string. However, Renner assumes finite-dimensional Hilbert spaces, so we cannot apply his results directly (recall that the energy test gave us a bound on Bob's dimension, but Eve created her purification before Bob performed his energy test). To resolve this, we use the leftover hashing lemma against infinite-dimensional side-information ([8, Proposition 21]) to derive our entropic condition on the key length (Lemma B.1.4). It remains to take the effect of classical communication during the error-correction phase into account. Thanks to Lemma B.1.6, we can remove the transcript from the information reconciliation step at the cost of introducing a leakage term even if one of the conditioning systems (Eve's purifying system) is still infinite-dimensional. We then use various properties of the smooth min-entropy to simplify the expression, giving an upper bound on the secure key rate. Following the methodology of [34], we establish the Asymptotic Equipartition Property (AEP) from Renner's thesis [85] and extend it to infinite-dimensional quantum side-information (Corollary B.2.17) [1]. Then, we use the dimension reduction method (Theorem 3.4.3) to obtain a finite-dimensional semidefinite program, which then can be solved by an extension of the numerical framework presented in [19, 110].

4.4.2. Noise Robust Energy Test

As outlined in Section 4.2, one of the crucial tasks when analysing the finite-size security of DM CV-QKD protocols is handling Bob's possible infinite-dimensional quantum states. Since existing energy tests do either require additional hardware, rely on high phase-space rotation symmetries or only make probabilistic statements about most, but not all, systems remaining after the test, we develop our own energy test.
Besides that, we aim for a practically useful energy test, which is an energy test which does not abort almost all the time in realistic, in particular, noisy environments. Therefore, we want our energy test to be noise-robust. Unfortunately, we are not able to perform a 'maximum photon number' or 'photon-cutoff number' measurement directly. Thus, we need to establish a connection between a 'virtual' maximum photon number measurement and the heterodyne measurement that we are actually able to perform by Born's rule. Having sketched the idea of our energy test, we first state our result in the form of a theorem and postpone the proof to Appendix A.
As outlined in the protocol description, after transmitting N rounds of signals, Alice and Bob perform testing on $k_T \ll N$ modes, i.e. Bob carries out heterodyne measurements to determine the quadratures of the chosen rounds. His measure-

[1] We generalize this form of the AEP rather than using the extension of the fully quantum AEP [34] as it applies for all block lengths and is simpler to apply for numerical calculations.

ment results can be used for the following statement.

Theorem 4.4.1: Noise Robust Energy Test

Consider signal states of the form $\rho^{\otimes N}$ *and let* $k_T \in \mathbb{N}$, $k_T \ll N$, *be the number of signals sacrificed for testing. Let* $l_T \in \mathbb{N}$ *be the number of rounds that may not satisfy the testing condition. Denote by* $(Y_1, ..., Y_{k_T})$ *the results of the test measurement. Pick a weight* $w \in [0, 1]$, *a photon cutoff number* n_c *and a testing parameter* $\beta_{test} > 0$. *For ideal detectors define* $r^{\text{ideal}} := \frac{\Gamma(n_c+1,0)}{\Gamma(n_c+1,\beta_{test})}$ *and for trusted, non-ideal detectors* $r^{\text{non-ideal}} := \frac{1}{\Gamma(1,\beta_{test})}$. *Finally, let* $\Pi^{\perp}$ *be the projector onto the complement of the photon cutoff space* $\mathcal{H}^{n_c}$. *Then, for all* ρ *such that* $\mathrm{Tr}\left[\Pi^{\perp}\rho\right] \geqslant w$,

$$Pr\left[\left|\left\{Y_i : \ Y_i < \beta_{test}^2\right\}\right| \leqslant l_T\right] \leqslant \frac{\left(1 - \frac{w}{r}\right)^{k_T - l_T + 1}}{k_T - l_T + 1} =: \epsilon_{ET},$$

where $r \in \{r^{\text{ideal}}, r^{\text{non-ideal}}\}$, *depending on the detector model and where* $\Gamma(n, a)$ *is the upper incomplete gamma function.*

Proof. See Appendix A. □

In other words, the energy test tells us that for all ρ that satisfy $\mathrm{Tr}\left[\Pi^{\perp}\rho\right] \geqslant w$ the energy test will fail except with probability ϵ_{ET}.

Note that the theorem only tells us something in the case the energy test passes. If the energy test fails, we abort the whole protocol and therefore are (trivially) secure. Furthermore, as Alice's lab is assumed to be inaccessible to Eve, the test needs to be performed by Bob only.

After passing the energy test, working in a finite-dimensional Hilbert space allows us to specify the relevant set for our observables. This is the set we restrict our security analysis to (see our discussion in Section 4.3), based on statistical bounds for the observed values of our observables $\bar{X}$. This statistical test replaces the parameter estimation step in asymptotic security analyses.

Theorem 4.4.2: Acceptance Test

Consider k outcomes of an observable X that is bounded by x. Assume the state ρ is i.i.d. and denote the observed average by $\bar{X}$.
Then, the complement to the set that is ϵ_{AT}-filtered by the acceptance test is given by

$$\mathcal{S}^{AT} := \left\{\rho \in \mathcal{D}_{\leqslant}(\mathcal{H}_A \otimes \mathcal{H}_B^{n_c}) : \ \forall X \in \Theta, \ \left|\mathrm{Tr}\left[\rho X\right] - \bar{X}\right| \leqslant \mu_X\right\}, \tag{4.2}$$

where Θ denotes the set of Bob's observables and

$$\mu_X := \sqrt{\frac{2x^2}{k} \ln\left(\frac{2}{\epsilon_{AT}}\right)}.$$

In case X is a positive semidefinite operator, we obtain the improved bound

$$\mu_X := \sqrt{\frac{x^2}{2k} \ln\left(\frac{2}{\epsilon_{AT}}\right)}.$$

Proof. Using Hölder's inequality, we obtain for the observable X

$$||X\rho||_1 \leqslant ||X||_\infty ||\rho||_1 = ||X||_\infty =: x,$$

therefore $\mathbb{E}(X) = \mathrm{Tr}\left[\rho X\right] \leqslant x$. This implies that our measurement results w.r.t. the observable X lie within the interval $[-x, x]$ almost surely (or $[0, x]$ in case X is positive semi-definite). Hence, we can apply Hoeffding's inequality [50] which states that

$$\Pr\left[\left|\bar{X} - \mathbb{E}[X]\right| \geqslant \mu_X\right] \leqslant 2e^{-\frac{2k\mu_X^2}{(2x)^2}} =: \epsilon_{\mathrm{AT}}^X. \tag{4.3}$$

For positive semi-definite X replace $2x$ by x. Then, we obtain μ_X from basic algebra.
This allows us to define the relevant set by defining it as the set of all density matrices whose expected values for all observables X deviate less than μ_X from the corresponding observed statistics. For simplicity, we choose for all observables the same ϵ-parameter, $\forall X, X' \in \Theta : \ \epsilon_{\mathrm{AT}}^X = \epsilon_{\mathrm{AT}}^{X'} =: \epsilon_{\mathrm{AT}}$ and obtain the set in Eq. (4.2). □

For an observable X we can associate every density matrix with its corresponding expected value. This theorem tells us that states whose expected values deviate more than μ_X from (at least one of) our observations are accepted only with a probability smaller or equal to ϵ_{AT}. For the rest of the security analysis, it suffices to focus on $\mathcal{S}^{\mathrm{AT}}$, the set of states that are likely to pass the test, at the cost of some small error probability ϵ_{AT}.

4.4.3. Formalisation of the protocol steps

Every protocol step can be described mathematically as a quantum channel. In what follows, formalise the relevant steps to set the stage for the security proof in the upcoming section.

1. Bob performs an energy test on k_T modes, while the remaining $n := N - k_T$ modes as well as Eve's system remain untouched. Let us denote the measurement results by Z^{k_T}.

   In case Bob obtains the measurement results Z^{k_T} such that the energy test is successful, the map outputs a classical register $|r\rangle$ containing '1' and in case the test fails, the register contains '0'. Furthermore, Bob announces his outcomes publicly Z^{k_T}. We translate this now into an energy testing map

   $$\mathcal{E}^{\mathrm{ET}} := \mathrm{id}_{A^n B^n E} \otimes \left(\mathcal{E}^{\mathrm{ET},\,2} \circ \mathcal{E}^{\mathrm{ET},\,1}\right)_{A^{k_T} B^{k_T}} .$$

   The two maps composing the energy testing map are defined as follows,

   $$\mathcal{E}^{\mathrm{ET},\,1} :\ \rho_{A^{k_T} B^{k_T}} \mapsto \int_{Z^{k_T} \in \mathbb{C}} p(Z^{k_T}\ |\rho_{A^{k_T} B^{k_T}})\, |Z^{k_T}\rangle\langle Z^{k_T}|\ d\mu =: \rho^{|\rho}_{Z^{k_T}}.$$

   and

   $$\mathcal{E}^{\mathrm{ET},\,2} :\ \sigma \mapsto \Pi_{\mathrm{ET}} \sigma \Pi_{\mathrm{ET}} + (\mathbb{1} - \Pi_{\mathrm{ET}})\sigma(\mathbb{1} - \Pi_{\mathrm{ET}}),$$

   where we set $\Pi_{\mathrm{ET}} := \sum_{\mathcal{A}} |Z^{k_T}\rangle\langle Z^{k_T}|$ with $\mathcal{A}$ being the set containing all bit strings Z^{k_T} that cause the energy test to abort with probability $1-_{\mathrm{ET}}$ and

   $$\rho_{Z^k} := \int_{Z^k \in \mathbb{C}} p\left(Z^k | \rho_{A^k B^k}\right) |Z^k\rangle\langle Z^k|\ d\mu.$$

2. If the energy test passes, Alice and Bob perform parameter estimation. To use their data economically, they may use the same rounds for parameter estimation as Bob used for the energy test, as this information is already public anyways. Hence, they use a parameter-estimation routine.

   $$\begin{aligned} &\mathcal{E}^{\mathrm{AT}} :\ \rho^{ET}_{A^n B^n E} \otimes |y\rangle\langle y|^{\otimes k_T} \\ &\mapsto \rho^{\mathrm{AT}}_{A^n B^n E} := \begin{cases} \rho^{\mathrm{ET}}_{A^n B^n E} \otimes |0\rangle\langle 0|, & \text{if AT failed,} \\ \rho^{\mathrm{ET}}_{A^n B^n E} \otimes |1\rangle\langle 1|, & \text{if AT passed} \end{cases}. \end{aligned}$$

3. We may combine those maps into a map covering the whole testing procedure,

$$\begin{aligned}\mathcal{E}^{\text{Test}} &: \ \rho_{A^N B^N E} \mapsto \rho^{\text{ET\&AT}}_{A^n B^n E'} \\ &:= \rho_{A^n B^n E} \otimes \left(\Pi_{\text{ET}} \rho^{|\rho}_{Z^{k_T}} \Pi_{\text{ET}} \otimes |0\rangle\langle 0|_T + (\mathbb{1} - \Pi_{\text{ET}}) \rho^{|\rho}_{Z^{k_T}} (\mathbb{1} - \Pi_{\text{ET}}) \otimes |1\rangle\langle 1|_T \right),\end{aligned}$$

where now $|1\rangle\langle 1|_T$ indicates that both the energy test and the acceptance test passed and $|0\rangle\langle 0|_T$ stands for all other cases. Note that the right side of the tensor product represents public information. Therefore, we can absorb this expression into Eve's system by renaming it E'.

4. In case the testing procedures were successful, Alice and Bob apply a key map to obtain classical data and perform classical post-processing

$$\mathcal{E}^{\text{class}} : \ \rho^{\text{ET\&AT}}_{A^n B^n E'} \mapsto \rho_{X^n Y^n E'}.$$

4.4.4. Finite-size security proof

After having finished all preparations, we now establish the security proof of the present CV-QKD protocol against i.i.d. collective attacks. We state our main result, the security statement against i.i.d. collective attacks, in the following theorem and prove it afterwards. Note that we postpone the proof of technical statements and lemmas used in our proof to Appendix B to improve readability.

Theorem 4.4.3: Security statement against i.i.d. collective attacks

Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be separable Hilbert spaces and let $\epsilon_{ET}, \epsilon_{AT}, \bar{\epsilon}, \epsilon_{EC}, \epsilon_{PA} > 0$. If the output of the quantum phase of the objective QKD protocol is i.i.d., the protocol is $\epsilon_{ET} + \epsilon_{AT} + \bar{\epsilon} + \epsilon_{EC} + \frac{\epsilon_{PA}}{2}$-secure given that, in case the protocol does not abort, the secure key length is chosen to satisfy

$$\begin{aligned}\frac{\ell}{N} \leqslant \frac{n}{N} \left[\min_{\rho \in \mathcal{S}^{E\&A}} H(X|E')_\rho - \delta(\bar{\epsilon}) - \Delta(w) \right] \\ - \delta^{EC}_{\text{leak}} - \frac{2}{N} \log_2 \left(\frac{1}{\epsilon_{PA}} \right),\end{aligned} \tag{4.4}$$

where $\delta^{EC}_{\text{leak}}$ takes the classical error-correction cost into account, $\Delta(w)$ is given in Eq. (3.45) and $\delta(\epsilon) := 2 \log_2 (rank(\rho_X) + 3) \sqrt{\frac{\log_2(2/\epsilon)}{n}}$.

Proof. According to our assumption, after completing N rounds of the quantum phase in the present QKD protocol, Alice and Bob share the state $\rho^{\otimes N}_{AB} \in \mathcal{D}((\mathcal{H}_A \otimes$

$\mathcal{H}_B)^{\otimes N}$). There exists a purification $\rho_{ABE} \in \mathcal{S}_1(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E)$ of ρ_{AB}, where the purifying system E can be infinite-dimensional. Hence, $\rho_{ABE}^{\otimes N} \in \mathcal{S}_1((\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E)^{\otimes N})$ purifies $\rho_{AB}^{\otimes N}$. To ease the notation, we define $\mathcal{H} := \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$. We argue first that the relevant state after both the energy test and the acceptance test still has a tensor-product structure. Due to the nature of statistical testing, in our security analysis we never know the actual state Bob receives, but only decide to proceed or abort the protocol, based on if the state we receive lies within a pre-defined set. Therefore, in the next step, we show that the states we consider in our security analysis are $\epsilon_{\mathrm{ET}} + \epsilon_{\mathrm{AT}}$-close to this unknown state. Finally, we choose the worst-case state contained in the feasible set, i.e., the state that gives Eve the most advantage and Alice and Bob the lowest key rate. In what follows, we formalise those steps rigorously.
By Lemma B.1.1, we know that there exists a measure ν on $\mathcal{S}_1(\mathcal{H})$ such that

$$\left\| \rho_{ABE}^{\otimes N} - \int_{\sigma \in \mathcal{S}_1(\mathcal{H})} \sigma^{\otimes N} \, \nu(\sigma) \right\|_1 = 0.$$

Since the data processing inequality for the trace distance under completely positive trace non-increasing maps holds for general density operators as well (see Lemma B.1.3), we apply the map $\mathcal{E}^{\mathrm{ET}}$ modelling our energy test and obtain

$$\left\| \rho^{\mathrm{ET}} - \int_{\sigma \in \mathcal{S}_1(\mathcal{H})} \sigma^{\mathrm{ET}} \, \nu(\sigma) \right\|_1 = 0, \tag{4.5}$$

where the superscript ET indicates that the energy test has been applied. Note that we omitted the N-fold tensor product in the superscript of the states to improve readability. We define the set of states that have not been filtered by the energy test with probability greater than $1 - \epsilon_{\mathrm{ET}}$,

$$\mathcal{S}^{\mathrm{ET}} := \{\sigma \in \mathcal{S}_1(\mathcal{H}) : \ \mathrm{Tr}_E[\sigma] \ \text{ is not } \epsilon_{\mathrm{ET}}\text{-securely filtered}\}.$$

Similarly, we can apply our (CPTNI) acceptance testing map $\mathcal{E}^{\mathrm{AT}}$ and obtain

$$\left\| \rho^{\mathrm{E\&A}} - \int_{\sigma \in \mathcal{S}_1(\mathcal{H})} \sigma^{\mathrm{E\&A}} \, \nu(\sigma) \right\|_1 = 0. \tag{4.6}$$

Analogously, as a subset of all states that have not been filtered by the energy test, we define the set of states that have not been filtered by the acceptance test with probability greater than $1 - \epsilon_{\mathrm{AT}}$

$$\mathcal{S}^{\mathrm{E\&A}} := \left\{\sigma \in \mathcal{S}^{\mathrm{ET}} : \ \mathrm{Tr}_E[\sigma] \ \text{ is not } \epsilon_{\mathrm{AT}}\text{-securely filtered}\right\}.$$

To ease the notation, in what follows, we omit the superscript E&A for states occurring in integrals as for those the set they belong to is clear from the context.

We can split up the set of pure states as follows $\mathcal{S}_1(\mathcal{H}) = \mathcal{S}^{\mathrm{ET}} \cup \overline{\mathcal{S}^{\mathrm{ET}}}$, where $\bar{\cdot}$ denotes the complement of a set, and similarly $\mathcal{S}^{\mathrm{ET}} = \mathcal{S}^{\mathrm{E\&A}} \cup \overline{\mathcal{S}^{\mathrm{E\&A}}}$. Therefore, we obtain

$$\int_{\sigma\in\mathcal{S}^{\mathrm{ET}}} \sigma\ \nu(\sigma) = \int_{\sigma\in\mathcal{S}_1(\mathcal{H})} \sigma\ \nu(\sigma) - \int_{\sigma\in\overline{\mathcal{S}^{\mathrm{ET}}}} \sigma\ \nu(\sigma) \tag{4.7}$$

and

$$\int_{\sigma\in\mathcal{S}^{\mathrm{E\&A}}} \sigma\ \nu(\sigma) = \int_{\sigma\in\mathcal{S}^{\mathrm{ET}}} \sigma\ \nu(\sigma) - \int_{\sigma\in\overline{\mathcal{S}^{\mathrm{E\&A}}}} \sigma\ \nu(\sigma). \tag{4.8}$$

We derive

$$\begin{aligned}
&\left\|\rho^{\mathrm{ET}} - \int_{\mathcal{S}^{\mathrm{ET}}} \sigma\ \nu(\sigma)\right\|_1 \\
&\leqslant \left\|\rho^{\mathrm{ET}} - \int_{\mathcal{S}_1(\mathcal{H})} \sigma\ \nu(\sigma)\right\|_1 + \left\|\int_{\mathcal{S}_1(\mathcal{H})} \sigma\ \nu(\sigma) - \int_{\mathcal{S}^{\mathrm{ET}}} \sigma\ \nu(\sigma)\right\|_1 \\
&= 0 + \left\|\int_{\overline{\mathcal{S}^{\mathrm{ET}}}} \sigma\ \nu(\sigma)\right\|_1 \\
&\leqslant \int_{\overline{\mathcal{S}^{\mathrm{ET}}}} ||\sigma||_1\ \ \nu(\sigma) \\
&\leqslant \epsilon_{\mathrm{ET}},
\end{aligned}$$

where the first step follows from the triangle inequality. For the second step, we applied Eq. (4.5) and Eq. (4.7). For the last step, we used that ν is a probability measure, and $||\sigma||_1 \leqslant 1$.
Similarly, one can show that

$$\left\|\rho^{\mathrm{E\&A}} - \int_{\mathcal{S}^{\mathrm{E\&A}}} \sigma\ \nu(\sigma)\right\|_1 \leqslant \epsilon_{\mathrm{AT}}.$$

We use these two statements to conclude

$$\begin{aligned}
&\left\|\rho_{ABE} - \int_{\mathcal{S}^{\mathrm{E\&A}}} \sigma\ \nu(\sigma)\right\|_1 \\
&\leqslant \left\|\rho_{ABE} - \int_{\mathcal{S}_1(\mathcal{H})} \sigma\nu(\sigma)\right\|_1 + \left\|\int_{\mathcal{S}_1(\mathcal{H})} \sigma\ \nu(\sigma) - \int_{\mathcal{S}^{\mathrm{E\&A}}} \sigma\ \nu(\sigma)\right\|_1 \\
&\leqslant \left\|\int_{\mathcal{S}_1(\mathcal{H})} \sigma\ \nu(\sigma) - \int_{\mathcal{S}^{\mathrm{ET}}} \sigma\ \nu(\sigma)\right\|_1 + \left\|\int_{\mathcal{S}^{\mathrm{ET}}} \sigma\ \nu(\sigma) - \int_{\mathcal{S}^{\mathrm{E\&A}}} \sigma\ \nu(\sigma)\right\|_1 \\
&\leqslant \left\|\int_{\overline{\mathcal{S}^{\mathrm{ET}}}} \sigma\ \nu(\sigma)\right\|_1 + \left\|\int_{\overline{\mathcal{S}^{\mathrm{E\&A}}}} \sigma\ \nu(\sigma)\right\|_1.
\end{aligned}$$

