Secure Communication with Unreliable Entanglement Assistance

Meir Lederman

Secure Communication with Unreliable Entanglement Assistance

Research Thesis

Submitted in partial fulfillment of the requirements
for the degree of Master of Science

Meir Lederman

Submitted to the Senate
of the Technion — Israel Institute of Technology
Sivan 5785 Haifa June 2025

This research was done in the The Andrew and Erna Viterbi Faculty of Electrical and Computer Engineering, under the supervision of Prof. Uzi Pereg.

The results in this thesis have been published as articles by the author and research collaborators in conferences and journals during the course of the author's research period:

Meir Lederman and Uzi Pereg. Secure communication with unreliable entanglement assistance. In *Proc. IEEE Int. Symp. Inf. Theory (ISIT 2024)*, pages 1017–1022, 2024.

Meir Lederman and Uzi Pereg. Semantic security with unreliable entanglement assistance: Interception and loss. In *Proc. IEEE Inf. Theory Workshop (ITW 2024)*, pages 693–698, 2024.

Meir Lederman and Uzi Pereg. Secure communication with unreliable entanglement assistance: Interception and loss. *Submitted to IEEE Trans. Inf. Theory*, 2025.

Acknowledgements

I would like to express my sincere gratitude to my advisor, Prof. Uzi Pereg, for his invaluable guidance and support throughout this work. I am also deeply grateful to my family and friends for their constant support and encouragement throughout this journey.

The author of this thesis states that the research, including the collection, processing and presentation of data, addressing and comparing to previous research, etc., was done entirely in an honest way, as expected from scientific research that is conducted according to the ethical standards of the academic world. Also, reporting the research and its results in this thesis was done in an honest and complete manner, according to the same standards.

The generous financial help of the Technion is gratefully acknowledged.

Contents

List of Figures

Abstract

In this work we consider secure communication over quantum wiretap channels, with unreliable entanglement assistance, when the assistance is unreliable due to two reasons: Interception or Loss. In the first model, Eve may intercept the entanglement resource. In the second model, Eve is passive, and the resource may dissipate to the environment beyond her reach. Both models are based on a hard decision approach, where Bob either receives the assistance entirely, or not at all. Once communication begins, Alice encodes without prior knowledge on whether Bob has received the assistance or not. Nonetheless, we assume that Bob knows whether he has the assistance or not. This is a practical assumption, based on the common use of heralded entanglement generation in practical implementations.

The operational principle of communication with unreliable entanglement assistance is to adapt the transmission rate to the availability of entanglement assistance, without resorting to feedback and repetition. To this end, we define two message sets, M and M', transmitted at rates R and R', respectively. The rate R is a guaranteed rate that is associated with the information that Bob should be able to decode in both cases, whether he has the assistance or not. The rate R' is an excess rate, corresponding to additional information that Bob should be able to decode only when the assistance is available. Hence, if Bob does not have the assistance, he decodes at a rate of R, and if Bob has the assistance, he decodes at an overall rate of $R + R'$.

For the passive model, we derive a multi-letter formula for the secrecy capacity for general quantum wiretap channels, subject to a maximal error criterion and semantic security. For the interception model, we derive achievable rates, and a multi-letter formula for the special class of degraded channels.

We demonstrate our results through two examples, the quantum erasure channel and the amplitude damping channel. Specifically, we show that time division is optimal for the erasure channel in both the interception and passive models. On the other hand, we observe that time division is not necessarily possible for the amplitude damping channel under interception, and the boundary of our achievable region is disconnected. Nonetheless, In the passive model, our rate region outperforms time division.

Abbreviations and Notations

Symbol	Description
X, Y, Z	Classical systems
A, B, C	Quantum systems
X^n	n–length sequences $(X_1, \ldots, X_n)$
$p_X(x)$, $P_{Y\|X}(y\|x)$	PMF of X and DMC transition probabilities
$\mathcal{P}(\mathcal{X})$	The set of all probability distributions on $\mathcal{X}$
$P_{Y\|X}^n(y^n\|x^n)$	Memoryless extension $\prod_i P_{Y\|X}(y_i\|x_i)$
M	Number of messages in a code
$\mathcal{M}$	Set of messages
f, g	Encoder $f : \{1, \ldots, M\} \to \mathcal{X}^n$, decoder $g : \mathcal{Y}^n \to \{1, \ldots, M\}$
$R = \frac{1}{n} \log M$	Coding rate (bits per channel use)
$P_{e,\max}^{(n)}$	Maximal probability of decoding error
S	Common randomness shared by sender/receiver
$\mathcal{H}_A, \mathcal{H}_B, \mathcal{H}_E$	Finite-dimensional Hilbert spaces of systems A, B, E
$\mathcal{L}(\mathcal{H}_A)$	Set of linear operators on $\mathcal{H}_A$
$\mathscr{S}(\mathcal{H}_A)$	Set of density operators on $\mathcal{H}_A$
ρ_A	Density operator (state) on $\mathcal{H}_A$
$\|\psi\rangle \in \mathcal{H}_A$	Pure state (unit vector) in $\mathcal{H}_A$
$\mathrm{Tr}[\cdot]$	Trace of an operator
$\|\rho - \sigma\|_1$	Trace distance between ρ and σ
$H(X)$	Classical entropy of X
$H(\rho)$	Von Neumann (quantum) entropy of ρ
$H(X\|Y)$	Conditional entropy
$H(A\|B)_\rho$	Conditional quantum entropy
$I(X;Y)$	Classical mutual information
$I(A;B)_\rho$	Quantum mutual information
$I(A\rangle B)_\rho$	Coherent information
$\chi(\mathcal{N})$	Holevo information of a quantum channel $\mathcal{N}$
$\mathcal{A}_\delta^{(n)}(p_X)$	δ-typical set with respect to a probability distribution p_X
$\Pi_\delta^{(n)}(\rho)$	Quantum δ-typical projector
$\mathcal{N}_{A\to B}$	Quantum channel from A (Alice) to B (Bob)

$\mathcal{N}_{A\to BE}$	Quantum wiretap channel, from A to B and E (Eve)
$\mathbb{1}$	Identity operator
$\mathtt{id}$	Ideal (noiseless) channel
G_A^n	The entanglement resource intended for Alice
G_B^n	The entanglement resource intended for Bob
$\Psi_{G_A^n G_B^n}$	Pre–shared entangled state between Alice and Bob
$C(P_{Y\|X})$	Channel capacity of a classical channel
$C_{\mathrm{CR}}(P_{Y\|X})$	Channel capacity of a classical channel with common-randomness assistance
$C_{\mathrm{S}}(P_{YZ\|X})$	Secrecy capacity of a classical channel
$C(\mathcal{L})$	Channel capacity of a quantum channel
$C_{\mathrm{S}}(\mathcal{N})$	Secrecy capacity of a quantum channel
$C_{\mathrm{EA}}(\mathcal{L})$	Entanglement-assisted capacity of a quantum channel
$C_{\mathrm{PE–EA}}(\mathcal{N})$	Secrecy capacity under a passive eavesdropper with (reliable) entanglement assistance
$C_{\mathrm{SI–EA}}(\mathcal{N})$	Secrecy capacity under interception with (reliable) entanglement assistance
$C_{\mathrm{EA}^*}(\mathcal{N})$	Capacity with unreliable entanglement assistance
$C_{\mathrm{PE–EA}^*}(\mathcal{N})$	Secrecy capacity under a passive eavesdropper with unreliable entanglement assistance
$C_{\mathrm{SI–EA}^*}(\mathcal{N})$	Secrecy capacity under interception with unreliable entanglement assistance

Thesis Outline

The thesis is divided into six chapters:

- **Chapter 1** reviews the notion of channel capacity and entanglement assistance. The chapter covers known capacity results in different settings: without assistance, with reliable entanglement assistance, and with unreliable entanglement assistance—all in the absence of secrecy constraints.
- **Chapter 2** reviews the secrecy capacity. We begin with different security criteria and review secrecy capacity results without assistance, with reliable and secure entanglement assistance, and with unsecure entanglement assistance.
- **Chapter 3** presents the main contribution on security with unreliable entanglement assistance in the interception model.
- **Chapter 4** presents the main contribution on security with unreliable entanglement assistance under passive eavesdropping.
- **Chapter 5** contains detailed analysis for the results stated in Chapters 3 and 4.
- **Chapter 6** summarizes the thesis and outlines directions for future work.

Table 2 indicates the chapter in which each setting is presented. The rows indicate the assistance that is provided to Alice and Bob before communication begins. The columns represent the security guarantee. Here, "Unsecure" means that there is no secrecy constraint, "Passive Eve" refers to the model in which the eavesdropper cannot access the shared resource, and "Interception" refers to the model where Eve may steal (intercept) the assistance.

	Unsecure	**Passive Eve**	**Interception**
No assistance	Chap.1	Chap.2	Chap.2
Reliable assistance	Chap.1	Chap.2	Chap.2
Unreliable assistance	Chap.1	Chap.4	Chap.4

Table 2: Thesis organization.

Table 3 provides the capacity notation and the capacity theorem for each setting:

	Unsecure	**Passive Eve**	**Interception**
No assistance	$C(\mathcal{L})$ (Th. 1.3, [1, 2])	$C_S(\mathcal{N})$ (Th. 2.3, [3, 4])	$C_S(\mathcal{N})$ (Th. 2.3, [3, 4])
Reliable assistance	$C_{\mathrm{EA}}(\mathcal{L})$ (Th. 1.4, [5])	$C_{\text{PE-EA}}(\mathcal{N})$ (Th. 2.7, [5])	$C_{\text{SI-EA}}(\mathcal{N})$ (Th. 2.5, [6])
Unreliable assistance	$C_{\mathrm{EA}^*}(\mathcal{L})$ (Th. 1.5, [7])	$C_{\text{PE-EA}^*}(\mathcal{N})$ (Th. 4.1)	$C_{\text{SI-EA}^*}(\mathcal{N})$ (Th. 3.1)

Table 3: Capacity notation and theorem references.

Chapter 1

Entanglement Assistance

Entanglement resources play a pivotal role in a wide range of quantum networking scenarios, including physical-layer security [8, 9], network communication protocols [10, 11, 12], quantum interferometry [13], quantum sensor networks [14, 15], and communication complexity [16]. Moreover, the presence of shared entanglement can substantially enhance communication rates over quantum channels [17, 18], as demonstrated in recent experimental implementations [19].

In general, quantum communication protocols can be categorized into two types: *unassisted* and *entanglement-assisted*, depending on whether the sender and receiver share entanglement prior to communication. In this context, "assistance" refers to a shared resource of correlation, which is cannot be used in order to send information by itself. Nevertheless, correlation assistance can be leveraged to enhance the communication rate in some cases. The motivation is as follows: In a dynamic communication network, the design may utilize inactive periods to generate shared assistance. Once information arrives and the transmission resumes, the transmitter and the receiver may use the assistance in order to increase throughput.

This chapter begins with preliminaries on quantum systems, classical and quantum information-theoretic measures, and typical projectors. We then present the capacity of a classical channel and the capacity with common-randomness assistance. Next, we present the capacities of quantum channels under three settings: unassisted, entanglement-assisted, and *unreliable* entanglement-assisted. The chapter concludes with the quantum packing lemma, a fundamental tool in the analysis of quantum capacities.

1.1 Preliminaries

Quantum information theory provides a general probabilistic framework that captures the performance behavior for communication system of a quantum nature. As the quantum theory reduces to the classical description in the classical limit, quantum information theory can be viewed as a generalization of the classical Shannon theory.

1.1.1 Classical Entropy and Mutual Information

A central theme in classical information theory is the quantification of information. Two key measures are entropy and mutual information, which form the foundation for characterizing the performance of communication systems.

The entropy of a discrete random variable X with probability mass function $p_X(x)$ is defined as:

$$H(p_X) = -\sum_{x\in\mathcal{X}} p_X(x)\log p_X(x),$$

and represents the average uncertainty or information content of X. We often use the simplified notation of $H(X) \equiv H(p_X)$. When X is uniformly distributed over M symbols, $H(X) = \log M$, which corresponds to maximum uncertainty. The set of all probability distributions on $\mathcal{X}$ is denoted by $\mathcal{P}(\mathcal{X})$.

Given two random variables X and Y, the mutual information between them is defined as:

$$I(X;Y) = H(X) + H(Y) - H(XY),$$

and quantifies the amount of information Y provides about X, and vice versa. Equivalently, it can also be written as:

$$I(X;Y) = \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p_{XY}(x,y)\log\frac{p_{XY}(x,y)}{p_X(x)p_Y(y)}.$$

Mutual information plays a central role in defining the limits of communication over noisy channels.

1.1.2 Quantum Systems

We use standard notation in quantum information processing. We label quantum systems by $A, B, C, ...$, and classical systems by $X, Y, Z, ...$

A quantum system is represented by a Hilbert space. We assume that the dimensions are finite. The Hilbert space for a system A is denoted by $\mathcal{H}_A$. We denote a vector in this space by the "ket" notation,

$$|\psi\rangle \in \mathcal{H}_A\,, \tag{1.1}$$

and its conjugate by the "bra" notation,

$$\langle\psi| \equiv (|\psi\rangle)^\dagger\ . \tag{1.2}$$

A quantum bit (qubit) is represented by a Hilbert space of dimension 2.

Example 1.1.1. Consider a qubit, $\mathcal{H}_A = \mathbb{C}^2$. The computational basis $\{|0\rangle, |1\rangle\}$, con-

sists of the following vectors:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \, , \; |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \, . \tag{1.3}$$

Density Operators

The state of System A is represented by a density operator ρ_A, *i.e.*, a unit-trace positive semidefinite operator:

$$\rho_A \geq 0 \, , \; \mathrm{Tr}(\rho_A) = 1 \, . \tag{1.4}$$

The set of all density operators on $\mathcal{H}_A$ is denoted by $\mathscr{S}(\mathcal{H}_A)$. The set of linear operators from $\mathcal{H}_A$ to $\mathcal{H}_A$ is denoted by $\mathcal{L}(\mathcal{H}_A)$. Hence, $\mathscr{S}(\mathcal{H}_A) \subseteq \mathcal{L}(\mathcal{H}_A)$. The state is said to be pure if ρ_A has rank 1, or equivalently, $\rho_A = |\psi\rangle\langle\psi|$ for some unit-vector $|\psi\rangle \in \mathcal{H}_A$.

A bipartite state ρ_{AB} of a pair of systems, A and B, is represented by a density operator on the tensor-product Hilbert space, $\mathcal{H}_A \otimes \mathcal{H}_B$. That is,

$$\rho_{AB} \in \mathscr{S}(\mathcal{H}_A \otimes \mathcal{H}_B) \, . \tag{1.5}$$

Entanglement

A state ρ_{AB} is called *separable* if there exists an ensemble of product states,

$$\{p_X(x) \, , \; \varphi_x \otimes \theta_x\} \tag{1.6}$$

in $\mathscr{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$, such that

$$\rho_{AB} = \sum_x p_X(x) \varphi_x \otimes \theta_x \, . \tag{1.7}$$

We say that A and B are *entangled* if ρ_{AB} is not separable.

In the special case of a pure state $|\psi_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, we say that A and B are entangled if the state cannot be written as a product, i.e.,

$$|\psi_{AB}\rangle \neq |\phi\rangle \otimes |\chi\rangle \tag{1.8}$$

for all $|\phi\rangle \in \mathcal{H}_A$ and $|\chi\rangle \in \mathcal{H}_B$.

Example 1.1.2. Consider two qubit systems A and B, with $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^2$. The Einstein–Podolsky–Rosen (EPR) state, $\left|\Phi^+\right\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$, is defined as

$$\left|\Phi^+\right\rangle_{AB} = \frac{1}{\sqrt{2}} \left(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B \right) \tag{1.9}$$

(also known as a Bell state). The corresponding density operator is given by

$$\rho_{AB} = \left|\Phi^+\right\rangle\!\left\langle\Phi^+\right|_{AB} \in \mathscr{S}(\mathcal{H}_A \otimes \mathcal{H}_B)\,. \tag{1.10}$$

In this case, we say that the qubits A and B are *maximally entangled*.

Quantum Measurements

Quantum measurements involve inherent uncertainty and may even disturb and change the state. A measurement is thus characterized in terms of the probability distribution of the measurement outcome and the corresponding post-measurement state. The outcome distribution of a quantum measurement can be described in terms of a collection of operators. Specifically, a positive operator-valued measure (POVM) is a set,

$$\{D_m\}_{m=1}^{M}\,, \tag{1.11}$$

of positive semidefinite linear operators in $\mathcal{L}(\mathcal{H}_A)$ such that

$$\sum_{m=1}^{M} D_m = \mathbb{1} \tag{1.12}$$

where $\mathbb{1}$ is the identity operator on $\mathcal{H}_A$. Each operator D_m is associated with a measurement outcome m. In a measurement carried out using such a POVM, the probability of the measurement outcome m is given by the Bourne rule,

$$\Pr(m) = \mathrm{Tr}(D_m \rho_A)\,. \tag{1.13}$$

Unitary and Isometric Evolutions

In an isolated system, the evolution of quantum states is always unitary, i.e., ρ_A may evolve to

$$\rho'_A = V \rho_A V^\dagger\,, \tag{1.14}$$

where $V : \mathcal{H}_A \to \mathcal{H}_A$ is unitary, $V^\dagger V = V V^\dagger = \mathbb{1}_A$. If we allow extension of the system using auxiliaries, the notion of a noiseless evolution can be generalized to an isometry, rather than a unitary. An operator $V : \mathcal{H}_A \to \mathcal{H}_B$ is called an isometry if $V^\dagger V = \mathbb{1}_A$. In this case, we must have $\dim(\mathcal{H}_A) \leq \dim(\mathcal{H}_B)$. In error-correction codes that do not account for security, encoders are typically isometric.

Example 1.1.3. The Pauli unitary operators can be viewed as quantum logical gates on $\mathcal{H} = \mathbb{C}^2$:

$$\Sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \Sigma_Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \Sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\,. \tag{1.15}$$

Example 1.1.4. Consider two qubit systems A and B, with $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^2$. The Bell states can be defined by

$$\left|\Phi^{(i,j)}\right\rangle_{AB} = (\Sigma_X^i \Sigma_Z^j \otimes \mathbb{1}) \left|\Phi^+\right\rangle_{AB} \tag{1.16}$$

where Σ_X and Σ_Z are the Pauli operators from Example 1.1.3. Each state is maximally entangled and together they form an orthonormal basis for $\mathcal{H}_A \otimes \mathcal{H}_B$,

1.1.3 Quantum Entropy and Information Measures

The von Neumann entropy for a density operator ρ is defined as

$$H(\rho) \equiv -\operatorname{Tr}[\rho \log \rho]\,. \tag{1.17}$$

The quantum entropy, $H(\rho)$, is identical to the classical entropy with respect to the eigenvalue distribution. Specifically, every density operator has a spectral decomposition of the following form:

$$\rho = \sum_{x=1}^{\dim(\mathcal{H})} p_X(x)\, |\psi_x\rangle\langle\psi_x|\,, \tag{1.18}$$

where the eigenvalues $p_X(x)$ form a probability distribution over $\{1, 2, \ldots, \dim(\mathcal{H})\}$, and the eigenvectors $|\psi_x\rangle$ form an orthonormal basis for $\mathcal{H}_A$. Then, the quantum entropy satisfies

$$H(\rho) = H(p_X)\,. \tag{1.19}$$

For a quantum system A in a state ρ_A, we often use the notation $H(A)_\rho \equiv H(\rho_A)$.

Consider a bipartite state $\rho_{AB} \in \mathscr{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$. In analogy to the classical definition, the quantum mutual information is defined as

$$I(A;B)_\rho \equiv H(A)_\rho + H(B)_\rho - H(AB)_\rho\,. \tag{1.20}$$

Furthermore, the conditional quantum entropy is defined by

$$H(A|B)_\rho = H(AB)_\rho - H(B)_\rho\,. \tag{1.21}$$

The conditional mutual information is defined accordingly: $I(A;B|C)_\rho = H(A|C)_\rho + H(B|C)_\rho - H(A,B|C)_\rho$.

We note that in the quantum setting, the conditional quantum entropy can be negative, even in finite dimensions. The coherent information from A to B is defined

as

$$I(A\rangle B)_\rho \equiv H(B)_\rho - H(AB)_\rho \tag{1.22}$$
$$= -H(A|B)_\rho \,. \tag{1.23}$$

Example 1.1.5. Consider the EPR state from Example 1.1.2,

$$\left|\Phi^+\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left[|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B\right]$$
$$= \frac{1}{\sqrt{2}}\left[\begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} + \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix}\right] . \tag{1.24}$$

The corresponding density operator is given by

$$\rho_{AB} = \left|\Phi^+\right\rangle\!\left\langle\Phi^+\right|_{AB} \tag{1.25}$$
$$= \begin{pmatrix} \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & \frac{1}{2} \end{pmatrix} . \tag{1.26}$$

This is a pure state (of rank 1), and therefore

$$H(AB)_\rho = 0 \,. \tag{1.27}$$

Next, we compute the reduced state of subsystem A. Tracing out system B yields a maximally mixed state:

$$\rho_A = \mathrm{Tr}_B(\rho_{AB}) \tag{1.28}$$
$$= \frac{1}{2}\mathbb{1} \tag{1.29}$$
$$= \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} , \tag{1.30}$$

where $\mathbb{1}$ is the identity operator on $\mathcal{H}_A$. The eigenspectrum of ρ_A is given by $p_X = \left(\frac{1}{2}, \frac{1}{2}\right)$, hence the quantum entropy is

$$H(A)_\rho = H(p_X) = \log 2 = 1 \,. \tag{1.31}$$

By symmetry, we also have

$$H(B)_\rho = 1 \,. \tag{1.32}$$

We can now compute the mutual information between A and B:

$$I(A;B)_\rho = H(A)_\rho + H(B)_\rho - H(AB)_\rho = 1 + 1 - 0 = 2\,. \tag{1.33}$$

Finally, the conditional quantum entropy is

$$H(A|B)_\rho = H(AB)_\rho - H(B)_\rho = 0 - 1 = -1\,, \tag{1.34}$$

and the coherent information is

$$I(A\rangle B)_\rho = -H(A|B)_\rho = 1\,. \tag{1.35}$$

1.1.4 Quantum Trace Distance

A fundamental measure of distinguishability between quantum states is the trace distance. For two operators $\rho, \sigma \in \mathscr{L}(\mathcal{H})$, the trace distance is defined as

$$\|\rho - \sigma\|_1 := \mathrm{Tr}\left[\sqrt{(\rho-\sigma)^\dagger(\rho-\sigma)}\right], \tag{1.36}$$

and the normalized trace distance is $\frac{1}{2}\|\rho - \sigma\|_1$. The normalized trace distance takes values in the interval $[0, 1]$. If ρ and σ commute, then the normalized trace distance is the same as the *total variation distance* between eigenspectra of ρ and σ.

1.1.5 Typical Projectors

Classical Types

We begin with the definition of a classical type. Consider a classical sequence $x^n \equiv (x_1, x_2, \ldots, x_n) \in \mathcal{X}^n$. The type of the sequence x^n is defined as the empricial distribution $\hat{P}_{x^n}(a) = \frac{N(a|x^n)}{n}$ for $a \in \mathcal{X}$, where $N(a|x^n)$ is the number of occurences of the letter a in the sequence x^n. Consider a type P on $\mathcal{X}$. The associated type class $\mathcal{T}^{(n)}(P)$ is then

$$\mathcal{T}^{(n)}(P) = \{x^n \in \mathcal{X}^n : \hat{P}_{x^n} = P\}\,. \tag{1.37}$$

Let $\delta > 0$. The δ-typical set, $\mathcal{A}_\delta^{(n)}(p_X)$, with respect to an (arbitrary) probability distribution p_X, is defined as the set of all sequences x^n whose type is close to p_X in the following sense:

$$\mathcal{A}_\delta^{(n)}(p_X) = \left\{x^n \in \mathcal{X}^n : \left|\hat{P}_{x^n}(a) - p_X(a)\right| \le \delta \cdot p_X(a)\,, \ \text{ for all } a \in \mathcal{X}\right\}. \tag{1.38}$$

Quantum Typical Projectors

Next, we move to the quantum method of types. Consider an ensemble $\{p_X(x), |x\rangle\}_{x\in\mathcal{X}}$, with an average state,

$$\sigma = \sum_{x\in\mathcal{X}} p_X(x)\,|x\rangle\langle x|\ . \tag{1.39}$$

Let $A_1,\ldots,A_n$ be a sequence of systems, associated with the tensor-product Hilbert space, $\mathcal{H}_A^{\otimes n}$. The δ-typical projector with respect to the ensemble above projects onto the subspace that is spanned by $|x^n\rangle \equiv \bigotimes_{i=1}^n |x_i\rangle_{A_i}$, where x^n are classical δ-typical sequences. Specifically,

$$\Pi_\delta^{(n)}(\sigma) = \sum_{x^n\in\mathcal{A}_\delta^{(n)}(p_X)} |x^n\rangle\langle x^n|\ . \tag{1.40}$$

The typical projector satisfies the following properties. There exists $a>0$ and $\epsilon>0$ such that

$$1-2^{-an} \le \mathrm{Tr}\{\Pi_\delta^{(n)}(\sigma)\sigma^{\otimes n}\} \le 1\,, \tag{1.41}$$

$$(1-2^{-an})2^{n(1-\delta)H(\sigma)} \le \mathrm{Tr}\{\Pi_\delta^{(n)}(\sigma)\} \le 2^{n(1+\delta)H(\sigma)}\,, \tag{1.42}$$

$$(1-2^{-an})2^{-n(1+\delta)H(\sigma)}\Pi_\delta^{(n)}(\sigma) \le \Pi_\delta^{(n)}(\sigma)\sigma^{\otimes n}\Pi_\delta^{(n)}(\sigma) \le 2^{-n(1-\delta)H(\sigma)}\Pi_\delta^{(n)}(\sigma)\,, \tag{1.43}$$

for sufficiently large n (see [20, Th. 1.1] and [21, Sec. 15.1.2]). These properties result from the classical asymptotic equipartition property (AEP) [22, Sec. 3.1]. We now give the quantum interpretation.

Intuition. Let

$$\sigma \in \mathscr{S}(\mathcal{H}_A) \tag{1.44}$$

be a given density operator. Consider a sequence of systems $A_1, A_2, \ldots, A_n$ in the joint state

$$\rho_{A_1\cdots A_n} = \sigma^{\otimes n}\,. \tag{1.45}$$

The δ-typical projector, $\Pi_\delta^{(n)}(\sigma)$, projects onto the *δ-typical subspace*,

$$\mathfrak{T}(\sigma) \subset \mathcal{H}_A^{\otimes n}\,, \tag{1.46}$$

given by

$$\mathfrak{T}(\sigma) = \mathrm{span}\{\ |x^n\rangle\ :\quad x^n \in \mathcal{A}_\delta^{(n)}(p_X)\}\,. \tag{1.47}$$

Suppose we perform a binary measurement specified by the operators $\{D_0, D_1\}$, where

$$D_1 = \Pi_\delta^{(n)}(\sigma)\,, \tag{1.48}$$

$$D_0 = \mathbb{1} - D_1\,. \tag{1.49}$$

This is referred to as a *typical measurement*, where the measurement outcome "1" corresponds to the typical subspace, whereas "0" corresponds to the non-typical subspace. Then,

- Property (1.41) means that the probability of a projection onto the typical subspace approaches certainty, i.e., $\Pr(\text{“1”}) \to 1$ as $n \to \infty$.

- Property (1.42) shows that the dimension of this typical subspace is approximately $2^{nH(\rho)}$. That is, $\dim\left[\mathfrak{T}(\sigma)\right] \approx 2^{nH(\sigma)}$.

- Property (1.43) implies that the state $\sigma^{\otimes n}$ is close to a symmetric (maximally mixed) state on the typical subspace. The eigenvalues are either $\approx 2^{-nH(\sigma)}$, or negligible.

Quantum Conditional Typical Projectors

Furthermore, we now define the *conditional* δ-typical subspace and projector. Consider an ensemble $\{p_X(x), \rho_B^x\}$, with an average state $\sigma_B = \sum_{x\in\mathcal{X}} p_X(x)\rho_B^x$. Given a fixed sequence $x^n \in \mathcal{X}^n$ and for every $a \in \mathcal{X}$, let $I_n(a)$ denote the set of indices $i \in [1:n]$ such that $x_i = a$. Then, the conditional δ-typical projector is defined as $\Pi_\delta^{(n)}(\sigma_B|x^n) = \bigotimes_{a\in\mathcal{X}} \left(\Pi_\delta^{(|I_n(a)|)}(\rho_B^a)\right)_{\{B_i : i\in I_n(a)\}}$.

