4-5-2018

Entropic Bounds on Two-Way Assisted Secret-Key Agreement Capacities of Quantum Channels

Noah Anthony Davis
Louisiana State University and Agricultural and Mechanical College, noahadavis@outlook.com

Follow this and additional works at: https://digitalcommons.lsu.edu/gradschool_dissertations
Part of the Information Security Commons, and the Quantum Physics Commons

Recommended Citation
https://digitalcommons.lsu.edu/gradschool_dissertations/4561

This Dissertation is brought to you for free and open access by the Graduate School at LSU Digital Commons. It has been accepted for inclusion in LSU Doctoral Dissertations by an authorized graduate school editor of LSU Digital Commons. For more information, please contact gradetd@lsu.edu.
ENTROPIC BOUNDS ON TWO-WAY ASSISTED SECRET-KEY AGREEMENT CAPACITIES OF QUANTUM CHANNELS

A Dissertation

Submitted to the Graduate Faculty of the Louisiana State University and Agricultural and Mechanical College in partial fulfillment of the requirements for the degree of Doctor of Philosophy in The Department of Physics & Astronomy

by

Noah Anthony Davis
B.S., Louisiana State University, 2012
M.S., Louisiana State University, 2016
May 2018
Acknowledgments

I would like to extend a heartfelt thanks to my advisor Dr. Mark M. Wilde. In addition to your patience and obvious efforts toward my education, you helped me when I especially needed support. I thank my committee members, Drs. Dana Browne, Jonathan Dowling, Juhan Frank, Jeffrey Roland, and Mark Wilde, for spending their time reviewing and engaging me on my research. Thanks to the LSU Department of Physics and Astronomy, the National Science Foundation, and the Department of Energy for funding my graduate studies.

I am grateful to the Department of Physics and Astronomy as a whole and the office staff in particular for hosting me and handling me through my many years at LSU. I have had important connections with many department members. Thanks to Dr. Dubravka Rupnik for caring to show me the beauty of modern physics. Dr. Dana Browne, thank you for our many thoughtful discussions, your guidance in educating and spreading intellectual passion to students, and for your direct advice when I have needed it. I thank Dr. John DiTusa for his guidance through my first experiences as a researcher and his continued support. Thanks to Dr. Mette Gaarde and Dr. Kenneth Schafer for advice and for research leadership in earlier projects.

In the Chemistry Department, Dr. Julia Chan and Dr. Kresimir Rupnik took particular interest in me and were very helpful in my development as a scientist.

I am thankful to the many excellent teachers I have had, and I am especially grateful to Amy Esté whose excitement colored my first physics class in high school and helped lead me to pursuing the subject in college.

Thank you to my parents, who helped me learn to live well by shaping my senses of humor and responsibility. Along with my brothers, you have always encouraged my curiosity.

I appreciate my group mates who have been welcoming friends that happily exchange quips, teach me about the world, and discuss my technical questions. Kunal in particular has shared my interests.

I am deeply thankful to my wife, Sarah, and my children, Penelope and Ravi. You are a major source of inspiration and purpose, and you have sacrificed many hours for me to pursue my goals.
# Table of Contents

Acknowledgments ........................................................................................................... ii

Abstract ............................................................................................................................ iv

Chapter 1 Introduction ...................................................................................................... 1
  1.1 Central Ideas ............................................................................................................ 1
  1.2 Historical Preliminaries for Quantum Information .................................................. 2
  1.3 Technical Preliminaries ........................................................................................... 7

Chapter 2 Energy-Constrained Two-Way Assisted Private and Quantum Capacities ........ 25
  2.1 Properties of Conditional Quantum Mutual Information ........................................ 25
  2.2 Energy-Constrained Secret-Key-Agreement Capacity .............................................. 28
  2.3 Energy-Constrained Squashed Entanglement is an Upper Bound on Energy-
     Constrained Secret-Key-Agreement Capacity .......................................................... 35
  2.4 Bounds on Energy-Constrained Secret-Key-Agreement Capacities of Phase-
    Insensitive Quantum Gaussian Channels .................................................................... 40
  2.5 Multipartite Conditional Mutual Informations and Squashed Entanglement .......... 54
  2.6 Quantum Broadcast Channels and Secret-Key-Agreement Capacity Regions .......... 64

Chapter 3 Broadcast Amplitude Damping Channels and Capacities ............................... 72
  3.1 Introduction ............................................................................................................ 72
  3.2 Amplitude Damping Channel .................................................................................. 72
  3.3 Broadcast Amplitude Damping Channel .................................................................. 74

Chapter 4 Conclusion ....................................................................................................... 81

References ......................................................................................................................... 83

Appendix A Thermal State Optimality ............................................................................ 92

Vita ................................................................................................................................. 98
Abstract

In order to efficiently put quantum technologies into action, we must know the characteristics of the underlying quantum systems and effects. An interesting example is the use of the secret-key-agreement capacity of a quantum channel as a guide and measure for the implementation of quantum key distribution (QKD) and distributed quantum computation. We define the communication task of establishing a secret key over a quantum channel subject to an energy constraint on the input state and while allowing for unlimited local operations and classical communication (LOCC) between a sender and receiver. We then use the energy-constrained squashed entanglement to bound the capacity of the channel for secret-key agreement, and we show that a thermal state input maximizes a relaxation of this bound for phase-insensitive, single-mode Gaussian channels. We also establish improved upper bounds on the energy-constrained secret-key-agreement capacity for a bosonic thermal channel that is not entanglement breaking. We then generalize our results to the multipartite setting and show that the energy-constrained multipartite squashed entanglement bounds the LOCC-assisted private capacity region for a quantum broadcast channel. Next, we define the broadcast amplitude damping channel. In the setting of QKD, we discuss a communication task using the broadcast amplitude damping channel and give bounds on its achievable rate region.
1 Introduction

1.1 Central Ideas

As individuals and as a society, we rely heavily on computation and on information theory, with our digital interactions evolving as these areas evolve. Tasks such as playing minesweeper, analyzing traffic flow, predicting trends in consumer markets, ordering duct tape from Amazon.com, and posting memes on Reddit are all possible as a consequence of applied information theory in some manner. And, just as the exploration of the quantum world has vastly impacted astronomy, chemistry, and many other disciplines both within and outside of proper “physics,” the study of information is transformed by the consideration of quantum effects. This pervasiveness of quantum influence urges the study of quantum information.

I use the term quantum information to describe the broad collection of topics including quantum computation, quantum Shannon theory, and quantum complexity, as well as many other topics involving quantum considerations to informational quantities along with experimental implementations in all of these fields. The many subfields overlap significantly, and one often benefits from the advancement of another. For these reasons, they are not separated in this thesis. However, we will steer steadily toward a particular area of quantum informational studies, which pertains to the capacities of quantum channels to transmit private and quantum information.

The consideration of quantum effects in the context of information theory brings many possibilities for improvement. The quantum factoring algorithm [1, 2] is an example that significantly reduces the complexity of finding prime factors of an integer using a quantum computer. Beyond algorithmic speedups, quantum computers could be used to efficiently simulate quantum systems that surpass practical memory and calculation abilities for classical computers [3, 4].

Cryptographic schemes are of particular interest for the application of quantum theory. Current classical encryption methods [5–7], trusted by teenagers and international leaders alike, rely on a binary number called the secret key. The encryption strength is directly tied to the security of

\[ \text{One particularly interesting subfield, not discussed herein, is quantum metrology: the use of quantum mechanical effects to make ultra-high sensitivity measurements.} \]
the key, and the security of most systems currently in use rests on computational assumptions. In contrast, quantum communication allows for generating an information-theoretically secure key, shared among trusted parties, via a method known as quantum key distribution (QKD) [8–10].

The rate (bits of key per channel use) at which QKD can be accomplished is known to fall off exponentially with distance for a variety of protocols [8–11]. This rate-loss trade-off previously suggested the question of whether some other protocol could be designed to outperform the exponential fall-off. An important notion in addressing this question is the capacity (the maximum achievable rate) of a quantum channel, which is a fundamental characteristic of the channel and is independent of any specific communication protocol. The exponential fall-off has been established as a fundamental limit for bosonic loss channels [12], and a number of works [13–23] have since considered this problem and generalizations of it. However, the precise capacities of specific channels and for specific protocols are still of much interest. Ultimately, the capacities of a particular quantum channel are important factors in determining any practical uses of that channel for quantum key distribution or distributed quantum computing.

This dissertation starts as an introduction to the considerations of quantum informational sciences before addressing the problem of bounding capacities of quantum channels. We begin with a brief history of quantum information theory and review some of the fundamental tools of the trade before moving to definitions of quantities more specific to the aims of this dissertation. The main body of this work begins in Chapter 2 with a treatment of energy-constrained, two-way assisted private and quantum communication over a quantum channel, as presented in Ref. [24]. The task is formally defined in a general setting and the energy-constrained, assisted capacities are bounded by the squashed entanglement of the channel. In Chapter 3 we define a broadcast amplitude damping channel and discuss its capacities with considerations toward establishing entanglement and secret key between the involved parties. Finally, in Chapter 4 some brief reflective thoughts are given on the work presented and on interesting future directions of this research.

1.2 Historical Preliminaries for Quantum Information

I intend for this section to serve as further introduction to some of the perspectives in this work. It is for an interested party who considers themself significantly less than an expert but nonetheless
wishes to discuss quantum information theory at a ball game or holiday party. I do not wish to
diminish any of the great many important and beautiful developments not specifically addressed
in this section. Rather, I simply hope to highlight a few points to set the mood before the more
technical work begins.

The study of information theory could be argued to reach into ancient civilizations’ substitution
ciphers or into prehistoric analysis of weather and wildlife patterns, but the foundation of the
modern pursuit is widely considered to be a 1948 article by Claude Shannon [25]. Shannon’s paper
builds on and formalizes concepts ranging from the use of bits for information storage to channel
capacities. A decade earlier, Alan Turing had published\(^2\) an important paper [28] discussing the
computational problems of decision making and computability and in which he defined what we
now call a universal Turing machine (which forms the basis of much of modern computer science).
Throughout the Second World War, military funding helped fuel these two (and many lesser known)
individuals in the rapid development of encryption and codebreaking, control systems, and other
signal processing techniques. After the war, the proliferation of these techniques has led to the
information and computing age. Shannon is widely regarded as the father of information theory;
and Turing can be considered the father of modern computer science and artificial intelligence.

Although quantum mechanics does not have as obvious a father as information theory, Max
Planck laid a strong foundation in 1900 [29] in one of a series of papers addressing blackbody
radiation. The article suggested that energy is transferred in bursts instead of an uninterrupted
flow, and it proposed a constant with units of angular momentum as the unit size of these bursts.
The number now known as Planck’s constant gives the ratio of a photon’s energy to its frequency.
Planck’s constant \(h\) or its reduced form \(\hbar = \frac{h}{2\pi}\) is considered a fundamental constant of nature.

So, in quantum mechanics, we consider that properties like energy and angular momentum occur
in discrete steps rather than continuously. The term “quantum” actually means “some amount,”
and “to quantize” is to divide something into these discrete amounts. The quantum interpretation
of nature flourished in the 20\(^{th}\) century, leading to the development of many of the electronic

\(^2\)Gödel [26], Church [27], and Turing [28] each published work that equivalently define computable functions. The Church-Turing thesis expresses the equivalence of these approaches as a determination of computability.
conveniences that we use daily. It continues to be integral to our exploration of the universe as evidenced by the ubiquity of semiconductor electronics and the existence of this dissertation.

Critical to an explanation of quantum mechanics is the notion of uncertainty. Of course, this brings to mind the famous Heisenberg uncertainty principle [30], which states that the absolute precision with which complementary quantities can be measured is fundamentally limited (and this limit is related to Planck’s constant). But, really, I refer to the nondeterministic, probability driven nature of the quantum world. The roll of a die is an example of a deterministic probability problem. Each value of an ideal, fair die has a probability of $1/6$, but the outcome of the roll is determined exactly by the forces imparted on the die during and throughout the roll. We simply treat the problem with probability out of ignorance of the many important factors. Quantum mechanics is fundamentally probabilistic; the outcome is not determined by local, hidden variables as in the classical case. This idea, known as Bell’s theorem, was published by John Bell [31] in 1964 in an important article addressing the famous Einstein-Podolsky-Rosen paradox [32] and was first experimentally demonstrated in 1981 [33] and 1982 [34]. These tests received criticism for potential issues which could hide the “true” behavior of nature. Loophole-free experiments were finally published in 2015 [35–37] which seem to satisfy all but the most stubborn of local realists. Bell’s “solution” cast the problematic non-locality presented in the EPR paradox as a fundamental feature of quantum mechanics in which a measurement on one system can instantaneously affect another, distant system in a way that does not transmit classical information faster than the speed of light. This feature of non-locality is what we call entanglement.

A quantum state is a mathematical representation of some quantum system (for independent learning, illustrative examples of quantum systems include a particle in a box, a quantum harmonic oscillator, and an electron in a magnetic field). This representation can often be conveniently handled as a matrix (a vector being a matrix with a row or column count of one) which, together with a description of its evolution, completely characterizes the quantum system. Any measurable quantity (referred to as an observable) can be obtained from the quantum state by using the appropriate operator (another matrix). The three most popular mathematical “pictures” of quantum mechanics are referred to as the Heisenberg picture, which incorporates the time-dependent evolution of the system into the operators, the Schrödinger picture, which has the states evolve in time, and the
interaction picture, which splits the time dependence into both the operators and the states. In particular situations, one of these pictures may be easier to work with than the others, but in each case the mathematics follow the rules of linear algebra, making matrix manipulation an invaluable concept. Whenever a concept is unclear, it often helps to consider that the quantities involved can usually be cast as matrices, albeit sometimes the dimensions of said matrices is infinite.

A great boon in working with quantum states is the introduction of “bra-ket” notation (Dirac notation) by P.A.M. Dirac in 1939 [38]. In bra-ket notation we denote a column vector with a ket $|\psi\rangle$ consisting of an arbitrary label within a right-angled bracket. The bra $\langle \phi |$ denotes a row vector. The arbitrary labels $\psi$ and $\phi$ may be inconsequentially replaced by any convenient symbols. Bra-ket notation simplifies working with operators and vectors by condensing the number of necessary symbols and by making operator usage straightforward. Two very useful points Dirac makes in his original paper are as follows:

1. any quantity enclosed in a matching bra and ket is a number,
2. a quantity with an unclosed bra or ket is a vector in the appropriate vector space.

The notation allows quick manipulation of quantum state vectors, and these points aid in the quick conceptualization of the quantities without having to painstakingly work potentially large matrix problems or handle esoteric polynomials. While this is a development in mathematical notation rather than physics, it was made by a historically important physicist and applies directly to quantum mechanics. The original paper is a very quick read that I recommend for enrichment to all professional and hobbyist physicists.

The quantization of spin angular momentum,\(^3\) as first experimentally demonstrated in the Stern-Gerlach experiment [39], presents a convenient mechanism for digital data. In particular, spin-$\frac{1}{2}$ particles such as electrons, protons, and neutrons have two distinct spin states that we can label $|0\rangle$ and $|1\rangle$. This system, along with other two-level quantum systems, readily maps to the familiar binary values used in modern computing and communications, 0 and 1. So, if computers talk in 1s and 0s, then quantum computers should talk in $|1\rangle$s and $|0\rangle$s; if information is stored in bits, then

\(^3\)Spin angular momentum is a special property of atomic scale phenomena; it’s part of the “magic” behind magnets.
quantum information should be stored in quantum bits, or qubits for short.

The distinctness of a qubit can be represented using the Bloch sphere pictured in Fig 1.1. We have a state $|\psi\rangle$ that we restrict, such that its vector representation only touches points on the surface of the sphere. As time progresses, the angles $\theta$ and $\varphi$ may change, and $|\psi\rangle$ may wander all over the surface of the sphere. When we take a measurement of $|\psi\rangle$ as $|0\rangle$ or $|1\rangle$, the probability of the outcome is related to the distance of $|\psi\rangle$ to $|0\rangle$ or $|1\rangle$ on the $Z$ axis. But we can just as easily measure with respect to the $\pm X$ axis or the $\pm Y$ axis. This is called measuring in a different basis. And measurement of a quantum system will affect the state for future measurements. Say we take a $Z$ measurement with the result that our system is in the $|0\rangle$ state. If we then immediately perform a measurement on the $X$ axis, the system will have a perfect 50:50 chance of being in the positive and negative $X$ states, because the state vector is exactly between those two poles on the surface of the Bloch sphere. So, with a 50% chance, we measure positive $X$. If we again immediately perform a measurement, this time on $Z$ again, what is the probability of again finding the system in the $|0\rangle$ state? Could it be 100%, since we already saw the system in that state? No, the probability is distributed evenly once again with a 50:50 chance of measuring $|0\rangle$ and $|1\rangle$. The positive $X$ measurement result randomizes the probability distribution in perpendicular bases, even a previously measured basis. This effect ties in strongly with the uncertainty principle discussed above. Importantly, at times far from measurement, the system may exist in any state or a probabilistic superposition of many states; the state vector’s position on the Bloch sphere is not necessarily well defined if not taken in the context of a measurement. This phenomenon is different from simply not knowing the position before measurement, and it is an underlying mechanism of many quantum effects.

As quantum and informational sciences progressed, the overlapping study did as well. In 1973, Holevo established that, though a qubit can seemingly “hold” more, the maximum amount of classical information accessible from $n$ qubits is simply $n$ bits [40]. In 1970, James Park [41] proved that it is impossible to exactly copy an unknown quantum state; we now call this the no-cloning theorem. This contribution, however, has gone mostly unnoticed [42], and the development is commonly attributed to 1982 articles by Wootters and Zurek [43] and, independently, Dieks [44]. The BB84 protocol, published by Bennett and Brassard in 1984, takes advantage of implications of
the no-cloning theorem to keep a message secret from eavesdroppers, becoming the first quantum key distribution (QKD) protocol [8]. Quantum teleportation [45] in 1993 and Shor’s factoring algorithm [1] in 1994 opened the doors to eventual quantum advantages over classical communication and computation, respectively. For now, some of the best quantum computers [46–49] have practical limitations, but they are already available for public use or private purchase. In some cases, they have been suggested to have achieved speedups over classical computers.

1.3 Technical Preliminaries

In order to study the quantum aspects of information and communication, we first review foundational features, consisting of terms and measures that serve to describe and quantify key properties of the systems in question, as well as the operations performed on those systems. The reader can find background other than that presented here by consulting [50–54].

---

This section contains much of the background information from an article by Noah Davis, Maksim Shirokov, and Mark M. Wilde [24] which can be found at arXiv:1801.08102v2 [quant-ph].
1.3.1 Quantum Systems, States, and Channels

We denote some first Hilbert space as \( H_A \) and another one as \( H_B \). Throughout, the Hilbert spaces that we consider are generally infinite-dimensional and separable, unless stated otherwise. The tensor product of \( H_A \) and \( H_B \) is itself a Hilbert space, represented as \( H_A \otimes H_B = H_{AB} \).

Let \( L(H_A) \) denote the set of bounded linear operators acting on \( H_A \), and let \( L_+(H_A) \) denote the subset of positive, semi-definite operators acting on \( H_A \). Let \( L_1(H) \) denote the set of trace-class operators, those operators \( X \) for which the trace norm is finite:

\[
\|X\|_1 \equiv \text{Tr}\{|X|\} < \infty, 
\]

where \( |X| \equiv \sqrt{X^*X} \). The set of states (also called density operators) \( D(H_A) \subset L_+(H_A) \) contains all operators \( \rho_A \in L_+(H_A) \) such that \( \text{Tr}\{\rho_A\} = 1 \). The state \( \rho_{AB} \in D(H_{AB}) \) is called an extension of a state \( \rho_A \in D(H_A) \) if \( \rho_A = \text{Tr}_B\{\rho_{AB}\} \), where \( \text{Tr}_B \) denotes the partial trace over \( H_B \).

Every density operator \( \rho \in D(H) \) can be expressed in terms of a spectral decomposition of a denumerable number of eigenvectors and eigenvalues:

\[
\rho = \sum_i p_i |\phi_i\rangle \langle \phi_i|, \tag{1.1}
\]

where the probabilities \( \{p_i\}_i \) are the eigenvalues and \( \{|\phi_i\rangle\}_i \) are the eigenvectors. A state \( \rho \in D(H) \) is called a pure state if there exists a unit vector \( |\psi\rangle \in H \) such that \( \rho = |\psi\rangle \langle \psi| \). When this is not the case, we say that the state is a mixed state, because a spectral decomposition indicates that any state can be interpreted as a probabilistic mixture of pure states.

We can purify a state \( \rho_A = \sum_i p_i |\phi_i\rangle \langle \phi_i|_A \) by introducing a set of orthonormal vectors \( \{|i\rangle_R\}_i \) and extending it to a pure state in the tensor-product space \( H_{RA} \). Then

\[
|\psi\rangle_{RA} = \sum_i \sqrt{p_i} |\phi_i\rangle_A |i\rangle_R \tag{1.2}
\]

is a unit vector in \( H_{RA} \), and \( \rho_{RA} = |\psi\rangle \langle \psi|_{RA} \) is a pure state in \( D(H_{RA}) \). A state purification is a special kind of extension, given that \( \rho_A = \text{Tr}_R\{\rho_{RA}\} \).

A key feature of quantum systems is the phenomenon of entanglement [55]. A state made up of multiple systems is said to be entangled if it cannot be written as a probabilistic mixture of product states. For example, \( \rho_{AB} = \sum_z p_Z(z) |\psi^z\rangle \langle \psi^z|_A \otimes |\phi^z\rangle \langle \phi^z|_B \) represents an unentangled, separable
state in $D(\mathcal{H}_{AB})$ [56], where $p_Z(z)$ is a probability distribution and $\{|\psi^z\rangle_A\}_z$ and $\{|\phi^z\rangle_B\}_z$ are sets of unit vectors.

The Schmidt decomposition theorem gives us a tool for simplifying the form of pure, two-party (bipartite) states and particularly for determining whether a pure, bipartite state is entangled. An arbitrary bipartite unit vector $|\psi\rangle_{AB}$ can be written as $|\psi\rangle_{AB} = \sum_i \sqrt{p_i} |i\rangle_A |i\rangle_B$ where $\{|i\rangle_A\}_i$ and $\{|i\rangle_B\}_i$ are orthonormal bases in the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, and $\{p_i\}_i$ are strictly positive, real probabilities. The set $\{\sqrt{p_i}\}_i$ is the set of Schmidt coefficients. For finite-dimensional $|\psi\rangle_{AB}$, the number $d$ of Schmidt coefficients is called the Schmidt rank of the vector, and it satisfies the following inequality: $d \leq \min[\dim(\mathcal{H}_A), \dim(\mathcal{H}_B)]$. For infinite-dimensional $|\psi\rangle_{AB}$, the Schmidt rank $d$ can clearly be equal to infinity. The state $|\psi\rangle_{AB}$ is an entangled state if and only if $d \geq 2$. For finite-dimensional $\mathcal{H}_A$ and $\mathcal{H}_B$, such that $\mathcal{H}_A$ is isomorphic to $\mathcal{H}_B$, we define a maximally entangled state in terms of the following unit vector:

$$|\Phi\rangle_{AB} = \frac{1}{\sqrt{d}} \sum_{i=1}^d |i\rangle_A |i\rangle_B. \quad (1.3)$$

According to the Choi-Kraus theorem, a linear map $\mathcal{N}_{A\to B}$ from $\mathcal{L}_1(\mathcal{H}_A)$ to $\mathcal{L}_1(\mathcal{H}_B)$ is completely positive and trace preserving (CPTP) if and only if it can be written in the following way:

$$\mathcal{N}_{A\to B}(X_A) = \sum_l V_l X_A V_l^\dagger, \quad (1.4)$$

where $X_A \in \mathcal{L}_1(\mathcal{H}_A)$, $V_l$ is a bounded linear operator mapping $\mathcal{H}_A \to \mathcal{H}_B$, and $\sum_l V_l^\dagger V_l = I_A$. This is called the Choi-Kraus representation, and $\{V_l\}_l$ is called the set of Kraus operators. Such a linear map is referred to as a quantum channel, and it takes quantum states to other quantum states. Quantum channels can be concatenated in a serial or parallel way, and such a combination is also a quantum channel.

An isometric extension $U^N_{A\to BE}$ of a quantum channel $\mathcal{N}_{A\to B}$ is a linear isometry taking $\mathcal{H}_A$ to $\mathcal{H}_B \otimes \mathcal{H}_E$, satisfying

$$\mathcal{N}_{A\to B}(X_A) = \text{Tr}_E \{U^N_{A\to BE}(X_A)\}, \quad (1.5)$$

for all $X_A \in \mathcal{L}_1(\mathcal{H}_A)$, where the isometric channel $U^N_{A\to BE}$ is defined in terms of the isometry $U^N_{A\to BE}$
as
\[ \mathcal{U}^{N}_{A\rightarrow BE}(X_A) = \mathcal{U}^{N}_{A\rightarrow BE}X_A(\mathcal{U}^{N}_{A\rightarrow BE})^\dagger. \quad (1.6) \]

We can construct a canonical isometric extension of a quantum channel in the following way:

\[ \mathcal{U}^{N}_{A\rightarrow BE} = \sum_{l} V_l \otimes |l\rangle_E, \quad (1.7) \]

where \{\{|l\rangle_E\}\}, is an orthonormal basis. One can check that (1.5) is satisfied for this choice.