Hence, we showed that

$$\left\| \rho_{ABE}^{\otimes n} - \int_{\mathcal{S}^{\mathrm{E\&A}}} \sigma \ \nu(\sigma) \right\|_1 \leqslant \epsilon_{\mathrm{ET}} + \epsilon_{\mathrm{AT}}. \tag{4.9}$$

Finally, since the map describing the classical post-processing, $\mathcal{E}^{\mathrm{key}}$, is CPTNI as well, we apply Lemma B.1.3 once again, and obtain

$$\left\| \rho_{X^n Y^n E'} - \int_{\mathcal{S}^{\mathrm{E\&A}}} \sigma \ \nu(\sigma) \right\|_1 \leqslant \epsilon_{\mathrm{ET}} + \epsilon_{\mathrm{AT}}. \tag{4.10}$$

The register E' combines the purification space and all the classical information released to Eve up to now. So, it suffices to show that the remaining parts of the protocol are secure on $\rho_{X^n Y^n E'}$.
The two remaining problems we face are that Alice and Bob's keys are only partially correlated and only partially secret. The first problem is tackled by performing error-correction, while the second one is addressed by the privacy amplification routine, which is characterized by the leftover hashing lemma [85, Lemma 5.6.1] which we extend to infinite-dimensional side-information in Lemma B.1.4. As shown by Renner [85, Lemma 5.6.1], if Alice and Bob apply a randomly chosen hash function from the family of two-universal hash-functions to their bit-string, the output is secure as long as it is smaller than Eve's uncertainty about their initial bit-string, where the uncertainty is measured in terms of the smooth min-entropy. Since in the present case the purifying system E is infinite-dimensional, we cannot apply Renner's result directly, but derive a leftover hashing lemma against infinite-dimensional side-information (Lemma B.1.4 in the Appendix).
In Lemma B.1.4, we set $\epsilon' := \epsilon_{\mathrm{ET}} + \epsilon_{\mathrm{AT}} + \bar{\epsilon}$ (the nature of this choice will become obvious later) as well as $\epsilon_{\mathrm{PA}} := 2(\epsilon_{\mathrm{sec}} - \epsilon')$ and obtain

$$\ell \leqslant H_{\min}^{\epsilon'}(X|E'C)_\rho - 2\log_2\left(\frac{1}{\epsilon_{\mathrm{PA}}}\right),$$

where C denotes the information reconciliation transcript. Note that we re-scaled ϵ' by a factor of 2 when we define ϵ_{PA}, hence the factor of 2 in the smoothing of the smooth min-entropy expression from the statement of Lemma B.1.4 is already included in our new ϵ'.
Lemma B.1.6, extends a statement in [85, Lemma 6.4.1] to infinite-dimensional side-information, allows us to remove a classical register from the smooth min-entropy at the cost of $\mathrm{leak}_{\mathrm{EC}}$ bits,

$$\ell \leqslant H_{\min}^{\epsilon'}(X|E')_\rho - 2\log_2\left(\frac{1}{\epsilon_{\mathrm{PA}}}\right) - \mathrm{leak}_{\mathrm{EC}}. \tag{4.11}$$

All that remains is to convert the smooth min-entropy term into something we can optimise over. Therefore, we define the state $\bar{\rho} := \int_{\sigma \in \mathcal{S}^{\mathrm{E\&A}}} \sigma_{X^n E'} \otimes |\sigma\rangle\langle\sigma| \, \nu(\sigma)$, where the artificially introduced register keeps track of the states in the mixture. From Eq. (4.9) we know that the ρ that occurs in the smooth min-entropy expression in Eq. (4.11) and $\bar{\rho}$ are $\epsilon_{\mathrm{ET}} + \epsilon_{\mathrm{AT}}$-close to each other. Recalling that we set $\epsilon' = \epsilon_{\mathrm{ET}} + \epsilon_{\mathrm{AT}} + \bar{\epsilon}$, we observe that the $\bar{\epsilon}$-ball around $\bar{\rho}$ is contained in the ϵ'-ball around ρ (note that this motivates our choice for ϵ'). Since the definition of the smooth min-entropy includes a supremum over the corresponding ϵ-ball, we conclude

$$H_{\min}^{\epsilon'}(X|E')_{\rho} \geqslant H_{\min}^{\bar{\epsilon}}(X|E')_{\bar{\rho}}.$$

Next, we use Lemma B.1.8 and Lemma B.1.9, extensions to infinite-dimensional side-information of the strong subadditivity property for smooth min-entropies ([85, Lemma 3.2.7]) and the rule for conditioning smooth min-entropies on classical registers ([85, Lemma 3.2.8]), to rewrite our smooth min-entropy expression. In more detail, we condition on the register that indexes over the set $\mathcal{S}^{\mathrm{E\&A}}$, denoted by 'conditioning on the set itself', and then remove the introduced register by choosing the worst-case,

$$\begin{aligned} H_{\min}^{\bar{\epsilon}}(X|E')_{\bar{\rho}} &\geqslant H_{\min}^{\bar{\epsilon}}(X|E'\mathcal{S}^{\mathrm{E\&A}})_{\bar{\rho}} \\ &\geqslant \min_{\sigma \in \mathcal{S}^{\mathrm{E\&A}}} H_{\min}^{\bar{\epsilon}}(X|E')_{\sigma}. \end{aligned}$$

Thanks to Proposition B.1.10 and the i.i.d. structure of our signals, $\rho_{X^N Y^N} = \rho_{X^n Y^n} \otimes \rho_{X^{k_T} Y^{k_T}}$, the rounds we used for testing (and sifting) are independent of the key generation rounds and can be removed from the conditioning system in the min-entropy expression without cost (hence, do not give Eve any advantage). Combining these results, we arrive at

$$\ell \leqslant \min_{\sigma \in \mathcal{S}^{\mathrm{E\&A}}} H_{\min}^{\bar{\epsilon}}(X|E')_{\sigma} - 2\log_2\left(\frac{1}{\epsilon_{\mathrm{PA}}}\right) - \mathrm{leak}_{\mathrm{EC}}. \tag{4.12}$$

Finally, we use Corollary B.2.17, which is our version of the asymptotic equipartition property [85, Corollary 3.3.7], to rewrite the smooth min-entropy in terms of the von-Neumann entropy

$$\ell \leqslant n\left[\min_{\sigma \in \mathcal{S}^{\mathrm{E\&A}}} H(X|E')_{\sigma} - \delta(\bar{\epsilon})\right] - 2\log_2\left(\frac{1}{\epsilon_{\mathrm{PA}}}\right) - \mathrm{leak}_{\mathrm{EC}}. \tag{4.13}$$

While this completes our finite-size analysis, we want to optimise over finite-dimensional (in more detail: low-dimensional) states. Our energy test (Theorem 4.4.1) guarantees that any state that is not ϵ_{ET}- filtered has at most weight

w outside the cutoff-space (defined by the parameter n_c in the energy test), hence satisfies $\mathrm{Tr}\left[\rho\Pi^{n_c}\right] = 1 - w$. Using [105, Theorem 1], we can relate the values of our objective function on inputs in infinite-dimensional Hilbert space to its values on projections on a finite-dimensional subspace $\mathcal{H}^{n_c}$ by taking an additional weight-dependent correction term $\Delta(w)$ into account. Hence, we finally arrive at

$$\begin{aligned}\ell \leqslant n \left[\min_{\sigma\in\mathcal{S}^{\mathrm{E\&A}}} H(X|E')_\sigma - \delta(\bar{\epsilon}) - \Delta(w)\right] \\ - 2\log_2\left(\frac{1}{\epsilon_{\mathrm{PA}}}\right) - \mathrm{leak}_{\mathrm{EC}}.\end{aligned} \tag{4.14}$$

Finally, we divide both sides by N, the total number of signals sent, and arrive at

$$\begin{aligned}\frac{\ell}{N} \leqslant \frac{n}{N}\left[\min_{\sigma\in\mathcal{S}^{\mathrm{E\&A}}} H(X|E')_\sigma - \delta(\bar{\epsilon}) - \Delta(w)\right] \\ - \frac{2}{N}\log_2\left(\frac{1}{\epsilon_{\mathrm{PA}}}\right) - \delta^{\mathrm{EC}}_{\mathrm{leak}},\end{aligned} \tag{4.15}$$

where we defined $\delta^{\mathrm{EC}}_{\mathrm{leak}} := \frac{\mathrm{leak}_{\mathrm{EC}}}{N}$ (see Section 4.4.6). As we defined $\epsilon_{\mathrm{PA}} = 2(\epsilon_{\mathrm{sec}} - \epsilon')$, we obtain $\epsilon_{\mathrm{sec}} = \frac{\epsilon_{\mathrm{PA}}}{2} + \epsilon_{\mathrm{ET}} + \epsilon_{\mathrm{AT}} + \bar{\epsilon}$. Hence, the key we obtain is ϵ_{sec} secret and $\epsilon_{\mathrm{cor}} = \epsilon_{\mathrm{EC}}$ correct, so $\epsilon := \epsilon_{\mathrm{sec}} + \epsilon_{\mathrm{cor}}$ secure, which finishes the proof.

□

4.4.5. Finite-size optimisation problem

Notice that the objective function of the optimisation in the asymptotic limit (3.23) is the same as for the finite-size problem (4.4), while the feasible sets differ. Furthermore, there are additional correction terms for the finite-size version of the key rate formula. However, as these terms are constant with respect to the performed optimisation, they do not influence the structure of the SDP.

In the finite-size regime, we do not know the expected values of our observables with certainty. As outlined in the protocol description, we fix some small $\epsilon_{\mathrm{AT}} > 0$ and a testing ratio $\mathrm{TR} \in (0, 1)$ such that $k := \mathrm{TR} \cdot N$ and perform testing on k randomly selected rounds. According to Theorem 4.4.2, we obtain bounds μ_j which define our acceptance set. Therefore, our actual optimisation problem reads

$$
\begin{aligned}
\alpha := \min\ & f(\rho) \\
\text{s.t.}\ & \\
& \mathrm{Tr}_B\left[\rho\right] = \rho_A, \\
& \left|\mathrm{Tr}\left[\hat{\Gamma}_j \rho\right] - \gamma_j\right| \leqslant \mu_j, \\
& \mathrm{Tr}\left[\rho\right] = 1, \\
& \rho \geqslant 0
\end{aligned}
\tag{4.16}
$$

for $j \in \{1, ..., 2N_{\mathrm{St}}\}$. Note that the trace equal to one constraint is not subject to finite-size effects.

It is shown in Appendix C that finally, after applying the dimension reduction method, and various steps to bring the SDP to a more favourable form, we obtain the following (primal) optimisation problem

$$
\begin{aligned}
\beta := \min\ & f(\bar{\rho}) \\
\text{s.t.}\ & \\
& 1 - w \leqslant \mathrm{Tr}\left[\bar{\rho}\right] \leqslant 1, \\
& \mathrm{Tr}\left[P\right] + \mathrm{Tr}\left[N\right] \leqslant 2\sqrt{w}, \\
& P \geqslant \mathrm{Tr}_B\left[\bar{\rho}\right] - \rho_A \\
& N \geqslant -\left(\mathrm{Tr}_B\left[\bar{\rho}\right] - \rho_A\right), \\
& \mathrm{Tr}\left[\left(|i\rangle\langle i| \otimes \hat{n}_{\beta_j}\right)\bar{\rho}\right] \leqslant \mu_j + \langle \hat{n}_{\beta_j} \rangle - a_j, \\
& \mathrm{Tr}\left[\left(|i\rangle\langle i| \otimes \hat{n}_{\beta_j}\right)\bar{\rho}\right] \leqslant -\mu_j + \langle \hat{n}_{\beta_j} \rangle + b_j, \\
& \mathrm{Tr}\left[\left(|i\rangle\langle i| \otimes \hat{n}^2_{\beta_j}\right)\bar{\rho}\right] \leqslant \mu_j + \langle \hat{n}^2_{\beta_j} \rangle - a_j, \\
& \mathrm{Tr}\left[\left(|i\rangle\langle i| \otimes \hat{n}^2_{\beta_j}\right)\bar{\rho}\right] \leqslant -\mu_j + \langle \hat{n}^2_{\beta_j} \rangle + b_j, \\
& \bar{\rho}, P, N \geqslant 0, \\
& \vec{a}, \vec{b} \geqslant 0.
\end{aligned}
\tag{4.17}
$$

This optimisation problem gives a lower bound on the first term in the key rate formula in Eq. (4.4), $\alpha \geqslant \beta$. After taking numerical imprecisions into account and applying the relaxation theorem in [110], the dual problem reads (as shown

in Appendix C):

$$\begin{aligned}\gamma := &- \max\ \vec{y}\ \left(\vec{\lambda}+\vec{\epsilon}\right) + \left(2\sqrt{w}+\epsilon_{\text{num}}\right) s + \operatorname{Tr}\left[\rho_A\ \tau\right] - \operatorname{Tr}\left[\rho_A\ \Theta\right] \\ &\text{s.t.} \\ &\nabla f(\rho) + \sum_{j=1}^{6N_{\text{St}}} y_j \hat{\Gamma}_j + \tau \otimes I_B - \Theta \otimes I_B \geqslant 0, \\ &s \cdot I - \tau \geqslant 0, \\ &s \cdot I + \Theta \geqslant 0, \\ &\vec{y} \geqslant 0,\ s \geqslant 0,\ \tau \geqslant 0,\ \Theta \geqslant 0,\end{aligned} \tag{4.18}$$

where the $\hat{\Gamma}_j$ and γ_j are defined as follows

$$\begin{aligned}\hat{\Gamma}_j &:= \hat{n}_{\beta_j}, & \gamma_j &:= \langle \hat{n}_{\beta_j} \rangle, \\ \hat{\Gamma}_{N_{\text{St}}+j} &:= -\hat{n}_{\beta_j}, & \gamma_{N_{\text{St}}+j} &:= -\langle \hat{n}_{\beta_j} \rangle, \\ \hat{\Gamma}_{2N_{\text{St}}+j} &:= \hat{n}^2_{\beta_j}, & \gamma_{2N_{\text{St}}+j} &:= \langle \hat{n}^2_{\beta_j} \rangle, \\ \hat{\Gamma}_{3N_{\text{St}}+j} &:= -\hat{n}^2_{\beta_j}, & \gamma_{3N_{\text{St}}+j} &:= \langle \hat{n}^2_{\beta_j} \rangle, \\ \hat{\Gamma}_{4N_{\text{St}}+j} &:= \mathbb{1}, & \gamma_{4N_{\text{St}}+j} &:= 1, \\ \hat{\Gamma}_{5N_{\text{St}}+j} &:= -\mathbb{1}, & \gamma_{5N_{\text{St}}+j} &:= w-1,\end{aligned}$$

and

$$\vec{\lambda} := \begin{pmatrix} \gamma_1 + \mu_1 \\ \vdots \\ \gamma_{6N_{\text{St}}} + \mu_{6N_{\text{St}}} \end{pmatrix}.$$

Furthermore, note that we defined $\epsilon_{\text{num}} := \epsilon_{\text{rep}}$ (see remark in Appendix C of [105] for details) to take numerical imprecisions into account and $\vec{\epsilon}$ is a vector containing ϵ_{num} in every component. Solving (4.18) gives us a reliable lower bound on the first term in Eq. (4.4), $\min_{\sigma \in \mathcal{S}^{\text{E\&A}}} H(X|E')_\sigma \geqslant \gamma$.

4.4.6. Error correction

In this subsection, we briefly explain the information-reconciliation leakage term. In the case one is able to carry out the information reconciliation procedure in the Slepian-Wolf limit [97], the EC leakage term reads

$$\delta_{\text{EC}} := H(Y|X) = H(Y) - I(X:Y).$$

Here, X and Y represent Alice's and Bob's key strings. Since we cannot expect to perform error correction in the optimal limit, we assume only a fraction $0 < \beta \leqslant 1$ of the mutual information between Alice's and Bob's key strings can be used. Hence, $I(X:Y)$ in the formula above is replaced by $\beta I(X:Y)$. Therefore,

$$\begin{aligned}\delta_{\mathrm{EC}} \mapsto \delta_{\mathrm{EC}}^{\beta} &:= H(Y) - \beta I(X:Y) \\ &= H(Y) - \beta\left[H(Y) - H(Y|X)\right] \\ &= (1-\beta)H(Y) + \beta H(Y|X).\end{aligned}$$

Finally, the total leakage term is the sum of the correction term we just derived and the verification term. We obtain

$$\mathrm{leak}_{\mathrm{EC}} \leqslant n\ \delta_{\mathrm{EC}}^{\beta} + \log_2\left(\frac{2}{\epsilon_{\mathrm{EC}}}\right). \tag{4.19}$$

As the present protocol allows postselection, not all signals might be used for signal generation. Hence, not all signals have to undergo the information reconciliation procedure. Therefore, we replace $\mathrm{leak}_{\mathrm{EC}} \mapsto p_{\mathrm{pass}}\mathrm{leak}_{\mathrm{EC}}$, where p_{pass} is the probability that a round passes the postselection routine.

5. Numerical Results

After deriving a lower bound on the secure finite-size key rate (Theorem 4.4.3) and applying a modified version of the numerical method in Refs. [19, 110] in Section 4.4.5, it remains to calculate numerical key rates for a particular protocol. Exemplarily, we chose the QPSK protocol in Ref. [64]. We note that large parts of this chapter are taken from our publication [55].

5.1. Quadratue phase-shift keying protocol

After proving the security of a general discretely-modulated CV-QKD protocol, in order to provide numerical key rates, we restrict our considerations to the special case of $N_{\mathrm{St}} = 4$ signal states arranged on a circle in the phase space, a so-called quadrature phase-shift keying protocol. Therefore, in every round, Alice prepares one of the states $\{|\alpha\rangle, |i\alpha\rangle, |-\alpha\rangle, |-i\alpha\rangle\}$ with equal probability, where $\alpha \in \mathbb{R}$ is arbitrary but fixed. Bob then performs heterodyne detection on the states he receives. While our security proof works both for direct- and reverse reconciliation, we proceed with reverse reconciliation which is known to outperform direct reconciliation for CV-QKD protocols. Therefore, Bob performs the key map and assigns symbols to his measurement results, depending on in which area of the phase space the measurement outcomes lie. This includes the option of performing postselection to increase the key rate. For more details regarding the protocol, we refer to [64, Protocol 2]. Since our description of the numerical method in Section 3.4 was general, the expressions there apply to the present special case if we insert $N_{\mathrm{St}} = 4$.