Similarly as before, the conditional typical projector satisfies the properties below. There exist $a > 0$ and $\epsilon_n(\delta)$ such that

$$1 - 2^{-an} \leq \mathrm{Tr}\left\{\Pi_\delta^{(n)}(\sigma_B|x^n)\rho_{B^n}^{x^n}\right\} \leq 1 \tag{1.50}$$

$$(1-2^{-an})2^{n(1-\epsilon_n(\delta))H(B|X')_\sigma} \leq \mathrm{Tr}\left\{\Pi_\delta^{(n)}(\sigma_B|x^n)\right\} \leq 2^{n(1+\epsilon_n(\delta))H(B|X')_\sigma} \tag{1.51}$$

$$\begin{aligned} 2^{-n(1+\epsilon_n(\delta))H(B|X')_\sigma}\,\Pi_\delta^{(n)}(\sigma_B|x^n) &\leq \Pi_\delta^{(n)}(\sigma_B|x^n)\rho_{B^n}^{x^n}\Pi_\delta^{(n)}(\sigma_B|x^n) \\ &\leq 2^{-n(1-\epsilon_n(\delta))H(B|X')_\sigma}\,\Pi_\delta^{(n)}(\sigma_B|x^n) \end{aligned} \tag{1.52}$$

for sufficiently large n, where $\epsilon_n(\delta)$ tends to zero as $n \to \infty$ and $\delta \to 0$ (see [20, Th. 1.2] and [21, Sec. 15.2.4]), $\rho_{B^n}^{x^n} = \bigotimes_{i=1}^n \rho_{B_i}^{x_i}$, and the classical random variable X' is distributed according to the type of x^n.

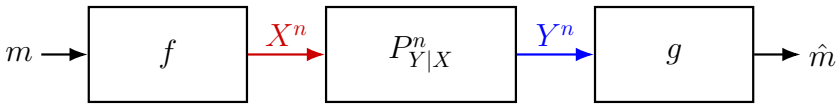


Figure 1.1: Classical channel model.

1.2 Classical Channels

1.2.1 Channel Model

In classical information theory, a *communication channel* is an abstract model describing the probabilistic relationship between the transmitted and received signals. A standard model is the *discrete memoryless channel (DMC)*, described by a conditional probability distribution $P_{Y|X}(y|x)$, where $x \in \mathcal{X}$ is an input symbol and $y \in \mathcal{Y}$ is an output symbol. The memoryless assumption implies that the channel's behavior at each time step is independent of past inputs or outputs.

Formally, for a sequence of inputs $X^n = (X_1, \ldots, X_n)$, the corresponding outputs $Y^n = (Y_1, \ldots, Y_n)$ are generated according to:

$$P^n_{Y|X}(y^n|x^n) = \prod_{i=1}^{n} P_{Y|X}(y_i|x_i).$$

1.2.2 Coding Definitions (Unassisted)

Reliable communication over a noisy channel requires the use of a *channel coding scheme*. A $(2^{nR}, n)$ code consists of:

- An **encoding** function $f : \{1, \ldots, 2^{nR}\} \to \mathcal{X}^n$, assigning each message a codeword of length n (we assume throughout this thesis that 2^{nR} is an integer).
- A **decoding** function $g : \mathcal{Y}^n \to \{1, \ldots, 2^{nR}\}$, producing an estimate for the transmitted message based on the received sequence.

We denote the code by (f, g).

The communication scheme is depicted in Figure 1.1. The sender, Alice, selects a message $m \in \{1, ..., 2^{nR}\}$. She encodes the message by the codeword $x^n = f(m)$, and transmits x^n through n uses of the classical channel. Bob recieves y^n and decodes by $\hat{m} = g(y^n)$.

The error probability given that Alice sent a message $m \in \{1, ..., 2^{nR}\}$ is

$$P_e^{(n)}(f, g|m) = \Pr\left[g(Y^n) \neq m \mid m\right] = \sum_{y^n : g(y^n) \neq m} P^n_{Y|X}(y^n|f(m)), \tag{1.53}$$

and the maximum error probability is defined as

$$P_{e,\max}^{(n)}(f,g) = \max_m P_e^{(n)}(f,g|m). \tag{1.54}$$

The *rate* of the code is the ratio of information bits per channel use:

$$R = \frac{\log M}{n} \text{ (bits per channel use)}, \tag{1.55}$$

where $M = 2^{nR}$ denotes the total number of messages.

A $(2^{nR}, n, \varepsilon)$ classical code satisfies

$$P_{e,\max}^{(n)}(f,g) \leq \varepsilon\,. \tag{1.56}$$

A rate R is called achievable if $\forall \varepsilon > 0$ and sufficiently large n, there exists a $(2^{nR}, n, \varepsilon)$ classical code.

The *channel capacity* is defined as the supremum of achievable rates. We denote the capacity of a classical channel by $C(P_{Y|X})$.

1.2.3 Shannon's Capacity Theorem

Shannon's fundamental result establishes the capacity limit for reliable communication over a noisy channel [23].

Theorem 1.1 (see [23])**.** *The capacity of a classical channel $P_{Y|X}$ is given by*

$$C(P_{Y|X}) = \max_{p_X} I(X;Y)$$

where the maximum is over all input distributions p_X on $\mathcal{X}$, and we compute the mutual information $I(X;Y)$ with respect to the joint distribution $p_{XY}(x,y) = p_X(x)P_{Y|X}(y|x)$.

Shannon's channel coding theorem states that:

- For any rate $R < C$, there exists a sequence of (M,n) codes such that $\liminf_{n\to\infty} \frac{\log M}{n} \geq R$ and $P_{e,\max}^{(n)} \to 0$.
- For any rate $R > C$, no sequence of codes can achieve $P_{e,\max}^{(n)} \to 0$.

Hence, the channel capacity C characterizes the maximum achievable rate for reliable communication.

1.3 Common-Randomness Assistance

In addition to the conventional communication model, one may consider the scenario where the sender and receiver have access to shared *common randomness*, independent of the channel input and output. This auxiliary resource can enhance the ability to coordinate actions and construct more elaborate coding strategies.

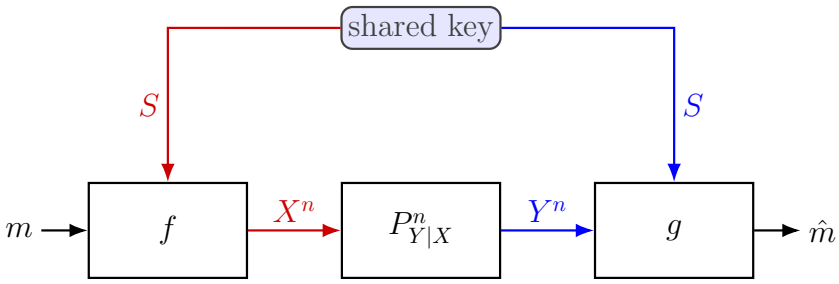


Figure 1.2: Common randomness channel model.

1.3.1 Definition

The common randomness is represented here by a random variable $S \sim p_S$, known to both the sender and the receiver.

Formally, a $(2^{nR}, n)$ code with common randomness assistance consists of a pair $\{(f, g)\}$, where:

- $f : \{1, \ldots, 2^{nR}\} \times \mathcal{S}_n \to \mathcal{X}^n$ is the encoding function.
- $g : \mathcal{Y}^n \times \mathcal{S}_n \to \{1, \ldots, 2^{nR}\}$ is the corresponding decoding function.

The coding scheme with common-randomness assistance is illustrated in Figure 1.2.

The rest of the coding definitions are similar to the unassisted case. We denote the common-randomness-assisted capacity by $C_{\text{CR}}(P_{Y|X})$, where the subscript 'CR' stands for common-randomness.

1.3.2 Capacity with Common Randomness

For memoryless channels, the availability of unlimited common randomness does *not* increase the capacity for reliable communication. This was established by Ahlswede in his foundational work [24], where he introduced the *elimination technique* to show that the randomized code ensemble can be derandomized without loss in capacity.

Theorem 1.2 (Ahlswede [24])**.** *The capacity of a classical channel $P_{Y|X}$ with common-randomness assistance satisfies:*

$$C_{\text{CR}}(P_{Y|X}) = C(P_{Y|X}) = \max_{p_X} I(X;Y).$$

We note that common randomness is yet valuable in settings beyond standard coding, such as secrecy systems [25], zero-error communication [26], and coordination problems [27]. In such cases, common randomness facilitates strong synchronization, private key agreement, and improved system design.

1.4 Quantum Channels

Quantum channels describe the physical evolution of quantum systems and serve as mathematical models for noisy transmission media, such as optical fibers [28]. The capacity of a quantum channel is the ultimate characteristic for communication throughput, i.e, the optimal rate at which information can be reliably transmitted with asymptotically vanishing error.

1.4.1 Channel Model

A quantum channel is defined as completely-positive trace-preserving (CPTP) linear map,

$$\mathcal{N}_{A\to B} : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B) \tag{1.57}$$

(see [21, Def. 4.4.2-4.4.3] for the definition of the CPTP properties). The quantum channel maps Alice's quantum state ρ_A on Alice's Hilbert space $\mathcal{H}_A$, to Bob's quantum state $\rho_B = \mathcal{N}_{A\to B}(\rho_A)$ on Bob's Hilbert space $\mathcal{H}_B$. The ideal (noiseless) channel $\mathrm{id} : \mathcal{L}(\mathcal{H}) \to \mathcal{L}(\mathcal{H})$ is defined by the relation $\mathrm{id}(\rho) = \rho$ for all ρ.

We assume that the channel is memoryless. That is, if the input $A^n \equiv A_1 A_2 \dots A_n$ is sent through the channel, then the input state ρ_{A^n} undergoes the tensor-product map $\mathcal{N}_{A\to B}^{\otimes n}$. Therefore, the output state is

$$\rho_{B^n} = \mathcal{N}_{A\to B}^{\otimes n}\left(\rho_{A^n}\right) . \tag{1.58}$$

Every quantum channel has a Stinspring representation, i.e, there exists an operator $V : \mathcal{H}_A \to \mathcal{H}_B \otimes \mathcal{H}_E$ such that

$$\mathcal{N}_{A\to B}(\rho) = \mathrm{Tr}_E(V\rho V^\dagger) \tag{1.59}$$

for $\rho \in \mathcal{L}(\mathcal{H}_A)$, where $V^\dagger V = \mathbb{1}$.

In addition, every quantum channel can be represented as a Kraus map, i.e, an operator-sum form:

$$\mathcal{N}_{A\to B}(\rho) = \sum_i K_i \rho K_i^\dagger \tag{1.60}$$

with $\sum_i K_i K_i^\dagger = \mathbb{1}$.

The quantum channel generalizes the classical channel $P_{Y|X}$, which can be viewed as a linear map from the input distribution p_X to an output distribution p_Y.

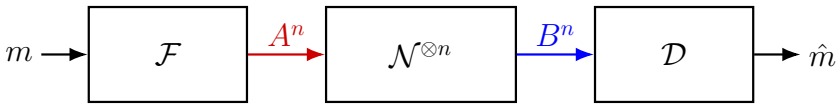


Figure 1.3: Quantum channel model.

1.4.2 Coding Definitions (Unassisted)

To communicate classical information over a quantum channel $\mathcal{N}_{A\to B}$, one uses an *ensemble of quantum states* to encode classical messages. A $(2^{nR}, n)$ code for communication of classical information over a quantum channel consists of:

- An encoding map $\mathcal{F} : \{1, \ldots, 2^{nR}\} \to \mathscr{S}(\mathcal{H}_A^{\otimes n})$, which assigns to each message m a quantum codeword $\varphi_m = \mathcal{F}(m)$, where $\varphi_m \in \mathscr{S}(\mathcal{H}_A^{\otimes n})$.
- A measurement POVM $\mathcal{D}_{B^n} = \{D_m\}_{m=1}^{2^{nR}}$, which consists of measurement operators $D_m \in \mathscr{S}(\mathcal{H}_B^{\otimes n})$ for $m \in \{1, \ldots, 2^{nR}\}$, such that $\sum_{m=1}^{2^{nR}} D_m = \mathbb{1}_{B^n}$. The measurement POVM is used by the receiver to decode the message.

The communication scheme is depicted in Figure 1.3. To send a message m, Alice encodes her input by preparing the input state

$$\rho_{A^n}^m = \mathcal{F}(m)\,, \tag{1.61}$$

where $A^n = (A_1, \ldots, A_n)$, and then transmits A^n through the memoryless channel, $\mathcal{N}_{A\to B}$. The output state is thus

$$\rho_{B^n}^m = \mathcal{N}_{A\to B}^{\otimes n}\left(\rho_{A^n}^m\right)\,, \tag{1.62}$$

where $B^n = (B_1, \ldots, B_n)$. Bob receives B^n, and then performs the decoding measurement $\{D_m\}_{m=1}^{2^{nR}}$ to obtain an estimate, which is distributed according to

$$\Pr(\hat{m}|m) = \operatorname{Tr}(D_{\hat{m}} \cdot \rho_{B^n}^m)\,. \tag{1.63}$$

The error probability given that Alice sent the message $m \in \{1, .., 2^{nR}\}$ is

$$P_e^{(n)}(\mathcal{F}, \mathcal{D}|m) = 1 - \operatorname{Tr}\{D_m \rho_{B^n}^m\}, \tag{1.64}$$

and the maximum error probability is defined by

$$P_{e,\max}^{(n)}(\mathcal{F}, \mathcal{D}) = \max_m P_e^{(n)}(\mathcal{F}, \mathcal{D}|m). \tag{1.65}$$

A $(2^{nR}, n, \varepsilon)$ code over a quantum channel satisfies

$$P_{e,\max}^{(n)}(\mathcal{F}, \mathcal{D}) \leq \varepsilon. \tag{1.66}$$

A rate R is said to be achievable if $\forall \varepsilon > 0$ and sufficiently large n, there exists a $(2^{nR}, n, \varepsilon)$ code. The channel capacity is defined as the supremum of achievable rates.

We denote the (unassisted) capacity of a quantum channel $\mathcal{N}_{A\to B}$ by $C(\mathcal{N})$.

1.4.3 Unassisted Capacity Theorem

The unassisted capacity of a quantum channel $\mathcal{N}_{A\to B}$ is characterized by the Holevo–Schumacher–Westmoreland (HSW) theorem [1, 2]. It describes the optimal rate at which classical information can be transmitted reliably over many independent uses of a quantum channel, without any additional resources such as entanglement or common randomness.

The Holevo information of a quantum channel $\mathcal{N}_{A\to B}$ is defined as:

$$\chi(\mathcal{N}) \equiv \max I(X;B)_\omega \,, \tag{1.67}$$

where the maximization is over classical-quantum states of the form:

$$\omega_{XB} = \sum_x p_X(x) \, |x\rangle\langle x| \otimes \mathcal{N}_{A\to B}(\omega_A^x) \,, \tag{1.68}$$

and $\{|x\rangle\}$ is an orthonormal basis on the classical register X.

Remark. It is important to notice that in the quantum setting, X is not the channel input, but rather an auxiliary random variable (a classical system). In general, auxiliary variables appear in many network information settings, both classical and quantum. Here, the variable X selects the input state from a collection of quantum states, $\{\psi_A^x : x \in \mathcal{X}\}$.

The unassisted capacity was independently characterized by Holevo [1] and Schumacher and Westmoreland [2]. Hence, the result is commonly referred to as the HSW Theorem.

Theorem 1.3 (HSW Capacity Theorem [1, 2])**.** *The capacity of a quantum channel $\mathcal{N}_{A\to B}$ satsfies:*

$$C(\mathcal{N}) \geq \chi(\mathcal{N}) \,. \tag{1.69}$$

Furthermore,

$$C(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} \chi(\mathcal{N}^{\otimes n}), \tag{1.70}$$

where $\chi(\mathcal{N}^{\otimes n})$ is the Holevo information with respect to the product channel $\mathcal{N}_{A\to B}^{\otimes n} : \mathcal{L}(\mathcal{H}_A^{\otimes n}) \to \mathcal{L}(\mathcal{H}_B^{\otimes n})$.

For channels with additive Holevo information, the capacity simplifies to the single-letter formula [29, Sec. 8.3]:

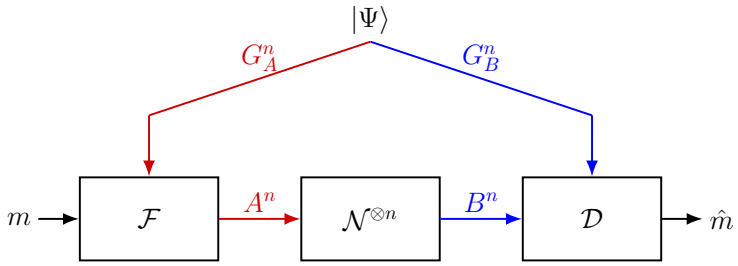


Figure 1.4: Entanglement-assisted quantum channel model.

$$C(\mathcal{N}) = \chi(\mathcal{N})\,. \tag{1.71}$$

This holds for many channels, such as the erasure channel, dephasing channel, depolarizing channel, quantum Gaussian channel, etc. In the past, many researchers believed that (1.71) holds for all channels.

In general, however, regularization is necessary, as Hastings [30] showed that there exist channels with a super-additive behavior, such that

$$\frac{1}{n}\chi(\mathcal{N}^{\otimes n}) > \chi(\mathcal{N}). \tag{1.72}$$

A single-letter capacity formula is an open problem in general.

1.5 Entanglement-Assisted Communication

1.5.1 Model and Motivation

In the entanglement-assisted model, the sender and the receiver are allowed to share an arbitrary amount of prior entanglement before communication begins. This shared entanglement is independent of the channel and can be leveraged to enhance the communication rate. Specifically, the idea is to utilize inactive periods to generate shared entanglement, which can later be used in order to increase throughput, once the transmission resumes.

We view the entanglement-assisted setting as the quantum parallel of communication with common randomness, as in Section 1.3. Nonetheless, the behavior is different, as entanglement assistance can significantly improve achievable rates. In the entanglement-assisted communication setting, Alice applies an encoding map that acts jointly on her share of the entangled state and the message, and transmits the resulting state through the quantum channel. Bob then decodes using both the channel output and his share of the entanglement.

1.5.2 Coding Definitions

A $(2^{nR}, n)$ entanglement-assisted code for communication over a quantum channel consists of:

- A shared entangled state $\Psi_{G_A^n G_B^n} \in \mathscr{S}(\mathcal{H}_{G_A^n} \otimes \mathcal{H}_{G_B^n})$ between the sender and the receiver, where G_A^n is the entanglement resource at the transmitter, and G_B^n at the receiver.
- A collection of encoding maps $\mathcal{F}^{(m)}_{G_A^n \to A^n} : \mathscr{S}(\mathcal{H}_{G_A^n}) \to \mathscr{S}(\mathcal{H}_A^{\otimes n})$ for $m \in \{1, .., 2^{nR}\}$.
- A decoding POVM $\mathcal{D}_{B^n G_B^n} = \{D_m\}_{m=1}^{2^{nR}}$, such that $\sum_{m=1}^{2^{nR}} D_m = \mathbb{1}$, where $D_m \in \mathscr{S}(\mathcal{H}_B^{\otimes n} \otimes \mathcal{H}_{G_B^n})$ for $m \in \{1, \ldots, 2^{nR}\}$. The decoding POVM is associated with the measurement performed by the receiver in order to estimate the message, using both the channel output and his share of entanglement.

We denote the code by $(\Psi, \mathcal{F}, \mathcal{D})$. The communication scheme is depicted in Figure 1.4. Alice selects a message $m \in \{1, ..., 2^{nR}\}$. She prepares the input state by applying the encoding map on her share of entanglement assistance:

$$\rho^m_{A^n G_B^n} = (\mathcal{F}^{(m)}_{G_A^n \to A^n} \otimes \mathrm{id})(\Psi_{G_A^n G_B^n}), \tag{1.73}$$

and transmits A^n through n uses of the quantum channel. Here, the ideal (noiseless) channel, id, acts on Bob's share of entanglement assistance, G_B^n, since Alice does not have access to this resource. The output state is thus

$$\rho^m_{B^n G_B^n} = \left(\mathcal{N}^{\otimes n}_{A \to B} \otimes \mathrm{id}\right)(\rho^m_{A^n G_B^n}). \tag{1.74}$$

Bob receives B^n, and then performs the decoding measurement $\{D_m\}_{m=1}^{2^{nR}}$ to obtain an estimate, which is distributed according to

$$\Pr(\hat{m}|m) = \mathrm{Tr}(D_{\hat{m}} \cdot \rho^m_{B^n G_B^n}). \tag{1.75}$$

The conditional error probability, given that Alice sent the message m, is

$$P_e^{(n)}(\Psi, \mathcal{F}, \mathcal{D}|m) = 1 - \mathrm{Tr}\left[D_m \cdot \rho^m_{B^n G_B^n}\right]. \tag{1.76}$$

The maximum error probability is

$$P^{(n)}_{e,\max}(\Psi, \mathcal{F}, \mathcal{D}) = \max_m P_e^{(n)}(\Psi, \mathcal{F}, \mathcal{D}|m). \tag{1.77}$$

A $(2^{nR}, n, \varepsilon)$ entanglement-assisted code over a quantum channel satisfies

$$P^{(n)}_{e,\max}(\Psi, \mathcal{F}, \mathcal{D}) \leq \varepsilon. \tag{1.78}$$

A rate R is said to be achievable if $\forall \varepsilon > 0$ and sufficiently large n, there exists a $(2^{nR}, n, \varepsilon)$ code with entanglment assistance.

The capacity is defined as the supremum of achievable rates with entanglment assistance. We denote the entanglement-assisted capacity of a quantum channel $\mathcal{N}$ by $C_{\mathrm{EA}}(\mathcal{N})$.

1.5.3 Entanglement-Assisted Capacity

The entanglement-assisted capacity of a quantum channel $\mathcal{N}_{A\to B}$ is the maximum rate at which classical information can be transmitted reliably using the channel, assuming unlimited prior entanglement. Remarkably, the capacity formula has a single-letter form.

Theorem 1.4 (Bennet et al. [5])**.** *The entanglement-assisted capacity of a quantum channel $\mathcal{N}_{A\to B}$ is given by:*

$$C_{\mathrm{EA}}(\mathcal{N}) = \max_{|\phi_{GA}\rangle} I(G;B)_{\omega}\,, \tag{1.79}$$

where the maximum is over all bipartite states $|\phi_{GA}\rangle$, and

$$\omega_{GB} = (\mathrm{id}\otimes\mathcal{N})(|\phi_{GA}\rangle\langle\phi_{GA}|)\,,$$

with $\dim(\mathcal{H}_G) \leq \dim(\mathcal{H}_A)$.

We note that G is an auxiliary system in the optimization formula. This auxiliary can be interpreted as Bob's entanglement resource.

The entanglement-assisted capacity formula is additive, meaning $\mathsf{f}(\mathcal{N}^{\otimes n}) = n \cdot \mathsf{f}(\mathcal{N})$ where $\mathsf{f}(\mathcal{N}) = \max I(G;B)_{\omega}$. It also provides an upper bound on the unassisted capacity, as $C(\mathcal{N}) \leq C_{EA}(\mathcal{N})$. The entanglement-assisted capacity can significantly exceed the unassisted capacity [31, 32].

1.5.4 Superdense Coding

A fundamental example that illustrates the advantage of entanglement assistance is *superdense coding* [33]. Based on the Holevo bound [34], the capacity of a noiseless quantum channel without entanglement assistance is

$$1\left[\frac{\text{classical bit}}{\text{qubit transmission}}\right].$$

Superdense coding shows that entanglement assistance can be utilized to double this capacity. That is, if Alice and Bob are provided with entanglement resource, the transmission rate becomes

$$2\left[\frac{\text{classical bits}}{\text{qubit transmission}}\right].$$

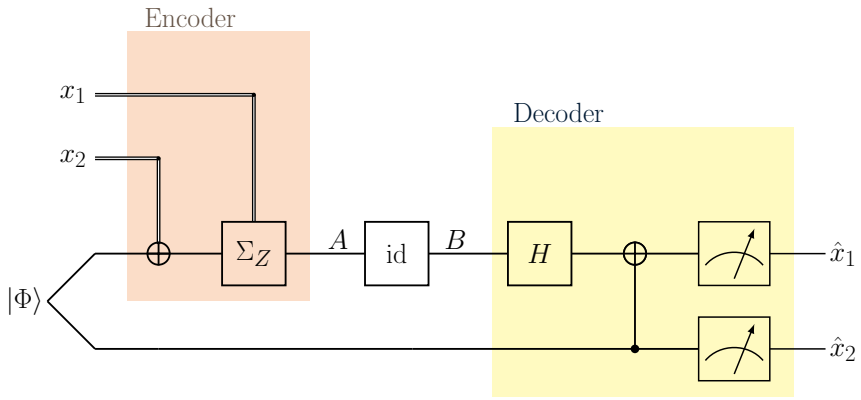


Figure 1.5: Illustration of Superdense Coding

Specifically, it turns out that a single EPR pair is sufficient (see Example 1.1.2). The protocol includes the following:

- A shared entangled state $\left|\Phi^+\right\rangle_{G_AG_B} \in \mathcal{H}_{G_A} \otimes \mathcal{H}_{G_B}$ between the sender and the receiver, where G_A is the entanglement resource at the transmitter and G_B at the receiver.

- Encoding operators $\Sigma_X^i \Sigma_Z^j$, for $i, j \in \{0, 1\}$, where Σ_X and Σ_Z are the Pauli operators (see Example 1.1.3).

- A decoding POVM, corresponding to a Bell-state measurement.

The method is demonstrated in Figure 1.5. Alice selects a two-bit message $m = (m[0], m[1])$, where $m[i] \in \{0, 1\}$. She prepares the input state by applying $X^{m[0]}Z^{m[1]}$ on her share of the entangled resource:

$$\left|\Phi^{(m)}\right\rangle_{AG_B} = (\Sigma_X^{m[0]}\Sigma_Z^{m[1]} \otimes \mathrm{id}) \left|\Phi^+\right\rangle_{G_AG_B}, \tag{1.80}$$

and transmits A through the noiseless quantum channel $\mathrm{id}_{A\to B}$. We note that $\left\{\left|\Phi^{(m)}\right\rangle\right\}$ constitute the Bell basis in Example 1.1.4.

Bob receives system B, and performs a Bell-state measurement on $\left|\Phi^{(m)}\right\rangle_{BG_B}$ (the Bell measurement is represented in Figure 1.5 by the application of a Hadamard gate and a CNOT gate, followed by a measurement in the computational basis). This measurement allows him to perfectly distinguish between the four orthogonal Bell states and recover the message $(m[0], m[1])$ with probability 1.

Thus, superdense coding enables entanglement-assisted communication at a rate of 2 classical bits per qubit transmission via the noiseless qubit channel.

1.6 Unreliable Entanglement-Assisted Communication

Entanglement resources are useful in many applications. Unfortunately, it is a fragile resource [35, 36]. In order to generate entanglement assistance in optical communication, the transmitter first prepares an entangled pair locally, and then transmits half of it [37]. Since photons are easily lost to the environment [38], current implementations incorporate a back channel to notify the transmitter in case of a failure, with numerous repetitions. This approach has clear disadvantages and may even result in system collapse. However, ensuring resilience and reliability is critical for developing future communication networks [39].

In the classical literature of cooperation resources, Steinberg introduced the concept of uncertain cooperation in classical information theory in 2014 [40], and Huleihel and Steinberg later expanded on it [41]. Their framework captures ad-hoc networks where key resources—bandwidth, time slots, energy—may or may not be available, since availability depends on factors beyond the designer's control (for example, relay battery levels, weather conditions, or peer willingness). Previous work has examined unreliable cooperation in multi-user scenarios such as the multiple-access channel [42] and broadcast channel [43, 44, 45], as well as in related frameworks like outage analysis [46, 47], ARQ [48, 49], cognitive radios [50], and the broadcast approach for fading channels—where the transmission rate is dynamically adapted to the channel state [51, 52, 53]. In contrast, we focus here on the reliability of static entanglement resources in a point-to-point quantum channel.

Communication with *unreliable* entanglement assistance was recently introduced by Pereg et al. [7] as a setup where a back channel and repetition are not required. Instead, the rate is adapted to the availability of entanglement assistance. Thereby, the principle of operation ensures reliability by design. In communication with unreliable entanglement assistance, Alice and Bob are provided with unreliable entanglement resources, as the communicating parties are uncertain about the availability of entanglement assistance.