An isometric extension of a quantum channel shows that we can think of a channel as involving not only a sender and receiver but also a passive environment represented by system \(E\) above. In order to determine the output of the extended channel \(\mathcal{U}^{N}_{A\rightarrow BE}\) to the environment, we simply trace over the output system \(B\) instead of the environment \(E\). The resulting channel is known as a complementary channel [57], with the following action on an input state \(\rho_A\):

\[ \hat{\mathcal{N}}_{A\rightarrow E}(\rho_A) = \text{Tr}_{B}\{\mathcal{U}^{N}_{A\rightarrow BE}(\rho_A)\}. \quad (1.8) \]

A channel complementary to \(\mathcal{N}_{A\rightarrow B}\) is a CPTP map from \(L_1(\mathcal{H}_A)\) to \(L_1(\mathcal{H}_E)\) and is unique up to an isometry acting on the space \(\mathcal{H}_E\) (see, e.g., Ref. [51,53]).

The quantum instrument formalism provides the most general description of a quantum measurement [58]. A quantum instrument is a set of completely positive, trace non-increasing maps \(\{\mathcal{M}^{x}_{A\rightarrow B}\}_x\) such that the sum map \(\sum_{x} \mathcal{M}^{x}_{A\rightarrow B}\) is a quantum channel [58]. One can equivalently think of it as a quantum channel that takes as input a quantum system and gives as output both a quantum system and a classical system:

\[ \mathcal{M}_{A\rightarrow BX}(\rho_A) = \sum_{x} \mathcal{M}^{x}_{A\rightarrow B}(\rho_A) \otimes |x\rangle\langle x|_X. \quad (1.9) \]

Here \(\{|x\rangle\}_x\) is a classical orthonormal basis identified with the outcomes of the instrument. Throughout this paper, we consider only the case when the measurement has a finite or denumerable number of outcomes.

In discussing quantum systems corresponding to tensor-product Hilbert spaces, it is useful to
consider which parties can influence which subsystems, and we give names to the parties corresponding to the label on their subsystem. For example, it is conventional to say that Alice has access to system $A$, Bob to system $B$, and Eve to system $E$, which we often refer to as the environment as well. Eve is so named because the third party is regarded as a passive adversary or eavesdropper in a cryptographic context. By taking system $E$ to encompass anything not in another specified system, we can consider the most general cases of Eve’s participation.

In this thesis, we consider the use of a quantum channel interleaved with rounds of local operations and classical communication (LOCC). These rounds of LOCC can be considered channels themselves as follows:

1. Alice performs a quantum instrument on her system, resulting in both quantum and classical outputs.

2. Alice sends a copy of the classical output to Bob.

3. Bob performs a quantum channel on his system conditioned on the classical data that he receives from Alice.

4. Bob then performs a quantum instrument on his system and forwards the classical output to Alice.

5. Finally, Alice performs a quantum channel on her system conditioned on the classical data from Bob.

6. Iterate the above steps an arbitrarily large, yet finite number of times.

The sequence of actions in the first through third steps is called “local operations and one-way classical communication,” and they can be expressed as a quantum channel of the following form:

$$ S_{AB} \equiv \sum_z G_A^z \otimes J_B^z, $$

where $\{G_A^z\}$ is a denumerable set of completely positive, trace non-increasing maps, such that the sum map $\sum_z G_A^z$ is trace preserving, and $\{J_B^z\}$ is a set of channels. These conditions imply that
$S_{AB}$ is a channel. The fourth and fifth steps above can also take the form of (1.10) with the system labels reversed.

As indicated above, a full round of LOCC consists of the concatenation of some number of these channels back and forth between Alice and Bob [59,60]. This concatenation is a particular kind of separable channel and takes the form

$$L_{AB} \equiv \sum_y E^y_A \otimes F^y_B,$$

where $\{E^y_A\}_y$ and $\{F^y_B\}_y$ are denumerable sets of completely positive, trace non-increasing maps such that $L_{AB}$ is CPTP. We stress again that we only consider LOCC channels with a finite or denumerable number of classical values, and we refer to them as denumerably decomposable LOCC channels.

1.3.2 Trace Distance and Quantum Fidelity

We defined the trace norm $\|X\|_1$ of an operator $X$ previously. Being a norm, it is homogeneous, non-negative definite, and obeys the triangle inequality. It is also convex and invariant under multiplication by isometries; i.e., for $\lambda \in [0, 1]$, we have that $\|\lambda X + (1-\lambda)Y\|_1 \leq \lambda \|X\|_1 + (1-\lambda)\|Y\|_1$, and for isometries $U$ and $V^\dagger$, we have that $\|UXV^\dagger\|_1 = \|X\|_1$.

The trace norm of an operator leads to the trace distance between two of them. The trace distance between two density operators $\rho$ and $\sigma$ quantifies the distinguishability of the two states [61–63] and satisfies the inequality: $0 \leq \|\rho - \sigma\|_1 \leq 2$. From the triangle inequality, we see that the trace distance is maximized for orthogonal states; i.e., when $\rho\sigma = 0$, then $\|\rho - \sigma\|_1 = \|\rho\|_1 + \|\sigma\|_1 = 2$. Note that sometimes we employ the normalized trace distance, which is equal to half the usual trace distance: $0 \leq \frac{1}{2}\|\rho - \sigma\|_1 \leq 1$.

Another way to measure the closeness of quantum states is given by the quantum fidelity [64]. The pure-state fidelity for pure-state vectors $|\psi\rangle_A$ and $|\phi\rangle_A$ is given by

$$F(\psi_A, \phi_A) \equiv |\langle \psi | \phi \rangle_A|^2,$$
from which we conclude that $0 \leq F(\psi_A, \phi_A) \leq 1$. The general definition of the fidelity for arbitrary density operators $\rho_A$ and $\sigma_A$ is as follows:

$$F(\rho_A, \sigma_A) \equiv \|\sqrt{\rho_A}\sqrt{\sigma_A}\|_1^2. \quad (1.13)$$

Uhlmann’s theorem is the statement that the following equality holds [64]:

$$F(\rho_A, \sigma_A) = \sup_{U_R} |\langle \phi^\rho |_{RA} U_R \otimes I_A |\phi^\sigma \rangle_{RA}|^2, \quad (1.14)$$

where $|\phi^\rho \rangle_{RA}$ and $|\phi^\sigma \rangle_{RA}$ are purifications of $\rho_A$ and $\sigma_A$ with purifying system $R$ and $U_R$ is a unitary acting on system $R$.

1.3.3 Entropy and Information

In order to study the information contained and transmitted in various systems and operations, we now recall a number of common measures used to quantify information. With these measures defined below, we also focus on generalizations of the quantities as functions of operators acting on infinite-dimensional, separable Hilbert spaces, as considered in, e.g., Ref. [65]. The first and most common measure is the quantum entropy and is defined for a state $\rho \in \mathcal{D}(\mathcal{H})$ as

$$H(\rho) \equiv \text{Tr}\{\eta(\rho)\}, \quad (1.15)$$

where $\eta(x) = -x \log_2 x$ if $x > 0$ and $\eta(0) = 0$. The trace in the above equation can be taken with respect to any denumerable orthonormal basis of $\mathcal{H}$ [66, Definition 2]. The quantum entropy is a non-negative, concave, lower semicontinuous function on $\mathcal{D}(\mathcal{H})$ [67]. It is also not necessarily finite (see, e.g., Ref. [68]). When $\rho_A$ is the state of a system $A$, we write

$$H(A)_{\rho} \equiv H(\rho_A). \quad (1.16)$$

The entropy is a familiar thermodynamic quantity and is roughly a measure of the disorder in a system. One property of quantum entropy that we use here is its duality: for a pure state $|\psi\rangle \langle \psi|_{RA}$,
quantum entropy is such that \( H(A) = H(R) \).

For a positive semi-definite, trace-class operator \( \omega \) such that \( \text{Tr}\{\omega\} \neq 0 \), we extend the definition of quantum entropy as

\[
H(\omega) \equiv \text{Tr}\{\omega\} H\left( \frac{\omega}{\text{Tr}\{\omega\}} \right).
\]

Observe that \( H(\omega) \) reduces to the definition in (1.15) when \( \omega \) is a state with \( \text{Tr}\{\omega\} = 1 \).

Furthermore, the quantum entropies of any two-party division of a pure state will be equal as in the following example. For a five-party pure state \(|\psi\rangle_{ABCDE}\), we have that

\[
H(ABCD) = H(E),
\]

\[
H(ABC) = H(DE),
\]

\[
H(AB) = H(CDE),
\]

\[
H(A) = H(BCDE).
\]

This property is true only for splits which contain all constituent parties of the pure state. In general \( H(AB) \) will not be equal to \( H(DE) \) unless the extension to the \( C \) system is trivial, so that \(|\psi\rangle_{ABDE}\) is also a pure state.

The quantum relative entropy \( D(\rho||\sigma) \) of \( \rho, \sigma \in \mathcal{D}(\mathcal{H}) \) is defined as [69,70]

\[
D(\rho||\sigma) \equiv [\ln 2]^{-1} \sum_{i,j} |\langle \phi_i | \psi_j \rangle|^2 [p(i) \ln \left( \frac{p(i)}{q(j)} \right) + q(j) - p(i)],
\]

where \( \rho = \sum_i p(i) |\phi_i \rangle \langle \phi_i | \) and \( \sigma = \sum_j q(j) |\psi_j \rangle \langle \psi_j | \) are spectral decompositions of \( \rho \) and \( \sigma \) with \( \{ |\phi_i \rangle \}_i \) and \( \{ |\psi_j \rangle \}_j \) orthonormal bases. The prefactor \([\ln 2]^{-1}\) is there to ensure that the units of the quantum relative entropy are bits. We take the convention in (1.19) that \( 0 \ln 0 = 0 \ln \left( \frac{0}{0} \right) = 0 \) but \( \ln \left( \frac{0}{c} \right) = +\infty \) for \( c > 0 \). Each term in the sum in (1.19) is non-negative due to the inequality

\[
x \ln(x/y) + y - x \geq 0
\]

holding for all \( x, y \geq 0 \) [69]. Thus, by Tonelli’s theorem, the sums in (1.19) may be taken in either
order as discussed in Refs. [69,70], and it follows that

$$D(\rho\|\sigma) \geq 0$$

(1.21)

for all $\rho, \sigma \in \mathcal{D}(\mathcal{H})$, with equality holding if and only if $\rho = \sigma$ [69]. If the support of $\rho$ is not contained in the support of $\sigma$, then $D(\rho\|\sigma) = +\infty$. The converse statement need not hold in general: there exist $\rho, \sigma \in \mathcal{D}(\mathcal{H})$ with the support of $\rho$ contained in the support of $\sigma$ such that $D(\rho\|\sigma) = +\infty$. Thus, for states $\rho$ and $\sigma$, we have that

$$D(\rho\|\sigma) \in [0, \infty].$$

(1.22)

It is also worth noting that relative entropy is not generally symmetric; i.e., there exist states $\rho$ and $\sigma$ for which

$$D(\rho\|\sigma) \neq D(\sigma\|\rho).$$

(1.23)

One of the most important properties of the quantum relative entropy $D(\rho\|\sigma)$ is that it is monotone with respect to a quantum channel $\mathcal{N} : \mathcal{L}_1(\mathcal{H}_A) \to \mathcal{L}_1(\mathcal{H}_B)$ [71]:

$$D(\rho\|\sigma) \geq D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)).$$

(1.24)

The above inequality is often called the “data processing inequality.” This inequality implies that the quantum relative entropy is invariant under the action of an isometry $U$:

$$D(\rho\|\sigma) = D(U\rho U^\dagger\|U\sigma U^\dagger).$$

(1.25)

The quantum mutual information of a bipartite state $\rho_{AB}$ is defined in terms of the relative entropy [70] as

$$I(A; B)_\rho \equiv D(\rho_{AB}\|\rho_A \otimes \rho_B).$$

(1.26)
Note that, with this definition, we have that

\[ I(A; B)_\rho \in [0, \infty] \] (1.27)

as a consequence of (1.22). The following inequality applies to quantum mutual information [70]:

\[ I(A; B)_\rho \leq 2 \min\{H(A)_\rho, H(B)_\rho\} \] (1.28)

and establishes that it is finite if one of the marginal entropies is finite. For a general positive semi-definite trace-class operator \( \omega_{AB} \) such that \( \text{Tr}\{\omega_{AB}\} \neq 0 \), we extend the definition of mutual information as in Ref. [72]

\[ I(A; B)_\omega \equiv \text{Tr}\{\omega\}I(A; B)_{\omega_{\text{tr}(\omega)}}. \] (1.29)

Note that, while the relative entropy is not generally symmetric, mutual information is symmetric under the exchange of systems \( A \) and \( B \)

\[ I(A; B)_\rho = I(B; A)_\rho, \] (1.30)

due to (1.25) and by taking the isometry therein to be a unitary swap of the systems \( A \) and \( B \). For a state \( \rho_{AB} \) such that the entropies \( H(A)_\rho \) and \( H(B)_\rho \) are finite, the mutual information reduces to

\[ I(A; B)_\rho = H(A)_\rho + H(B)_\rho - H(AB)_\rho. \] (1.31)

For a state \( \rho_{AB} \) such that \( H(A)_\rho < \infty \), the conditional entropy is defined as [73]

\[ H(A|B)_\rho \equiv H(A)_\rho - I(A; B)_\rho, \] (1.32)

and the same definition applies for a positive semi-definite trace-class operator \( \omega_{AB} \), by employing the extended definitions of entropy in (1.17) and mutual information in (1.29). Thus, as a
consequence of the definition, (1.28), and the duality relation in (1.35) below, we have that

\[ H(A|B)_\rho \in [-H(A)_\rho, H(A)_\rho] . \] (1.33)

If \( H(B)_\rho \) is also finite, then the conditional entropy simplifies to the following more familiar form:

\[ H(A|B)_\rho = H(AB)_\rho - H(B)_\rho. \] (1.34)

For a tripartite pure state \( \psi_{ABC} \) such that \( H(A)_\psi < \infty \), the conditional entropy satisfies the following duality relation [73]:

\[ H(A|B)_\psi = -H(A|C)_\psi. \] (1.35)

Ref. [73, Proposition 1] states that conditional entropy is subadditive: for a four-party state \( \rho_{ABCD} \), we have that

\[ H(AB|CD)_\rho \leq H(A|C)_\rho + H(B|D)_\rho. \] (1.36)

This in turn is a consequence of the strong subadditivity of quantum entropy [74,75].

The conditional quantum mutual information (CQMI) of tripartite states \( \omega_{ABE} \in \mathcal{D}(\mathcal{H}_{ABE}) \), with \( \mathcal{H}_{ABE} \) a separable Hilbert space, was defined only recently in Ref. [72], as a generalization of the information measure commonly used in the finite-dimensional setting. The definition from Ref. [72] involves taking a supremum over all finite-rank projections \( P_A \in \mathcal{L}(\mathcal{H}_A) \) or \( P_B \in \mathcal{L}(\mathcal{H}_B) \), in order to write CQMI in terms of the quantum mutual information in the following equivalent ways:

\[ I(A; B|E)_\omega = \sup_{P_A} I(A; BE)_{Q_A \omega Q_A} - I(A; E)_{Q_A \omega Q_A} \] (1.37)

\[ = \sup_{P_B} I(AE; B)_{Q_B \omega Q_B} - I(E; B)_{Q_B \omega Q_B}, \] (1.38)

where \( Q_A = P_A \otimes I_{BE} \) and \( Q_B = P_B \otimes I_{AE} \). Due to the data-processing inequality in (1.24), with the channel taken to be a partial trace, we have that

\[ I(A; B|E)_\omega \in [0, \infty]. \] (1.39)
The conditional mutual information, as defined above, is a lower semi-continuous function of tripartite quantum states \[72, \text{Theorem 2}\]; i.e., for any sequence \(\{\omega^n_{ABE}\}_n\) of tripartite states converging to the state \(\omega^0_{ABE}\), the following inequality holds

\[
\liminf_{n \to \infty} I(A; B|E)_{\omega^n} \geq I(A; B|E)_{\omega^0}.
\]  

(1.40)

If \(I(A; BE)_{\omega}, I(A; E)_{\omega} < \infty\), as is the case if \(H(A)_{\omega} < \infty\), then the definition reduces to the familiar one from the finite-dimensional case:

\[
I(A; B|E)_{\omega} = I(A; BE)_{\omega} - I(A; E)_{\omega}.
\]  

(1.41)

For more examples of these entropies see Refs. \[53, 54\], and for more details on derivation of these quantities in infinite dimensions see Refs. \[73\] and \[65\].

1.3.4 Squashed Entanglement

The information measure of most concern in this thesis is the squashed entanglement. Defined and analyzed in Ref \[76\], and extended to the infinite-dimensional case in Ref \[65\], the squashed entanglement of a state \(\rho_{AB} \in \mathcal{D}(\mathcal{H}_{AB})\) is defined as \[76\]

\[
E_{sq}(A; B)_{\rho} = \frac{1}{2} \inf_{\omega_{ABE}} I(A; B|E)_{\omega},
\]  

(1.42)

where \(\omega_{ABE} \in \mathcal{D}(\mathcal{H}_{ABE})\) satisfies \(\text{Tr}_E\{\omega_{ABE}\} = \rho_{AB}\), with \(\mathcal{H}_E\) taken to be an infinite-dimensional, separable Hilbert space. (See Refs. \[77, 78\] for discussions related to squashed entanglement.) An equivalent definition is given in terms of an optimization over squashing channels, as follows:

\[
E_{sq}(A; B)_{\rho} = \frac{1}{2} \inf_{\mathcal{S}_{E \to E'}} I(A; B|E')_{\tau},
\]  

(1.43)

where \(\tau_{ABE'} = \mathcal{S}_{E \to E'}(\phi_{ABE}^\rho)\), with \(\phi_{ABE}^\rho\) a purification of \(\rho_{AB}\). The infimum is with respect to all squashing channels \(\mathcal{S}_{E \to E'}\) from system \(E\) to a system \(E'\), the latter corresponding to an infinite-dimensional, separable Hilbert space. The reasoning for this equivalence is the same as that given
in Ref. [76]. Due to the expression in (1.43), squashed entanglement can be interpreted as the leftover correlation after an adversary attempts to “squash down” the correlations in $\rho_{AB}$. Squashed entanglement obeys many of the properties considered important for an entanglement measure, such as LOCC monotonicity, additivity for product states, and convexity [76]. These properties are discussed in the next section.

Suppose that Alice, in possession of the systems $RA$ of a pure state $\phi_{RA}$, wishes to construct a shared state with Bob. If Alice and Bob are connected by a quantum channel $\mathcal{N}_{A\rightarrow B}$ mapping system $A$ to $B$, then they can establish the shared state

$$\omega_{RB} = \mathcal{N}_{A\rightarrow B}(\phi_{RA}). \quad (1.44)$$

Going to the purified picture, an isometric channel $\mathcal{U}_{A\rightarrow BE}^\mathcal{N}$ extends $\mathcal{N}_{A\rightarrow B}$, so that the output state of the extended channel is $\phi_{RBE} = \mathcal{U}_{A\rightarrow BE}^\mathcal{N}(\phi_{RA})$ when the input is $\phi_{RA}$. Suppose that a third party Eve has access to the system $E$, such that she could then perform a squashing channel $\mathcal{S}_{E\rightarrow E'}$, bringing system $E$ to system $E'$. In this way, she could attempt to thwart the correlation between Alice and Bob’s systems, as measured by conditional mutual information. Related to the above physical picture, the squashed entanglement of the channel $\mathcal{N}_{A\rightarrow B}$ is defined as the largest possible squashed entanglement that can be realized between systems $R$ and $B$ [12,79]:

$$E_{sq}(\mathcal{N}) \equiv \sup_{\phi_{RA}} E_{sq}(R;B)_{\omega}, \quad (1.45)$$

where the supremum is with respect to all possible pure bipartite input states $\phi_{RA}$, with system $R$ isomorphic to system $A$, and $\omega_{RB}$ is defined in (1.44).

If specific requirements are placed on the channel input states, such as an energy constraint as discussed in Section 2.2.1 below, the optimization should reflect those stipulations, leading to the energy-constrained squashed entanglement of a channel $\mathcal{N}$:

$$E_{sq}(\mathcal{N},G,P) \equiv \sup_{\phi_{RA}: \text{Tr}(G\phi_{A}) \leq P} E_{sq}(R;B)_{\omega}. \quad (1.46)$$

Here $G$ is an energy observable (Hamiltonian) acting on the channel input system $A$, the positive
real $P \in [0, \infty)$ is a constraint on the expected value of that observable such that $\text{Tr}\{G\phi_A\} \leq P$, and the supremum is with respect to all pure input states $\phi_{RA}$ to the channel that obey the given constraint. It suffices to optimize the quantity in (1.46) with respect to pure, bipartite input states, following from purification, the Schmidt decomposition theorem, and LOCC monotonicity of squashed entanglement. These notions are discussed in more detail in Section 2.2.

As discussed in Ref. [79], the squashed entanglement of a channel can be written in a different way by considering an isometric channel $V_{SE \rightarrow E'} \circ U_{A \rightarrow BE}$ extending the squashing channel $S_{E \rightarrow E'}$. Let $\varphi_{RE'E'}$ denote the following pure output state when the pure state $\phi_{RA}$ is input:

$$\varphi_{RE'E'} = (V_{SE \rightarrow E'} \circ U_{A \rightarrow BE}) (\phi_{RA}).$$  

(1.47)

By taking advantage of the duality of conditional entropy and in the case that the entropy $H(B)_{\varphi}$ is finite, the alternate way of writing follows from the equality

$$I(R; B|E')_{\varphi} = H(B|E')_{\varphi} - H(B|RE')_{\varphi}$$

$$= H(B|E')_{\varphi} + H(B|F)_{\varphi}.$$  

(1.48)

Thus, we can write the energy-constrained squashed entanglement of a channel as

$$E_{sq}(\mathcal{N}, G, P) = \sup_{\rho_A: \text{Tr}\{G\rho_A\} \leq P} E_{sq}(\rho_A, \mathcal{N}_{A \rightarrow B}),$$

(1.50)

where

$$E_{sq}(\rho_A, \mathcal{N}_{A \rightarrow B}) \equiv \inf_{\omega_{RE'E'}} \frac{1}{2} [H(B|E')_{\omega} + H(B|F)_{\omega}],$$

(1.51)

$$\omega_{BE'F} = (V_{SE \rightarrow E'} \circ U_{A \rightarrow BE}) (\rho_A),$$

(1.52)

and we take advantage of the representation in (1.50) in our paper.

1.3.5 Entanglement Monotones and Squashed Entanglement

In this section, we review the notion of an entanglement monotone [55] and how squashed entanglement [76] and its extended definition in Ref. [65] satisfies the requirements of being an entanglement monotone. Let $E(A; B)_{\omega}$ be a function of an arbitrary bipartite state $\omega_{AB}$. Then
$E(A; B)_{\omega}$ is an entanglement monotone if it satisfies the following conditions:

1) $E(A; B)_{\omega} = 0$ if and only if $\omega_{AB}$ is separable.

2) $E$ is monotone under selective unilocal operations. That is,

$$E(A; B)_{\omega} \geq \sum_k p_k E(A; B)_{\omega^k},$$

(1.53)

where

$$p_k = \text{Tr}(\mathcal{N}_A^k(\omega_{AB})), \quad \omega_{AB}^k = p_k^{-1} \mathcal{N}_A^k(\omega_{AB})$$

(1.54)

for any state $\omega_{AB}$ and any collection $\{\mathcal{N}_A^k\}$ of unilocal completely positive maps such that the sum map $\sum_k \mathcal{N}_A^k$ is a channel.

3) $E$ is convex, in the sense that for states $\rho_{AB}^0$, $\rho_{AB}^1$, and $\rho_{AB}^\lambda = \lambda \rho_{AB}^0 + (1 - \lambda) \rho_{AB}^1$, where $\lambda \in [0, 1]$,

$$E(A; B)_{\rho^\lambda} \leq \lambda E(A; B)_{\rho^0} + (1 - \lambda) E(A; B)_{\rho^1}$$

(1.55)

When the condition in 3) holds, then the condition in 2) is equivalent to monotonicity under LOCC.

An entanglement monotone is additionally considered an entanglement measure if, for any pure state $\psi_{AB}$, it is equal to the quantum entropy of a marginal state:

$$E(A; B)_{\psi} = H(A)_{\psi} = H(B)_{\psi}.$$  

(1.56)

Other desirable properties for an entanglement monotone include

• additivity for a product state $\omega_{AB} \otimes \theta_{A'B'}$:

$$E(A'A'; B'B')_{\omega \otimes \theta} = E(A; B)_{\omega} + E(A'; B')_{\theta},$$

(1.57)

• subadditivity for a product state $\omega_{AB} \otimes \theta_{A'B'}$:

$$E(A'A'; B'B')_{\omega \otimes \theta} \leq E(A; B)_{\omega} + E(A'; B')_{\theta},$$

(1.58)
• strong superadditivity for a state $\omega_{AA'BB'}$:

$$E(AA';BB')_\omega \geq E(A;B)_\omega + E(A';B')_\omega, \quad (1.59)$$

• monogamy for a state $\omega_{ABC}$:

$$E(A;BC)_\omega \geq E(A;B)_\omega + E(A;C)_\omega, \quad (1.60)$$

• asymptotic continuity:

$$\lim_{n \to \infty} \frac{E(\rho^n_{AB}) - E(\sigma^n_{AB})}{1 + \log_2(\dim \mathcal{H}_{AB})} = 0, \quad (1.61)$$

which should hold for any sequences $\{\rho^n_{AB}\}_n$ and $\{\sigma^n_{AB}\}_n$ of states such that $\|\rho^n_{AB} - \sigma^n_{AB}\|_1$ converges to zero as $n \to \infty$.