5.2. Choice of the weight

In our security proof, the weight $w = \mathrm{Tr}\left[\rho\Pi^{\perp}\right]$ plays a two-fold role. On the one hand, it appears as a parameter in the energy test, while on the other hand, it determines the size of the correction term $\Delta(w)$ arising from the dimension reduction method. While the asymptotic dimension reduction method gives a bound on the weight via another semidefinite program, in our case w is chosen freely during the energy test. This means that, in principle, one could choose the weight

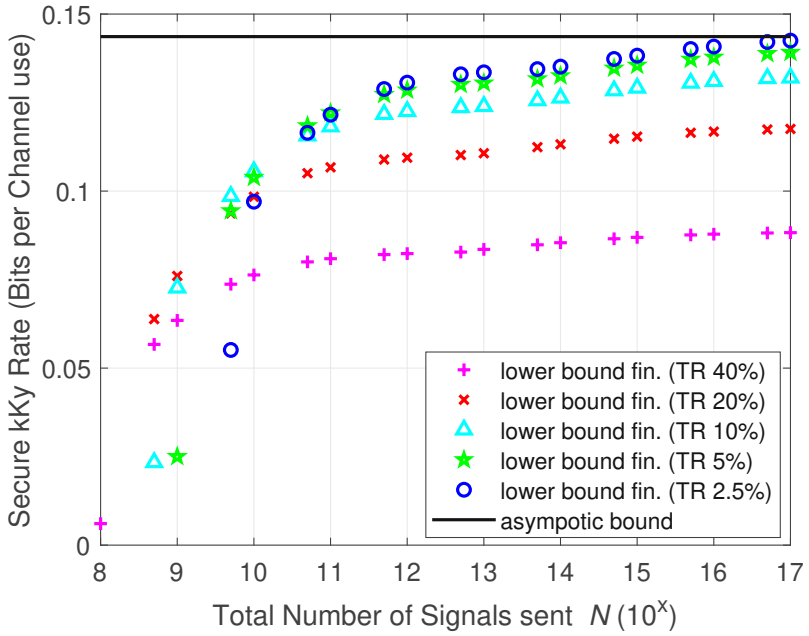

Figure 5.1.: Secure key rates over total number of signals sent N for $L = 10$km, $\alpha = 0.95$, $\Delta_r = 0.60$.

arbitrarily small, resulting in a negligible correction term without corrupting our security statement (possibly resulting in a large ϵ_{ET}. However, since the energy test only makes a statement in the case when the test passes and aborts otherwise (and therefore is trivially secure), this comes at the cost of a high failure rate of the energy test, hence ultimately a low average key rate. Therefore, the choice of the weight w is a balancing act between aiming for a low correction term and making the energy test pass with high probability. In order to assure that, we required that the energy test passes with high probability in the honest implementation, i.e., when Eve is passive. Therefore, we modelled the quantum channel connecting Alice and Bob as a noisy and lossy Gaussian channel with excess noise ξ and transmittance η and calculated the expected weight w_{exp} outside the cutoff space. Then, one possible choice for the weight is $w \geqslant w_{\mathrm{exp}}$. Alternatively, we can fix ϵ_{ET} and just solve the expression for ϵ_{ET} obtained from the energy testing theorem (Theorem 4.4.1) for w to obtain w_ϵ. In practice, we introduce a minimal weight w_{min} and choose the weight $w := \max\{w_{\mathrm{exp}}, w_\epsilon, w_{\mathrm{min}}\}$ to make sure it is both compatible with the chosen ϵ_{ET} and large enough such that the energy test passes with high probability on the honest implementation.

5.3. Details about the Implementation

Before we come to our numerical results, we briefly discuss our choice of parameters and some technical details. To demonstrate the performance of the chosen four-state phase-shift keying protocol under our finite-size security proof, we simulate the expectation values (see Eq. (4.16) and optimisation problems derived thereof) obtained from an experiment by modelling Alice's coherent states passing a noisy and lossy Gaussian channel with excess noise ξ and channel transmittance η. The excess noise is understood as preparation noise on Alice's side so that it is taken to be fixed at the input of the channel. Hence, Bob experiences the effective noise $\eta\xi$. Note that we measure the noise in the shot noise units. Within the whole work, our transmittance model as a function of the transmission distance L is $\eta = 10^{-0.02L}$. This corresponds to a transmission of -0.2 dB/km which is a common value for optical fibres at the telecom wavelength.

While the total number of transmitted signals N, as well as the testing ratio $\frac{k_T}{N}$ varies, we fix l_T (see Theorem 4.4.3) to be 1% of k_T. Furthermore, we fix the ϵ parameters to be $\epsilon_{\mathrm{ET}} = \epsilon_{\mathrm{AT}} = \bar{\epsilon} = \epsilon_{\mathrm{EC}} = \frac{1}{5} \times 10^{-10} = \frac{1}{2}\epsilon_{\mathrm{PA}}$ such that our total security parameter is $\epsilon = 10^{-10}$. We emphasise that our security proof is independent of the choice of parameters and that those values are chosen for demonstration purposes only.

We applied the numerical framework in [19, 110] to find a lower bound on the minimisation problem in Eq. (4.17) and Eq. (4.18). For a brief review of the method see Section 3.4. The coding was carried out in MATLAB™, version R2020a and the semidefinite programs were modelled using CVX [42, 41], where we used the MOSEK solver (Version 9.1.9) [1] to solve the semidefinite programs.

A crucial point with respect to computation time is the calculation of the region operators in Eq. (3.38) in the displaced number basis. An expression for the matrix elements in the displaced basis, given in [105, Appendix B], contains an integral that needs to be calculated numerically, which is computationally costly, in particular for larger cutoff numbers n_c. Therefore, in the current work, we present an alternative approach. We use the analytical expressions for region operators in the non-displaced number basis from [56, 64] and apply a basis change to the displaced number basis. Calling the corresponding transformation matrices T, we have $R^z_{B,\mathrm{disp}} = TR^z_B T^\dagger$. In principle, the occurring matrices are infinite-dimensional. Assuming the dimension of Bob's system in our numerical implementation is $d \times d$ (based on the energy test), we only require the first $(d \times d)$-subblock of $R^z_{B,\mathrm{disp}}$ for the numerical method. However, it turns out to be difficult to prove rigorously the numerical error we make by this cutoff. Therefore, we calculate the

analytical matrix elements up to dimension $(3d \times 3d)$ and apply the corresponding $(3d \times 3d)$-dimensional transformation matrices T. We repeat the same process with dimension $(5d \times 5d)$ and compare the first $d \times d$-subblock of the resulting matrices. We accept the result and proceed if the component-wise absolute difference between both matrices is 10^{-16} or smaller (in fact, it turns out that the differences in almost all cases are 0 up to numerical precision), showing that increasing the dimension further does not affect the matrix elements any more. Otherwise, we increase the dimension. Even though we have to calculate significantly larger 'intermediate matrices' to ensure high numerical precision, this method turns out to be significantly faster than calculating the matrix elements numerically and avoids numerical integration errors (which are larger than the numerical errors of our method at the level of machine precision).

We conclude by a brief remark about the expected values in our optimisation problems given in Eq. (4.17) and Eq. (4.18). As derived in [105, 106], assuming a lossy and noisy Gaussian channel, we obtain for the expected values occurring in the primal as well as in the dual optimisation problem $\langle \hat{n}_{\beta_j} \rangle = \frac{\xi}{2}$ and $\langle \hat{n}^2_{\beta_j} \rangle = \frac{\xi(1+\xi)}{2}$. For the expected values in the trusted detector noise scenario, we refer to the remark at the end of Section 3.4.4. For the key rate plots in the upcoming section, we assume a lossy and noisy Gaussian channel, hence using those expected values to formulate our optimisation problem.

5.4. Simulation Results

We present plots of the obtained secure key rates for various parameter choices. If not mentioned otherwise, we fix $\xi = 0.01$ and in all plots, we assume that an error-correction code with efficiency $\beta = 0.95$ is used, which is achievable with the latest low-density parity-check codes. If we do not state a particular value for α and Δ_r, the corresponding curves have been obtained after optimising over α and Δ_r via coarse-grained search. We chose the cutoff-space dimension $n_c = 20$, which turned out to be a sound compromise between numerical feasibility (calculation time) and impact on the obtained key rates (see the role of the cutoff number in the security proof in Section 3.4).
First, we discuss our results for untrusted, ideal detectors (so $\eta_d = 1$ and $\nu_{\text{el}} = 0$), which is followed by results for trusted, non-ideal detectors ($\eta_d < 1$ and $\nu_{\text{el}} > 0$).

5.4.1. Untrusted, ideal detectors

In what follows, we present our results for untrusted, ideal detectors. The key rates shown are measured in bits per channel use and the plotted asymptotic key

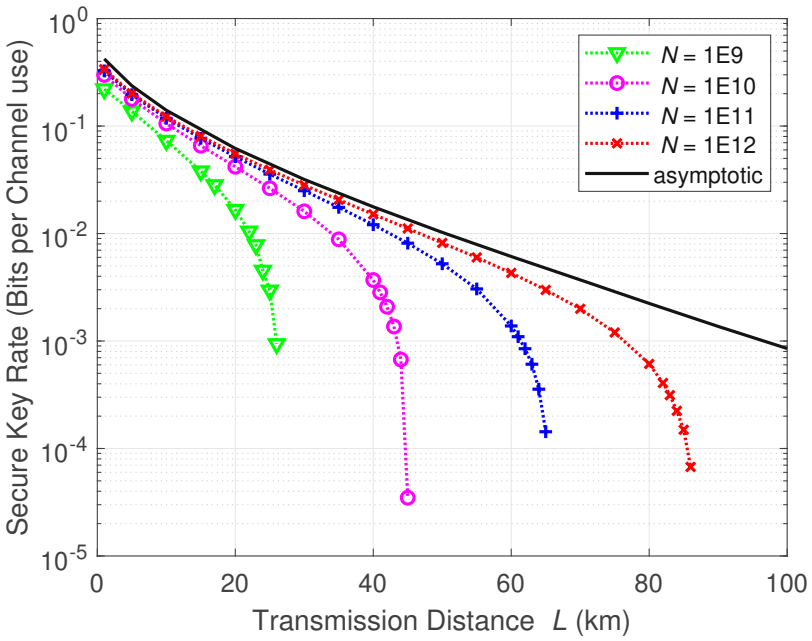

Figure 5.2.: Secure key rates over transmission distance L for different total number of signals N, optimised the coherent state amplitude α and the radial postselection parameter Δ_r and fixed testing ratio TR = 10%.

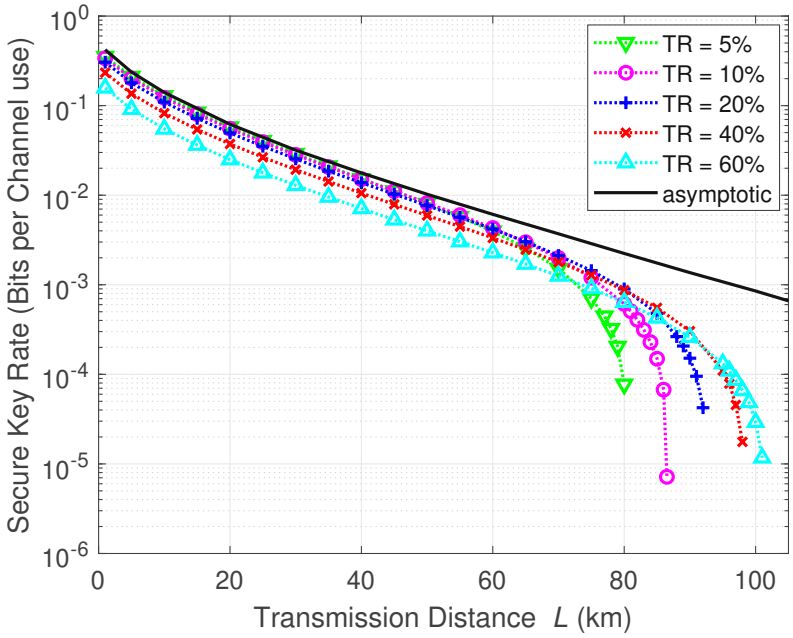

Figure 5.3.: Secure key rates over transmission distance L for fixed $N = 10^{12}$, optimised the coherent state amplitude α and the radial postselection parameter Δ_r and different testing ratios TR.

rate curves were generated with the method described in [105].

Figure 5.1 shows the obtained secure key rates over the total number of signals sent N. We fixed the transmission distance to be 10 km, the coherent state amplitude $\alpha = 0.95$ and the radial postselection parameter $\Delta_r = 0.60$, while we varied the testing ratios (TR). As one can see, we obtain secure key rates for $N \geqslant 10^8$ for TR $= 40\%$. Furthermore, our secure key rates approach the asymptotic limit from Ref. [105] for $N \to \infty$ and low testing ratios. This shows that our analysis is tight in the asymptotic limit. We note that we had to readjust the asymptotic key rate curve in Figure 5.1 according to [105] by the correction term $\Delta(w)$ since the weight in the asymptotic regime without testing is determined differently than in our analysis including an energy test (see also discussion in Section 5.2). Therefore, we are able to work with smaller weights, hence smaller correction terms. In order to make the key rate curves comparable, we, therefore, had to readjust the asymptotic curve.

Next, we consider the performance of our secure key rates as a function of the transmission distance for a different number of total rounds N. We fix the testing ratio to TR $= 10\%$. Again, we note that for the asymptotic key rates, we do not sacrifice signals for testing effectively. Hence the asymptotic key rates are

conceptionally different to the finite-size key rates in the plot and would correspond to finite-size key rates with a testing ratio equal to 0%. This explains the difference in key rates between the asymptotic reference curve and the finite-size key rates for low transmission distances. From Figure 5.1 we know that we cannot expect positive secure key rates for $N = 10^8$ or smaller at $L = 10$km, therefore we start our investigation at $N = 10^9$, where we have hope to surpass $L = 10$km significantly and go up to $N = 10^{12}$, which is the largest N we assume is achievable in experiments with state-of-the-art lasers and heterodyne detectors in a practical amount of time. In Figure 5.2, we present our results. Note that we optimised over the coherent state amplitude α and the postselection parameter Δ_r via coarse-grained search. We observe positive key rates up to 26 km for $N = 10^9$, up to 45 km for $N = 10^{10}$, up to 65 km for $N = 10^{11}$ and up to 86 km for $N = 10^{12}$.
It remains to discuss how much we can improve our results by varying the testing ratio TR. In Figure 5.3, we fix $N = 10^{12}$, optimise over α and Δ_r via coarse-grained search and examine the impact of testing ratios between 5% and 60%. As expected, it turns out that for low transmission distances, low testing ratios are advantageous, while the maximal achievable transmission distance can be improved significantly by increasing the fraction of signals used for testing. This is because for high transmission distances the expectation values in our constraints become small, hence (for the same testing as for lower distances) their uncertainties become relatively large. Higher testing counteracts this effect and increases the secure key rates. Sacrificing 60% of the signals for testing increases the maximal achievable transmission distance from 80 km (for 5% testing) to 101 km.

5.4.2. Trusted, non-ideal detectors

Next, we present our results for the case of trusted, non-ideal detectors. For demonstration purposes we choose $\eta_d = 0.72$ and $\nu_{\text{el}} = 0.04$ and emphasise that our analysis is not restricted to this choice. We fix the excess noise again to $\xi = 0.01$. Note that this means the curves for trusted, non-ideal detectors have a higher total noise level compared to the curves for untrusted, ideal detectors in the previous section. Again, we add asymptotic key rate curves, derived following the method presented in [105], for comparison. Like in the untrusted, non-ideal case, our key rates are tight, i.e. for low testing ratio TR and a high number of rounds N, the obtained finite-size key rates converge to the asymptotic limit.
We examine the performance of our security proof for a different total number of rounds, while we fix the testing ratio at 10% and optimise over the coherent state amplitude α and the radial postselection parameter Δ_r via coarse-grained search. The resulting key rate curves can be seen in Figure 5.4. We see that, as expected, the secure key rates are lower than for the untrusted, ideal detector, but the maximal achievable transmission distances decrease only moderately compared

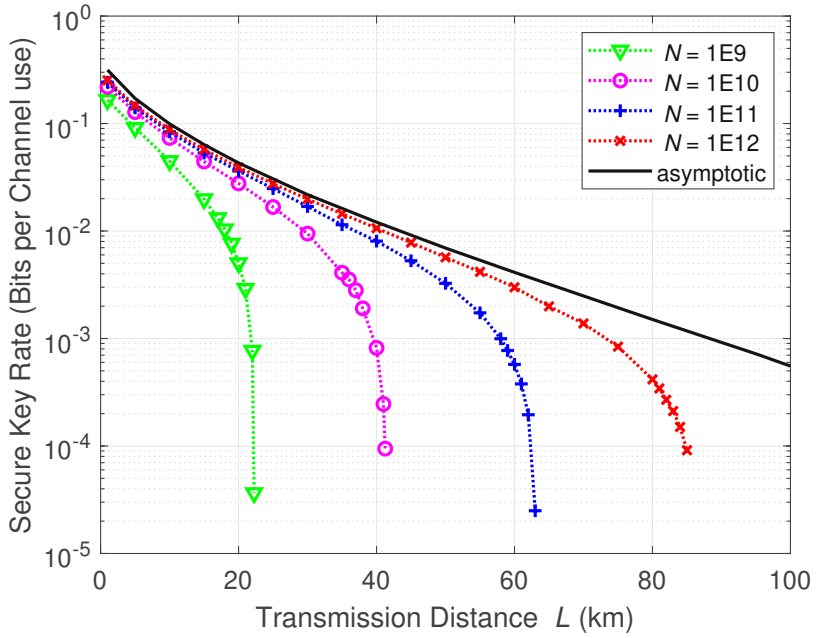

Figure 5.4.: Secure key rates over transmission distance L for trusted, non-ideal detector for with $\nu_{\text{el}} = 0.04$ and $\eta_d = 0.72$. We plot key rates for different total number of signals N for optimised the coherent state amplitude α and the radial postselection parameter Δ_r and fixed testing ratio TR = 10%.

to the untrusted detector with the same excess noise level. For $N = 10^9$ signals we observe positive key rates up to 22 km (compared to 26 km for untrusted, ideal detectors), for $N = 10^{10}$ we obtain non-negative key rates up to 41 km (compared to 45 km), for $N = 10^{11}$ up to 63km (compared to 65 km) and for $N = 10^{12}$ up to 85 km (compared to 86 km). We see that the difference in maximal achievable transmission distance between the untrusted, ideal and the trusted, non-ideal detector scenario decreases with increasing N.

In Figure 5.5, we plot the obtained secure key rates as a function of the transmission distance L for different testing ratios, while we fix $N = 10^{12}$ and optimise over the coherent state amplitude α and the radial postselection parameter Δ_r. As expected the obtained secure key rates are lower than those for the untrusted, ideal detector. However, for an excess noise level of $\xi = 0.01$, it turns out that the maximal achievable transmission distances do not differ significantly in the trusted detector scenario. For example, when the testing rate is 60% of the signals, the maximal achievable transmission distance for the trusted, non-ideal detector is 100km while in the untrusted, ideal detector case we obtained 101km. Therefore, even for

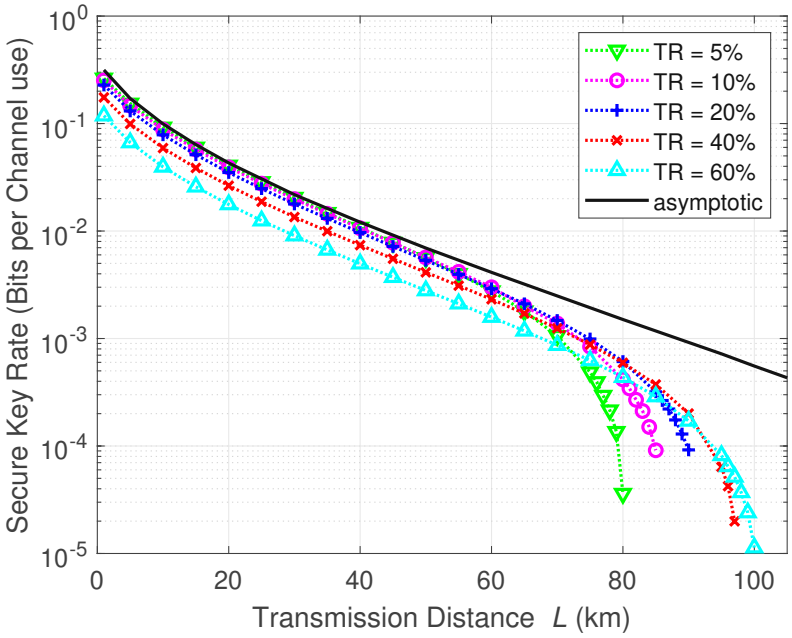

Figure 5.5.: Secure key rates over transmission distance L for a trusted, non-ideal detector with $\nu_{\text{el}} = 0.04$ and $\eta_d = 0.72$. We fixed $N = 10^{12}$, optimised the coherent state amplitude α and the postselection parameter Δ_r and examined different testing ratios TR.

realistic detectors, our method yields practically relevant secure finite-size key rates. We note that this small difference between key rates using ideal, untrusted detectors and noisy, trusted detectors was already observed for the asymptotic case in [106, Section 5.3]. The reason behind this is that Bob's noisy observables can be related to his ideal observables by linear combinations. Hence, effectively, the feasible set remains unchanged, while only the objective function changes due to the POVM elements of the noisy, non-ideal heterodyne detector.