Specifically, Alice wishes to send two messages, at rates R and R'. She encodes both messages using her share of the entanglement resources, as she does not know whether Bob will have access to the entangled resources. Bob has two decoding procedures. If the entanglement assistance has failed to reach Bob's location, he performs a decoding operation to recover the first message alone. Hence, the communication system operates on a rate R. Whereas if Bob has entanglement assistance, he decodes both messages, hence the overall transmission rate is $R + R'$. In other words, R is a *guaranteed rate*, and R' is the *excess rate* of information that entanglement assistance provides. We define the capacity region as the set of all rate pairs (R, R') that can be achieved with asymptotically vanishing decoding errors.

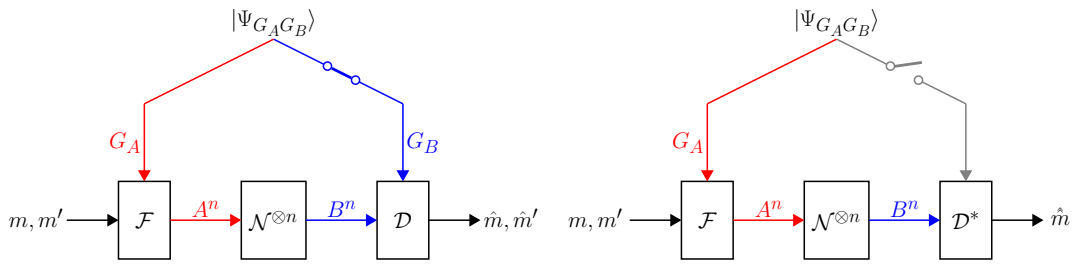


Figure 1.6: Illustration of unreliable entanglement assistance that is controlled by an imaginary switch. Thus, there are two scenarios: (a) "On": Bob decodes both m and m'. (b) "Off": Bob decodes m alone.

1.6.1 Coding Definitions

A $(2^{nR}, 2^{nR'}, n)$ code with unreliable entanglement assistance consists of the following:

- Two message sets $\{1, \ldots, 2^{nR}\}$ and $\{1, \ldots, 2^{nR'}\}$ where $2^{nR}, 2^{nR'}$ are assumed to be integers.
- A pure entangled state $\Psi_{G_A^n, G_B^n}$.
- A collection of encoding maps, $\mathcal{F}^{m,m'}_{G_A^n \to A^n} : \mathscr{S}(\mathcal{H}_{G_A^n}) \to \mathscr{S}(\mathcal{H}_A^{\otimes n})$, for $m \in \{1, \ldots, 2^{nR}\}$ and $m' \in \{1, \ldots, 2^{nR'}\}$.
- Two decoding POVMs, $\mathcal{D}_{B^n G_B^n} = \{D_{m,m'}\}$ and $\mathcal{D}^*_{B^n} = \{D^*_m\}$.

We denote the code by $(\mathcal{F}, \Psi, \mathcal{D}, \mathcal{D}^*)$

The communication scheme is depicted in Figure 1.6. The sender Alice has the systems A^n and G_A^n as well, where G_A^n and G_B^n represent the entanglement resources. The model captures two scenarios, i.e. when entanglement assistance is present or absent. This is illustrated in Figure 1.6 by an imaginary switch that controls the assistance. Without assistance, Bob is only required to decode one message, and given entanglement assistance, he should recover both messages.

Specifically, Alice chooses two classical messages, $m \in \{1, \ldots, 2^{nR}\}$ and $m' \in \{1, \ldots, 2^{nR'}\}$. She prepares the input state by

$$\rho^{m,m'}_{A^n G_B^n} = \left(\mathcal{F}^{(m,m')}_{G_A^n \to A^n} \otimes \mathrm{id}\right)\left(\Psi_{G_A^n G_B^n}\right), \tag{1.81}$$

and transmits A^n over n channel uses of $N_{A \to B}$. The channel output of Bob is

$$\rho^{m,m'}_{B^n G_B^n} = (\mathcal{N}^{\otimes n}_{A \to B} \otimes \mathrm{id})(\rho^{m,m'}_{A^n G_B^n}). \tag{1.82}$$

If the entanglement assistance is present, i.e. Bob has access to the entanglement resource G_B^n, then he should recover both messages. He combines the output with the

entangled system G_B^n and performs the measurement POVM $\mathcal{D}_{B^nG_B^n} = \{D_{m,m'}\}$ to obtain an estimate $(\hat{m}, \hat{m'})$.

Otherwise, if entanglement assistance is absent, then Bob decondes less information. If Bob does not have the resource G_B^n, then he is only required to recover the first message, m. Hence, he performs the measurement $\mathcal{D}^*_{B^n} = \{D^*_m\}$ to obtain an estimate $\hat{m}$ of the first message alone. For this reason, the first message, m, is referred to as the guaranteed information, and the second message, m', as the excess information that entanglement assistance provides.

Each scenario is associated with a different error probability. In the presence of entanglement assistance, the conditional probability of error given that the messages m and m' were sent is:

$$P_e^{(n)}(\mathcal{F}, \Psi, \mathcal{D}|m, m') = 1 - \mathrm{Tr}\left[D_{m,m'}(\mathcal{N}^{\otimes n}_{A\to B} \otimes \mathrm{id})(\mathcal{F}^{(m,m')}_{G_A^n \to A^n} \otimes \mathrm{id})(\Psi_{G_A^n, G_B^n})\right], \quad (1.83)$$

as the decoder measures $\mathcal{D}_{B^nG_B^n} = \{D_{m,m'}\}$ in this scenario. Without assistance, the conditional probability of error is:

$$P_e^{*(n)}(\mathcal{F}, \Psi, \mathcal{D}^*|m, m') = 1 - \mathrm{Tr}\left[D^*_m(\mathcal{N}^{\otimes n}_{A\to B} \circ \mathcal{F}^{(m,m')}_{G_A^n \to A^n})(\Psi_{G_A^n})\right], \quad (1.84)$$

as the decoder does not have access to G_B^n and measures $\mathcal{D}^*_{B^n} = \{D^*_m\}$ in this scenario.

Notice that the encoded input remains the same in both scenarios, since Alice does not know whether entanglement assistance is present or not. Therefore, the error depends on m and m' in both cases.

We denote the maximal error probabilities by:

$$P^{(n)}_{e,\max}(\mathcal{F}, \Psi, D) = \max_{m,m'} P_e^{(n)}(\mathcal{F}, \Psi, D|m, m'), \quad (1.85)$$

$$P^{*(n)}_{e,\max}(\mathcal{F}, \Psi, \mathcal{D}^*) = \max_{m,m'} P_e^{*(n)}(\mathcal{F}, \Psi, \mathcal{D}^*|m, m'). \quad (1.86)$$

A $(2^{nR}, 2^{nR'}, n, \varepsilon)$ code with unreliable entanglement assistance satisfies

$$P^{(n)}_{e,\max}(\mathcal{F}, \Psi, \mathcal{D}) \leq \varepsilon \quad (1.87)$$

and

$$P^{*(n)}_{e,\max}(\mathcal{F}, \Psi, \mathcal{D}^*) \leq \varepsilon\,. \quad (1.88)$$

A rate pair (R, R') is called achievable if for every $\varepsilon > 0$ and sufficiently large n, there exists a $(2^{nR}, 2^{nR'}, n, \varepsilon)$ code with unreliable entanglement assistance.

The capacity region $C_{\mathrm{EA}^*}(\mathcal{N})$ with unreliable entanglement assistance is defined as the set of all achievable rate pairs.

Remark. The communication scheme with unreliable entanglement assistance is con-

ceptually analogous to a scenario with unreliable common randomness. However, while common randomness does not enhance the communication rate, entanglement assistance does. Thus, the model is meaningful only in the entanglement-assisted setting.

Remark. Entanglement assistance does not increase the capacity of a classical channel. In this case, the capacity region is given by

$$C_{\mathrm{EA}^*}(P_{Y|X}) = \left\{(R, R') : R + R' \leq C(P_{Y|X})\right\}$$

for a classical channel $P_{Y|X}$.

1.6.2 Capacity Results

General Channels

Define

$$R_{\mathrm{EA}*}(\mathcal{N}) = \bigcup_{p_X, \varphi_{G_1G_2}, \mathcal{F}^{(x)}} \left\{ \begin{array}{rcl} (R, R') : & R \leq & I(X;B)_\omega \\ & R' \leq & I(G_2;B|X)_\omega \end{array} \right\}, \tag{1.89}$$

where

$$\omega_{XG_2A} = \sum_{x \in \mathcal{X}} p_X(x) \, |x\rangle\langle x| \otimes (\mathrm{id} \otimes \mathcal{F}^{(x)}_{G_1 \to A})(\varphi_{G_2G_1}) \,, \tag{1.90}$$

and

$$\omega_{XG_2B} = (\mathrm{id} \otimes \mathcal{N}_{A\to B})(\omega_{XG_2A}) \,. \tag{1.91}$$

Theorem 1.5 (Pereg et al. [7])**.** *The capacity region of a quantum channel $\mathcal{N}_{A\to B}$ with unreliable entanglement assistance satisfies*

$$C_{\mathrm{EA}^*}(\mathcal{N}) \supseteq R_{\mathrm{EA}^*}(\mathcal{N}) \,. \tag{1.92}$$

Furthermore,

$$C_{\mathrm{EA}^*}(\mathcal{N}) = \bigcup_{n=1}^{\infty} \frac{1}{n} R_{\mathrm{EA}^*}(\mathcal{N}^{\otimes n}) \,. \tag{1.93}$$

Entanglement Breaking Channels

Entanglement breaking is a fundamental property of a broad class of quantum channels that map any entangled input state into a separable output state [54]. A quantum channel $\mathcal{N}_{A\to B}$ is called *entanglement breaking* if, for every input state $\rho_{AA'}$, where A'

is an arbitrary reference system, the channel output is separable, i.e.,

$$(\mathcal{N}_{A\to B}\otimes \mathrm{id}_{A'})(\rho_{AA'}) = \sum_{x\in\mathcal{X}} p_X(x)\,\psi_B^x\otimes\psi_{A'}^x\,,$$

for some probability mass function p_X and pure states ψ_B^x and $\psi_{A'}^x$.

The Kraus representation of an entanglement-breaking channel consists of Kraus operators with unit rank. Moreover, any entanglement-breaking channel can be expressed as a sequential composition of a measurement channel followed by a classical-to-quantum channel (see [55, Corollary 4.6.1]).

From a Shannon-theoretic viewpoint, entanglement-breaking channels are relatively well understood. Their unassisted capacity is given by the single-letter Holevo information [56], i.e., $C(\mathcal{N}) = \chi(\mathcal{N})$. While such a channel cannot be used in order to generate entanglement, classical messages can still be transmitted, and entanglement assistance can significantly enhance their capacity [31]. In the setting of unreliable entanglement assistance, the capacity region for entanglement-breaking channels is given by a single-letter formula.

Theorem 1.6 (Pereg [57])**.** *The capacity region of an entanglement-breaking quantum channel $\mathcal{N}_{A\to B}$ with unreliable entanglement assistance is given by*

$$C_{\mathrm{EA}^*}(\mathcal{N}) = R_{\mathrm{EA}^*}(\mathcal{N})\,. \tag{1.94}$$

1.7 Regularization and Single-Letter Characterizations

As demonstrated by the results in this chapter, some capacity results are expressed in the form of a *regularization* limit:

$$\mathsf{f}_{\mathrm{reg}}(\mathcal{N}) = \lim_{n\to\infty}\frac{1}{n}\mathsf{f}_1(\mathcal{N}^{\otimes n})\,. \tag{1.95}$$

Regularized expressions are also referred to as *multi-letter formulas*. Such formulas are given, for example, in the capacity theorem for a general quantum channel, without assistance, as well as in the unreliable entanglement-assisted capacity.

The main limitation of regularized capacity formulas lies in their lack of computability and conceptual transparency. Since they involve limits over increasing blocklengths, such expressions typically do not admit closed-form evaluations and are difficult to compute in practice [58].

Another limitation of regularized formulas is their lack of uniqueness. That is, a multi-letter formula does not uniquely characterize the capacity of a channel for a given task. For example [21, Sec. 13.1.3], consider the capacity of a classical channel, which is given by $C(P_{Y|X}) = \max_{p(x)} I(X;Y) = \max_{p(x)}[H(X) - H(X|Y)]$. Define $I_a(P_{Y|X}) \triangleq \max_{p(x)}[H(X) - aH(X|Y)]$. It is clear that $C(P_{Y|X}) > I_a(P_{Y|X})$ for $a > 1$. However, if we consider the multi-letter formula of $I_a(P_{Y|X})$, we find that it

coincides with the capacity: $\lim_{n\to\infty} \frac{1}{n} I_a(P_{Y|X}^n) = C(P_{Y|X})$ for all $a \geq 1$. Thus, the capacity formula is not unique under regularization.

A further limitation is the lack of insights into optimal code design. Single-letter formulas provide valuable guidance on how to design optimal coding strategies across a variety of scenarios. For example, in the multiple access channel, the single-letter characterization highlights approaches such as time-sharing and successive-cancellation decoding [59, 60]. In parallel Gaussian channels, they lead to practical ideas such as the water-filling method for power allocation [61].

Nonetheless, for specific classes of channels—such as entanglement-breaking channels—single-letter formulas have been established. Regularization-free characterizations remain an active area of research, as they not only facilitate practical computations but also provide deeper insight into the structure of quantum information tasks.

1.8 Packing Lemma

We conclude this chapter with the quantum packing lemma, a pivotal tool in the analysis of quantum information-theoretic tasks.

The quantum packing lemma plays a central role in establishing achievability results, particularly in entanglement-assisted communication scenarios. It provides a general framework for encoding classical messages into a Hilbert space such that the receiver can reliably distinguish them. Specifically, if the sender prepares an ensemble of quantum states and the receiver applies an appropriate set of projectors, the lemma ensures the existence of a decoding measurement with low average error probability.

This lemma underpins all the capacity theorems presented in this chapter and plays a central role in the analysis of secrecy capacities, including the results of this thesis.

Lemma 1.8.1 (Quantum Packing Lemma [10])**.** *Let $\{p_X(x), \sigma_x\}_{x\in\mathcal{X}}$ be a quantum ensemble with average state $\sigma = \sum_x p_X(x)\sigma_x$. Suppose there exist a code projector Π and codeword projectors $\{\Pi_x\}_{x\in\mathcal{X}}$ satisfying:*

$$\mathrm{Tr}\{\Pi\sigma_x\} \geq 1-\varepsilon, \tag{1.96}$$

$$\mathrm{Tr}\{\Pi_x\sigma_x\} \geq 1-\varepsilon, \tag{1.97}$$

$$\mathrm{Tr}\{\Pi_x\} \leq \mathsf{h}, \tag{1.98}$$

$$\Pi_x\Pi \leq \frac{1}{\mathsf{H}}\Pi, \tag{1.99}$$

for all $x \in \mathcal{X}$, where $\varepsilon \in (0,1)$, and $0 < \mathsf{h} < \mathsf{H}$. Let $\mathcal{M}$ be a set of messages of size $|\mathcal{M}|$. Construct a random codebook $\mathcal{C} = \{X(m)\}_{m\in\mathcal{M}}$ where each $X(m)$ is independently drawn from p_X. Define the corresponding codeword states as $\sigma_{X(m)}$. Then, there exists a POVM $\{D_m\}_{m\in\mathcal{M}}$ such that the expected average probability of

correct decoding satisfies:

$$\mathbb{E}_{\mathcal{C}}\left\{\frac{1}{|\mathcal{M}|}\sum_{m\in\mathcal{M}}\mathrm{Tr}\left[D_m\sigma_{X(m)}\right]\right\}\geq 1-2\left(\varepsilon+2\sqrt{\varepsilon}\right)-4|\mathcal{M}|\cdot\frac{\mathsf{h}}{\mathsf{H}}. \tag{1.100}$$

Chapter 2

Secrecy Capacity

Secure communication is a fundamental goal in both classical and quantum information theory. The concept of *secrecy capacity* characterizes the maximum rate at which information can be reliably transmitted from a sender to an intended receiver, while ensuring that an eavesdropper gains negligible information about the transmitted message. This notion plays a central role in cryptographic applications and physical-layer security, where the goal is to exploit the properties of the communication channel itself to guarantee confidentiality.

In the classical setting, secrecy is typically studied through the wiretap channel model introduced by Wyner [62], where an eavesdropper observes a degraded version of the main communication. In the quantum regime, secrecy capacities extend to both classical and quantum communication, leveraging phenomena such as entanglement and measurement disturbance. A notable example of a practical secrecy scheme is quantum key distribution (QKD), where the goal is to generate a shared secret key between two parties that remains secure against any quantum adversary [63]. Physical layer security complements the cryptographic key distribution approach, and leverages the inherent disturbance of the physical channel to ensure secure transmissions without relying on secret keys [64].

This chapter reviews the notion of secrecy capacity for both classical and quantum channels, along with known single-letter expressions and regularized formulas. We begin by defining the quantum wiretap channel and several security notions, including weak security, strong security, and semantic security. We then present the secrecy capacity of the classical wiretap channel. We then turn to quantum channels, presenting the secrecy capacity of a quantum wiretap channel, under three scenarios: unassisted, entanglement-assisted with adversarial access to the entanglement, and entanglement-assisted with a passive adversary. The chapter concludes with the quantum covering lemma, a fundamental tool in the analysis of quantum secrecy capacities.

2.1 Quantum Wiretap Channel

The quantum wiretap channel is a fundamental model for secure communication in the quantum setting.

A quantum wiretap channel $\mathcal{N}_{A\to BE} : \mathscr{S}(\mathcal{H}_A) \to \mathscr{S}(\mathcal{H}_B \otimes \mathcal{H}_E)$ maps a state at the sender's system to a joint state of the legitimate receiver and eavesdropper's systems. The sender, receiver, and eavesdropper are often referred to as Alice, Bob and Eve, respectively. Hence, if Alice prepares her input A in the state ρ_A, the joint output of Bob and Eve is given by $\rho_{BE} = \mathcal{N}_{A\to BE}(\rho_A)$.

We denote the marginal channel to the legitimate receiver, i.e., from Alice to Bob, by $\mathcal{L}_{A\to B}$, and the adversarial marginal, from Alice to Eve, by $\overline{\mathcal{L}}_{A\to E}$. The marginal channels are also referred to as the main channel and the eavesdropper's channel, respectively.

The quantum wiretap channel $\mathcal{N}_{A\to BE}$ is called *degraded* if there exists a degrading channel $\mathcal{P}_{B\to E}$ such that

$$\overline{\mathcal{L}}_{A\to E} = \mathcal{P}_{B\to E} \circ \mathcal{L}_{A\to B}\,.$$

The classical parallel is commonly referred to as a a *stochastically* degraded wiretap channel.

We assume that the channel is memoryless, i.e., if Alice sends a sequence of input systems $A^n \equiv (A_1, \ldots, A_n)$, then the channel input ρ_{A^n} undergoes the tensor-product mapping $\mathcal{N}_{A\to BE}^{\otimes n}$.

2.2 Security Criteria

To ensure security in the wiretap channel, one typically requires the eavesdropper's output state to be (almost) uncorrelated with the transmitted message. Several notions of security have been proposed to formalize this idea, including *weak secrecy*, *strong secrecy*, and *semantic security*.

2.2.1 Weak vs. Strong Secrecy

Let M denote the transmitted message and E^n the eavesdropper's quantum system after n uses of the channel.

Strong secrecy. The system satisfies strong secrecy if the mutual information between the message and Eve's system vanishes in the limit of $n \to \infty$:

$$\lim_{n\to\infty} I(M; E^n)_\rho = 0\,, \tag{2.1}$$

for a uniformly distributed message, M.

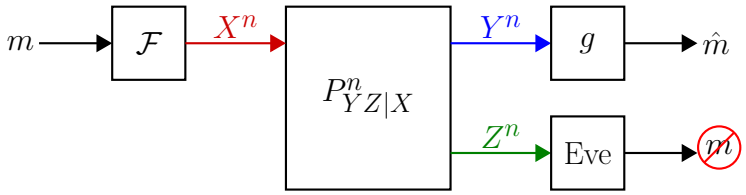


Figure 2.1: Classical wiretap channel model.

This ensures that the correlation between the message and the information that is leaked to the eavesdropper becomes negligible, providing a strong guarantee of confidentiality.

Weak secrecy. A weaker requirement is:

$$\lim_{n\to\infty} \frac{1}{n} I(M; E^n)_\rho = 0\,, \tag{2.2}$$

for a uniformly distributed message M.

This condition only requires that the *rate* of information leakage vanishes asymptotically. Since it allows for a sublinear amount of leakage, weak secrecy is generally insufficient for cryptographic applications but still relevant in some information-theoretic models [65].

2.2.2 Semantic Security and Indistinguishability

Semantic security requires that Eve cannot gain any advantage in learning anything about the message, regardless of its distribution. In quantum information theory, this is often formulated in terms of *indistinguishability*:

Let $\rho^m_{E^n}$ denote the eavesdropper's state when a message $m \in \{1, \ldots, 2^{nR}\}$ is sent. The communication scheme is said to satisfy semantic security if

$$\max_{m\in\{1,\ldots,2^{nR}\}} \frac{1}{2} \left\|\rho^m_{E^n} - \theta_{E^n}\right\|_1 \leq \delta, \tag{2.3}$$

for arbitrarily small $\delta > 0$ and sufficiently large n, where θ_{E^n} is a constant state that does not depend on m. This condition ensures that Eve's state becomes indistinguishable (in probability) from a state that is completely independent of the transmitted message.

2.3 Classical Wiretap Channel

In classical information theory, a discrete memoryless wiretap channel is modeled by a transition probability $P_{YZ|X}$, where X is the channel input, and Y and Z denote the outputs at the legitimate receiver and the eavesdropper, respectively.

2.3.1 Coding Definitions

Reliable communication over the wiretap channel requires both reliable communication to the legitimate receiver and secrecy against the eavesdropper.

A $(2^{nR}, n)$ secrecy code consists of:

- An encoding channel, $F : \{1, \ldots, 2^{nR}\} \to \mathcal{X}^n$.
- A decoder, $g : \mathcal{Y}^n \to \{1, \ldots, 2^{nR}\}$.

The communication scheme is depicted in Figure 2.1. Alice selects a message m from $\{1, \ldots, 2^{nR}\}$. She generates a codeword x^n according to the probability distribution $F(\cdot|m)$, and transmits x^n through n uses of the classical wiretap channel. The channel outputs of Bob and Eve, respectively, are distributed according to

$$Q(y^n, z^n|m) = \sum_{x^n \in \mathcal{X}^n} F(x^n|m) P^n_{YZ|X}(y^n, z^n|x^n)\,. \tag{2.4}$$

Bob receives y^n and decodes by $\hat{m} = g(y^n)$.

The error probability given that the message m was sent is

$$P_e^{(n)}(F, g|m) = \Pr[g(Y^n) \neq m \mid m] = \sum_{y^n : g(y^n) \neq m} Q(y^n|m), \tag{2.5}$$

for $m \in \{1, ..., 2^{nR}\}$. Hence, the maximum error probability is

$$P_{e,\max}^{(n)}(F, g) = \max_m P_e^{(n)}(F, g|m). \tag{2.6}$$

Define the security level, with respect to an eavesdropper distribution $Q_0 \in \mathcal{P}(\mathcal{Z}^n)$, by:

$$\Delta_{\mathrm{S}}(F, Q_0) = \max_m \frac{1}{2} \|Q(\cdot|m) - Q_0(\cdot)\|_1\,, \tag{2.7}$$

where $Q_0(z^n)$ is an output distribution that does not depend on m.

A $(2^{nR}, n, \varepsilon, \delta)$ secrecy code satisfies

$$P_{e,\max}^{(n)}(F, g) \leq \varepsilon \tag{2.8}$$

and

$$\Delta_{\mathrm{S}}(F, Q_0) \leq \delta \tag{2.9}$$

for some $Q_0 \in \mathcal{P}(\mathcal{Z}^n)$.

A rate R is said to be achievable if, for every $\varepsilon, \delta > 0$ and sufficiently large n, there exists a $(2^{nR}, n, \varepsilon, \delta)$ code.

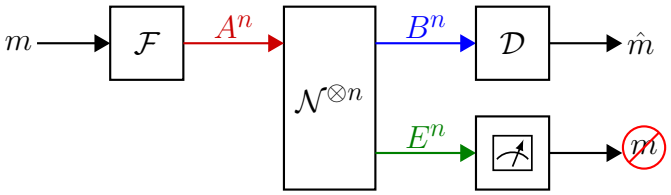


Figure 2.2: Quantum wiretap channel model.

The secrecy capacity $C_S(P_{YZ|X})$ is the supremum of all such achievable secrecy rates.

2.3.2 Classical Secrecy Capacity

The capacity theorems for classical wiretap channels were originally established by Wyner in the degraded case [62], and extended to the general wiretap channel by Csiszár and Körner [66], laying the foundation for information-theoretic security.

Theorem 2.1 (Wyner [62])**.** *The classical secrecy capacity of a discrete memoryless degraded wiretap channel $P_{YZ|X}$ is given by the single-letter expression:*

$$C_S(P_{YZ|X}) = \max_{p_X} \left[I(X;Y) - I(X;Z) \right]. \tag{2.10}$$

Theorem 2.2 (Csiszár and Körner [66])**.** *The classical secrecy capacity of a general discrete memoryless wiretap channel $P_{YZ|X}$, under the strong secrecy criterion, admits a single-letter characterization:*

$$C_S(P_{YZ|X}) = \max_{p_{UX}} \left[I(U;Y) - I(U;Z) \right], \tag{2.11}$$

where the auxiliary random variable U satisfies $|\mathcal{U}| \leq |\mathcal{X}|$.

This result demonstrates that, despite the need for auxiliary variables, the secrecy capacity of general wiretap channels can still be expressed in a single-letter form.

2.4 Quantum Channels (Unassisted)

2.4.1 Coding Definitions

To transmit classical information securely over a quantum wiretap channel $\mathcal{N}_{A\to BE}$, one uses a secrecy code that ensures both reliability and security from an eavesdropper. A $(2^{nR}, n)$ secrecy code consists of the following:

- An encoding map $\mathcal{F} : \{1, ..., 2^{nR}\} \to \mathscr{S}(\mathcal{H}_A^{\otimes n})$, which assigns each message $m \in \{1, ..., 2^{nR}\}$ to a quantum codeword $\rho_{A^n}^m \in \mathscr{S}(\mathcal{H}_A^{\otimes n})$.

- A measurement POVM $\mathcal{D}_{B^n} = \{D_m\}_{m=1}^{2^{nR}} \subset \mathscr{S}(\mathcal{H}_B^{\otimes n})$ such that $\sum_{m=1}^{2^{nR}} D_m = \mathbb{1}_{B^n}$, used by the receiver to decode the message.

We denote the code by $(\mathcal{F}, \mathcal{D})$. The communication scheme is depicted in Figure 2.2. Alice selects a message $m \in \{1, ..., 2^{nR}\}$, and encodes the message by preparing the input state $\rho_{A^n}^m$. The output state is

$$\rho_{B^n}^m = \mathcal{L}_{A\to B}^{\otimes n}\left(\rho_{A^n}^m\right), \tag{2.12}$$

where $\mathcal{L}_{A\to B}$ is the marginal channel for Bob.

Bob receives B^n, and then performs the decoding measurement $\{D_m\}_{m=1}^{2^{nR}}$ to obtain an estimate, which is distributed according to

$$\Pr(\hat{m}|m) = \mathrm{Tr}(D_{\hat{m}} \cdot \rho_{B^n}^m). \tag{2.13}$$

The error probability given the message m was sent is

$$P_e^{(n)}(\mathcal{F}, \mathcal{D} \mid m) = 1 - \mathrm{Tr}\left[D_m \cdot \rho_{B^n}^m\right]. \tag{2.14}$$

The maximal probability of error is defined by

$$P_{e,\max}^{(n)}(\mathcal{F}, \mathcal{D}) = \max_m P_e^{(n)}(\mathcal{F}, \mathcal{D} \mid m). \tag{2.15}$$

To ensure security, we also require that Eve's states corresponding to different messages are nearly indistinguishable. Formally, Let $\mathcal{L}_{A\to E}$ denote the complementary channel to Eve, and define the state at Eve's side when message m is sent by

$$\rho_{E^n}^m = \mathcal{L}_{A\to E}^{\otimes n}(\rho_{A^n}^m). \tag{2.16}$$

Define the security level with respect to a constant state θ_{E^n}, by:

$$\Delta_{\mathrm{S}}(\mathcal{F}, \theta_{E^n}) = \max_m \frac{1}{2}\|\rho_{E^n}^m - \theta_{E^n}\|_1. \tag{2.17}$$

A $(2^{nR}, n, \varepsilon, \delta)$ secrecy code satisfies

$$P_{e,\max}^{(n)}(\mathcal{F}, \mathcal{D}) \le \varepsilon, \qquad \Delta_{\mathrm{S}}(\mathcal{F}, \theta_{E^n}) \le \delta, \tag{2.18}$$

for some θ_{E^n}.

