A New Approach to Lossy Compression and Applications to Security

Chen Eva Song

A Dissertation
Presented to the Faculty
of Princeton University
in Candidacy for the Degree
of Doctor of Philosophy

Recommended for Acceptance
by the Department of
Electrical Engineering
Advisers: Paul Cuff and H. Vincent Poor

November 2015

Abstract

In this thesis, rate-distortion theory is studied in the context of lossy compression communication systems with and without security concerns. A new source coding proof technique using the "likelihood encoder" is proposed that achieves the best known compression rate in various lossy compression settings. It is demonstrated that the use of the likelihood encoder together with Wyner's soft-covering lemma yields simple achievability proofs for classical source coding problems. We use the likelihood encoder technique to show the achievability parts of the point-to-point rate-distortion function, the rate-distortion function with side information at the decoder (i.e. the Wyner-Ziv problem), and the multi-terminal source coding inner bound (i.e. the Berger-Tung problem). Furthermore, a non-asymptotic analysis is used for the point-to-point case to examine the upper bound on the excess distortion provided by this method. The likelihood encoder is also compared, both in concept and performance, to a recent alternative random-binning based technique.

Also, the likelihood-encoder source coding technique is further used to obtain new results in rate-distortion based secrecy systems. Several secure source coding settings, such as using shared secret key and correlated side information, are investigated. It is shown that the rate-distortion based formulation for secrecy fully generalizes the traditional equivocation-based secrecy formulation. The extension to joint source-channel security is also considered using similar encoding techniques. The rate-distortion based secure source-channel analysis is applied to optical communication for reliable and secure delivery of an information source through a multimode fiber channel subject to eavesdropping.

Acknowledgements

First and foremost, I would like to express my sincere gratitude to my advisors Prof. Paul Cuff and Prof. Vincent Poor for their continuous selfless advice, encouragement and support throughout the course of my thesis. They are the kindest coaches, colleagues, and friends that always give me freedom of exploring new research.

I would like to thank my thesis reader and examiner, Prof. Sergio Verdú, for his insightful comments and passion for perfection. My thanks also goes to the rest of my thesis committee: Prof. Emmanuel Abbe and Prof. Prateek Mittal.

Uncountable interesting discussions and idea exchanges happened during the past five years with my fellow labmates: Curt Schieler, Sai (Sanket) Satpathy, Jingbo Liu, Sree(chakra) Goparaju, Rafael Schaefer, Samir Perlaza, Iñaki Esnaola, Victoria Kostina, Salim ElRouayheb, Sander Wahls, Ronit Bustin, Nino(slav) Marina, Yue Zhao, Giacomo Bacci, Rene Guillaume, etc.

I would like to give very special thanks to my friends: Alex Xu, Cynthia Lu, Jiasi Chen, and Mia Chen for laughing and crying with me whenever I need them.

I am thankful to the friendly staff in Department of Electrical Engineering and Princeton University.

I really enjoyed the university resource – Baker Rink, which allowed me to start figure skating during my time at Princeton and made my dream from childhood come true.

Finally, I take this opportunity to express my profound gratitude to my parents and my husband Edward for their love, understanding and support – both spiritually and financially.

To my parents.

Contents

Abstract iii

Acknowledgements iv

1 Introduction **1**

1.1 Preview 1

2 Preliminaries **8**

2.1 Notation 8

2.2 Distortion Measure 9

2.3 Total Variation Distance 10

2.4 The Likelihood Encoder 11

2.5 Soft-covering Lemmas 11

3 Point-to-point Lossy Compression **14**

3.1 Introdution 14

3.2 Problem Formulation 15

3.3 Achievability Using the Likelihood Encoder 16

3.4 Excess Distortion 20

3.4.1 Probability of Excess Distortion 20

3.4.2 Non-asymptotic Performance 21

3.4.3 Comparison with Random Binning Based Proof 23

3.5 A Non-Asymptotic Analysis Using Jensen's Inequality 34

3.6 Summary 36

4 Multiuser Lossy Compression **38**

4.1 Introduction . . . 38

4.2 Approximation Lemma . . . 39

4.3 The Wyner-Ziv Setting . . . 39

4.3.1 Problem Formulation . . . 39

4.3.2 Proof of Achievability . . . 41

4.4 The Berger-Tung Inner Bound . . . 46

4.4.1 Problem Formulation . . . 46

4.4.2 Proof of Achievability . . . 48

4.5 Summary . . . 54

5 Rate-Distortion Based Security in the Noiseless Wiretap Channel **55**

5.1 Introduction . . . 55

5.2 Secure Source Coding Via Secret Key . . . 56

5.2.1 The Shannon Cipher System and Perfect Secrecy . . . 56

5.2.2 Naive Rate-Distortion Based Secrecy . . . 58

5.3 Secure Source Coding with Side Information at the Decoders . . . 60

5.3.1 Problem Formulation . . . 61

5.3.2 Inner Bound . . . 63

5.3.3 Outer Bound . . . 72

5.3.4 Special Cases . . . 73

5.3.5 Example . . . 74

5.4 Secure Source Coding with Causal Disclosure . . . 76

5.4.1 Problem Formulation . . . 77

5.4.2 Main Results . . . 79

5.4.3 Equivocation . . . 79

5.4.4 Binary Source . . . 81

5.4.5 Gaussian Source . . . 81

5.5 Summary . . . 89

6 Source-Channel Security in the Noisy Wiretap Channel **91**

6.1 Introduction . . . 91

6.2 Operational Separate Source-Channel Security . . . 92

6.2.1 Naive Formulation . . . 92

6.2.2 With Causal Source Disclosure at the Eavesdropper . . . 101

6.2.3 Binary Symmetric Broadcast Channel and Binary Source . . . 113

6.2.4 Applications to Multimode Fiber . . . 114

6.3 Joint Source-Channel Security . . . 122

6.3.1 Problem Revisit . . . 122

6.3.2 Secure Hybrid Coding . . . 124

6.3.3 Scheme Comparision . . . 130

6.3.4 The Perfect Secrecy Outer Bound . . . 131

6.3.5 Numerical Example . . . 132

6.4 Summary . . . 132

6.5 Appendix . . . 134

6.5.1 Proof of Lemma 6.1 . . . 134

6.5.2 Proof of Lemma 6.2 . . . 134

6.5.3 Proof of (6.24) . . . 137

6.5.4 Justification of the condition $\max_{(R_s,R_p)\in\mathcal{R}} R_s > 0$ . . . 138

6.5.5 Proof of Theorem 6.2 and Theorem 6.7 . . . 138

6.5.6 Proof of Lemma 6.3 . . . 146

6.5.7 Sufficient condition on Theorem 6.11 . . . 147

6.5.8 Proof of Theorem 6.15 . . . 148

7 Conclusion **159**

Bibliography **161**

Chapter 1

Introduction

1.1 Preview

Information theory, founded by Claude Shannon in 1948, has provided insights into the fundamental issues in data compression and date transmission. In addition to data compression and transmission, it has also impacted other areas such as cryptography, machine learning, and computer networks over the decades.

This thesis focuses on the aspect of information theory that 1) re-approaches the lossy data compression problems in achievability; 2) establishes the connection between security and lossy data compression in communication systems. With the rise of big data in analytics and data management, storing and transferring data reliably and securely has become a critical issue. Secure communication can take one of two routes: cryptography or information-theoretic secrecy. These areas are similar in the sense that both study how to transmit data securely to an intended receiver in the presence of an adversary. While cryptography deals with designing protocols and algorithms that make the ciphered text computationally hard to break with current technology, information-theoretic secrecy tackles a more fundamental question by asking whether there exists an encryption scheme such that the ciphered text is unbreakable even if the adversary is given unlimited computing power. In this thesis, we consider this latter approach. However, our approach to analyzing the security of a communication system is based on rate-distortion theory, which differs from the traditional approach of information-theoretic secrecy; instead of measuring the

statistical dependence between the original information and the ciphered text (by a quantity called equivocation), we use a distortion metric to evaluate how an adversary can make the most use of the leaked information to form a sequence of actions against the intended receiver. Traditional information-theoretic secrecy uses equivocation-rate to quantify the level of security, which requires a large size of secret key to allow a non-negligible amount of normalized equivocation. In our analysis of secure communication, although unlimited computing power is still granted to the adversary, we allow the adversary to potentially learn part of the ciphered text as long as the actions it can form are harmless to the intended receiver. This relaxation is proven to significantly reduce the secret key size.

A highlight of this thesis is a tool called the "likelihood encoder" introduced in Chapter 2. The likelihood encoder is a source compressor that achieves optimum rate given by the rate-distortion function for lossy compression. With this encoder, one is able to construct a communication system that can be approximated by a much simpler distribution that makes the analysis effortless. Although the likelihood encoder is mostly used to get new results in secrecy settings in this thesis, its applications to classical source coding provide a very different observation and treatment from other existing optimum rate achieving techniques.

Lossy Compression

Source coding, frequently referred to as data compression in applications, has been studied for decades. Basic technologies, such as JPEG and MP3, are ubiquitous in data storage. Traditionally, lossy compression in information theory studies the tradeoff between the rate of compression and the quality of reconstruction in the fundamental limit (rate-distortion theory) by allowing processing of the data in a big batch. An example of lossy compression applied to image storage is given in Fig. 1.1.

In Chapter 3, we review the simplest setting for lossy compression – point-to-point lossy compression. Within this simple setting, we provide a detailed step-by-step methodology using the likelihood encoder as a lossy source compressor and its corresponding analysis. This is the starting point to become familiarized with this tool, since the analysis for the more complicated systems in later chapters are variations of this basic case.

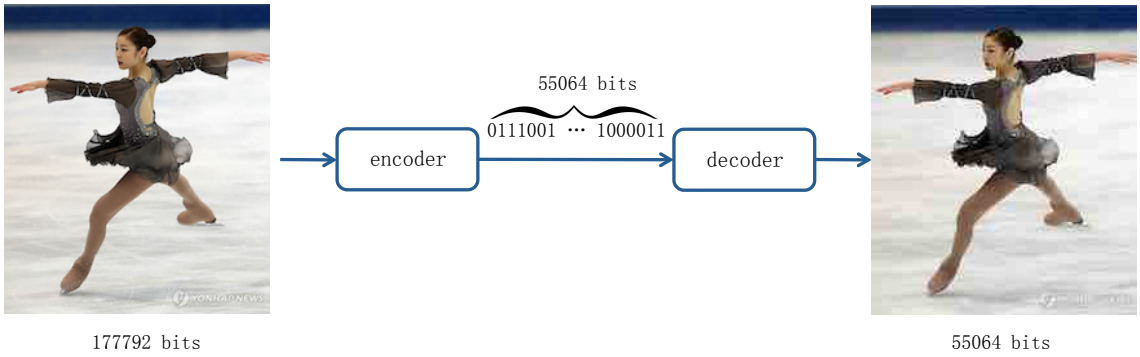

Figure 1.1: Lossy image compression: quality is traded off for size.

In Chapter 4, we extend the analysis using the likelihood encoder to more sophisticated setups: lossy compression with side information at the decoder, a.k.a the Wyner-Ziv setting, and multi-terminal lossy source compression with joint decoding, a.k.a. the Berger-Tung setting.

Secure Source Coding

The goal of secure source coding is to simultaneously 1) compress data efficiently so that an intended receiver can reconstruct the data with high fidelity and 2) encrypt the data in such a way that an eavesdropper does not learn anything "meaningful" about the data. Here the word "meaningful" has different interpretations. In Shannon's formulation [1] of perfect secrecy, in order to prevent the eavesdropper from learning "meaningful" information about the data source S, it is required that the encrypted message M available to the eavesdropper and the source are statistically independent, i.e. $P_S = P_{S|M}$. It turns out that, under this formulation, a separation principle applies: one can achieve optimality simply by first compressing the source with the most efficient compression algorithm and then encrypting the compressed data with a one-time pad. Although it may appear that we do not lose any efficiency in compression to the legitimate receiver, one should notice that this comes at the additional cost of sharing common randomness between the transmitter and the legitimate receiver, in this case, a shared secret key. Under the requirement for perfect secrecy, the secret key needs to be at least the size of the compressed data. This motivates us to ask the following questions: what if we only have a limited size of secret key? are we still able

to encrypt the data in a way that favors the legitimate users the most? These questions lead us to investigate partial secrecy.

Perfect secrecy is so fundamental and simple that it could be expressed with many different metrics. Information theorists like using entropy and mutual information, but that doesn't make it the correct way to state partial secrecy. The traditional approach to information theoretic security in the partial secrecy regime simply adopts the same metric for perfect secrecy. That is, instead of asking for $H(S|M) = H(S)$ (under perfect secrecy), one studies the tradeoff between the equivocation $H(S|M)$ and the secret key size. Such extension of using conditional entropy to measure partial secrecy is problematic in the sense that it does not capture how the eavesdropper can make use of the information to form actions against the legitimate users.

One may ask the question: if lossy reproduction is allowed at the legitimate receiver, why not allow that the eavesdropper recovers a distorted version of the message? Yamamoto [2] started reexamining the Shannon cipher system from a rate-distortion approach by studying the tradeoff among efficiency of compression, secret key size and the "minimum distortion" at the eavesdropper. Here the term "minimum distortion" simply means that, one should assume a rational eavesdropper that reconstructs the source so as to minimize the distortion. Under this formulation, the legitimate users (the transmitter and the legitimate receiver) who get to design the communication protocol and the adversary (the eavesdropper) are put in a game-theoretic setting, where they are playing a zero-sum game by properly choosing a payoff function that captures the distortions from both the legitimate receiver and the eavesdropper. Therefore, from the system designer's point of view, Yamamoto's setup focuses on finding a good encoding (compression and encryption) scheme under the assumption of a rational eavesdropper. Since we no longer have the luxury of sufficient secret key size to protect all of the data to achieve perfect secrecy, it becomes important to understand which information bits to hide to benefit the legitimate users the most in the sense of forcing a large distortion at the eavesdropper. Schieler and Cuff [3] showed that this relaxation of the secrecy requirement greatly reduced the size of secret key needed.