As discussed in Ref. [65], for states in infinite-dimensional Hilbert spaces, global asymptotic continuity is too restrictive. For example, the discontinuity of the quantum entropy means that any entanglement monotone that possesses property (1.56) is necessarily discontinuous. It is therefore reasonable to require instead that $E$ is lower semi-continuous [65]:

$$\liminf_{n \to \infty} E(\omega^n_{AB}) \geq E(\omega^0_{AB}) \quad (1.62)$$

for any sequence $\{\omega^n_{AB}\}$ of states converging to the state $\omega^0_{AB}$ in trace norm.

The squashed entanglement obeys all of the above properties [65, 76, 80–84]. It additionally satisfies the following uniform continuity inequality: Given states $\rho_{AB}$ and $\sigma_{AB}$ satisfying

$$\frac{1}{2} \|\rho_{AB} - \sigma_{AB}\|_1 \leq \varepsilon \text{ for } \varepsilon \in [0, 1]$$

then

$$|E_{sq}(A;B)_\rho - E_{sq}(A;B)_\sigma| \leq \sqrt{2\varepsilon} \log_2 \min[\dim(H_A), \dim(H_B)] + g(\sqrt{2\varepsilon}) \quad (1.63)$$

where

$$g(x) \equiv (1 + x) \log_2(1 + x) - x \log_2(x). \quad (1.64)$$

This follows by combining the well known Fuchs–van de Graaf inequalities [85], Uhlmann’s theorem for fidelity [64], and the continuity bound from Ref. [86, Corollary 1] for conditional mutual information.
1.3.6 Private States

The main goal of any key distillation protocol is for two parties Alice and Bob to distill a tripartite state as close as possible to an ideal tripartite secret-key state, which is protected against a third-party Eve. An ideal tripartite secret-key state $\gamma_{ABE}$ is such that local projective measurements $\mathcal{M}_A$ and $\mathcal{M}_B$ on it, in the respective orthonormal bases $\{|i\rangle_A\}_i$ and $\{|i\rangle_B\}_i$, lead to the following form:

$$(\mathcal{M}_A \otimes \mathcal{M}_B)(\gamma_{ABE}) = \frac{1}{K} \sum_{i=1}^{K} |i\rangle_A \langle i| \otimes |i\rangle_B \otimes \sigma_E.$$  \hspace{1cm} (1.65)

The key systems are finite-dimensional, but the eavesdropper’s system $E$ could be described by an infinite-dimensional, separable Hilbert space. The tripartite key state $\gamma_{ABE}$ contains $\log_2 K$ bits of secret key. By inspecting the right-hand side of (1.65), we see that the key value is uniformly random and perfectly correlated between systems $A$ and $B$, as well as being in tensor product with the state of system $E$, implying that the results of any experiment on the $AB$ systems will be independent of those given by an experiment conducted on the $E$ system. While a perfect ideal tripartite key state may be difficult to achieve in practice, a state that is nearly indistinguishable from the ideal case is good enough for practical purposes. If a state $\rho_{ABE}$ satisfies the following inequality:

$$F(\gamma_{ABE}, \rho_{ABE}) \geq 1 - \varepsilon,$$  \hspace{1cm} (1.66)

for some $\varepsilon \in [0,1]$ and $\gamma_{ABE}$ an ideal tripartite key state, then $\rho_{ABE}$ is called an $\varepsilon$-approximate tripartite key state [19,87,88].

By purifying a tripartite secret-key state $\gamma_{ABE}$ with “shield systems” $A'$ and $B'$ and then tracing over the system $E$, the resulting state is called a bipartite private state, which takes the following form [87,88]:

$$\gamma_{ABA'B'} = U_{ABA'B'}(|\Phi\rangle\langle\Phi|_{AB} \otimes \sigma_{A'B'})U_{ABA'B'}^\dagger,$$  \hspace{1cm} (1.67)

where

$$|\Phi\rangle_{AB} = \frac{1}{\sqrt{K}} \sum_{i=1}^{K} |i\rangle_A |i\rangle_B$$  \hspace{1cm} (1.68)

is a maximally entangled state with Schmidt rank $K$ and $\sigma_{A'B'}$ is an arbitrary state of the shield.
systems $A'B'$. Due to the fact that the system $E$ of the tripartite key state $\gamma_{ABE}$ corresponds generally to an infinite-dimensional, separable Hilbert space, the same is true for the shield systems $A'B'$ of $\gamma_{ABA'B'}$. The unitary operator $U_{ABA'B'}$ is called a “twisting” unitary and has the following form:

$$U_{ABA'B'} = \sum_{i,j=1}^{K} |i\rangle_A \otimes |j\rangle_B \otimes U_{ij}^{AB},$$  

(1.69)

where each $U_{ij}^{AB}$ is a unitary operator. Note that, due to the correlation between the $A$ and $B$ systems in the state $\Phi_{AB}$, only the diagonal terms $U_{ii}^{AB}$ of the twisting unitary are relevant when measuring the systems $A$ and $B$ in the orthonormal bases $\{|i\rangle_A\}_i$ and $\{|i\rangle_B\}_i$, respectively [87,88].

If a state $\rho_{ABA'B'}$ satisfies

$$F(\gamma_{ABA'B'}, \rho_{ABA'B'}) \geq 1 - \varepsilon,$$

(1.70)

for some $\varepsilon \in [0,1]$ and $\gamma_{ABA'B'}$ an ideal bipartite private state, then $\rho_{ABA'B'}$ is called an $\varepsilon$-approximate bipartite private state [19,87,88].

The converse of the above statement holds as well [87,88], and the fact that it does is one of the main reasons that the above notions are useful in applications. That is, given a bipartite private state of the form in (1.67), we can then purify it by an $E$ system, and tracing over the shield systems $A'B'$ leads to a tripartite key state of the form in (1.65). These relations extend to the approximate case as well, by an application of Uhlmann’s theorem for fidelity [64]: purifying an $\varepsilon$-approximate tripartite key state $\rho_{ABE}$ with shield systems $A'B'$ and tracing over system $E$ leads to an $\varepsilon$-approximate bipartite private state, and vice versa.

The squashed entanglement of a bipartite private state of $\log_2 K$ bits is normalized such that [82]

$$E_{sq}(AA'; BB')_\gamma \geq \log_2 K.$$  

(1.71)

This result has recently been extended to the approximate case: Ref. [21, Theorem 2] establishes that, for an $\varepsilon$-approximate bipartite private state $\rho_{ABA'B'}$, the following inequality holds

$$E_{sq}(AA'; BB')_\rho + 2\sqrt{\varepsilon} \log_2 K + 2g(\sqrt{\varepsilon}) \geq \log_2 K.$$  

(1.72)

24
2 Energy-Constrained Two-Way Assisted Private and Quantum Capacities

With an established idea of private states, we move on to the capacity of a quantum channel to send private information with the assistance of local operations and classical communication (LOCC) on the parts of the sender, receiver, and eavesdropper. Before considering the capacities of the channels and in order to bound those capacities we must make some developments in our tools: particularly, the Conditional Quantum Mutual Information (CQMI). We then discuss the communication task in detail, including defining and establishing bounds on the energy-constrained, two-way assisted private capacity of a quantum channel. In Sections 2.5 and 2.6, these ideas are considered in a multipartite setting of which the single-sender, single-receiver case can be considered a specific example.

2.1 Properties of Conditional Quantum Mutual Information

In this section, we establish a number of simple properties of conditional quantum mutual information (CQMI) for states of infinite-dimensional, separable Hilbert spaces. These properties will be useful in later sections of this thesis.

2.1.1 CQMI and Duality under a Finite-Entropy Assumption

Lemma 1 (Duality) Let $\psi_{ABED}$ be a pure state such that $H(B)_{\psi} < \infty$. Then the conditional quantum mutual information $I(A; B|E)_{\psi}$ can be written as

$$I(A; B|E)_{\psi} = H(B|E)_{\psi} + H(B|D)_{\psi}. \quad (2.1)$$

Proof. Begin with the definition of CQMI from (1.38):

$$I(A; B|E)_{\psi} = \sup_{P_B} [I(B; AE)_{Q_B\psi Q_B} - I(B; E)_{Q_B\psi Q_B} : Q_B = P_B \otimes I_{AE}], \quad (2.2)$$

This chapter consists largely of sections from an article by Noah Davis, Maksim Shirokov, and Mark M. Wilde [24] which can be found at arXiv:1801.08102v2 [quant-ph].
where we have exploited the symmetry of mutual information as recalled in (1.30). The assumption $H(B) < \infty$ is strong, implying that $I(B; AE) < \infty$, so that we can write $I(A; B|E) = I(B; AE) - I(B; E)$ [72]. Then we find that

$$I(A; B|E) = H(B) - H(B) + I(B; AE) - I(B; E).$$

From the definition in (1.32), it is clear that the last line is equal to a difference of conditional entropies, leading to

$$I(A; B|E) = H(B|E) - H(B|AE).$$

Finally, we invoke the duality of conditional entropy from (1.35) in order to arrive at the statement of the lemma. ■

### 2.1.2 Subadditivity Lemma for Conditional Quantum Mutual Information

In this section, we prove a lemma that generalizes one of the main technical results of Refs. [12, 79] to the infinite-dimensional setting of interest here. This lemma was the main tool used in Refs. [12, 79] to prove that the squashed entanglement of a quantum channel is an upper bound on its secret-key-agreement capacity. After Refs. [12, 79] appeared, this lemma was later interpreted as implying that amortization does not increase the squashed entanglement of a channel [89–91].

**Lemma 2** Let $\phi_{A'AB'E'F''}$ be a pure state, and let $U_{A\rightarrow BE'F'}$ be an isometric quantum channel. Set

$$\psi_{A'BB'E'E'F'F''} \equiv U_{A\rightarrow BE'F'}(\phi_{A'AB'E''F''}),$$

and suppose that $H(B) < \infty$. Then the following inequality holds

$$I(A'; BB'|E'E'') \leq H(B|E') + H(B|F') + I(A' A; B'|E'').$$

Note that both sides of the inequality in (2.6) could be equal to $+\infty$.
Proof. Let \( \{P^k_{B'}\}_k \) be a sequence of finite-rank projectors acting on the space \( \mathcal{H}_{B'} \), which strongly converges to the identity \( I_{B'} \). Define the sequence \( \{\phi^k_{A'AB'E''F''}\}_k \) of projected states as

\[
\phi^k_{A'AB'E''F''} = \lambda_k^{-1}[(P^k_{B'} \otimes T)\phi_{A'AB'E''F''}(P^k_{B'} \otimes T)],
\]

where

\[
T \equiv I_{A'} \otimes I_A \otimes I_{E''} \otimes I_{F''},
\]

\[
\lambda_k \equiv \text{Tr}\{(P^k_{B'} \otimes T)\phi_{A'AB'E''F''}\},
\]

\[
\lim_{k \to \infty} \lambda_k = 1.
\]

This then leads to the following sequence of projected states:

\[
\psi^k_{A'B'B'E'E''F''F''} \equiv \mathcal{U}_{A \to B'E'F'}(\phi^k_{A'AB'E''F''}).
\]

Note that each state \( \psi^k_{A'B'B'E'E''F''F''} \) is pure for all \( k \geq 1 \). Then the conditional entropy and the conditional mutual information of the sequence converge to those of the original state [72, 73]:

\[
\lim_{k \to \infty} H(B|E')_{\psi^k} = H(B|E')_{\psi},
\]

\[
\lim_{k \to \infty} H(B|F')_{\psi^k} = H(B|F')_{\psi},
\]

\[
\lim_{k \to \infty} I(A'; B\overline{B}_k|E'E'')_{\psi^k} = I(A'; B\overline{B}'|E'E'')_{\psi},
\]

\[
\lim_{k \to \infty} I(A'A; \overline{B}_k|E'')_{\phi^k} = I(A'A; B'|E'')_{\phi}.
\]

The limits in (2.12)–(2.13) follow because \( \lim_{k \to \infty} H(B)_{\psi^k} = H(B)_{\psi} < \infty \), by applying Ref. [72, Lemma 2] and Ref. [73, Proposition 2]. The limits in (2.14)–(2.15) follow, with possible \(+\infty\) on the right-hand side, from the lower semicontinuity of conditional quantum mutual information and its monotonicity under local operations [72, Theorem 2].

Due to the fact that \( H(B\overline{B}_k)_{\psi^k} < \infty \) for all \( k \geq 1 \), we can write the CQMI of the state \( \psi^k_{A'B'B'E'E''F''F''} \) in terms of conditional entropies as in (2.4) and then use the duality of conditional
entropy as in (1.35) to find that

\[
I(A'; B B_k^\ell|E' E'')_{\psi^k} = H(B B_k^\ell|E' E'')_{\psi^k} - H(B B_k^\ell|A' E' E'')_{\psi^k} \\
= H(B B_k^\ell|E' E'')_{\psi^k} + H(B B_k^\ell|F' F'')_{\psi^k}.
\]

We then employ the subadditivity of conditional entropy from (1.36) to split up each of these two terms and regroup the resulting terms:

\[
H(B B_k^\ell|E' E'')_{\psi^k} + H(B B_k^\ell|F' F'')_{\psi^k} \leq H(B|E')_{\psi^k} + H(B|F')_{\psi^k} + I(A' A'; B B_k^\ell|E' E'')_{\phi^k}
\]

This is then recognizable as two conditional entropies from after the channel use added to the conditional mutual information from before the channel use:

\[
I(A'; B B_k^\ell|E' E'')_{\psi^k} \leq H(B|E')_{\psi^k} + H(B|F')_{\psi^k} + I(A' A'; B B_k^\ell|E' E'')_{\phi^k}
\]

Taking the limit \( k \to \infty \) of this expression and applying (2.12)–(2.15) gives the inequality stated in (2.6):

\[
I(A'; BB^\ell|E' E'')_{\psi} = \lim_{k \to \infty} I(A'; B B_k^\ell|E' E'')_{\psi^k} \\
\leq \lim_{k \to \infty} [H(B|E')_{\psi^k} + H(B|F')_{\psi^k} + I(A' A'; B B_k^\ell|E' E'')_{\phi^k}] \\
= H(B|E')_{\psi} + H(B|F')_{\psi} + I(A' A'; B'|E'')_{\phi}.
\]

This concludes the proof. ■

2.2 Energy-Constrained Secret-Key-Agreement Capacity

We now outline a protocol for energy-constrained secret key agreement between two parties Alice and Bob. The resources available to Alice and Bob in such a protocol are \( n \) uses of a quantum
channel \( \mathcal{N} \) interleaved by rounds of LOCC. The energy constraint is such that the average energy of the \( n \) states input to each channel use should be bounded from above by a fixed positive real number, where the energy is with respect to a given energy observable. It is sensible to consider an energy constraint \( P \) for any such protocol in light of the fact that any real transmitter is necessarily power limited. A third party Eve has access to all of the classical information exchanged between Alice and Bob, as well as the environment for each of the \( n \) uses of the channel \( \mathcal{N} \). So, for a photon-loss channel, Eve possesses all the light that is not received by Bob.

### 2.2.1 Secret-Key-Agreement Protocol with an Average Energy Constraint

We first recall the notion of an energy observable:

**Definition 1 (Energy Observable)** For a Hilbert space \( \mathcal{H} \), let \( G \in \mathcal{L}_+(\mathcal{H}) \) denote a positive semi-definite operator, defined in terms of its action on a vector \( |\psi\rangle \) as

\[
G|\psi\rangle = \sum_{j=1}^{\infty} g_j |e_j\rangle \langle e_j|\psi\rangle,
\]

for \( |\psi\rangle \) such that \( \sum_{j=1}^{\infty} g_j |\langle e_j|\psi\rangle|^2 < \infty \). In the above, \( \{ |e_j\rangle \}_j \) is an orthonormal basis and \( \{ g_j \}_j \) is a sequence of non-negative, real numbers. Then \( \{ |e_j\rangle \}_j \) is an eigenbasis for \( G \) with corresponding eigenvalues \( \{ g_j \}_j \). We also follow the convention that

\[
\text{Tr}\{ G \rho \} = \sup_n \text{Tr}\{ \Pi_n G \Pi_n \rho \},
\]

where \( \Pi_n \) is a spectral projector for \( G \) corresponding to the interval \( [0, n] \) [51, 92].

We now formally define an energy-constrained secret-key-agreement protocol. Fix \( n, K \in \mathbb{N} \), an energy observable \( G \), a positive real \( P \in [0, \infty) \), and \( \varepsilon \in [0, 1] \). An \(( n, K, G, P, \varepsilon )\) secret-key-agreement protocol invokes \( n \) uses of a quantum channel \( \mathcal{N} \), with each channel use interleaved by a denumerably decomposable LOCC channel. Such a protocol generates an \( \varepsilon \)-approximate tripartite key state of dimension \( K \). Furthermore, the average energy of the channel input states, with respect to the energy observable \( G \), is no larger than \( P \). Such a protocol is depicted in Figure 2.1.
Figure 2.1. A secret-key-agreement protocol begins with Alice and Bob preparing a separable state of systems $A'_1A_1B'_1$ using LOCC. Alice then feeds the $A_1$ system into the first channel use to generate the $B_1$ system. After repeating this procedure $n$ times, with rounds of LOCC interleaved between every channel use, Alice and Bob perform a final round of LOCC, which yields the key systems $K_A$ and $K_B$.

In more detail, such a protocol begins with Alice and Bob performing an LOCC channel $\mathcal{L}^{(1)}_{A'_iA_1B'_1} \to A'_iA_1B'_1$ to generate a state $\rho^{(1)}_{A'_iA_1B'_1}$ that is separable with respect to the cut $A'_iA_1|B'_1$. Since the channel is a denumerably decomposable LOCC channel, the state $\rho^{(1)}_{A'_iA_1B'_1}$ is a denumerably decomposable separable state, as considered in Ref. [65, Definition 1]. Alice then inputs the system $A_1$ to the first channel use, resulting in the state

$$\sigma^{(1)}_{A'_1B_1B'_1} \equiv \mathcal{N}_{A_1 \to B_1}(\rho^{(1)}_{A'_1A_1B'_1}). \tag{2.24}$$

For now, we do not describe the systems that the eavesdropper obtains, and we only do so in the next subsection. Alice and Bob then perform a second LOCC channel, producing the state

$$\rho^{(2)}_{A'_2A_2B'_2} \equiv \mathcal{L}^{(2)}_{A'_iB_1B'_1 \to A'_2A_2B'_2}(\sigma^{(1)}_{A'_1B_1B'_1}). \tag{2.25}$$

Next, Alice feeds system $A_2$ into the second channel use, which leads to the state

$$\sigma^{(2)}_{A'_2B_2B'_2} \equiv \mathcal{N}_{A_2 \to B_2}(\rho^{(2)}_{A'_2A_2B'_2}). \tag{2.26}$$

The procedure continues in this manner with a total of $n$ rounds of LOCC interleaved with $n$ uses.
of the channel as follows. For \( i \in \{2, \ldots, n\} \), the relevant states of the protocol are as follows:

\[
\begin{align*}
\rho_{A_i'B_i'}^{(i)} & \equiv \mathcal{L}_{A_{i-1}'B_{i-1}'}^{(i)}(\rho_{A_{i-1}'B_{i-1}'}^{(i-1)}), \\
\sigma_{A_i'B_i'}^{(i)} & \equiv \mathcal{N}_{A_i \rightarrow B_i}(\rho_{A_i'B_i'}^{(i)}). 
\end{align*}
\] (2.27) (2.28)

The primed systems correspond to separable Hilbert spaces. After the \( n^\text{th} \) channel use, a final LOCC channel is performed to produce key systems \( K_A \) and \( K_B \) for Alice and Bob, respectively, such that the final state is as follows:

\[
\omega_{K_A K_B} \equiv \mathcal{L}_{A_n'B_n'B_n'}^{(n+1)}(\rho_{A_n'B_n'B_n'}^{(n)}).
\] (2.29)

The average energy of the \( n \) channel input states with respect to the energy observable \( G \) is constrained by \( P \) as follows:

\[
\frac{1}{n} \sum_{i=1}^{n} \text{Tr}\{G \rho_{A_i}^{(i)}\} \leq P.
\] (2.30)

In the above, \( \rho_{A_i}^{(i)} \) is the marginal of the channel input states defined in (2.27).

### 2.2.2 The Purified Protocol

We now consider the role of a third party Eve in a secret-key-agreement protocol. The initial state \( \rho_{A_1'A_1'B_1'}^{(1)} \) is a separable state of the following form:

\[
\rho_{A_1'A_1'B_1'}^{(1)} \equiv \sum_{y_1} p_{Y_1}(y_1) \tau_{A_1'A_1}^{y_1} \otimes \zeta_{B_1}^{y_1},
\] (2.31)

where \( Y_1 \) is a classical random variable corresponding to the message exchanged between Alice and Bob, which is needed to establish this state. The state \( \rho_{A_1'A_1'B_1'}^{(1)} \) can be purified as

\[
|\rho^{(1)}\rangle_{A_1'A_1'S_{A_1}B_1'S_{B_1}Y_1} \equiv \sum_{y_1} \sqrt{p_{Y_1}(y_1)} \tau_{A_1'A_1}^{y_1} S_{A_1} \otimes |\zeta_{B_1}^{y_1}\rangle_{B_1'B_1} \otimes |y_1\rangle_{Y_1},
\] (2.32)

where the local shield systems \( S_{A_1} \) and \( S_{B_1} \) are described by separable Hilbert spaces and in principle could be held by Alice and Bob, respectively, \( |\tau_{Y_1}^{y_1}\rangle_{A_1'A_1} \) and \( |\zeta_{B_1}^{y_1}\rangle_{B_1'B_1} \) purify \( \tau_{A_1'A_1}^{y_1} \) and \( \zeta_{B_1}^{y_1} \).
respectively, and Eve possesses system $Y_1$, which contains a coherent classical copy of the classical data exchanged.

Each LOCC channel $\mathcal{L}^{(i)}_{A'_i-1B'_i-1\rightarrow A'_iA_iB'_i}$ for $i \in \{2, \ldots, n\}$ is of the form in (1.11) as

$$\mathcal{L}^{(i)}_{A'_i-1B'_i-1\rightarrow A'_iA_iB'_i} = \sum_{y_i} \mathcal{E}^{y_i}_{A'_i-1\rightarrow A'_iA_i} \otimes \mathcal{F}^{y_i}_{B'_i-1\rightarrow B'_i},$$

and can be purified to an isometry in the following way:

$$U^{\mathcal{L}^{(i)}}_{A'_i-1B'_i-1\rightarrow A'_iA_iS_{A_i}B'_iS_{B_i}Y_i} \equiv \sum_{y_i} U^{\mathcal{E}^{y_i}}_{A'_i-1\rightarrow A'_iA_iS_{A_i}} \otimes U^{\mathcal{F}^{y_i}}_{B'_i-1B'_i-1\rightarrow B'_iS_{B_i}S_{B_i}Y_i},$$

where $\{U^{\mathcal{E}^{y_i}}_{A'_i-1\rightarrow A'_iA_iS_{A_i}}\}_{y_i}$ and $\{U^{\mathcal{F}^{y_i}}_{B'_i-1B'_i-1\rightarrow B'_iS_{B_i}}\}_{y_i}$ are collections of linear operators (each of which is a contraction, that is, $\|U^{\mathcal{E}^{y_i}}_{A'_i-1\rightarrow A'_iA_iS_{A_i}}\|_{\infty}, \|U^{\mathcal{F}^{y_i}}_{B'_i-1B'_i-1\rightarrow B'_iS_{B_i}}\|_{\infty} \leq 1$) such that the linear operator in (2.34) is an isometry. The systems $S_{A_i}$ and $S_{B_i}$ are shield systems belonging to Alice and Bob, respectively, and $Y_i$ is a system held by Eve, containing a coherent classical copy of the classical data exchanged in this round. So a purification of the state $\rho^{(i)}_{A'_iA_iB'_i}$ after each LOCC channel is as
follows:

\[ |\rho^{(i)}\rangle_{A'_i A_i S_{A_i} A'_i S_{B_i} E_i^{i-1} Y_i^1} \equiv U^{(i)}_{A'_i A_i B_{i-1} B'_i E_{i-1} A'_i A_i S_{A_i} A'_i S_{B_i} Y_i} |\sigma^{(i-1)}\rangle_{A'_i A_i B_{i-1} B'_i E_{i-1} S_{A_i} S_{B_i} E_i^{i-1} Y_i^1}, \]  

(2.35)

where we have employed the shorthands \( S_{A_i} \equiv S_{A_1} \cdots S_{A_i} \) and \( S_{B_i} \equiv S_{B_1} \cdots S_{B_i} \), with a similar shorthand for \( E_i^{i-1} \) and \( Y_i^1 \). A purification of the state \( |\sigma^{(i)}\rangle_{A'_i A_i S_{A_i} A'_i S_{B_i} E_i^{i-1} Y_i^1} \) after each use of the channel \( N_{A_i \rightarrow B_i} \) is

\[ |\sigma^{(i)}\rangle_{A'_i A_i S_{A_i} A'_i S_{B_i} E_i^{i-1} Y_i^1} \equiv U^N_{A_i \rightarrow B_i E_i} |\rho^{(i)}\rangle_{A'_i A_i S_{A_i} A'_i S_{B_i} E_i^{i-1} Y_i^1}, \]  

(2.36)

where \( U^N_{A_i \rightarrow B_i E_i} \) is an isometric extension of \( i \)th channel use \( N_{A_i \rightarrow B_i} \). The final LOCC channel also takes the form in (1.11)

\[ L^{(n+1)}_{A'_n A_n B'_n \rightarrow K_A K_B} = \sum_{y_{n+1}} E^{y_{n+1}}_{A'_n \rightarrow K_A} \otimes F^{y_{n+1}}_{B_n B'_n \rightarrow K_B}, \]

(2.37)

and it can be purified to an isometry similarly as

\[ U^{L^{(n+1)}}_{A'_n A_n B'_n \rightarrow K_A S_{A_{n+1}} K_B S_{B_{n+1}} Y_{n+1}} \equiv \sum_{y_{n+1}} U^{E^{y_{n+1}}}_{A'_n \rightarrow K_A S_{A_{n+1}}} \otimes U^{F^{y_{n+1}}}_{B_n B'_n \rightarrow K_B S_{B_{n+1}}} \otimes |y_{n+1}\rangle_{Y_{n+1}}. \]  

(2.38)

The systems \( S_{A_{n+1}} \) and \( S_{B_{n+1}} \) are again shield systems belonging to Alice and Bob, respectively, and \( Y_{n+1} \) is a system held by Eve, containing a coherent classical copy of the classical data exchanged in this round. As written above, each channel use \( N_{A_i \rightarrow B_i} \) can be purified, as in (1.6) and (1.7), to an isometric channel \( U^N_{A_i \rightarrow B_i E_i} \) such that Eve possesses system \( E_i \) for all \( i \in \{1, \ldots, n\} \).