A rate R is said to be achievable if, for every $\varepsilon, \delta > 0$ and sufficiently large n, there exists a $(2^{nR}, n, \varepsilon, \delta)$ code.

The secrecy capacity $C_S(\mathcal{N})$ of a quantum channel $\mathcal{N}$ is defined as the supremum of all achievable rates.

2.4.2 Secrecy Capacity

Consider a quantum wiretap channel $\mathcal{N}_{A\to BE}$, and suppose that Alice and Bob do not share entanglement a priori. The private information of the quantum wiretap channel is defined by

$$I_{\mathrm{S}}(\mathcal{N}) \equiv \max_{p_X(x),\omega_A^x} \left[I(X;B)_\omega - I(X;E)_\omega \right], \tag{2.19}$$

where the maximization is over the ensemble of quantum input states, and

$$\omega_{XBE} \equiv \sum_{x\in\mathcal{X}} p_X(x) \left|x\right\rangle\!\left\langle x\right| \otimes \mathcal{N}_{A\to BE}(\omega_A^x), \tag{2.20}$$

with $|\mathcal{X}| \leq \dim(\mathcal{H}_A)^2 + 1$.

Remark. The variable X in the definition above is an auxiliary classical random variable used to describe the ensemble of quantum inputs. It is not a direct channel input, but rather plays a role analogous to the auxiliary variable U in Theorem 2.2.

Theorem 2.3 (see [3, 4])**.** *The secrecy capacity of a quantum wiretap channel $\mathcal{N}_{A\to BE}$ without assistance is given by*

$$C_S(\mathcal{N}) = \lim_{k\to\infty} \frac{1}{n} I_S(\mathcal{N}^{\otimes n}). \tag{2.21}$$

A single-letter formula for the secrecy capacity remains an open problem for a general quantum wiretap channel. The private information is known to be super additive as well [67].

2.4.3 Degraded Channels

For degraded quantum wiretap channels, the secrecy capacity admits a single-letter characterization, in contrast to the general case where regularization is required [68, 67]. This result mirrors the classical setting and simplifies both analysis and computation.

Theorem 2.4 (see [4, 69])**.** *The secrecy capacity of a degraded quantum wiretap channel $\mathcal{N}_{A\to BE}$ is given by*

$$C_S(\mathcal{N}) = \max_{p_X(x),\omega_A^x} \left[I(X;B)_\omega - I(X;E)_\omega \right], \tag{2.22}$$

where $\omega_{XBE} = \sum_x p_X(x) \left|x\right\rangle\!\left\langle x\right| \otimes \mathcal{N}(\omega_A^x)$, and the maximization is over classical-quantum input ensembles $\{p_X(x), \omega_A^x\}$, with $|\mathcal{X}| \leq [\dim(\mathcal{H}_A)]^2$.

This result holds regardless of the secrecy criterion. The degraded structure allows one to bound Eve's information via a post-processing of Bob's output, enabling a simpler security analysis.

2.5 Entanglement Assisted Secrecy Capacity

Qi et al. [6] consider secure communication with reliable entanglement assistance. In principle, if the transmitter and receiver share perfect entanglement beforehand, it can be utilized to generate a joint key, and then encode the information using the one-time pad protocol. Their model, however, does not allow Alice and Bob to generate a secret key in this manner, as Qi et al. [6] assume that the eavesdropper has access to the legitimate receiver's entanglement resource.

In other words, the entanglement assistance is *not* secure. The model can viewed as the quantum analog of a wiretap channel with common randomness that is available to Alice, Bob, and Eve.

While the assumption that both Bob and Eve can measure the same system may seem to contradict the no-cloning theorem, our interception model provides an operational meaning to their setting. We now present the definitions and results of Qi et al. [6].

2.5.1 Coding Definitions

To transmit classical information securely over a quantum wiretap channel $\mathcal{N}_{A\to BE}$ with entanglement assistance, we consider the adversarial setting where the eavesdropper (Eve) has access not only to the output of the wiretap channel but also to Bob's share of the entangled resource.

A $(2^{nR}, n)$ secrecy code with entanglement assistance is defined as before, and consists of:

- A pure entangled state $\Psi_{G_A^n G_B^n} \in \mathscr{S}(\mathcal{H}_{G_A^n} \otimes \mathcal{H}_{G_B^n})$, initially shared between Alice and Bob, where Eve is assumed to also have access to the system G_B^n.
- A collection of encoding maps $\mathcal{F}^{(m)}_{G_A^n \to A^n} : \mathscr{S}(\mathcal{H}_{G_A^n}) \to \mathscr{S}(\mathcal{H}_A^{\otimes n})$, which, given $m \in \{1, ..., 2^{nR}\}$, map $\Psi_{G_A^n}$ to a codeword $\rho^m_{A^n}$.
- A decoding POVM $\mathcal{D}_{B^n G_B^n} = \{D_m\}_{m=1}^{2^{nR}} \subset \mathscr{S}(\mathcal{H}_B^{\otimes n} \otimes \mathcal{H}_{G_B^n})$ such that $\sum_{m=1}^{2^{nR}} D_m = \mathbb{1}$, used by the receiver to decode the message using both the channel output and his share of entanglement.

We denote the code by $(\Psi, \mathcal{F}, \mathcal{D})$.

In the secret communication scheme with entanglement assistance, Alice selects a message $m \in \{1, ..., 2^{nR}\}$. She prepares the input state by applying the encoding map

$$\rho^m_{A^n G_B^n} = (\mathcal{F}^{(m)}_{G_A^n \to A^n} \otimes \mathrm{id})(\Psi_{G_A^n G_B^n}), \tag{2.23}$$

and transmits A^n through n uses of the quantum channel.

The output state is thus

$$\rho^m_{B^n G^n_B} = \left(\mathcal{L}^{\otimes n}_{A\to B} \otimes \mathrm{id}\right)\left(\rho^m_{A^n} \otimes \Psi_{G^n_B}\right), \tag{2.24}$$

where $\mathcal{L}_{A\to B}$ is the marginal channel to Bob.

Bob receives B^n, and then performs the decoding measurement $\{D_m\}_{m=1}^{2^{nR}}$ to obtain an estimate, which is distributed according to

$$\Pr(\hat{m}|m) = \mathrm{Tr}(D_{\hat{m}} \cdot \rho^m_{B^n G^n_B}). \tag{2.25}$$

The error probability given a message m was sent is:

$$P_e^{(n)}(\Psi, \mathcal{F}, \mathcal{D} \mid m) = 1 - \mathrm{Tr}\left[D_m \cdot \rho^m_{B^n G^n_B}\right]. \tag{2.26}$$

The maximal error probability is

$$P^{(n)}_{e,\max}(\Psi, \mathcal{F}, \mathcal{D}) = \max_m P_e^{(n)}(\Psi, \mathcal{F}, \mathcal{D} \mid m). \tag{2.27}$$

To ensure security, we now require privacy against an adversary who holds both the channel output E^n and the entangled system G^n_B. In our framework, this means that Eve has intercepted the entanglement resource. Let

$$\omega^m_{E^n G^n_B} = \left(\mathcal{L}^{\otimes n}_{A\to E} \otimes \mathrm{id}\right)\left(\rho^m_{A^n} \otimes \Psi_{G^n_B}\right) \tag{2.28}$$

be Eve's state when message m is sent. The security level under interception of Eve with respect to a constant state $\theta_{E^n G_B}$ is

$$\Delta_{\mathrm{SI}}(\Psi, \mathcal{F}, \theta_{E^n G^n_B}) = \max_m \frac{1}{2}\left\|\omega^m_{E^n G^n_B} - \theta_{E^n G^n_B}\right\|_1, \tag{2.29}$$

where SI indicates security under interception.

A $(2^{nR}, n, \varepsilon, \delta)$ secrecy code with entanglement assistance satisfies

$$P^{(n)}_{e,\max}(\Psi, \mathcal{F}, \mathcal{D}) \le \varepsilon, \qquad \Delta_{\mathrm{SI}}(\Psi, \mathcal{F}, \theta_{E^n G^n_B}) \le \delta, \tag{2.30}$$

for some $\theta_{E^n G^n_B}$.

A rate R is said to be achievable if, for every $\varepsilon, \delta > 0$ and sufficiently large n, there exists a $(2^{nR}, n, \varepsilon, \delta)$ code.

The entanglement-assisted secrecy capacity in this adversarial setting, denoted $C_{\text{SI-EA}}(\mathcal{N})$, is defined as the supremum of all such achievable rates. The subscript 'SI-EA' stands for security under interception, with entanglement assistance.

Remark. The no-cloning theorem states that it is impossible to create an identical copy of an arbitrary unknown quantum state [70]. While the assumption that both Bob and Eve have access to the same entangled subsystem appears to contradict this principle,

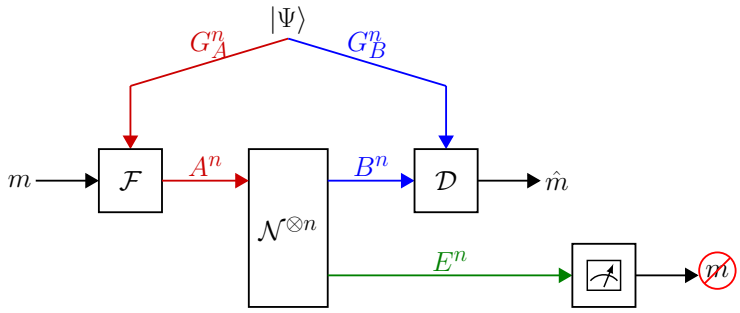


Figure 2.3: Entanglement-assisted wiretap channel model with a passive eavesdropper.

our interception model gives an operational interpretation of such a setting by treating the entanglement as a resource that may be intercepted rather than duplicated (See Sec. 3.2.5).

2.5.2 Capacity Results

Define

$$I_{\text{SI-EA}}(\mathcal{N}) = \max_{\varphi_{GA}} [I(G;B)_\omega - I(G;E)_\omega] \,, \tag{2.31}$$

where the maximum is over all bipartite states φ_{GA}, and

$$\omega_{GBE} \equiv (\mathrm{id} \otimes \mathcal{N}_{A\to BE})(\varphi_{GA}) \,. \tag{2.32}$$

Theorem 2.5 (see [6]). *The secrecy capacity of a quantum wiretap channel $\mathcal{N}_{A\to BE}$ with (reliable) entanglement assistance is bounded by*

$$C_{\text{SI-EA}}(\mathcal{N}) \geq I_{\text{SI-EA}}(\mathcal{N}) \,. \tag{2.33}$$

Furthermore, if the channel is degraded, the bound is tight.

Theorem 2.6 (see [6]). *The secrecy capacity of a degraded quantum wiretap channel $\mathcal{N}_{A\to BE}$ with (reliable) entanglement assistance satsifies*

$$C_{\text{SI-EA}}(\mathcal{N}) = I_{\text{SI-EA}}(\mathcal{N}) \,. \tag{2.34}$$

A single-letter formula for the entanglement-assisted secrecy capacity for general channels is an open problem.

2.6 Passive Model

Another natural model to consider is one in which the eavesdropper is passive and does not have access to the entanglement assistance, as in the standard wiretap scenario. See

Figure 2.3. In this setting, the sender and receiver may utilize the shared entanglement to establish a secret key in advance, thereby ensuring security from the eavesdropper. The model can thus be viewed as the quantum analog of a wiretap channel with key assistance, assumed to be secure beyond Eve's reach.

Assuming unlimited entanglement assistance, the generation of the key does not pose a constraint. Consequently, the problem reduces to that of reliable communication with entanglement assistance, without additional secrecy considerations.

The entanglement-assisted secrecy capacity of a quantum channel $\mathcal{N}$ with a passive eavesdropper is denoted by $C_{\text{PE-EA}}(\mathcal{N})$, where 'PE-EA' stands for a passive eavesdropper, while Alice and Bob are provided with reliable entanglement assistance. In this model, the secrecy capacity coincides with the entanglement-assisted capacity given in Theorem 1.4:

Theorem 2.7. *The entanglement-assisted secrecy capacity of a quantum channel $N_{A\to BE}$, when Eve is passive and cannot access Bob's share of entanglement, is:*

$$C_{\text{PE}-\text{EA}}(\mathcal{N}) = C_{\text{EA}}(\mathcal{N}) = \max_{|\phi_{GA}\rangle} I(G;B)_{\omega}\,, \tag{2.35}$$

where the maximum is over all bipartite states $|\phi_{GA}\rangle$, and

$$\omega_{GB} = (\mathrm{id}\otimes\mathcal{N})(|\phi_{GA}\rangle\langle\phi_{GA}|)\,,$$

with $\dim(\mathcal{H}_G) \leq \dim(\mathcal{H}_A)$.

This result is analogues to classical communication assisted by common randomness that is hidden from the adversary, i.e., a shared secret key. If the eavesdropper is passive and does not have access to the secret key, there is no secrecy penalty, and the secrecy capacity matches the capacity without secrecy [71].

One can achieve this using one-time pad (OTP) encryption. In the classical case, Alice and Bob share a random key and encrypt the message using bitwise XOR. In the quantum setting, for example, if they share EPR states (see Example 1.1.2), they can measure their respective states to generate identical random bits, which serve as a shared secret key. This is equivalent to assuming that Alice and Bob have a pre-shared secret key, which Eve cannot access.

2.7 Soft Covering Lemma and Channel Resolvability

We conclude this chapter with the quantum soft covering lemma, which plays a key role in establishing indistinguishability guarantees in secrecy analysis. The soft covering lemma is a fundamental technical tool in both classical and quantum information theory. It provides a probabilistic guarantee that a randomly generated codebook will closely approximate the average behavior of a given ensemble. This result is especially

powerful in the context of secrecy capacities, along with other tasks such as channel simulation [5] and lossy compression [55, 72].

In our analysis, the quantum soft covering lemma plays a central role in establishing security guarantees. Specifically, it allows us to show that the ensemble average of the eavesdropper's states—generated by a random codebook—is close to the overall average state. As a result, the eavesdropper cannot reliably distinguish which particular codeword was sent.

Lemma 2.7.1 (see [73])**.** *Let $\{p_X(x), \sigma_x\}_{x\in\mathcal{X}}$ be an ensemble, with mean state $\sigma \equiv \sum_{x\in\mathcal{X}} p_X(x)\sigma_x$. Furthermore, suppose that there is a code projector Π and codeword projectors $\{\Pi_x\}_{x\in\mathcal{X}}$, that satisfy:*

$$\mathrm{Tr}\{\Pi\sigma_x\} \geq 1-\epsilon\,, \tag{2.36}$$

$$\mathrm{Tr}\{\Pi_x\sigma_x\} \geq 1-\epsilon\,, \tag{2.37}$$

$$\mathrm{Tr}\{\Pi\} \leq \mathsf{H}\,, \tag{2.38}$$

$$\Pi_x\sigma_x\Pi_x \leq \frac{1}{\mathsf{h}}\Pi_x\,, \tag{2.39}$$

for all $x \in \mathcal{X}$, where $\varepsilon \in (0,1)$, and $0 < \mathsf{h} < \mathsf{H}$. Consider a random codebook $\mathscr{C} \equiv \{X(k)\}_{k\in\mathcal{K}}$ of size $|\mathcal{K}|$, where each codeword is independently drawn according to $p_X(x)$.

Then,

$$\Pr\left\{\left\|\frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}}\sigma_{X(k)} - \sigma\right\|_1 > \epsilon + 4\sqrt{\epsilon} + 24\sqrt[4]{\epsilon}\right\} \leq 1 - 2\mathsf{H}\exp\left(-\frac{\epsilon^3}{4\ln 2}\cdot\frac{|\mathcal{K}|\mathsf{h}}{\mathsf{H}}\right). \tag{2.40}$$

This result ensures that the average of the quantum states $\sigma_{X(k)}$ over the codebook $\mathscr{C}$ is close to the target mean state σ with high probability.

We note that the quantum soft covering lemma can be viewed as a direct consequence of quantum channel resolvability. In particular, quantum channel resolvability studies the approximation of the average output state of a quantum channel by using a randomly selected codebook. The quality of this approximation is set by the distance between the ensemble average and the target output state. The covering lemma can thus be viewed as a corollary of the general resolvability framework [74] (see also [75]).

Chapter 3

Security Under Interception

In this chapter, we present our results on security under interception. We consider secure communication with unreliable entanglement assistance, where the assistance could be intercepted by the adversary, Eve. We require correct decoding by Bob and semantic security against Eve.

The interception model is highly relevant in the current landscape of quantum communications, where entanglement is not only difficult to generate but also inherently fragile. Ensuring secure communication in such scenarios is critical to the advancement of quantum cryptography and security.

We establish an achievable rate region for communication with unreliable entanglement assistance under interception. Furthermore, we derive a multi-letter capacity formula also for the interception model for the class of degraded wiretap channels.

To demonstrate our results, we consider the erasure channel and the amplitude damping channel. For the erasure channel, we show that time-division is optimal and we derive a single-letter formula. For the amplitude damping channel, we encounter a phenomenon that is somewhat rare in network information theory [76]: Time sharing is impossible and the boundary of our achievable region is disconnected.

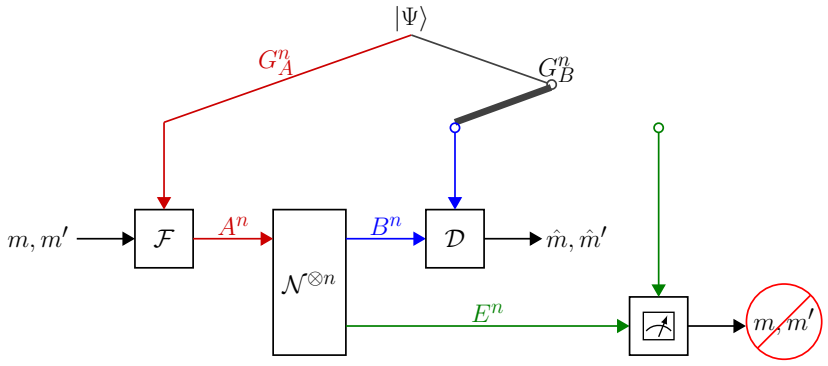
3.1 Interception Model

Before communication begins, the legitimate parties try to generate entanglement assistance. To this end, Alice prepares an entangled pair locally and transmits one particle.

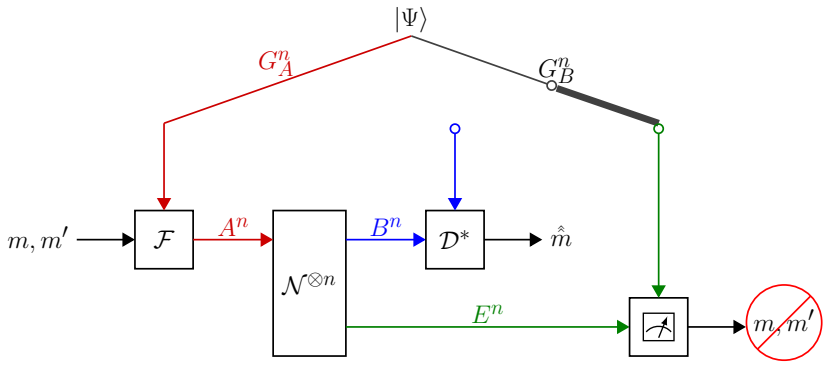
While the particle travels from the transmitter, Eve tries to steal it, hence the particle may fail to reach Bob.

In the optimistic case, Alice and Bob generate entanglement successfully prior to the transmission of information. Hence, Bob can decode the information while using the entangled resource, which is not available to Eve.

However, in the pessimistic case, Eve intercepts the assistance and Bob must decode without it. Nonetheless, secrecy needs to be maintained, whether Bob or Eve hold the entangled resource.



(a)



(b)

Figure 3.1: Interception illustration with an imaginary switch. As Eve may steal the resource, there are two scenarios: (a) "Left": Bob decodes both m and m'. (b) "Right": Bob decodes m alone.

Consider the following approach. Alice encodes two messages at rates R and R', unaware of whether Bob holds the entanglement resource or not. Whereas, Bob and Eve know whether the resource is in their possession. In practice, this is realized through heralded entanglement generation [77]. If the entangled resource is not available to Bob, then he decodes the first message alone; hence, the transmission rate is R. Whereas, given entanglement assistance, Bob decodes both messages, hence the overall rate is $R + R'$. The rate R is thus associated with information that is guaranteed to be sent, while R' with the excess information that entanglement assistance provides. In this manner, we adapt the transmission rate to the availability of entanglement assistance.

3.2 Coding Definitions

We now present the coding definitions for secure communication with unreliable entanglement assistance, under the interception model.

Before communication begins, the legitimate parties try to generate entanglement assistance. In the optimistic case, Alice and Bob have entanglement resources, G_A^n and

G_B^n, respectively (see Figure 3.1(a)). However, G_B^n is not necessarily available to Bob, due interception.

In the communication phase, Alice sends n inputs through a memoryless quantum wiretap channel $\mathcal{N}_{A\to BE}$, while she is unaware of whether Bob has the entanglement resource. Nevertheless, based on the common use of heralded entanglement generation in practical systems [77], we assume that Bob knows whether he has the assistance or not.

3.2.1 Coding with Unreliable Assistance

Definition 3.2.1. A $(2^{nR}, 2^{nR'}, n)$ secrecy code with unreliable entanglement assistance under interception consists of the following:

- Two message sets $\{1,\dots,2^{nR}\}$ and $\{1,\dots,2^{nR'}\}$, where 2^{nR} and $2^{nR'}$ are assumed to be integers.
- A pure entangled state $\Psi_{G_A^n,G_B^n}$.
- A collection of encoding maps $\mathcal{F}^{(m,m')}_{G_A^n\to A^n} : \mathscr{S}(\mathcal{H}_{G_A^n}) \to \mathscr{S}(\mathcal{H}_A^{\otimes n})$ for $m \in \{1,\dots,2^{nR}\}$ and $m' \in \{1,\dots,2^{nR'}\}$.
- Two decoding POVMs $\mathcal{D}_{B^nG_B^n} = \{D_{m,m'}\}$ and $\mathcal{D}^*_{B^n} = \{D^*_m\}$.

We denote the code by $(\Psi, \mathcal{F}, \mathcal{D}, \mathcal{D}^*)$.

The communication scheme is depicted in Figure 3.1. Alice selects two messages, $m \in \{1,\dots,2^{nR}\}$ and $m' \in \{1,\dots,2^{nR'}\}$. In addition, Alice holds the resource G_A^n. She prepares the input state by applying the encoding map,

$$\rho^{m,m'}_{A^nG_B^n} = \left(\mathcal{F}^{(m,m')}_{G_A^n\to A^n} \otimes \mathrm{id}\right)\left(\Psi_{G_A^nG_B^n}\right), \tag{3.1}$$

and transmits A^n through n uses of the quantum wiretap channel. The channel output of Bob and Eve is

$$\rho^{m,m'}_{B^nE^nG_B^n} = (\mathcal{N}^{\otimes n}_{A\to BE} \otimes \mathrm{id})(\rho^{m,m'}_{A^nG_B^n}). \tag{3.2}$$

Bob receives B^n. As opposed to Alice, both Bob and Eve know whether they hold G_B^n or not (thanks to heralded entanglement generation). Depending on the availability of the entanglement assistance, he decides whether to decode both messages or only the guaranteed information. Given entanglement assistance, Bob has access to G_B^n, in which case he performs a measurement using the POVM $\mathcal{D}_{B^nG_B^n} = \{D_{m,m'}\}$ to recover both messages. If Eve intercepts the assistance, then Bob recovers the message m alone, using the POVM $\mathcal{D}^*_{B^n} = \{D^*_m\}$.

Bob is required to decode correctly the guaranteed information m, whether the entanglement resource is stolen or not. Whereas, Bob only needs to decode the excess

information m' if the entanglement was stolen and thus not available to him. In both cases, Alice and Bob need to maintain full secrecy from Eve.

3.2.2 Correct Decoding Criteria

Since there are two scenarios in our setting, we also have two error criteria. In the presence of entanglement assistance, Bob decodes with $\mathcal{D}_{B^n G_B^n} = \{D_{m,m'}\}$. Hence, the conditional probability of error given that Alice sent the messages m and m' is:

$$\begin{aligned} P_e^{(n)}(\Psi, \mathcal{F}, \mathcal{D}|m, m') &= 1 - \mathrm{Tr}\left\{ D_{m,m'}\, \rho_{B^n G_B^n}^{m,m'} \right\} \\ &= 1 - \mathrm{Tr}\left\{ D_{m,m'} (\mathcal{L}_{A\to B}^{\otimes n} \otimes \mathrm{id})(\mathcal{F}_{G_A^n \to A^n}^{(m,m')} \otimes \mathrm{id})(\Psi_{G_A^n, G_B^n}) \right\} . \end{aligned} \tag{3.3}$$

In the absence of entanglement assistance, Bob decodes with $\mathcal{D}^*_{B^n} = \{D_m\}$, and the conditional error probability is:

$$\begin{aligned} P_e^{*(n)}(\Psi, \mathcal{F}, \mathcal{D}^*|m, m') &= 1 - \mathrm{Tr}\left\{ D_m^*\, \rho_{B^n}^{m,m'} \right\} \\ &= 1 - \mathrm{Tr}\left\{ D_m^* (\mathcal{L}_{A\to B}^{\otimes n} \circ \mathcal{F}_{G_A^n \to A^n}^{(m,m')})(\Psi_{G_A^n}) \right\} . \end{aligned} \tag{3.4}$$

Notice that both probabilities depend on m and m', since Alice does not know whether the assistance is available to Bob or not, so she encodes both messages.

Next, define the maximal probabilities of error as:

$$P_{e,\max}^{(n)}(\Psi, \mathcal{F}, \mathcal{D}) = \max_{m,m'} P_e^{(n)}(\Psi, \mathcal{F}, \mathcal{D}|m, m') , \tag{3.5}$$

$$P_{e,\max}^{*(n)}(\Psi, \mathcal{F}, \mathcal{D}^*) = \max_{m,m'} P_e^{*(n)}(\Psi, \mathcal{F}, \mathcal{D}^*|m, m') . \tag{3.6}$$

3.2.3 Security Criteria Under Interception

Suppose that Eve may steal the entanglement resource G_B^n. In the pessimistic case, Eve intercepts the entanglement resource, and Bob decodes without it. In other words, Alice and *Eve* share the entanglement, instead of Bob. See Figure 3.1(b).

Semantic security requires that Eve cannot gain any information on Alice's message, regardless of the message distribution. Hence, the state of Eve's resources needs to be close to a *constant state* that does not depend on Alice's messages. Formally, define the security level under interception, with respect to a constant state $\theta_{E^n G_B^n}$, by

$$\Delta_{\mathrm{SI}}(\Psi, \mathcal{F}, \theta_{E^n G_B^n}) = \max_{m,m'} \frac{1}{2} \left\| \rho_{E^n G_B^n}^{m,m'} - \theta_{E^n G_B^n} \right\|_1 . \tag{3.7}$$

Notice that we include the entangled resource G_B^n in the indistinguishability criterion due to the pessimistic case above.

The notion of SI denotes security under interception.

3.2.4 Capacity Region

Definition 3.2.2. A $(2^{nR}, 2^{nR'}, n, \epsilon, \delta)$ secrecy code with unreliable entanglement assistance under interception satisfies

$$\max\left(P_{e,\max}(\Psi, \mathcal{F}, \mathcal{D}), P^*_{e,\max}(\Psi, \mathcal{F}, \mathcal{D}^*)\right) \leq \epsilon \tag{3.8}$$

and

$$\Delta_{\text{SI}}(\Psi, \mathcal{F}, \theta_{E^n G_B^n}) \leq \delta \tag{3.9}$$

for some $\theta_{E^n G_B^n}$.

A rate pair (R, R') is called achievable if $\forall\ \epsilon, \delta > 0$ and sufficiently large n, there exists a $(2^{nR}, 2^{nR'}, n, \epsilon, \delta)$ code.

The secrecy capacity region with unreliable entanglement assistance under interception is the closure of the set of all such pairs, and we deonte it by $C_{\text{SI-EA}^*}(\mathcal{N})$, where SI is security under interception, and EA* denoted unreliable entanglement assistance.