6. Conclusion

Summing up, in this work we provide a composable finite-size security proof for discretely modulated continuous-variable security proof against i.i.d. collective attacks. We introduce and prove a new, noise-robust energy testing theorem that allows to bound the weight of quantum states outside a finite-dimensional cutoff space based on experimental observations. This theorem is a key ingredient for our proof, but can turn out to be useful in related contexts and other proof attempts as well. Having bound the dimension of Bob's system, we apply Renner's finite-size security proof framework [85] and extend it to cover infinite-dimensional side-information. After applying the dimension reduction method [105] to rigorously take the influence of the cutoff into account, we obtain a lower bound on the secure finite-size key rate against i.i.d. collective attacks. To calculate the secure key rate, it remains to solve a highly nonlinear semi-definite program over a subset of a finite-dimensional Hilbert space. We tackle this by applying the numerical method presented in [19, 110] and extending it to the structure of our finite-size optimisation problem. This allows us to obtain tight lower bounds on the secure key rate. Our analysis covers both the theoretically interesting case of ideal, untrusted detectors on Bob's side, as well as the practically relevant case of non-ideal detectors with trusted detection noise. We demonstrate our general method for a quadrature phase-shift keying protocol and show that secure finite-size keys can be obtained up to about 100km transmission distance under experimentally viable conditions.

Besides that, we discuss numerical improvements of the security proof method that enable a quicker and more efficient computation of secure key rates. As computation time is a crucial factor for numerical security proofs, this marks an important improvement towards higher practicality.

This work, therefore, is another significant step towards widespread practical deployment of QKD systems, which will be essential for future secret communication. We expect immediate practical implications as we provide a security proof that can be used to calculate tight secure finite-size key rates for experimental DM CV-QKD systems under realistic conditions. Furthermore, the numerical approach allows us to be very flexible regarding changes in the protocol structure and therefore is able to deal with postselection and can easily be adapted to take more refined physical models into account.

6.1. Outlook

However, this work does not mark the end of the road for DM CV-QKD protocols and their security proofs. While we prove security against i.i.d. collective attacks, probably the most interesting task, left for future work, is lifting our analysis to general attacks. While there are several methods known that lift secure key rates against collective attacks to secure key rates against coherent attacks, not all of them can be applied directly. For example, the quantum de Finetti theorem [86] and the postselection technique [18] depend on the dimension of the considered quantum system, which even after applying our energy test, strictly speaking, is still infinite-dimensional. We would require a chain rule for smooth min-entropies that allows us to remove infinite-dimensional registers, which is not feasible. We note that this is even an overlooked technical detail in the de Finetti paper by Renner and Cirac [86]. Therefore, there seems to be no immediate solution and it might require alternative techniques to circumvent this issue. However, simply imposing a photon-number cutoff, our ideas can be adapted to handle coherent attacks by applying methods similar to those developed in Ref. [36].
An interesting alternative is provided by the Entropy Accumulation Theorem (EAT), in particular, the recently developed Generalised Entropy Accumulation Theorem (GEAT) [71] that allows for analysing prepare-and-measure protocols. However, due to the novelty of this technique, not all difficulties and challenges when applying to DM CV-QKD protocols are immediately obvious. It remains an interesting task for the future to combine both results.
We expect that there are feasible ways to lift our collective attack proof to coherent attacks and leave analyses in this direction for future work.

APPENDIX

A. Proof of the energy testing theorem

In this section, we are going to prove our energy testing theorem (Theorem 4.4.1) for both ideal detectors and trusted non-ideal detectors. We begin with the proof for ideal detectors.

Proof. We start by proving an operator inequality related to heterodyne measurements, similarly to Lemma III.2 in [86] for homodyne detection. We define the following operators

$$W_1 := P^{\frac{\hat{q}^2+\hat{p}^2-1}{2} \geqslant n_c}, \tag{A.1}$$

$$V_1 := \frac{1}{\pi} \int_{|\alpha|^2 \geqslant \beta_{\text{test}}^2} |\alpha\rangle\langle\alpha| \, d\mu_\alpha, \tag{A.2}$$

where W_1 is the projector onto the span of the eigenvectors of the operator $\frac{\hat{q}^2+\hat{p}^2-1}{2}$ corresponding to (generalized) eigenvalues greater or equal to n_c, and V_1 describes our test measurement, where the heterodyne detection gives outcomes with amplitudes greater or equal to β_{test}. Defining $W_0 := \mathbb{1} - W_1$ and $V_0 := \mathbb{1} - V_1$, it can be easily seen that $\{V_0, V_1\}$ and $\{W_0, W_1\}$ form POVMs.
Recall, that the photon-number operator is defined as $\hat{n} = \frac{1}{2}(\hat{q}^2 + \hat{p}^2 - 1)$. One observes $W_1 := \sum_{n \geqslant n_c} |n\rangle\langle n|$ and, using $\langle \gamma e^{i\theta}|n\rangle = \frac{e^{-\frac{\gamma^2}{2}} \gamma^n e^{-i\theta n}}{\sqrt{n!}}$ (see, for example [2, p. 37]), it can be seen that $V_1 = \sum_{n\in\mathbb{N}} \frac{\Gamma(n+1,\beta_{\text{test}})}{\Gamma(n+1,0)} |n\rangle\langle n|$. Therefore, comparing the coefficients of V_1 and W_1 and recalling that for fixed first argument the incomplete gamma function is monotonically decreasing in its second argument, we conclude $\langle n|W_1|\rangle n \leqslant 1 \leqslant \frac{\Gamma(n_c+1,0)}{\Gamma(n_c+1,\beta_{\text{test}})} \langle n|V_1|n\rangle \; \forall n \in \mathbb{N}$. Hence, we found

$$W_1 \leqslant \frac{\Gamma(n_c+1,0)}{\Gamma(n_c+1,\beta_{\text{test}})} V_1. \tag{A.3}$$

To ease notation, we define $r^{\text{ideal}}(n_c,\beta) := \frac{\Gamma(n_c+1,0)}{\Gamma(n_c+1,\beta_{\text{test}})}$. The operator W_0 is the projector onto the cutoff space $\mathcal{H}^{n_c}$ and W_1 projects onto the orthogonal complement of the cutoff space. Therefore,

$$w = \mathbb{E}\left[W_1\right] = \text{Tr}\left[\rho W_1\right] \leqslant r^{\text{ideal}}(n_c,\beta_{\text{test}}) \text{Tr}\left[\rho V_1\right] = r^{\text{ideal}}(n_c,\beta_{\text{test}}) \mathbb{E}\left[V_1\right].$$

Hence, $\frac{w}{r^{\text{ideal}}(n_c,\beta_{\text{test}})} \leqslant \mathbb{E}\left[V_1\right]$.
Next, we express the probability that the test passes but the photon number cutoff space does not contain most of the weight. We define the binary vector $\vec{f}_{k_T}$ to be of size k_T, containing a 0 in its k-th entry if the energy test for round k passes (so if the outcome of the POVM $\{V_0, V_1\}$ is '0') and 1 otherwise. To ease the notation, we use the shortcut r for $r^{\text{ideal}}(n_c, \beta_{\text{test}})$ and denote the hamming weight of a vector $\vec{v}$ by $\text{HW}(\vec{v})$.

$$\begin{aligned}
&\Pr\left[\max_{i=1,\ldots,k_T} Y_i < \beta^2 \text{ for all but } l_T \text{ rounds } \wedge \operatorname{Tr}[\rho W_1] \geqslant w\right] \\
\leqslant &\Pr\left[\text{HW}(\vec{f}_{k_T}) \leqslant l_T \wedge \mathbb{E}\left[V_1\right] \geqslant \frac{w}{r}\right] \\
= &\sum_{i=0}^{l_T} \int_{\frac{w}{r}}^{1} Q_y^{k_T}\left(\text{HW}(\vec{f}_{k_T}) = i\right)\, dy,
\end{aligned}$$

where $Q_y^{k_T}(i)$ is the probability of drawing a sequence of type i for a fixed weight y when testing k_T i.i.d. random variables and the inequality can be explained by the relation in (A.3). We derive

$$\begin{aligned}
&\sum_{i=1}^{l_T} \int_{\frac{w}{r}}^{1} Q_y^{k_T}\left(\text{HW}(\vec{f}_{k_T}) = i\right)\, dy \\
&= \sum_{i=1}^{l_T} \int_{\frac{w}{r}}^{1} 2^{-k\left(H(P_{\vec{i}})+D(P_{\vec{i}}||Q)\right)}\, dy \\
&= \sum_{i=1}^{l_T} \int_{\frac{w}{r}}^{1} 2^{k\left((1-\frac{i}{k_T})\log_2(1-y)+\frac{i}{k}\log_2(y)\right)}\, dy \\
&= \sum_{i=1}^{l_T} \int_{\frac{w}{r}}^{1} (1-y)^{k-i} y^i\, dy \\
&\leqslant \sum_{i=1}^{l_T} \binom{l_T}{i} \int_{\frac{w}{r}}^{1} (1-y)^{k_T-i} y^i\, dy = \int_{\frac{w}{r}}^{1} (1-y)^{k_T-l_T} \sum_{i=1}^{l_T} \binom{l_T}{i} (1-y)^{l_T-i} y^i\, dy \\
&= \int_{\frac{w}{r}}^{1} (1-y)^{k_T-l_T}(1-y)^{k_T-l_T}\, dy = \frac{\left(1-\frac{w}{r}\right)^{k_T-l_t+1}}{k_T-l_T+1},
\end{aligned}$$

where the first equality follows from [20, Theorem 12.1.2]. Naming the last expression ϵ_{ET} concludes the proof. □

It remains to prove the energy testing theorem for trusted, non-ideal detectors. The second part of the proof follows the arguments of the proof for ideal detectors. However, the measurement operator for trusted, non-ideal detectors differs from

the measurement operator V_1 for the ideal detector. Therefore it remains to show that the measurement operator for the trusted, non-ideal case dominates W_1 as well (possibly with another constant $r(n_c, \beta_{\text{test}})$.

Proof. According to [63] the POVM elements for the trusted, non-ideal heterodyne measurement with efficiency η_d and electronic noise ν_{el} are given by

$$G_y = \frac{1}{\eta_d \pi} \hat{D}\left(\frac{y}{\sqrt{\eta_d}}\right) \hat{\rho}_{\text{th}}\left(\overline{n}_d\right) \hat{D}^\dagger\left(\frac{y}{\sqrt{\eta_d}}\right), \tag{A.4}$$

where $\overline{n}_d := \frac{1-\eta_d+\nu_{\text{el}}}{\eta_d}$. Therefore, the modified measurement operator is $\tilde{V}_1 := \int_{y^2 \geqslant \beta^2} G_y \; d\mu_y$. We use [72, Eq. (6.13) and (6.14)] to express G_y in the number basis. For simplification, we define $C_{n,m} := \frac{1}{\pi \eta_d^{\frac{m-n}{2}+1}} \sqrt{\frac{n!}{m!}} \frac{\overline{n}_d^n}{(1+\overline{n}_d)^{m+1}}$, $a := \frac{1}{\eta_d(1+\overline{n}_d)}$ and $b := \eta_d \overline{n}_d (1+\overline{n}_d)$, and obtain for $n \leqslant m$

$$\langle n|G_y|m\rangle = C_{n,m} e^{-a|y|^2} (y^*)^{m-n} L_n^{(m-n)}\left(-\frac{|y|^2}{b}\right), \tag{A.5}$$

where

$$L_k^\alpha(x) = \sum_{j=0}^{k} (-1)^j \binom{k+\alpha}{k-j} \frac{x^j}{j!} \tag{A.6}$$

is the generalised Laguerre polynomial of degree k and with parameter α [76]. The following calculation is a special case of the derivation in [56, Appendix G].

$$\begin{aligned}
\tilde{V}_1 &= \int_{y^2 \geqslant \beta^2} G_y \; d\mu_y \\
&= \sum_{m,n} C_{n,m} |n\rangle\langle n| \int_{y^2 \geqslant \beta^2} y^{m-n+1} e^{-a y^2} L_n^{(m-n)}\left(-\frac{y^2}{b}\right) \; dy \int_{\theta=0}^{2\pi} e^{-i\theta} \; d\theta \\
&= \sum_{m,n} C_{n,m} |n\rangle\langle m| \int_{y^2 \geqslant \beta^2} y^{m-n+1} e^{-a y^2} L_n^{(m-n)}\left(-\frac{y^2}{b}\right) \; dy \; 2\pi \delta_{n,m} \\
&= 2\pi \sum_{n} C_{n,n} |n\rangle\langle n| \int_{y^2 \geqslant \beta^2} y e^{-a y^2} L_n\left(-\frac{y^2}{b}\right) \; dy \\
&= \pi \sum_{n} C_{n,n} |n\rangle\langle n| \int_{z \geqslant \beta} e^{-az} L_n\left(-\frac{z}{b}\right) \; dz \\
&= \pi \sum_{n} C_{n,n} |n\rangle\langle n| \sum_{j=0}^{n} \binom{n}{n-j} \frac{1}{a^{j+1} b^j} \frac{\Gamma(j+1, \beta_{\text{test}})}{\Gamma(j+1)} \; dz
\end{aligned}$$

Note that we substituted $y^2 \mapsto z$ for the fifth equality and that we used the definition of the Laguerre polynomials to obtain the last line. Inserting $C_{n,n}$ and simplifying the obtained expression yields

$$\tilde{V}_1 = \sum_n \left(\frac{\overline{n}_d}{1+\overline{n}_d}\right)^n \sum_{j=0}^{n} \binom{n}{j} \left(\frac{1}{\overline{n}_d}\right)^j \frac{\Gamma(j+1,\beta_{\text{test}})}{\Gamma(j+1)} |n\rangle\langle n|.$$

We define and simplify

$$\begin{aligned} U :=& \frac{\Gamma(1,\beta)}{\Gamma(1)} \sum_n \left(\frac{\overline{n}_d}{1+\overline{n}_d}\right)^n \sum_{j=0}^{n} \binom{n}{j} \left(\frac{1}{\overline{n}_d}\right)^j |n\rangle\langle n| \\ =& \Gamma(1,\beta) \sum_n \left(\frac{\overline{n}_d}{1+\overline{n}_d}\right)^n \left(\frac{1}{\overline{n}_d}+1\right)^n |n\rangle\langle n| \\ =& \Gamma(1,\beta) \sum_n |n\rangle\langle n|. \end{aligned}$$

Note that the quotient $\frac{\Gamma(j+1,\beta_{\text{test}})}{\Gamma(j+1)}$ is monotonically increasing in j, therefore $\forall j \in \mathbb{N}: \frac{\Gamma(1,\beta_{\text{test}})}{\Gamma(1)} \leqslant \frac{\Gamma(j+1,\beta_{\text{test}})}{\Gamma(j+1)}$. Hence, $U \leqslant \tilde{V}_1$. Based on the structure of W_1, we observe $W_1 \leqslant \frac{1}{\Gamma(1,\beta_{\text{test}})} U$. Defining $r^{\text{non-ideal}}(\beta_{\text{test}}) := \frac{1}{\Gamma(1,\beta_{\text{test}})}$ and combining our operator relations, we obtain

$$W \leqslant r^{\text{non-ideal}}(\beta_{\text{test}}) U \leqslant r^{\text{non-ideal}}(\beta_{\text{test}}) \tilde{V}_1. \tag{A.7}$$

The rest of the proof is the same as for the ideal case, where every $r^{\text{ideal}}(n_c, \beta_{\text{test}})$ needs to be replaced by $r^{\text{non-ideal}}(\beta_{\text{test}})$. □

B. Detailed Derivations for the Security Proof

In this section, we present and prove technical theorems and lemmas that we use in the security proof to generalise existing finite-dimensional statements to their infinite-dimensional counterparts.

B.1. Technical Lemmas

Lemma B.1.1

If $|\Psi\rangle \in \mathcal{S}_1(\mathcal{H})$, there exists a Borel measure ν on $\mathcal{S}_1(\mathcal{H})$ such that

$$\left\| |\Psi\rangle^{\otimes n} - \int_{\sigma \in \mathcal{S}_1(\mathcal{H})} \sigma^{\otimes n} \nu(\sigma) \right\|_1 = 0.$$

Proof. The idea of the proof is to directly construct this point-measure ν on Borel($\mathcal{S}_1(\mathcal{H})$). Therefore, let $\nu(\{|\Psi\rangle\}) = 1$ as well as $\nu(\mathcal{S}_1(\mathcal{H})) = 1$. Note that the latter condition makes ν automatically normalised. Countable additivity is satisfied since at most one disjoint set can contain $|\Psi\rangle$. Using countable additivity, we obtain $\nu(\{|\Psi\rangle\}) = \nu(\{|\Psi\rangle\} \cup \varnothing) = \nu(\{|\Psi\rangle\}) + \nu(\varnothing)$ and conclude that $\nu(\varnothing) = 0$. Finally, for any Borel set $\mathcal{A} \subseteq \mathcal{S}_1(\mathcal{H})$ we have $\nu(\mathcal{A}) = \begin{cases} 0 & \text{if } |\Psi\rangle \notin \mathcal{A} \\ 1 & \text{otherwise.} \end{cases}$ Therefore, we conclude that ν is a Borel measure. □

Proposition B.1.2: Relation between ϵ-Balls

For $\rho \in \mathcal{D}_{\leqslant}(\mathcal{H})$ we have $\mathcal{B}^{\epsilon}_{PD}(\rho) \subseteq \mathcal{B}^{2\epsilon}_{TD}(\rho) \subseteq \mathcal{B}^{\sqrt{2\epsilon}}_{PD}(\rho)$.

Proof. Consider $\rho \in \mathcal{D}_{\leqslant}(\mathcal{H})$ and $\sigma \in \mathcal{B}^{\epsilon}_{\mathrm{PD}}(\rho)$.
For the first inclusion, by one of the Fuchs-van de Graaf inequalities (Eq. (2.5)), we have $\Delta(\rho, \sigma) \leqslant \mathcal{P}(\rho, \sigma) \leqslant \epsilon$, hence if $\sigma \in \mathcal{B}^{\epsilon}_{\mathrm{PD}}(\rho)$, we have $2\Delta(\rho, \sigma) \leqslant 2\epsilon$. Thus, due to the definition of the trace-distance ball (without a factor $\frac{1}{2}$), every $\sigma \in \mathcal{B}^{\epsilon}_{\mathrm{PD}}(\rho)$ is contained in $\mathcal{B}^{2\epsilon}_{\mathrm{TD}}(\rho)$.