The final state at the end of the purified protocol is a pure state \( |\omega\rangle_{K_A S_A K_B S_B E^n Y_{n+1}} \), given by

\[ |\omega\rangle_{K_A S_A K_B S_B E^n Y_{n+1}} = U^{L^{(n+1)}}_{A'_n A_n B'_n \rightarrow K_A S_{A_{n+1}} K_B S_{B_{n+1}} Y_{n+1}} |\sigma^{(n)}\rangle_{A'_n A_n B'_n S_{A_{n+1}} B'_n S_{B_{n+1}} E^n Y_{n+1}}. \]  

(2.39)

Alice is in possession of the key system \( K_A \) and the shield systems \( S_A \equiv S_{A_1} \cdots S_{A_{n+1}} \), Bob possesses the key system \( K_B \) and the shield systems \( S_B \equiv S_{B_1} \cdots S_{B_{n+1}} \), and Eve holds the environment systems \( E^n \equiv E_1 \cdots E_n \). The \( S_A, S_B, \) and \( E^n \) systems all correspond to separable Hilbert spaces of generally infinite dimensions. Additionally, Eve has coherent copies \( Y_{n+1} \equiv Y_1 \cdots Y_{n+1} \) of all the
classical data exchanged. By tracing over the systems $E^n$ and $Y^{n+1}$, it is clear that the protocol is an LOCC-assisted protocol whose aim is to generate an approximate bipartite private state on the systems $K_A S_A K_B S_B$.

For a fixed $n, K \in \mathbb{N}$ and $\varepsilon \in [0, 1]$, the protocol is an $(n, K, G, P, \varepsilon)$ secret-key-agreement protocol if the final state $\omega_{K_A S_A K_B S_B}$ satisfies

$$F(\omega_{K_A S_A K_B S_B}, \gamma_{K_A S_A K_B S_B}) \geq 1 - \varepsilon, \quad (2.40)$$

where $\gamma_{K_A S_A K_B S_B}$ is a bipartite private state as in (1.67). Alternatively (and equivalently), the criterion is that the final state $\omega_{K_A K_B E^n Y^{n+1}}$ satisfies

$$F(\omega_{K_A K_B E^n Y^{n+1}}, \gamma_{K_A K_B E^n Y^{n+1}}) \geq 1 - \varepsilon, \quad (2.41)$$

where $\gamma_{K_A K_B E^n Y^{n+1}}$ is a tripartite key state as in (1.65).

### 2.2.3 Achievable Rates and Energy-Constrained Secret-Key-Agreement Capacity

The rate $R = \frac{\log_2 K}{n}$ is a measure of the efficiency of the protocol, measured in secret key bits communicated per channel use. We say that the rate $R$ is achievable if, for all $\varepsilon \in (0, 1)$, $\delta > 0$, and sufficiently large $n$, there exists an $(n, 2^{n(R-\delta)}, G, P, \varepsilon)$ secret-key-agreement protocol.

We call $P_2(\mathcal{N}, G, P)$ the energy-constrained secret-key-agreement capacity of the channel $\mathcal{N}$, and it is equal to the supremum of all achievable rates subject to the energy constraint $P$ with respect to the energy observable $G$.

### 2.2.4 Energy-Constrained LOCC-assisted Quantum Communication

We define the energy-constrained LOCC-assisted quantum capacity $Q_2(\mathcal{N}, G, P)$ of a channel $\mathcal{N}$ similarly. In this case, an $(n, K, G, P, \varepsilon)$ energy-constrained LOCC-assisted quantum communication protocol is defined similarly as in Section 2.2.1, but the main difference is that the final state $\omega_{K_A K_B}$ should satisfy the following inequality:

$$F(\omega_{K_A K_B}, \Phi_{AB}) \geq 1 - \varepsilon, \quad (2.42)$$
where $\Phi_{AB}$ is a maximally entangled state. Achievable rates are defined similarly as in the previous subsection, and the energy-constrained LOCC-assisted quantum capacity $Q_2(N, G, P)$ of the channel $N$ is defined to be equal to the supremum of all achievable rates.

It is worthwhile to note that the end goal of an LOCC-assisted quantum communication protocol is more difficult to achieve than a secret-key-agreement protocol for the same channel $N$, energy observable $G$, energy constraint $P$, number $n$ of channel uses, and error parameter $\varepsilon$. This is because a maximally entangled state $\Phi_{KAKB}$ is a very particular kind of bipartite private state $\gamma_{KSASKB}$, as observed in Refs. [87,88]. Given this observation, it immediately follows that the energy-constrained LOCC-assisted quantum capacity is bounded from above by the energy-constrained secret-key-agreement capacity:

$$Q_2(N, G, P) \leq P_2(N, G, P). \quad (2.43)$$

### 2.3 Energy-Constrained Squashed Entanglement is an Upper Bound on Energy-Constrained Secret-Key-Agreement Capacity

The main goal of this section is to prove that the energy-constrained squashed entanglement of a quantum channel is an upper bound on its energy-constrained secret-key-agreement capacity. Before doing so, we recall the notion of a Gibbs observable [51,92–96] and the finite output-entropy condition [51,93,94] for quantum channels.

**Definition 2 (Gibbs Observable)** An energy observable $G$ is a Gibbs observable if

$$\text{Tr}\{\exp(-\beta G)\} < \infty \quad (2.44)$$

for all $\beta > 0$.

This condition implies that there exists a well defined thermal state for $G$, having the following form for all $\beta > 0$ [97] (see also Refs. [93,95]):

$$e^{-\beta G}/\text{Tr}\{e^{-\beta G}\}. \quad (2.45)$$

**Condition 1 (Finite Output Entropy)** Let $G$ be a Gibbs observable as in Definition 2, and let $P \in [0, \infty)$ be an energy constraint. A quantum channel $N$ satisfies the finite output-entropy
condition with respect to $G$ and $P$ if \cite{51,93,94}  

\[
\sup_{\rho: \text{Tr}\{G\rho\} \leq P} H(\mathcal{N}(\rho)) < \infty. \tag{2.46}
\]

If a channel $\mathcal{N}$ satisfies the finite output-entropy condition with respect to $G$ and $P$, then any complementary channel $\hat{\mathcal{N}}$ of $\mathcal{N}$ also satisfies the condition \cite{98}:  

\[
\sup_{\rho: \text{Tr}\{G\rho\} \leq P} H(\hat{\mathcal{N}}(\rho)) < \infty. \tag{2.47}
\]

**Lemma 3** Finiteness of the output entropy of a channel $\mathcal{N}$ implies finiteness of the squashed entanglement of that channel. That is, if  

\[
\sup_{\rho: \text{Tr}\{G\rho\} \leq P} H(\mathcal{N}(\rho)) < \infty \tag{2.48}
\]

holds, then  

\[
E_{\text{sq}}(\mathcal{N}) < \infty. \tag{2.49}
\]

**Proof.** The statement is a consequence of (1.28). Indeed, applying the definition of squashed entanglement and picking the extension system $E$ to be trivial, we then get that  

\[
E_{\text{sq}}(A; B)_{\omega} \leq \frac{1}{2} I(A; B)_{\omega}. \tag{2.50}
\]

Applying Condition 1 to (1.28) and combining (2.50) with the definition in (1.45) yields the statement of the lemma. \qed

We now establish the following weak-converse bound that applies to an arbitrary $(n, K, G, P, \varepsilon)$ energy-constrained secret-key-agreement protocol.

**Proposition 1** Let $\mathcal{N}$ be a quantum channel satisfying the finite output-entropy condition (Condition 1), let $G$ be a Gibbs observable as in Definition 2, and let $P \in [0, \infty)$ be an energy constraint. Fix $n, K \in \mathbb{N}$ and $\varepsilon \in (0, 1)$. Then an $(n, K, G, P, \varepsilon)$ energy-constrained secret-key-agreement protocol for $\mathcal{N}$ is subject to the following upper bound in terms of the energy-constrained squashed entanglement
entanglement of the channel $\mathcal{N}$:

$$\frac{1 - 2\sqrt{\varepsilon}}{n} \log_2 K \leq E_{sq}(\mathcal{N}, G, P) + 2\frac{n}{n}g(\sqrt{\varepsilon}), \quad (2.51)$$

where $g(\cdot)$ is defined in (1.64).

**Proof.** By assumption, the final state $\omega_{K_A S_A K_B S_B}$ of any $(n, K, G, P, \varepsilon)$ secret-key-agreement protocol is an $\varepsilon$-approximate bipartite private state, as given in (2.40). Thus, the bound in (1.72) applies, leading to the following bound:

$$\log_2 K \leq E_{sq}(K_A S_A; K_B S_B)_{\omega} + 2\sqrt{\varepsilon} \log_2 K + 2g(\sqrt{\varepsilon}). \quad (2.52)$$

Let $U^{\mathcal{N}}_{A \rightarrow BE}$ be an isometric channel extending the original channel $\mathcal{N}_{A \rightarrow B}$. Let $V^S_{E \rightarrow E'F}$ denote an isometric extension of a squashing channel that can act on the environment system $E$ of the isometric channel $U^{\mathcal{N}}_{A \rightarrow BE}$, and let $W^n_{E_1^{n-1}Y_n \rightarrow E_n''F''_n}$ denote an isometric extension of a squashing channel that can act on the systems $E_1^{n-1}Y_n$. Then we define the states

$$|\tau^{(n)}\rangle_{A'_n B_n S_{A'_n} B'_n S_{B'_n} E'_n F'_n F''_n} \equiv (V^S_{E_n \rightarrow E'_n F_n} \otimes W^n_{E_1^{n-1}Y_n \rightarrow E_n''F''_n})|\sigma^{(n)}\rangle_{A'_n B_n S_{A'_n} B'_n S_{B'_n} E''_n Y''_n}, \quad (2.53)$$

and

$$|\zeta^{(n)}\rangle_{A'_n A_n S_{A'_n} B'_n S_{B'_n} E''_n F''_n} \equiv W^n_{E_1^{n-1}Y_n \rightarrow E_n''F''_n}|\rho^{(n)}\rangle_{A'_n A_n S_{A'_n} B'_n S_{B'_n} E''_n Y''_n}. \quad (2.54)$$

We invoke the LOCC monotonicity of squashed entanglement and the definition of squashed entanglement from (1.42), as well as Lemma 2, to find that

$$2E_{sq}(K_A S_A; K_B S_B)_{\omega} \leq 2E_{sq}(A'_n S_{A'_n}; B_n S_{B'_n})_{\sigma^{(n)}} \quad (2.55)$$

$$\leq I(A'_n S_{A'_n}; B_n S_{B'_n} E'_n F'_n)_{\tau^{(n)}} \quad (2.56)$$

$$\leq H(B_n | E'_n)_{\tau^{(n)}} + H(B_n | F_n)_{\tau^{(n)}} + I(A'_n S_{A'_n} A_n; B'_n S_{B'_n} | E''_n)_{\zeta^{(n)}}. \quad (2.57)$$

The conditions needed to apply Lemma 2 indeed hold, following by hypothesis from (2.30) and the finite output-entropy condition. Since the isometric extension $W^n_{E_1^{n-1}Y_n \rightarrow E_n''F''_n}$ of a squashing
channel is an arbitrary choice, the inequality above holds for the infimum over all such squashing channel extensions, and we find that

\[
E_{\text{sq}}(A'_n S_{A_1^n}; B_n S_{B_1^n} B'_n)_{\sigma(n)} \leq \frac{1}{2} \left[ H(B_n | E'_n)_{\tau(n)} + H(B_n | F_n)_{\tau(n)} \right] + E_{\text{sq}}(A'_n S_{A_1^n}; B'_n S_{B_1^n})_{\rho(n)}. \tag{2.58}
\]

We can then again invoke the LOCC monotonicity of squashed entanglement to find that

\[
E_{\text{sq}}(A'_n S_{A_1^n}; B'_n S_{B_1^n})_{\rho(n)} \leq E_{\text{sq}}(A'_{n-1} S_{A_1^{n-1}}; B_{n-1} B'_{n-1} S_{B_1^{n-1}})_{\sigma(n-1)}. \tag{2.59}
\]

Now repeating the above reasoning \(n - 1\) more times (applying Lemma 2 and LOCC monotonicity of squashed entanglement iteratively), we find that

\[
2E_{\text{sq}}(K_A S_A; K_B S_B)_{\omega} \leq \sum_{i=1}^{n} \left[ H(B_i | E'_i)_{\tau(i)} + H(B_i | F_i)_{\tau(i)} \right] + 2E_{\text{sq}}(A'_1 A_1; B'_1)_{\rho(1)} \tag{2.60}
\]

\[
= \sum_{i=1}^{n} \left[ H(B_i | E'_i)_{\tau(i)} + H(B_i | F_i)_{\tau(i)} \right] \tag{2.61}
\]

\[
= \frac{1}{n} \sum_{i=1}^{n} \left[ H(B_i | E'_i)_{\tau(i)} + H(B_i | F_i)_{\tau(i)} \right] \tag{2.62}
\]

\[
\leq n \left[ H(B | E')_{\tau} + H(B | F)_{\tau} \right]. \tag{2.63}
\]

The first equality follows because the state \(\rho^{(1)}_{A_1' A_1 B_1'}\) is separable, being the result of the initial LOCC, and so \(E_{\text{sq}}(A'_1 A_1; B'_1)_{\rho(1)} = 0\). Note here that we are invoking the assumption that the protocol begins with a denumerably decomposable separable state [65, Definition 1] and the fact that \(E_{\text{sq}} = 0\) for such states [65, Proposition 2]. The last inequality follows from the concavity of conditional entropy [73], defining \(\tau_{BE'F}\) as the average output state of the channel:

\[
\tau_{BE'F} \equiv \frac{1}{n} \sum_{i=1}^{n} \gamma_{E_i \rightarrow E'_i F_i}^{S}(\sigma_{B_i E_i}^{(i)}). \tag{2.64}
\]

Since the inequality above holds for an arbitrary choice of the isometric channel \(\gamma_{E \rightarrow E'F}^{S}\) extending a squashing channel, and the average channel input state for the protocol satisfies the energy
constraint in (2.30) by assumption, we find that

\[
E_{sq}(K_A S_A; K_B S_B) \omega \leq n \inf_{V_{E \rightarrow E'}^S} \frac{1}{2} [H(B|E')_\tau + H(B|F)_\tau] \tag{2.65}
\]

\[
\leq n E_{sq}(N, G, P), \tag{2.66}
\]

where we have employed the alternative representation of squashed entanglement from (1.50). Now combining (2.52) and (2.66), we conclude the proof. ■

By applying Proposition 1 and taking the limit as \(n \rightarrow \infty\) and then as \(\varepsilon \rightarrow 0\), we arrive at the following theorem:

**Theorem 4** Let \(N\) be a quantum channel satisfying the finite output-entropy condition (Condition 1), let \(G\) be a Gibbs observable as in Definition 2, and let \(P \in [0, \infty)\) be an energy constraint. Then the energy-constrained squashed entanglement of the channel \(N\) is an upper bound on its energy-constrained secret-key-agreement capacity:

\[
P_2(N, G, P) \leq E_{sq}(N, G, P). \tag{2.67}
\]

Immediate consequences of Proposition 1 and Theorem 4 are bounds for rates of LOCC-assisted quantum communication. Indeed, let \(N\) be a quantum channel satisfying the finite output-entropy condition (Condition 1), let \(G\) be a Gibbs observable as in Definition 2, and let \(P \in [0, \infty)\) be an energy constraint. Fix \(n, K \in \mathbb{N}\) and \(\varepsilon \in (0, 1)\). Then an \((n, K, G, P, \varepsilon)\) energy-constrained LOCC-assisted quantum communication protocol for \(N\) is subject to the following upper bound in terms of its energy-constrained squashed entanglement:

\[
\frac{1 - 2\sqrt{\varepsilon}}{n} \log_2 K \leq E_{sq}(N, G, P) + \frac{2}{n} g(\sqrt{\varepsilon}). \tag{2.68}
\]

Then this implies that

\[
Q_2(N, G, P) \leq E_{sq}(N, G, P). \tag{2.69}
\]
2.4 Bounds on Energy-Constrained Secret-Key-Agreement Capacities of Phase-Insensitive Quantum Gaussian Channels

The main result of Section 2.3 is that the energy-constrained squashed entanglement is an upper bound on the energy-constrained secret-key-agreement capacity of quantum channels that satisfy the finite output-entropy condition with respect to a given Gibbs observable. In this section, we specialize this result to particular phase-insensitive bosonic Gaussian channels that accept as input a single mode and output multiple modes. We prove here that a relaxation of the energy-constrained squashed entanglement of these channels is optimized by a thermal state input (when the squashed entanglement is written with respect to the representation in (1.50)). Our results in this section thus generalize statements from prior works in Refs. [12,14,79].

We also note the following point here before proceeding with the technical development. The prior works [12,14,79] argued that a thermal-state input should be the optimal choice for a particular relaxation of the energy-constrained squashed entanglement. However, it appears that these works have not given a full justification of these claims. In particular, Refs. [12,79] appealed only to the extremality of Gaussian states [99] to argue that a thermal state should be optimal. However, it is necessary to argue that, among all Gaussian states, the thermal state is optimal. In Ref. [14], arguments about covariance of single-mode phase-insensitive Gaussian channels with respect to displacements and squeezing unitaries were given, but there was not an explicit proof of the latter covariance with respect to the squeezers, and furthermore, the squeezing unitaries can change the energy of the input state. Thus, in light of these questionable aspects, it seems worthwhile to provide a clear proof of the optimality of the thermal-state input, and our development in this section accomplishes this goal. The approach taken here is strongly related to that given in Section 5.2 and Remark 21 of Ref. [100].

2.4.1 Single-Mode, Phase-Insensitive Bosonic Gaussian Channels and Their Properties

We begin in what follows by considering the argument for the particular case of phase-insensitive single-mode bosonic Gaussian channels. Three classes of channels of primary interest are thermal, amplifier, and additive-noise channels.
A thermal channel can be described succinctly in terms of the following Heisenberg-picture evolution:

\[ \hat{b} = \sqrt{\eta} \hat{a} + \sqrt{1 - \eta} \hat{e}, \]  

where \( \hat{a} \), \( \hat{b} \), and \( \hat{e} \) represent respective bosonic annihilation operators for the sender, receiver, and environment. The parameter \( \eta \in (0, 1) \) represents the transmissivity of the channel, and the state of the environment is a bosonic thermal state \( \theta(N_B) \) of the following form:

\[ \theta(N_B) \equiv \frac{1}{N_B + 1} \sum_{n=0}^{\infty} \left( \frac{N_B}{N_B + 1} \right)^n |n\rangle \langle n|, \]  

where \( N_B \geq 0 \) is the mean photon number of the above thermal state. So a thermal channel is characterized by two parameters: \( \eta \in (0, 1) \) and \( N_B \geq 0 \). If \( N_B = 0 \), then the channel is called a pure-loss channel because the environment state is prepared in a vacuum state and the only corruption of the input signal is due to loss. An alternate description of a thermal channel in terms of its Kraus operators is available in Ref. [101], and in what follows, we denote it by \( \mathcal{L}_{\eta,N_B} \).

It is helpful to consider a unitary extension of a thermal channel. That is, we can consider a thermal channel arising as the result of a beamsplitter interaction between the input mode and the thermal-state environment mode, followed by a partial trace over the output environment mode. We can represent this interaction in the Heisenberg picture as follows:

\[ \hat{b} = \sqrt{\eta} \hat{a} + \sqrt{1 - \eta} \hat{e}, \]  

\[ \hat{e}' = -\sqrt{1 - \eta} \hat{a} + \sqrt{\eta} \hat{e}, \]  

where \( \hat{e}' \) denotes the output environment mode. Let \( U^{\mathcal{L}_{\eta,N_B}} \) denote the Schrödinger-picture, two-mode unitary describing this interaction. It is well known that this unitary obeys the following phase covariance symmetry for all \( \phi \in \mathbb{R} \):

\[ U^{\mathcal{L}_{\eta,N_B}} e^{i\hat{n}_{AE} \phi} = e^{i\hat{n}_{BE}' \phi} U^{\mathcal{L}_{\eta,N_B}}, \]  

where \( \hat{n}_{AE} = \hat{n}_A + \hat{n}_E \) is the total photon number operator for the input mode \( A \) and environment.
mode $E$, while $\hat{n}_{BE'} = \hat{n}_B + \hat{n}_{E'}$ is that for the output mode $B$ and the output environment mode $E'$. Thus, we can equivalently write the above phase covariance symmetry as

$$U^{L_{\eta,NB}}(e^{i\hat{n}_A\phi} \otimes e^{i\hat{n}_E\phi}) = (e^{i\hat{n}_B\phi} \otimes e^{i\hat{n}_{E'}\phi})U^{L_{\eta,NB}}.$$  \hfill (2.74)

Due to this relation, the fact that a thermal state is phase invariant (i.e., $e^{i\hat{n}_E\phi}\theta(N_B)e^{-i\hat{n}_E\phi} = \theta(N_B)$), and the fact that the thermal channel results from a partial trace after the unitary transformation $U^{L_{\eta,NB}}$, it follows that the thermal channel is phase covariant in the following sense:

$$\mathcal{L}_{\eta,NB}(e^{i\hat{n}_A\phi}\rho_Ae^{-i\hat{n}_A\phi}) = e^{i\hat{n}_B\phi}\mathcal{L}_{\eta,NB}(\rho_A)e^{-i\hat{n}_B\phi},$$  \hfill (2.75)

where $\rho_A$ is an arbitrary input state. This is the reason that thermal channels are called phase-insensitive.

Another class of channels to consider are amplifier channels. An amplifier channel can also be described succinctly in terms of the following Heisenberg-picture evolution:

$$\hat{b} = \sqrt{G}\hat{a} + \sqrt{G-1}\hat{e},$$  \hfill (2.76)

where $\hat{a}$, $\hat{b}$, and $\hat{e}$ again represent respective bosonic annihilation operators for the sender, receiver, and environment. The parameter $G \in (1,\infty)$ represents the gain of the channel, and the state of the environment is a bosonic thermal state $\theta(N_B)$ with $N_B \geq 0$. So an amplifier channel is characterized by two parameters: $G \in (1,\infty)$ and $N_B \geq 0$. If $N_B = 0$, then the channel is called a pure-amplifier channel because the environment state is prepared in a vacuum state and the only corruption of the input signal is due to amplification, which inevitably introduces noise due to the no-cloning theorem [41, 43]. An alternate description of an amplifier channel in terms of its Kraus operators is available in Ref. [101], and in what follows, we denote it by $A_{\theta,NB}$.

It is again helpful to consider a unitary extension of an amplifier channel. That is, we can consider an amplifier channel arising as the result of a two-mode squeezer interaction between the input mode and the thermal-state environment mode, followed by a partial trace over the output
environment mode. We can represent this interaction in the Heisenberg picture as follows:

\[
\hat{b} = \sqrt{G} \hat{a} + \sqrt{G - 1} \hat{e}^\dagger,
\]

\[
\hat{e}' = \sqrt{G - 1} \hat{a}^\dagger + \sqrt{G} \hat{e},
\]

(2.77)

where \( \hat{e}' \) denotes the output environment mode. Let \( U^{A_g,N_B} \) denote the Schrödinger-picture, two-mode unitary describing this interaction. It is well known that this unitary obeys the following phase covariance symmetry for all \( \phi \in \mathbb{R} \)

\[
U^{A_g,N_B}(e^{i\hat{n}_A \phi} \otimes e^{-i\hat{n}_E \phi}) = (e^{i\hat{n}_B \phi} \otimes e^{-i\hat{n}_E' \phi})U^{A_g,N_B}.
\]

(2.78)

Due to this relation, the fact that a thermal state is phase invariant, and the fact that the amplifier channel results from a partial trace of the unitary transformation \( U^{A_g,N_B} \), it follows that the amplifier channel is phase covariant in the following sense:

\[
A_{g,N_B}(e^{i\hat{n}_A \phi} \rho_A e^{-i\hat{n}_A \phi}) = e^{i\hat{n}_B \phi} A_{g,N_B}(\rho_A)e^{-i\hat{n}_B \phi},
\]

(2.79)

where \( \rho_A \) is an arbitrary input state. So amplifier channels are also called phase-insensitive.