3.2.5 Remarks

Heralded Entanglement Generation

In practical implementations, heralded entanglement generation allows Bob to reliably determine whether entanglement has been successfully established. Therefore, the assumption that Bob is aware of the presence or absence of the entangled resource is well-justified. In optical communication settings, *heralded entanglement* [77, 78] involves both Alice and Bob locally creating an entangled photon or spin-photon pair (as illustrated in Figure 3.2). These pairs are denoted by $|\Phi_{G_A P_A}\rangle$ and $|\Phi_{G_B P_B}\rangle$, where P_A and P_B refer to the respective photons. To generate entanglement, Alice sends her photon P_A to Bob. If the transmission is successful, Bob receives both P_A and P_B, enabling him to perform a Bell-state measurement. The successful measurement collapses the photonic systems while projecting the remaining quantum systems G_A and G_B into an entangled state. If the photon fails to arrive, the measurement outcome indicates this failure.

Security of Excess Message

A straightforward method to leverage entanglement assistance is to first generate a shared secret key, and then use it to encrypt the message via a one-time pad protocol. However, this approach poses a security risk in the interception model: if Eve intercepts the entanglement resource, she also obtains Alice's key, resulting in a complete breach of secrecy.

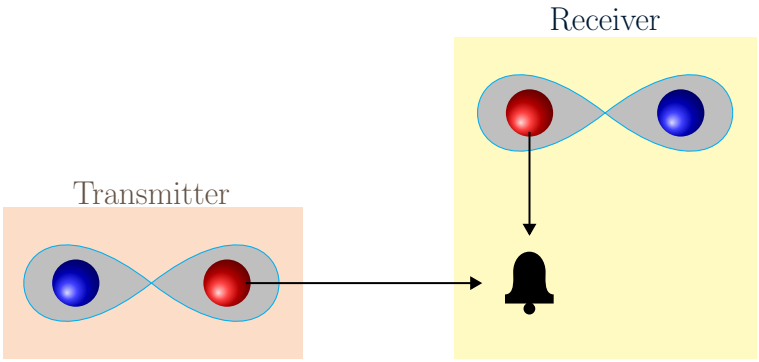


Figure 3.2: Heralded entanglement generation in optical systems.

Eve's Interception Consequences

Eve's interception has severe consequences on entanglement-assisted communication. For example, suppose that Alice uses the super dense coding protocol to encode two classical bits, and then transmits her qubit via a quantum erasure channel. Consider the event that Bob receives an erasure, hence Eve receives the transmitted qubit. Nevertheless, without the entanglement resource, there is no leakage, because each qubit by itself has no correlation with Alice's messages. On the other hand, if Eve has both qubits, then she can use the super dense decoder in order to recover Alice's bits.

Hard Decision Approach

Our model considers two extreme scenarios, i.e., the entanglement resources are either entirely available to Bob or not at all. In digital communications, this strategy aligns with a *hard decision* approach [79]. Indeed, the decoder in our setting makes a hard decision on whether the entanglement resources are viable. This approach fundamentally differs from noisy entanglement models that ensure reliability with respect to the average state [80].

Correlation Between Guaranteed Information and Entanglement Resource

We observe that guaranteed information could have correlation with the receiver's entanglement resource. Indeed, the guaranteed information m needs to be encoded in such a manner that Bob could recover it even in the absence of the entanglement resource, see Figure 3.1(b). Nevertheless, Alice encodes *her* resource G_A^n using an encoding map that depends on both m and m' (the details will be given in Sec. 5.1). As a result, the encoding operation may induce correlation between the guaranteed information m and the entangled resource G_B^n. We will see the consequences of this observation on the rate region formula.

3.3 Results

We consider communication with unreliable entanglement assistance under interception. Recall that Alice does not know whether the entanglement resource has reached Bob's location, hence she encodes two messages, at rates R and R'. If entanglement assistance is available to Bob, he recovers both messages. Yet, if Eve has stolen the resource, he recovers the first message alone. Nonetheless, we require the information to be secret from Eve in both scenarios (see security requirement in (3.7)).

First, we establish an achievable secrecy rate region. Let $\mathcal{N}_{A\to BE}$ be a quantum wiretap channel. Define

$$R_{\text{SI-EA}^*}(\mathcal{N}) \equiv \bigcup_{p_X,\varphi_{G_1G_2},\mathcal{F}^{(x)}} \left\{ \begin{array}{c} (R,R') \,:\, R \le [I(X;B)_\omega - I(X;EG_2)_\omega]_+ \\ R' \le [I(G_2;B|X)_\omega - I(G_2;E|X)_\omega]_+ \end{array} \right\} \tag{3.10}$$

where $[x]_+ \equiv \max(x,0)$. The union is over all auxiliary variables $X \sim p_X$, bipartite states $\varphi_{G_1G_2}$, and encoding channels $\mathcal{F}^{(x)}_{G_1\to A}$, hence

$$\omega_{XG_2A} \equiv \sum_{x\in\mathcal{X}} p_X(x)\,|x\rangle\langle x| \otimes (\text{id}\otimes\mathcal{F}^{(x)}_{G_1\to A})(\varphi_{G_2G_1})\,, \tag{3.11}$$

$$\omega_{XG_2BE} \equiv (\text{id}\otimes\text{id}\otimes\mathcal{N}_{A\to BE})(\omega_{XG_2A})\,. \tag{3.12}$$

Remark. While the setting resembles layered secrecy broadcast models [81, 82], the analysis is much more involved, and the formulas have a different form. Specifically, instead of the mutual information term $I(X;E)_\omega$ in the private information formula, we now have $I(X;EG_2)_\omega$ that includes the receiver's entanglement resource, cf. (2.19) and (3.10).

Remark. Based on the model description, it may seem at a first glance as if X should not be correlated with G_2, since the guaranteed information needs to be recovered in the absence of the entanglement resource. However, as pointed out in Sec. 3.2.5, Alice's encoding may induce correlation between the guaranteed information and the receiver's resource. Similarly, in the rate region formula, the application of the encoding channel $\mathcal{F}^{(x)}_{G_1\to A}$ could create correlation between X and G_2 (see (3.11)).

3.3.1 General Channels

Our main result, for general quantum wiretap channels, is given in the theorem below.

Theorem 3.1. *The region $R_{\text{SI}-\text{EA}^*}(\mathcal{N})$ is achievable with unreliable entanglement assistance under interception. That is, the capacity region is bounded by*

$$C_{\text{SI}-\text{EA}^*}(\mathcal{N}) \supseteq R_{\text{SI}-\text{EA}^*}(\mathcal{N})\,. \tag{3.13}$$

The proof of Theorem 3.1 is given in Sec. 5.1. We modify the quantum superposition coding (SPC) scheme in [7] by inserting local randomness elements that are used in the encoding, one for each message, in order to confuse Eve. In the analysis, we use the quantum covering lemma [73] in a non-standard manner. In addition, our proof modifies the methods of Cai [83, 12], originally applied to multiple-access channels (without secrecy), using random message permutations.

Remark. In the coding scheme described in Sec. 3.2, we specified that Bob applies one of two distinct POVMs, depending on who holds the entanglement resource — Bob or Eve. If Bob has entanglement assistance, then he performs $\mathcal{D}_{B^n G_B^n}$ to decode both m and m'. Otherwise, if Eve has sabotaged his assistance, Bob performs $\mathcal{D}^*_{B^n}$ to decode m alone. Nonetheless, the quantum SPC scheme [7] employs a sequential decoder. On the first stage, Bob performs a measurement to obtain an estimate for the guaranteed message m. Then, Bob moves on to the second stage. In the presence of the entanglement resource, Bob performs a second measurement to estimate the excess message m', and in the absence of his resource, he aborts. The gentle measurement lemma [84, 85] guarantees that there is no collapse after the first measurement, i.e., the output state remains nearly unchanged.

3.3.2 Degraded Channels

For the class of degraded channels, we establish a multi-letter capacity formula.

Theorem 3.2. *Let $\mathcal{N}_{A\to BE}$ be a degraded quantum wiretap channel. The capacity region with unreliable entanglement assistance under interception satisfies*

$$C_{\text{SI}-\text{EA}^*}(\mathcal{N}) = \bigcup_{n=1}^{\infty} \frac{1}{n} R_{\text{SI}-\text{EA}^*}(\mathcal{N}^{\otimes n})\,. \tag{3.14}$$

The proof of Theorem 3.2 is given in Sec. 5.2.

3.4 Examples

3.4.1 Amplitude Damping Channel

Consider the amplitude damping channel, specified by the input-output relation:

$$\mathcal{L}_{A\to B}(\rho) = K_0 \rho K_0^\dagger + K_1 \rho K_1^\dagger\,, \tag{3.15}$$

$$\text{with } K_0 = |0\rangle\langle 0| + \sqrt{1-\gamma}\,|1\rangle\langle 1|\ ,\ K_1 = \sqrt{\gamma}\,|0\rangle\langle 1|\ , \tag{3.16}$$

where $\gamma \in \left[0, \frac{1}{2}\right]$.

The amplitude damping channel has a Stinespring representation, such that the complementary channel, from Alice to Eve, is an amplitude damping channel as well,

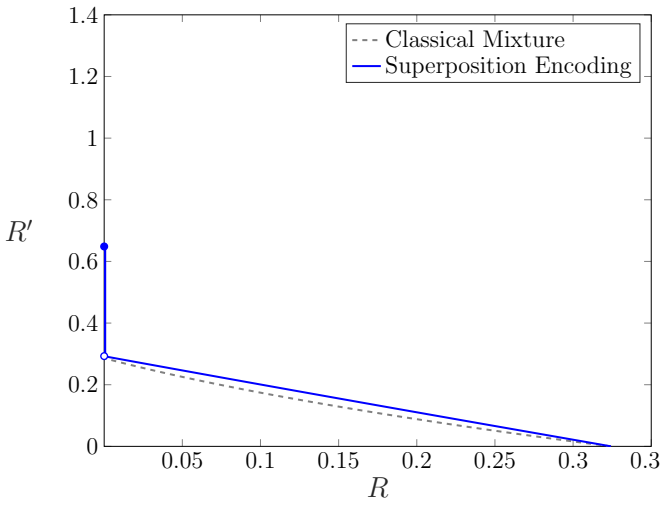


Figure 3.3: Achievable rate region for the amplitude damping channel with unreliable entanglement assistance under interception, for $\gamma = 0.3$.

with a parameter $(1-\gamma)$ [86, Sec. II-A]. The amplitude damping channel is degraded. The secrecy capacity of the channel, without assistance, is given by $C_{\mathrm{S}}(\mathcal{N}) = \max_{q\in[0,1]} h_2((1-\gamma)q) - h_2(\gamma q)$ (see [86, Eq.(36)]). The entanglement-assisted capacity, without secrecy, is given by $C_{\mathrm{EA}}(\mathcal{L}) = \max_{p\in[0,1]} h_2(p) + h_2((1-\gamma)p) - h_2(\gamma p)$ (see [86, Eq. (38)]), and it can be achieved with a state of the form $|\phi_1\rangle = \sqrt{1-p}\,|0\rangle \otimes |0\rangle + \sqrt{p}\,|1\rangle \otimes |1\rangle$.

We numerically compute achievable regions for each setting, using the following ensemble. Define $|u_\beta\rangle = \sqrt{1-\beta}\,|0\rangle\,|0\rangle + \sqrt{\beta}\,|\phi_1\rangle$, and set $|\phi_{G_1G_2}\rangle = \frac{1}{\||u_\beta\rangle\|}\,|u_\beta\rangle$, $p_X = (1-q, q)$, and $\mathcal{F}^{(x)}(\rho) = \Sigma_X^x \rho \Sigma_X^x$, $x \in \{0,1\}$, where Σ_X is the Pauli bit-flip operator. We note that $\beta = 0$ yields the optimal choice without assistance, whereas $\beta = 1$ is optimal when entanglement assistance is available reliably.

The resulting achievable region for the interception model, is indicated by the solid blue line in Figure 3.3. For comparison, the dashed line indicates the region that is achieved through a classical mixture of optimal strategies, for communication with and without entanglement assistance. We observe that time division is impossible because the use of entanglement can lead to a leakage of guaranteed information. As can be seen in Figure 3.3, the point $(R, R') = (0, 0.648)$ is disconnected from the set of boundary points for which $R > 0$.

3.4.2 Erasure Channel

Consider the qubit erasure channel, specified by

$$\mathcal{L}_{A\to B}(\rho) = (1-\epsilon)\rho + \epsilon\,|e\rangle\langle e|\ , \tag{3.17}$$

where $|e\rangle$ is an erasure state that is orthogonal to the qubit space and $\epsilon \in \left[0, \frac{1}{2}\right]$. The channel has the following isometric extension,

$$\mathcal{N}_{A\to BE}(\rho) = V\rho V^\dagger\,, \tag{3.18}$$

where the isometry $V : \mathcal{H}_A \to \mathcal{H}_B \otimes \mathcal{H}_E$ is given by $V = \sqrt{1-\epsilon}\mathbb{1}_{A\to B} \otimes |e\rangle_E + \sqrt{\epsilon}\mathbb{1}_{A\to E} \otimes |e\rangle_B$. The erasure channel is degraded as well.

The capacity of the quantum erasure channel without entanglement assistance and without secrecy constraints is given by $C(\mathcal{N}) = 1-\epsilon$ [87]. When entanglement assistance is available, the entanglement-assisted capacity increases to $C_{\mathrm{EA}}(\mathcal{N}) = 2(1-\epsilon)$ [17]. Under secrecy constraints and without assistance, the secrecy capacity drops to $C_{\mathrm{S}}(\mathcal{N}) = 1-2\epsilon$ [21, Proposition. 24.7.1]. In the setting with secrecy constraints and entanglement assistance, the capacity becomes $C_{\text{SI-EA}}(\mathcal{N}) = 2(1-2\epsilon)$.

In our model of security with unreliable entanglement assistance under interception, we obtain a single-letter capacity characterization. The capacity in this case can be achieved through atime-division strategy, dividing the block between two secure schemes, either completely relying on entanglement assistance, or not at all. Thereby, there is no gain beyond the straightforward time-sharing approach.

Theorem 3.3. *Time division is optimal for the qubit erasure channel with unreliable entanglement assistance and security under interception, i.e,*

$$C_{\mathrm{SI-EA}^*}(\mathcal{N}) = \bigcup_{0\le\lambda\le 1} \left\{ \begin{array}{rcl} (R,R') : R \le & (1-\lambda)(1-2\epsilon) \\ R' \le & 2\lambda(1-2\epsilon) \end{array} \right\}. \tag{3.19}$$

Proof. Achievability follows by a classical mixture of the optimal strategies, with and without entanglement assistance. That is, set $|\phi_{G_1G_2}\rangle$ to be an EPR state, $p_X = (1-\lambda,\lambda)$, and $\mathcal{F}^{(x)}(\rho)$ as in the previous example. To show the converse part, let $(R,R') \in \frac{1}{n}R_{\text{SI-EA}*}(\mathcal{N}^{\otimes n})$, and let Z be an erasure flag. We have

$$\begin{aligned} R &\le \frac{1}{n}(I(X;B^n)_\omega - I(X;E^nG_2^n)_\omega) \\ &= \frac{1}{n}(I(X;B^n|Z)_\omega - I(X;E^nG_2^n|Z)_\omega) \\ &= \frac{1}{n}((1-\epsilon)I(X;A^n)_\omega - \epsilon I(X;A^nG_2^n)_\omega) \\ &\le \frac{1}{n}(1-2\epsilon)I(X;A^n)_\omega \\ &\le (1-2\epsilon)\left(1 - \frac{1}{n}H(A^n|X)_\omega\right). \end{aligned} \tag{3.20}$$

The first inequality follows from Theorem 3.2, using the fact that the erasure channel is degraded, allowing for a multi-letter secrecy capacity formula. The first equality follows from the fact that there are isometries mapping B^n and E^n to B^nZ and E^nZ,

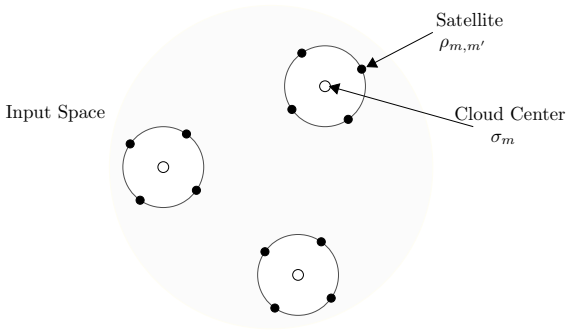


Figure 3.4: Quantum superposition coding.

respectively. The second equality follows from the definition of the erasure channel, and because when there is an erasure, X is independent of the erasure state. The second inequality holds because mutual information is non-negative. The last inequality is due to the fact that $I(X;A^n)_\omega = H(A^n)_\omega - H(A^n|X)_\omega \leq n - H(A^n|X)_\omega$.

Similarly,

$$R' \leq \frac{1}{n}(1-2\epsilon)I(G_2^n;A^n|X)_\omega \leq \frac{1}{n}(1-2\epsilon)2H(A^n|X)_\omega \,. \tag{3.21}$$

The first inequality follows from the same initial steps as the former, and the second holds since $I(A;B)_\rho \leq 2H(A)_\rho$ in general. The converse part follows by defining $\lambda \equiv \frac{1}{n}H(A^n|X)_\omega$.

3.5 Discussion

3.5.1 Operational Meaning of Interception

At a first glance, the assumption in the model of Qi et al. [6], presented in Sec. 2.5, that Eve has access to the receiver's entangled resource may appear to contradict the no-cloning theorem, which prohibits the duplication of an unknown quantum state [70]. However, this assumption can be given operational meaning through our interception model. In our setting, Eve's access to the entanglement is interpreted as an interception: either Bob or Eve possesses the entangled share, but not both. This interpretation avoids any violation of the no-cloning principle and provides a physical justification for the scenario considered by Qi et al. [6]. The capacity in their model can thus be interpreted as the maximal value of the excess rate, i.e.,

$$C_{\text{SI-EA}}(\mathcal{N}) \equiv \max\left\{R' \,:\, (0,R') \in C_{\text{SI-EA}*}(\mathcal{N})\right\} .$$

3.5.2 Quantum Superposition Coding Technique

The analysis modifies the quantum superposition coding (SPC) scheme from [7]. The quantum SPC scheme was inspired by the classical SPC technique [88, 22]. Originally, the classical SPC scheme consists of a collection of sequences $u^n(m)$ and $v^n(m')$, where m and m' are messages that are associated with different users in a multi-user network. In this scheme, the sequences $u^n(m)$ are referred to as cloud centers, while $v^n(m')$ are displacement vectors. The resulting codewords, denoted as $c^n(m, m') = u^n(m)+v^n(m')$ are referred to as satellites.

In analogy, quantum SPC [7] uses quantum operations that map quantum cloud centers to quantum satellite states. Suppose that Alice and Bob share an entangled state ϕ a priori. Each cloud center is associated with a classical sequence $x^n(m)$, and at the center of each cloud there is a state, $\sigma_m = \mathcal{F}^{(x^n(m))}(\phi)$, where $\mathcal{F}^{(x^n(m))}$ is a quantum encoding map that is conditioned on $x^n(m)$. Applying random Pauli operators that encode the message m' takes us from the cloud center to a satellite $\rho_{m,m'}$ on the cloud that depends on both messages, m and m'. The channel input is thus the satellite state. See Figure 3.4. Bob decodes in two steps.

Initially, Bob aims to recover the cloud, i.e., he estimates the message m. If the entanglement resource is unavailable to Bob at this stage, the decoding process concludes after the first step. However, if Bob has access to entanglement assistance, he proceeds to the second step to decode the satellite associated with message m'. It was later shown that quantum SPC is optimal for entanglement-breaking quantum channels with unreliable entanglement assistance [57].

In our model, Alice inserts local randomness elements k and k' to confuse Eve. Effectively, she encodes the pair (m, k) and (m', k'), instead of m and m', respectively. Hence, the analysis in the secure setting is more involved compared to the basic quantum SPC from [7].

3.5.3 Semantic Security and Maximal Error Criterion

Our model imposes two stringent requirements: semantic security and the maximal error criterion. These are notably stronger than the more common standards in classical and quantum information theory. In particular, most achievability results are typically derived under the average error probability criterion [21, 4, 89], which allows for more tractable analysis using random coding arguments and expectation bounds. By contrast, maximal error probability requires reliable decoding uniformly over all messages and is generally more challenging to satisfy. The requirement of semantic security further strengthens the confidentiality guarantee beyond standard security notions, ensuring indistinguishability of message distributions. Consequently, our results establish a stronger form of security and reliability compared to traditional frameworks.

Chapter 4

Security Under Passive Eavesdropping

In this chapter, we present our results on security under passive eavesdropping. We consider secure communication with unreliable entanglement assistance, where the assistance is unreliable because it may be lost to the environment. However, as opposed to the interception model, the eavesdropper in this setting does not have access to the lost entanglement. This model resembles scenarios in quantum key distribution (QKD) settings where not all losses are attributed to the eavesdropper, as addressed by Graifer et al. [90].

We establish a regularized capacity formula for general quantum wiretap channels. This stands in contrast to the interception model, where we derived a regularized capacity formula only for the class of degraded channels.

To demonstrate our results, we analyze the quantum erasure channel and the amplitude damping channel. For the erasure channel, we show that time-division is optimal and derive a single-letter formula. For the amplitude damping channel, we present an achievable region that outperforms time-division.

4.1 Passive Model

We consider secure communication with unreliable entanglement assistance, under the assumption that Eve is passive and cannot intercept the entangled resource. In this model, the entanglement assistance is unreliable because it may be lost to the environment.

The coding strategy mirrors that of the interception model. Alice encodes two messages, at rates R and R', without knowing whether Bob has access to the entanglement resource. In contrast, Bob knows whether the resource is available to him.

If the entangled resource is unavailable, Bob decodes only the first message, achieving a rate of R. Whereas, if the entanglement is available, Bob decodes both messages, attaining a total rate of $R+R'$. The rate R thus corresponds to guaranteed information,

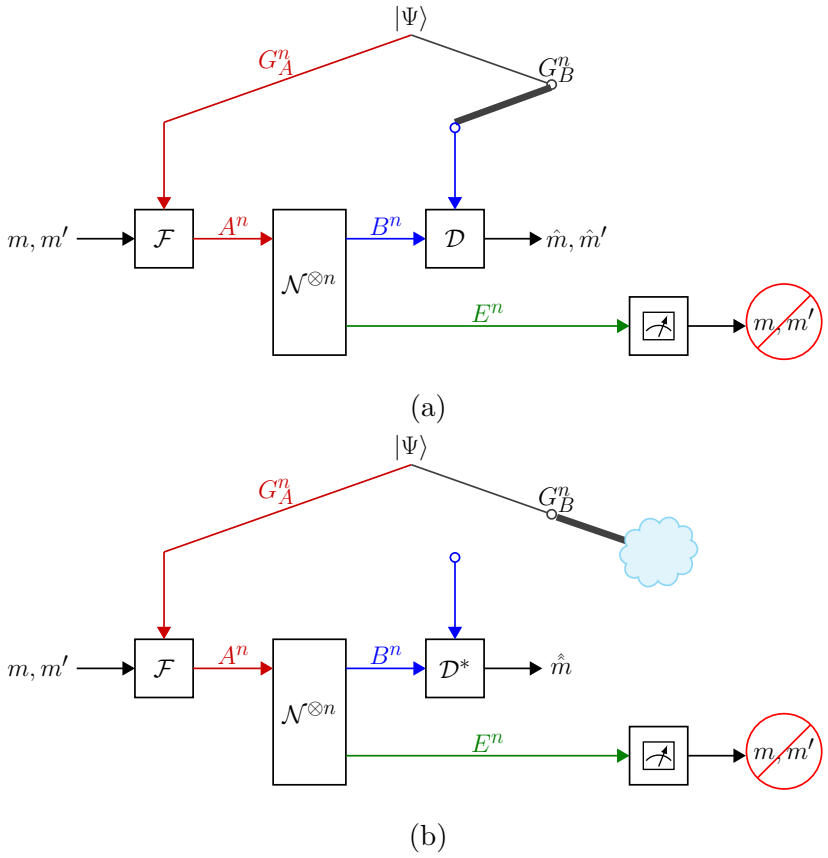


Figure 4.1: Unreliable entanglement assistance under the passive model, where the resource may get lost to the environment. We model this with an imaginary switch. There are two scenarios: (a) "Left": Bob decodes both m and m'. (b) "Right": Bob decodes m alone.

while R' represents the excess information enabled by entanglement assistance. In this way, the communication rate is adapted to the presence or absence of entanglement assistance.

4.2 Coding Definitions

We now present the coding definitions for secure communication with unreliable entanglement assistance, under the model of a passive eavesdropper. The definitions closely follow those of the interception model, with the key difference being the security requirement. In this model, the pessimistic case assumes that the entanglement assistance is unavailable to both Bob and Eve. Consequently, neither party can use the entanglement resource to decode the message, which simplifies the security condition compared to the interception scenario.

4.2.1 Coding with Unreliable Assistance

Before communication begins, the legitimate parties try to generate entanglement assistance. In the optimistic case, Alice and Bob have entanglement resources, G_A^n and G_B^n, respectively (see Figure 4.1(a)). However, in the pessimistic case, the assistance gets lost to the environment (see Figure 4.1(b)).

Definition 4.2.1. A $(2^{nR}, 2^{nR'}, n)$ secrecy code with unreliable entanglement assistance under the passive-eavesdropper model consists of:

- Two message sets $\{1, \ldots, 2^{nR}\}$ and $\{1, \ldots, 2^{nR'}\}$, where 2^{nR} and $2^{nR'}$ are assumed to be integers.
- A pure entangled state $\Psi_{G_A^n, G_B^n}$.
- A collection of encoding maps $\mathcal{F}_{G_A^n \to A^n}^{(m,m')} : \mathscr{S}(\mathcal{H}_{G_A^n}) \to \mathscr{S}(\mathcal{H}_A^{\otimes n})$ for $m \in \{1, \ldots, 2^{nR}\}$ and $m' \in \{1, \ldots, 2^{nR'}\}$.
- Two decoding POVMs $\mathcal{D}_{B^n G_B^n} = \{D_{m,m'}\}$ and $\mathcal{D}_{B^n}^* = \{D_m^*\}$.

We denote the code by $(\Psi, \mathcal{F}, \mathcal{D}, \mathcal{D}^*)$.

As in Section. 3.2, Alice prepares

$$\rho_{A^n G_B^n}^{m,m'} = (\mathcal{F}_{G_A^n \to A^n}^{(m,m')} \otimes \mathrm{id})(\Psi_{G_A^n G_B^n}),$$

sends A^n through $\mathcal{N}_{A \to BE}^{\otimes n}$ to obtain $\rho_{B^n E^n G_B^n}^{m,m'}$, and Bob receives B^n (and G_B^n only if the assistance was not lost).

4.2.2 Decoding and Error Criteria

Bob's two decoding strategies and their error probabilities $P_{e,max}^{(n)}(\Psi, \mathcal{F}, \mathcal{D})$ and $P_{e,max}^{*(n)}(\Psi, \mathcal{F}, \mathcal{D}^*)$ are identical to (3.5) and (3.6), respectively.

4.2.3 Security Criteria Under Passive Eavesdropper

The passive model assumes that Eve does not gain access to the resource G_B^n. In the pessimistic case, the entanglement resource is lost to the environment, and neither Bob nor Eve can benefit from it. See Figure 4.1(b). The security level with respect to a constant state θ_{E^n} is given by,

$$\Delta_{\mathrm{PE}}(\Psi, \mathcal{F}, \theta_{E^n}) = \max_{m,m'} \frac{1}{2} \left\| \rho_{E^n}^{m,m'} - \theta_{E^n} \right\|_1 \tag{4.1}$$

(cf. (3.7)). The security requirement for the passive model can thus be viewed as a relaxation of the one we had in the interception model.

The subscript 'PE' stands for a passive eavesdropper.

4.2.4 Capacity Region

Definition 4.2.2. A $(2^{nR}, 2^{nR'}, n, \epsilon, \delta)$ secrecy code under the passive model satisfies

$$\max\{P_{e,\max}^{(n)},\ P_{e,\max}^{*(n)}\} \leq \epsilon, \qquad \Delta_{\text{PE}}(\Psi, \mathcal{F}, \theta_{E^n}) \leq \delta$$

for some θ_{E^n}.

A rate pair (R, R') is called achievable if $\forall \epsilon, \delta > 0$ and sufficiently large n there exists a $(2^{nR}, 2^{nR'}, n, \epsilon, \delta)$ code. The secrecy capacity region with unreliable entanglement assistance under a passive eavesdropper, denoted $C_{\text{PE-EA}^*}(\mathcal{N})$, is the closure of all achievable pairs.

4.3 Results

Here, we consider the model of a passive eavesdropper, where Eve cannot intercept the assistance. The entangled resource is unreliable as it may get lost to the environment.