For the second inclusion, assume $\sigma \in \mathcal{B}^{2\epsilon}_{\mathrm{TD}}(\rho)$. Then, by the other Fuchs-van de Graaf inequality in Eq. (2.5), we have $\mathcal{P}(\rho,\sigma) \leqslant \sqrt{2\Delta(\rho,\sigma)} \leqslant \sqrt{2\epsilon}$. Hence, if $\sigma \in \mathcal{B}^{2\epsilon}_{\mathrm{TD}}(\rho)$ it is as well contained in $\mathcal{B}^{\sqrt{2\epsilon}}_{\mathrm{PD}}$. □

Lemma B.1.3: Data-Processing Inequality for the Trace Distance under CPTNI Maps

Let $\mathcal{H}$ be a separable Hilbert space and let ρ, σ be compact, self-adjoint trace-class-1 operators over the separable Hilbert space $\mathcal{H}$ and let $\mathcal{E}$ be a completely positive trace non-increasing (CPTNI) map.
Then,

$$||\mathcal{E}(\rho) - \mathcal{E}(\sigma)||_1 \leqslant ||\rho - \sigma||_1 .$$

Proof. Consider ρ, σ compact, self-adjoint and trace-class-1 operators, as in the statement. Then, trivially, $\rho - \sigma$ is self-adjoint as well.
Furthermore, we show that $\rho - \sigma$ is compact. Since ρ is compact, for all bounded sequences $(x_n)_{n\in\mathbb{N}} \subseteq \mathcal{H}$ there exists a subsequence $(x_{n_k})_{k\in\mathbb{N}}$ such that $(\rho x_{n_k})_{k\in\mathbb{N}}$ converges for $k \to \infty$. Clearly, $(x_{n_k})_{k\in\mathbb{N}}$ is bounded as well. Similarly, since σ is compact according to assumption, there exists a subsequence $\left(x_{n_{k_l}}\right)_{l\in\mathbb{N}} \subseteq \mathbb{H}$ such that $(\sigma n_{k_l})_{l\in\mathbb{N}}$ converges for $l \to \infty$. Summing up, for every sequence $(x_n)_{n\in\mathbb{N}} \subseteq \mathcal{H}$ we found a subsequence $\left(x_{n_{k_l}}\right)_{l\in\mathbb{N}}$ such that both $\left(\rho_{n_{k_l}}\right)_{l\in\mathbb{N}}$ and $\left(\sigma_{n_{k_l}}\right)_{l\in\mathbb{N}}$ converge for $l \to \infty$. Since the difference of convergent sequences converges, $\left((\rho-\sigma)x_{n_{k_l}}\right)_{l\in\mathbb{N}}$ converges as well. Hence, $\rho - \sigma$ is compact.
Now we may apply the spectral theorem for compact, self-adjoint operators on $\rho - \sigma$ and find an orthonormal basis diagonalising $\rho - \sigma$. Let P be the positive part and Q the negative part of the diagonal form of $\rho - \sigma$, $\rho - \sigma = U(P + Q)U^\dagger$, where $P \perp Q$. Note that we found P, Q diagonal, $P \perp Q$ with $||\rho-\sigma||_1 = ||P+Q||_1$. Since $\mathcal{E}$ is a CPTNI map, we can find a Kraus representation $\mathcal{E}(\tau) = \sum_i K_i \tau K_i^\dagger$ where $\sum_i K_i^\dagger K_i = \mathbb{1}$. Inserting $\tau = UDU^\dagger$, where D is the diagonal form and U the corresponding transformation, we obtain

$$\mathcal{E}(\tau) = \mathcal{E}(U\tau U^\dagger) = \sum_i K_i U D U^\dagger K_i^\dagger = \sum_i K_i U D \left(K_i U\right)^\dagger = \sum_i \tilde{K}_i D \tilde{K}_i^\dagger.$$

Note that we defined $\tilde{K}_i := K_i U$ and observe

$$\sum_i \tilde{K}_i^\dagger \tilde{K}_i \tilde{K}_i^\dagger = \sum_i \left(K_i U\right)^\dagger K_i U = U^\dagger \left(\sum_i K_i^\dagger K_i\right) U = U^\dagger U = \mathbb{1}.$$

Define the new channel $\tilde{\mathcal{E}}(\tau) = \sum_i \tilde{K}_i \tau \tilde{K}_i^\dagger$. Finally, we conclude

$$\begin{aligned}||\mathcal{E}(\rho) - \mathcal{E}(\sigma)||_1 =& ||\mathcal{E}(\rho - \sigma)||_1 = ||\tilde{\mathcal{E}}(P+Q)||_1 = ||\tilde{\mathcal{E}}(P) + \tilde{\mathcal{E}}(Q)||_1 \\ \leqslant& ||\tilde{\mathcal{E}}(P)||_1 + ||\tilde{\mathcal{E}}(Q)||_1 = \mathrm{Tr}\left[\tilde{\mathcal{E}}(P)\right] + \mathrm{Tr}\left[\tilde{\mathcal{E}}(Q)\right] \\ \leqslant& \mathrm{Tr}\left[P\right] + \mathrm{Tr}\left[Q\right] = \mathrm{Tr}\left[P+Q\right] = ||P+Q||_1 \\ =& ||\rho - \sigma||_1,\end{aligned}$$

which proves the claim.

□

Lemma B.1.4: Leftover Hashing Lemma against Infinite-Dimensional Side-Information

Let $\rho_{XE} \in \mathcal{D}_{\leqslant}(\ell_X^\infty \otimes \mathcal{H}_E)$, where X is finite. Let $\epsilon' > 0$ such that $\epsilon_{PA} := 2(\epsilon_{sec} - 2\epsilon')$, where $\epsilon_{sec} \geqslant 2\epsilon' + \frac{1}{2}\sqrt{2^{\ell - H^{\epsilon'}_{min(PD)}(X|E)_\rho}}$ in case of purified-distance smoothing and in case of trace-distance smoothing $\epsilon_{sec} \geqslant 2\epsilon' + \frac{1}{2}\sqrt{2^{\ell - H^{2\epsilon'}_{min(TD)}(X|E)_\rho}}$.
Then for the purified-distance smoothing ball, if

$$\ell \leqslant H^{\epsilon'}_{min(PD)}(X|E)_\rho - 2\log_2\left(\frac{1}{\epsilon_{PA}}\right),$$

or, for the trace-distance smoothing ball, if

$$\ell \leqslant H^{2\epsilon'}_{min(TD)}(X|E)_\rho - 2\log_2\left(\frac{1}{\epsilon_{PA}}\right),$$

the obtained key is ϵ_{sec}-secure.

Proof. We start the proof with [8, Proposition 21] for the case $|K| = 2^\ell$ since we are interested in bit-strings. Then, Proposition 21 states that for X, K, two sets of finite cardinality with $|K| = 2^\ell \leqslant |X|$, $\{\mathcal{F}, \mathcal{P}_\mathcal{F}\}$, a family of two-universal $\{X, K\}$-hash functions, $\rho_{XE} = (\rho_E^x)_{x\in X} \in \mathcal{D}_{\leqslant}(\ell_X^\infty \otimes \mathcal{M}_E)$ and $\epsilon' > 0$

$$\mathbb{E}_\mathcal{F}||(T_f \otimes \mathrm{id}_E)(\rho_{XE}) - \pi_K \otimes \rho_E||_1 \leqslant \sqrt{2^{\ell - H^{\epsilon'}_{\min}(X|E)_\rho}} + 4\epsilon'$$

holds. Here $\mathbb{E}_\mathcal{F}$ denotes the expectation with respect to $\mathcal{P}_\mathcal{F}$, T_f is the map applying the hash function and $\pi_K = \frac{1}{|K|}\sum_{s\in K} |s\rangle\langle s|$. . Note that K denotes the alphabet the hash function map into and that Ref. [8] uses the purified distance in the smooth min-entropy definition.

First, we rewrite the left-hand side

$$\begin{aligned}
&\mathbb{E}_{\mathcal{F}}||(T_f \otimes \mathrm{id}_E)(\rho_{XE}) - \pi_k \otimes \rho_E||_1 \\
&= \sum_f p(f)||T_f \otimes \mathrm{id}_E)(\rho_{XE}) - \pi_K \otimes \rho_E||_1 \\
&= \left|\left| \sum_f p(f) \left[T_f \otimes \mathrm{id}_E)(\rho_{XE}) - \pi_K \otimes \rho_E\right] \otimes |f\rangle\langle f| \right|\right|_1 \\
&= ||\rho_{F(x)EF} - \pi_K \otimes \rho_{EF}||_1.
\end{aligned}$$

We replace the left-hand side of the original statement with what we just derived and divide by two to obtain a statement in trace-distance and obtain

$$\frac{1}{2}||\rho_{F(x)EF} - \pi_k \otimes \rho_{EF}||_1 \leqslant 2\epsilon' + \frac{1}{2}\sqrt{2^{\ell - H^{\epsilon'}_{\min(\mathrm{PD})}(X|E)_\rho}} \leqslant \epsilon_{\mathrm{sec}}.$$

Let $\epsilon_{\mathrm{PA}} := 2(\epsilon_{\mathrm{sec}} - 2\epsilon') > 0$. Then, we derive

$$2^{\ell - H^{\epsilon'}_{\min(\mathrm{PD})}(X|E)_\rho} \leqslant \epsilon^2_{\mathrm{PA}} = 4(\epsilon_{\mathrm{sec}} - 2\epsilon')^2 \Rightarrow \ell \leqslant H^{\epsilon'}_{\min(\mathrm{PD})}(X|E)_\rho - 2\log_2\left(\frac{1}{\epsilon_{\mathrm{PA}}}\right).$$

This gives us the statement in purified-distance smoothing. By Proposition B.1.2, we yield the proposed statement in trace-distance smoothing. □

Lemma B.1.5: Chain Rule for Smooth min-Entropies

Let $\mathcal{H}_A, \mathcal{H}_B, \mathcal{H}_C$ be separable Hilbert spaces with $|\mathcal{H}_B| = n$.
Then for smoothing in trace-distance,

$$H^{\epsilon}_{min(TD)}(AB|C)_\rho - \log_2(n) \leqslant H^{\epsilon}_{min(TD)}(A|BC)_\rho,$$

as well as for smoothing in purified distance

$$H^{\epsilon}_{min(PD)}(AB|C)_\rho - \log_2(n) \leqslant H^{\epsilon}_{min(PD)}(A|BC)_\rho,$$

Proof. The proof in purified-distance smoothing can be found in [32, Lemma 4.5.6] and it is straightforward to show that the proof given there works for trace-distance smoothing as well. □

Lemma B.1.6: Removing a Classical Communication Register

Let $\mathcal{H}_C, \mathcal{H}_{E'}$ and $\mathcal{H}_X$ be separable Hilbert spaces and $\dim(\mathcal{H}_C) < \infty$ as well as $\dim(\mathcal{H}_X) < \infty$, where X is the raw key and C the transcript of the communication between Alice and Bob. Let $\rho \in \mathcal{D}(\mathcal{H}_X \otimes \mathcal{H}_{E'} \otimes \mathcal{H}_C)$ and let $\rho_{XE'} \in \mathcal{D}(\mathcal{H}_X \otimes \mathcal{H}_{E'})$ be the state after tracing out the register C.
Then both for smoothing in trace-distance,

$$H^{\epsilon}_{min(TD)}(X|E'C)_\rho \geqslant H^{\epsilon}_{min(TD)}(X|E')_\rho - leak_{EC}$$

Proof. This proof follows closely the proof of [91, Lemma 2]. We define Y to be the other party's local information used during information reconciliation and start with the left-hand side of the statement,

$$\begin{aligned} H^{\epsilon}_{\min(\mathrm{TD})}(X|E'C)_\rho &\geqslant H^{\epsilon}_{\min(\mathrm{TD})}(XC|E')_\rho - \log_2(|C|) \\ &\geqslant H^{\epsilon}_{\min(\mathrm{TD})}(X|E')_\rho + H_{\min(\mathrm{TD})}(C|XE')_\rho - \log_2(|C|) \\ &\geqslant H^{\epsilon}_{\min(\mathrm{TD})}(X|E')_\rho + H_{\min(\mathrm{TD})}(C|XYE')_\rho - \log_2(|C|) \\ &\geqslant H^{\epsilon}_{\min(\mathrm{TD})}(X|E')_\rho + H_{\min(\mathrm{TD})}(C|XYE')_\rho - \log_2(|C|). \end{aligned}$$

The first inequality follows from the chain rule for smooth-min entropies (Lemma B.1.5) and the second inequality is an extension of [85, Lemma 3.2.10] for an infinite-dimensional register $C \to E'$. We remark that proving this extension requires extending the min-entropy part of [85, Lemma 3.1.8] which we have done in Lemma B.1.9 and [85, Lemma 3.1.1] where the proof for the infinite-dimensional case is identical to the proof given there. The third line is obtained by the strong subadditivity property of the smooth min-entropy (Lemma B.1.8) and the last inequality comes from the fact that $E' \leftrightarrow (X, E') \leftrightarrow C$ forms a Markov-chain since C is computed by Alice and Bob as a function of XY. Finally, since $\log_2(|C|)$ stands for the number of all possible information-reconciliation transcripts, we may replace it with the actual leakage $\mathrm{leak}_{\mathrm{EC}}$ giving the number of bits needed to implement the used information-reconciliation scheme. □

Proposition B.1.7: Discarding Classical Information cannot Increase Smooth min-Entropy [32, Lemma 4.5.7.]

Let $\mathcal{H}_A, \mathcal{H}_B$ and $\mathcal{H}_X$ be separable Hilbert spaces and $\dim(\mathcal{H}_X) < \infty$.
Then, in the purified distance,

$$H^{\epsilon}_{min(PD)}(A|B)_\rho \leqslant H^{\epsilon}_{min(PD)}(AX|B)_\rho. \tag{B.1}$$

Proof. See proof of Lemma 4.5.7. in [32]. □

Lemma B.1.8: Strong Subadditivity of Smooth min-Entropy

Let $\mathcal{H}_A, \mathcal{H}_B$ and $\mathcal{H}_C$ be separable Hilbert spaces and $\rho \in \mathcal{D}_{\leqslant}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$. Then, for either smoothing ball

$$H^{\epsilon}_{min(TD)}(A|BC)_{\rho} \leqslant H^{\epsilon}_{min(TD)}(A|B)_{\rho}.$$

$$H^{\epsilon}_{min(PD)}(A|BC)_{\rho} \leqslant H^{\epsilon}_{min(PD)}(A|B)_{\rho}.$$

Proof. The proof for trace-distance follows from [85, Lemma 3.2.7] which states the strong subadditivity for finite-dimensional Hilbert spaces since this proof only relies on [85, Lemma 3.1.7] (its proof is identical for separable Hilbert spaces) and the fact that the trace-distance is monotonic under CPTNI maps (which we have established in Lemma B.1.3). Therefore, it remains to prove the statement in purified distance smoothing.
Consider the map $\mathcal{E}(\omega_B) := \omega_B \otimes \mathbb{1}_C$. By the data-processing inequality [32, Proposition 4.5.1] for $\mathcal{E} : \mathcal{M}_{\overline{C}} \to \mathcal{M}_{\overline{B}}$ and $\omega \in \mathcal{D}_{\leqslant}(\mathcal{M}_{AB})$, where $\mathcal{M}$ stands for a von Neumann algebra and $\mathcal{E}^*$ denotes the dual map of $\mathcal{E}$, we obtain

$$H^{\epsilon}_{\min(\mathrm{PD})}(A|\overline{B})_{\omega} \leqslant H^{\epsilon}_{\min(\mathrm{PD})}(A|\overline{C})_{\mathrm{id}_A \otimes \mathcal{E}^*(\omega)}, \tag{B.2}$$

where the smoothing of the min-entropy is done in the purified distance. Letting $\mathcal{M}_{\overline{B}} := \mathcal{B}(\mathcal{H}_B) \otimes \mathcal{B}(\mathcal{H}_C)$ and $\mathcal{M}_{\overline{C}} = \mathcal{B}(\mathcal{H}_B)$ and $\omega = \rho$, we obtain

$$H^{\epsilon}_{\min(\mathrm{PD})}(A|BC)_{\rho} \leqslant H^{\epsilon}_{\min(\mathrm{PD})}(A|B)_{\mathrm{id}_{AB} \otimes \mathrm{Tr}_C[\rho]} = H^{\epsilon}_{\min(\mathrm{PD})}(A|B)_{\rho_{AB}}. \tag{B.3}$$

This completes the proof in the purified distance. □

Lemma B.1.9: Conditioning on Classical Register

Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be separable Hilbert spaces and Z a classical register. Consider $\rho_{ABZ} \in \mathcal{D}_{\leqslant}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \ell^{\infty}_Z)$.
Then we have

$$H^{\epsilon}_{min(TD)}(AB|Z)_{\rho} \geqslant \inf_{z \in (\lambda_z)_z} H^{\epsilon}_{min(TD)}(A|B)_{\rho^z_{AB}} \tag{B.4}$$

in trace distance and

$$H^{\epsilon}_{min(PD)}(AB|Z)_{\rho} \geqslant \inf_{z \in (\lambda_z)_z} H^{\frac{\epsilon^2}{2}}_{min(PD)}(A|B)_{\rho^z_{AB}} \tag{B.5}$$

in purified distance.

Proof. Since Z is a classical register, hence z's are mutually orthogonal, by the definition of the min-entropy (see Section 2.3.1) we have $\forall z$

$$\begin{aligned}&\lambda \mathrm{Tr}\left[\rho_{AB}^z\right] \sum_z \mathbb{1}_A \otimes |z\rangle\langle z| - \sum_z \rho_{AB}^z \otimes |z\rangle\langle z| \geqslant 0\\ \Leftrightarrow &\lambda \mathrm{Tr}\left[\rho_{AB}^z\right] \cdot \mathbb{1}_A - \rho_{AB}^z \geqslant 0.\end{aligned}$$

Therefore, again recalling the definition of the min-entropy, we obtain

$$H_{\min}(A|BZ) = \inf_z H_{\min}(A|B)_{\rho_{AB}^z}. \tag{B.6}$$

Using the definition of smoothed min-entropies, we know that for every $\delta > 0$ and for every $z \in Z$ there exists $\tilde{\rho}_{AB}^z \in \mathcal{B}^\epsilon(\rho_{AB}^z)$ such that

$$H_{\min}(\tilde{\rho}_{AB}^z||\rho_B^z) = \inf_z H_{\min}(\rho_{AB}^z||\rho_B^z) - \delta,$$

for example if we let $\tilde{\rho}_{AB}^z$ be the optimiser for the smooth min-entropy. Then, defining $\tilde{\rho}_{ABZ} := \sum_z \tilde{\rho}_{AB}^z$, we obtain from Eq. (B.6)

$$H_{\min}(\tilde{\rho}_{ABZ}||\rho_{BZ}) = \inf_z H_{\min}(\tilde{\rho}_{AB}^z||\rho_B^z) \geqslant H_{\min}^\epsilon(\rho_{AB}^z||\rho_B^z) - \delta.$$

It remains to show that $\tilde{\rho}_{ABZ}$ is in the smoothing ball of ρ_{ABZ}. We use the trace-distance ball, where $\tilde{\rho}_{ABZ}$ is guaranteed to be a subnormalized state. Therefore, following [85], we first prove Eq. (B.4)

$$||\tilde{\rho}_{ABZ} - \rho_{ABZ}||_1 = \inf_z ||\tilde{\rho}_{AB}^z - \rho_{AB}^z||_1 \leqslant \sum_z \mathrm{Tr}\left[\rho_{AB}^z\right] \epsilon \leqslant \epsilon,$$

which concludes the proof in trace-distance smoothing. Using Proposition B.1.2, we obtain Eq. (B.5).

□

Proposition B.1.10: Conditioning on an Independent Register

Let $\mathcal{H}_A, \mathcal{H}_B$ and $\mathcal{H}_C$ be separable Hilbert spaces and $\rho_{AB} \in \mathcal{D}_\leqslant(\mathcal{H}_{AB})$, $\rho_C \in \mathcal{D}_\leqslant(\mathcal{H}_C)$ and define $\rho_{ABC} := \rho_{AB} \otimes \rho_C$.
Then, the following smooth min-entropy relations hold

$$H_{min(TD)}^\epsilon(A|BC)_\rho = H_{min(TD)}^\epsilon(A|B)_\rho.$$

$$H_{min(PD)}^\epsilon(A|BC)_\rho = H_{min(PD)}^\epsilon(A|B)_\rho.$$

Proof. We prove two inequalities. The first one, $H_{\min}^\epsilon(A|BC)_\rho \leqslant H_{\min}^\epsilon(A|B)_\rho$ follows from the strong subadditivity property, proven in Lemma B.1.8 (for both smoothing balls). Therefore, it remains to prove the reverse direction.

Define the map $\Phi : X_{ABC} \mapsto X_{AB} \otimes \rho_C$, which traces off the register C of X_{ABC} and prepares ρ_C instead. As a composition of two CPTP maps, Φ is CPTP as well. By construction, ρ_{ABC} is invariant under Φ. Using the data processing inequality for smooth min-entropies, we obtain $H_{\min}^{\epsilon}(A|BC)_{\tilde{\rho}_{AB}\otimes\rho_C} \geqslant H_{\min}^{\epsilon}(A|BC)_{\tilde{\rho}_{ABC}}$. The data processing inequality for purified distance tells us that if $\tilde{\rho} \in \mathcal{B}_{\mathrm{PD}}^{\epsilon}(\rho)$ then $\Phi(\tilde{\rho}) \in \mathcal{B}_{\mathrm{PD}}^{\epsilon}(\rho)$ as well. Since the smooth min-entropy is defined via a supremum, we can restrict our considerations to states of the form $\tilde{\rho}_{AB} \otimes \rho_C$.