Another class of single-mode, phase-insensitive bosonic Gaussian channels are called additive-noise channels. These channels are easily described in the Schrödinger picture and are characterized by a single parameter \( \xi \geq 0 \), which is the variance of the channel. Additive-noise channels can be written as the following transformation:

\[
\rho_A \rightarrow \int d^2\alpha \frac{\exp(-|\alpha|^2/\xi)}{\pi \xi} D(\alpha)\rho_A D(-\alpha),
\]

(2.80)

and can be interpreted as applying a unitary displacement operator \( D(\alpha) \) randomly chosen according to a complex, isotropic Gaussian distribution \( \frac{\exp(-|\alpha|^2/\xi)}{\pi \xi} \) of variance \( \xi \). These channels are phase-covariant as well and are thus phase-insensitive.

A well known theorem from Refs. [102, 103] establishes that any single-mode, phase-insensitive bosonic Gaussian channel \( \mathcal{N} \) can be written as the serial concatenation of a pure-loss channel \( \mathcal{L}_{T,0} \)
of transmissivity $T \in [0, 1]$ followed by a pure-amplifier channel $A_{\mathcal{g},0}$ of gain $\mathcal{g} > 1$:

$$\mathcal{N} = A_{\mathcal{g},0} \circ \mathcal{L}_{T,0}. \quad (2.81)$$

This theorem has been extremely helpful in obtaining good upper bounds on various capacities of single-mode, phase-insensitive bosonic Gaussian channels [12, 14, 79, 100, 104–107].

### 2.4.2 Bounds for Single-Mode, Phase-Insensitive Bosonic Gaussian Channels

In the following theorem, we prove that a thermal input state is the optimal state for a relaxation of the energy-constrained squashed entanglement of a single-mode, phase-insensitive bosonic Gaussian channel. This in turn gives an upper bound on the energy-constrained secret-key-agreement capacities of these channels, which has already been claimed in Refs. [12, 14, 79].

**Theorem 5** Let $\mathcal{N}$ be a single-mode, phase-insensitive bosonic Gaussian channel as in (2.81). Then its energy-constrained squashed entanglement is bounded as

$$E_{sq}(\mathcal{N}, \hat{n}, N_S) \leq \frac{1}{2} [H(B|E'_1 E'_2)_{\omega} + H(B|F'_1 F'_2)_{\omega}], \quad (2.82)$$

where $\hat{n}$ is the photon number operator acting on the channel input mode, $N_S \geq 0$ is an energy constraint, $\omega_{BE'_1 E'_2 F'_1 F'_2}$ is the following state:

$$\omega_{BE'_1 E'_2 F'_1 F'_2} = \mathcal{W}_{A\rightarrow BE'_1 E'_2 F'_1 F'_2}(\theta(N_S)), \quad (2.83)$$

and $\mathcal{W}$ is an isometric channel of the form

$$\mathcal{W}_{A\rightarrow BE'_1 E'_2 F'_1 F'_2} = (\mathcal{V}_{E'_2 \rightarrow E'_2 F'_2} \circ \mathcal{U}_{A\rightarrow B_i E_2}) \circ (\mathcal{V}_{E'_1 \rightarrow E'_1 F'_1} \circ \mathcal{U}_{A\rightarrow B_i E_1}). \quad (2.84)$$

In the above, $\mathcal{U}_{E_{T,0}}$ is an isometric channel extending the pure-loss channel $\mathcal{L}_{T,0}$ and realized from (2.72). Also, $\mathcal{U}_{A_{\mathcal{g},0}}$ is an isometric channel extending the pure-amplifier channel $A_{\mathcal{g},0}$ and realized from (2.77). Both $\mathcal{V}_{E_1 \rightarrow E'_1 F'_1}$ and $\mathcal{V}_{E_2 \rightarrow E'_2 F'_2}$ are bosonic Gaussian isometric channels that are phase covariant. Figure 2.3 depicts an example of the isometric channel $\mathcal{W}_{A\rightarrow BE'_1 E'_2 F'_1 F'_2}$. 
Figure 2.3. A depiction of the isometric channel $W_{A \rightarrow BE}^{E_1'F_1'}$ from Theorem 5. Note that this is the precise construction used in Ref. [14]. As stated in Theorem 5, the isometric channel $W_{A \rightarrow BE}^{E_1'F_1'}$ is equal to $(V_{E_2 \rightarrow E'_2F'_2}^{A} \circ U_{B_1 \rightarrow BE_2}^{A}) \circ (V_{E_1 \rightarrow E'_1F'_1}^{E} \circ U_{A \rightarrow B_1E_1}^{T,0})$. The modes labeled “env1” and “env2” are respective environmental modes for the isometric channels $U_{E_1 \rightarrow E'_1F'_1}^{E}$ (top left) and $U_{A \rightarrow B_1E_1}^{T,0}$ (top right) and are prepared in the pure vacuum state. The other isometric channels $V_{E_1 \rightarrow E'_1F'_1}^{E}$ (bottom left) and $V_{E_2 \rightarrow E'_2F'_2}^{A}$ (bottom right) are chosen here to be 50-50 beamsplitters, following Ref. [14]. The modes $F_1$ and $F_2$ are also prepared in the pure vacuum state. Given this setup, Theorem 5 states that, among all possible input states with mean photon number $\leq N_S$, the thermal state $\theta(N_S)$ maximizes the entropy function $H(B|E'_1E'_2) + H(B|F'_1F'_2)$.

An immediate consequence of Theorems 4 and 5 is the following corollary:

**Corollary 1** With the same notation as in Theorem 5, the energy-constrained secret-key-agreement capacity of the channel $\mathcal{N}$ is bounded as

$$P_2(\mathcal{N}, \hat{n}, N_S) \leq \frac{1}{2} [H(B|E'_1E'_2) + H(B|F'_1F'_2)].$$

(2.85)

**Proof of Theorem 5.** For convenience, we summarize the main steps of the proof here. We note that certain aspects of the proof bear some similarities to related approaches given in the literature [51,98,107], and the strongest overlap is with Remark 21 and Section 5.2 in Ref. [100].

1. First, we employ the representation of a channel’s squashed entanglement in (1.50), and set $U_{B_1 \rightarrow BE_2}^{A} \circ U_{A \rightarrow B_1E_1}^{T,0}$ to be the isometric extension of $\mathcal{N} = A_{\varphi,0} \circ L_{T,0}$.

2. Then, we relax the infimum over all squashing isometries by setting it to be equal to $V_{E_1 \rightarrow E'_1F'_1}^{E} \otimes
This leads to the isometric channel $\mathcal{W}_{A\rightarrow B'E'_{2}F'_{2}}$ described in the theorem statement.

3. Next, we employ the extremality of Gaussian states [99] to conclude that the entropy objective function $H(B|E'_{1}E'_{2}) + H(B|F'_{1}F'_{2})$ is maximized when the input state to mode $A$ is Gaussian.

4. We then employ the phase covariance of $\mathcal{W}_{A\rightarrow B'E'_{2}F'_{2}}$ and concavity of conditional entropy to conclude that, for input states having a fixed mean photon number $N_S$, the entropy objective function $H(B|E'_{1}E'_{2}) + H(B|F'_{1}F'_{2})$ is maximized when the input state to mode $A$ is phase invariant.

5. Steps 3 and 4 imply that, for input states having a fixed mean photon number $N_S$, the optimal input state to mode $A$ should be a thermal state $\theta(N_S)$. This follows because $\theta(N_S)$ is the unique single-mode state of fixed mean photon number $N_S$ that is both Gaussian and phase invariant.

6. Finally, we use the displacement covariance of $\mathcal{W}_{A\rightarrow B'E'_{2}F'_{2}}$ and concavity of conditional entropy to conclude that the entropy objective function $H(B|E'_{1}E'_{2}) + H(B|F'_{1}F'_{2})$ is monotone with respect to $N_S$. This finally implies that $\theta(N_S)$ is the optimal input state among all those having mean photon number $\leq N_S$.

Steps one through three do not require any further justification, and so we proceed to step four. In what follows, we take the isometric channels $\mathcal{V}_{E_{1}\rightarrow E'_{1}F'_{1}}$ and $\mathcal{V}_{E_{2}\rightarrow E'_{2}F'_{2}}$ to be 50-50 beamsplitters, following the heuristic from Ref. [14] (based on numerical evidence that these are the best choices among all local phase-insensitive Gaussian channels). Thus, the isometries are manifestly phase covariant. However, note that our argument applies to arbitrary phase-covariant, bosonic Gaussian isometries $\mathcal{V}_{E_{1}\rightarrow E'_{1}F'_{1}}$ and $\mathcal{V}_{E_{2}\rightarrow E'_{2}F'_{2}}$.

Let $\rho_A$ denote an arbitrary input state of mean photon number $N_S$. The state $\rho_A$ can be input to the isometric channel $\mathcal{W}_{A\rightarrow B'E'_{2}F'_{2}}$. The entropy objective function $H(B|E'_{1}E'_{2})_{\mathcal{W}(\rho)} + H(B|F'_{1}F'_{2})_{\mathcal{W}(\rho)}$ is equal to a sum of conditional entropies and so we make use of two properties of
conditional entropy: its invariance under local unitaries and concavity. Set

$$\hat{N} \equiv \hat{n}_B + \hat{n}_{E_1'} - \hat{n}_{E_2'} + \hat{n}_{F_1'} - \hat{n}_{F_2'},$$

(2.86)

and consider the following phase shift unitary, depending on a phase $\phi \in \mathbb{R}$:

$$e^{i\hat{N}\phi} \equiv e^{i\hat{n}_B\phi} \otimes e^{i\hat{n}_{E_1}'\phi} \otimes e^{-i\hat{n}_{E_2}'\phi} \otimes e^{i\hat{n}_{F_1}'\phi} \otimes e^{-i\hat{n}_{F_2}'\phi}.$$  

(2.87)

Then it follows from the invariance of conditional entropy under local unitaries that

$$H(B|E_1'E_2')_{W(\rho)} + H(B|F_1'F_2')_{W(\rho)} = H(B|E_1'E_2')_{e^{i\hat{N}\phi}W(\rho)e^{-i\hat{N}\phi}} + H(B|F_1'F_2')_{e^{i\hat{N}\phi}W(\rho)e^{-i\hat{N}\phi}}. \quad (2.88)$$

Now exploiting the phase covariance of all of the isometric channels involved in $W_{A\rightarrow BE_1'E_2'F_1'F_2'}$ (see (2.74) and (2.78)), we find that the right hand side above is equal to

$$H(B|E_1'E_2')_{W(e^{i\hat{n}_A\rho}e^{-i\hat{n}_A\rho})} + H(B|F_1'F_2')_{W(e^{i\hat{n}_A\rho}e^{-i\hat{n}_A\rho})}.$$  

(2.89)

These equalities hold for any phase $\phi$ on the input, and so we can average over the input phase $\phi$ without changing the entropy objective function:

$$H(B|E_1'E_2')_{W(\rho)} + H(B|F_1'F_2')_{W(\rho)} = \frac{1}{2\pi} \int_0^{2\pi} d\phi \left[ H(B|E_1'E_2')_{W(e^{i\hat{n}_A\rho}e^{-i\hat{n}_A\rho})} + H(B|F_1'F_2')_{W(e^{i\hat{n}_A\rho}e^{-i\hat{n}_A\rho})} \right]. \quad (2.90)$$

Let us define the phase-invariant state $\rho_A$ as

$$\rho_A \equiv \frac{1}{2\pi} \int_0^{2\pi} d\phi \ e^{i\hat{n}_A\phi} \rho_A e^{-i\hat{n}_A\phi},$$  

(2.91)

and note that the mean photon number of $\rho_A$ is equal to $N_S$, which follows from the assumption that $\rho_A$ has mean photon number $N_S$ and the fact that phase averaging does not change the mean photon number. Now exploiting the concavity of conditional entropy and the equality in (2.90), we
find that

\[ H(B|E_1'E_2') W(\rho) + H(B|F_1'F_2') W(\rho) \leq H(B|E_1'E_2') W(\rho) + H(B|F_1'F_2') W(\rho). \] (2.92)

By combining with step three (extremality of Gaussian states), we conclude that, for an arbitrary state \( \rho_A \) of mean photon number \( N_S \), there exists a Gaussian, phase-invariant state that achieves the same or higher value of the entropy objective function \( H(B|E_1'E_2') + H(B|F_1'F_2') \). So this completes step four, and step five is the next conclusion, which is that the thermal state \( \theta(N_S) \) maximizes the entropy objective function with respect to all input states with mean photon number equal to \( N_S \).

We now move on to the final step six. In order to prove that the entropy objective function monotonically increases as a function of the mean photon number \( N_S \) of an input thermal state, we repeat steps similar to those above that we used for step four. Recall again that conditional entropy is invariant under local unitaries, and so we can apply arbitrary displacements without changing the entropy objective function. In particular, since the local displacements can be arbitrary, we take advantage of the specific covariances of beam splitters and two-mode squeezers from (2.72) and (2.77) when choosing the local displacements. We employ the following shorthand for the local displacements acting on the output modes of \( \mathcal{W} \):

\[
D_{\text{out}}^\alpha \equiv D_B(\sqrt{T\mathcal{G}}\alpha) \otimes D_{E_1'}(\sqrt{\eta_2(1-T)\alpha}) \otimes D_{F_1'}(\sqrt{(1-\eta_2)(1-T)\alpha})
\]

\[
\otimes D_{E_2'}(\sqrt{\eta_3 T(\mathcal{G}-1)\alpha^*}) \otimes D_{F_2'}(\sqrt{(1-\eta_3)T(\mathcal{G}-1)\alpha^*}), \] (2.93)

where \( \eta_2 \) and \( \eta_3 \) are the transmissivities of the beamsplitters \( \mathcal{V}_{E_1\rightarrow E_1'} \) and \( \mathcal{V}_{E_2\rightarrow E_2'} \), respectively (here, however just set to \( 1/2 \) for both). Let \( \theta(N_1) \) be a thermal state of mean photon number \( N_1 \geq 0 \). Then we find that

\[
H(B|E_1'E_2') W(\theta(N_1)) + H(B|F_1'F_2') W(\theta(N_1)) = H(B|E_1'E_2') D_{\text{out}}^\alpha W(\theta(N_1)) D_{\text{out}}^{\alpha\dagger} + H(B|F_1'F_2') D_{\text{out}}^\alpha W(\theta(N_1)) D_{\text{out}}^{\alpha\dagger}. \] (2.94)

Employing the displacement covariance of the isometric Gaussian channel \( \mathcal{W} \), we recast the local displacements on the outputs as a displacement of the input state:

\[
D_{\text{out}}^\alpha W(\theta(N_1)) D_{\text{out}}^{\alpha\dagger} = \mathcal{W}(D_A(\alpha)\theta(N_1)D_A^\dagger(\alpha)). \] (2.95)
Since this is true for any displacement $\alpha$, an expectation with respect to a probability distribution over $\alpha$ does not change the quantity, and by combining with (2.94), we find that

$$H(B|E'_1E'_2)_{W(\theta(N_1))} + H(B|F'_1F'_2)_{W(\theta(N_1))} =$$

$$\int d^2 \alpha \ p^{N_2}(\alpha) \left[ H(B|E'_1E'_2)_{W(D(\alpha)\theta(N_1)D^\dagger(\alpha))} + H(B|F'_1F'_2)_{W(D(\alpha)\theta(N_1)D^\dagger(\alpha))} \right].$$

(2.96)

In the above, we choose the distribution $p^{N_2}(\alpha)$ to be a complex, isotropic Gaussian with variance $N_2 \geq 0$. Now recall the well known fact that Gaussian random displacements of a thermal state produce a thermal state of higher mean photon number:

$$\int d^2 \alpha \ p^{N_2}(\alpha) \ D(\alpha)\theta(N_1)D^\dagger(\alpha) = \theta(N_1 + N_2).$$

(2.97)

The concavity of conditional entropy and the equality in (2.97) then imply that

$$H(B|E'_1E'_2)_{W(\theta(N_1))} + H(B|F'_1F'_2)_{W(\theta(N_1))} \leq H(B|E'_1E'_2)_{W(\theta(N_1+N_2))} + H(B|F'_1F'_2)_{W(\theta(N_1+N_2))}.$$}

(2.98)

Since $N_1, N_2 \geq 0$ are arbitrary, we conclude that the entropy objective function $H(B|E'_1E'_2) + H(B|F'_1F'_2)$ is monotone increasing with respect to the mean photon number of the input thermal state. This now completes step six, and as such, we conclude the proof. ■

**Remark 1** We note here that Ref. [14, Section C.2] provided an alternative way to handle step six in the above proof.

**Remark 2** Following Remark 21 of Ref. [100], the method used in the proof of Theorem 5 to establish the upper bound in (2.82) on $E_{sq}(N, \hat{n}, N_S)$ can be applied in far more general situations. Suppose that $\mathcal{N}$ is a single-mode input and multi-mode output channel. Suppose that $\mathcal{N}$ is phase covariant, such that a phase rotation on the input state is equivalent to a product of local phase rotations on the output. Suppose that $\mathcal{N}$ is covariant with respect to displacement operators, such that a displacement operator acting on the input state is equivalent to a product of local displacement operators on the output. Then by relaxing the energy-constrained squashed entanglement in such a
way that the squashing isometry has the same general phase and displacement covariances, it follows that, among all input states with mean photon number ≤ $N_S$, the resulting objective function is maximized by a thermal state input with mean photon number equal to $N_S$.

**Remark 3** We can apply Theorem 5 and Corollary 1 to the pure-loss channel in order to recover one of the main claims of Refs. [12, 79]. That is, the energy-constrained secret-key-agreement capacity of the pure-loss channel $\mathcal{L}_{\eta,0}$ is bounded from above as

$$P_2(\mathcal{L}_{\eta,0}, \hat{n}, N_S) \leq g(N_S(1 + \eta)/2) - g(N_S(1 - \eta)/2). \quad (2.99)$$

Also, the following bound holds for the pure-amplifier channel $\mathcal{A}_{\mathcal{G},0}$, as a special case of a more general result stated in Ref. [14]:

$$P_2(\mathcal{A}_{\mathcal{G},0}, \hat{n}, N_S) \leq g(N_S[\mathcal{G} + 1]/2 + [\mathcal{G} - 1]/2) - g([N_S + 1][\mathcal{G} - 1]/2). \quad (2.100)$$

Since the bound in (2.100) was not explicitly stated in Ref. [14], for convenience, the arXiv posting of Ref. [14] includes a Mathematica file that can be used to derive (2.100). Furthermore, other bounds on energy-constrained secret-key-agreement capacities of more general phase-insensitive channels are stated in Ref. [14].

**2.4.3 Improved Bounds for Energy-Constrained Secret-Key-Agreement Capacities of Bosonic Thermal Channels**

In this section, we discuss a variation of the method from Ref. [14] that leads to improvements of the bounds reported there. To begin with, we note that any single-mode phase-insensitive channel $\mathcal{M}$, which is not entanglement breaking [108], can be decomposed as a pure-amplifier channel of gain $\mathcal{G} > 1$ followed by a pure-loss channel of transmissivity $T \in (0, 1]$:

$$\mathcal{M} = \mathcal{L}_{T,0} \circ \mathcal{A}_{\mathcal{G},0}. \quad (2.101)$$

This result was found independently in Ref. [100, Theorem 30] and Refs. [107, 109] (see also Ref. [110]). It has been used in Ref. [109] to bound the unconstrained (and unassisted) quantum
capacity of a thermal channel, and it has been used in Ref. [100] to bound the energy-constrained (and unassisted) quantum and private capacities of an amplifier channel. After Ref. [109] appeared, it was subsequently used in Ref. [100] to bound the energy-constrained (and unassisted) quantum and private capacities of a thermal channel. It has also been used most recently in Ref. [107] in similar contexts.

For a thermal channel $\mathcal{L}_{\eta,N_B}$ of transmissivity $\eta \in [0,1]$ and thermal photon number $N_B \geq 0$, the decomposition is as above with

$$T = \eta - (1 - \eta) N_B,$$  \hspace{1cm} (2.102) \\
$$\mathcal{G} = \eta/T.$$  \hspace{1cm} (2.103)

Thus, given that a thermal channel is entanglement breaking when $\eta \leq (1 - \eta) N_B$ [111], it is clear that the decomposition is only valid (i.e., $T \in (0,1]$) whenever the thermal channel is not entanglement breaking. However, this is no matter when bounding secret-key-agreement or LOCC-assisted quantum capacities, due to the fact that they vanish for any entanglement-breaking channel.

Now, the main idea that leads to an improved energy-constrained bound is simply to employ
the decomposition in (2.101) and the same squashing isometries used in Ref. [14]. In other words, we are just swapping the top-left beamsplitter with the top-right two-mode squeezer in Figure 2.3. For concreteness, we have depicted this change in Figure 2.4. Let $\mathcal{W}$ denote the overall isometry taking the input mode $A$ to the output modes $BE_1'E_2'F_1'F_2'$, as depicted in Figure 2.4. Then by the same reasoning as in the proof of Theorem 5 and subsequently given in Remark 2, it follows that the thermal state $\theta(N_S)$ of mean photon number $N_S \geq 0$ optimizes a relaxation of the energy-constrained squashed entanglement corresponding to $\mathcal{W}$. This relaxation evaluates to

$$\frac{1}{2} \left[ H(B|E_1'E_2')_W(\theta(N_S)) + H(B|F_1'F_2')_W(\theta(N_S)) \right] = H(B|E_1'E_2')_W(\theta(N_S)), \quad (2.104)$$

with the latter equality following due the symmetry resulting from choosing each squashing isometry to be a 50-50 beamsplitter. This in turn implies the following:

**Proposition 2** For a thermal channel $\mathcal{L}_{\eta,N_B}$ of transmissivity $\eta \in [0,1]$ and thermal photon number $N_B \geq 0$ such that $\eta > (1 - \eta) N_B$, its energy-constrained secret-key-agreement capacity is bounded as

$$P_2(\mathcal{L}_{\eta,N_B}, \hat{n}, N_S) \leq H(B|E_1'E_2')_W(\theta(N_S)), \quad (2.105)$$

where $\mathcal{W}$ is the isometry depicted in Figure 2.4.

Now consider a general phase-insensitive single-mode bosonic Gaussian channel $\mathcal{M}$ that is not entanglement-breaking. By applying Proposition 2 and step six in the proof of Theorem 5, we find that the quantity $H(B|E_1'E_2')_W(\theta(N_S))$ is monotone increasing with $N_S$, with $\mathcal{W}$ the corresponding isometry in Figure 2.4. Furthermore, the limit exists for all $T \in (0,1)$ and $\mathcal{G} > 1$ and converges to the same expression as given in Ref. [14, Eq. (29)]:

$$\lim_{N_S \to \infty} H(B|E_1'E_2')_W(\theta(N_S)) = \frac{(1 - T^2)\mathcal{G} \log_2 \left( \frac{1 + T}{1 - T} \right) - (\mathcal{G}^2 - 1)T \log_2 \left( \frac{\mathcal{G} + 1}{\mathcal{G} - 1} \right)}{1 - \mathcal{G}^2 T^2}. \quad (2.106)$$

We evaluated the latter limit with the aid of Mathematica and note here that the source files are available for download with the arXiv posting of Ref. [24].

The fact that the expression in (2.106) is no different from that found in Ref. [14, Eq. (29)] can
be intuitively explained in the following way: Given that the input state to $W$ is a thermal state, the limit $N_S \to \infty$ in some sense is like a classical limit, and in this limit, the commutation of the pure-loss channel and the pure-amplifier channel in (2.101) makes no difference for the resulting expression. However, the values for $T$ and $\mathcal{F}$ for a thermal channel $\mathcal{L}_{\eta,N_B}$ for the decomposition in (2.101) are quite different from the values that $T$ and $\mathcal{F}$ would take in the decomposition in (2.81), and this is part of the reason that the decomposition in (2.101) leads to an improved bound for a thermal channel $\mathcal{L}_{\eta,N_B}$.

In particular, for a thermal channel $\mathcal{L}_{\eta,N_B}$, the expression in (2.106) converges to zero in the entanglement-breaking limit $\eta \to N_B/(N_B + 1)$ (or, equivalently, $N_B \to \eta/(1 - \eta)$ (this limit calculation is included in our Mathematica files also). Due to this fact and the monotonicity of $H(B|E_1' E_2')_{W(\theta(N_S))}$ with $N_S$, we conclude that the bound from Proposition 2 converges to zero in the entanglement-breaking limit for any finite photon number $N_S$. This explains the improved behavior of the bound in (2.105), as compared to that from Ref. [14], as we discuss in what follows.

Comparison of bounds on energy-constrained secret-key-agreement capacity of a thermal channel

We have evaluated the bound in (2.105) numerically, and we found strong numerical evidence that it outperforms the bound from Ref. [14] for any values of $N_S \geq 0$, $\eta \in [0, 1]$, and $N_B \geq 0$ such that $\eta > (1 - \eta) N_B$.

It is also interesting to compare the bound in (2.105) with the bounds from Ref. [14] and Refs. [15, 19], for particular parameter regimes. In Refs. [15, 19], the following photon-number-independent bound was established:

$$P_2(\mathcal{L}_{\eta,N_B}, \hat{n}, N_S) \leq -\log_2([1 - \eta] \eta^{N_B}) - g(N_B).$$  \hspace{1cm} (2.107)

Figure 2.5 plots the three different bounds for a fixed photon number $N_S = 0.1$ and thermal photon number $N_B = 1$. Therein, we see that the bound in (2.105) improves upon the bounds from Ref. [14] and Refs. [15, 19] for all transmissivities $\eta \in [1/2, 1]$. At $\eta = 1/2$, the channel becomes entanglement breaking for the aforementioned choice $N_B = 1$, and we see that the bound in (2.105)
Figure 2.5. Comparison of the “DSW18 bound” from (2.105) with prior bounds from Ref. [14] and Refs. [15, 19], with \( \eta \in [0.5, 1] \), \( N_S = 0.1 \) and \( N_B = 1 \). The plot shows that the bound in (2.105) converges to zero as the channel becomes entanglement breaking.

is converging to zero in the entanglement-breaking limit \( \eta \to 1/2 \), for fixed \( N_B = 1 \). The bound in (2.105) is also tighter than the one in (2.107) for all values depicted in the plot.