Define:

$$R_{\text{PE-EA}^*}(\mathcal{N}) \equiv \bigcup_{p_X, \varphi_{G_1G_2}, \mathcal{F}^{(x)}} \left\{ (R, R') : \begin{array}{rl} R \leq & [I(X;B)_\omega - I(X;E)_\omega]_+ \\ R' \leq & I(G_2;B|X)_\omega \end{array} \right\} \tag{4.2}$$

where ω_{XG_2BE} is as in (3.12).

Our main result for the passive model is given below.

Theorem 4.1. *The region $R_{\text{PE}-\text{EA}^*}(\mathcal{N})$ is achievable with unreliable entanglement assistance and a passive eavesdropper. That is, the capacity region is bounded by*

$$C_{\text{PE}-\text{EA}^*}(\mathcal{N}) \supseteq R_{\text{PE}-\text{EA}^*}(\mathcal{N})\,. \tag{4.3}$$

Furthermore, the capacity region with unreliable entanglement assistance and a passive eavesdropper satisfies

$$C_{\text{PE}-\text{EA}^*}(\mathcal{N}) = \bigcup_{n=1}^{\infty} \frac{1}{n} R_{PE\text{-}EA^*}(\mathcal{N}^{\otimes n})\,. \tag{4.4}$$

Notice that here we have a regularized formula for a general wiretap channel, and not just degraded channels (cf. Theorem 3.2 and Theorem 4.1).

The analysis follows similar steps to those in Sections 5.1-5.2, with a few simplifications arising from the relaxation of the security assumption, as Eve is not granted access to the entangled resource in this model. The full details are provided in Sec. 5.3.

Remark. In this model, Eve does not have access to the entangled resource. Hence, Alice can employ time-padding to encode the excess message m' . This method, for example, ensures that Eve cannot decode the excess message without access to the resource. As a result, the bound for R' excludes Eve's system.

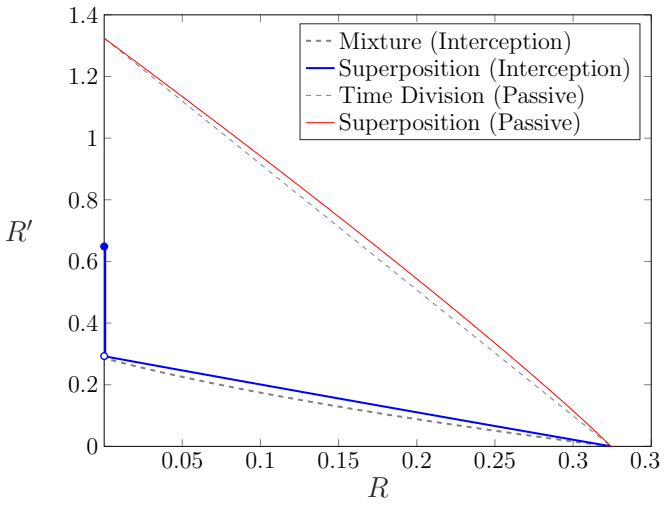


Figure 4.2: Achievable rate regions for the amplitude damping channel with unreliable entanglement assistance for $\gamma = 0.3$.

4.4 Examples

4.4.1 Amplitude Damping Channel

Consider the amplitude damping channel, along with the encoding scheme defined in Section 3.4.1.

The resulting achievable regions, for both the interception and passive models, are indicated by the solid lines in Figure 4.2, in blue and red, respectively. For comparison, the dashed lines indicate the regions that are achieved through a classical mixture of optimal strategies, for communication with and without entanglement assistance.

We observe that the achievable region under the passive model strictly contains that of the interception model. This is expected, as the security requirements are weaker in the passive case. In particular, the achievable values of R' are higher, which reflects the fact that in the passive model, the excess message m' can be securely transmitted whenever the entanglement assistance is available, without any rate penalty, as seen in (4.2).

Furthermore, while time-sharing is not possible in the interception setting, we observe that in the passive model, our coding scheme outperforms such time division, yielding a strictly larger region.

4.4.2 Erasure Channel

Consider the qubit erasure channel. In the passive model, the capacity region is also achieved by a single-letter time-sharing formula, as stated in the following theorem:

Theorem 4.2. *Time division is optimal for the qubit erasure channel with unreliable*

entanglement assistance and a passive eavesdropper, i.e,

$$C_{\mathrm{PE-EA}^*}(\mathcal{N}) = \bigcup_{0\leq\lambda\leq 1} \left\{ \begin{array}{rcl} (R, R') \,:\, R \leq & & (1-\lambda)(1-2\epsilon) \\ R' \leq & & 2\lambda(1-\epsilon) \end{array} \right\}. \tag{4.5}$$

Achievability follows by a classical mixture of the optimal strategies, the strategy for unassisted secure capacity, and the strategy for assisted capacity without a security demand. The converse follows similar arguments as in (3.20).

Chapter 5

Analysis

In this chapter, we present the proofs of the main theorems for both the interception and passive models. Section 5.1 contains the proof of Theorem 3.1, which establishes the inner bound for the interception model. Section 5.2 provides the converse proof for the degraded case (Theorem 3.2). Finally, Section 5.3 presents the proof of Theorem 4.1, corresponding to the passive model.

5.1 Proof of Theorem 3.1 (Achievability)

In this section, we prove Theorem 3.1, which establishes the inner bound on the capacity region for the interception model over general quantum wiretap channels.

Consider secure communication with unreliable entanglement assistance under interception. We show that every secrecy rate pair (R, R') in the interior of $R_{\text{SI-EA}^*}(\mathcal{N})$ is achievable. Suppose Alice wishes to send a pair of messages, $(m, m') \in \{1, \ldots, 2^{nR}\} \times \{1, \ldots, 2^{nR'}\}$. In the optimistic case, entanglement is successfully generated prior to the transmission of information, hence Bob can decode while using the entangled resource, which is not available to Eve. However, in the pessimistic case in this model, Eve intercepts the resource, in which case, Bob must decode without it.

The coding scheme modifies the quantum SPC construction from [7]. Here, we insert local randomness elements, which will be denoted in the analysis as k, k', and are used in the encoding of each message in order to confuse Eve. Our secrecy analysis relies on the quantum covering lemma [73], as stated in Lemma 2.7.1.

For semantic security, our proof modifies the methods of Cai [83, 12], originally applied to multiple-access channels (without secrecy), using random message permutations.

Before we state the proof, we make the following observations. First, we note that pure states $|\phi_{G_1G_2}\rangle$ are sufficient to exhaust the union in the rate region formula in (3.10), since G_1 can be extended to include a purifying reference system. In addition, we can restrict the proof to isometric encoding maps, $F^{(x)}_{G_1\to A}$ for $x \in \mathcal{X}$, by similar arguments as in [7]. To see this, consider using a collection of encoding channels,

$\mathcal{F}^{(x)}_{G_1\to A'}$ for $x \in \mathcal{X}$, for transmission via $\widehat{\mathcal{N}}_{A'\to BE}$. Every quantum channel $\mathcal{F}^{(x)}_{G_1\to A'}$ has a Stinespring representation, with an isometry $F^{(x)}_{G_1\to A'A_0}$. Since it is an encoding map, we may think of A_0 as Alice's ancilla. Then, let $A \equiv (A', A_0)$ be the augmented channel input. We are effectively coding over the channel $\mathcal{N}_{A\to BE}$, where $\mathcal{N}_{A\to BE}(\rho_{A'A_0}) = \widehat{\mathcal{N}}_{A'\to BE}(\mathrm{Tr}_{A_0}(\rho_{A'A_0}))$, using the isometric map $F^{(x)}_{G_1\to A}$. From this point, we will focus on the quantum wiretap channel $\mathcal{N}_{A\to BE}$ and use the isometric encoding map $F^{(x)}_{G_1\to A}$.

5.1.1 Notation

We introduce the following notation. For every $x \in \mathcal{X}$, consider the input state

$$|\psi^x_{AG_2}\rangle = (F^{(x)}_{G_1\to A} \otimes \mathbb{1})\,|\phi_{G_1G_2}\rangle\,, \tag{5.1}$$

which results in the output

$$\omega^x_{BEG_2} = (\mathcal{N}_{A\to BE} \otimes \mathrm{id})(\psi^x_{AG_2})\,. \tag{5.2}$$

Then, consider a Schmidt decomposition,

$$|\psi^x_{AG_2}\rangle = \sum_{y\in\mathcal{Y}} \sqrt{p_{Y|X}(y|x)}\,\left|\xi_{y|x}\right\rangle \otimes \left|\xi'_{y|x}\right\rangle \tag{5.3}$$

where $p_{Y|X}$ is a conditional probability distribution. We will often use the notation $|\psi^{x^n}\rangle = \bigotimes_{i=1}^n |\psi^{x_i}\rangle$.

Next, let us define a unitary operator that will be useful in the definition of our encoder. Denote the Heisenberg-Weyl operators, on a qudit of dimension d, by

$$\Sigma(a,b) = \Sigma_X^a \Sigma_Z^b\,,\ \text{for } a,b \in \{0,\ldots,d-1\}\,, \tag{5.4}$$

where $\Sigma_X = \sum_{k=0}^{d-1} |k+1 \mod d\rangle\langle k|$ and $\Sigma_Z = \sum_{k=0}^{d-1} \exp\left\{\frac{2\pi i k}{d}\right\} |k\rangle\langle k|$.

Let $x^n \in \mathcal{X}^n$ be a given sequence. For every conditional type t on $\mathcal{Y}^n$ given x^n, we will apply an operator of the form $(-1)^{c_t}\Sigma(a_t,b_t)$ for $a_t, b_t \in \{0,\ldots,d_t-1\}$ and $c_t \in \{0,1\}$, where d_t is the size of the corresponding conditional type class. Then, define the unitary

$$U(\gamma) = \bigoplus_t (-1)^{c_t}\Sigma(a_t,b_t) \tag{5.5}$$

corresponding to a vector $\gamma = ((a_t,b_t,c_t)_t)$, where the direct sum is over all conditional types. Furthermore, let Γ_{x^n} denote the set of all such vectors γ.

5.1.2 Code Construction

We now describe the construction of a secrecy code with unreliable entanglement assistance. Let $|\phi_{G_1G_2}\rangle^{\otimes n}$ be the assistance that Alice and Bob would like to share. We also

let R_0 and R'_0 denote the rates of the Alice's local random elements, where $0 < R_0 < R$ and $0 < R'_0 < R'$.

Classical Codebook Generation

Select $2^{n(R+R_0)}$ sequences independently at random,

$$\left\{x^n(m,k)\right\}_{m\in\{1,\ldots,2^{nR}\},\, k\in\{1,\ldots,2^{nR_0}\}}, \tag{5.6}$$

each i.i.d. $\sim p_X$. Then, for every m and k, select $2^{n(R'+R'_0)}$ conditionally independent sequences at random,

$$\left\{\gamma(m',k'|x^n(m,k)\right\}_{m'\in\{1,\ldots,2^{nR'}\},\, k'\in\{1,\ldots,2^{nR'_0}\}}, \tag{5.7}$$

each uniformly distributed over $\Gamma_{x^n(m,k)}$. The codebooks are publicly revealed, to Alice, Bob, and Eve.

Encoding

Alice chooses a message pair (m,m'). To ensure secrecy, Alice further selects local randomness elements, k and k', chosen uniformly at random, from $\{1,\ldots,2^{nR_0}\}$ and $\{1,\ldots,2^{nR'_0}\}$, respectively. To encode the first message m, she applies the encoding map

$$F^{(x^n)}_{G_1^n\to A^n} = \bigotimes_{i=1}^{n} F^{(x_i)}_{G_1\to A}\,, \text{ with } x^n \equiv x^n(m,k)\,, \tag{5.8}$$

on her share of the entangled state $|\phi_{G_1G_2}\rangle^{\otimes n}$. The resulting input state is $\left|\psi^{x^n}_{A^nG_2^n}\right\rangle$ (see (5.1)).

To encode the excess message m', she applies the unitary $U(\gamma)$, with $\gamma \equiv \gamma(m',k'|x^n)$. This yields the input state

$$\left|\chi^{\gamma,x^n}_{A^nG_2^n}\right\rangle = (U(\gamma)\otimes \mathbb{1})\left|\psi^{x^n}_{A^nG_2^n}\right\rangle. \tag{5.9}$$

Alice transmits A^n through n uses of the wiretap channel $\mathcal{N}_{A\to BE}$. The output is

$$\rho^{\gamma,x^n}_{B^nE^nG_2^n} = (\mathcal{N}^{\otimes n}_{A\to BE}\otimes \mathrm{id})(\chi^{\gamma,x^n}_{A^nG_2^n})\,. \tag{5.10}$$

Decoding

Bob has two decoding strategies. If Bob holds the entangled resource G_2^n, then he decodes both messages, m and m'. However, if Eve has stolen G_2^n, then Bob decodes the message m alone. Specifically, Bob decodes in two steps. First, he performs a measurement, using a POVM $\{\Lambda_{m,k}\}$, which will be described later, in order to estimate

the message m. If he has access to the entanglement resource G_2^n, then he continues to decode the message m' using a second POVM $\{\Upsilon_{m',k'}\}$, which will also be described later.

5.1.3 Code Properties

Before we go into the error analysis, we show that Alice's operations for encoding the second message m' can be effectively reflected to Bob's side.

Using the schmidt decomposition in (5.3), we have

$$\left|\psi_{A^nG_2^n}^{x^n}\right\rangle = \sum_{y^n\in\mathcal{Y}^n} \sqrt{P_{Y^n|x^n}(y^n|x^n)}\left|\xi_{y^n|x^n}\right\rangle \otimes \left|\xi'_{y^n|x^n}\right\rangle$$

for $x^n \in \mathcal{X}^n$.

Now, we can partition the sum over $y^n \in \mathcal{Y}^n$ according to conditional type classes $T_n(t|x^n)$, where $t \in \mathcal{P}_n(\mathcal{Y})$. That is, we write:

$$\begin{aligned}\left|\psi_{A^nG_2^n}^{x^n}\right\rangle &= \sum_{t\in\mathcal{P}_n(\mathcal{Y})}\sum_{y^n\in T_n(t|x^n)} \sqrt{P_{Y^n|x^n}(y^n|x^n)}\left|\xi_{y^n|x^n}\right\rangle \otimes \left|\xi'_{y^n|x^n}\right\rangle \\ &= \sum_{t\in\mathcal{P}_n(\mathcal{Y})} \sqrt{P(t|x^n)}\cdot\frac{1}{\sqrt{|T_n(t|x^n)|}}\sum_{y^n\in T_n(t|x^n)}\left|\xi_{y^n|x^n}\right\rangle \otimes \left|\xi'_{y^n|x^n}\right\rangle \\ &= \sum_{t\in\mathcal{P}_n(\mathcal{Y})} \sqrt{P(t|x^n)}\left|\Phi_t\right\rangle, \end{aligned} \tag{5.11}$$

where

$$P(t|x^n) = \sum_{y^n\in T_n(t|x^n)} P_{Y^n|x^n}(y^n|x^n), \tag{5.12}$$

$$\left|\Phi_t\right\rangle = \frac{1}{\sqrt{|T_n(t|x^n)|}}\sum_{y^n\in T_n(t|x^n)}\left|\xi_{y^n|x^n}\right\rangle \otimes \left|\xi'_{y^n|x^n}\right\rangle. \tag{5.13}$$

Note that $|\Phi_t\rangle$ is a maximally entangled state on the product of the typical subspaces associated with $T_n(t|x^n)$.

Using the ricochet property [91, Eq. (17)]

$$(U\otimes \mathrm{id})\left|\Phi_{AB}\right\rangle = (\mathrm{id}\otimes U^T)\left|\Phi_{AB}\right\rangle. \tag{5.14}$$

We can then reflect the unitary operation to the entangled resource at the receiver along with the environment:

$$\left|\chi_{A^nG_2^n}^{\gamma,x^n}\right\rangle = (\mathbb{1}\otimes U^T(\gamma))\left|\psi_{A^nG_2^n}^{x^n}\right\rangle. \tag{5.15}$$

Thus, we can write the output state as follows:

$$\begin{aligned}
&\rho^{\gamma,x^n}_{B^nE^nG_2^n} = (\mathcal{N}^{\otimes n}_{A\to BE} \otimes \mathrm{id})(\chi^{\gamma,x^n}_{A^nG_2^n}) \\
&= (\mathcal{N}^{\otimes n}_{A\to BE} \otimes \mathrm{id})((\mathbb{1} \otimes U^T(\gamma))\psi^{x^n}_{A^nG_2^n}(\mathbb{1} \otimes U^*(\gamma))) \\
&= (\mathbb{1} \otimes U^T(\gamma)) \left[(\mathcal{N}^{\otimes n}_{A\to BE} \otimes \mathrm{id})(\psi^{x^n}_{A^nG_2^n})\right] (\mathbb{1} \otimes U^*(\gamma)) \\
&= (\mathbb{1} \otimes U^T(\gamma))\omega^{x^n}_{B^nE^nG_2^n}(\mathbb{1} \otimes U^*(\gamma)) \qquad (5.16)
\end{aligned}$$

where $\omega^x_{BEG_2}$ is as in (5.2).

5.1.4 Error Analysis

We now analyze the probability for erroneous decoding by Bob, for the guaranteed message and the excess message. Let $\alpha > 0$ be arbitrarily small. We analyze the error probability in each scenario.

Eve has stolen the resource

We begin with the pessimistic case, where Bob does not have the entangled resource G_2^n, as it was stolen by Eve. Bob's reduced state is given by

$$\begin{aligned}
\rho^{\gamma,x^n}_{B^n} &= \mathrm{Tr}_{E^nG_2^n}((\mathbb{1} \otimes U^T(\gamma))\omega^{x^n}_{B^nE^nG_2^n}(\mathbb{1} \otimes U^*(\gamma))) \\
&= \omega^{x^n}_{B^n} \,. \qquad (5.17)
\end{aligned}$$

The second equality follows from trace cyclicity, as $U^*U^T = \mathbb{1}$. Observe that the state does not depend on γ. That is, the reduced output state is not affected by the encoding of m'. Therefore, based on the HSW Theorem [1, 2], there exists a decoding POVM $\mathcal{D}^*_{B^n} = \{\Lambda_{m,k}\}$ such that

$$\mathbb{E}\left[\frac{1}{2^{n(R+R')}} \sum_{m,m'} P_e^{*(n)}(\Psi, \mathcal{F}, \mathcal{D}^*|m, m')\right] \leq \alpha \,, \qquad (5.18)$$

for sufficiently large n, provided that

$$R + R_0 < I(X;B)_\omega - \epsilon_1 \,. \qquad (5.19)$$

Bob has entanglement assistance

We move to the optimistic case, where Eve has failed to intercept G_2^n, hence Bob holds the entangled resource. Based on the analysis above, Bob's first measurement recovers the correct guaranteed message m, with a high probability. In general, upon performing a measurement, it may lead to a state collapse. Denote the post-measurement state, after the first measurement, by $\tilde{\rho}^{\gamma,x^n}_{B^nG_2^n}$. According to the gentle measuring lemma [84, 85], this state is close in trace distance to the original state, before the measurement

took place, as

$$\frac{1}{2}\left\|\tilde{\rho}^{\gamma,x^n}_{B^nE^nG_2^n}-\rho^{\gamma,x^n}_{B^nE^nG_2^n}\right\|\leq 2^{-n\frac{1}{2}(I(X;B)_\omega-R-R_0-\epsilon_1)}\,, \tag{5.20}$$

which tends to zero if (5.19) holds. Hence, we may focus our error analysis on the original state, before the measurement:

$$\begin{aligned}\rho^{\gamma,x^n}_{B^nG_2^n}&=\mathrm{Tr}_{E^n}(\rho^{\gamma,x^n}_{B^nE^nG_2^n})\\&=\mathrm{Tr}_{E^n}((\mathbb{1}\otimes U^T(\gamma))\omega^{x^n}_{B^nE^nG_2^n}(\mathbb{1}\otimes U^*(\gamma)))\\&=(\mathbb{1}\otimes U^T(\gamma))\omega^{x^n}_{B^nG_2^n}(\mathbb{1}\otimes U^*(\gamma))\end{aligned} \tag{5.21}$$

where $\gamma\equiv\gamma(m',k'|x^n)$, and $\omega^{x^n}_{B^nG_2^n}=\mathrm{Tr}_{E^n}(\omega^{x^n}_{B^nE^nG_2^n})$. Based on the arguments in Appendix A.1, which are based on the quantum packing lemma in Lemma 1.8.1, there exists a POVM $\{\Upsilon_{m',k'|x^n}\}$ such that the expected error probability is bounded by

$$\mathbb{E}\left[\frac{1}{2^{n(R+R')}}\sum_{m,m'}P_e(\Psi,\mathcal{F},\mathcal{D}|m,m')\right]\leq\alpha\,, \tag{5.22}$$

for sufficiently large n, provided that

$$R'+R'_0<I(G_2;B|X)_\omega-\epsilon_2\,. \tag{5.23}$$

5.1.5 Secrecy Analysis

We note that secrecy is required whether Eve has intercepted Bob's entanglement resource G_2^n or not.

Consider Eve's joint state, including both her output and the entanglement resource, which could be in her possession. Similarly, as before, we express Eve's joint state as

$$\rho^{\gamma,x^n}_{E^nG_2^n}=(\mathbb{1}\otimes U^T(\gamma))\omega^{x^n}_{E^nG_2^n}(\mathbb{1}\otimes U^*(\gamma)) \tag{5.24}$$

where $\omega^{x^n}_{E^nG_2^n}=\mathrm{Tr}_{B^n}(\omega^{x^n}_{B^nE^nG_2^n})$ (see (5.2)).

Next, we analyze the secrecy for each of Alice's messages. Denote

$$\begin{aligned}\Delta_{m'|m,k}(\mathscr{C})&=\frac{1}{2}\left\|\frac{1}{2^{nR'_0}}\sum_{k'=1}^{2^{nR'_0}}\rho^{\gamma(m',k'|x^n),x^n}_{E^nG_2^n}-\zeta^{x^n}_{E^nG_2^n}\right\|_1,\\\Delta^*_m(\mathscr{C})&=\frac{1}{2}\left\|\frac{1}{2^{nR_0}}\sum_{k=1}^{2^{nR_0}}\omega^{x^n}_{E^nG_2^n}-\omega^{\otimes n}_{EG_2}\right\|_1,\end{aligned} \tag{5.25}$$

with $x^n\equiv x^n(m,k)$, and $\zeta^{x^n}_{E^nG_2^n}=\frac{1}{|\Gamma_{x^n}|}\sum_{\gamma\in\Gamma_{x^n}}\rho^{\gamma,x^n}_{E^nG_2^n}$.

Guaranteed information indistinguishability bound

We apply the quantum covering lemma [73], Lemma 2.7.1, with the ensemble below,

$$\{p_{X^n}(x^n), \omega^{x^n}_{E^nG_2^n}\}_{x^n \in \mathcal{X}^n}\,, \tag{5.26}$$

and the following typical projectors, $\Pi = \Pi^{(n)}_\delta(\omega_{E^nG_2^n})$ and $\Pi_{x^n} = \Pi^{(n)}_\delta(\omega_{E^nG_2^n}|x^n)$. In Appendix A.2, we show that the conditions of Lemma 2.7.1 are met for every m. Thus,

$$\Pr\left(\Delta^*_m(\mathscr{C}) > e^{-\frac{\lambda}{2}n}\right) \leq \exp\left\{-2^{n(R_0 - I(X;EG_2)_\omega - \epsilon_4)}\right\}. \tag{5.27}$$

for sufficiently large n. The last bound tends to zero in a double exponential rate, provided that

$$R_0 > I(X;EG_2)_\omega + \epsilon_4\,. \tag{5.28}$$

Excess information indistinguishability bound

Let $x^n \equiv x^n(m,k)$ be fixed. Consider the uniform ensemble,

$$\left\{p(\gamma|x^n) = \frac{1}{|\Gamma_{x^n}|}, \rho^{\gamma,x^n}_{E^nG_2^n}\right\}_{\gamma \in \Gamma_{x^n}}. \tag{5.29}$$

Using the quantum covering lemma, Lemma 2.7.1 we show in Appendix A.2 that Alice's encoding simulates the average state,

$$\zeta^{x^n}_{E^nG_2^n} = \frac{1}{|\Gamma_{x^n}|}\sum_{\gamma \in \Gamma_{x^n}} \rho^{\gamma,x^n}_{E^nG_2^n} \tag{5.30}$$

using the code projectors:

$$\begin{aligned}\Pi &= \Pi^{(n)}_\delta(\omega_{E^n}|x^n) \otimes \Pi^{(n)}_\delta(\omega_{G_2^n}|x^n)\,,\\ \Pi_\gamma &= (I \otimes U^T(\gamma))\Pi^{(n)}_\delta(\omega_{E^nG_2^n}|x^n)(I \otimes U^*(\gamma))\,.\end{aligned}$$

By Lemma 2.7.1, for every $m' \in \{1,\ldots,2^{nR'}\}$ and sufficiently large n,

$$\Pr\left(\Delta_{m'|m,k}(\mathscr{C}) > e^{-\frac{\mu}{2}n}\right) \leq \exp\left\{-2^{n(R'_0 - I(G_2;E|X)_\omega - \epsilon_5)}\right\}, \tag{5.31}$$

which tends to zero in a double exponential rate, provided that

$$R'_0 > I(E;G_2|X)_\omega + \epsilon_5\,. \tag{5.32}$$

5.1.6 De-randomization

We now show that there exists a deterministic codebook under the requirements of *average error probabilities and maximal indistinguishability*. Consider the following error events,

$$\mathcal{A}_1 = \{\frac{1}{2^{n(R+R')}} \sum_{m,m'} P_e(\mathscr{C}|m,m') > \sqrt{\alpha}\}\,, \tag{5.33}$$

$$\mathcal{A}_2 = \{\frac{1}{2^{n(R+R')}} \sum_{m,m'} P_e^*(\mathscr{C}|m,m') > \sqrt{\alpha}\}\,, \tag{5.34}$$

$$\mathcal{B} = \{\exists (m,m') : \frac{1}{2}\left\|\rho_{E^nG_B^n}^{m,m'} - \omega_{EG_2}^{\otimes n}\right\|_1 > \delta\}\,. \tag{5.35}$$

By the union bound,

$$\Pr(\mathcal{A}_0 \cup \mathcal{A}_1 \cup \mathcal{B}) \leq \Pr(\mathcal{A}_0) + \Pr(\mathcal{A}_1) + \Pr(\mathcal{B})\,. \tag{5.36}$$

By Markov's inequality, $\Pr(\mathcal{A}_j) \leq \sqrt{\alpha}$ (see (5.18), (5.22)). As for the last term, by the triangle inequality,

$$\begin{aligned}
&\frac{1}{2}\left\|\rho_{E^nG_B^n}^{m,m'} - \omega_{EG_2}^{\otimes n}\right\|_1 \\
&= \frac{1}{2}\left\|\frac{1}{2^{n(R_0+R_0')}} \sum_{k=1}^{2^{nR_0}} \sum_{k'=1}^{2^{nR_0'}} \rho_{E^nG_B^n}^{\gamma(m',k'|x^n),x^n} - \omega_{EG_2}^{\otimes n}\right\|_1 \\
&\leq \frac{1}{2}\left\|\frac{1}{2^{nR_0}} \sum_{k=1}^{2^{nR_0}} \left(\frac{1}{2^{nR_0'}} \sum_{k'=1}^{2^{nR_0'}} \rho_{E^nG_B^n}^{\gamma(m',k'|x^n),x^n} - \zeta_{E^nG_2^n}^{x^n}\right)\right\|_1 + \frac{1}{2}\left\|\frac{1}{2^{nR_0}} \sum_{k=1}^{2^{nR_0}} \zeta_{E^nG_2^n}^{x^n} - \omega_{EG_2}^{\otimes n}\right\|_1 \\
&\leq \frac{1}{2^{nR_0}} \sum_{k=1}^{2^{nR_0}} \Delta_{m'|m,k}(\mathscr{C}) + \frac{1}{2}\left\|\frac{1}{2^{nR_0}} \sum_{k=1}^{2^{nR_0}} \zeta_{E^nG_2^n}^{x^n(m,k)} - \omega_{EG_2}^{\otimes n}\right\|_1\,.
\end{aligned} \tag{5.37}$$

If we were to remove the encoding of γ, then Eve's output would have been $\omega_{E^nG_2^n}^{x^n}$, instead of $\zeta_{E^nG_2^n}^{x}$. Therefore, by trace monotonicity under quantum operations, the last trace norm is bounded by $\Delta_m^*(\mathscr{C})$ (see (5.25)). Thus,

$$\begin{aligned}
&\Pr\left(\frac{1}{2}\left\|\rho_{E^nG_B^n}^{m,m'} - \omega_{EG_2}^{\otimes n}\right\|_1 > \delta\right) \\
&\leq \Pr\left(\frac{1}{2^{nR_0}} \sum_{k=1}^{2^{nR_0}} \Delta_{m'|m,k}(\mathscr{C}) \geq \frac{\delta}{2}\right) + \Pr\left(\Delta_m^*(\mathscr{C}) > \frac{\delta}{2}\right) \\
&\leq \Pr\left(\exists k : \Delta_{m'|m,k}(\mathscr{C}) \geq \frac{\delta}{2}\right) + \exp\{-2^{n\epsilon_6}\} \\
&\leq \exp\{-2^{n\epsilon_7}\}
\end{aligned} \tag{5.38}$$

hence, $\Pr(\mathcal{B}) \leq 2^{n(R_0+R)} \cdot \exp\{-2^{n\epsilon_7}\} \leq \exp\left\{-2^{\frac{1}{2}n\epsilon_7}\right\}$, for some $\epsilon_7 > 0$ and sufficiently large n. Hence, we deduce from (5.19), (5.23), (5.28), (5.32), that there exists a deter-

ministic codebook $\mathscr{C}$ such that the message-average error and indistinguishability tend to zero, if

$$R < I(X;B)_\omega - I(X;EG_2)_\omega - \epsilon_1 - \epsilon_4\,,$$
$$R' < I(G_2;B|X)_\omega - I(G_2;E|X)_\omega - \epsilon_2 - \epsilon_5\,.$$

5.1.7 Semantic Security and Maximal Error Criteria

We now complete the analysis for the maximum criteria. The proof modifies the methods of Cai [83, 12], originally applied to multiple-access channels.