Finally, let for any $\tilde{\rho}_{AB} \in \mathcal{B}_{\mathrm{PD}}^{\epsilon}(\rho)$ the tuple (λ, σ_B) optimise $H_{\min}(A|B)_{\tilde{\rho}}$. Then, λ is the smallest real number satisfying $\lambda \mathbb{1}_A \otimes \sigma_B - \tilde{\rho}_{AB} \geqslant 0$. Then, since Φ is a CPTP map, $\lambda \mathbb{1}_A \otimes \sigma_B \otimes \rho_C - \tilde{\rho}_{AB} \otimes \rho_C \geqslant 0$. While λ optimised the first inequality, there might be a smaller λ satisfying the last inequality and therefore, $H_{\min}(A|B)_{\rho} \leqslant H_{\min}(A|BC)_{\rho}$. As this holds for any $\tilde{\rho}_{AB} \in \mathcal{B}_{\mathrm{PD}}^{\epsilon}(\rho)$ we can take the supremum and obtain $H_{\min}^{\epsilon}(A|B)_{\rho} \leqslant H_{\min}^{\epsilon}(A|BC)_{\rho}$, which completes the proof. The argument works similarly in trace-distance. □

B.2. Generalisation of the Asymptotic Equipartition Property

In this section, we generalise the asymptotic equipartition property [85, Corollary 3.3.7] to infinite dimensions. The proof there requires an ordering on the eigenvalues as well as the Birkhoff-von-Neumann theorem, so it needs some care to generalise the AEP statement to infinite dimensions. We note that in [32, 34] they extend the fully quantum asymptotic equipartition property to infinite dimensions. However, as noted in [36] this version is harder to apply numerically. The basic idea of our proof relies on the fact that the infinite-dimensional min-entropy can be converged via projections [34]. Before we come to the actual proof, it requires some preparations.

We start by extending the definition of the max-relative entropy to infinite dimensions.

Definition B.2.11: Infinite-Dimensional max-Relative Entropy

Let $\mathcal{H}_A$ be a Hilbert space and let $P, Q \in Pos(\mathcal{H}_A)$. Then the max-relative entropy is defined by

$$D_{max}(P||Q) = \inf\{\lambda : \ P \leqslant 2^{\lambda} Q\}.$$

Next, we prove that $D_{\max}$ is a Rényi-divergence just as in finite dimensions.

Proposition B.2.12: Properties of max-Relative Entropy

For the max-relative entropy, as defined in Eq. (B.2) the following holds

(1) Normalisation: $D_{max}(aP||bQ) = D_{max}(P||Q) + \log_2(a) - \log_2(b)$

(2) Dominance: For $P, Q, Q' \in Pos(\mathcal{H}_A)$ *and* $Q \leqslant Q'$ *we have* $D_{max}(P||Q) \geqslant D_{max}(P||Q')$.

Proof. We prove the two points separately.

(1) Let $\lambda^* := D_{\max}(P||Q)$ and $\lambda := D_{\max}(aP||bQ)$. Using the definition of the max-relative entropy, we obtain $P \leqslant 2^{\lambda^*}Q$ and $aP \leqslant 2^{\lambda}bQ$ which implies $P \leqslant 2^{\lambda}\frac{b}{a}Q$. Therefore, it follows $2^{\lambda^*} = 2^{\lambda}\frac{b}{a}$, hence $\lambda = \lambda^* + \log_2(a) - \log_2(b)$.

(2) Again, for $\lambda^* := D_{\max}(P||Q)$, we have $P \leqslant 2^{\lambda^*}Q$. Since $Q \leqslant Q'$, we have $P \leqslant 2^{\lambda^*}Q \leqslant 2^{\lambda^*}Q'$. So, λ^* is feasible for $D_{\max}(P||Q')$. Hence, it is an upper bound. This proves the claim.

□

Observe that $H_{\min}(\rho_{AB}||\sigma_B) = -D_{\max}(\rho_{AB}||\mathbb{1}_A \otimes \sigma_B)$, which gives us the following corollary.

Corollary B.2.13: Properties of min-Entropy

Let $\rho \in Pos(\mathcal{H}_A \otimes \mathcal{H}_B)$ *and* $\sigma, \sigma' \in Pos(\mathcal{H}_A)$ *such that* $\sigma \leqslant \sigma'$.
Then the following statements hold,

(1) Normalisation: $H_{min}(a\rho||b\sigma) = H_{min}(\rho||\sigma) - \log_2(a) + \log_2(b)$

(2) Dominance: $H_{min}(\rho||\sigma) \leqslant H_{min}(\rho||\sigma')$.

Definition B.2.14: Infinite-Dimensional Smooth Min Entropy

Let $\mathcal{H}_A$ *and* $\mathcal{H}_B$ *be separable Hilbert spaces and let* $\rho \in Pos(\mathcal{H}_A \otimes \mathcal{H}_B)$ *as well as* $\sigma \in Pos(\mathcal{H}_B)$.

For $\epsilon \in (0, \sqrt{\mathrm{Tr}\,[\rho]})$ *the smooth min-entropy is given by*

$$H^{\epsilon}_{min}(\rho||\sigma) := \sup_{\tilde{\rho} \in \mathcal{B}^{\epsilon}_{TD}(\rho)} H_{min}(\tilde{\rho}||\sigma).$$

Note that this coincides with the definition given in the main text (Section 2.3.1). Next, we want to generalise [34, Lemma 2]. Therefore, we introduce sequences of

projectors $\{\Pi^k\}_{k\in\mathbb{N}}$ onto finite-dimensional subspaces $U \subseteq \mathcal{H}$ of the relevant Hilbert space $\mathcal{H}$, that converge to the identity $\mathbb{1}_{\mathcal{H}}$ with respect to $||\cdot||_1$. Then we define a sequence of non-normalised projected states as $\hat{\rho}^k := \Pi^k\hat{\rho}\Pi^k$. For a more detailed description, we refer the reader to [34, Section II]. We note that the following could be trivially further generalised to a continuity claim for the smoothed max-relative entropy.

Lemma B.2.15

Let $\rho_B \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and let $\{\hat{\rho}^k_{AB}\}_{k=1}^{\infty}$ a sequence of normalised projected states converging to ρ_{AB} in the $||\cdot||_1$-norm. Let $\sigma_B \in \mathcal{D}(\mathcal{H}_B)$ and $\{\hat{\sigma}^k_B\}_{k=1}^{\infty}$ be a sequence of normalised projected states that converge to σ_B.
For any fixed $t \in (0,1)$ there exists $k_0 \in \mathbb{N}$ such that $\forall k \geqslant k_0$ we have

$$H^{\epsilon}_{min(TD)}(\rho_B||\sigma_B) \geqslant H^{t\epsilon}_{min(TD)}(\hat{\rho}^k_{AB}||\hat{\sigma}^k_B) + \log\left(Tr\left[\Pi^k_B\sigma\Pi^k_B\right]\right),$$

where the smoothing is done in trace-distance.

Proof. For fixed σ the statement can be established by showing

$$\forall k \geqslant k_0 : \ \mathcal{B}^{t\epsilon}_{\mathrm{TD}}\left(\hat{\rho}^k_{AB}\right) \subseteq \mathcal{B}^{\epsilon}_{\mathrm{TD}}(\rho_{AB}), \tag{B.7}$$

where the proof is then identical to the proof of [34, Lemma 2]. Therefore, we take this result as established, so $\exists k_0$ such that

$$\forall k \geqslant k_0 : \ H^{\epsilon}_{\min}(\rho||\sigma) \geqslant H^{\epsilon}_{\min}(\hat{\rho}^k_{AB}||\sigma). \tag{B.8}$$

We are using this result and Corollary B.2.13 to prove the general case. We deduce

$$\begin{aligned} H^{t\epsilon}_{\min(\mathrm{TD})}(\hat{\rho}^k_{AB}||\hat{\sigma}^k_B) &= H^{t\epsilon}_{\min(\mathrm{TD})}\left(\hat{\rho}^k_{AB}\left|\left|\frac{\sigma^k_B}{\mathrm{Tr}\left[\Pi^k_B\sigma\Pi^k_B\right]}\right.\right.\right) \\ &= H^{t\epsilon}_{\min(\mathrm{TD})}\left(\hat{\rho}^k_{AB}||\sigma^k_B\right) + \log\left(\frac{1}{\mathrm{Tr}\left[\Pi^k_B\sigma\Pi^k_B\right]}\right), \end{aligned}$$

where we applied the normalisation property in Corollary B.2.13 for the second equality. Then, using the dominance property in Corollary B.2.13 and noting that $\sigma \geqslant \Pi^k_B\sigma\Pi^k_B = \sigma^k$, we obtain

$$H^{t\epsilon}_{\min(\mathrm{TD})}\left(\hat{\rho}^k_{AB}||\sigma^k_B\right) \leqslant H^{t\epsilon}_{\min(\mathrm{TD})}\left(\hat{\rho}^k_{AB}||\sigma_B\right).$$

Putting things together, we showed

$$H^{t\epsilon}_{\min(\mathrm{TD})}(\hat{\rho}^k_{AB}||\hat{\sigma}^k_B) \leqslant H^{t\epsilon}_{\min(\mathrm{TD})}\left(\hat{\rho}^k_{AB}||\sigma_B\right) - \log\left(\mathrm{Tr}\left[\Pi^k_B\sigma\Pi^k_B\right]\right).$$

Thanks to the statement in Eq. (B.8) we know already that there exists such a k_0 to bound $H^{\epsilon}_{\min(\mathrm{TD})}(\hat{\rho}^k_{AB}||\sigma)$ from above. This completes the proof. □

In the next Lemma, we extend Renner's AEP [85, Theorem 3.3.6] to infinite-dimensional side-information. Note that we cannot generalise register A to infinite-dimensions, as the correction term is a function of the dimension of this register. However, this generalisation is not required for QKD anyways.

Lemma B.2.16

Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be separable Hilbert spaces where $\mathcal{H}_A$ is finite-dimensional, $|\mathcal{H}_A| < \infty$. Let $\rho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and $n \in \mathbb{N}$.
Then for any $\epsilon \in (0,1)$

$$\frac{1}{n} H^{\epsilon}_{min(TD)}(\rho_{AB}^{\otimes n} || \sigma_B^{\otimes n}) \geqslant H(AB)_\rho - H(B)_\rho - D(\rho_B || \sigma_B) - \delta,$$

where $\delta = 2 \log\left(rank(\rho_A) + \mathrm{Tr}\left[\rho_B^2 \left(\mathbb{1}_A \otimes \sigma_B^{-1}\right) + 2\right]\right) \sqrt{\frac{\log\left(\frac{1}{\epsilon}\right)}{n} + 1}$ *and smoothing is in terms of trace distance. In terms of purified distance, we replace $\epsilon \mapsto \sqrt{\epsilon}$.*

Proof. We follow the proof of [34, Proposition 8]. Let $\left(\Pi_A^k, \Pi_B^k\right)$ be sequences of projectors such that $\forall k' \geqslant k : \ \Pi_A^k \leqslant \Pi_A^{k'}$ that converges to the identity in the weak operator topology and similarly for the projectors in B. Then, the n-fold projectors $\left(\left(\Pi_A^k\right)^{\otimes n}, \left(\Pi_B^k\right)^{\otimes n}\right)$ satisfy these conditions as well.
Fix $t \in (0,1)$. Then, by Lemma B.2.15 there $\exists k_0 \in \mathbb{N}$ such that $\forall k \geqslant k_0$

$$H^{\epsilon}_{\min(\mathrm{TD})}\left(\rho_{AB}^{\otimes n} \middle|\middle| \sigma_B^{\otimes n}\right) \geqslant H^{t\epsilon}_{\min(\mathrm{TD})}\left(\left(\hat{\rho}_{AB}\right)^{\otimes n} \middle|\middle| \left(\hat{\sigma}_B\right)^{\otimes n}\right) - n \log\left(\mathrm{Tr}\left[\Pi^k \sigma \Pi^k\right]\right)$$

holds. We used that the trace is multiplicative over tensor products. Next, since we are working on projections, we can apply [85, Theorem 3.3.6] and obtain

$$\frac{1}{n} H^{\epsilon}_{\min(\mathrm{TD})}\left(\rho_{AB}^{\otimes n} \middle|\middle| \sigma_B^{\otimes n}\right) \geqslant H\left(\hat{\rho}_{AB}^k\right) - H\left(\hat{\rho}_B^k\right) - D\left(\hat{\rho}_B^k \middle|\middle| \hat{\sigma}_B^k\right) - \delta(t\epsilon) - \log\left(\mathrm{Tr}\left[\Pi^k \sigma \Pi^k\right]\right). \tag{B.9}$$

When we take the limit of $k \to \infty$ the left-hand side doesn't change, while the right-hand side, by our assumptions on the projections, recovers the true states. The log-term drops, as $\log\left(\mathrm{Tr}\left[\sigma\right]\right) = \log(1) = 0$. Hence, we obtain

$$\frac{1}{n} H^{\epsilon}_{\min(\mathrm{TD})}\left(\rho_{AB}^{\otimes n} \middle|\middle| \sigma_B^{\otimes n}\right) \geqslant H\left(\rho_{AB}\right) - H\left(\rho_B\right) - D\left(\rho_B || \sigma_B\right) - \delta(t\epsilon).$$

Finally, taking the limit $t \to 1$ completes the proof. □

We obtain the final result of this section, the generalised Asymptotic Equipartition Property, as a corollary.

Corollary B.2.17: Asymptotic Equipartition Property

Let $\mathcal{H}_X$ and $\mathcal{H}_E$ be separable Hilbert spaces, where $\mathcal{H}_X$ is finite-dimensional. Let ρ_{XE} be a classical-quantum state.
Then, for smoothing in terms of trace-distance

$$\frac{1}{n} H^{\epsilon}_{min(TD)}(X|E)_{\rho^{\otimes n}_{XE}} \geqslant H(X|E) - \delta(\epsilon),$$

where $\delta(\epsilon) := 2\log(rank(\rho_X)+3)\sqrt{\frac{\log(2/\epsilon)}{n}}$. For smoothing in terms of purified distance every ϵ needs to be replaced by $\sqrt{\epsilon}$.

Proof. The proof is now identical to [85, Corollary 3.3.7], where we omit the simplifications in the end of the proof. The purified-distance bound can be obtained by Proposition B.1.2. □

C. Derivation of the finite-dimensional optimisation problem

In this section, explain and derive the primal and dual SDP we have to solve in order to obtain a lower bound on the secure key rate. Our starting point is the infinite-dimensional optimisation problem, given in Eq. (4.16), that we obtain based on Bob's observations. By introducing slack variables, the inequality constraints can be turned into equality constraints.

$$
\begin{aligned}
&\min\ f(\rho)\\
&\text{s.t.}\\
&\qquad \mathrm{Tr}_B\left[\rho\right] = \rho_A,\\
&\qquad \left|\mathrm{Tr}\left[\hat{\Gamma}_j\rho\right] - \gamma_j\right| \leqslant \mu_j,\\
&\qquad \mathrm{Tr}\left[\rho\right] = 1,\\
&\qquad \rho \geqslant 0
\end{aligned}
\qquad \Leftrightarrow \qquad
\begin{aligned}
&\min\ f(\rho)\\
&\text{s.t.}\\
&\qquad \mathrm{Tr}_B\left[\rho\right] = \rho_A,\\
&\qquad \mathrm{Tr}\left[\hat{\Gamma}_j\rho\right] + a_j = \mu_j + \gamma_j,\\
&\qquad -\mathrm{Tr}\left[\hat{\Gamma}_j\rho\right] + b_j = \mu_j - \gamma_j,\\
&\qquad \mathrm{Tr}\left[\rho\right] = 1,\\
&\qquad \rho \geqslant 0,\\
&\qquad \vec{a}, \vec{b} \geqslant 0
\end{aligned}
$$

Next, we apply the dimension reduction method [105] and obtain the expanded finite-dimensional optimisation

$$
\begin{aligned}
&\min\ f(\overline{\rho})\\
&\text{s.t.}\\
&\quad \frac{1}{2}\left|\left|\mathrm{Tr}_B\left[\overline{\rho}\right]-\rho_A\right|\right|_1 \leqslant 2\sqrt{w},\\
&\quad \mu_j+\gamma_j-a_j-w\left|\left|\hat{\Gamma}_j\right|\right|_\infty \leqslant \mathrm{Tr}\left[\hat{\Gamma}_j\overline{\rho}\right] \leqslant \mu_j+\gamma_j-a_j,\\
&\quad -\mu_j+\gamma_j+b_j-w\left|\left|\hat{\Gamma}_j\right|\right|_\infty \leqslant \mathrm{Tr}\left[\hat{\Gamma}_j\overline{\rho}\right] \leqslant -\mu_j+\gamma_j+b_j,\\
&\quad 1-w \leqslant \mathrm{Tr}\left[\overline{\rho}\right] \leqslant 1,\\
&\quad \overline{\rho} \geqslant 0,\\
&\quad \vec{a},\vec{b} \geqslant 0,
\end{aligned}
$$

where we replaced the infinite-dimensional ρ by the finite-dimensional $\overline{\rho}$ and used the improved bound $\sqrt{w}$ for the trace-norm constraint from [106, page 59]. As in our case the $\hat{\Gamma}J$'s are infinite-dimensional, $||\hat{\Gamma}_j||_\infty = \infty$. Since w is non-negative, the left-hand side of the inequalities on $\mathrm{Tr}\left[\hat{\Gamma}_j\overline{\rho}\right]$, therefore, become trivial and can be omitted. Furthermore, we can rewrite the trace-norm constraint (see, for example, [108]). We obtain

$$
\begin{aligned}
&\min\ f(\overline{\rho})\\
&\text{s.t.}\\
&\quad \mathrm{Tr}\left[P\right]+\mathrm{Tr}\left[N\right] \leqslant 2\sqrt{w},\\
&\quad P \geqslant \mathrm{Tr}_B\left[\overline{\rho}\right]-\rho_A,\\
&\quad N \geqslant -\left(\mathrm{Tr}_B\left[\overline{\rho}\right]-\rho_A\right),\\
&\quad \mathrm{Tr}\left[\hat{\Gamma}_j\overline{\rho}\right] \leqslant \mu_j+\gamma_j-a_j,\\
&\quad \mathrm{Tr}\left[\hat{\Gamma}_j\overline{\rho}\right] \leqslant -\mu_j+\gamma_j+b_j,\\
&\quad 1-w \leqslant \mathrm{Tr}\left[\overline{\rho}\right] \leqslant 1,\\
&\quad \overline{\rho},N,P \geqslant 0,\\
&\quad \vec{a},\vec{b} \geqslant 0.
\end{aligned}
\tag{C.1}
$$

The numerical method in [110] lower bounds the minimum of the objective function as follows. Let $\overline{\rho}^*$ minimise f over the feasible set $\mathcal{S}$. Then, we have

$$
f(\overline{\rho}^*) \geqslant f(\overline{\rho})+\mathrm{Tr}\left[(\overline{\rho}^*-\overline{\rho})\nabla f(\overline{\rho}\right] \geqslant f(\overline{\rho})+\min_{\sigma\in\mathcal{S}}\mathrm{Tr}\left[(\sigma-\overline{\rho})\nabla f(\overline{\rho}\right] \tag{C.2}
$$

$$
= f(\overline{\rho})-\mathrm{Tr}\left[\overline{\rho}\nabla f(\overline{\rho}]\right)-\min_{\sigma\in\mathcal{S}}\mathrm{Tr}\left[\sigma\nabla f(\overline{\rho})\right]. \tag{C.3}
$$

Therefore, in what follows, we consider this linearised problem. The feasible set is given by the constraints in Eq. (C.1). Furthermore, for ease of notation, we denote all measurement operators by the label $\hat{\Lambda}$ and call the right-hand sides of the constraints related to measurements and the trace-condition λ_j to obtain a more abstract form of our optimisation problem. Then, the problem reads

$$\begin{aligned} &\min \langle \nabla f(\overline{\rho}), \sigma \rangle \\ &\text{s.t.} \\ &\qquad \lambda_k - \mathrm{Tr}\left[\hat{\Lambda}_k \sigma\right] \geqslant 0, \\ &\qquad 2\sqrt{w} - \mathrm{Tr}\left[P\right] - \mathrm{Tr}\left[N\right] \geqslant 0, \\ &\qquad P - \mathrm{Tr}_B\left[\sigma\right] + \rho_A \geqslant 0, \\ &\qquad N + \mathrm{Tr}_B\left[\overline{\rho}\right] - \rho_A \geqslant 0, \\ &\qquad \overline{\rho}, N, P \geqslant 0. \end{aligned} \tag{C.4}$$