Figure 2.6 plots the three different bounds for other parameter regimes, now with \( N_S \in [0, 1] \), \( \eta = 0.1 \), and \( N_B \) set to \( 3 \times 10^{-7}, 1 \times 10^{-3}, \) and 0.1. These choices correspond to values expected in a variety of experimental scenarios, as first discussed in Ref. [23] and subsequently considered in Ref. [112]. The bound in (2.105) is essentially indistinguishable from that in Ref. [14] for \( N_B = 3 \times 10^{-7} \), but then the bound in (2.105) performs better as \( N_B \) increases.

The Matlab files used to generate Figures 2.5 and 2.6 are available for download with the arXiv posting of Ref. [24].

2.5 Multipartite Conditional Mutual Informations and Squashed Entanglement

In this section, we review two different definitions of multipartite conditional mutual information from Refs. [113–118], and we prove that they satisfy a duality relation that generalizes the following well known duality relation for conditional mutual information:

\[
I(A; B|C)_\psi = I(A; B|D)_\psi, \tag{2.108}
\]
Figure 2.6. Comparison of the “DSW18 bound” from (2.105) with prior bounds from Ref. [14] and Refs. [15, 19], with $N_S \in [0, 1]$, $\eta = 0.1$, and $N_B \in \{3 \times 10^{-7}, 1 \times 10^{-3}, 0.1\}$ (respectively, (a), (b), (c), above). The DSW18 bound from (2.105) is indistinguishable from the bound from Ref. [14] for small $N_B$, but then the bounds are very different for higher $N_B$. In (a), GEW16 is not visible because it overlaps with DSW18.
which holds for an arbitrary four-party pure state $\psi_{ABCD}$. This duality relation was established in Ref. [119] and interpreted operationally therein in terms of the quantum state redistribution protocol [119,120], and it was recently generalized to the infinite-dimensional case in Ref. [72], by employing the definition of conditional mutual information from (1.37)–(1.38).

After establishing the multipartite generalization of the duality relation in (2.108), we prove that it implies that two definitions of multipartite squashed entanglement [117,118] that were previously thought to be different are in fact equal to each other.

We finally then recall various properties of multipartite squashed entanglement, including how to evaluate it for multipartite GHZ and private states.

2.5.1 Multipartite Conditional Quantum Mutual Informations

We now recall two different multipartite generalizations of conditional mutual information [113–118]. Consider an $m$-party state $\rho_{A_1 \cdots A_m}$ acting on a tensor product of infinite-dimensional, separable Hilbert spaces. Let $\rho_{A_1 \cdots A_mE}$ denote an extension of this state, which in turn can be purified to $\phi_{A_1 \cdots A_mE}$. The two generalizations of conditional quantum mutual information are known as the conditional total correlation and the conditional dual total correlation:

**Definition 3 ([72,113,117,118])** The conditional total correlation of a state $\rho_{A_1 \cdots A_mE}$ is defined as

$$I(A_1; \cdots; A_m|E) \equiv \sum_{i=2}^{m} I(A_i; A_{i-1}^i|E)\rho. \quad (2.109)$$

The notation $A_{i-1}^i$ refers to all the systems $A_1 \cdots A_{i-1}$.

**Definition 4 ([72,114–116])** The conditional dual total correlation of a state $\rho_{A_1 \cdots A_mE}$ is defined as

$$\tilde{I}(A_1; \cdots; A_m|E) \equiv \sum_{i=2}^{m} I(A_i; A_{i-1}^i|A_{i+1}^m E)\rho, \quad (2.110)$$

where $A_{i+1}^m \equiv A_{i+1} \cdots A_m$.

Many years after the dual total correlation was defined and analyzed in Refs. [114,115], the conditional version of it was called “secrecy monotone” in Ref. [116] and analyzed there.
Note that the above quantities are invariant with respect to permutations of the systems $A_1, \ldots, A_m$. This is more easily seen in the finite-dimensional case. That is, if the state $\rho_{A_1 \cdots A_m E}$ is finite-dimensional, then we have the following identities:

$$I(A_1; \cdots; A_m|E)_\rho = \sum_{i=1}^{m} H(A_i|E)_\rho - H(A_1 \cdots A_m|E)_\rho$$  \hspace{1cm} (2.111)

and

$$\tilde{I}(A_1; \cdots; A_m|E)_\rho = \sum_{i=1}^{m} H(A_{[m]\{i\}}|E)_\rho - (m-1)H(A_1 \cdots A_m|E)_\rho = H(A_1 \cdots A_m|E)_\rho - \sum_{i=1}^{m} H(A_i|A_{[m]\{i\}}|E)_\rho.$$  \hspace{1cm} (2.112)

Although the two generalizations of CQMI in (2.109) and (2.110) are generally incomparable, they are related by the following identity [118]:

$$I(A_1; \cdots; A_m|E)_\rho + \tilde{I}(A_1; \cdots; A_m|E)_\rho = \sum_{i=1}^{m} I(A_i; A_{[m]\{i\}}|E)_\rho.$$  \hspace{1cm} (2.113)

The invariance of the above quantities with respect to permutations of the subsystems, as well as the validity of the identity in (2.113) in the general infinite-dimensional case, are consequences of Propositions 5 and 7 in Ref. [72].

2.5.2 Duality for the Conditional Total Correlation and the Conditional Dual Total Correlation

We now generalize the duality of CQMI in (2.108) to the multipartite setting:

**Theorem 6** For a multipartite pure state $\phi_{A_1 \cdots A_m E F}$, the following equality holds

$$I(A_1; \cdots; A_m|E)_{\phi^\rho} = \tilde{I}(A_1; \cdots; A_m|F)_{\phi^\rho}.$$  \hspace{1cm} (2.114)

**Proof.** There are at least two ways to see this. For the general infinite-dimensional case, we can
simply apply definitions and the duality relation in (2.108). We find that

\[
I(A_1; \cdots; A_m|E)_{\phi^\rho} = \sum_{i=2}^{m} I(A_i; A_i^{i-1}|E)_{\phi^\rho} = \sum_{i=2}^{m} I(A_i; A_i^{i-1}|A_{i+1}^m F)_{\phi^\rho} = \tilde{I}(A_1; \cdots; A_m|F)_{\phi^\rho}.
\] (2.115)

(2.116)

(2.117)

In the less general case in which conditional entropies are finite, we can apply a slightly different, but related method. Recall that conditional entropy obeys a duality property: for a pure state \(\psi_{ABC}\), we have that \(H(A|B)_{\psi} = -H(A|C)_{\psi}\). Using the identities given above and this duality, we find that

\[
I(A_1; \cdots; A_m|E)_{\phi^\rho} = \sum_{i=1}^{m} H(A_i|E)_{\phi^\rho} - H(A_1 \cdots A_m|E)_{\phi^\rho} = \sum_{i=1}^{m} H(A_i|A_{[m]\{i}\} F)_{\phi^\rho} + H(A_1 \cdots A_m|F)_{\phi^\rho} = \tilde{I}(A_1; \cdots; A_m|F)_{\phi^\rho}.
\] (2.118)

(2.119)

(2.120)

This concludes the proof. \(\blacksquare\)

**Remark 4** It is interesting to compare the somewhat long route by which Han arrived at the conditional dual total correlation in Ref. [115], versus the comparatively short route by which we arrive at it in Theorem 6. This latter method of using purifications and related entropy identities is unique to quantum information theory. It is also pleasing to find that the conditional total correlation and the conditional dual total correlation are dual to each other in the entropic sense of Theorem 6.

### 2.5.3 Equivalence of Multipartite Squashed Entanglements

Two multipartite generalizations of the squashed entanglement of a state \(\rho_{A_1 \cdots A_m}\) are based on the conditional total correlation and the conditional dual total correlation [117,118]:

\[
E_{sq}(A_1; \cdots; A_m)_{\rho} \equiv \frac{1}{2} \inf_{\rho_{A_1 \cdots A_m E}} \left\{ I(A_1; \cdots; A_m|E)_{\rho} : \text{Tr}_E \{\rho_{A_1 \cdots A_m E}\} = \rho_{A_1 \cdots A_m} \right\}.
\] (2.121)
\[
\tilde{E}_{\text{sq}}(A_1; \cdots ; A_m)_{\rho} \equiv \frac{1}{2} \inf_{\rho_{A_1 \cdots A_mE}} \left\{ \tilde{I}(A_1; \cdots ; A_m|E)_{\rho} : \text{Tr}_E(\rho_{A_1 \cdots A_mE}) = \rho_{A_1 \cdots A_m} \right\}. \tag{2.122}
\]

By employing Theorem 6, we find that these quantities are in fact always equal to each other, so that there is no need to consider two separate definitions, as was previously done in Refs. [13,118]:

**Theorem 7** For a multipartite state \( \rho_{A_1 \cdots A_m} \), the following equality holds

\[
E_{\text{sq}}(A_1; \cdots ; A_m)_{\rho} = \tilde{E}_{\text{sq}}(A_1; \cdots ; A_m)_{\rho}. \tag{2.123}
\]

**Proof.** Let \( \rho_{A_1 \cdots A_mE} \) be an extension of \( \rho_{A_1 \cdots A_m} \), and let \( \phi^\rho_{A_1 \cdots A_mE} \) be a purification of \( \rho_{A_1 \cdots A_mE} \). Then by Theorem 6,

\[
I(A_1; \cdots ; A_m|E)_{\rho} = \tilde{I}(A_1; \cdots ; A_m|F)_{\phi^\rho} \geq 2\tilde{E}_{\text{sq}}(A_1; \cdots ; A_m)_{\rho}. \tag{2.124}
\]

The inequality holds because \( \phi^\rho_{A_1 \cdots A_mE} \) is a particular extension of \( \rho_{A_1 \cdots A_m} \), and the squashed entanglement involves an infimum over all extensions of \( \rho_{A_1 \cdots A_m} \). Since the inequality holds for all extensions of \( \rho_{A_1 \cdots A_m} \), we can conclude that

\[
E_{\text{sq}}(A_1; \cdots ; A_m)_{\rho} \geq \tilde{E}_{\text{sq}}(A_1; \cdots ; A_m)_{\rho}. \tag{2.126}
\]

A proof for the other inequality \( \tilde{E}_{\text{sq}}(A_1; \cdots ; A_m)_{\rho} \geq E_{\text{sq}}(A_1; \cdots ; A_m)_{\rho} \) goes similarly. \( \blacksquare \)

**Remark 5** One of the main results of Ref. [13] was to establish bounds on the secret-key-agreement capacity region of a quantum broadcast channel in terms of multipartite squashed entanglements. Theorem 7 demonstrates that essentially half of the upper bounds written down in Ref. [13] were in fact redundant. The same is true for the key distillation bounds from Ref. [118].

### 2.5.4 Partitions and multipartite squashed entanglement

In this brief section, we recall some notation from Ref. [13, Section 2.7], which we use in what follows as a shorthand for describing various partitions of a set of quantum systems and their
corresponding multipartite squashed entanglements. Given a set $W$ of quantum systems, a partition $G = \{\chi_1, \ldots, \chi_{|G|}\}$ is a set of non-empty subsets of $W$ such that

$$\bigcup_{\chi_i \in G} \chi_i = W, \quad (2.127)$$

and for all $\chi_i, \chi_j \in G$, $i \neq j$,

$$\chi_i \cap \chi_j = \emptyset. \quad (2.128)$$

For example, one possible partition of $W = \{A, B, C\}$ is given by $G = \{\{A\}, \{B\}, \{C\}\}$. The power set $\mathcal{P}(W)$ is the set of all subsets of $W$. The sets $\mathcal{P}_{\geq 1}(W)$ and $\mathcal{P}_{\geq 2}(W)$ are the sets of all subsets of $W$ with greater than or equal to one and two members, respectively. That is, for $W = \{A, B, C\}$,

$$\mathcal{P}(W) = \{\emptyset, \{A\}, \{B\}, \{C\}, \{A, B\}, \{A, C\}, \{B, C\}, \{A, B, C\}\}, \quad (2.129)$$

$$\mathcal{P}_{\geq 1}(W) = \{\{A\}, \{B\}, \{C\}, \{A, B\}, \{A, C\}, \{B, C\}, \{A, B, C\}\}, \quad (2.130)$$

$$\mathcal{P}_{\geq 2}(W) = \{\{A, B\}, \{A, C\}, \{B, C\}, \{A, B, C\}\}. \quad (2.131)$$

Given a set $\mathcal{Y}$, let $\omega_\mathcal{Y}$ denote a $|\mathcal{Y}|$-partite state shared by the parties specified by the elements of $\mathcal{Y}$. If $G$ is a partition of $\mathcal{Y}$, then the notation

$$E_{sq}(G)_\omega \quad (2.132)$$

refers to the multipartite squashed entanglement with parties grouped according to partition $G$. For example, if $\mathcal{Y} = \{A, B, C\}$, $\omega_\mathcal{Y} = \omega_{ABC}$, $G_1 = \{\{A\}, \{B\}, \{C\}\}$, and $G_2 = \{\{AB\}, \{C\}\}$, then

$$E_{sq}(G_1)_\omega = E_{sq}(A; B; C)_\omega, \quad (2.133)$$

and

$$E_{sq}(G_2)_\omega = E_{sq}(AB; C)_\omega. \quad (2.134)$$

### 2.5.5 Multipartite Private States

One multipartite generalization of the maximally entangled state in (1.3) is the Greenberger-Horne-Zeilinger (GHZ) state. A GHZ state of $\log_2 K$ entangled bits of an $m$-party system $A_1, \ldots,$
takes the form
\[ |\Phi\rangle_{A_1\cdots A_m} = \frac{1}{\sqrt{K}} \sum_{i=1}^{K} |i\rangle_{A_1} \otimes \cdots \otimes |i\rangle_{A_m} \]  
(2.135)

where \{\{|i\rangle_{A_1}\}, \ldots, \{|i\rangle_{A_m}\}\} are orthonormal basis sets for their respective systems. The bipartite private states from (1.67) are similarly generalized to the multipartite case [121], so that a state of \(\log_2 K\) private bits is as follows:

\[ \gamma_{A_1\cdots A_m A'_1\cdots A'_m} = U_{A_1\cdots A_m A'_1\cdots A'_m} \langle \Phi | \Phi \rangle_{A_1\cdots A_m} \otimes \rho_{A'_1\cdots A'_m} U_{A_1\cdots A_m A'_1\cdots A'_m}^\dagger, \]  
(2.136)

with the GHZ state generalizing the role of the maximally entangled state, and the twisting unitary from (1.69) is generalized as

\[ U_{A_1\cdots A_m A'_1\cdots A'_m} = \sum_{i_1, \ldots, i_m=1}^{K} |i_1, \ldots, i_m\rangle \langle i_1, \ldots, i_m|_{A_1\cdots A_m} \otimes U_{A'_1\cdots A'_m}^{i_1\cdots i_m}, \]  
(2.137)

where \(U_{A'_1\cdots A'_m}^{i_1\cdots i_m}\) are unitary operators depending on the values \(i_1, \ldots, i_m\).

### 2.5.6 Properties of Multipartite Squashed Entanglement

Multipartite squashed entanglement possesses a number of useful properties that have been proven separately in Ref. [13] for the quantities in (2.121) and (2.122). In light of Theorem 7, we now know that these measures are equal. Since we require these properties in what follows, we recall some of them here:

**Lemma 8 (Subadditivity [13])** Given a pure state \(\phi_{R A_1\cdots A_m B_1\cdots B_m E F}\), the following inequality holds

\[ E_{sq}(R; A_1 B_1; \cdots ; A_m B_m)_{\phi} \leq E_{sq}(R A^m E; B_1; \cdots ; B_m)_{\phi} + E_{sq}(R B^m F; A_1; \cdots ; A_m)_{\phi} \]  
(2.138)

where the notation \(A^m\) refers to all systems \(A_1 \cdots A_m\) and a similar convention for \(B^m\).

Technically speaking, Ref. [13] did not establish the above statement in the general infinite-dimensional case, but we note here that the approach from Ref. [72] can be used to establish the lemma above.
Lemma 9 (Monotonicity for Groupings [13]) Squashed entanglement is non-increasing when subsystems are grouped. That is, given a state $\rho_{A_1 \cdots A_m}$, the following inequality holds

$$E_{sq}(A_1; A_2; \cdots; A_m) \geq E_{sq}(A_1A_2; A_3; \cdots; A_m) \rho.$$  (2.139)

Lemma 10 (Product States [13]) Let

$$\omega_{AB_1 \cdots B_m} = \rho_A \otimes \sigma_{B_1 \cdots B_m}$$  (2.140)

where $\rho_A$ and $\sigma_{B_1 \cdots B_m}$ are density operators. Then

$$E_{sq}(A; B_1; \cdots; B_m)_\omega = E_{sq}(B_1; \cdots; B_m)_{\sigma}.$$  (2.141)

We also have the following alternative representation of multipartite squashed entanglement, which was employed implicitly in Ref. [13]:

Lemma 11 Let $\rho_{A_1 \cdots A_m}$ be a multipartite density operator such that the entropy $H(A_i) \rho < \infty$ for all $i \in \{2, \ldots, m\}$. Then its multipartite squashed entanglement can be written as

$$E_{sq}(A_1; A_2; \cdots; A_m) \rho = \frac{1}{2} \inf_{\mathcal{V}_{E \to E'F}} \left[ \sum_{i=2}^m H(A_i|E')_\omega + H(A_2 \cdots A_m|F)_\omega \right],$$  (2.142)

where the infimum is with respect to an isometric channel $\mathcal{V}_{E \to E'F}$,

$$\omega_{A_1 \cdots A_mE'F} \equiv \mathcal{V}_{E \to E'F}(\phi_{A_1 \cdots A_mE}^\rho),$$  (2.143)

and $\phi_{A_1 \cdots A_mE}^\rho$ is a purification of $\rho_{A_1 \cdots A_m}$.

Proof. A proof follows easily from the definition of $E_{sq}(A_1; A_2; \cdots; A_m) \rho$ in (2.121), rewriting it in terms of a squashing isometry as has been done in the bipartite case, and employing duality of conditional entropy. ■
2.5.7 Multipartite Squashed Entanglement for GHZ and Private States

The multipartite squashed entanglement of a maximally entangled state or a private state scales linearly with the number of parties \([13, 118]\). That is, for \(\Phi_{A_1 \cdots A_m}\) a GHZ state as in (2.135) and \(\gamma_{A_1 \cdots A_m}\) a private state as in (2.136), then the following relations hold

\[
E_{sq}(A_1; \cdots ; A_m)_{\Phi} = \frac{m}{2} \log_2 K, \tag{2.144}
\]

\[
E_{sq}(A_1; \cdots ; A_m)_{\gamma} \geq \frac{m}{2} \log_2 K. \tag{2.145}
\]

Now consider a set \(W = \{A, B, C\}\) of systems and let \(\Psi_{ABC}\) be composed of maximally entangled states \(\Phi\) and private states \(\gamma\) over the systems \(A, B,\) and \(C\), according to the power set in (2.131) for two or more members:

\[
\Psi_{ABC} = \Phi_{A_1B_1} \otimes \Phi_{A_2C_2} \otimes \Phi_{B_3C_3} \otimes \Phi_{A_4B_4C_4} \otimes \gamma_{A_5B_5} \otimes \gamma_{A_6C_6} \otimes \gamma_{B_7C_7} \otimes \gamma_{A_8B_8C_8}. \tag{2.146}
\]

In the above, we have subdivided the systems \(A, B,\) and \(C\) for the various correlations so that, in the given example,

\[
A = A_1A_2A_4A_5A_6A_8, \tag{2.147}
\]

\[
B = B_1B_3B_4B_5B_7B_8, \tag{2.148}
\]

\[
C = C_2C_3C_4C_6C_7C_8. \tag{2.149}
\]

For each of the constituent states given in (2.146), we denote the number of entangled bits or private bits as \(E\) or \(K\), respectively, as done in Ref. [13]. For example,

\[
E_{AB} = H(A_1)_{\Phi} = H(B_1)_{\Phi} = \log_2 K_{A_1}, \tag{2.150}
\]

\[
K_{ABC} = H(A_8)_{\gamma} = H(B_8)_{\gamma} = H(C_8)_{\gamma} = \log_2 K_{A_8}, \tag{2.151}
\]

and so the tuple \((E_{AB}, E_{AC}, E_{BC}, E_{ABC}, K_{AB}, K_{AC}, K_{BC}, K_{ABC})\) characterizes the entangled and private bit content of the state. By using (2.144) and (2.145), along with the additivity of squashed
entanglement for tensor-product states and adopting the notation in (2.150) and (2.151), we find that

\[
E_{sq}(A; B; C)_\Psi = E_{sq}(A_1; B_1)_\Phi + E_{sq}(A_2; C_2)_\Phi + E_{sq}(B_3; C_3)_\Phi + E_{sq}(A_4; B_4; C_4)_\Phi \\
+ E_{sq}(A_5; B_5)_\gamma + E_{sq}(A_6; C_6)_\gamma + E_{sq}(B_7; C_7)_\gamma + E_{sq}(A_8; B_8; C_8)_\gamma \tag{2.152}
\]

\[
\geq E_{AB} + E_{AC} + E_{BC} + \frac{3}{2}E_{ABC} + K_{AB} + K_{AC} + K_{BC} + \frac{3}{2}K_{ABC}. \tag{2.153}
\]

As in (2.133) and (2.134), if \(\Psi_{ABC} = \Psi_Y\) for \(Y = \{A, B, C\}\), and for partitions \(G_1 = \{\{A\}, \{B\}, \{C\}\}\) and \(G_2 = \{\{AB\}, \{C\}\}\) then \(E_{sq}(G_1) = E_{sq}(A; B; C)_\Psi\) as shown in (2.133). For \(E_{sq}(G_2)\), we have that

\[
E_{sq}(G_2) = E_{sq}(AB; C)_\Psi \tag{2.154}
\]

\[
= E_{sq}(A_2; C_2)_\Phi + E_{sq}(B_3; C_3)_\Phi + E_{sq}(A_4B_4; C_4)_\Phi \\
+ E_{sq}(A_6; C_6)_\gamma + E_{sq}(B_7; C_7)_\gamma + E_{sq}(A_8B_8; C_8)_\gamma \tag{2.155}
\]

\[
\geq E_{AC} + E_{BC} + E_{ABC} + K_{AC} + K_{BC} + K_{ABC}. \tag{2.156}
\]

### 2.6 Quantum Broadcast Channels and Secret-Key-Agreement Capacity Regions

A quantum broadcast channel is a channel as defined in (1.4), except that it is a map from one sender to multiple receivers [122]. A protocol for energy-constrained, multipartite secret key agreement is much the same as in the bipartite case outlined in Section 2.2, with a constraint on the average energy of the channel input states and with rounds of LOCC between channel uses. For demonstrative purposes, in this section we focus exclusively on the case of a single sender and two receivers. We make use of an energy observable \(G\) and energy constraint \(P \in [0, \infty)\). A quantum broadcast channel \(N_{A\rightarrow BC}\) satisfies the finite output-entropy condition with respect to \(G\) and \(P\) if

\[
\sup_{\rho_A : V \{G_{\rho_A} \leq P\}} H(N_{A\rightarrow BC}(\rho_A)) < \infty. \tag{2.157}
\]

In what follows, for example, we denote the rate of entanglement generation between the sender \(A\) and the receiver \(B\) by \(R_{AB}^E\) and the rate of key generation by \(R_{AB}^K\). Generalizing this, we have a
vector $\vec{R}$ of rates, for which we employ the following shorthand:

$$\vec{R} \equiv (R^E_{AB}, R^E_{AC}, R^E_{BC}, R^K_{AB}, R^K_{AC}, R^K_{BC}, R^K_{ABC}).$$

(2.158)

In a general $(n, \vec{R}, G, P, \varepsilon)$ protocol, the sender Alice and the receivers Bob and Charlie are tasked to use a quantum broadcast channel $\mathcal{N}_{A \rightarrow BC}$ $n$ times to establish a shared state $\Omega_{ABC}$ such that

$$F(\Omega_{ABC}, \Psi_{ABC}) \geq 1 - \varepsilon,$$

(2.159)

with $\Psi$ defined in (2.146) and the elements of $\vec{R}$ are given by, e.g., Ref. [13]

$$R^E_{AB} = \frac{E_{AB}}{n} = \frac{1}{n} H(A_1)_\Psi,$$

(2.160)

$$R^K_{AB} = \frac{K_{AB}}{n} = \frac{1}{n} H(A_5)_\Psi.$$

(2.161)

In such a protocol, Alice, Bob, and Charlie begin by performing an LOCC channel $\mathcal{L}_{\emptyset \rightarrow A'_i A'_1 B'_1 C'_1}$ to create a state $\rho^{(1)}_{A'_1 A'_1 B'_1 C'_1}$ that is separable with respect to the cut $A'_1 A_1 | B'_1 | C'_1$, and where $A'_1$, $B'_1$, and $C'_1$ are scratch systems. Alice then uses $A_1$ as the input to the first channel use, resulting in the state

$$\sigma^{(1)}_{A'_1 B'_1 B'_1 C'_1} \equiv \mathcal{N}_{A_1 \rightarrow B_1 C_1} (\rho^{(1)}_{A'_1 A'_1 B'_1 C'_1}).$$

(2.162)

Alice, Bob, and Charlie then perform a second LOCC channel, producing

$$\rho^{(2)}_{A'_2 A'_2 B'_2 C'_2} \equiv \mathcal{L}_{A'_1 B'_1 B'_1 C'_1 \rightarrow A'_2 A'_2 B'_2 C'_2} (\sigma^{(1)}_{A'_1 B'_1 B'_1 C'_1}).$$

(2.163)

The procedure continues in this manner, as in Section 2.2, with a total of $n$ rounds of LOCC interleaved with $n$ uses of the channel as follows: for $i \in \{2, \ldots, n\}$

$$\rho^{(i)}_{A'_i A'_i B'_i C'_i} \equiv \mathcal{L}_{A'_{i-1} B'_{i-1} B'_{i-1} C'_{i-1} \rightarrow A'_i A'_i B'_i C'_i} (\sigma^{(i-1)}_{A'_{i-1} B'_{i-1} B'_{i-1} C'_{i-1}}),$$

(2.164)

$$\sigma^{(i)}_{A'_i B'_i B'_i C'_i} \equiv \mathcal{N}_{A_i \rightarrow B_i C_i} (\rho^{(i)}_{A'_i A'_i B'_i C'_i}).$$

(2.165)

After the $n$th channel use, a final, $(n + 1)$th LOCC channel is performed. Going to the purified
picture as before, tracing over the eavesdropper’s systems while retaining the shield systems, the goal is to establish the state \( \Omega_{ABC} \) satisfying \( F(\Omega_{ABC}, \Psi_{ABC}) \geq 1 - \varepsilon \), where \( \Psi_{ABC} \) is the ideal state from (2.146). Finally, the same average energy constraint for the channel input states, as in (2.30), should be satisfied.