However, the shortcomings of Yamamoto's secrecy formulation for secrecy are exposed under a careful examination. Yamamoto's rate-distortion model of the Shannon cipher

system remains a valid game-theoretic setting if the legitimate receiver and the eavesdropper are each given only one chance to reproduce the source. In reality, the eavesdropper may have multiple chances to make its estimate. An intuitive example is the following. Suppose the source is a black-and-white image, one-bit pixels. One can force the highest possible distortion (under Hamming distortion) at the eavesdropper by simply flipping all the pixel bits, shown in Fig. 1.2. Yet the eavesdropper actually learns so much about the source that it can guarantee to decode the exact image within two attempts. Therefore, it may be overoptimistic to consider Yamamoto's model as secure source coding.

Figure 1.2: The Hamming distortion between the two images is at the maximum, but one can fully recover one image from the other without any loss of information.

A patch for Yamamoto's weak notion of security is provided by Cuff [4] [5] by allowing the eavesdropper to have access to causal information about the source. To be more intuitive, it is helpful to think under the game-theoretic setting where each player (transmitter/legitimate receiver and the eavesdropper) takes a sequence of actions. When the eavesdropper is calculating its current best move, it already observes the past moves of the transmitter/legitimate receiver. It is obvious that this modification favors the eavesdropper as it has the freedom to readjust its strategy after each move. Although this causal disclosure of the source may appear to be an unnatural reinforcement, it is shown by Schieler and Cuff [6] that the causal disclosure is key to specify a stable secrecy model for source coding that fully generalizes the traditional equivocation approach.

In Chapter 5, we discuss the rate-distortion based secure source coding in detail. We start with a review of Shannon's perfect secrecy formulation, followed by Yamamoto's game-

theoretic formulation. We then investigate a variation of Yamamoto's model by replacing the secret key with side information. That is, instead of having a shared secret key between the transmitter and the legitimate receiver, the legitimate receiver and the eavesdropper are given different side information that is correlated with the source during decoding. This is a good example of physical-layer security in source coding, where security is achieved by exploiting the physical structure of the communication network without using any common randomness explicitly. Finally, we strengthen the security model by considering causal source disclosure to the eavesdropper. The mathematical relation between the equivocation and the rate-distortion approaches is described.

Secure Source-Channel Coding

In joint source-channel coding, we want to compress the data by removing redundancy and transmit it with high fidelity over a noisy channel by adding redundancy at the same time. In the lucky cases such as point-to-point communication, where we have only one data source and one receiver, it is well known in information theory that separating the two processes (source coding and channel coding) is optimal when processing the data in a big batch. In other words, one does not lose any efficiency in the communication by first compressing the data source with the best compression algorithm and then structure the compressed information bits for the channel using the best channel code. Unfortunately, in the general cases of an arbitrary communication network, with and without security concerns, separating these two processes is not optimal, not even in the point-to-point communication from the non-asymptotic perspective.

For secure source-channel coding, physical-layer security also comes into play. Wyner [7] pioneered the area of information theoretic secrecy by studying secure transmission of data through a noisy broadcast channel, a.k.a. the wire-tap channel. In this setting, no secret key is used and the security is established only by taking advantage of the properties of the channel itself. Naturally, the legitimate receiver's channel needs to be stronger than the eavesdropper's channel in some sense to ensure secure transmission of the data; otherwise, what is decodable to the legitimate receiver is also decodable to the eavesdropper. Although physical-layer security is mainly studied in the context of secure channel

coding, many properties carry over to source-channel security. The obvious starting point in considering the latter problem is to conduct secure source coding and secure channel coding operationally separately. An operationally separate source-channel coding scheme is still a joint source-channel coding scheme in the sense that the source encoder and channel encoder need to first establish an agreement such that the output from the source encoder meets certain requirements, but once those requirements are satisfied, the source encoder and channel encoder have the freedom of choosing their own algorithms. Rarely is an operationally separate scheme optimal in secure source-channel settings, which motivates us to explore more sophisticated joint source-channel coding schemes.

A new joint source-channel coding approach was introduced in the context of multiuser lossy communication by Minero et al. [8]. This joint coding technique is unique and simple in the following aspects: 1) the source encoding and channel encoding operations decouple; 2) the same codeword is used for both source coding and channel coding; and 3) the scheme achieves best known performance among existing joint source-channel coding schemes. This hybrid coding is of particular interest because the structure of the code aligns well with our likelihood encoder. Although hybrid coding was originally demonstrated with the standard analysis using the joint-typicality encoder, the process can be greatly simplified by using the corresponding analysis of the likelihood encoder. In this thesis, we focus on the application of the hybrid coding technique to security in a wire-tap channel.

In Chapter 6, we discuss secure source-channel coding over a noisy wiretap channel through physical-layer security. Following the footsteps from Chapter 5 for secure source coding, we first study the operationally separate source-channel model under the rate-distortion based game-theoretic setting without causal source disclosure and the stronger secrecy setting by allowing causal source disclosure, respectively. We then apply the hybrid coding scheme to the setting with causal source disclosure and compare results with the operationally separate coding scheme.

Chapter 2

Preliminaries

2.1 Notation

A sequence $X_1, ..., X_n$ is denoted by X^n. Limits taken with respect to "$n \to \infty$" are abbreviated as "$\to_n$". When X denotes a random variable, x is used to denote a realization, $\mathcal{X}$ is used to denote the support of that random variable, and $\Delta_{\mathcal{X}}$ is used to denote the probability simplex of distributions with alphabet $\mathcal{X}$. A Markov relation is denoted by the symbol $-$. We use $\mathbb{E}_P$ and $\mathbb{P}_P$ to indicate expectation and probability taken with respect to a distribution P; however, when the distribution is clear from the context, the subscript will be omitted. To keep the notation uncluttered, the arguments of a distribution are sometimes omitted when the arguments' symbols match the subscripts of the distribution, e.g. $P_{X|Y}(x|y) = P_{X|Y}$. We use a bold capital letter $\mathbf{P}$ to denote that a distribution P is random (with respect to a random codebook).

In the analysis involving the likelihood encoder, P is reserved to denote the true induced distribution of a communication system specified by a particular choice of encoder and decoder. When $\overline{P}_X$ is used to denote a single-letter distribution, $\overline{P}_{X^n}$ is reserved to denote the independent and identically distributed (i.i.d.) process with marginal $\overline{P}_X$, i.e. $\overline{P}_{X^n}(x^n) = \prod_{t=1}^n \overline{P}_X(x_t)$. We use $\mathbb{R}$ to denote the set of real numbers and $\mathbb{R}^+$ to denote the nonnegative subset.

2.2 Distortion Measure

Definition 2.1. *A distortion measure is a mapping*

$$d\colon \mathcal{X} \times \mathcal{Y} \mapsto \mathbb{R}^{+} \tag{2.1}$$

from the set of source alphabet-reproduction alphabet pairs into the set of non-negative real numbers.

Definition 2.2. *The maximum distortion is defined as*

$$d_{max} = \max_{(x,y)\in\mathcal{X}\times\mathcal{Y}} d(x,y). \tag{2.2}$$

A distortion measure is said to be bounded if

$$d_{max} < \infty. \tag{2.3}$$

Definition 2.3. *The distortion between two sequences is defined to be the per-letter average distortion*

$$d(x^n, y^n) = \frac{1}{n}\sum_{t=1}^{n} d(x_t, y_t). \tag{2.4}$$

Two common distortion measures that are used frequently in this thesis are given as follows.

Definition 2.4. *The Hamming distortion is given by*

$$d(x,y) = \begin{cases} 0 & : x = y \\ 1 & : x \neq y \end{cases} \tag{2.5}$$

Definition 2.5. *The squared error distortion is given by*

$$d(x,y) = (x-y)^2. \tag{2.6}$$

To measure the distortion of X incurred by representing it as Y, we use the expected distortion $\mathbb{E}[d(X,Y)]$.

2.3 Total Variation Distance

The total variation distance between two probability measures P and Q on the same σ-algebra $\mathcal{F}$ of subsets of the sample space $\mathcal{X}$ is defined as

$$\|P-Q\|_{TV} \triangleq \sup_{\mathcal{A}\in\mathcal{F}} |P(\mathcal{A})-Q(\mathcal{A})|. \tag{2.7}$$

The total variation distance has the following properties that are used frequently throughout this thesis. These properties are all easy to prove and can be found in standard textbooks.

Property 2.1. *Total variation distance satisfies the following properties:*

(a) If $\mathcal{X}$ is countable, then total variation distance can be rewritten as

$$\|P-Q\|_{TV} = \frac{1}{2}\sum_{x\in\mathcal{X}} |p(x)-q(x)|, \tag{2.8}$$

where $p(\cdot)$ and $q(\cdot)$ are the probability mass functions of X under P and Q, respectively.

(b) Let $\varepsilon > 0$ and let $f(x)$ be a function in a bounded range with width $b \in \mathbb{R}^+$. Then

$$\|P-Q\|_{TV} < \varepsilon \implies \left|\mathbb{E}_P[f(X)] - \mathbb{E}_Q[f(X)]\right| < \varepsilon b. \tag{2.9}$$

(c) Total variation distance satisfies the triangle inequality. For any $S \in \Delta_{\mathcal{X}}$,

$$\|P-Q\|_{TV} \le \|P-S\|_{TV} + \|S-Q\|_{TV}. \tag{2.10}$$

(d) Let $P_X P_{Y|X}$ and $Q_X P_{Y|X}$ be two joint distributions on $\Delta_{\mathcal{X}\times\mathcal{Y}}$. Then

$$\|P_X P_{Y|X} - Q_X P_{Y|X}\|_{TV} = \|P_X - Q_X\|_{TV}. \tag{2.11}$$

(e) For any $P, Q \in \Delta_{\mathcal{X}\times\mathcal{Y}}$,

$$\|P_X - Q_X\|_{TV} \leq \|P_{XY} - Q_{XY}\|_{TV}. \tag{2.12}$$

2.4 The Likelihood Encoder

We now define the likelihood encoder, operating at rate R, which receives a sequence $x_1, ..., x_n$ and maps it to a message $M \in [1 : 2^{nR}]$. In normal usage, a decoder will then use M to form an approximate reconstruction of the $x_1, ..., x_n$ sequence.

The encoder is specified by a codebook of $u^n(m)$ sequences and a joint distribution P_{UX}. Consider the likelihood function for each codeword, with respect to a memoryless channel from U to X, defined as follows:

$$\mathcal{L}(m|x^n) \triangleq P_{X^n|U^n}(x^n|u^n(m)) = \prod_{t=1}^{n} P_{X|U}(x_t|u_t(m)). \tag{2.13}$$

A likelihood encoder is a stochastic encoder that determines the message index with probability proportional to $\mathcal{L}(m|x^n)$, i.e.

$$P_{M|X^n}(m|x^n) = \frac{\mathcal{L}(m|x^n)}{\sum_{m' \in [1:2^{nR}]} \mathcal{L}(m'|x^n)} \propto \mathcal{L}(m|x^n). \tag{2.14}$$

2.5 Soft-covering Lemmas

Now we introduce the core lemmas that serve as the foundation for analyzing several source coding problems in both lossy compression and secrecy. One can consider the role of the soft-covering lemma in analyzing the likelihood encoder as analogous to that of the joint asymptotic equipartition property (J-AEP) which is used for the analysis of joint-typicality encoders [9] [10]. The general idea of the soft-covering lemma is that the distribution induced by selecting uniformly from a random codebook and passing the codeword through a memoryless channel is close to an i.i.d. distribution as long as the codebook size is large enough.

Two versions of soft-covering lemmas are presented. The basic soft-covering lemma is in general sufficient for the achievability proofs of lossy compression settings. However, the superposition soft-covering lemma is required for analyzing the performance of a communication system with secrecy constraints.

Here we give a short review on the genesis of the soft-covering lemmas. This concept of soft-cover was first introduced by Wyner [7] in the context of common information. Although Wyner proved the result under normalized relative entropy instead of total variation distance, the exact metric that was used is not so important. This concept was re-examined in a stricter sense in [12] under the metric of total variation distance, where the result involves both achievability and converse. In [12], the soft-covering concept is referred to as "resolvability" and the achievability part is readily addressed by Wyner's soft-covering principle under a different metric. The soft-covering concept was then generalized in [11] for distributed channel synthesis where multiple variations of the basic soft-covering concept were investigated, such as the superposition versions of the soft-covering. The result on soft-covering from [11] also provided an additional exponential bound.

Lemma 2.1. *(**Basic soft-covering**, [11] [12] [7]) Given a joint distribution P_{UX}, let $\mathcal{C}^{(n)}$ be a random collection of sequences $U^n(m)$, with $m = 1, ..., 2^{nR}$, each drawn independently and i.i.d. according to P_U. Denote by $\mathbf{P}_{X^n}$ the output distribution induced by selecting an index m uniformly at random and applying $U^n(m)$ to the memoryless channel specified by $P_{X|U}$. Then if $R > I(X;U)$,*

$$\mathbb{E}_{\mathcal{C}^{(n)}}\left[\left\|\mathbf{P}_{X^n} - \prod_{t=1}^{n} P_X\right\|_{TV}\right] \leq e^{-\gamma n}, \tag{2.15}$$

for some $\gamma > 0$.