Guaranteed information (expurgation)

Consider the semi-average error probability,

$$e(m) \equiv \frac{1}{2^{nR'}} \sum_{m'=1}^{2^{nR'}} P_e(\mathscr{C}|m,m')\,. \tag{5.39}$$

Based on the analysis above, the average of $\{e(m)\}_{m=1}^{2^{nR}}$ is bounded by $\alpha^{1/2}$. Therefore, at most a fraction of $\eta = \alpha^{1/4}$ of the messages m have $e(m) > \eta$. Then, we can expurgate the worst $\eta \cdot 2^{nR}$ messages, and the corresponding codewords. The guaranteed rate of the expurgated code is $R - \frac{1}{n}\log\big((1-\eta)^{-1}\big)$, which tends to R as $n \to \infty$. Denote the expurgated message set by $\mathcal{M}_{\text{exp}}$.

Excess information (message permutation)

We now construct a new code to satisfy the maximum criteria. The transmission consists of two stages. In the first stage, Alice selects a uniform "key" $L \in \{1,\ldots,n^2\}$. Assuming $R' > 0$, Alice can send L with negligible rate loss, such that the message-average error probabilities vanish. In the second stage, Alice chooses a permutation π_L on the message set $\{1,\ldots,2^{nR'}\}$, and encodes the message pair $(m_0, m_0') = (m, \pi_L(m'))$ using the codebook $\mathscr{C}$. Bob obtains an estimate, $\hat{L}$ and $(\hat{m}_0, \hat{m}_0')$, and then declares his estimation for the original messages as $\hat{m} = \hat{m}_0$ and $\hat{m}' = \pi_{\hat{L}}^{-1}(\hat{m}_0')$.

Based on our previous analysis, the message-average error probability in the first stage is bounded by

$$\Pr\Big(\hat{L} \neq L\Big) = \frac{1}{n^2}\sum_{\ell=1}^{n^2} P_e(\mathscr{C}|1,\ell) \leq \sqrt{\alpha}\,. \tag{5.40}$$

Now, consider the second block. Let $\Pi_1,\ldots,\Pi_{n^2}$ be an i.i.d. sequence of random permutations, uniformly distributed on the permutation group on the excess message

set $\{1,\ldots,2^{nR'}\}$. Denote the random codebook by $\Pi(\mathscr{C})$. For a given m',

$$\Pr(\Pi_{\ell'}(m') = \bar{m}') = \frac{(2^{nR'}-1)!}{(2^{nR'})!} = \frac{1}{2^{nR'}} \tag{5.41}$$

for all $\bar{m}' \in \{1,\ldots,2^{nR'}\}$ and $\ell' \in \{1,\ldots,n^2\}$. Thus, for every message pair $(m,m') \in \mathcal{M}_{\text{exp}} \times \{1,\ldots,2^{nR'}\}$,

$$\begin{aligned}
&\mathbb{E}\left[P_e^{(n)}(\Pi(\mathscr{C})|m,m')\right] \\
&= \sum_{\bar{m}'} \Pr(\Pi_{\ell'}(m') = \bar{m}') P_e^{(n)}(\mathscr{C}|m,\bar{m}') \\
&= \frac{1}{2^{nR'}} \sum_{\bar{m}'} P_e^{(n)}(\mathscr{C}|m,\bar{m}') = e(m) \le \lambda\,.
\end{aligned} \tag{5.42}$$

Now, by the Chernoff bound [83, Lemma 3.1],

$$\Pr\left(\frac{1}{n^2}\sum_{l'=1}^{n^2} P_e^{(n)}(\Pi(\mathscr{C})|m.m') > 4\lambda\right) < e^{-\lambda n^2}\,. \tag{5.43}$$

Therefore, the probability that, for some (m,m'), $\frac{1}{n^2}\sum_{l'=1}^{n^2} P_e^{(n)}(\Pi(\mathscr{C})|m,m') > 4\lambda$, tends to zero in a super-exponential rate by the union bound. We deduce that there exists a realization $(\pi_1,\ldots,\pi_{n^2})$ such that

$$P_e^{(n)}(\pi(\mathscr{C})|m,m') = \frac{1}{n^2}\sum_{\ell'=1}^{n^2} P_e^{(n)}(\pi_{\ell'}(\mathscr{C})|m,m') \le 4\lambda \tag{5.44}$$

for all $(m,m') \in \mathcal{M}_{\text{exp}} \times \{1,\ldots,2^{nR'}\}$.

This completes the proof.

5.2 Proof of Theorem 3.2

Consider a degraded wiretap channel. Achievability follows from Theorem 3.1. It remains to prove the converse part for the multi-letter capacity formula in Theorem 3.2.

Suppose Alice and Bob would like to share the entangled resource $\Psi_{G_A^n G_B^n}$, yet Bob's share may be stolen by Eve. In our model, there are two scenarios. Namely, either Bob holds the entanglement resource G_B^n, or Eve, depending on whether Eve has succeeded in her attempt to steal the resource. Alice first prepares a classical maximally correlated

state,

$$\pi_{KMK'M'} = \left(\frac{1}{2^{nR}} \sum_{m=1}^{2^{nR}} |m\rangle\langle m|_M \otimes |m\rangle\langle m|_K \right) \otimes \left(\frac{1}{2^{nR'}} \sum_{m'=1}^{2^{nR'}} |m'\rangle\langle m'|_{M'} \otimes |m'\rangle\langle m'|_{K'} \right) \tag{5.45}$$

where M, K, M', and K' are classical registers, such that M and K are in perfect classical correlation, and so are M' and K'. Bob needs to recover the value of M in both cases, whether he holds the resource or Eve. Whereas, Bob need only recover M', if he holds the resource. Security requires that both M and M' are hidden from Eve, whether she intercepted G_B^n or not.

Alice applies an encoding map $\mathcal{F}_{MM'G_A^n \to A^n}$ on MM' and her share of entanglement, G_A^n. Hence, the input state is

$$\sigma_{KK'A^nG_B^n} = \mathcal{F}_{MM'G_A^n \to A^n}(\pi_{KMK'M'} \otimes \Psi_{G_A^nG_B^n}), \tag{5.46}$$

and transmits A^n through n channel uses, hence the output

$$\omega_{KK'B^nE^nG_B^n} = \mathcal{N}_{A\to BE}^{\otimes n}(\psi_{KK'A^nG_B^n}). \tag{5.47}$$

If the entanglement resource is available to Bob, then he applies a decoding channel $\mathcal{D}_{B^nG_B^n \to \hat{M}\hat{M}'}$, creating

$$\rho_{KK'\hat{M}\hat{M}'E^n} = \mathcal{D}_{B^nG_B^n \to \hat{M}\hat{M}'}(\omega_{KK'B^nG_B^nE^n}). \tag{5.48}$$

If Eve has stolen the entanglement resource, then Bob applies a decoding channel $\mathcal{D}^*_{B^n \to \tilde{M}}$, hence

$$\rho^*_{KK'\tilde{M}E^n} = \mathcal{D}^*_{B^n \to \tilde{M}}(\omega_{KK'B^nG_B^nE^n}). \tag{5.49}$$

Consider a sequence of $(2^{nR}, 2^{nR'}, n)$ codes, with vanishing errors and leakage, i.e.,

$$\frac{1}{2}\|\rho_{K\hat{M}K'\hat{M}'} - \pi_{KMK'M'}\|_1 \leq \alpha_n, \tag{5.50}$$

$$\frac{1}{2}\left\|\rho^*_{K\tilde{M}} - \pi_{KM}\right\|_1 \leq \alpha^*_n, \tag{5.51}$$

and

$$I(KK'; E^nG_B^n)_\omega \leq \beta_n \tag{5.52}$$

where α_n, α^*_n, and β_n tend to zero as $n \to \infty$. Eq. (5.52) represents a weaker form of

secrecy, yet this is sufficient for the converse part. Based on entropy continuity,

$$\left|I(K;M)_\pi - I(K;\hat{M})_{\rho^*}\right| \leq n\varepsilon_n^*\,, \tag{5.53}$$

$$\left|I(K;M'|K)_\pi - I(K;\hat{M}'|K)_\rho\right| \leq n\varepsilon_n\,, \tag{5.54}$$

where $\varepsilon_n, \varepsilon_n^* \to 0$ when $n \to \infty$ (see [7, App.C, part B]) Consider the scenario where Bob receives B^n alone, while Eve gets both E^n and G_B^n. Now,

$$\begin{aligned} nR &= I(K;M)_\pi \\ &\leq I(K;\hat{M})_{\rho^*} + n\epsilon_n^* \\ &\leq I(K;B^n)_\omega + n\epsilon_n^* \\ &\leq I(K;B^n)_\omega - I(K;E^nG_B^n)_\omega + n(\varepsilon_n^* + \beta_n) \end{aligned} \tag{5.55}$$

where the second line follows from (5.53), the third from the data processing inequality (see (5.49)), and the last from (5.52). We move to the more challenging bound, on the excess rate. Here, we use the degraded property. Consider the scenario where Bob holds both B^n and G_B^n. As before, we use (5.52) and (5.54) to show that

$$\begin{aligned} nR' &= I(K';M'|K)_\pi \\ &\leq I(K';G_B^nB^n|K)_\omega - I(K';E^nG_B^n|K)_\omega + n(\varepsilon_n + \beta_n)\,. \end{aligned}$$

We can also write this as

$$\begin{aligned} &n(R' - \varepsilon_n - \beta_n) \leq I(K'G_B^n;B^n|K)_\omega - I(K'G_B^n;E^n|K)_\omega - \\ &\left[I(G_B^n;B^n|K)_\omega - I(G_B^n;E^n|K)_\omega\right]\,. \end{aligned}$$

Due to our assumption that the quantum wiretap channel is degraded, the expression within the square brackets above is nonnegative. Thus,

$$n(R' - \varepsilon_n - \beta_n) \leq I(K'G_B^n;B^n|K)_\omega - I(K'G_B^n;E^n|K)_\omega\,. \tag{5.56}$$

To complete the regularized converse proof, set $X = K$ and $G_2 = (K', G_B^n)$ in (5.55) and (5.56), and take $n \to \infty$.

5.3 Proof of Theorem 4.1

5.3.1 Achievability

The achievability proof for the passive eavesdropper case follows the general structure of the proof from Sec. 5.1 for the interception model, except for several important simplifications and distinctions, arising from the passive nature of Eve:

Guaranteed Rate:

For the guaranteed message, the indistinguishability bound simplifies from:

$$\Delta_m^*(\mathscr{C}) = \frac{1}{2}\left\| \frac{1}{2^{nR_0}} \sum_{k=1}^{2^{nR_0}} \omega_{E^n G_2^n}^{x^n} - \omega_{EG_2}^{\otimes n} \right\|_1 \tag{5.57}$$

to:

$$\Delta_m^{\text{passive}}(\mathscr{C}) = \frac{1}{2}\left\| \frac{1}{2^{nR_0}} \sum_{k=1}^{2^{nR_0}} \omega_{E^n}^{x^n} - \omega_{E}^{\otimes n} \right\|_1 \tag{5.58}$$

Here we can apply the covering lemma in the same manner but with $\omega_{E^n}^{x^n}$, and the projectors

$$\Pi = \Pi_\delta^{(n)}(\omega_{E^n})\,, \tag{5.59}$$

$$\Pi_{x^n} = \Pi_\delta^{(n)}(\omega_{E^n|x^n})\,. \tag{5.60}$$

Hence, the bound on R_0 will be $R_0 < I(X;E)_\omega + \epsilon_5$, instead of $R_0 < I(X;EG_2)_\omega + \epsilon_5$ (See A.2). This is the cause for the different bound for the guaranteed rate R.

Excess Rate:

Since in the passive model Eve cannot have access to G_2^n, Alice and Bob can use the entangled resource to generate a shared key beforehand and ensure security automatically for the excess message. Hence, requiring additional local randmoness k' is not needed.

In the interception case, the rate R' must satisfy (see Equation (3.10)):

$$R' \leq [I(G_2;B|X)_\omega - I(G_2;E|X)_\omega]_+\,. \tag{5.61}$$

However, in the passive model, there is no $I(G_2;E|X)_\omega$ penalty, and we simply get:

$$R' \leq I(G_2;B|X)_\omega\,. \tag{4.2}$$

This is because the excess message is protected by the one-time pad, so leakage from G_2 is not a concern.

5.3.2 Converse

The converse proof for the passive model again follows a similar structure to the proof of Theorem 3.2 (Sec. 5.2), except that the main difference is that degradability of the channel is not required.

In the interception model, the converse proof for R' (Equation (5.56)) relied crucially

on the *degradedness* condition:

$$R' \leq I(K'G_B^n; B^n|K)_\omega - I(K'G_B^n; E^n|K)_\omega$$

so that the difference

$$I(G_B^n; B^n|K)_\omega - I(G_B^n; E^n|K)_\omega \geq 0$$

could be dropped (non-negative).

However, in the passive model, Eve cannot have G_B^n, so this penalty term is entirely absent. The bound on R' becomes:

$$R' \leq I(K'G_B^n; B^n|K)_\omega$$

which can be established *without assuming degradedness*.

Thus, the converse proof applies to **all** channels, and we immediately get the regularized capacity formula:

$$C_{\text{PE-EA}^*}(\mathcal{N}) = \bigcup_{n=1}^{\infty} \frac{1}{n} R_{\text{PE-EA}^*}(\mathcal{N}^{\otimes n})\,.$$

This concludes the proof sketch and technical distinction between the passive and interception models.

Chapter 6

Conclusion and Future Directions

We study secure communication with unreliable entanglement assistance. Alice wishes to send a secret message to Bob, while exploiting pre-shared entanglement assistance. In our setting, the assistance is *unreliable* due to one of two reasons: Interception or loss. In the interception model, Eve may steal the entanglement assistance (see Figure 3.1(b)). Whereas, loss implies that Eve is passive and the assistance may get lost to the environment (see Figure 4.1(b)). Our present work continues the line of research that started with [7] and [57] on unreliable entanglement assistance. However, the previous works [7, 57] did not include security concerns.

Here, we derive achievable rate regions for both the interception and loss models, under a maximal error criterion and semantic security requirements. Furthermore, for the interception model, we establish a multi-letter capacity formula for the special case of degraded channels, while in the passive model, a multi-letter expression is obtained for general quantum wiretap channels.

In the interception model, the guaranteed rate bound includes both Eve's system E and Bob's entangled resource G_B (see (3.10)), which reflects Eve's access to the entanglement assistance if she succeeds to intercept the resource. On the other hand, in the passive eavesdropper model, the guaranteed rate bound does not involve the entangled resource G_B (see (4.2)), as the assistance is beyond Eve's reach.

Moreover, the bound on the excess rate, in the passive model, does not include Eve's system at all (see (4.2)), i.e., secrecy does not entail a rate reduction. This is expected because given reliable entanglement assistance, Alice and Bob can secure a shared key, and apply the one-time pad encryption to the excess message.

As an example, we consider the erasure channel and the amplitude damping channel. For the erasure channel, time division is optimal. This is "good news" from a practical perspectives, as time division is much easier to implement. We observe that in general, time division is impossible if Eve can actively intercept Bob's entanlged resource, since Alice's operations on her share of the entanglement could leak information on the guaranteed information. For the amplitude damping channel, the boundary of our achievable region is disconnected in agreement with this property. In the passive model,

on the other hand, our encoding scheme outperforms time division.

Some questions still remain open, as we do not have a full understanding of the behavior of the capacity region, its convexity properties, and the type of entanglement that allows positive guaranteed rate under interception. Furthermore, while we have presented a regularized characterization, a single-letter capacity formula for the class of degraded channels could lead to further insights.

From a broader perspective, it would be interesting to explore unreliable entanglement assistance beyond the setting of point-to-point or broadcast communication. This includes multi-user communication scenarios, as well as other information-theoretic tasks that may benefit from entanglement assistance, such as coordination, secret-key generation (e.g., QKD), and more.

Finally, investigating the experimental implications of unreliable entanglement presents another compelling research direction.

Appendix A

Packing Lemma and Covering Lemma Properties

This appendix provides further details and supporting arguments for the information-theoretic tools used in the main achievability proof in Sec. 5.1. Specifically, we verify the conditions required for applying the quantum packing lemma and quantum covering lemma. These results justify the claims regarding reliable decoding and security in the presence or absence of entanglement assistance, as used in Sec. 5.1.

A.1 Packing Lemma with Entanglement Assistance

To justify the statement in the main text, we apply the quantum packing lemma in the presence of entanglement assistance. Fix a codeword $x^n \in \mathcal{X}^n$, and define the ensemble $\{\rho_{B^nG_2^n}^{\gamma,x^n}\}_\gamma$ with expected density operator

$$\bar{\rho}_{B^nG_2^n}^{x^n} = \frac{1}{|\Gamma_{x^n}|} \sum_{\gamma \in \Gamma_{x^n}} \rho_{B^nG_2^n}^{\gamma,x^n}.$$

Let Π be the projector onto the δ-typical subspace of $\bar{\rho}_{B^nG_2^n}^{x^n}$, and Π_γ the projector associated with the codeword $\rho_{B^nG_2^n}^{\gamma,x^n}$. Using standard typicality arguments and results from [7, Appendix II], the following bounds hold:

$$\mathrm{Tr}(\Pi\bar{\rho}) \geq 1 - 2\varepsilon_2(\delta), \tag{A.1}$$

$$\mathrm{Tr}(\Pi_\gamma\bar{\rho}) \geq 1 - \varepsilon_3(\delta), \tag{A.2}$$

$$\mathrm{Tr}(\Pi_\gamma) \leq 2^{n(H(BG_2|X)+\varepsilon_4(\delta))}, \tag{A.3}$$

$$\Pi\bar{\rho}\Pi \leq 2^{-n(H(B|X)+H(G_2|X)-\varepsilon_5(\delta))}\Pi. \tag{A.4}$$

These bounds ensure that the requirements of the packing lemma in 1.8.1 are satisfied. Hence, there exists a decoding POVM $\{\Upsilon_{m',k'|x^n}\}$ with vanishing average error,

provided the rate satisfies

$$R' + R'_0 < I(G_2; B|X)_\omega - \epsilon_2.$$

A.2 Covering Lemma Properties

Now, we apply the tools of typical projectors to prove the properties of the quantum covering lemma. In the achievability proof, we establish two indistinguishability bounds, which are achieved using the quantum covering lemma [73] Lemma 2.7.1.

A.2.1 Guaranteed information indistinguishability bound

To show the indistinguishability bound in Eq.(5.27), for the guaranteed information, we apply the quantum covering lemma [73], Lemma 2.7.1, with the ensemble below,

$$\{p_{X^n}(x^n), \omega^{x^n}_{E^n G_2^n}\}_{x^n \in \mathcal{X}^n}\,, \tag{A.5}$$

and the following typical projectors,

$$\Pi = \Pi^{(n)}_\delta(\omega_{E^n G_2^n})\,, \tag{A.6}$$

$$\Pi_{x^n} = \Pi^{(n)}_\delta(\omega_{E^n G_2^n}|x^n)\,. \tag{A.7}$$

Based on standard typical projectors properties (see Section 1.1.5), there exists $\lambda > 0$ such that

$$\mathrm{Tr}(\Pi \omega^{\otimes n}_{EG_2}) \geq 1 - e^{-\lambda n}\,, \tag{A.8}$$

$$\mathrm{Tr}(\Pi_{x^n} \omega^{\otimes n}_{EG_2}) \geq 1 - e^{-\lambda n}\,, \tag{A.9}$$

$$\mathrm{Tr}(\Pi) \leq 2^{n(H(EG_2)_\omega + \epsilon_4)}\,, \tag{A.10}$$

$$\Pi_{x^n} \omega^{x^n}_{E^n G_2^n} \Pi_{x^n} \leq 2^{-n(H(EG_2|X)_\omega - \epsilon_4)} \Pi_{x^n}\,. \tag{A.11}$$

Thus, by the quantum covering lemma, for every $m \in \{1, \ldots, 2^{nR}\}$ and sufficiently large n,

$$\Pr\left(\Delta^*_m(\mathscr{C}) > e^{-\frac{\lambda}{2}n}\right) \leq \exp\left\{-2^{n(R_0 - I(X;EG_2)_\omega - \epsilon_5)}\right\}. \tag{A.12}$$

We have thus shown that Eq.(5.27) in the main proof holds.

A.2.2 Excess information indistinguishability bound

Next, we prove the indistinguishability bound in Eq.(5.31) in the main proof, for the excess information.

Recall that given a fixed $x^n \equiv x^n(m,k)$, we consider the uniform ensemble,

$$\left\{p(\gamma|x^n) = \frac{1}{|\Gamma_{x^n}|}, \rho_{E^nG_2^n}^{\gamma,x^n}\right\}_{\gamma\in\Gamma_{x^n}} . \tag{A.13}$$

with the average state,

$$\zeta_{E^nG_2^n}^{x^n} = \frac{1}{|\Gamma_{x^n}|}\sum_{\gamma\in\Gamma_{x^n}} \rho_{E^nG_2^n}^{\gamma,x^n} . \tag{A.14}$$

In addition, we define the code projectors in terms of the δ-typical projectors and the encoding unitary:

$$\Pi = \Pi_\delta^{(n)}(\omega_{E^n}|x^n) \otimes \Pi_\delta^{(n)}(\omega_{G_2^n}|x^n) , \tag{A.15}$$

$$\Pi_\gamma = (I \otimes U^T(\gamma))\Pi_\delta^{(n)}(\omega_{E^nG_2^n}|x^n)(I \otimes U^*(\gamma)) , \tag{A.16}$$

where ω_{E^n} and $\omega_{G_2^n}$ are the reduced states of $\omega_{E^nG_2^n}$. In order to apply the quantum covering lemma, we need to show that there exists $\mu > 0$ such that the following properties hold:

$$\mathrm{Tr}(\Pi\rho_{E^nG_2^n}^{\gamma,x^n}) \geq 1 - e^{-\mu n} , \tag{A.17}$$

$$\mathrm{Tr}(\Pi_\gamma\rho_{E^nG_2^n}^{\gamma,x^n}) \geq 1 - e^{-\mu n} , \tag{A.18}$$

$$\mathrm{Tr}(\Pi) \leq 2^{n(H(E|X)_\omega + H(G_2|X)_\omega + \epsilon_6)} , \tag{A.19}$$

$$\Pi_\gamma\rho_{E^nG_2^n}^{\gamma,x^n}\Pi_\gamma \leq 2^{-n(H(EG_2|X)_\omega - \epsilon_6)}\Pi_\gamma . \tag{A.20}$$

The first three arguments are similar to those in [91, Appendix II], while establishing (A.20) is more involved in our setting. For completeness, we give the details for all properties below.

We begin with the second property, in (A.18). Observe that

$$\begin{aligned}
&\mathrm{Tr}\Big\{\rho_{E^nG_2^n}^{\gamma,x^n}\Pi_\gamma\Big\} \\
&= \mathrm{Tr}\Big\{(\mathbb{1} \otimes U^T(\gamma))\omega_{E^nG_2^n}^{x^n}(\mathbb{1} \otimes U^*(\gamma)) \\
&\cdot (\mathbb{1} \otimes U^T(\gamma))\Pi_\delta^{(n)}(\omega_{E^nG_2^n}|x^n)(\mathbb{1} \otimes U^T(\gamma))\Big\} \\
&= \mathrm{Tr}\Big\{(\mathbb{1} \otimes U^T(\gamma))\omega_{E^nG_2^n}^{x^n}\Pi_\delta^{(n)}(\omega_{E^nG_2^n}|x^n)(\mathbb{1} \otimes U^T(\gamma))\Big\} \\
&= \mathrm{Tr}\Big\{\omega_{E^nG_2^n}^{x^n}\Pi_\delta^{(n)}(\omega_{E^nG_2^n}|x^n))\Big\} \\
&\geq 1 - \frac{1}{2}\epsilon_6
\end{aligned} \tag{A.21}$$

for sufficiently large n. The first equality follows from substituting the expressions for $\rho_{E^nG_2^n}^{\gamma,x^n}$ from Eq. (60) in the main manuscript, and for Π_γ in (A.16). The second equality

holds since $U^*(\gamma) = (U^T(\gamma))^{-1}$, the third holds due to the trace cyclic property, and the inequality is due to the conditional typical projector property in (1.50).

The third property, in (A.19), immediately follows from the dimension bound in (1.51).

Now, we prove the first property, in (A.17). To this end, we express the projector Π in terms of the complementary projectors below,

$$\hat{\Pi}_\delta^{(n)}(\omega_{E^n}|x^n)) \equiv \mathbb{1} - \Pi_\delta^{(n)}(\omega_{E^n}|x^n))\,, \tag{A.22}$$

$$\hat{\Pi}_\delta^{(n)}(\omega_{G_2^n}|x^n)) \equiv \mathbb{1} - \Pi_\delta^{(n)}(\omega_{G_2^n}|x^n))\,. \tag{A.23}$$

Then,

$$\begin{aligned}
\Pi &= \Pi_\delta^{(n)}(\omega_{E^n}|x^n) \otimes \Pi_\delta^{(n)}(\omega_{G_2^n}|x^n) \\
&= (\mathbb{1} - \hat{\Pi}_\delta^{(n)}(\omega_{E^n}|x^n)) \otimes (\mathbb{1} - \hat{\Pi}_\delta^{(n)}(\omega_{G_2^n}|x^n)) \\
&= \mathbb{1}\otimes\mathbb{1} - \hat{\Pi}_\delta^{(n)}(\omega_{E^n}|x^n) \otimes \mathbb{1} - \mathbb{1} \otimes \hat{\Pi}_\delta^{(n)}(\omega_{G_2^n}|x^n) \\
&+ \hat{\Pi}_\delta^{(n)}(\omega_{E^n}|x^n) \otimes \hat{\Pi}_\delta^{(n)}(\omega_{G_2^n}|x^n) \\
&\geq \mathbb{1}\otimes\mathbb{1} - \hat{\Pi}_\delta^{(n)}(\omega_{E^n}|x^n) \otimes \mathbb{1} - \mathbb{1} \otimes \hat{\Pi}_\delta^{(n)}(\omega_{G_2^n}|x^n)
\end{aligned} \tag{A.24}$$

where the first equality holds by the definition of Π in (A.15), and the second by (A.22)-(A.23).