We identify

$$\begin{aligned} X &= \left(\sigma \oplus P \oplus N\right), \\ H_1 &= \left(\nabla f(\overline{\rho}) \oplus 0 \oplus 0\right), \\ H_2 &= -\left(-\lambda_1 \oplus \ldots \oplus \lambda_{6N_{\mathrm{St}}} \oplus 2\sqrt{w} \oplus \rho_A \oplus -\rho_A\right), \\ Y &= \left(y_1 \oplus \ldots \oplus y_{6N_{\mathrm{St}}} \oplus s \oplus \tau \oplus \Theta\right), \end{aligned}$$

as well as the linear map

$$\begin{aligned} \mathcal{N}(X) &= \mathcal{N}(X_1 \oplus X_2 \oplus X_3) \\ &= (-\mathrm{Tr}\left[X_1 \hat{\Lambda}_1\right] \oplus \ldots \oplus -\mathrm{Tr}\left[X_1 \hat{\Lambda}_{6N_{\mathrm{St}}}\right] \oplus -\mathrm{Tr}\left[X_2\right] \oplus \\ &\quad - \mathrm{Tr}\left[X_3\right] \oplus X_2 - \mathrm{Tr}_B\left[X_1\right] \oplus X_3 - \mathrm{Tr}_B\left[X_1\right]) \end{aligned}$$

which brings our SDP to the form

(P) Primal problem:

$$\begin{aligned} \alpha := \inf &\langle X, H_1 \rangle_{\mathcal{H}_1} \\ &\text{s.t.} \\ &\qquad \mathcal{N}(X) - H_2 \in \mathcal{K}_2, \\ &\qquad X \in \mathcal{K}_1 \end{aligned}$$

(D) Dual problem:

$$\begin{aligned} \beta := \sup &\langle Y, H_2 \rangle_{\mathcal{H}_2} \\ &\text{s.t.} \\ &\qquad H_1 - \mathcal{N}^*(X) \in \mathcal{K}_1^*, \\ &\qquad Y \in \mathcal{K}_2^* \end{aligned}$$

Note that $\mathcal{K}_1$ denotes the cone

$$\mathcal{K}_1 := \left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} : x_1, x_2, x_2 \geqslant 0 \right\},$$

$\mathcal{K}_1^*$ denotes the dual cone of $\mathcal{K}$ and $\langle \cdot, \cdot \rangle_{\mathcal{H}_1}$ and $\langle \cdot, \cdot \rangle_{\mathcal{H}_2}$ are the inner products on the Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$, where the optimisation problems are set. In our case, we have $\mathcal{K}_1^* = \mathcal{K}_1$ and the first inner product is the Hilbert-Schmidt inner product over the Hilbert space of bounded linear operators and the second inner product is the inner product induced by the component-wise inner products of Hilbert spaces of the constituents of Y. It remains to find the dual (adjoint) of $\mathcal{N}$, defined by $\langle Y, \mathcal{N}(X) \rangle_{\mathcal{H}_2} = \langle \mathcal{N}^*(Y), X \rangle_{\mathcal{H}_1}$. One can show that

$$\begin{aligned} &\mathcal{N}^* \left(y_1 \oplus \ldots \oplus y_{6N_{\mathrm{St}}} \oplus s \oplus \tau \oplus \Theta \right) \\ &= \left(\left(- \sum_{j=1}^{6N_{\mathrm{St}}} y_j \hat{\Lambda}_j - \tau \otimes I_B - \Theta \otimes I_B \right) \oplus (-s \cdot I + \tau) \oplus (-s \cdot I + \Theta) \right). \end{aligned}$$

Therefore, the dual problem reads

$$\begin{aligned} &- \max \ \vec{y} \cdot \vec{\lambda} + 2\sqrt{w} s + \mathrm{Tr}\left[\rho_A \tau\right] - \mathrm{Tr}\left[\rho_A \Theta\right] \\ &\quad \text{s.t.} \\ &\qquad \nabla f(\overline{\rho}) + \sum_{j=1}^{6N_{\mathrm{St}}} y_j \hat{\Lambda}_j + \tau \otimes I_B - \Theta \otimes I_B \geqslant 0, \\ &\qquad s \cdot I - \tau \geqslant 0, \\ &\qquad s \cdot I + \Theta \geqslant 0, \\ &\qquad \vec{y} \geqslant 0, \ \ s \geqslant 0, \ \ \tau, \Theta \geqslant 0. \end{aligned}$$

Finally, we apply the relaxation in [110] to take numerical imprecisions into account. This adds ϵ_{num} to the vector $\vec{v}$ as well as to $2\sqrt{w}$. Therefore, as claimed, we finally obtain the dual of the form given in Eq. (4.18).

D. Bound on the Weight for DM CV-QKD protocols

An integral task when applying the dimension reduction method is to bound the weight outside the considered finite-dimensional subspace. In our work, the energy test provides us a weight. However, in an earlier stage of the present proof, we were required to calculate the weight directly. Theorem 5 in [105] gives a bound on the weight for the asymptotic optimisation problem which is given by equality constraints. In the finite-size case, based on statistical analyses, we obtain only bounds on the expectations of our observables, and hence have to deal with inequality constraints. Therefore, we showed that even for this more general case, we obtain the same bound for the weight. Although this way of bounding the weight outside the cutoff space is not required in the final version of our proof, we provide our result, in case it might be of use for someone's future work.
Let be Π_{β_i} the projector onto the Hilbert space spanned by displaced Fock states $|n_{\beta_i}\rangle$ with photon number smaller or equal to n_c and let $\Pi := \sum_{i=0}^{n_c} |i\rangle\langle i| \otimes \Pi_{\beta_i}$ the corresponding projector onto Alice's and Bob's joint Hilbert space. Then, for the j-th weight we have

$$\begin{aligned} w_j \geqslant & \max \operatorname{Tr}\left[\overline{\Pi}_{\beta_j}\rho\right] \\ & \text{s.t.} \\ & \left|\operatorname{Tr}\left[\hat{\Gamma}_i\rho\right] - \gamma_i\right| \leqslant \mu_i, \\ & \rho \geqslant 0, \end{aligned}$$

where $i \in \{1, ..., M\}$. Introducing slack-variables, this is equivalent to

$$\begin{aligned} w_j \geqslant & \max \operatorname{Tr}\left[\overline{\Pi}_{\beta_j}\rho\right] \\ & \text{s.t.} \\ & \operatorname{Tr}\left[\hat{\Gamma}_i\rho\right] + a_i = \mu_i + \gamma_i, \\ & -\operatorname{Tr}\left[\hat{\Gamma}_i\rho\right] + a_i = \mu_i - \gamma_i, \\ & \rho \geqslant 0. \end{aligned}$$

Let us define

$$\begin{aligned} A &:= \overline{\Pi}_{\beta_j} \oplus \vec{0} \oplus \vec{0}, \\ \sigma &:= \rho \oplus \vec{a} \oplus \vec{b}, \\ \hat{\Gamma}^{+} &:= \hat{\Gamma}_i \oplus |i\rangle\langle i| \oplus \vec{0}, \\ \hat{\Gamma}^{-} &:= -\hat{\Gamma}_i \oplus \vec{0} \oplus |i\rangle\langle i| \end{aligned}$$

to simplify the SDP to

$$\begin{aligned} w_j \geqslant & \max \operatorname{Tr}\left[A\sigma\right] \\ & \text{s.t.} \\ & \operatorname{Tr}\left[\hat{\Gamma}_i^{\pm}\rho\right] = \mu_i \pm \gamma_i, \\ & \sigma \geqslant 0. \end{aligned}$$

It can be shown that the dual problem reads

$$\begin{aligned} & \min \sum_{i=1}^{M} \left(y_i(\mu_i + \gamma_i) + y_{i+M}(\mu_i - \gamma_i)\right) \\ & \text{s.t.} \\ & A \leqslant \sum_{i=1}^{M} \left(\overline{\Gamma}_i^{+} y_i + \overline{\Gamma}_i - y_{i+M}\right), \\ & y \in \mathbb{R}^{2M}. \end{aligned}$$

Note that $A \leqslant \sum_{i=1}^{M} \left(\overline{\Gamma}_i^{+} y_i + \overline{\Gamma}_i - y_{i+M}\right)$ breaks down to

$$\begin{aligned} \overline{\Pi}_{\beta_i} &\leqslant \sum_{i=1}^{M} \hat{\Gamma}_i^{\top}(y_i - y_{i+M}), \\ 0 &\leqslant \sum_{i=1}^{M} |i\rangle\langle i|\, y_i, \\ 0 &\leqslant \sum_{i=1}^{M} |i\rangle\langle i|\, y_{i+M}, \end{aligned}$$

which implies $\forall i \in \{1, ...2M\} : y_i \geqslant 0$. Replacing $\hat{\Gamma}_i$ by the actual observables and

γ_i by their expectations leads to the following dual problem

$$\begin{aligned}
&\min \Big[y_1(1+\mu_1) + y_2(\langle \hat{n}_{\beta_j} \rangle + \mu_2) + y_3(\langle \hat{n}^2_{\beta_j} \rangle + \mu_3) \\
&\qquad + y_4(-1+\mu_4) + y_5(-\langle \hat{n}_{\beta_j} \rangle + \mu_5) + y_6(-\langle \hat{n}^2_{\beta_j} \rangle + \mu_6) \Big] \\
&\text{s.t.} \\
&(y_1 - y_4)\mathbb{1}_B + (y_2 - y_5)\hat{n}_{\beta_j} + (y_3 - y_6)\hat{n}^2_{\beta_i} \geqslant \overline{\Pi}_{\beta_j}, \\
&\vec{y} \geqslant \vec{0}.
\end{aligned}$$

Note that all $\overline{\Pi}_{\beta_j}$ have the form

$$\overline{\Pi}_{\beta_j} = \begin{pmatrix} 0_{(n_c+1)\times(n_c+1)} & \\ & \mathbb{1} \end{pmatrix}.$$

Therefore, we can satisfy the constraints by choosing

$$\begin{aligned}
y_1 &= 0 = y_4, \\
y_2 &= -y_3 = -\frac{1}{n_c(n_c+1)}, \\
y_3 &= -y_6 = \frac{1}{n_c(n_c+1)},
\end{aligned}$$

and obtain as an upper bound for the j-th weight

$$w_j \leqslant \frac{\langle \hat{n}^2_{\beta_j} \rangle - \langle \hat{n}_{\beta_j} \rangle}{n_c(n_c+1)}, \tag{D.1}$$

which coincides with the weight in the restricted case with equality constraints. We obtain the total weight

$$w = \sum_j p(j) w_j \leqslant \sum_j p(j) \frac{\langle \hat{n}^2_{\beta_j} \rangle - \langle \hat{n}_{\beta_j} \rangle}{n_c(n_c+1)}. \tag{D.2}$$

E. Glossary

E.1. Abbreviations and important Terms

This section lists abbreviations and terms used in the present thesis alphabetically.

Asymptotic Limit is an idealisation for security proofs where one presumes Alice and Bob exchange infinitely many signals. Lifting this assumption means proving security in the finite-size regime. See Section 3.3.2 for a more in-depth discussion.

AT stands for Acceptance Test, see Theorem 4.4.2.

Composability is a security notion that ensures that protocols that are proven secure remain secure if they are used as a subprotocol in a larger protocol. For more details, see Section 3.3.3.

CP stands for Completely Positive [map], see Definition 2.1.15.

CPTP stands for Completely Positive Trace Preserving [map, see CP and TP].

CV QKD stands for Continuous-Variable Quantum Key Distribution.

Direct Reconciliation is a special case of information reconciliation, where the flow of classical information is in the same direction as the flow of quantum signals, that is Alice sends classical information to Bob who then corrects his bit-string according to the instructions he received from Alice.

DM stands for Discrete Modulation.

DV QKD stands for Discrete-Variable Quantum Key Distribution.

EC stands for Error Correction.

ET stands for Energy Test, see Theorem 4.4.1.

Error Correction is a way to execute information reconciliation. However, often it is used as a synonym for information reconciliaton as well.

Finite-Size Regime describes the realistic scenario where Alice and Bob exchange only a finite amount of signals before generating their key. We refer to Section 3.3.2 for a more detailed discussion.

GM stands for Gaussian Modulation.

Homodyne Detection is the name of a method for measuring one quadrature of light. The incoming state is mixed with the light coming from the local oscillator, a strong reference light source, at a $50:50$ beamsplitter. The intensity of the superposed signal is measured with photodiodes. The quadrature component is then proportional to the difference in the output photo-currents. For more details we refer the reader to Section 2.4.

Heterodyne Detection is another method for measuring the quadratures of light. At the cost of an additional 3dB loss compared to the homodyne detector, heterodyne detectors can measure both quadrature components simultaneously. It introduces an additional $50:50$ beamsplitter and measures the output states each with a heterodyne detector. For more details we refer the reader to Section 2.4.

Information Reconciliation describes the process of Alice and Bob using classical communication to synchronise their only partially correlated bit strings, while information is leaked to the eavesdropper via the classical channel.

PA stands for privacy amplification.

PE stands for Parameter Estimation. Note that for the finite-size regime PE is replaced by the notion of acceptance sets and acceptance testing.

Postprocessing summarises classical protocol steps that transform the raw key into a shorter secret key.

Postselection describes a process where selectively certain measurement results are discarded aiming to improve the performance of the protocol (e.g., higher key rates, higher noise-tolerance, fewer data needed to be postprocessed).

POVM stands for Positive Operator-Valued Measure (see Definition 2.2.21 and Definition 2.2.22).

Privacy Amplification is the procedure when Alice and Bob distil a secret key from a common random variable that is partially known to an adversary.

PSK is short for Phase-Shift Keying and is a modulation pattern for data transmission, where the sent signals are prepared with the same amplitude but a different phase.

QKD stands for Quantum Key Distribution which is a method to establish a shared secret key between two remote parties.

QPSK is short for Quadrature Phase-Shift Keying and is the special case of Phase-Shift Keying, where four signal states are used.

Quantum Channel is a completely positive trace preserving map, see Definition 2.2.24.

Raw Key is the bit-string obtained by measuring the incoming quantum signals before performing classical protocol steps like sifting, error-correction and privacy-amplification.

Reverse Reconciliation is a special case of information reconciliation, where the flow of classical information is opposite to the direction of the quantum phase. So, Bob sends classical information to Alice who then corrects her bit-string according to the instructions he received from Bob.

SDP is the abbreviation for Semidefinite Program.

Security Proof is a mathematical statement giving a lower bound on the achievable secure key rate for a Quantum Key Distribution protocol under some model for the physical system and certain additional assumptions.

Secure Key Rate is the fraction of transmitted signals that can be used for encryption.

TNI stands for Trace Non-Increasing [map], see Definition 2.1.15.

TP stands for Trace Preserving [map], see Definition 2.1.15.

Trusted Detector describes a model for a detector, where (parts of) the electronic noise is trusted and therefore assumed not to be controlled by an eavesdropper.

E.2. Symbols used

This section lists symbols used in the present thesis.

E.2.1. Sets, fields and spaces

$\mathbb{N}$ is the set of natural numbers $\{1, 2, ...\}$.

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

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

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

$\mathcal{H}$ denotes a separable Hilbert space over $\mathbb{C}$, see Definition 2.1.1.

$\mathcal{H}^*$ denotes the dual space of a Hilbert space $\mathcal{H}$, see Definition 2.1.2.

$\mathcal{B}(\mathcal{H}_A, \mathcal{H}_B)$ denotes the set of all bounded operators, mapping from Hilbert space $\mathcal{H}_A$ to the Hilbert space $\mathcal{H}_B$, see Definition 2.1.4.

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

$\mathrm{Pos}(\mathcal{H})$ denotes the set of all positive semi-definite operators on $\mathcal{H}$, see Definition 2.1.6.

$\mathcal{T}(\mathcal{H})$ denotes the set of all trace-class operators over $\mathcal{H}$ (see Definition 2.1.11).

$\mathcal{T}_1(\mathcal{H})$ denotes the set of all trace-class operators over $\mathcal{H}$ with Schatten 1-norm equal to 1, see Definition 2.1.11.

$\mathcal{T}^+(\mathcal{H})$ denotes the set of positive trace-class operators over $\mathcal{H}$, see Definition 2.1.11.

$\mathcal{D}(\mathcal{H})$ denotes the set of density operators over $\mathcal{H}$, see Definition 2.2.17.

$\mathcal{D}_{\leqslant}(\mathcal{H})$ denotes the set of subnormalised density operators over $\mathcal{H}$.

E.2.2. Maps and Distance-Measures

$\otimes$ denotes the tensor product, see Definition 2.1.13.

$\cdot^\dagger$ denotes the dual of a linear map, see Definition 2.1.16.

$\Delta(\cdot, \cdot)$ denotes the trace-distance between two positive operators, see Definition 2.2.26.

$F(\cdot,\cdot)$ denotes the Fidelity between two density operators, see Definition 2.2.27.

$F_*(\cdot,\cdot)]$ denotes the generalised fidelity between two subnormalised density operators, see Definition 2.2.28.

$\mathcal{P}(\cdot,\cdot)$ denotes the purified distance between two quantum states, see Definition 2.2.29.

$\mathrm{Tr}\,[\cdot]$ denotes the trace of an operator, see Definition 2.1.8.

$\mathrm{Tr}_A\cdot$ denotes the partial trace of a bipartite operator $\rho_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$, see Definition 2.1.14.

$||\cdot||_\infty$ denotes the operator norm of an operator, see Definition 2.1.3.

$||\cdot||_p$ denotes the Schatten p-norm of an operator, see Definition 2.1.9.

E.2.3. Entropic Quantities and Probabilities

$H(\cdot)$ denotes the classical or Shannon entropy of a discrete random variable, see Definition 2.3.31.

$H(\cdot,\cdot)$ denotes the classical joint entropy of two discrete random variables, see Definition 2.3.32.

$H(\cdot,|\cdot)$ denotes the classical conditional entropy of two discrete random variables, see Definition 2.3.33.

$I(\cdot:\cdot)$ denotes the classical mutual information, see Definition 2.3.34.

$H(\cdot)_\rho$ denotes the von Neumann entropy of a quantum state ρ, see Definition 2.3.35.

$H(\cdot,\cdot)_\rho$ denotes the joint von Neumann entropy of a bipartite quantum state ρ, see Definition 2.3.36.

$H(\cdot,|\cdot)_\rho$ denotes the conditional von Neumann entropy of a bipartite quantum state ρ, see Definition 2.3.37.

$D(\cdot||\cdot)$ denotes the quantum relative entropy between a quantum state in the first argument and a positive operator in the second argument, see Definition 2.3.39.

$H_{\min}(\cdot|\cdot)$ denotes the min-entropy of a quantum state, see Definition 2.3.40.

$H_{\max}(\cdot|\cdot)$ denotes the max-entropy of a quantum state, see Definition 2.3.41.

$H^{\epsilon}_{\min}(\cdot|\cdot)$ denotes the smooth min-entropy of a quantum state, see Definition 2.3.42.

$H^{\epsilon}_{\max}(\cdot|\cdot)$ denotes the smooth max-entropy of a quantum state, see Definition 2.3.42.

$P(\cdot,\cdot)$ denotes the joint probability of two events.

$P(\cdot|\cdot)$ denotes the conditional probability of two events.

E.2.4. Miscellaneous

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

$\bar{.}$ denotes the complex conjugate of a complex number.

$\geqslant$ is a short notation for non-negativity of an operator.

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

$\mathrm{id}_{\mathcal{H}}$ denotes the identity map on the Hilbert space $\mathcal{H}$.

$\mathbb{E}$ denotes the expectation value of an observable.

$|.\rangle$ is a vector in a Hilbert space $\mathcal{H}$ in BraKet notation.

$\langle.|$ denotes a linear-form on a Hilbert space $\mathcal{H}$ in BraKet notation.

$\langle.|.\rangle$ denotes the action of a bra on a ket. The Riesz-Frechet representation theorem allows us to use this notation to denote the inner product between two states.

$|.\rangle\langle.|$ is the outer product between two quantum states, defined as a map from $\mathcal{H}$ to $\mathcal{H}$, $|\psi\rangle\langle\phi|\sigma\rangle := \langle\phi|\sigma\rangle|\psi\rangle$.

$\langle.\rangle_{\rho}$ denotes the expectation value of an operator $\hat{O}$ in the state (associated with) ρ.

$\langle.,.\rangle$ denotes the inner product between two vectors.

$e^{\cdot}$ denotes the exponential function. The exponential of a matrix or a bounded operator A is defiend via the series $e^A := \sum_{n=0}^{\infty} \frac{A^n}{n!}$.

$\log_b(.)$ denotes the logarithm to the base b. If $\log_b$ is applied to a matrix or a bounded operator A, we mean by $\log_b(A)$ the matrix that satisfies $b^{\log_b(A)} = A$. The logarithm of a diagonalisable matrix $M = T^{-1}DT$ is defined via $\log_b(M) = T^{-1}\log_b(D)T$.