Lemma 2.2. *(**Superposition soft-covering for secrecy**, [6]) Given a joint distribution P_{UVXZ}, let $\mathcal{C}_U^{(n)}$ be a random codebook of 2^{nR_1} sequences in $\mathcal{U}^n$, each drawn independently according to $\prod_{t=1}^{n} P_U(u_t)$ and indexed by $m_1 \in [1 : 2^{nR_1}]$. For each m_1, let $\mathcal{C}_V^{(n)}(m_1)$ be a random codebook of 2^{nR_2} sequences in $\mathcal{V}^n$, each drawn independently according to*

$\prod_{t=1}^{n} P_{V|U}(v_t|u_t(m_1))$ *and indexed by* $(m_1, m_2) \in [1 : 2^{nR_2}]$. *Let*

$$\begin{aligned} & \mathbf{P}_{M_1 M_2 X^n Z^k}(m_1, m_2, x^n, z^k) \\ \triangleq \; & 2^{-n(R_1+R_2)} \prod_{t=1}^{n} P_{X|UV}(x_t|U_t(m_1), V_t(m_1, m_2)) P_{Z|XUV}(z_t|x_t, u_t, v_t)^{\mathbb{1}\{t\in[1:k]\}}, \end{aligned} \tag{2.16}$$

and

$$\begin{aligned} & \mathbf{Q}_{M_1 X^n Z^k}(m_1, x^n, z^k) \\ \triangleq \; & 2^{-nR_1} \prod_{t=1}^{n} P_{X|U}(x_t|U_t(m_1)) P_{Z|XU}(z_t|x_t, U_t(m_1))^{\mathbb{1}\{t\in[1:k]\}} \end{aligned} \tag{2.17}$$

If $R_2 > I(X; V|U)$, *then*

$$\mathbb{E}_{\mathcal{C}^{(n)}} \left[\left\| \mathbf{P}_{M_1 X^n Z^k} - \mathbf{Q}_{M_1 X^n Z^k} \right\|_{TV} \right] \leq e^{-\gamma n} \tag{2.18}$$

for any $\alpha < \frac{R_2 - I(X;V|U)}{I(Z;V|UX)}$, $k \leq \alpha n$, *where* $\gamma > 0$ *depends on the gap* $\frac{R_2 - I(X;V|U)}{I(Z;V|UX)} - \alpha$.

Chapter 3

Point-to-point Lossy Compression

3.1 Introdution

Rate-distortion theory, founded by Shannon in [13] and [14], provides the fundamental limits of lossy source compression. The minimum rate required to represent an i.i.d. source sequence under a given tolerance of distortion is given by the rate-distortion function. Standard proofs [9], [10] of achievability for these rate-distortion problems often use joint-typicality encoding, i.e. the encoder looks for a codeword that is jointly typical with the source sequence.

In this chapter, we propose using a likelihood encoder to achieve these source coding results. The likelihood encoder is a stochastic encoder. As stated in [15], for a chosen joint distribution P_{XY}, to encode a source sequence $x_1, ..., x_n$ (i.e. x^n) with codebook $y^n(m)$, the encoder stochastically chooses an index m proportional to the likelihood of $y^n(m)$ passed through the memoryless "test channel" $P_{X|Y}$.

The advantage of using such an encoder is that it naturally leads to an idealized distribution which is simple to analyze, based on the "test channel." The distortion performance of the idealized distribution carries over to the true system induced distribution because the two distributions are shown to be close in total variation.

The application of the likelihood encoder together with the soft-covering lemma is not limited to only discrete alphabets. The proof for sources from continuous alphabets is readily included, since the soft-covering lemma imposes no restriction on alphabet size.

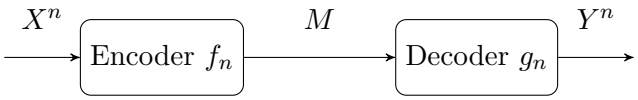

Figure 3.1: Point-to-point lossy compression setup

Therefore, no extra work, i.e. quantization of the source, is needed to extend the standard proof for discrete sources to continuous sources as in [10].

It is worth noting that this encoder has also been used in [16] for achieving lossy compression results. However, their analysis is very different from ours.

3.2 Problem Formulation

Rate-distortion theory determines the optimal compression rate R for an i.i.d. source sequence X^n distributed according to $X_t \sim P_X$ with the following constraints:

- Encoder $f_n : \mathcal{X}^n \mapsto \mathcal{M}$ (possibly stochastic);
- Decoder $g_n : \mathcal{M} \mapsto \mathcal{Y}^n$ (possibly stochastic);
- Compression rate: R, i.e. $|\mathcal{M}| = 2^{nR}$.

The system performance is measured according to the time-averaged distortion (as defined in the Section 2.1):

- Time averaged distortion: $d(X^n, Y^n) = \frac{1}{n}\sum_{t=1}^{n} d(X_t, Y_t)$.

Definition 3.1. *A rate distortion pair (R, D) is achievable if there exists a sequence of rate R encoders and decoders (f_n, g_n), such that*

$$\limsup_{n\to\infty} \mathbb{E}[d(X^n, Y^n)] \leq D.$$

Definition 3.2. *The rate distortion function is* $R(D) \triangleq \inf_{\{(R,D) \text{ is achievable}\}} R$.

The above mathematical formulation is illustrated in Fig. 5.4. The characterization of this fundamental quantity in information theory is given in [14] as

$$R(D) = \min_{P_{Y|X}:\mathbb{E}[d(X,Y)]\leq D} I(X;Y), \tag{3.1}$$

where the mutual information is taken with respect to

$$P_{XY} = P_X P_{Y|X}. \tag{3.2}$$

In other words, we are able to achieve distortion level D with any rate less than $R(D)$ given in the right hand side of (3.1).

The converse part of the proof for (3.1) can be found in standard textbooks such as [9] [10], and is not presented here.

3.3 Achievability Using the Likelihood Encoder

To prove achievability, we will use the likelihood encoder and approximate the overall behavior of the system by a well-behaved distribution. The soft-covering lemma allows us to claim that the approximating distribution matches the system.

Here we make an additional note on the notation. As mentioned in the Section 2.1, P is reserved for denoting the system induced distribution. The single letter distributions appearing in (3.1) are replaced with $\overline{P}$ in the following proof. The marginal and conditional distributions derived from $\overline{P}_{XY}$ are denoted as $\overline{P}_X$, $\overline{P}_Y$, $\overline{P}_{X|Y}$ and $\overline{P}_{Y|X}$. Since $\overline{P}_X = P_X$, these can be used interchangeably. We use $\overline{P}_{X^nY^n}$ to denote the product of an i.i.d. distribution, i.e.

$$\overline{P}_{X^nY^n} = \prod_{t=1}^{n} \overline{P}_{XY}, \tag{3.3}$$

and similarly for the marginal and conditional distributions derived from $\overline{P}_{XY}$.

Let $R > R(D)$, where $R(D)$ is from the right hand side of (3.1). We prove that R is achievable for distortion D. By the rate-distortion formula stated in (3.1), we can fix $\overline{P}_{Y|X}$ such that $R > I(X;Y)$ and $\mathbb{E}[d(X,Y)] < D$, where the mutual information and the expectation are taken with respect to $\overline{P}_{XY}$. We will use the likelihood encoder derived from $\overline{P}_{XY}$ and a random codebook $\{y^n(m)\}$ generated according to $\overline{P}_Y$ to prove the result. The decoder will simply reproduce $y^n(M)$ upon receiving the message M.

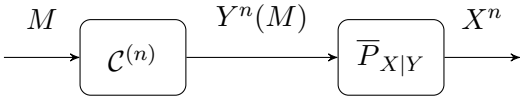

Figure 3.2: Idealized distribution conditioned on a codebook $\mathcal{C}^{(n)}$ with test channel $\overline{P}_{X|Y}$.

The distribution induced by the encoder and decoder is

$$\begin{aligned} & \mathbf{P}_{X^n M Y^n}(x^n, m, y^n) \\ = \; & P_{X^n}(x^n)\mathbf{P}_{M|X^n}(m|x^n)\mathbf{P}_{Y^n|M}(y^n|m) \qquad (3.4) \\ \triangleq \; & P_{X^n}(x^n)\mathbf{P}_{LE}(m|x^n)\mathbf{P}_D(y^n|m) \qquad (3.5) \end{aligned}$$

where $\mathbf{P}_{LE}$ is the likelihood encoder and $\mathbf{P}_D$ is a codeword lookup decoder.

We now concisely restate the behavior of the encoder and decoder, as components of the induced distribution.

Codebook generation: We independently generate 2^{nR} sequences in $\mathcal{Y}^n$ according to $\prod_{t=1}^n \overline{P}_Y(y_t)$ and index them by $m \in [1 : 2^{nR}]$. We use $\mathcal{C}^{(n)}$ to denote the random codebook.

Encoder: The encoder $\mathbf{P}_{LE}(m|x^n)$ is the likelihood encoder that chooses M stochastically with probability proportional to the likelihood function given by

$$\mathcal{L}(m|x^n) = \overline{P}_{X^n|Y^n}(x^n|Y^n(m)). \qquad (3.6)$$

Decoder: The decoder $\mathbf{P}_D(y^n|m)$ is a codeword lookup decoder that simply reproduces $Y^n(m)$.

Analysis: We will consider two distributions for the analysis, the induced distribution $\mathbf{P}$ and an approximating distribution $\mathbf{Q}$, which is much easier to analyze. We will show that $\mathbf{P}$ and $\mathbf{Q}$ are close in total variation (on average over the random codebook). Hence, $\mathbf{P}$ achieves the performance of $\mathbf{Q}$.

Design the approximating distribution $\mathbf{Q}$ via a uniform distribution over a random codebook and a test channel $\overline{P}_{X|Y}$ as shown in Fig. 3.2. We will refer to a distribution of this structure as an idealized distribution. The joint distribution under the idealized

distribution $\mathbf{Q}$ shown in Fig. 3.2 can be written as

$$\begin{aligned}
& \mathbf{Q}_{X^n M Y^n}(x^n, m, y^n) \\
= \;& Q_M(m)\mathbf{Q}_{Y^n|M}(y^n|m)\mathbf{Q}_{X^n|M}(x^n|m) && (3.7)\\
= \;& \frac{1}{2^{nR}}\mathbb{1}\{y^n = Y^n(m)\}\prod_{t=1}^{n}\overline{P}_{X|Y}(x_t|Y_t(m)) && (3.8)\\
= \;& \frac{1}{2^{nR}}\mathbb{1}\{y^n = Y^n(m)\}\prod_{t=1}^{n}\overline{P}_{X|Y}(x_t|y_t). && (3.9)
\end{aligned}$$

The idealized distribution $\mathbf{Q}$ has the following property: for any $(x^n, y^n) \in \mathcal{X}^n \times \mathcal{Y}^n$,

$$\begin{aligned}
& \mathbb{E}_{\mathcal{C}^{(n)}}[\mathbf{Q}_{X^n Y^n}(x^n, y^n)] \\
= \;& \mathbb{E}_{\mathcal{C}^{(n)}}\left[\frac{1}{2^{nR}}\sum_m \mathbb{1}\{y^n = Y^n(m)\}\right]\prod_{t=1}^{n}\overline{P}_{X|Y}(x_t|y_t) && (3.10)\\
= \;& \frac{1}{2^{nR}}\sum_m \mathbb{E}_{\mathcal{C}^{(n)}}[\mathbb{1}\{y^n = Y^n(m)\}]\prod_{t=1}^{n}\overline{P}_{X|Y}(x_t|y_t) && (3.11)\\
= \;& \frac{1}{2^{nR}}\sum_m \overline{P}_{Y^n}(y^n)\prod_{t=1}^{n}\overline{P}_{X|Y}(x_t|y_t) && (3.12)\\
= \;& \overline{P}_{X^n Y^n}(x^n, y^n). && (3.13)
\end{aligned}$$

This implies, in particular, that the distortion under the idealized distribution $\mathbf{Q}$ averaged over the random codebook conveniently simplifies to $\mathbb{E}_{\overline{P}}[d(X, Y)]$. That is,

$$\begin{aligned}
& \mathbb{E}_{\mathcal{C}^{(n)}}\left[\mathbb{E}_{\mathbf{Q}}[d(X^n, Y^n)]\right] \\
= \;& \mathbb{E}_{\mathcal{C}^{(n)}}\left[\sum_{x^n, y^n}\mathbf{Q}_{X^n Y^n}(x^n, y^n)d(x^n, y^n)\right] && (3.14)\\
= \;& \sum_{x^n, y^n}\mathbb{E}_{\mathcal{C}^{(n)}}[\mathbf{Q}_{X^n Y^n}(x^n, y^n)]d(x^n, y^n) && (3.15)\\
= \;& \sum_{x^n, y^n}\overline{P}_{X^n, Y^n}(x^n, y^n)d(x^n, y^n) && (3.16)\\
= \;& \mathbb{E}_{\overline{P}}[d(X^n, Y^n)] && (3.17)\\
= \;& \mathbb{E}_{\overline{P}}[d(X, Y)], && (3.18)
\end{aligned}$$

where (3.16) follows from (3.13). It is worth emphasizing that although $\mathbf{Q}$ is very different from the i.i.d. distribution on (X^n, Y^n), it is exactly the i.i.d. distribution when averaged over codebooks and thus achieves the same expected distortion.

Our motivation for using the likelihood encoder comes from this construction of $\mathbf{Q}$. Notice the following **important** facts:

$$\mathbf{Q}_{M|X^n}(m|x^n) = \mathbf{P}_{LE}(m|x^n), \tag{3.19}$$

and

$$\mathbf{Q}_{Y^n|M}(y^n|m) = \mathbf{P}_D(y^n|m). \tag{3.20}$$

Now invoking the basic soft-covering lemma (Lemma 2.1), since $R > I(X;Y)$, we have

$$\mathbb{E}_{\mathcal{C}^{(n)}}\left[\|\overline{P}_{X^n} - \mathbf{Q}_{X^n}\|_{TV}\right] \leq \epsilon_n, \tag{3.21}$$

where $\epsilon_n \to_n 0$. This gives us

$$\begin{aligned} & \mathbb{E}_{\mathcal{C}^{(n)}}\left[\|\mathbf{P}_{X^nY^n} - \mathbf{Q}_{X^nY^n}\|_{TV}\right] \\ \leq\ & \mathbb{E}_{\mathcal{C}^{(n)}}\left[\|\mathbf{P}_{X^nY^nM} - \mathbf{Q}_{X^nY^nM}\|_{TV}\right] && (3.22) \\ \leq\ & \epsilon_n, && (3.23) \end{aligned}$$

where (3.22) follows from Property 2.1(e) and (3.23) follows from (3.19),(3.20) and Property 2.1(d).