Therefore,

$$\begin{aligned}
&\mathrm{Tr}\Big\{\rho_{E^nG_2^n}^{\gamma|x^n}\Pi\Big\} = \mathrm{Tr}\Big\{(\mathbb{1}\otimes U^T(\gamma))\omega_{E^nG_2^n}^{x^n}(\mathbb{1}\otimes U^*(\gamma))\Pi\Big\} \\
&\geq \mathrm{Tr}\Big\{(\mathbb{1}\otimes U^T(\gamma))\omega_{E^nG_2^n}^{x^n}(\mathbb{1}\otimes U^*(\gamma))\cdot(\mathbb{1}\otimes\mathbb{1})\Big\} \\
&- \mathrm{Tr}\Big\{(\mathbb{1}\otimes U^T(\gamma))\omega_{E^nG_2^n}^{x^n}(\mathbb{1}\otimes U^*(\gamma)) \\
&\cdot(\hat{\Pi}_\delta^{(n)}(\omega_{E^n}|x^n)\otimes\mathbb{1})\Big\} \\
&- \mathrm{Tr}\Big\{(\mathbb{1}\otimes U^T(\gamma))\omega_{E^nG_2^n}^{x^n}(\mathbb{1}\otimes U^*(\gamma)) \\
&\cdot(\mathbb{1}\otimes\hat{\Pi}_\delta^{(n)}(\omega_{G_2^n}|x^n))\Big\}\,.
\end{aligned} \tag{A.25}$$

By the trace cyclic property, the first trace term equals $\mathrm{Tr}(\omega_{E^nG_2^n}^{x^n}) = 1$, and the second is

$$\begin{aligned}
\mathrm{Tr}(\omega_{E^nG_2^n}^{x^n}\hat{\Pi}_\delta^{(n)}(\omega_{E^n}|x^n)) &= 1 - \mathrm{Tr}(\omega_{E^nG_2^n}^{x^n}\Pi_\delta^{(n)}(\omega_{E^n}|x^n)) \\
&\leq \frac{1}{2}\epsilon_6
\end{aligned} \tag{A.26}$$

where the inequality holds by (A.21). Similarly, the last trace term in (A.25) is bounded by $\frac{1}{2}\epsilon_6$. Substituting those terms in (A.25) yields the desired bound (A.17).

It remains to show the last bound, in (A.20). Observe that

$$\begin{aligned}
&\Pi_\gamma \rho_{E^n G_2^n}^{\gamma,x^n} \Pi_\gamma \\
&= (\mathbb{1} \otimes U^T(\gamma))\Pi_\delta^{(n)}(\omega_{E^n G_2^n}|x^n)(\mathbb{1} \otimes U^*(\gamma)) \\
&\cdot (\mathbb{1} \otimes U^T(\gamma))\omega_{E^n G_2^n}^{x^n}(\mathbb{1} \otimes U^*(\gamma)) \\
&\cdot (\mathbb{1} \otimes U^T(\gamma))\Pi_\delta^{(n)}(\omega_{E^n G_2^n}|x^n)(\mathbb{1} \otimes U^*(\gamma)) \\
&= (\mathbb{1} \otimes U^T(\gamma)) \cdot \Pi_\delta^{(n)}(\omega_{E^n G_2^n}|x^n)\omega_{E^n G_2^n}^{x^n}\Pi_\delta^{(n)}(\omega_{E^n G_2^n}|x^n) \\
&\cdot (\mathbb{1} \otimes U^*(\gamma))
\end{aligned} \tag{A.27}$$

where the last equality holds since $U^T(\gamma) = (U^*(\gamma))^{-1}$. Based on the properties of conditional typical projectors,

$$\begin{aligned}
&\Pi_\delta^{(n)}(\omega_{E^n G_2^n}|x^n)\omega_{E^n G_2^n}^{x^n}\Pi_\delta^{(n)}(\omega_{E^n G_2^n}|x^n) \\
&\leq 2^{-n(H(EG_2|X)_\omega - \epsilon_6)}\Pi_\delta^{(n)}(\omega_{E^n G_2^n}|x^n)
\end{aligned} \tag{A.28}$$

(see (1.52) in Sec. 1.1.5). Thus,

$$\begin{aligned}
&\Pi_\gamma \rho_{E^n G_2^n}^{\gamma,x^n} \Pi_\gamma \\
&\leq 2^{-n(H(EG_2|X)_\omega - \epsilon_6)}(\mathbb{1} \otimes U^T(\gamma)) \\
&\cdot \Pi_\delta^{(n)}(\omega_{E^n G_2^n}|x^n)(\mathbb{1} \otimes U^*(\gamma)) \\
&\equiv 2^{-n(H(EG_2|X)_\omega - \epsilon_6)}\Pi_\gamma
\end{aligned} \tag{A.29}$$

where the last equality follows the definition of Π_γ in (A.16), thus proving (A.20). We have thus proved the covering lemma conditions, (A.17)-(A.20), which imply Eq. (5.31) in the main proof.

This concludes the proof for the indistinguishability bounds, for both the guaranteed information and the excess information.

Bibliography

[1] A. S. Holevo, "The capacity of the quantum channel with general signal states," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 269–273, Jan 1998.

[2] B. Schumacher and M. D. Westmoreland, "Sending classical information via noisy quantum channels," *Phys. Rev. A*, vol. 56, no. 1, p. 131, July 1997.

[3] N. Cai, A. Winter, and R. W. Yeung, "Quantum privacy and quantum wiretap channels," *Prob. Inform. Transm.*, vol. 40, pp. 318–336, 2004.

[4] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 44–55, 2005.

[5] C. H. Bennett, I. Devetak, A. W. Harrow, P. W. Shor, and A. Winter, "Entanglement-assisted capacity of a quantum channel and the reverse shannon theorem," in *IEEE Trans. Inf. Theory*, vol. 48, no. 10, 2002, pp. 2637–2655.

[6] H. Qi, K. Sharma, and M. M. Wilde, "Entanglement-assisted private communication over quantum broadcast channels," *J. Phys. A: Math. Theo.*, vol. 51, no. 37, p. 374001, 2018.

[7] U. Pereg, C. Deppe, and H. Boche, "Communication with unreliable entanglement assistance," *IEEE Trans. Inf. Theory*, vol. 69, no. 7, pp. 4579–4599, 2023.

[8] J. Yin, Y. H. Li, S. K. Liao, M. Yang, Y. Cao, L. Zhang, J. G. Ren, W. Q. Cai, W. Y. Liu, and S. L. Li, "Entanglement-based secure quantum cryptography over 1,120 kilometres," *Nature*, vol. 582, no. 7813, pp. 501–505, 2020.

[9] E. Zlotnick, B. Bash, and U. Pereg, "Entanglement-assisted covert communication via qubit depolarizing channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT'2023)*, 2023, pp. 198–203.

[10] M.-H. Hsieh, I. Devetak, and A. Winter, "Entanglement-assisted capacity of quantum multiple-access channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 7, pp. 3078–3090, 2008.

[11] F. Dupuis, P. Hayden, and K. Li, "A father protocol for quantum broadcast channels," *IEEE Trans. Inf. Theory*, vol. 56, no. 6, pp. 2946–2956, June 2010.

[12] U. Pereg, C. Deppe, and H. Boche, "The multiple-access channel with entangled transmitters," `arXiv:2303.10456 [quant-ph]`. Submitted to IEEE Trans. Inf. Theory, 2023.

[13] V. Giovannetti, S. Lloyd, and L. Maccone, "Quantum-enhanced measurements: beating the standard quantum limit," *Science*, vol. 306, no. 5700, pp. 1330–1336, 2004.

[14] P. Komar, E. Kessler, M. Bishof, L. Jiang, A. Sárkozy, T. Zelevinsky, J. Ye, and M. D. Lukin, "A quantum network of clocks," *Nature Physics*, vol. 10, no. 8, pp. 582–587, 2014.

[15] T. J. Proctor, P. A. Knott, and J. A. Dunningham, "Multiparameter estimation in networked quantum sensors," *Phys. Rev. Lett.*, vol. 120, no. 8, p. 080501, 2018.

[16] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, "Quantum communication complexity advantage implies violation of a bell inequality," *Rev. Mod. Phys.*, vol. 82, no. 1, p. 665, 2010.

[17] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, "Entanglement-assisted classical capacity of noisy quantum channels," *Phys. Rev. Lett.*, vol. 83, no. 15, p. 3081, Oct 1999.

[18] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, "Entanglement-assisted capacity of a quantum channel and the reverse shannon theorem," *IEEE Trans. Inf. Theory*, vol. 48, no. 10, pp. 2637–2655, Oct 2002.

[19] J. Chen *et al.*, "Long-distance distribution of high-dimensional entanglement enabled by multiplexed quantum memories," *Nature Photonics*, vol. 15, pp. 123–129, 2021.

[20] G. Kramer, "Topics in multi-user information theory," *Found. Trends Commun. Inf. Theory*, vol. 4, no. 4–5, pp. 265–444, 2008.

[21] M. M. Wilde, *Quantum Information Theory*, 2nd ed. Cambridge Univ. Press, 2017.

[22] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Wiley, 2006.

[23] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, 1948.

[24] R. Ahlswede, "Elimination of correlation in random codes for arbitrarily varying channels," *Z. Wahrscheinlichkeitstheorie verw. Gebiete*, vol. 44, pp. 159–175, 1978.

[25] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, 1993.

[26] C. E. Shannon, "The zero error capacity of a noisy channel," *IRE Trans. Inf. Theory*, vol. 2, no. 3, pp. 8–19, 1956.

[27] P. Cuff, H. H. Permuter, and T. M. Cover, "Coordination capacity," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4181–4206, 2010.

[28] C. M. Caves and P. D. Drummond, "Quantum limits on bosonic communication rates," *Rev. Mod. Phys.*, vol. 66, no. 2, pp. 481–537, 1994.

[29] A. S. Holevo, *Quantum systems, channels, information: a mathematical introduction.* Walter de Gruyter, 2012, vol. 16.

[30] M. B. Hastings, "Superadditivity of communication capacity using entangled inputs," *Nature Physics*, vol. 5, no. 4, p. 255, March 2009.

[31] S. Hao, H. Shi, W. Li, J. H. Shapiro, Q. Zhuang, and Z. Zhang, "Entanglement-assisted communication surpassing the ultimate classical capacity," *Phys. Rev. Lett.*, vol. 126, no. 25, p. 250501, 2021.

[32] C. H. Bennett, I. Devetak, P. W. Shor, J. A. Smolin, A. V. Thapliyal, and A. Winter, "Inequalities and separations among assisted capacities of quantum channels," *Phys. Rev. Lett.*, vol. 93, no. 14, p. 140501, 2004.

[33] C. H. Bennett and S. J. Wiesner, "Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states," *Phys. Rev. Lett.*, vol. 69, no. 20, p. 2881, Nov 1992.

[34] A. S. Holevo, "Bounds for the quantity of information transmitted by a quantum communication channel," *Problemy Peredachi Informatsii*, vol. 9, no. 3, pp. 3–11, 1973.

[35] G. S. Jaeger and . V. Sergienko, "Entanglement sudden death: a threat to advanced quantum key distribution?" *Natural Comput.*, vol. 13, no. 4, pp. 459–467, 2014.

[36] E. T. Campbell and S. C. Benjamin, "Measurement-based entanglement under conditions of extreme photon loss," *Physical Rev. Lett.*, vol. 101, no. 13, p. 130502, 2008.

[37] J. Yin, Y. Cao, Y. H. Li, J. G. Ren, S. K. Liao, L. Zhang, W. Q. Cai, W. Y. Liu, B. Li, and H. Dai, "Satellite-to-ground entanglement-based quantum key distribution," *Physical Rev. Lett.*, vol. 119, no. 20, p. 200501, 2017.

[38] A. Czerwinski and K. Czerwinska, "Statistical analysis of the photon loss in fiber-optic communication," *Photon.*, vol. 9, no. 8, p. 568, 2022.

[39] G. Fettweis and H. Boche, "On 6G and trustworthiness," *Commun. ACM*, vol. 65, no. 4, pp. 48–49, 2022.

[40] Y. Steinberg, "Channels with cooperation links that may be absent," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT'2014)*, 2014, pp. 1947–1951.

[41] W. Huleihel and Y. Steinberg, "Channels with cooperation links that may be absent," *IEEE Trans. Inf. Theory*, vol. 63, no. 9, pp. 5886–5906, 2017.

[42] ——, "Multiple access channel with unreliable cribbing," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT'2016)*, 2016, pp. 1491–1495.

[43] D. Itzhak and Y. Steinberg, "The broadcast channel with degraded message sets and unreliable conference," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT'2017)*, 2017, pp. 1043–1047.

[44] ——, "The broadcast channel with degraded message sets and unreliable conference," *IEEE Trans. Inf. Theory*, vol. 67, no. 9, pp. 5623–5650, 2021.

[45] U. Pereg and Y. Steinberg, "Arbitrarily varying broadcast channel with uncertain cooperation," in *Proc. Int'l Zurich Semin. Inf. Commun. (IZS'2020)*. ETH Zurich, 2020, pp. 63–67.

[46] L. H. Ozarow, S. Shamai, and A. D. Wyner, "Information theoretic considerations for cellular mobile radio," *IEEE Trans. Vehicular Tech.*, vol. 43, no. 2, pp. 359–378, 1994.

[47] R. Karasik, O. Simeone, and S. Shamai, "Robust uplink communications over fading channels with variable backhaul connectivity," *IEEE Trans. Wireless Commun.*, vol. 12, no. 11, pp. 5788–5799, 2013.

[48] G. Caire and D. Tuninetti, "The throughput of hybrid-arq protocols for the Gaussian collision channel," *IEEE Trans. Inf. Theory*, vol. 47, no. 5, pp. 1971–1988, 2001.

[49] A. Steiner and S. Shamai, "Multi-layer broadcasting hybrid-ARQ strategies for block fading channels," *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, pp. 2640–2650, 2008.

[50] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa, "Breaking spectrum gridlock with cognitive radios: An information theoretic perspective," *Proc. of the IEEE*, vol. 97, no. 5, pp. 894–914, May 2009.

[51] Y. Liang, L. Lai, H. V. Poor, and S. Shamai, "A broadcast approach for fading wiretap channels," *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 842–858, 2013.

[52] S. Shamai and A. Steiner, "A broadcast approach for a single-user slowly fading mimo channel," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2617–2635, Oct 2003.

[53] A. Cohen, M. Médard, and S. S. Shitz, "Broadcast approach meets network coding for data streaming," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT'2022)*, 2022, pp. 25–30.

[54] M. Horodecki, P. W. Shor, and M. B. Ruskai, "Entanglement breaking channels," *Rev. Math. Phys.*, vol. 15, no. 06, pp. 629–641, 2003.

[55] M. M. Wilde, N. Datta, M.-H. Hsieh, and A. Winter, "Quantum rate-distortion coding with auxiliary resources," *IEEE Trans. Inf. Theory*, vol. 59, no. 10, pp. 6755–6773, 2013.

[56] P. W. Shor, "Additivity of the classical capacity of entanglement-breaking quantum channels," *J. Math. Phys.*, vol. 43, no. 9, pp. 4334–4340, May 2002.

[57] U. Pereg, "Communication over entanglement-breaking channels with unreliable entanglement assistance," *Physical Rev. A*, vol. 108, p. 042616, 2023.

[58] J. Körner, "The concept of single-letterization in information theory," in *Open Prob. Commun. Comp.* Springer, 1987, pp. 35–36.

[59] R. Ahlswede *et al.*, "The capacity region of a channel with two senders and two receivers," *Ann. Prob.*, vol. 2, no. 5, pp. 805–814, 1974.

[60] M. Wiese and H. Boche, "The arbitrarily varying multiple-access channel with conferencing encoders," *IEEE Trans. Inf. Theory*, vol. 59, no. 3, pp. 1405–1416, March 2013.

[61] E. Biglieri, J. Proakis, and S. Shamai, "Fading channels: information-theoretic and communications aspects," *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 2619–2692, Oct 1998.

[62] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J*, vol. 54(8), pp. 1355–1387, 1975.

[63] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, pp. 7–11, 2014.

[64] R. F. Schaefer, H. Boche, and H. V. Poor, "Secure communication under channel uncertainty and adversarial attacks," *Proc. IEEE*, vol. 103, no. 10, pp. 1796–1813, 2015.

[65] M. Bloch and J. Barros, *Physical-layer security: from information theory to security engineering*. Cambridge Univ. Press, 2011.

[66] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[67] K. Li, A. Winter, X. Zou, and G. Guo, "Private capacity of quantum channels is not additive," *Phys. Rev. Lett.*, vol. 103, no. 12, p. 120501, 2009.

[68] D. Elkouss and S. Strelchuk, "Superadditivity of private information for any number of uses of the channel," *Phys. Rev. Lett.*, vol. 115, no. 4, p. 040501, 2015.

[69] I. Devetak and P. W. Shor, "The capacity of a quantum channel for simultaneous transmission of classical and quantum information," *Commun. in Math. Phys.*, vol. 256, no. 2, pp. 287–303, 2005.

[70] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, pp. 802–803, 1982.

[71] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3047–3061, 2004.

[72] T. A. Atif, S. S. Pradhan, and A. Winter, "Quantum soft-covering lemma with applications to rate-distortion coding, resolvability and identification via quantum channels," *arXiv preprint arXiv:2306.12416*, 2023.

[73] R. Ahlswede and A. Winter, "Strong converse for identification via quantum channels," *IEEE Trans. Inf. Theory*, vol. 48, no. 3, pp. 569–579, 2002.

[74] M. Hayashi, *Quantum information.* Springer, 2006.

[75] M. Tahmasbi and M. R. Bloch, "Toward undetectable quantum key distribution over bosonic channels," *IEEE J. Sel. Areas Inf. Theory*, vol. 1, no. 2, pp. 585–598, 2020.

[76] H. Boche and J. Nötzel, "Positivity, discontinuity, finite resources, and nonzero error for arbitrarily varying quantum channels," *J. Math. Phys.*, vol. 55, no. 12, p. 122201, 2014.

[77] S. Barz, G. Cronenberg, A. Zeilinger, and P. Walther, "Heralded generation of entangled photon pairs," *Nature Photon.*, vol. 4, no. 8, pp. 553–556, 2010.

[78] W. Zo, S. Chin, and Y.-S. Kim, "Heralded optical entanglement distribution via lossy quantum channels: A comparative study," *Optics Express*, vol. 33, no. 6, pp. 12 459–12 474, 2025.

[79] J. G. Proakis, *Digital Communications*, 4th ed. McGraw-Hill, 2001.

[80] Q. Zhuang, E. Y. Zhu, and P. W. Shor, "Additive classical capacity of quantum channels assisted by noisy entanglement," *Phys. Rev. Lett.*, vol. 118, no. 20, p. 200503, 2017.

[81] S. Zou, Y. Liang, L. Lai, H. V. Poor, and S. Shamai, "Broadcast networks with layered decoding and layered secrecy: Theory and applications," *Proc. IEEE*, vol. 103, no. 10, pp. 1841–1856, 2015.

[82] U. Pereg, R. Ferrara, and M. R. Bloch, "Key assistance, key agreement, and layered secrecy for bosonic broadcast channels," in *Proc. IEEE Inf. Theory Workshop (ITW'2021)*, 2021, pp. 1–6.

[83] N. Cai, "The maximum error probability criterion, random encoder, and feedback, in multiple input channels," *Entropy*, vol. 16, no. 3, pp. 1211–1242, 2014.

[84] U. Pereg, "Communication over quantum channels with parameter estimation," *IEEE Trans. Inf. Theory*, vol. 68, no. 1, pp. 359–383, 2022.

[85] A. Winter, "Coding theorem and strong converse for quantum channels," *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2481–2485, Nov 1999.

[86] V. Giovannetti and R. Fazio, "Information-capacity description of spin-chain correlations," *Phys. Rev. A*, vol. 71, no. 3, p. 032314, 2005.

[87] C. H. Bennett, D. P. DiVincenzo, and J. A. Smolin, "Capacities of quantum erasure channels," *Phys. Rev. Lett.*, vol. 78, no. 16, p. 3217, 1997.

[88] T. M. Cover, "Broadcast channels," *IEEE Trans. Inf. Theory*, vol. 18, no. 1, pp. 2–14, Jan 1972.

[89] M. Hayashi and H. Nagaoka, "General formulas for capacity of classical-quantum channels," *IEEE Trans. Inf. Theory*, vol. 49, no. 7, pp. 1753–1768, 2003.

[90] M. Graifer, Y. Kochman, and O. Shayevitz, "Quantum key distribution with state replacement," in *Proc. 59th Annu. Allerton Conf. Commun. Control Comput.* IEEE, 2023, pp. 1–8.

[91] M. Hsieh, I. Devetak, and A. Winter, "Entanglement-assisted capacity of quantum multiple-access channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 7, pp. 3078–3090, July 2008.

generation, שבו אליס ובוב מכינים כל אחד זוג שזור, אליס שולחת פוטון אחד לבוב, ובוב מבצע מדידת בל משותפת על הפוטון שקיבל יחד עם אחד הפוטונים. בעקבות המדידה, החלקיקים הנותרים הופכים שזורים.

המטרה המרכזית של עבודה זו היא אפיון קצבי השידור האפשריים להעברת מידע באופן אמין וסודי בכל אחד מהמקרים לעיל. האנליזה מתבצעת תחת דרישות מחמירות של הסתברות שגיאה מקסימלית חסומה וסודיות סמנטית.

התוצאה המרכזית היא חסם פנימי על תחום קיבול הסודיות עבור מודל הירוט, ונוסחת קיבול אסימפטוטית עבור המודל הפסיבי. כמו כן, עבור המחלקה של ערוצים מדורגים, פיתחנו נוסחת קיבול אסימפטוטית גם במודל הירוט.

שיטת הקידוד בהוכחה מבוססת על קידוד בשכבות, שבו ההודעה המובטחת בקצב R מקודדת תחילה, ולאחר מכן מוסיפים שכבת קידוד נוספת של ההודעה העודפת בקצב $\mathrm{R'}$ - שתי השכבות מופעלות על אותו מצב קוונטי ראשוני של המשאב הנמצא בידי אליס. מבנה זה מאפשר פענוח סדרתי: בוב מפענח תחילה את ההודעה המובטחת, שהוא נדרש לשחזר בכל מקרה, בין אם קיבל את משאב השזירות או לא. לאחר מכן, אם המשאב השזור אכן הגיע לבוב, אז הוא מפענח את ההודעה העודפת. אחרת, הוא מוותר.

לצורך הבטחת סודיות, כל הודעה מקודדת יחד עם אלמנטים אקראיים שתפקידם הוא לטשטש את המידע בפני איב, גם במקרה בו היא גנבה את סיוע השזירות.

אנליזת הסתברות השגיאה נעשתה באמצעות טענת האריזה הקוונטית, בעוד שלצורך אנליזת הסודיות נעשה שימוש בטענת הכיסוי הקוונטית שמבטיחה כי הפלט הנצפה על ידי איב נראה כמעט בלתי תלוי בהודעה המשודרת. הוכחת הדרישה להסתברות שגיאה מקסימלית מבוססת על הגישה של Cai, שפותחה במקור לניתוח ערוצים מרובי גישות, ומתבססת על שימוש בפרמוטציות אקראיות.

בנוסף, בחנו שתי דוגמאות לערוצי תקשורת שימושיים: ערוץ מחיקה וערוץ מנחית אמפליטודה. עבור ערוץ המחיקה, הראינו כי אסטרטגיית קידוד המבוססת על חלוקת זמן בין שתי אסטרטגיות קצה, המביאות למקסימום את הקצב R או את הקצב $\mathrm{R'}$, היא אופטימלית, הן עבור מודל הירוט והן עבור המודל הפסיבי. לעומת זאת, עבור ערוץ מנחית אמפליטודה, קידוד המבוסס על שכבות אסטרטגיות הקצה מראה שחלוקת זמן אינה בהכרח אפשרית במודל הירוט, וכי השפה של תחום הקצבים בר ההשגה אינה רציפה.

תקציר

העבודה עוסקת בתקשורת סודית בסיוע שזירות בלתי אמינה. אנו חוקרים העברת מידע קלאסי דרך ערוץ קוונטי רועש בין המשדר (אליס) לבין המקלט (בוב) בנוכחות מצותתת (איב). ידוע כי סיוע שזירות יכול להגדיל את קצב התקשורת במידה ניכרת. במודל של סיוע שזירות, מניחים שיש לאליס ובוב גישה לחלקיקים שזורים קוונטית לפני תחילת השידור. הרעיון הוא לנצל פרקי זמן "שקטים" במערכת כדי ליצור משאבי שזירות, ואחרי כן, כשמגיע המידע, נרצה להשתמש במשאבים אלו כדי לשלוח את המידע בקצב גבוה יותר. בפרט, במקרה של ערוץ אידאלי חסר רעש, סיוע שזירות מכפיל את קצב השידור. ראוי לציין ששזירות מהווה משאב סטטי שלא מאפשר תקשורת בפני עצמו, בדומה למשאב אקראיות משותפת, כלומר מפתח המורכב מביטים אקראיים שזמינים לאליס ובוב לפני השידור. עם זאת, במערכות מעשיות קשה לייצר שזירות אמינה בין שני צדדים מרוחקים. האתגר המשמעותי ביותר הוא אובדן פוטונים, למשל כתוצאה מחוסר אידאליות של סיבים אופטיים או בליעה באטמוספרה בשידור אופטי לווייני.

הגישה הסטנדרטית לטיפול באובדן במהלך יצירת השזירות היא שימוש בערוץ משוב. באופן הזה, בוב מודיע לאליס אם קיבל את משאב השזירות באמצעות ערוץ המשוב. ואם לא, אז אליס חוזרת על התהליך ושולחת את המשאב השזור. גישה זו לא בהכרח ישימה ועלולה לגרום לקריסה של המערכת בתנאים שבהם אין אפשרות ליצור שזירות. מנגד, המושג של סיוע שזירות בלתי אמין מציע הסתגלות פרואקטיבית: אליס שולחת שתי הודעות – הודעה מובטחת בקצב R, ו - הודעה עודפת בקצב R'. הדרישה היא כי בוב יפענח את ההודעה המובטחת תמיד, ואת ההודעה העודפת רק אם הוא קיבל את המשאב השזור. כך, קצב הפענוח של בוב מותאם לדינמיקת השזירות בפועל: R ללא סיוע שזירות, ו-$(R+R')$ כאשר יש סיוע שזירות.

עבודה זו עוסקת בביצועים של תקשורת סודית בסיוע שזירות בלתי אמינה בשני מודלים המתאימים לתרחישי אבטחה שונים:

1. מודל הירוט - האויב עלול ליירט את המשאב השזור, ובכך למנוע את הגעתו לבוב.

2. המודל הפסיבי - האויב פסיבי ואין לו גישה למשאב השזירות, אך המשאב עלול להיאבד לסביבה ניטרלית.

כל אחד מהמודלים נוקט בגישת Hard Decision המתייחסת לשני מקרי קצה מנקודת המבט של המפענח: המשאב השזור זמין בשלמותו או בכלל לא. ההנחה היא שאליס מקודדת מבלי לדעת לאן הגיע משאב השזירות, ואילו בוב ואיב יודעים מי מביניהם קיבל את משאב השזירות. זוהי הנחה פרקטית, מפני שיצור שזירות ממומש באופן מעשי בתהליך של heralded entanglement

המחקר בוצע בהנחייתו של פרופסור עוזי פרג, בפקולטה להנדסת חשמל ומחשבים.

התוצאות שבחיבור זה פורסמו כמאמרים מאת המחבר ושותפיו למחקר בכנסים ובכתבי-עת במהלך תקופת מחקר התזה של המחבר, אשר גרסאותיהם העדכניות ביותר הינן:

Meir Lederman and Uzi Pereg. Secure communication with unreliable entanglement assistance. In *Proc. IEEE Int. Symp. Inf. Theory (ISIT 2024)*, pages 1017–1022, .2024

Meir Lederman and Uzi Pereg. Semantic security with unreliable entanglement assistance: Interception and loss. In *Proc. IEEE Inf. Theory Workshop (ITW 2024)*, pages 693–698, .2024

Meir Lederman and Uzi Pereg. Secure communication with unreliable entanglement assistance: Interception and loss. *Submitted to IEEE Trans. Inf. Theory*, .2025

תודות

ברצוני להביע את תודתי הכנה למנחה שלי, פרופ׳ עוזי פרג, על ההכוונה, התמיכה והליווי לאורך כל העבודה. כמו כן, אני מודה מעומק הלב למשפחתי ולחבריי על התמיכה והעידוד לאורך הדרך.

מחבר/ת חיבור זה מצהיר/ה כי המחקר, כולל איסוף הנתונים, עיבודם והצגתם, התייחסות והשוואה למחקרים קודמים וכו׳, נעשה כולו בצורה ישרה, כמצופה ממחקר מדעי המבוצע לפי אמות המידה האתיות של העולם האקדמי. כמו כן, הדיווח על המחקר ותוצאותיו בחיבור זה נעשה בצורה ישרה ומלאה, לפי אותן אמות מידה.

הכרת תודה מסורה לטכניון על מימון מחקר זה.

תקשורת סודית בסיוע שזירות בלתי אמינה

חיבור על מחקר

לשם מילוי חלקי של הדרישות לקבלת התואר
מגיסטר למדעים

מאיר לדרמן

הוגש לסנט הטכניון — מכון טכנולוגי לישראל
סיוון התשפ"ה חיפה יוני 2025

תקשורת סודית בסיוע שזירות בלתי אמינה

מאיר לדרמן