E.3. Variables Used

This section lists important variables used in the present thesis.

$\hat{a}$ is the annihilation operator, see Section 2.4.

$\hat{a}^\dagger$ is the creation operator, see Section 2.4.

α denotes the complex amplitude of the coherent state $|\alpha\rangle$.

β denotes the reconciliation efficiency, that is the efficiency of classical error correction.

β_{test} is the testing parameter for the energy test, see Theorem 4.4.1.

χ stands for the Holevo quantity.

$\hat{d}$ denotes a second order quadrature operator, see Section 3.4.

Δ_r denotes the radial postselection parameter.

δ_{EC} is the information leakage in the Slepian-Wolfe limit, see Section 4.4.6.

$\delta_{\text{leak}}^{\text{EC}}$ is the information leakage for imperfect information reconciliation, see Section 4.4.6.

$\mathcal{E}_{A'\to B}$ is the map, modelling the quantum channel connecting Alice and Bob, see Section 3.4.

E_y denotes the POVM for ideal heterodyne measurement.

ϵ is the total security parameter, see Theorem 4.4.3.

$\tilde{\epsilon}$ stands for the small perturbation that guarantees differentiability of the optimisation problem's objective function, see Section 3.4.1.

$\bar{\epsilon}$ is the smoothing-epsilon.

ϵ_{AT} is the security parameter of the acceptance test, see Theorem 4.4.2.

ϵ_{ET} is the security parameter of the energy test, see Theorem 4.4.1.

ϵ_{EC} is the security parameter of the error-correction subroutine.

ϵ_{PA} is the security parameter of the privacy amplification subroutine.

η denotes the transmittance of the quantum channel connecting Alice and Bob. In accordance with state-of-the-art optical fibres, in the whole work, we chose $\eta = 10^{-0.02L}$.

η_d denotes the detector-efficiency within the trusted, non-ideal detector model, see 3.4.4.

f denotes the objective function of optimisation problem for untrusted, ideal detectors.

f^{noisy} denotes the objective function of optimisation problem for trusted, non-ideal detectors.

$\hat{F}_P$ denotes the first-order p-quadrature operator within the trusted, non-ideal detector model, see 3.4.4.

$\hat{F}_Q$ denotes the first-order q-quadrature operator within the trusted, non-ideal detector model, see 3.4.4.

$\mathcal{G}$ denotes the completely positive trace non-increasing map that describes several protocol steps, see Section 3.4.

G_y denotes the POVM of the trusted, non-ideal detector, see Section 3.4.4.

$\hat{\Gamma}_i$ is a generic symbol, standing for the i-th measurement operator that is used to define the feasible set.

γ_i is a generic scalar, standing for the right-hand-side of the i-th constraint required to define the feasible set.

$\mathcal{I}$ stands for an index set. If it is not specified in more detail, its size is clear from the context.

k_T is the number of signals sacrificed for testing, see Theorem 4.4.1.

L denotes the length of the optical fibre between Alice and Bob, measured in km.

leak_{EC} is the total leakage term, including error verification, see Section 4.4.6.

l_T is the number of testing rounds that may violate the testing condition, see Theorem 4.4.1.

μ_X is the acceptance bound related to the observable X, see Theorem 4.4.2

N denotes the total number of signals transmitted.

n denotes the number of rounds left after testing, $n := N - k_T$.

$\hat{n}$ denotes the number operator, see Section 3.4.

$\hat{n}_{\beta_i}$ denotes the displaced number operator, see Section 3.4.4.

n_c denotes the photon cutoff number, see Section 3.4.2.

N_{St} denotes the number of states of a certain protocol (see Chapter 3.2).

ν_{el} is the electronic noise in the trusted, non-ideal detector model, measured in shot-noise units, see Section 3.4.4.

$\hat{p}$ denotes the momentum-operator.

p_i is the probability that the state, associated with the symbol i, is prepared by Alice, see Section 3.2.

p_{pass} denotes the probability that random round is kept until after the post-selection phase, see Section 3.4.1.

$\hat{q}$ is the spatial quadrature operator, see Section 3.2.

R_∞ is the asymptotic secret key rate.

R_B^z is the region operator associated with Bob's key map, corresponding to the region labelled by the symbol z, see Section 3.4.

ρ stands for a general density operator.

$\mathcal{S}_\infty$ denotes the feasible set associated with the optimisation problem for the asymptotic key rate, see Section 3.4.

$\hat{S}_P$ denotes the second-order p-quadrature operator within the trusted, non-ideal detector model, see 3.4.4.

$\hat{S}_Q$ denotes the second-order q-quadrature operator within the trusted, non-ideal detector model, see 3.4.4.

w denotes the weight outside the cutoff space, see Theorem 3.4.3.

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

$\mathcal{Z}$ denotes the pinching quantum channel that describes several protocol steps, see Section 3.4.

Bibliography

[1] M. ApS. *The MOSEK optimization toolbox for MATLAB manual. Version 9.0.*, 2019.

[2] S. M. Barnett and P. Radmore. *Methods in Theoretical Quantum Optics*. Oxford: Clarendon Press, Oxford, 1997.

[3] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim. The universal composable security of quantum key distribution. In J. Kilian, editor, *Theory of Cryptography*, pages 386–406, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.

[4] M. Ben-Or and D. Mayers. General security definition and composability for quantum & classical protocols, 2004.

[5] C. Bennett. Quantum Cryptography using any two Nonorthogonal States. *Phys. Rev. Lett.*, 1992.

[6] 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. IEEE.

[7] D. J. Bernstein and T. Lange. Post-quantum cryptography. *Nature*, 549(7671), Sept 2017.

[8] M. Berta, F. Furrer, and V. B. Scholz. The smooth entropy formalism for von neumann algebras. *J. Math. Phys.*, 57(1):015213, jan 2016.

[9] S. Boyd and L. Vandenberghe. *Convex Optimization*. Cambridge University Press, 2004.

[10] G. Brassard. Brief history of quantum cryptography: a personal perspective. In *IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, 2005.* IEEE.

[11] S. L. Braunstein and S. Pirandola. Side-channel-free quantum key distribution. *Phys. Rev. Lett.*, 108:130502, Mar 2012.

[12] K. Brádler and C. Weedbrook. Security proof of continuous-variable quantum key distribution using three coherent states. *Physical Review A*, 97(2), Feb 2018.

[13] J. Bub. Quantum Mechanics is About Quantum Information. *Found Phys*, 35(4):541–560, Apr. 2005.

[14] R. Canetti. Security and composition of multiparty cryptographic protocols. *J. Cryptol.*, 13(1):143–202, jan 2000.

[15] R. Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *FOCS*, pages 136–145. IEEE Computer Society, 2001.

[16] N. J. Cerf, M. Lévy, and G. V. Assche. Quantum distribution of gaussian keys using squeezed states. *Phys. Rev. A*, 63(5), apr 2001.

[17] A. F. Chalmers. *What Is This Thing Called Science?* Univ. of Queensland Press, 1999.

[18] M. Christandl, R. König, and R. Renner. Postselection technique for quantum channels with applications to quantum cryptography. *Phys. Rev. Lett.*, 102(2):020504, jan 2009.

[19] P. J. Coles, E. M. Metodiev, and N. Lütkenhaus. Numerical approach for unstructured quantum key distribution. *Nat. Commun.*, 7:11712, May 2016.

[20] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. Wiley-Interscience, USA, 1991.

[21] M. Curty, M. Lewenstein, and N. Lütkenhaus. Entanglement as a precondition for secure quantum key distribution. *Phys. Rev. Lett.*, 92:217903, May 2004.

[22] A. Denys, P. Brown, and A. Leverrier. Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. *Quantum*, 5:540, 2021.

[23] I. Devetak and A. Winter. Distillation of secret key and entanglement from quantum states. *Proc.R.Soc.*, 461:207–235, Jan 2005.

[24] E. Diamanti and A. Leverrier. Distributing secret keys with quantum continuous variables: Principle, security and implementations. *Entropy*, 17(12):6072–6092, Aug 2015.

[25] H. Dukas and B. e. Hoffmann. *Albert Einstein: The Human Side*. Princeton University Press, 1979.

[26] F. Dupuis, O. Fawzi, and R. Renner. Entropy accumulation. *Commun. Math. Phys.*, 379(3):867–913, sep 2020.

[27] A. K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991.

[28] 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.

[29] M. Frank and P. Wolfe. An algorithm for quadratic programming. *Nav. Res. Logist. Q.*, 3(1-2):95–110, 1956.

[30] C. A. Fuchs. Distinguishability and accessible information in quantum theory, 1996.

[31] C. A. Fuchs and J. van de Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Trans. Inf. Theory*, 45(4):1216–1227, 1999.

[32] F. Furrer. *Security of Continuous-Variable Quantum Key Distribution and Aspects of Device-Independent Security*. PhD thesis, Universität Hannover, Hannover, 2012.

[33] F. Furrer. Reverse-reconciliation continuous-variable quantum key distribution based on the uncertainty principle. *Phys. Rev. A*, 90(4), oct 2014.

[34] F. Furrer, J. Åberg, and R. Renner. Min- and max-entropy in infinite dimensions. *Commun. Math. Phys.*, 306(1):165–186, jun 2011.

[35] I. George, J. Lin, and N. Lütkenhaus. Numerical calculations of the finite key rate for general quantum key distribution protocols. *Phys. Rev. Research*, 3:013274, 2021.

[36] George, Ian. Numerical finite key analysis. Master's thesis, University of Waterloo, 2020.

[37] C. Gerry and P. Knight. *Introductory Quantum Optics*. Cambridge University Press, 2004.

[38] S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier. Asymptotic security of continuous-variable quantum key distribution with a discrete modulation. *Phys. Rev. X*, 9:021059, 2019.

[39] A. Gilchrist, N. K. Langford, and M. A. Nielsen. Distance measures to compare real and ideal quantum processes. *Phys. Rev. A*, 71(6), jun 2005.

[40] G. Gour. Introduction to quantum information, Mar. 2018.

[41] 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, London, 2008. `http://stanford.edu/~boyd/graph_dcp.html`.

[42] M. Grant and S. Boyd. CVX: Matlab software for disciplined convex programming, version 2.1. `http://cvxr.com/cvx`, Mar. 2014.

[43] D. Griffiths. *Introduction to Quantum Mechanics*. Cambridge University Press, 2017.

[44] F. Grosshans and P. Grangier. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.*, 88:057902, Jan 2002.

[45] F. Grosshans, J. Wenger, R. Tualle-Brouri, P. Grangier, G. Assche, and N. Cerf. Quantum key distribution using gaussian-modulated coherent states. *Nature*, 421, 01 2003.

[46] H. Häseler and N. Lütkenhaus. Quantum benchmarks for the storage or transmission of quantum light from minimal resources. *Phys. Rev. A*, 81:060306, Jun 2010.

[47] 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.

[48] M. Hillery. Quantum cryptography with squeezed states. *Phys. Rev. A*, 61:022309, Jan 2000.

[49] T. Hirano, T. Ichikawa, T. Matsubara, M. Ono, Y. Oguri, R. Namiki, K. Kasai, R. Matsumoto, and T. Tsurumaru. Implementation of continuous-variable quantum key distribution with discrete modulation. *Quantum Science and Technology*, 2(2):024010, jun 2017.

[50] W. Hoeffding. Probability Inequalities for Sums of Bounded Random Variables. *J. Am. Stat. Assoc.*, 58(301):13–30, 1963.

[51] 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.

[52] M. Jammer. *The Philosophy of Quantum Mechanics: The Interpretations of Quantum Mechanics in Historical Perspective*. New York: Wiley, 1974.

[53] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier. Analysis of imperfections in practical continuous-variable quantum key distribution. *Phys. Rev. A*, 86:032309, Sep 2012.

[54] W. Kaballo. *Grundkurs Funktionalanalysis*. Spektrum Akademischer Verlag, 2011.

[55] F. Kanitschar, I. George, J. Lin, T. Upadhyaya, and N. Lütkenhaus. Finite-Size Security for Discrete-Modulated Continuous-Variable Quantum Key Distribution Protocols. *manuscript forthcoming*, 2022.

[56] F. Kanitschar and C. Pacher. Optimizing Continuous-Variable Quantum Key Distribution with Phase-Shift Keying Modulation and Postselection. *Phys. Rev. Applied*, 18:034073, Sep 2022.

[57] F. P. Kanitschar. Postselection Strategies for CV-QKD Protocols with Phase-Shift Keying Modulation, 2021.

[58] E. Kaur, S. Guha, and M. M. Wilde. Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution. *Physical Review A*, 103(1), Jan 2021.

[59] R. König, R. Renner, A. Bariska, and U. Maurer. Small accessible quantum information does not imply security. *Phys. Rev. Lett.*, 98:140502, Apr 2007.

[60] 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. *Adv. Quantum Technol.*, 1(1):1800011, Jun 2018.

[61] U. Leonhardt. *Essential Quantum Optics: From Quantum Measurements to Black Holes*. Cambridge University Press, 2010.

[62] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf. Security of continuous-variable quantum key distribution against general attacks. *Phys. Rev. Lett.*, 110:030502, Jan 2013.

[63] J. Lin and N. Lütkenhaus. Trusted Detector Noise Analysis for Discrete Modulation Schemes of Continuous-Variable Quantum Key Distribution. *Phys. Rev. Appl.*, 14(6):064030, Dec 2020.

[64] J. Lin, T. Upadhyaya, and N. Lütkenhaus. Asymptotic Security Analysis of Discrete-Modulated Continuous-Variable Quantum Key Distribution. *Phys. Rev. X*, 9(4):041064, Dec 2019.

[65] M. Liu, F. Kanitschar, A. Arqand, and E. Y. Z. Tan. Lipschitz continuity of quantum-classical conditional entropies with respect to angular distance, and related properties of angular distance. *arXiv:2210.04874 [quant-ph]*, 2022.

[66] H.-K. Lo, M. Curty, and B. Qi. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 108:130503, Mar 2012.

[67] 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. *Phys. Rev. A*, 76(4), Oct 2007.

[68] C. Lupo and Y. Ouyang. Quantum key distribution with nonideal heterodyne detection: Composable security of discrete-modulation continuous-variable protocols. *PRX Quantum*, 3:010341, Mar 2022.

[69] T. Matsuura, K. Maeda, T. Sasaki, and M. Koashi. Finite-size security of continuous-variable quantum key distribution with digital signal processing. *Nat. Commun.*, 12(1):252, Jan 2021.

[70] T. Metger, O. Fawzi, D. Sutter, and R. Renner. Generalised entropy accumulation. 2022.

[71] T. Metger and R. Renner. Security of quantum key distribution from generalised entropy accumulation. 2022.

[72] B. R. Mollow and R. J. Glauber. Quantum theory of parametric amplification. i. *Phys. Rev.*, 160:1076–1096, Aug 1967.

[73] J. v. Neumann. Mathematische begründung der quantenmechanik. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse*, 1927:1–57, 1927.

[74] J. v. Neumann. Zur algebra der funktionaloperationen und theorie der normalen operatoren. *Mathematische Annalen*, 102:370–427, 1930.

[75] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[76] K. Oldham, J. Myland, and J. Spanier. *The Laguerre Polynomials Ln(x)*, pages 209–216. Springer, New York, NY, 2008.

[77] P. Papanastasiou and S. Pirandola. Continuous-variable quantum cryptography with discrete alphabets: Composable security under collective Gaussian attacks. *Physical Review Research*, 3(1), Jan 2021.

[78] A. Peres. *Quantum Theory: Concepts and Methods*. Fundamental Theories of Physics. Springer Netherlands, 1995.

[79] K. Petersen and M. Pedersen. The Matrix Cookbook. `http://www2.imm.dtu.dk/pubdb/p.php?3274`, 2012.

[80] B. Pfitzmann and M. Waidner. A model for asynchronous reactive systems and its application to secure message transmission. In *Proceedings 2001 IEEE Symposium on Security and Privacy. SP 2001*, pages 184–200, 2001.

[81] 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. *Adv. Opt. Photonics*, 12(4):1012, Dec 2020.

[82] C. Portmann and R. Renner. Cryptographic security of quantum key distribution, 2014.

[83] I. W. Primaatmaja, K. T. Goh, E. Y. Z. Tan, J. T. F. Khoo, S. Ghorai, and C. C. W. Lim. Security of device-independent quantum key distribution protocols: a review, 2022.

[84] T. C. Ralph. Continuous variable quantum cryptography. *Phys. Rev. A*, 61:010303, Dec 1999.

[85] R. Renner. *Security of Quantum Key Distribution*. PhD thesis, ETH Zürich, Zürich, Switzerland, 2005.

[86] R. Renner and J. I. Cirac. de finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. *Phys. Rev. Lett.*, 102:110504, Mar 2009.

[87] R. Renner and R. König. Universally composable privacy amplification against quantum adversaries. In J. Kilian, editor, *Theory of Cryptography*, pages 407–425, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.

[88] J. Rigas, O. Gühne, and N. Lütkenhaus. Entanglement verification for quantum-key-distribution systems with an underlying bipartite qubit-mode structure. *Phys. Rev. A*, 73:012341, Jan 2006.

[89] W. Rudin. *Functional Analysis*. International series in pure and applied mathematics. McGraw-Hill, 1991.

[90] 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.

[91] V. Scarani and R. Renner. *Security Bounds for Quantum Cryptography with Finite Resources*, pages 83–95. Springer, 2008.

[92] W. P. Schleich. *Quantum Optics in Phase Space*. Wiley-VCH, Berlin, 2001.

[93] E. Schrödinger. Discussion of probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society*, 31(4):555–563, 1935.

[94] C. E. Shannon. A mathematical theory of communication. *Bell Syst. Tech. J.*, 27(3):379–423, 1948.

[95] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85(2):441–444, jul 2000.

[96] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs. Continuous variable quantum cryptography: Beating the 3 db loss limit. *Phys. Rev. Lett.*, 89:167901, Sep 2002.

[97] D. Slepian and J. Wolf. Noiseless coding of correlated information sources. *IEEE Trans. Inf. Theory*, 19(4):471–480, 1973.

[98] D. Sych and G. Leuchs. Coherent state quantum key distribution with multi letter phase-shift keying. *New J. of Phys.*, 12(5):053019, may 2010.

[99] M. Tomamichel. *Quantum Information Processing with Finite Resources*. Springer International Publishing, 2016.

[100] M. Tomamichel, R. Colbeck, and R. Renner. Duality between smooth min- and max-entropies. *IEEE Trans. Inf. Theory*, 56(9):4674–4681, sep 2010.

[101] M. Tribus and E. C. McIrvine. Energy and information. *Scientific American*, 225(3):179–190, 1971.

[102] R. Tumulka. *POVM (Positive Operator Value Measure)*, pages 480–484. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.

[103] T. Tyc and B. C. Sanders. Operational formulation of homodyne detection. *J. Physics A: Math.*, 37(29):7341–7357, Jul 2004.

[104] D. Unruh. Simulatable security for quantum protocols, 2004.

[105] T. Upadhyaya, T. van Himbeeck, J. Lin, and N. Lütkenhaus. Dimension reduction in quantum key distribution for continuous- and discrete-variable protocols. *PRX Quantum*, 2:020325, May 2021.

[106] Upadhyaya, Twesh. Tools for the Security Analysis of Quantum Key Distribution in Infinite Dimensions. Master's thesis, 2021.

[107] L. van Hove. Von Neumann's contributions to quantum theory. *Bulletin of the American Mathematical Society*, 64(3.P2):95–99, May 1958.

[108] J. Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018.

[109] M. M. Wilde. *Quantum Information Theory*. Cambridge University Press, 2017.

[110] A. Winick, N. Lütkenhaus, and P. J. Coles. Reliable numerical key rates for quantum key distribution. *Quantum*, 2:77, Jul 2018.

[111] A. Winter. Coding theorem and strong converse for quantum channels. *IEEE Trans. Inf. Theory*, 45(7):2481–2485, 1999.

[112] C. Wittmann, J. Fürst, C. Wiechers, D. Elser, H. Häseler, N. Lütkenhaus, and G. Leuchs. Witnessing effective entanglement over a 2 km fiber channel. *Opt. Express*, 18(5):4499–4509, Mar 2010.

[113] W. K. Wootters and W. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

[114] Y.-B. Zhao, M. Heid, J. Rigas, and N. Lütkenhaus. Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks. *Phys. Rev. A*, 79(1):012307, Jan 2009.