By Property 2.1(b),

$$|\mathbb{E}_{\mathbf{P}}[d(X^n, Y^n)] - \mathbb{E}_{\mathbf{Q}}[d(X^n, Y^n)]| \leq d_{max}\|\mathbf{P} - \mathbf{Q}\|_{TV}. \tag{3.24}$$

Now we apply the random coding argument.

$$
\begin{aligned}
& \mathbb{E}_{\mathcal{C}^{(n)}}\left[\mathbb{E}_{\mathbf{P}}[d(X^n, Y^n)]\right] \\
\leq\ & \mathbb{E}_{\mathcal{C}^{(n)}}\left[\mathbb{E}_{\mathbf{Q}}[d(X^n, Y^n)]\right] + \mathbb{E}_{\mathcal{C}^{(n)}}\left[\left|\mathbb{E}_{\mathbf{P}}[d(X^n, Y^n)] - \mathbb{E}_{\mathbf{Q}}[d(X^n, Y^n)]\right|\right] && (3.25) \\
\leq\ & \mathbb{E}_{\overline{P}}[d(X, Y)] + d_{max}\mathbb{E}_{\mathcal{C}^{(n)}}\left[\|\mathbf{P}_{X^nY^n} - \mathbf{Q}_{X^nY^n}\|_{TV}\right] && (3.26) \\
\leq\ & \mathbb{E}_{\overline{P}}[d(X, Y)] + d_{max}\epsilon_n && (3.27)
\end{aligned}
$$

where (3.26) follows from (3.18) and (3.24); (3.27) follows from (3.23). Taking the limit on the both sides gives:

$$\limsup_{n\to\infty} \mathbb{E}_{\mathcal{C}^{(n)}}\left[\mathbb{E}_{\mathbf{P}}[d(X^n, Y^n)]\right] \leq D, \tag{3.28}$$

Therefore, there exists a codebook satisfying the requirement. ■

3.4 Excess Distortion

3.4.1 Probability of Excess Distortion

The proof presented in the previous section is for the average distortion criterion, i.e. $\limsup_{\to\infty} \mathbb{E}\left[d(X^n, Y^n)\right] \leq D$. However, it is not hard to modify the proofs to show that they also hold for excess distortion.

With the same setup as in Section 3.2, we change the average distortion requirement in the definition of achievability (Definition 3.1) to excess distortion.

Definition 3.3. *A rate distortion pair (R, D) is achievable under **excess distortion** if there exists a sequence of rate R encoders and decoders (f_n, g_n), such that*

$$\mathbb{P}\left[d(X^n, Y^n) > D\right] \to_n 0.$$

The corresponding rate-distortion function is still given by $R(D)$ in (3.1).

For the excess distortion, we will use the exact same encoding/decoding scheme, along with the same random codebook $\mathcal{C}^n$, from Section 3.3. We make the following modifications.

We replace (3.14) to (3.18) with

$$\begin{aligned}
& \mathbb{E}_{\mathcal{C}^{(n)}}\left[\mathbb{P}_{\mathbf{Q}}\left[d(X^n,Y^n)>D\right]\right] \\
= \;& \mathbb{E}_{\mathcal{C}^{(n)}}\left[\sum_{x^n,y^n}\mathbf{Q}_{X^nY^n}(x^n,y^n)\mathbb{1}\{d(x^n,y^n)>D\}\right] && (3.29)\\
= \;& \sum_{x^n,y^n}\mathbb{E}_{\mathcal{C}^{(n)}}[\mathbf{Q}_{X^nY^n}(x^n,y^n)]\mathbb{1}\{d(x^n,y^n)>D\} && (3.30)\\
= \;& \sum_{x^n,y^n}\overline{P}_{X^n,Y^n}(x^n,y^n)\mathbb{1}\{d(x^n,y^n)>D\} && (3.31)\\
= \;& \mathbb{P}_{\overline{P}}[d(X^n,Y^n)>D], && (3.32)
\end{aligned}$$

and replace (3.25) to (3.27) with

$$\begin{aligned}
& \mathbb{E}_{\mathcal{C}^{(n)}}\left[\mathbb{P}_{\mathbf{P}}[d(X^n,Y^n)>D]\right] \\
\leq \;& \mathbb{E}_{\mathcal{C}^{(n)}}\left[\mathbb{P}_{\mathbf{Q}}[d(X^n,Y^n)>D]\right]+\epsilon_n && (3.33)\\
= \;& \mathbb{P}_{\overline{P}}\left[d(X^n,Y^n)>D\right]+\epsilon_n && (3.34)
\end{aligned}$$

where the last step follows from (3.32). Therefore, there exists a codebook that satisfies the requirement. ■

3.4.2 Non-asymptotic Performance

Let the achievable rate-distortion region $\mathcal{R}$ be

$$\mathcal{R} \triangleq \{(R,D) : R > R(D)\}.$$

For a fixed $(R,D) \in \mathcal{R}$, we aim to minimize the probability of excess distortion, using a random codebook and the likelihood encoder, over valid choices of $\overline{P}_{Y|X}$, and evaluate how fast the excess distortion decays with blocklength n under the optimal $\overline{P}_{Y|X}$. Mathematically, we want to obtain

$$\inf_{\overline{P}_{Y|X}} \mathbb{E}_{\mathcal{C}^n}\left[\mathbb{P}_{\mathbf{P}}\left[d(X^n,Y^n)>D\right]\right], \tag{3.35}$$

where the subscript $\mathbf{P}$ indicates probability taken with respect to the system induced distribution.

To evaluate how fast the probability of excess distortion approaches zero, note in (3.34) that the first term is governed (approximately) by the gap $D - \mathbb{E}_{\overline{P}}[d(X,Y)]$ and the second term is governed (approximately) by the the gap $R - I(X;Y)$, where the mutual information is with respect to distribution $\overline{P}_{XY}$. To see this, observe that for any $\beta > 0$,

$$\begin{aligned}
\epsilon_n' &\triangleq \mathbb{P}_{\overline{P}}[d(X^n, Y^n) > D] && (3.36)\\
&= \mathbb{P}_{\overline{P}}\left[\frac{1}{n}\sum_{t=1}^{n} d(X_t, Y_t) > D\right] && (3.37)\\
&\leq \inf_{\beta>0}\left[\frac{\mathbb{E}_{\overline{P}}[2^{\beta d(X,Y)}]}{2^{\beta D}}\right]^n && (3.38)\\
&= \exp\left(-n\log\left(\inf_{\beta>0}\mathbb{E}_{\overline{P}}\left[2^{\beta(d(X,Y)-D)}\right]\right)^{-1}\right) && (3.39)\\
&= \exp\left(-n\eta(\overline{P}_{Y|X})\right) && (3.40)
\end{aligned}$$

where (3.38) follows from the Chernoff bound and we have implicitly defined

$$\eta(\overline{P}_{Y|X}) \triangleq \log\left(\inf_{\beta>0}\mathbb{E}_{\overline{P}}\left[2^{\beta(d(X,Y)-D)}\right]\right)^{-1}. \tag{3.41}$$

An upper bound on the second term in (3.34) is given in [11], reproduced below:

$$\epsilon_n \leq \frac{3}{2}\exp\left(-n\gamma(\overline{P}_{Y|X})\right), \tag{3.42}$$

where

$$\gamma(\overline{P}_{Y|X}) \triangleq \max_{\alpha\geq 1, \alpha'\leq 2}\frac{\alpha-1}{2\alpha-\alpha'}\left(R - \check{I}_{\overline{P},\alpha}(X;Y) + (\alpha'-1)(\check{I}_{\overline{P},\alpha}(X;Y) - \bar{I}_{\overline{P},\alpha'}(X;Y))\right) \tag{3.43}$$

$$\check{I}_{\overline{P},\alpha}(X;Y) \triangleq \frac{1}{\alpha-1}\log\left(\mathbb{E}_{\overline{P}}\left[\left(\frac{\overline{P}_{X,Y}(X,Y)}{\overline{P}_X(X)\overline{P}_Y(Y)}\right)^{\alpha-1}\right]\right) \tag{3.44}$$

$$\bar{I}_{\overline{P},\alpha'}(X,Y) \triangleq \frac{1}{\alpha'-1}\log\left(\left(\mathbb{E}_{\overline{P}_X}\left[\sqrt{\mathbb{E}_{\overline{P}_{Y|X}}\left[\left(\frac{\overline{P}_{XY}(X,Y)}{\overline{P}_X(X)\overline{P}_Y(Y)}\right)^{\alpha'-1}\right]}\right]\right)^2\right) \tag{3.45}$$

Both ϵ'_n and ϵ_n decay exponentially with n. To obtain an upper bound on the excess distortion given in (3.35), we now have a new optimization problem in the following form:

$$\inf_{\overline{P}_{Y|X}} \exp\left(-n\eta(\overline{P}_{Y|X})\right) + \frac{3}{2}\exp\left(-n\gamma(\overline{P}_{Y|X})\right), \tag{3.46}$$

where $\eta(\overline{P}_{Y|X})$ and $\gamma(\overline{P}_{Y|X})$ are defined in (3.41) and (3.43). Note that only choices of $\overline{P}_{Y|X}$ such that $\mathbb{E}_{\overline{P}}[d(X,Y)] < D$ and $I(X;Y) < R$ should be considered for the optimization, as other choices render the bound degenerate.

We can relax (3.46) to obtain a simple upper bound on the excess distortion $\mathbb{P}_P[d(X^n, Y^n) > D]$ given in the following theorem.

Theorem 3.1. *The excess distortion $\mathbb{P}_P[d(X^n, Y^n) > D]$ using the likelihood encoder is upper bounded by*

$$\inf_{\overline{P}_{Y|X}} \frac{5}{2}\exp\left(-n\min\left\{\eta\left(\overline{P}_{Y|X}\right), \gamma\left(\overline{P}_{Y|X}\right)\right\}\right), \tag{3.47}$$

where $\eta(\overline{P}_{Y|X})$ and $\gamma(\overline{P}_{Y|X})$ are given in (3.41) *and* (3.43)*, respectively.*

Remark 1. *Note that this bound does not achieve the exponent that we know to be optimal [17, Theorem 9.5] for rate-distortion theory. It may very well be that the likelihood encoder does not achieve the optimal exponent, though it may also be an artifact of our proof or the bound for the soft-covering lemma.*

3.4.3 Comparison with Random Binning Based Proof

The likelihood encoder proof technique is similar to the random binning based analysis approach presented in [18] in many ways. In this section, we will compare the two schemes along with their non-asymptotic behaviors.

We shall first provide a recap of the scheme for point-to-point lossy compression that uses the so-called "output statistics of random binning" in the proof. Below we modify the way it was originally presented in [18] to ease the comparison with the proof given in Section 3.3.

The Proportional-Probability Encoder

We start by defining a source encoder that looks very similar in form to a likelihood encoder defined in Section 2.4. Like any other source encoder, a *proportional-probability encoder* receives a sequence $x_1, ..., x_n$ and produces an index $m \in [1 : 2^{nR}]$.

A codebook is specified by a non-empty collection $\mathcal{C}$ of sequences $y^n \in \mathcal{Y}^n$ and indices $m(y^n)$ assigned to each $y^n \in \mathcal{Y}^n$. The codebook and a joint distribution P_{XY} specify the proportional-probability encoder.

Let $\mathcal{G}(m|x^n)$ be the probability, as a result of passing x^n through a memoryless channel given by $P_{Y|X}$, of finding Y^n in the collection $\mathcal{C}$ and retrieving the index m from the codebook:

$$\begin{aligned} \mathcal{G}(m|x^n) &\triangleq \mathbb{P}_{P_{Y^n|X^n}}\left[Y^n \in \mathcal{C}, m(Y^n) = m \mid X^n = x^n\right] && (3.48) \\ &= \sum_{y^n \in \mathcal{C}} P_{Y^n|X^n}(y^n|x^n)\mathbb{1}\{m(y^n) = m\}, && (3.49) \end{aligned}$$

where $P_{Y^n|X^n} = \prod_{t=1}^{n} P_{Y|X}$.

A proportional-probability encoder is a stochastic encoder that determines the message index with probability proportional to $\mathcal{G}(m|x^n)$, i.e.

$$P_{M|X^n}(m|x^n) = \frac{\mathcal{G}(m|x^n)}{\sum_{m'=[1:2^{nR}]} \mathcal{G}(m'|x^n)} \propto \mathcal{G}(m|x^n). \tag{3.50}$$

Scheme Using the Proportional-Probability Encoder

Before going into the achievability scheme, we first state a lemma that will be used in the analysis.

Lemma 3.1 (Independence of random binning - Theorem 1 of [18])**.** *Given a probability mass function P_{XY}, and each $y^n \in \mathcal{Y}^n$ is independently assigned to a bin index $b \in [1 : 2^{nR_b}]$ uniformly at random, where $B(y^n)$ denotes this random assignment. Define the joint distribution*

$$\mathbf{P}_{X^n Y^n B}(x^n, y^n, b) \triangleq \prod_{i=1}^{n} P_{XY}(x_i, y_i)\mathbb{1}\{B(y^n) = b\}. \tag{3.51}$$

If $R_b < H(Y|X)$, then we have

$$\mathbb{E}_{\mathcal{B}}\left[\left\|\mathbf{P}_{X^nB} - P_{X^n}P_B^U\right\|_{TV}\right] \to_n 0, \tag{3.52}$$

where P_B^U is a uniform distribution on $[1 : 2^{nR_b}]$ and $\mathbb{E}_{\mathcal{B}}$ denotes expectation taken over the random binning.

We now outline the encoding-decoding scheme based on the proportional-probability encoder.

Fix a $\overline{P}_{Y|X}$ that satisfies $\mathbb{E}_{\overline{P}}[d(X,Y)] < D$ and choose the rates R and R' to satisfy $R' < H(Y|X)$ and $R + R' > H(Y)$, where the entropies are with respect to distribution $\overline{P}_{XY}$.

Codebook generation: Each $y^n \in \mathcal{Y}^n$ is randomly and independently assigned to the codebook $\mathcal{C}$ with probability $2^{-nR'}$. Then, independent of the construction of $\mathcal{C}$, each $y^n \in \mathcal{Y}^n$ is independently assigned uniformly at random to one of 2^{nR} bins indexed by M.