The rate tuple \( \vec{R} \) is achievable if for all \( \varepsilon \in (0, 1) \), \( \delta \geq 0 \), and sufficiently large \( n \), there exists an \( (n, \vec{R} - \delta, G, P, \varepsilon) \) protocol as outlined above. The energy-constrained secret-key-agreement capacity region of the channel \( \mathcal{N} \) is the closure of the region mapped out by all achievable rate tuples subject to the energy constraint \( P \).

### 2.6.1 Energy-Constrained Squashed Entanglement Upper Bound for the LOCC-Assisted Capacity Region of a Quantum Broadcast Channel

The main result of this section is a generalization of the result in Section 2.3, as well as a generalization of the main result in Ref. [13]. In particular, we prove that the energy-constrained, multipartite squashed entanglement is a key tool in bounding the LOCC-assisted capacity region of a quantum broadcast channel.

**Theorem 12** Let \( G \) be a Gibbs observable, and let \( P \in [0, \infty) \) be an energy constraint. Let \( \mathcal{N}_{A \to BC} \) be a quantum broadcast channel satisfying the finite-output entropy condition in (2.157) with respect to \( G \) and \( P \). Suppose that \( \vec{R} \) is an achievable rate tuple for LOCC-assisted private and quantum communication. Then the elements of the rate tuple \( \vec{R} \) are bounded in terms of multipartite squashed entanglement as

\[
R_{AE} + R_{AK} + R_{BE} + R_{BK} + R_{AEC} + R_{ABC} \leq E_{sq}(SB; C)\omega, \tag{2.166}
\]
\[
R_{AB} + R_{AE} + R_{BE} + R_{BK} + R_{ABC} + R_{ABC} \leq E_{sq}(SC; B)\omega, \tag{2.167}
\]
\[
R_{AB} + R_{AE} + R_{AC} + R_{AK} + R_{ABC} + R_{ABC} \leq E_{sq}(S; BC)\omega, \tag{2.168}
\]
\[
R_{AB} + R_{AE} + R_{AC} + R_{AK} + R_{ABC} + R_{ABC} + \frac{3}{2} (R_{ABC} + R_{ABC}) \leq E_{sq}(S; B; C)\omega, \tag{2.169}
\]

for some pure state \( \psi_{SA} \) satisfying \( \text{Tr}\{G\psi_{SA}\} \leq P \), with the state \( \omega_{SBC} \) defined in terms of it as

\[
\omega_{SBC} = \mathcal{N}_{A \to BC}(\psi_{SA}). \tag{2.170}
\]
Proof. The proof of this bound follows that of Proposition 1 and Ref. [13, Theorem 12], working backward through the communication protocol one channel use at a time in order to demonstrate the inequalities. For this reason, we keep the proof brief. Let us begin by considering the partition \( \mathcal{G}_1 = \{\{A\}, \{B\}, \{C\}\} \). From reasoning as in (2.153) but instead applying an estimate in Ref. [21, Theorem 6] to the condition \( F(\Omega_{ABC}, \Psi_{ABC}) \geq 1 - \varepsilon \), we find that

\[
n \left( R^E_{AC} + R^K_{AC} + R^E_{BC} + R^K_{BC} + R^E_{AB} + R^K_{AB} + \frac{3}{2}(R^E_{ABC} + R^K_{ABC}) \right) \leq E_{sq}(A; B; C) + f_2(n, \varepsilon), \tag{2.171}
\]

where \( f_2(n, \varepsilon) \) is a function such that \( f_2(n, \varepsilon)/n \) tends to zero as \( n \to \infty \) and as \( \varepsilon \to 0 \).

If we look at just the squashed entanglement term of (2.171), we can split it and group terms, working backward through the \( n \) channel uses of the protocol:

\[
E_{sq}(A; B; C) \leq E_{sq}(A'_n; B'_n; C'_n)_{\sigma(n)} \tag{2.172}
\]

\[
\leq E_{sq}(A'_n B'_n C'_n; R_n; B'_n; C'_n)_{\sigma(n)} + E_{sq}(A'_n B'_n C'_n R_n; B'_n; C'_n)_{\sigma(n)} \tag{2.173}
\]

\[
= E_{sq}(A'_n B'_n C'_n)_{\rho(n)} + E_{sq}(A'_n B'_n C'_n R_n; B'_n; C'_n)_{\sigma(n)} \tag{2.174}
\]

\[
\leq E_{sq}(A'_{n-1}; B_{n-1} B'_{n-1}; C'_{n-1})_{\sigma(n-1)} + E_{sq}(A'_n B'_n C'_n R_n; B'_n; C'_n)_{\sigma(n)} \tag{2.175}
\]

\[
\leq \sum_{i=1}^{n} E_{sq}(A'_i B'_i C'_i R_i; B'_i; C'_i)_{\sigma(i)}. \tag{2.176}
\]

The first inequality follows from the monotonicity of squashed entanglement under LOCC. For the second inequality the quantity has been split using the subadditivity property from Lemma 8 (there are also some implicit purifying systems \( R \) and \( E \), which we have not explicitly defined, but note that \( E \) denotes an environment of the broadcast channel). The equality is a result of the invariance of squashed entanglement under isometries, because an isometric extension of \( \mathcal{N} \) relates \( A_n \) to \( B_n C_n E_n \). The third inequality is the beginning of the first repetition of this procedure, in which we again apply the monotonicity of squashed entanglement under LOCC. Iterating this reasoning \( n \) times leads to the final inequality in (2.176). Working backward another step yields no additional terms, because the initial state is separable, having been created through LOCC. However, with purifying systems \( R_i \), we combine (2.176) with (2.171) to conclude that there exists a state \( \omega \), as
defined in (2.170), such that
\[
\sum_{i=1}^{n} \mathbb{E}_{\text{sq}}(A'_i B'_i C'_i R_i; B_i; C_i)_{\sigma(i)} \leq n \mathbb{E}_{\text{sq}}(S; B; C)_{\omega} \tag{2.177}
\]

and
\[
R^E_{AC} + R^K_{AC} + R^E_{BC} + R^K_{BC} + R^E_{AB} + R^K_{AB} + \frac{3}{2} (R^E_{ABC} + R^K_{ABC}) \leq \mathbb{E}_{\text{sq}}(S; B; C)_{\omega} + \frac{1}{n} f_2(n, \varepsilon). \tag{2.178}
\]

Taking the limit \( n \to \infty \) and then \( \varepsilon \to 0 \) yields (2.169). A similar rationale can be applied to obtain the other bounds, and key to the claim, as in the proof of Ref. [13, Theorem 12], is that the same state \( \omega \) can be used in all of the bounds. ■

\begin{remark}
Just as Ref. [13, Theorem 12] was generalized from the single-sender, two-receiver case to the single sender, \( m \)-receiver case in Ref. [13, Theorem 13], our above bounds for the energy-constrained capacity region of the quantum broadcast channel can be generalized to an \( m \)-receiver case through the consideration of the many possible partitions, as described in Section 2.5.4.
\end{remark}

2.6.2 Upper Bounds on the Energy-Constrained LOCC-Assisted Capacity Regions of a Pure-Loss Bosonic Broadcast Channel

In this section, we focus on a concrete quantum broadcast channel, known as the pure-loss broadcast channel. The model for this channel was introduced in Ref. [123] and subsequently studied in Refs. [13, 16]. It is equivalent to a linear sequence of beamsplitters, in which the sender inputs into the first one, the vacuum state is injected into all of the environment ports, the receivers each get one output from the sequence of beamsplitters and one output of the beamsplitters is lost to the environment (see Figure 3-13 of Ref. [123] or Figure 1c of Ref. [16]). In what follows, we adopt the same strategy as before for the single-mode pure-loss channel (and what was subsequently used in Ref. [13]), and we relax the squashing isometry for the environment mode to be a 50-50 beamsplitter.

Using this strategy, we now calculate bounds on rates of energy-constrained entanglement generation and key distillation achievable between the sender and one of the receivers. The same
reasoning as in Remark 2, along with the representation of multipartite squashed entanglement in Lemma 11 and the relaxation of it described above, allow us to conclude that, for a given input mean photon number constraint $N_S \geq 0$, a thermal state of that photon number is optimal.

Before stating the theorem, we establish the following notation:

- The set of all receivers is denoted by $\mathcal{B} = \{B_1, \ldots, B_m\}$. The total transmissivity for all receivers is $\eta_\mathcal{B} \in [0, 1]$.

- In the theorem below, the set $\mathcal{T}$ denotes a subset of the receivers ($\mathcal{T} \subseteq \mathcal{B}$), and its complement set is denoted by $\overline{\mathcal{T}} = \mathcal{B}\setminus\mathcal{T}$. The total transmissivity to the members of the set $\mathcal{T}$ is denoted by $\eta_\mathcal{T} = \sum_{B_i \in \mathcal{T}} \eta_{B_i}$, and the total transmissivity to the members of the complement set is denoted by $\eta_{\overline{\mathcal{T}}} = \sum_{B_i \in \overline{\mathcal{T}}} \eta_{B_i}$, such that $\eta_\mathcal{T} + \eta_{\overline{\mathcal{T}}} = \eta_\mathcal{B}$.

- The transmissivity to the adversary Eve is denoted by $\eta_E = 1 - \eta_\mathcal{B} = 1 - \eta_\mathcal{T} - \eta_{\overline{\mathcal{T}}}$.

With this notation, we can now establish the following theorem:

**Theorem 13** The energy-constrained LOCC-assisted capacity region of a pure-loss quantum broadcast channel, for entanglement and key distillation between the sender and each receiver, is bounded as

$$\sum_{B_i \in \mathcal{T}} R_{E AB_i}^E + R_{K AB_i}^K \leq g(N_S(1 + \eta_\mathcal{T} - \eta_{\overline{\mathcal{T}}})/2) - g(N_S(1 - \eta_\mathcal{T} - \eta_{\overline{\mathcal{T}}})/2). \quad (2.179)$$

for all non-empty $\mathcal{T} \subseteq \mathcal{B}$.

**Proof.** For the choices discussed above, it simply suffices to calculate various relaxations of the multipartite squashed entanglements when the thermal state of mean photon number $N_S$ is input. As mentioned above, the same reasoning as in Remark 2, along with the representation of multipartite squashed entanglement in Lemma 11 and the relaxation of it described above, allow us to conclude that, for a given input mean photon number constraint $N_S \geq 0$, a thermal state of that photon number is optimal. By applying Theorem 12 and Remark 6, the following bounds apply

$$\sum_{B_i \in \mathcal{T}} R_{E AB_i}^E + R_{K AB_i}^K \leq E_{sq}(R\overline{\mathcal{T}}; \mathcal{T}), \quad (2.180)$$

$$\leq \frac{1}{2}[H(\mathcal{T}|E_1) + H(\mathcal{T}|E_2)] \quad (2.181)$$
where the second inequality follows from relaxing the squashing isometry to be a 50-50 beamsplitter as discussed above, with output systems $E_1$ and $E_2$, and then it follows that the thermal state of mean photon number $N_S$ into the pure-loss bosonic broadcast channel is optimal. Now employing entropy identities, we find that

$$
\frac{1}{2}[H(T|E_1) + H(T|E_2)] = \frac{1}{2}[H(TE_1) - H(E_1) + H(TE_2) - H(E_2)]
$$

$$
= H(TE_1) - H(E_1). \quad (2.182)
$$

The last line in (2.183) combines terms that are equal, due to the fact that the transmissivity of the squashing channel is balanced (coming from a 50-50 beamsplitter). We then use the $g$ function to represent the entropies of the thermal states resulting from the use of the quantum broadcast channel, giving that

$$
H(TE_1) - H(E_1) = g(N_S(\eta_T + \eta_E/2)) - g(N_S\eta_E/2)
$$

$$
= g(N_S(\eta_T + (1 - \eta_T - \eta_T))/2) - g(N_S(1 - \eta_T - \eta_T)/2) \quad (2.185)
$$

$$
= g(N_S(1 + \eta_T - \eta_T)/2) - g(N_S(1 - \eta_T - \eta_T)/2). \quad (2.186)
$$

This concludes the proof. ■

We conclude this section with a few brief remarks. In the limit of large photon number $N_S \rightarrow \infty$, the bound in Theorem 13 reduces to

$$
\sum_{B_i \in \mathcal{T}} R_{AB_i}^E + R_{AB_i}^K \leq \log_2 \left( \frac{1 + \eta_T - \eta_T}{1 - \eta_T - \eta_T} \right), \quad (2.187)
$$

which is not as tight as the result of Ref. [16], in which the upper bound was found to be $\log_2 \left( \frac{1 - \eta_T}{1 - \eta_T - \eta_T} \right)$. However, for low photon number, the energy-constrained bounds of Theorem 13 can be tighter.

Let us look at some particular examples of the bound. For the case of two receivers, Bob and
Charlie, the set $\mathcal{T}$ can take a few different values. If $\mathcal{T} = \{B, C\}$ then $\overline{\mathcal{T}} = 0$ and

$$R_{AB}^E + R_{AB}^K + R_{AC}^E + R_{AC}^K + R_{ABC}^E + R_{ABC}^K \leq \log_2 \left( \frac{1 + \eta_B + \eta_C}{1 - \eta_B - \eta_C} \right)$$  \hspace{1cm} (2.188)

which has been discussed already in Ref. [13]. For the case $\mathcal{T} = C$, then $\overline{\mathcal{T}} = B$, and so

$$R_{AC}^E + R_{AC}^K \leq \log_2 \left( \frac{1 + \eta_C - \eta_B}{1 - \eta_B - \eta_C} \right).$$  \hspace{1cm} (2.189)

Other permutations of the sets $\mathcal{T}$ and $\overline{\mathcal{T}}$ can naturally be worked out for scenarios involving any number of receivers.
3 Broadcast Amplitude Damping Channels and Capacities

3.1 Introduction

Many common processes such as spontaneous emission may be modeled as the action of an amplitude damping channel under which an excited two-level system decays with some probability \[53, 54\]. The action of an amplitude damping channel on an excited state results in a mixed state. By using the resultant state as the input to a broadcast channel, each receiver is party to the broadcast amplitude damping channel; each output is of the form of that from an amplitude damping channel with decay probability adjusted by the transmission probability of the path to that particular receiver.

3.2 Amplitude Damping Channel

An amplitude damping channel \(D_{A\rightarrow B}\) with damping parameter \(\gamma \in [0, 1]\) is a completely positive, trace preserving map with Kraus operators

\[
A_0 = \sqrt{\gamma} |0\rangle_B \langle 1|_A \quad (3.1)
\]
\[
A_1 = |0\rangle_B \langle 0|_A + \sqrt{1-\gamma} |1\rangle_B \langle 1|_A. \quad (3.2)
\]

Its action on some state \(\zeta_A\) is given by the Kraus operators as

\[
D_{A\rightarrow B}(\zeta_A) = A_0 \zeta_A A_0^\dagger + A_1 \zeta_A A_1^\dagger. \quad (3.3)
\]

Under the action of an amplitude damping channel, an excited state input \(|\xi\rangle \langle \xi|_A = |1\rangle \langle 1|_A\) goes to the mixed state

\[
D(|\xi\rangle \langle \xi|_A) = \gamma |0\rangle \langle 0|_B + (1-\gamma) |1\rangle \langle 1|_B. \quad (3.4)
\]

This process can be better understood through a unitary extension \(U_D\) of the channel, which reveals that, with some probability, the decay process transmits the excitation to the environment rather
than to the receiver. That is, for input state vector $|\xi\rangle_{AE_{in}} = |10\rangle_{AE_{in}}$,

$$U^D|\xi\rangle_{AE_{in}} = \sqrt{\gamma}|01\rangle_{BE} + \sqrt{1-\gamma}|10\rangle_{BE}. \quad (3.5)$$

Upon tracing over the environment, the output state of the above extended amplitude damping channel has the form

$$\sigma_B = \text{Tr}_E\{U^D(\xi)\} = p_0|0\rangle_B + p_1|1\rangle_B, \quad (3.6)$$

where $p_1$ is the probability of measuring a photon in system $B$, and $p_0 = 1 - p_1$ is the probability of not measuring a photon [53, 54]. For an excited state input, the probability $p_1$ is exactly the complement of the decay parameter $\gamma$.

When the excited state $|1\rangle_B$ is input, the output state of an amplitude damping channel can be represented as a Bernoulli trial; its entropy is given by the binary entropy function of the detection probability (or the decay parameter from the symmetry of the binary entropy function) [53, 54]:

$$H(B) = h_2(p_1) = -p_1 \log p_1 - (1 - p_1) \log(1 - p_1) \quad = h_2(p_0) = -p_0 \log p_0 - (1 - p_0) \log(1 - p_0). \quad (3.7)$$

We can also use a superposition state $|\chi\rangle_{AE_{in}} = a|00\rangle_{AE_{in}} + b|10\rangle_{AE_{in}}$ (with $|a|^2 + |b|^2 = 1$) as input to the amplitude damping channel:

$$U^D|\chi\rangle_{AE_{in}} = a|00\rangle_{BE} + b \left(\sqrt{\gamma}|01\rangle_{BE} + \sqrt{1-\gamma}|10\rangle_{BE}\right). \quad (3.8)$$

A computational basis projection on the receiver’s state takes the form of (3.6),

$$\rho_B = \text{Tr}_E\{U^D(\chi)\}$$

$$= (|a|^2 + |b|^2\gamma)|0\rangle_B + |b|^2(1-\gamma)|1\rangle_B + \sqrt{1-\gamma}(ab^*|0\rangle_B + a^*b|1\rangle_B), \quad (3.9)$$

$$\varrho_B \equiv \sum_{i=0,1} |i\rangle_B \rho_B |i\rangle_B = p_0|0\rangle_B + p_1|1\rangle_B, \quad (3.10)$$
but the probabilities no longer directly correspond to the decay parameter:

\[ p_0 = |a|^2 + |b|^2 \gamma, \]  
\[ p_1 = |b|^2(1 - \gamma). \] (3.11) (3.12)

### 3.3 Broadcast Amplitude Damping Channel

We begin by considering a general bosonic broadcast channel [123] which produces outputs to \( m \) receivers from the input of a single sender. We follow the methods of Refs. [16, 17], exploiting the decomposition given in Ref. [124] to cast the broadcast channel as a linear optical network. Taking all the environmental inputs to the channel to be vacuum states \( |0\rangle \), we decompose the quantum broadcast channel into a line of sequential pure-loss channels. It was shown in Ref. [125] that the amplitude damping channel arises from restricting the input space of a pure-loss channel to \( \{|0\rangle, |1\rangle\} \). So, if we take our input state to be

\[ \chi_A = (1 - p)|0\rangle\langle 0|_A + \kappa|0\rangle\langle 1|_A + \kappa^*|1\rangle\langle 0|_A + p|1\rangle\langle 1|_A \] (3.13)

for \( p \in (0, 1] \) and \( |\kappa|^2 \leq 1 \), then the broadcast channel acts as the broadcast amplitude damping channel \( J_{A \rightarrow B_1 \ldots B_m} \). \( J_{A \rightarrow B_1 \ldots B_m} \) has a receiver dependent transmission probability

\[ p_{B_i} = \eta_{B_i} p \] (3.14)

where \( \eta_{B_i} \) is the transmissivity of \( L_{A \rightarrow B_1 \ldots B_m} \) to \( B_i \) and \( i \in \{1, \ldots, m\} \). So, the entropy of the output of \( J_{A \rightarrow B_1 \ldots B_m} \) to receiver \( B_i \) when the excited state \( |1\rangle\langle 1|_A \) is input is

\[ H(B_i)_\rho = h_2(p_{B_i}) = -p_{B_i} \log p_{B_i} - (1 - p_{B_i}) \log(1 - p_{B_i}). \] (3.15)

#### 3.3.1 Arbitrarity of Receiver Order

The quantum broadcast channel \( L_{A \rightarrow B_1 \ldots B_m} \) can be deconstructed according to the method described above, and two equivalent examples of such a deconstruction \( L^a \) and \( L^b \) are shown in Fig-
Figure 3.1. Equivalent Decompositions of Quantum Broadcast Channel $\mathcal{L}$. That is, the transmissivity to each receiver Bob$_i$ is identical in either case.

The transmissivities for the constituent pure-loss channels of $\mathcal{L}^\alpha$ in Figure 3.1a are denoted $\eta^\alpha_1, \eta^\alpha_2, \ldots, \eta^\alpha_m$ with the following condition on each transmissivity: $0 \leq \eta^\alpha_i \leq 1$ for $i \in \{1, \ldots, m\}$. Importantly, the total transmissivity to any single receiver is unchanged by the particular decomposition:

$$\eta_{E^\alpha} = \eta_{B^\alpha_i}.$$  \hspace{1cm} (3.16)

The total transmissivity to each receiver is given by the product of transmissivities and reflectivities of the pure-loss channels along the path to that receiver such that the sum of total transmissivities for all receivers is equal to one:

$$\eta_{E^\alpha} + \sum_{i=1}^{m} \eta_{B^\alpha_i} = 1.$$  \hspace{1cm} (3.17)

The broadcast channel $\mathcal{L}^\beta$ shown in Figure 3.1b gives an alternative order to the receivers and is composed of pure-loss channels with transmissivities $\eta^\beta_1, \eta^\beta_2, \ldots, \eta^\beta_m$ and a similar condition on the transmissivities: $0 \leq \eta^\alpha_i \leq 1$ for $i \in \{1, \ldots, m\}$. Again, the sum of total transmissivities for all receivers is equal to one (as we expect, since each receiver’s total transmissivity is unchanged):

$$\eta_{E^\beta} + \sum_{i=1}^{m} \eta_{B^\beta_i} = 1.$$  \hspace{1cm} (3.18)

Expressions for the total transmissivities to receivers of the two broadcast channels are given in Table 3.1. The two total transmissivities on each row of Table 3.1 are equal to one another, so we can treat the collection as a system of linear equations solving for the constituent transmissivities of $\mathcal{L}^\alpha$ in terms of those for $\mathcal{L}^\beta$.

For example, we may collect the receivers $B_2$ through $B_m$ for each channel into a single party
Table 3.1. Equivalent Total Transmissivities in m-Receiver Case

<table>
<thead>
<tr>
<th>Broadcast Channel $\mathcal{L}^\alpha$</th>
<th>Broadcast Channel $\mathcal{L}^\beta$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\eta_{E^\alpha} = 1 - \eta_1^\alpha$</td>
<td>$\eta_{E^\beta} = \prod_{i=1}^m \eta_i^\beta$</td>
</tr>
<tr>
<td>$\eta_{B_1^\alpha} = \eta_1^\alpha (1 - \eta_2^\alpha)$</td>
<td>$\eta_{B_1^\beta} = 1 - \eta_1^\beta$</td>
</tr>
<tr>
<td>$\eta_{B_2^\alpha} = \eta_1^\alpha \eta_2^\alpha (1 - \eta_3^\alpha)$</td>
<td>$\eta_{B_2^\beta} = \eta_1^\beta (1 - \eta_2^\beta)$</td>
</tr>
<tr>
<td>$\ldots$</td>
<td>$\ldots$</td>
</tr>
<tr>
<td>$\eta_{B_j^\alpha} = \left( \prod_{i=1}^j \eta_i^\alpha \right) (1 - \eta_{(j+1)}^\alpha)$</td>
<td>$\eta_{B_j^\beta} = \left( \prod_{i=2}^j \eta_{(i-1)}^\beta \right) (1 - \eta_j^\beta)$</td>
</tr>
<tr>
<td>$\ldots$</td>
<td>$\ldots$</td>
</tr>
<tr>
<td>$\eta_{B_m^\alpha} = \prod_{i=1}^m \eta_i^\alpha$</td>
<td>$\eta_{B_m^\beta} = \left( \prod_{i=1}^{m-1} \eta_i^\beta \right) (1 - \eta_m^\beta)$</td>
</tr>
</tbody>
</table>

Figure 3.2. Receivers Gathered. The transmissivity to each receiver is the same in either case.