Encoder: The encoder $\mathbf{P}_{PPE}(m|x^n)$ is the proportional-probability encoder with respect to $\overline{P}$. Specifically, the encoder chooses M stochastically according to (3.50), with $\mathcal{G}$ based on $\overline{P}$ as follows:

$$\mathcal{G}(m|x^n) = \sum_{y^n \in \mathcal{C}} \overline{P}_{Y^n|X^n}(y^n|x^n)\mathbb{1}\{m(y^n) = m\}, \tag{3.53}$$

where $\overline{P}_{Y^n|X^n}(y^n|x^n) = \prod_{t=1}^n \overline{P}_{Y|X}(y_t|x_t)$.

Decoder: The decoder $\mathbf{P}_D(y^n|m)$ selects a y^n reconstruction that is in $\mathcal{C}$ and has index $m = M$. There will usually be more than one such y^n sequence, but rarely will there be more than one "good" choice, due to the rates used. The decoder can choose that most probable y^n sequence or the unique typical sequence, etc. The proof in [18] uses a "mismatch stochastic likelihood coder" (MSLC) [16] [19], and we will use their analysis for the performance bound in Section 3.4.3.

Remark 2. *Intuitively, a decoder can successfully decode the sequence intended by the encoder since there are roughly $2^{nH(Y)}$ typical y^n sequences, and the collection $\mathcal{C}$ together*

with the binning index M provides high enough rate $R' + R > H(Y)$ to uniquely identify the sequence.

Analysis: The above scheme specifies a system induced distribution of the form

$$\mathbf{P}_{X^n M Y^n}(x^n, m, y^n) = P_{X^n}(x^n)\mathbf{P}_{PPE}(m|x^n)\mathbf{P}_D(y^n|m).$$

To analyze the above scheme, we start by replacing the codebook used for encoding and decoding with a set of codebooks. Recall that the codebook consists of a collection $\mathcal{C}$ and index assignments $m(y^n)$ that are both randomly constructed. Now consider a set of $2^{nR'}$ collections $\{\mathcal{C}_f\}_{f\in[1:2^{nR'}]}$, indexed by f, created by assigning each y^n sequence in $\mathcal{Y}^n$ randomly to exactly one collection equiprobably. From this we define a set of $2^{nR'}$ codebooks, one for each f, each one consisting of the collection $\mathcal{C}_f$ and the common message index function $m(y^n)$. We use $\mathcal{K}$ to denote this set of random codebooks.

By this construction, the original random collection $\mathcal{C}$ in the codebook used by the encoder and decoder is equivalent in probability to using the first codebook associated with $\mathcal{C}_1$. It is also equivalent to using a random codebook in the set, which is a point we will utilize shortly. The purpose of defining multiple codebooks is to facilitate general proof tools associated with uniform random binning.

Here we summarize the proof given in [18]. In addition to the system induced random variables, we introduce a random variable F which is uniformly distributed on the set $\{1, \ldots, 2^{nR'}\}$ and independent of X^n. The variable F selects the codebook to be used—everything else about the encoding and decoding remains the same. We have noted that the behavior and performance of this system with multiple codebooks is equivalent to that of the actual encoding and decoding. Nevertheless, we will formalize this connection in (3.69). For now, we refer to this new distribution that includes many codebooks as the pseudo induced distribution $\tilde{\mathbf{P}}$. According to $\tilde{\mathbf{P}}$, there is a set of randomly generated codebooks, and the one for use is selected by F.

The pseudo induced distribution can be expressed in the following form:

$$\begin{aligned} & \tilde{\mathbf{P}}_{FX^nMY^n}(f, x^n, m, y^n) \\ = \quad & P_F(f) P_{X^n}(x^n) \mathbf{P}_{PPE}(m|x^n, f) \mathbf{P}_D(y^n|m, f). \end{aligned} \tag{3.54}$$

We reiterate that

$$\mathbf{P}_{X^nMY^n} \stackrel{d}{=} \tilde{\mathbf{P}}_{X^nMY^n|F=f}, \quad \forall f \in [1 : 2^{nR'}]. \tag{3.55}$$

We now introduce one more random variable that never actually materialized during the implementation. Let $\tilde{Y}^n$ be the reconstruction sequence intended by the encoder. The encoding can be considered as a two step process. First, the encoder selects a $\tilde{Y}^n$ sequence from $\mathcal{C}_f$ with probability proportional to that induced by passing x^n through a memoryless channel given by $\overline{P}_{Y|X}$. Next, the encoder looks up the message index $m(\tilde{Y}^n)$ and transmits it as M.

Accordingly, we will replace the encoder in the pseudo induced distribution with the two parts discussed:

$$\mathbf{P}_{PPE}(m|x^n, f) = \sum_{\tilde{y}^n} \mathbf{P}_{E1}(\tilde{y}^n|x^n, f) \mathbf{P}_{E2}(m|\tilde{y}^n). \tag{3.56}$$

To analyze the expected distortion performance of the pseudo induced distribution $\tilde{\mathbf{P}}$, we introduce two approximating distributions $\mathbf{Q}^{(1)}$ and $\mathbf{Q}^{(2)}$.

Let us first define the distribution $\mathbf{Q}^{(1)}$:

$$\begin{aligned} & \mathbf{Q}^{(1)}_{FX^n\tilde{Y}^nMY^n}(f, x^n, \tilde{y}^n, m, y^n) \\ \triangleq \quad & \overline{P}_{X^nY^n}(x^n, \tilde{y}^n) \mathbf{Q}_{F|\tilde{Y}^n}(f|\tilde{y}^n) \mathbf{P}_{E2}(m|\tilde{y}^n) \mathbf{P}_D(y^n|m, f) \end{aligned} \tag{3.57}$$

where $\mathbf{Q}_{F|\tilde{Y}^n}(f|\tilde{y}^n) = \mathbb{1}\{\tilde{y}^n \in \mathcal{C}_f\}$. In words, $\mathbf{Q}^{(1)}$ is constructed from an i.i.d. distribution according to $\overline{P}$ on $(X^n, \tilde{Y}^n)$, two random binnings F and M, as specified by the construction of the set of codebooks $\mathcal{K}$, and a decoding of Y^n from the random binnings.

Now we arrive at the reason for using the proportional-probability encoder. Part 1 of the encoder that selects the $\tilde{Y}^n$ sequences is precisely the conditional probability specified by $\mathbf{Q}^{(1)}$:

$$\mathbf{Q}^{(1)}_{\tilde{Y}^n|X^nF}(\tilde{y}^n|x^n,f)=\mathbf{P}_{E1}(\tilde{y}^n|x^n,f).$$

Therefore, the only difference between the pseudo induced distribution $\tilde{\mathbf{P}}$ and $\mathbf{Q}^{(1)}$ is the conditional distribution of F given X^n, which should be independent and uniform according to $\tilde{\mathbf{P}}$. This is where Lemma 3.1 plays a role.

Applying Lemma 3.1 by identifying F as the uniform binning of $\tilde{Y}^n$, since $R'<H(Y|X)$ under distribution $\overline{P}_{XY}$, we obtain

$$\mathbb{E}_{\mathcal{K}}\left[\left\|\mathbf{Q}^{(1)}_{X^nF}-\tilde{P}_{X^nF}\right\|_{TV}\right]\leq\epsilon_n^{(rb)}\to_n 0. \tag{3.58}$$

Using Property 2.1(d), we have

$$\mathbb{E}_{\mathcal{K}}\left[\left\|\tilde{\mathbf{P}}_{FX^nY^nM\hat{Y}^n}-\mathbf{Q}^{(1)}_{FX^nY^nM\hat{Y}^n}\right\|_{TV}\right]\leq\epsilon_n^{(rb)}. \tag{3.59}$$

The next approximating distribution we define is $\mathbf{Q}^{(2)}$:

$$\mathbf{Q}^{(2)}_{FX^n\tilde{Y}^nMY^n}(f,x^n,\tilde{y}^n,m,y^n)\triangleq\mathbf{Q}^{(1)}_{FX^n\tilde{Y}^nM}(f,x^n,\tilde{y}^n,m)\mathbb{1}\{y^n=\tilde{y}^n\}. \tag{3.60}$$

Recall from Remark 2, decoding $\tilde{Y}^n$ will succeed with high probability if the total rate of the binnings is above the entropy rate of the sequence that was binned. This is well known from the Slepian-Wolf coding result [20] [21]. Therefore, since the total binning rate $R+R'>H(Y)$ under distribution $\overline{P}_Y$, according to the definition of total variation, we obtain

$$\mathbb{E}_{\mathcal{K}}\left[\left\|\mathbf{Q}^{(1)}_{\tilde{Y}^nY^n}-\mathbf{Q}^{(2)}_{\tilde{Y}^nY^n}\right\|_{TV}\right]\leq\epsilon_n^{(sw)}\to_n 0, \tag{3.61}$$

where $\epsilon_n^{(sw)}$ is the decoding error.

Again by Property 2.1(d), we have

$$\mathbb{E}_{\mathcal{K}}\left[\left\|\mathbf{Q}^{(1)}_{FX^n\tilde{Y}^nMY^n}-\mathbf{Q}^{(2)}_{FX^n\tilde{Y}^nMY^n}\right\|_{TV}\right]\leq\epsilon_n^{(sw)}. \tag{3.62}$$

Combining (3.59) and (3.62) using the triangle inequality, we obtain

$$\mathbb{E}_{\mathcal{K}}\left[\left\|\tilde{\mathbf{P}}_{FX^n\tilde{Y}^nMY^n}-\mathbf{Q}^{(2)}_{FX^n\tilde{Y}^nMY^n}\right\|_{TV}\right]\leq\epsilon_n^{(rb)}+\epsilon_n^{(sw)}. \tag{3.63}$$

Note that the distortion under any realization of $\mathbf{Q}^{(2)}$, regardless of the codebook, is

$$\begin{aligned}\mathbb{E}_{Q^{(2)}}[d(X^n,Y^n)] &= \mathbb{E}_{Q^{(2)}}[d(X^n,Y^n)] &(3.64)\\ &= \mathbb{E}_{\overline{P}}[d(X,Y)]. &(3.65)\end{aligned}$$

Applying Property 2.1(b), we can obtain

$$\mathbb{E}_{\mathcal{K}}\left[\mathbb{E}_{\tilde{\mathbf{P}}}[d(X^n,Y^n)]\right]\leq\mathbb{E}_{\overline{P}}[d(X,Y)]+d_{max}(\epsilon_n^{(rb)}+\epsilon_n^{(sw)}). \tag{3.66}$$

Furthermore, by symmetry and the law of total expectation, we have

$$\begin{aligned}&\mathbb{E}_{\mathcal{K}}\left[\mathbb{E}_{\tilde{\mathbf{P}}}[d(X^n,Y^n)]\right]\\ =\;&\mathbb{E}_F\left[\mathbb{E}_{\mathcal{K}}\left[\mathbb{E}_{\tilde{\mathbf{P}}}[d(X^n,Y^n)]\mid F\right]\right] &(3.67)\\ =\;&\mathbb{E}_{\mathcal{K}}\left[\mathbb{E}_{\tilde{\mathbf{P}}}[d(X^n,Y^n)]\mid F=1\right] &(3.68)\\ =\;&\mathbb{E}_{\mathcal{K}}\left[\mathbb{E}_{\mathbf{P}}[d(X^n,Y^n)]\right], &(3.69)\end{aligned}$$

where the last equality comes from the observation in (3.55).

Finally, applying the random coding argument, there exists a code that gives

$$\mathbb{E}_P[d(X^n,Y^n)]\leq\mathbb{E}_{\overline{P}}[d(X,Y)]+d_{max}\left(\epsilon_n^{(rb)}+\epsilon_n^{(sw)}\right),$$

which is less than D for n large enough.

Comparing the Likelihood Encoder with Proportional-Probability Encoder

Let us now compare the achievability proofs using the likelihood encoder approach and the *proportional-probability encoder* (random binning based) approach for the point-to-point rate distortion function.

We first notice that the error term in the likelihood encoder approach only arises from the soft-covering lemma, while the error terms in the proportional-probability approach come from two places, random binning and MSLC decoding.

Next, we will provide a non-asymptotic comparison between the two approaches with respect to excess distortion.

Some asymptotic analysis was given in [19] on channel coding with random binning. We can extend this to give non-asymptotic bounds for source coding problems also. Using Theorems 1 and 2 from [19], we can obtain the following theorem.

Theorem 3.2. *The excess distortion* $\mathbb{P}_P[d(X^n, Y^n) > D]$ *using the proportional-probability encoder is upper bounded by*

$$\inf_{\overline{P}_{Y|X}} \left\{ \exp\left(-n\eta(\overline{P}_{Y|X})\right) + \sigma_n(\overline{P}_{Y|X}) \right\} \tag{3.70}$$

where

$$\sigma_n(\overline{P}_{Y|X}) = \inf_{R' \in (H(Y)-R, H(Y|X))} \{A_n + B_n\} \tag{3.71}$$

and

$$A_n = \inf_{\delta \in (0, H(Y|X)-R')} \left\{ \mathbb{P}_{\overline{P}} \left[-\log \overline{P}_{Y^n|X^n}(Y^n|X^n) \le n(R'+\delta) \right] + \frac{1}{\sqrt{2}} 2^{-\frac{n\delta}{2}} \right\} \tag{3.72}$$

$$B_n = \inf_{\tau > 0} \left\{ \mathbb{P}_{\overline{P}} \left[n(R+R') - h(Y^n) \le n\tau \right] + 3 \times 2^{-n\tau} \right\}. \tag{3.73}$$

We can further bound the quantities in A_n and B_n in Theorem 3.2 by the Chernoff inequality following the steps (3.37) through (3.40) and obtain the following exponential

forms:

$$\begin{aligned}
&\mathbb{P}_{\overline{P}}\left[-\log \overline{P}_{Y^n|X^n}(Y^n|X^n) \le n(R'+\delta)\right] \\
\le\ & \inf_{\beta_1>0}\left\{\exp\left(-n\log\left(\mathbb{E}_{\overline{P}}\left[2^{\beta_1\left(R'+\delta-\log\frac{1}{\overline{P}_{Y|X}(Y|X)}\right)}\right]\right)^{-1}\right)\right\}, \qquad (3.74)
\end{aligned}$$

$$\begin{aligned}
&\mathbb{P}_{\overline{P}}\left[n(R+R') - h(Y^n) \le n\tau\right] \\
\le\ & \inf_{\beta_2>0}\left\{\exp\left(-n\log\left(\mathbb{E}_{\overline{P}}\left[2^{\beta_2\left(\log\frac{1}{\overline{P}_Y(Y)}-R-R'+\tau\right)}\right]\right)^{-1}\right)\right\}. \qquad (3.75)
\end{aligned}$$

Numerical Example

Next, we would like to compare the bounds given by the likelihood encoder in Theorem 3.1 and given by the proportional-probability encoder in Theorem 3.2.

Here we give a numerical comparison between the likelihood encoder and the proportional-probability encoder for a Bernoulli $\frac{1}{2}$ source and Hamming distortion. For simplicity, we consider only symmetric test channels of the form $\overline{P}_{Y|X}(0|0) = \overline{P}_{Y|X}(1|1) = a_0$.

Assume $D < \frac{1}{2}$ and fix a_0. Observe that $\eta(a_0) \triangleq \eta(\overline{P}_{Y|X})$ is a term shared by both the likelihood encoder and the proportional-probability encoder methods and it takes the following form:

$$\eta(a_0) = -\log_2\left(a_0 2^{-\beta^* D} + (1-a_0)2^{\beta^*(1-D)}\right), \qquad (3.76)$$

where

$$\beta^* = \log_2 \frac{Da_0}{(1-D)(1-a_0)}. \qquad (3.77)$$

For a Bernoulli $\frac{1}{2}$ source, the quantities from the likelihood encoder satisfies

$$\check{I}_\alpha(a_0) \triangleq \check{I}_{\overline{P},\alpha} = \bar{I}_{\overline{P},\alpha} = 1 + \frac{1}{\alpha-1}\log_2\left(a_0^\alpha + (1-a_0)^\alpha\right) \qquad (3.78)$$

$$\gamma(a_0) = \max_{\alpha \geq 1, \alpha' \leq 2} \frac{\alpha - 1}{2\alpha - \alpha'} \left(R - 1 + \frac{\alpha' - 2}{\alpha - 1} \log_2(a_0^\alpha + (1-a_0)^\alpha) - \log_2(a_0^{\alpha'} + (1-a_0)^{\alpha'}) \right) \quad (3.79)$$

Observe that the first term in B_n given in (3.73) is deterministic; therefore, we can choose

$$\tau^* = R + R' - 1. \quad (3.80)$$

The optimum β_1 in (3.74) is given by

$$\beta_1^* = \left[\log_{\frac{a_0}{1-a_0}} \left(-\frac{R' + \delta + \log_2(1-a_0)}{R' + \delta + \log_2(a_0)} \right) - 1 \right]^+. \quad (3.81)$$

Consequently, the exponent of the first term of A_n is given by

$$A_{1n}(R', \delta, a_0) \triangleq -\log_2 \left(a_0 2^{\beta_1^*(R' + \delta + \log_2(a_0))} + (1-a_0) 2^{\beta_1^*(R' + \delta + \log_2(1-a_0))} \right). \quad (3.82)$$

Let us define

$$\lambda(a_0) \triangleq \max_{R', \delta} \left(R + R' - 1, \frac{\delta}{2}, A_1(R', \delta, a_0) \right),$$

where the domains of R' and δ are omitted.

To summarize, for the likelihood encoder, we still need to optimize over α and α', and for the proportional-probability encoder, we need to optimize over R' and δ. Finally, for both, we optimize over a_0. The derived error exponent bounds for the likelihood encoder and the proportional-probability encoder are given by the following, respectively:

$$\text{Error exponent for the LE} = \max_{a_0} \min(\eta(a_0), \gamma(a_0)) \quad (3.83)$$

$$\text{Error exponent for the PPE} = \max_{a_0} \min(\eta(a_0), \lambda(a_0)). \quad (3.84)$$

Comparisons of the error exponents given in (3.83) and (3.84) are shown in Fig. 3.3, plotted as functions of D and R. The numerical comparisons show that the likelihood encoder has a better error exponent than the proportional-probability encoder, at least according to these derived upper bounds on the error.

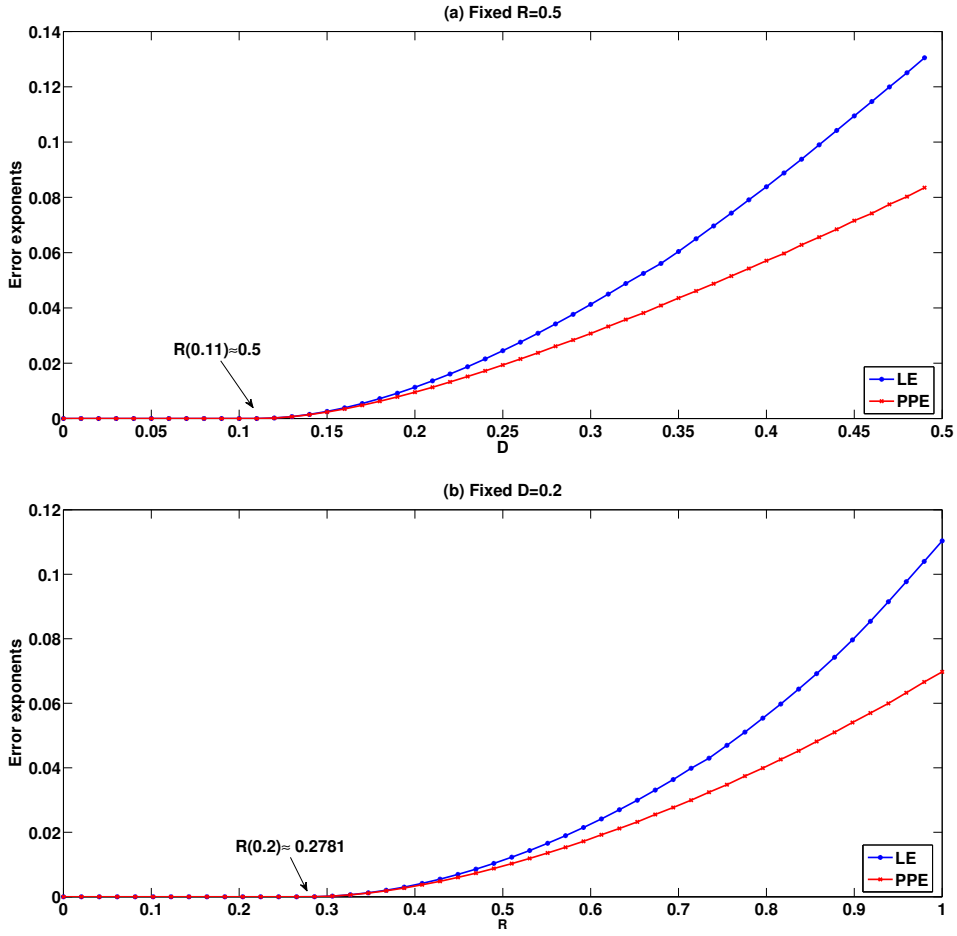

Figure 3.3: Error exponents by the likelihood encoder and the proportional-probability encoder (random binning based analysis) for a Bernoulli $\frac{1}{2}$ source and Hamming distortion, in (a) as a function of D for fixed $R = \frac{1}{2}$, and in (b) as a function of R for fixed $D = 0.2$. Notice that for this particular example, the optimal excess error actually decays super-exponentially, but this is not achieved with either of the proof techniques discussed.

3.5 A Non-Asymptotic Analysis Using Jensen's Inequality

The excess distortion can be examined using the same type of analysis as the "one shot achievability" for channel coding [16]. The key step again uses Jensen's inequality and it gives us an upper bound on the excess distortion.

Here, instead of looking at an i.i.d. source sequence, we perform the analysis on a general source with distribution given as P_X. Fix $\overline{P}_{Y|X}$ and denote $\overline{P}_{XY} = P_X \overline{P}_{Y|X}$.

Codebook generation: For each $m \in [1 : |\mathcal{M}|]$, independently generate $c(m)$ according to $\overline{P}_Y$. We denote the random codebook as $\mathcal{C}$.

Encoder: The encoder is the likelihood encoder

$$P_{M|X}(m|x) = \frac{\overline{P}_{X|Y}(x|c(m))}{\sum_{m'} \overline{P}_{X|Y}(x|c(m'))} \tag{3.85}$$

$$= \frac{2^{\imath(x;c(m))}}{\sum_{m'} 2^{\imath(x;c(m'))}} \tag{3.86}$$

We use $f(\cdot)$ to denote the stochastic encoding function.

Decoder: The decoder is a codeword lookup decoder

$$P_{Y|M}(y|m) = \mathbb{1}\{y = c(m)\} \tag{3.87}$$

Analysis: The system induced distribution can be written as

$$P_{XMY}(x, m, y) = P_X(x) P_{M|X}(m|x) P_{Y|M}(y|m) \tag{3.88}$$

The probability of correct decoding can be bounded as follows.

$$
\begin{aligned}
& \mathbb{E}_{\mathcal{C}}\left[\mathbb{P}\left[d(X, c(f(X))) \leq D\right]\right] \\
= \; & \mathbb{E}_{\mathcal{C}}\left[\mathbb{P}_P\left[d(X,Y) \leq D\right]\right] && (3.89)\\
= \; & \mathbb{E}_{\mathcal{C}}\left[\sum_{x,y} P_{XY}(x,y)\mathbb{1}\{d(x,y) \leq D\}\right] && (3.90)\\
= \; & \mathbb{E}_{\mathcal{C}}\left[\sum_{x,y} P_X(x)\frac{\sum_m 2^{\imath(x;c(m))}\mathbb{1}\{y = c(m)\}}{\sum_{m'} 2^{\imath(x;c(m'))}}\mathbb{1}\{d(x,y) \leq D\}\right] && (3.91)\\
= \; & \mathbb{E}_{\mathcal{C}}\left[\sum_{x} P_X(x)\frac{\sum_m 2^{\imath(x;c(m))}\sum_y \mathbb{1}\{y = c(m)\}\mathbb{1}\{d(x,y) \leq D\}}{\sum_{m'} 2^{\imath(x;c(m'))}}\right] && (3.92)\\
= \; & \sum_x P_X(x)\mathbb{E}_{\mathcal{C}}\left[\frac{\sum_m 2^{\imath(x;c(m))}\mathbb{1}\{d(x,c(m)) \leq D\}}{\sum_{m'} 2^{\imath(x;c(m'))}}\right] && (3.93)\\
= \; & \sum_x P_X(x)\mathbb{E}_{\mathcal{C}}\left[\frac{M2^{\imath(x;c(1))}\mathbb{1}\{d(x,c(1)) \leq D\}}{\sum_{m'} 2^{\imath(x;c(m'))}}\right] && (3.94)\\
= \; & \sum_x P_X(x)\mathbb{E}_{c(1)}\mathbb{E}_{\mathcal{C}|c(1)}\left[\frac{M2^{\imath(x;c(1))}\mathbb{1}\{d(x,c(1)) \leq D\}}{\sum_{m'} 2^{\imath(x;c(m'))}}\right] && (3.95)\\
\geq \; & \sum_x P_X(x)\mathbb{E}_{c(1)}\left[\frac{M2^{\imath(x;c(1))}\mathbb{1}\{d(x,c(1)) \leq D\}}{\mathbb{E}_{\mathcal{C}|c(1)}\sum_{m'} 2^{\imath(x;c(m'))}}\right] && (3.96)\\
= \; & \sum_x P_X(x)\mathbb{E}_{c(1)}\left[\frac{M2^{\imath(x;c(1))}\mathbb{1}\{d(x,c(1)) \leq D\}}{2^{\imath(x;c(1))} + (M-1)}\right] && (3.97)\\
\geq \; & \sum_x P_X(x)\mathbb{E}_{c(1)}\left[\frac{M2^{\imath(x;c(1))}\mathbb{1}\{d(x,c(1)) \leq D\}}{2^{\imath(x;c(1))} + M}\right] && (3.98)\\
= \; & \sum_x P_X(x)\mathbb{E}_{c(1)}\left[\frac{2^{\imath(x;c(1))}}{1 + M^{-1}2^{\imath(x;c(1))}}\mathbb{1}\{d(x,c(1)) \leq D\}\right] && (3.99)\\
= \; & \sum_x P_X(x)\sum_y \overline{P}_Y(y)\frac{\frac{\overline{P}_{XY}(x,y)}{P_X(x)\overline{P}_Y(y)}}{1 + M^{-1}2^{\imath(x;y)}}\mathbb{1}\{d(x,y) \leq D\} && (3.100)\\
= \; & \sum_{x,y} \overline{P}_{XY}(x,y)\frac{1}{1 + M^{-1}2^{\imath(x;y)}}\mathbb{1}\{d(x,y) \leq D\} && (3.101)\\
= \; & \mathbb{E}_{\overline{P}}\left[\frac{1}{1 + M^{-1}2^{\imath(X;Y)}}\mathbb{1}\{d(X,Y) \leq D\}\right] && (3.102)
\end{aligned}
$$

where (3.96) uses Jensen's inequality on convex function $f(x) = \frac{1}{x}$ and (3.97) comes from the fact that for $m' \neq 1$

$$\begin{aligned}
\mathbb{E}_{\mathcal{C}|c(1)} 2^{\imath(x;c(m'))} &= \sum_y \overline{P}_Y(y) 2^{\imath(x;y)} && (3.103)\\
&= \sum_y \overline{P}_Y(y) \frac{\overline{P}_{Y|X}(y|x)}{\overline{P}_Y(y)} && (3.104)\\
&= \sum_y \overline{P}_{Y|X}(y|x) = 1 && (3.105)
\end{aligned}$$