Table 3.2. Equivalent Total Transmissivities in Two-Receiver Case

<table>
<thead>
<tr>
<th>Broadcast Channel $\mathcal{L}^\alpha$</th>
<th>Broadcast Channel $\mathcal{L}^\beta$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\eta_{E^\alpha} = 1 - \eta_1^\alpha$</td>
<td>$\eta_{E^\beta} = \eta_1^\beta \eta_2^\beta$</td>
</tr>
<tr>
<td>$\eta_{B_1^\alpha} = \eta_1^\alpha (1 - \eta_2^\alpha)$</td>
<td>$\eta_{B_1^\beta} = 1 - \eta_1^\beta$</td>
</tr>
<tr>
<td>$\eta_{B_2^\alpha} = \eta_1^\alpha \eta_2^\alpha$</td>
<td>$\eta_{B_2^\beta} = \eta_1^\beta (1 - \eta_2^\beta)$</td>
</tr>
</tbody>
</table>
The resulting channels are pictured in Figure 3.2 and the total transmissivities are given in Table 3.2.

Then the transmissivities for the constituent channels of $L^\alpha$ are

$$\eta_1^\alpha = 1 - \eta_1^\beta \eta_2^\beta$$

$$\eta_2^\alpha = \frac{\eta_1^\beta - \eta_1^\beta \eta_2^\beta}{1 - \eta_1^\beta \eta_2^\beta}$$  (3.20)

These transmissivities will appropriately fall in the range $0 \leq \eta_i^\alpha \leq 1$ for $i \in \{1, \ldots, m\}$ for any arbitrary ordering of receivers as long as the transmissivities of the analogous channel are also in the appropriate range $0 \leq \eta_i^\beta \leq 1$ for $i \in \{1, \ldots, m\}$.

### 3.3.2 The Communication Task

In the following LOCC-assisted communication protocol, the sender Alice uses a quantum broadcast amplitude damping channel $J_{A \to B_1 \cdots B_m}$ to establish a combination of secret-key states and entanglement with the $m$ receivers Bob$_1$, \ldots, Bob$_m$ in the presence of an adversary Eve.

Let $B = \{B_1, \ldots, B_m\}$ be the set of trusted receivers Bob$_1$, \ldots, Bob$_m$ with total transmissivity $\eta_B = \sum_{B_i \in B} \eta_{B_i}$, let $T \subseteq B$ be a subset of trusted receivers with transmissivity $\eta_T = \sum_{B_i \in T} \eta_{B_i}$, and let $T = B - T$ be the complement to $T$ with power transmissivity $\eta_T = \eta_B - \eta_T$. Eve is considered to receive all other signal with transmissivity $\eta_E = 1 - \eta_B = 1 - \eta_T - \eta_T$.

The target state of the communication task is

$$\Psi_{R_1 \cdots R_m B_1 \cdots B_m} = \Phi_{R_1 B_1} \otimes \gamma_{R_1 B_1} \otimes \Phi_{R_2 B_2} \otimes \gamma_{R_2 B_2} \otimes \cdots \otimes \Phi_{R_m B_m} \otimes \gamma_{R_m B_m}$$  (3.21)

where $\Phi_{R_i B_i}$ and $\gamma_{R_i B_i}$ are maximally entangled states and private states, respectively. Alice begins by preparing at least $n$ quantum states and then uses the broadcast channel $n$ times to act on some of these systems (transmit them to the receivers). Between channel uses, Alice and the Bobs may conduct unlimited local operations and classical communications (LOCC). After the $n^{th}$ broadcast, a final round of LOCC is conducted to produce the state $\Omega_{R_1 \cdots R_m B_1 \cdots B_m}$ which is $\varepsilon$-close to the target state where $\varepsilon \in (0, 1)$:

$$F(\Omega_{R_1 \cdots R_m B_1 \cdots B_m}, \Psi_{R_1 \cdots R_m B_1 \cdots B_m}) \geq 1 - \varepsilon.$$  (3.22)

In this protocol, Alice and the $i^{th}$ receiver Bob$_i$ establish entanglement at a rate of $E_{AB_i}$ bits
per channel use and establish secret key at a rate of $K_{AB}$ private bits per channel use. A rate $(E_{AB_1}, \ldots, E_{AB_m}, K_{AB_1}, \ldots, K_{AB_m})$ is achievable if for a sufficiently large number $n$ of channel uses there exists an $(n, E_{AB_1}, \ldots, E_{AB_m}, K_{AB_1}, \ldots, K_{AB_m}, \varepsilon)$ protocol as described above. The capacity region of the channel corresponds to the region of all achievable rates.

**Theorem 14** Given a broadcast amplitude damping channel $\mathcal{J}_{A \to B_1 \ldots B_m}$, an achievable rate region for entanglement and secret key generation is given by the union of the following regions over $p \in [0, 1]$:

$$\sum_{B_i \in \mathcal{T}} E_{AB_i} + K_{AB_i} \leq h_2([1 - \eta_{\mathcal{T}}]p) - h_2([1 - \eta_{\mathcal{B}}]p)$$

(3.23)

for all non-empty $\mathcal{T} \subseteq \mathcal{B}$, where $\eta_{\mathcal{B}} = \sum_{i=1}^{m} \eta_{B_i}$ and $\eta_{\mathcal{T}} = \sum_{B_i \in \mathcal{T}} \eta_{B_i}$.

**Proof.** Alice may prepare many copies of an input state $\sqrt{1-p}|00\rangle_{RA} + \sqrt{p}|11\rangle_{RA}$ then use the broadcast amplitude damping channel $\mathcal{J}_{A \to B_1 \ldots B_m}$ $n$ times with unrestricted LOCC between her and the Bobs to produce some state $\Xi_{R\mathcal{B}_1 \ldots \mathcal{B}_m}$.

Announced in Ref. [126] and expanded upon in Ref. [127], state merging gives the conditional entropy $H(R|B)_\rho$ as the optimal cost in entangled qubits to transfer Alice’s part of a shared state $\rho_{RB}$ to Bob using LOCC. For a negative cost, entangled qubits are distilled at a rate of $-H(R|B)_\rho$.

Considering the state-merging protocol as employed in Ref. [17], in which the receivers sequentially send their shares of the state to Alice, and applying it to the communication task from above with output state $\Xi_{RB_1 \ldots B_m}$, the distillable entanglement between Alice and a subset of receivers $\mathcal{T} \subseteq \mathcal{B}$ is achievable up to

$$\sum_{B_i \in \mathcal{T}} E_{AB_i} \leq -H(\mathcal{T}|R\mathcal{T})_{\Xi}.$$ (3.24)

Because some number of entangled bits can be used to create an equal number of secret key bits, we can rewrite (3.24) as

$$\sum_{B_i \in \mathcal{T}} E_{AB_i} + K_{AB_i} \leq -H(\mathcal{T}|R\mathcal{T})_{\Xi}.$$ (3.25)
Using the duality of conditional entropy in (1.35), we have the following:

\[-H(T|R\mathcal{T})_\Xi = H(R\mathcal{T})_\Xi - H(TR\mathcal{T})_\Xi\]  \hspace{1cm} (3.26)
\[= H(TE)_\Xi - H(E)_\Xi\]  \hspace{1cm} (3.27)
\[= h_2([1 - \eta_T]p) - h_2([1 - \eta_B]).\]  \hspace{1cm} (3.28)

This concludes the proof. \[\blacksquare\]

**Theorem 15**  Given a broadcast amplitude damping channel \(\mathcal{J}_{A\rightarrow B_1...B_m}\) with \(\eta_B \in [0, 1]\), an outer bound on its achievable rate region for entanglement and secret key generation is given by the union of the following regions over \(p \in [0, 1]\):

\[
\sum_{B_i \in \mathcal{T}} E_{AB_i} + K_{AB_i} \leq h_2(p(1 + \eta_T - \eta_T)/2) - h_2(p(1 - \eta_T - \eta_T)/2) \]  \hspace{1cm} (3.29)

for all non-empty \(\mathcal{T} \subseteq \mathcal{B}\), where \(\eta_B = \sum_{i=1}^{m} \eta_{B_i}\) and \(\eta_T = \sum_{B_i \in \mathcal{T}} \eta_{B_i}\).

**Proof.** As in Theorem 13, we can apply the methods used in Theorem 12 and Remark 6 in Section 2.6. We also exploit the \(Z\)-covariance of the broadcast amplitude damping channel (similar to the phase covariance in the proof of Theorem 5) to see that the optimal input takes the form \(\phi_A = (1 - p)\lvert 0\rangle\langle 0\rvert_A + p\lvert 1\rangle\langle 1\rvert_A\). Using these and the symmetry of a 50:50 amplitude damping squashing channel we bound the capacity region with a relaxation of the squashed entanglement:

\[
\sum_{B_i \in \mathcal{T}} E_{AB_i} + K_{AB_i} \leq E_{\text{sq}}(R\mathcal{T}; \mathcal{T}, \mathcal{J}(\phi)) \]  \hspace{1cm} (3.30)
\[
\leq H(T|E_{\mathcal{S}})_{\mathcal{J}(\phi)} \]  \hspace{1cm} (3.31)
\[
= H(TE_{\mathcal{S}})_{\mathcal{J}(\phi)} - H(E_{\mathcal{S}})_{\mathcal{J}(\phi)}. \]  \hspace{1cm} (3.32)

Because each output is unitarily equivalent to the output of an amplitude damping channel, these entropies are simply binary entropy functions:

\[H(TE_{\mathcal{S}})_{\mathcal{J}(\phi)} = h_2(p_{TE_{\mathcal{S}}}), \quad H(E_{\mathcal{S}})_{\mathcal{J}(\phi)} = h_2(p_{E_{\mathcal{S}}})\]  \hspace{1cm} (3.33)

We rewrite the transmission probabilities \(p_{TE_{\mathcal{S}}} \) and \(p_{E_{\mathcal{S}}} \) using (3.14) then substitute transmissivities
(recall that \( \eta_T + \eta_T + \eta_E = 1 \)) so that

\[
\begin{aligned}
  h_2(p_{TEs}) &= h_2(p(\eta_T + \eta_E/2)) \\
  &= h_2(p(1 + \eta_T - \eta_T)/2)
\end{aligned}
\]  

(3.34)

\[
\begin{aligned}
  h_2(p_{Es}) &= h_2(p\eta_E/2)) \\
  &= h_2(p(1 - \eta_T - \eta_T)/2).
\end{aligned}
\]  

(3.35)

Combining (3.34) and (3.35) with (3.33) and (3.32), we arrive at (3.29).

Equation (3.23) in Theorem 14 provides an inner bound to the achievable rate region of the broadcast amplitude damping channel \( \mathcal{J}_{\mathcal{A} \rightarrow \mathcal{B}_1 \cdots \mathcal{B}_m} \) while (3.29) in Theorem 15 provides an outer bound to the achievable rate region. It is interesting to compare the outer bound of the capacity region we present in Theorem 15 with that in Theorem 13 of Section 2.6. Specifically, we replace the \( g \) function with the \( h_2 \) function and replace photon number \( N_S \) with \( p \) to go from (2.179) to (3.29).
4 Conclusion

The fundamental limits of a channel for secret-key agreement and LOCC-assisted quantum communication give an important benchmark against which we can measure the implementation of quantum technologies. In Chapter 2 we have formally defined these communication tasks, and we have provided upper bounds on the corresponding capacities. We looked more closely at single-mode, phase-insensitive Gaussian channels, and in this closer look we showed that a thermal state input optimizes a relaxation of the energy-constrained squashed entanglement of the channel. Our variation on a method from Ref. [14] allowed for improved upper bounds on the energy-constrained secret-key-agreement capacity of a bosonic thermal channel. These improved bounds are particularly well behaved in that they tend smoothly to zero in the limit as the channel becomes entanglement breaking. We then moved to a many-receiver setting to extend the definitions of the communication task and the results of our analysis similarly to Ref. [13]. We proved that the multipartite squashed entanglement bounds the capacity regions for multipartite energy-constrained secret-key-agreement and LOCC-assisted quantum communication.

Because the squashed entanglement bounds are independent of the particular examples we investigate, we expect the bounds to apply to other systems not specifically addressed here. We believe the communication task and corresponding squashed entanglement bounds can be generalized to quantum network efforts such as those in Refs. [18, 22, 90]. An important technical question is whether the energy-constrained squashed entanglement bounds could apply when the LOCC channels involved are not denumerably decomposable, and answering this question is directly related to the question discussed in Ref. [65, Remark 1]. We also are interested to investigate physical systems outside of the bosonic setting to apply our formalism.

In Chapter 3 we define a broadcast amplitude damping channel with no preference to receiver order and with potentially receiver-dependent damping parameters. We discuss the channel in the context of LOCC-assisted communication tasks and provide bounds on its capacity region for QKD. Interestingly, the discussion of the broadcast amplitude damping channel is limited to an input of at most one photon which technically places the bounds in the energy-constrained setting.
Chapter 3 serves as a step toward generalizing somewhat well understood quantum channels to the multipartite regime (multiple access and broadcast channels) in order to further the goal of quantum network implementation. We expect the capacity bound to apply in a general way to any physical system that meets our definition of a broadcast amplitude damping channel.

Quantum information studies are quickly changing the landscape of modern technologies. Purpose-built quantum simulators which use quantum annealing to solve optimization problems are available for your institution [49], and classical cryptographic efforts are working to specifically address the weaknesses of classical encryption to quantum attack [128]. By bounding capacities of quantum channels, we help to define the fundamental limits of quantum-assisted communication and networking, and we move toward enabling unprecedented quantum interconnection.
References


A. S. Holevo, Quantum Systems, Channels, Information. de Gruyter Studies in Mathematical Physics (Book 16), de Gruyter, November 2012.


E. Chitambar, D. Leung, L. Mančinska, M. Ozols, and A. Winter, “Everything you always wanted to know about LOCC (but were afraid to ask),” Communications in Mathematical Physics, vol. 328, pp. 303–326, May 2014. arXiv:1210.4583.


Appendix A  Thermal State Optimality

In this section we present an alternate argument that squashed entanglement is maximized by a thermal state input. Compare to the proof of Theorem 5 in 2.4.

**Theorem 16**  Let \( N_{A \rightarrow B} \) be a pure-loss channel, \( \theta_{RA} \) be a two-mode squeezed vacuum state, and \( \rho_{RA} \) be an arbitrary state with the property that \( \text{Tr}\{G_\omega\} = \text{Tr}\{G_\tau\} \) where \( G \) is a Gibbs observable (Definition 2), \( \tau_{RB} \) is the state resulting from inputting \( \theta_{RA} \), and \( \omega_{RB} \) results from the input of arbitrary state \( \rho_{RA} \). Then the squashed entanglement of the channel \( N_{A \rightarrow B} \) is maximized when \( \theta_{RA} \) is used as the input state. That is,

\[
E_{sq}(\theta, N) = E_{sq}(R; B)_\tau \geq E_{sq}(R; B)_\omega = E_{sq}(\rho, N). \tag{A.1}
\]

**Proof.** Consider Setup 1 depicted in Figure A.1, an experiment of two beam splitters which we label by bolding their transmissivities \( \eta_1 \) and \( \eta_2 \) with \( \eta_1, \eta_2 \in [0, 1] \). Consider also, two pairs of pure state outputs corresponding to using either \( \theta_{RA} \) or \( \rho_{RA} \) as input to Setup 1:

\[
\omega_{RBE} = \eta_1(\rho_A) \tag{A.2}
\]
\[
\omega_{RBE'}F = \eta_2(\omega_{RBE}) = (\eta_2 \circ \eta_1)(\rho_A) \tag{A.3}
\]
and
\[
\tau_{RBE} = \eta_1(\theta_A) \tag{A.5}
\]
\[
\tau_{RBE'}F = \eta_2(\tau_{RBE}) = (\eta_2 \circ \eta_1)(\theta_A). \tag{A.6}
\]

\( \theta_{RA} \) is a two-mode squeezed vacuum state so that the marginal \( \theta_A \) is a thermal state with partition function of the form

\[
\theta_A = e^{-\beta G} / \text{Tr}\{e^{-\beta G}\} \tag{A.7}
\]

where \( G \) is a Gibbs observable and \( \beta \) is a real number. \( \rho_A \) is the marginal of arbitrary state \( \rho_{RA} \).
Figure A.1. Setup 1. The $A$ share of a state in bipartite system $RA$ is used as input to a two beam splitter experiment. The second input to each beam splitter is a vacuum state.

with the same average photon number as $\theta_A$.

$$N_A^1 = \text{Tr}\{\rho_A N\} = \text{Tr}\{\theta_A N\}$$ \hspace{1cm} (A.8)

It is straightforward to use the transmissivities of the beam splitters to find the expected photon number for each system in Setup 1.

$$N_B^1 = \eta_1 N_A^1 = \text{Tr}\{\omega_B N\} = \text{Tr}\{\tau_B N\}$$ \hspace{1cm} (A.9)

$$N_E^1 = (1 - \eta_1) N_A^1 = \text{Tr}\{\omega_E N\} = \text{Tr}\{\tau_E N\}$$ \hspace{1cm} (A.10)

$$N_{E'}^1 = \eta_2 (1 - \eta_1) N_A^1 = \text{Tr}\{\omega_{E'} N\} = \text{Tr}\{\tau_{E'} N\}$$ \hspace{1cm} (A.11)

$$N_F^1 = (1 - \eta_2)(1 - \eta_1) N_A^1 = \text{Tr}\{\omega_F N\} = \text{Tr}\{\tau_F N\}$$ \hspace{1cm} (A.12)

If the experiment in Setup 1 is performed using $\theta_{RA}$ as the input the squashed entanglement will be

$$E_{sq}(R; B)_\tau = \frac{1}{2} \inf_{E \rightarrow E'} [H(B|E')_\tau + H(B|F)_\tau],$$ \hspace{1cm} (A.13)
and similarly, the squashed entanglement from inputting $\rho_{RA}$ will be

$$E_{sq}(R; B)_\omega = \frac{1}{2} \inf_{\nu_{E \to E'F}} \left[ H(B|E')_\omega + H(B|F)_\omega \right].$$  \hspace{1cm} (A.14)

Now consider Setup 2, the two beam splitter experiment depicted in Figure A.2. Two different pairs of pure states result from using the same two input states $\theta_{RA}$ and $\rho_{RA}$.

$$\sigma_{RB'F} = \eta_3(\rho_A)$$  \hspace{1cm} (A.15)

$$\sigma_{RCE'F} = \eta_4(\sigma_{RB'F}) = (\eta_4 \circ \eta_3)(\rho_A)$$  \hspace{1cm} (A.16)

and

$$\vartheta_{RB'F} = \eta_3(\theta_A)$$  \hspace{1cm} (A.17)

$$\vartheta_{RCE'F} = \eta_4(\vartheta_{RB'F}) = (\eta_4 \circ \eta_3)(\theta_A).$$  \hspace{1cm} (A.18)

It is once again straightforward to use the transmissivities to find the expected photon numbers of each system in Setup 2. We also note that by using the same input states the starting photon
number is identical in Setups 1 & 2.

\[ N^2_A = \text{Tr}\{\rho_A N\} = \text{Tr}\{\theta_A N\} = N^1_A \quad (A.19) \]

\[ N^2_B = \eta_3 N^2_A = \text{Tr}\{\sigma_B' N\} = \text{Tr}\{\vartheta_B' N\} \quad (A.20) \]

\[ N^2_E = \eta_4 \eta_3 N^2_A = \text{Tr}\{\sigma_E' N\} = \text{Tr}\{\vartheta_E' N\} \quad (A.21) \]

\[ N^2_F = (1 - \eta_3) N^2_A = \text{Tr}\{\sigma_F N\} = \text{Tr}\{\vartheta_F N\} \quad (A.22) \]

\[ N^2_C = (1 - \eta_4) \eta_3 N^2_A = \text{Tr}\{\sigma_C N\} = \text{Tr}\{\vartheta_C N\} \quad (A.23) \]

In order to establish Setup 2 as an analog of Setup 1, we define the transmissivities to match photon numbers in the \( E' \) and \( F \) systems between the setups.

\[ N^1_{E'} = \eta_2 (1 - \eta_1) N^1_A = \eta_4 \eta_3 N^2_A = N^2_{E'} \quad (A.24) \]

\[ N^1_F = (1 - \eta_2) (1 - \eta_1) N^1_A = (1 - \eta_3) N^2_A = N^2_F \quad (A.25) \]

so

\[ \eta_3 = 1 - (1 - \eta_1) (1 - \eta_2) = \eta_1 + \eta_2 (1 - \eta_1) \quad (A.26) \]

\[ \eta_4 = \frac{\eta_2 (1 - \eta_1)}{\eta_1 + \eta_2 (1 - \eta_1)} \quad (A.27) \]

(A.26) and (A.27) satisfy \( \eta_3, \eta_4 \in [0, 1] \) for \( \eta_1, \eta_2 \in [0, 1] \). Since the photon numbers have been matched we can see that

\[ \text{Tr}\{G\sigma\} = \text{Tr}\{G\vartheta\}. \quad (A.28) \]

To further the analogy between Setups 1 & 2 we examine entropies of select groups of systems.

\[ H(BE')_{\omega,\tau} = H(RF)_{\omega,\tau} = H(RF)_{\sigma,\vartheta} = H(B')_{\sigma,\vartheta} \quad (A.29) \]

\[ H(E')_{\omega,\tau} = H(E')_{\sigma,\vartheta} \quad (A.30) \]
The first and third equalities above are from the duality of entropy (1.35), while the second and fourth equalities come in consequence of using the same input states and matching the transmissivities \( A.26 \) \( A.27 \).

Using relative entropy, we examine the impact of using either \( \theta_{RA} \) or \( \rho_{RA} \) as input in Setup 2. The monotonicity of relative entropy with respect to channel use, in this case the beam splitter \( \eta_4 \), gives the following inequality:

\[
D(\sigma_{B'} \| \vartheta_{B'}) \geq D(\sigma_{E'} \| \vartheta_{E'}) \quad \text{(A.31)}
\]

Expand this inequality using the definition of relative entropy then regroup the terms by system.

\[
\text{Tr}\{\sigma_{B'} \log \sigma_{B'}\} - \text{Tr}\{\sigma_{B'} \log \vartheta_{B'}\} \geq \text{Tr}\{\sigma_{E'} \log \sigma_{E'}\} - \text{Tr}\{\sigma_{E'} \log \vartheta_{E'}\} \quad \text{(A.32)}
\]

\[
-H(B')_\sigma - \text{Tr}\{\sigma_{B'} \log \vartheta_{B'}\} \geq -H(E')_\sigma - \text{Tr}\{\sigma_{E'} \log \vartheta_{E'}\} \quad \text{(A.33)}
\]

\[
-\left[\text{Tr}\{\sigma_{B'} \log \vartheta_{B'}\} - \text{Tr}\{\sigma_{E'} \log \vartheta_{E'}\}\right] \geq H(B')_\sigma - H(E')_\sigma \quad \text{(A.34)}
\]

Next, we observe that \( \vartheta_{B'} \) is a thermal state, so the exponential form gives us

\[
\text{Tr}\{\sigma_{B'} \log \vartheta_{B'}\} = \text{Tr}\left\{\sigma_{B'} \log \frac{e^{-\beta G_{B'}}}{\text{Tr}\{e^{-\beta G_{B'}}\}}\right\}
\]

\[
= \text{Tr}\{\sigma_{B'} \log e^{-\beta G_{B'}}\} - \text{Tr}\{\sigma_{B'} \log \text{Tr}\{e^{-\beta G_{B'}}\}\}
\]

\[
= \text{Tr}\{\sigma_{B'}(-\beta G_{B'})\} - \log \text{Tr}\{e^{-\beta G_{B'}}\} \text{Tr}\{\sigma_{B'}\}
\]

\[
= -\beta \text{Tr}\{\sigma_{B'} G_{B'}\} - \log \text{Tr}\{e^{-\beta G_{B'}}\}, \quad \text{(A.35)}
\]

and similarly

\[
\text{Tr}\{\vartheta_{B'} \log \vartheta_{B'}\} = -\beta \text{Tr}\{\vartheta_{B'} G_{B'}\} - \log \text{Tr}\{e^{-\beta G_{B'}}\}. \quad \text{(A.36)}
\]

Because \( \text{Tr}\{G\vartheta\} = \text{Tr}\{G\vartheta\} \) \( A.28 \), we see that

\[
\text{Tr}\{\sigma_{B'} \log \vartheta_{B'}\} = \text{Tr}\{\vartheta_{B'} \log \vartheta_{B'}\}. \quad \text{(A.37)}
\]
This is a critical step. Applying (A.37) to (A.34) yields

\[ H(B')_\vartheta - H(E')_\vartheta \geq H(B')_\sigma - H(E')_\sigma. \quad (A.38) \]

The usefulness of the analogous beam splitter setups is now apparent when we use (A.29) and (A.30) with the definition of conditional entropy to rewrite (A.38) as

\[ H(BE')_\tau - H(E')_\tau \geq H(BE')_\omega - H(E')_\omega \quad (A.39) \]
\[ H(B|E')_\tau \geq H(B|E')_\omega. \quad (A.40) \]

By using the above logic on states \( \omega_{BF} \) and \( \tau_{BF} \) along with their counterparts \( \sigma_{BF} \) and \( \vartheta_{BF} \) and by combining the results we can show through (A.13) and (A.14) that the squashed entanglement of a thermal state is greater than or equal to that of an arbitrary state:

\[ E_{sq}(R; B)_\tau \geq E_{sq}(R; B)_\omega. \quad (A.41) \]
Vita

Noah Davis, born in 1990, grew up in Abita Springs, Louisiana. He graduated from Louisiana State University in 2012 with undergraduate degrees in physics and chemistry. Noah worked in research and development for a year before returning to LSU for his graduate studies in physics where he also enjoyed teaching undergraduate physics majors. His research interests include quantum effects, correlated systems, and high performance computing as well as interdisciplinary approaches to esoteric problems. Noah’s recreational interests and experiences range from outdoorsmanship and physical training to science fiction, music, and semantics.