Loosening the bound using the same technique as [16], for $\gamma > 0$, we have

$$\begin{aligned}
& \mathbb{E}_{\overline{P}} \left[\frac{1}{1 + M^{-1} 2^{\imath(X;Y)}} \mathbb{1}\{d(X,Y) \leq D\} \right] \\
\geq\ & \mathbb{E}_{\overline{P}} \left[\frac{1}{1 + M^{-1} 2^{\imath(X;Y)}} \mathbb{1}\left\{d(X,Y) \leq D \text{ and } \log|\mathcal{M}| - \imath(X;Y) \geq \gamma\right\} \right] && (3.106)\\
\geq\ & \frac{1}{2^{-\gamma} + 1} \mathbb{P}_{\overline{P}}\left[d(X,Y) \leq D \text{ and } \log|\mathcal{M}| - \imath(X;Y) \geq \gamma\right] && (3.107)
\end{aligned}$$

Therefore, the probability of excess distortion can be bounded as

$$\begin{aligned}
\mathbb{P}[\varepsilon] &= 1 - \mathbb{E}_{\mathcal{C}}\left[\mathbb{P}_{\overline{P}}\left[d(X, c(f(X))) \leq D\right]\right] && (3.108)\\
&= \mathbb{P}_{\overline{P}}[d(X;Y) > D \text{ or } \log|\mathcal{M}| - \imath(X;Y) < \gamma] \\
&\quad + (1 - \frac{1}{2^{-\gamma} + 1}) \mathbb{P}_{\overline{P}}[d(X;Y) \leq D \text{ and } \log|\mathcal{M}| - \imath(X;Y) \geq \gamma] && (3.109)\\
&\leq \mathbb{P}_{\overline{P}}[d(X;Y) > D \text{ or } \log|\mathcal{M}| - \imath(X;Y) < \gamma] + (1 - \frac{1}{2^{-\gamma} + 1}) && (3.110)\\
&\leq \mathbb{P}_{\overline{P}}[d(X;Y) > D] + \mathbb{P}_{\overline{P}}[\imath(X;Y) > \log|\mathcal{M}| - \gamma] + 2^{-\gamma} && (3.111)
\end{aligned}$$

3.6 Summary

In this chapter, we have demonstrated how the likelihood encoder can be used to obtain achievability result for the basic point-to-point lossy source compression problem. The analysis of the likelihood encoder relies on the soft-covering lemma. Although the proof method is unusual, we hope to have demonstrated that this method of proof is simple, both conceptually and mechanically. This proof method applies directly to continuous sources as

well with no need for additional arguments, because the soft-covering lemma is not restricted to discrete sources.

A parallel comparison of the non-asymptotic performance of the likelihood encoder and the "proportional-probability encoder" has been provided along with a numerical example. In this example, the likelihood encoder achieves better error exponents than does the proportional probability encoder.

Chapter 4

Multiuser Lossy Compression

4.1 Introduction

In this chapter, we propose using a likelihood encoder to achieve classical source coding results such as the Wyner-Ziv rate-distortion function and Berger-Tung inner bound [22] [23]. In the standard proofs using the joint asymptotic equipartition principle (J-AEP), the distortion analysis involves bounding several "error" events which may come from either encoding or decoding. In the cases where there are multiple information sources, such as side information at the decoder, intricacies arise, such as the need for a Markov lemma [9] and [10]. These subtleties also lead to error-prone proofs involving the analysis of error caused by random binning, which have been pointed out in several existing works [8] [24].

Since the analysis using the soft-covering lemma is not limited to discrete alphabets, no extra work, i.e. quantization of the source, is needed to extend the standard proof for discrete sources to continuous sources as in [10]. This advantage becomes more desirable for the multi-terminal case, since generalization of the type-covering lemma and the Markov lemma to continuous alphabets is non-trivial. Strong versions of the Markov lemma on finite alphabets that can prove the Berger-Tung inner bound can be found in [10] and [25]. However, generalization to the continuous alphabets is still an ongoing research topic. Some work, such as [26], has been dedicated to making this transition, yet is not strong enough to be applied to the Berger-Tung case.

4.2 Approximation Lemma

Lemma 4.1. *For a distribution P_{UVX} and $0 < \varepsilon < 1$, if $\mathbb{P}[U \neq V] \leq \varepsilon$, then*

$$\|P_{UX} - P_{VX}\|_{TV} \leq \varepsilon.$$

Proof. By definition,

$$\|P_{UX} - P_{VX}\|_{TV} = \sup_{\mathcal{A} \in \mathcal{F}} \{\mathbb{P}[(U, X) \in \mathcal{A}] - \mathbb{P}[(V, X) \in \mathcal{A}]\}.$$

Since for every $\mathcal{A} \in \mathcal{F}$

$$\begin{aligned}
& \mathbb{P}[(U, X) \in \mathcal{A}] - \mathbb{P}[(V, X) \in \mathcal{A}] \\
\leq\ & \mathbb{P}[(U, X) \in \mathcal{A}] - \mathbb{P}[(V, X) \in \mathcal{A}, (U, X) \in \mathcal{A}] && (4.1) \\
=\ & \mathbb{P}[(U, X) \in \mathcal{A}, (V, X) \neq \mathcal{A}] && (4.2) \\
\leq\ & \mathbb{P}[U \neq V] && (4.3) \\
\leq\ & \epsilon, && (4.4)
\end{aligned}$$

we have

$$\sup_{\mathcal{A} \in \mathcal{F}} \{\mathbb{P}[(U, X) \in \mathcal{A}] - \mathbb{P}[(V, X) \in \mathcal{A}]\} \leq \epsilon.$$

□

4.3 The Wyner-Ziv Setting

In this section, we will use the mechanism that was established in Section 3.3 and build upon it to solve a more complicated problem. The Wyner-Ziv problem, that is, the rate-distortion function with side information at the decoder, was solved in [27].

4.3.1 Problem Formulation

The source and side information pair (X^n, Z^n) is distributed i.i.d. according to $(X_t, Z_t) \sim P_{XZ}$. The system has the following constraints:

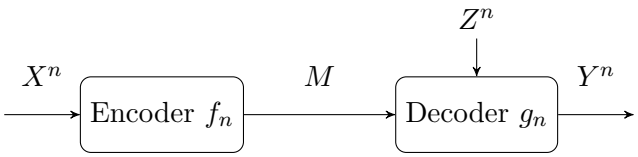

Figure 4.1: Rate-distortion theory for source coding with side information at the decoder—the Wyner-Ziv problem

- Encoder $f_n : \mathcal{X}^n \mapsto \mathcal{M}$ (possibly stochastic);
- Decoder $g_n : \mathcal{M} \times \mathcal{Z}^n \mapsto \mathcal{Y}^n$ (possibly stochastic);
- Compression rate: R, i.e. $|\mathcal{M}| = 2^{nR}$.

The system performance is measured according to the time-averaged distortion (as defined in the notation section):

- Time averaged distortion: $d(X^n, Y^n) = \frac{1}{n}\sum_{t=1}^{n} d(X_t, Y_t)$.

Definition 4.1. *A rate distortion pair (R, D) is achievable if there exists a sequence of rate R encoders and decoders (f_n, g_n), such that*

$$\limsup_{n\to\infty} \mathbb{E}\left[d(X^n, Y^n)\right] \leq D.$$

Definition 4.2. *The rate distortion function is $R(D) \triangleq \inf_{\{(R,D) \text{ is achievable}\}} R$.*

The above mathematical formulation is illustrated in Fig. 4.1.

As mentioned previously, the solution to this source coding problem is given in [27]. The rate-distortion function with side information at the decoder is

$$R(D) \quad = \quad \min_{P_{V|XZ} \in \mathcal{M}(D)} I(X; V|Z), \tag{4.5}$$

where the mutual information is with respect to

$$P_{XZV} = P_{XZ} P_{V|XZ}, \tag{4.6}$$

and

$$\mathcal{M}(D) = \Big\{ P_{V|XZ} : \quad V - X - Z, \\ |\mathcal{V}| \leq |\mathcal{X}| + 1, \\ \text{and there exists a function } \phi \text{ s.t.} \\ \mathbb{E}\left[d(X,Y)\right] \leq D, Y \triangleq \phi(V,Z) \Big\}. \tag{4.7}$$

The proof for the converse part can be found in the original paper [27] and other textbooks such as [10]. This is not presented in this thesis.

4.3.2 Proof of Achievability

We will introduce a virtual message which is produced by the encoder but not physically transmitted to the receiver so that this virtual message together with the actual message gives a high enough rate for applying the soft-covering lemma. Then we show that this virtual message can be reconstructed with vanishing error probability at the decoder by using the side information. This is analogous to the technique of random binning, where the index of the codeword within the bin is equivalent to the virtual message in our method.

Our proof technique again involves showing that the behavior of the system is approximated by a well-behaved distribution. The soft-covering lemma and channel decoding error bounds are used to analyze how well the approximating distribution matches the system.

Here again we reserve P for the system induced distribution and replace the single-letter distributions with $\overline{P}$ to denote any marginal or conditional distributions derived from the joint single-letter distribution $\overline{P}_{XZV}$. Since $\overline{P}_{XZ} = P_{XZ}$, these may be used interchangeably. We use $\overline{P}_{X^nZ^nV^n}$ to denote the product of an i.i.d. distribution, i.e.

$$\overline{P}_{X^nZ^nV^n} = \prod_{t=1}^{n} \overline{P}_{XZV}. \tag{4.8}$$

Let $R > R(D)$, where $R(D)$ is from the right hand side of (4.5). We prove that R is achievable for distortion D. Let M' be a virtual message with rate R' that is not physically transmitted. By the rate-distortion formula in (4.5), we can fix R' and $\overline{P}_{V|XZ} \in \mathcal{M}(D)$

($\overline{P}_{V|XZ} = \overline{P}_{V|X}$) such that $R + R' > I(X;V)$ and $R' < I(V;Z)$, and there exists a function $\phi(\cdot,\cdot)$ yielding $Y = \phi(V,Z)$ and $\mathbb{E}\left[d(X,Y)\right] \leq D$. We will use the likelihood encoder derived from $\overline{P}_{XV}$ and a random codebook $\{v^n(m,m')\}$ generated according to $\overline{P}_V$ to prove the result. The decoder will first use the transmitted message M and the side information Z^n to decode M' as $\hat{M}'$ and reproduce $v^n(M,\hat{M}')$. Then the reconstruction Y^n is produced as a symbol-by-symbol application of $\phi(\cdot,\cdot)$ to Z^n and V^n.

The distribution induced by the encoder and decoder is

$$\begin{aligned}
& \mathbf{P}_{X^nZ^nMM'\hat{M}'Y^n}(x^n,z^n,m,m',\hat{m}',y^n) \\
= \;& P_{X^nZ^n}(x^n,z^n)\mathbf{P}_{MM'|X^n}(m,m'|x^n)\mathbf{P}_{\hat{M}'|MZ^n}(\hat{m}'|m,z^n)\mathbf{P}_{Y^n|M\hat{M}'Z^n}(y^n|m,\hat{m}',z^n) && (4.9)\\
\triangleq \;& P_{X^nZ^n}(x^n,z^n)\mathbf{P}_{LE}(m,m'|x^n)\mathbf{P}_D(\hat{m}'|m,z^n)\mathbf{P}_\Phi(y^n|m,\hat{m}',z^n), && (4.10)
\end{aligned}$$

where $\mathbf{P}_{LE}(m,m'|x^n)$ is the likelihood encoder; $\mathbf{P}_D(\hat{m}'|m,z^n)$ is the first part of the decoder that decodes m' as $\hat{m}'$; and $\mathbf{P}_\Phi(y^n|m,\hat{m}',z^n)$ is the second part of the decoder that reconstructs the source sequence.

We now concisely restate the behavior of the encoder and decoder, as these components of the induced distribution.

Codebook generation: We independently generate $2^{n(R+R')}$ sequences in $\mathcal{V}^n$ according to $\prod_{t=1}^n \overline{P}_V(v_t)$ and index by $(m,m') \in [1:2^{nR}] \times [1:2^{nR'}]$. We use $\mathcal{C}^{(n)}$ to denote the random codebook.

Encoder: The encoder $\mathbf{P}_{LE}(m,m'|x^n)$ is the likelihood encoder that chooses M and M' stochastically with probability proportional to the likelihood function given by

$$\mathcal{L}(m,m'|x^n) = \overline{P}_{X^n|V^n}(x^n|V^n(m,m')). \tag{4.11}$$

Decoder: The decoder has two steps. Let $\mathbf{P}_D(\hat{m}'|m,z^n)$ be a good channel decoder (e.g. the maximum likelihood decoder) with respect to the sub-codebook $\mathcal{C}^{(n)}(m) = \{v^n(m,a)\}_a$ and the memoryless channel $\overline{P}_{Z|V}$. For the second part of the decoder, let $\phi(\cdot,\cdot)$ be the function corresponding to the choice of $\overline{P}_{V|XZ}$ in (4.7); that is, $Y = \phi(V,Z)$ and $\mathbb{E}_{\overline{P}}\left[d(X,Y)\right] \leq D$. Define $\phi^n(v^n,z^n)$ as the concatenation $\{\phi(v_t,z_t)\}_{t=1}^n$ and set the de-

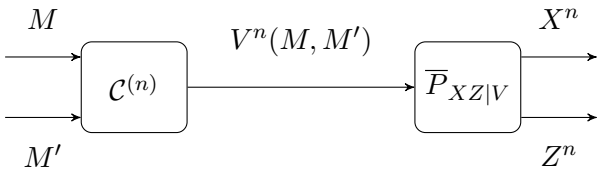

Figure 4.2: Idealized distribution with test channel $\overline{P}_{XZ|V}$

coder $\mathbf{P}_\Phi$ to be the deterministic function

$$\mathbf{P}_\Phi(y^n|m, \hat{m}', z^n) \triangleq \mathbb{1}\{y^n = \phi^n(V^n(m, \hat{m}'), z^n)\}. \tag{4.12}$$

Analysis: We will consider three distributions for the analysis, the induced distribution $\mathbf{P}$ and two approximating distributions $\mathbf{Q}^{(1)}$ and $\mathbf{Q}^{(2)}$. The idea is to show that 1) the system has nice behavior for distortion under $\mathbf{Q}^{(2)}$; and 2) $\mathbf{P}$ and $\mathbf{Q}^{(2)}$ are close in total variation (on average over the random codebook) through $\mathbf{Q}^{(1)}$.

The first approximating distribution, $\mathbf{Q}^{(1)}$, changes the distribution induced by the likelihood encoder to a distribution based on a reverse memoryless channel, as in the proof of point-to-point rate-distortion theory, and shown below in Fig. 4.2. This is shown to be a good approximation using the soft-covering lemma. The second approximating distribution, $\mathbf{Q}^{(2)}$, pretends that M', the index which is not transmitted, is used by the decoder to form the reconstruction. This is a good approximation because the decoder can accurately estimate M'.

Both approximating distributions $\mathbf{Q}^{(1)}$ and $\mathbf{Q}^{(2)}$ are built upon the idealized distribution over the information sources and messages, according to the test channel, as shown in Fig. 4.2. Note that this idealized distribution $\mathbf{Q}$ is no different from the one we considered for the point-to-point case, except for the message indices. The joint distribution under $\mathbf{Q}$ in

Fig. 4.2 can be written as

$$\begin{aligned}
& \mathbf{Q}_{X^nZ^nV^nMM'}(x^n, z^n, v^n, m, m') \\
= \; & Q_{MM'}(m, m')\mathbf{Q}_{V^n|MM'}(v^n|m, m')\mathbf{Q}_{X^nZ^n|MM'}(x^n, z^n|m, m') && (4.13) \\
= \; & \frac{1}{2^{n(R+R')}}\mathbb{1}\{v^n = V^n(m, m')\}\prod_{t=1}^{n}\overline{P}_{XZ|V}(x_t, z_t|V_t(m, m')) && (4.14) \\
= \; & \frac{1}{2^{n(R+R')}}\mathbb{1}\{v^n = V^n(m, m')\}\prod_{t=1}^{n}\overline{P}_{X|V}(x_t|v_t)\overline{P}_{Z|X}(z_t|x_t), && (4.15)
\end{aligned}$$

where (4.15) follows from the Markov chain relation under $\overline{P}$, $V - X - Z$. Note that by using the likelihood encoder, the idealized distribution $\mathbf{Q}$ satisfies

$$\mathbf{Q}_{MM'|X^nZ^n}(m, m'|x^n, z^n) = \mathbf{P}_{LE}(m, m'|x^n). \tag{4.16}$$

Furthermore, using the same technique as (3.13) and (3.18) given in the previous section, it can be verified that

$$\mathbb{E}_{\mathcal{C}^{(n)}}\left[\mathbf{Q}_{X^nZ^nV^n}(x^n, z^n, v^n)\right] = \overline{P}_{X^nZ^nV^n}(x^n, z^n, v^n). \tag{4.17}$$

Consequently,

$$\mathbb{E}_{\mathcal{C}^{(n)}}\left[\mathbb{E}_{\mathbf{Q}}\left[d\left(X^n, \phi^n(V^n, Z^n)\right)\right]\right] = \mathbb{E}_{\overline{P}}\left[d\left(X^n, \phi^n(V^n, Z^n)\right)\right]. \tag{4.18}$$

Define the two distributions $\mathbf{Q}^{(1)}$ and $\mathbf{Q}^{(2)}$ based on $\mathbf{Q}$ as follows:

$$\begin{aligned}
& \mathbf{Q}^{(1)}_{X^nZ^nMM'\hat{M}'Y^n}(x^n, z^n, m, m', \hat{m}', y^n) \\
\triangleq \; & \mathbf{Q}_{X^nZ^nMM'}(x^n, z^n, m, m')\mathbf{P}_D(\hat{m}'|m, z^n)\mathbf{P}_\Phi(y^n|m, \hat{m}', z^n) && (4.19) \\
& \mathbf{Q}^{(2)}_{X^nZ^nMM'\hat{M}'Y^n}(x^n, z^n, m, m', \hat{m}', y^n) \\
\triangleq \; & \mathbf{Q}_{X^nZ^nMM'}(x^n, z^n, m, m')\mathbf{P}_D(\hat{m}'|m, z^n)\mathbf{P}_\Phi(y^n|m, m', z^n). && (4.20)
\end{aligned}$$

Notice that $\mathbf{Q}^{(2)}$ differs from $\mathbf{Q}^{(1)}$ by allowing the decoder to use m' rather than $\hat{m}'$ when forming its reconstruction through ϕ^n.

Therefore, on account of (4.17),

$$\mathbb{E}_{\mathcal{C}^{(n)}}\left[\mathbf{Q}^{(2)}_{X^nZ^nY^n}(x^n,z^n,y^n)\right]=\overline{P}_{X^nZ^nY^n}(x^n,z^n,y^n). \tag{4.21}$$

Now applying the basic soft-covering lemma 2.1, since $R+R'>I(Z,X;V)=I(X;V)$, we have

$$\mathbb{E}_{\mathcal{C}^{(n)}}\left[\|\overline{P}_{X^nZ^n}-\mathbf{Q}_{X^nZ^n}\|_{TV}\right]\leq\epsilon_n\to_n 0. \tag{4.22}$$

And with (4.10), (4.16), (4.19) and Property 2.1(d), we obtain

$$\begin{aligned}
&\mathbb{E}_{\mathcal{C}^{(n)}}\left[\|\mathbf{P}_{X^nZ^nMM'\hat{M}'Y^n}-\mathbf{Q}^{(1)}_{X^nZ^nMM'\hat{M}'Y^n}\|_{TV}\right]\\
=\;&\mathbb{E}_{\mathcal{C}^{(n)}}\left[\|\overline{P}_{X^nZ^n}-\mathbf{Q}_{X^nZ^n}\|_{TV}\right] &(4.23)\\
\leq\;&\epsilon_n. &(4.24)
\end{aligned}$$

Since by definition $\mathbf{Q}^{(1)}_{X^nZ^nMM'\hat{M}'}=\mathbf{Q}^{(2)}_{X^nZ^nMM'\hat{M}'}$,

$$\mathbb{P}_{\mathbf{Q}^{(1)}}[\hat{M}'\neq M']=\mathbb{P}_{\mathbf{Q}^{(2)}}[\hat{M}'\neq M']. \tag{4.25}$$

Also, since $R'<I(V;Z)$, the codebook is randomly generated, and M' is uniformly distributed under Q, it is well known that the maximum likelihood decoder $\mathbf{P}_D$ (as well as a variety of other decoders) will drive the error probability to zero as n goes to infinity. This can be seen from Fig. 4.2, by identifying, for fixed M, that M' is the message to be transmitted over the memoryless channel $\overline{P}_{Z|V}$. Specifically,

$$\mathbb{E}_{\mathcal{C}^{(n)}}\left[\mathbb{P}_{\mathbf{Q}^{(1)}}[M'\neq\hat{M}']\right]\leq\delta_n\to_n 0. \tag{4.26}$$

Applying Lemma 4.1, we obtain

$$\mathbb{E}_{\mathcal{C}^{(n)}}\left[\|\mathbf{Q}^{(1)}_{X^nZ^nM\hat{M}'}-\mathbf{Q}^{(2)}_{X^nZ^nMM'}\|_{TV}\right]\leq\mathbb{E}_{\mathcal{C}^{(n)}}\left[\mathbb{P}_{\mathbf{Q}^{(1)}}[\hat{M}'\neq M']\right]\leq\delta_n. \tag{4.27}$$

Thus by Property 2.1(d) and definitions (4.19) and (4.20),

$$\mathbb{E}_{\mathcal{C}^{(n)}}\left[\|\mathbf{Q}^{(1)}_{X^nZ^nM\hat{M}'Y^n} - \mathbf{Q}^{(2)}_{X^nZ^nMM'Y^n}\|_{TV}\right] \leq \delta_n. \tag{4.28}$$

Combining (4.24) and (4.28) and using Property 2.1(c) and 2.1(e), we have

$$\mathbb{E}_{\mathcal{C}^{(n)}}\left[\|\mathbf{P}_{X^nY^n} - \mathbf{Q}^{(2)}_{X^nY^n}\|_{TV}\right] \leq \epsilon_n + \delta_n \tag{4.29}$$

where ϵ_n and δ_n are the error terms introduced from the soft-covering lemma and channel coding, respectively.

Repeating the same steps as (3.25) through (3.27) on $\mathbf{P}$, $\mathbf{Q}^{(2)}$, and $\overline{P}$, we obtain

$$\limsup_{n\to\infty} \mathbb{E}_{\mathcal{C}^{(n)}}\left[\mathbb{E}_{\mathbf{P}}[d(X^n,Y^n)]\right] \leq \limsup_{n\to\infty}\left\{\mathbb{E}_{\overline{P}}\left[d(X,Y)\right] + d_{max}(\epsilon_n+\delta_n)\right\} \leq D. \tag{4.30}$$

Therefore, there exists a codebook satisfying the requirement. ■

4.4 The Berger-Tung Inner Bound

In this section, we will demonstrate the use of the likelihood encoder via an alternative proof for achieving the Berger-Tung inner bound for the problem of multi-terminal source coding. Notice that no Markov lemma is needed in this proof. Similar to the single-user case, the key is to identify an auxiliary distribution that has nice properties and show that the system-induced distribution and the auxiliary distribution we choose are close in total variation.

4.4.1 Problem Formulation

We now consider a pair of correlated sources $({X_1}^n, {X_2}^n)$, distributed i.i.d. according to $(X_{1t}, X_{2t}) \sim P_{X_1X_2}$, independent encoders, and a joint decoder, satisfying the following constraints:

- Encoder 1 $f_{1n} : {\mathcal{X}_1}^n \mapsto \mathcal{M}_1$ (possibly stochastic);
- Encoder 2 $f_{2n} : {\mathcal{X}_2}^n \mapsto \mathcal{M}_2$ (possibly stochastic);

- Decoder $g_n : \mathcal{M}_1 \times \mathcal{M}_2 \mapsto {\mathcal{Y}_1}^n \times {\mathcal{Y}_2}^n$ (possibly stochastic);
- Compression rates: R_1, R_2, i.e. $|\mathcal{M}_1| = 2^{nR_1}$, $|\mathcal{M}_2| = 2^{nR_2}$.

The system performance is measured according to the time-averaged distortion:

- $d_1({X_1}^n, {Y_1}^n) = \frac{1}{n}\sum_{t=1}^n d_1(X_{1t}, Y_{1t})$,
- $d_2({X_2}^n, {Y_2}^n) = \frac{1}{n}\sum_{t=1}^n d_2(X_{2t}, Y_{2t})$,

  where $d_1(\cdot,\cdot)$ and $d_2(\cdot,\cdot)$ can be different distortion measures.

Definition 4.3. *(R_1, R_2) is achievable under distortion level (D_1, D_2) if there exists a sequence of rate (R_1, R_2) encoders and decoder (f_{1n}, f_{2n}, g_n) such that*

$$\limsup_{n\to\infty} \mathbb{E}[d_1({X_1}^n, {Y_1}^n)] \leq D_1, \tag{4.31}$$

$$\limsup_{n\to\infty} \mathbb{E}[d_2({X_2}^n, {Y_2}^n)] \leq D_2. \tag{4.32}$$

The achievable rate region is not yet known in general. But an inner bound, reproduced below, was given in [28] and [29] and is known as the Berger-Tung inner bound. The rates (R_1, R_2) are achievable if

$$R_1 > I(X_1; U_1|U_2), \tag{4.33}$$

$$R_2 > I(X_2; U_2|U_1), \tag{4.34}$$

$$R_1 + R_2 > I(X_1, X_2; U_1, U_2) \tag{4.35}$$

for some

$$P_{U_1X_1X_2U_2} = P_{X_1X_2} P_{U_1|X_1} P_{U_2|X_2}, \tag{4.36}$$

and functions $\phi_k(\cdot,\cdot)$ such that $\mathbb{E}[d_k(X_k, Y_k)] \leq D_k$, where $Y_k \triangleq \phi_k(U_1, U_2), k = 1, 2$. [1]

[1] This region, after optimizing over auxiliary variables, is in fact not convex, so it can be improved to the convex hull through time-sharing.

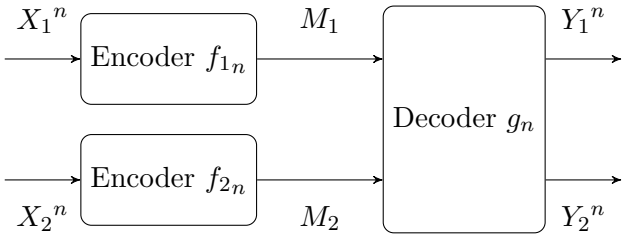

Figure 4.3: Berger-Tung problem setup

4.4.2 Proof of Achievability

For simplicity, we will focus on the corner points, $C_1 \triangleq (I(X_1;U_1), I(X_2;U_2|U_1))$ and $C_2 \triangleq (I(X_1;U_1|U_2), I(X_2;U_2))$, of the region given in (4.33) through (4.35) and use convexity to claim the complete region. Below we demonstrate how to achieve C_1. The point C_2 follows by symmetry.

We keep the same convention for using P to denote system induced distribution and using $\overline{P}$ to denote any marginal or conditional distributions derived from the joint single-letter distribution $\overline{P}_{U_1X_1X_2U_2}$. Since $\overline{P}_{X_1X_2} = P_{X_1X_2}$, these may be used interchangeably. We use $\overline{P}_{U_1{}^nX_1{}^nX_2{}^nU_2{}^n}$ to denote the product of an i.i.d. distribution, i.e.

$$\overline{P}_{U_1{}^nX_1{}^nX_2{}^nU_2{}^n} = \prod_{t=1}^{n} \overline{P}_{U_1X_1X_2U_2}. \tag{4.37}$$

Fix a $\overline{P}_{U_1U_2|X_1X_2} = \overline{P}_{U_1|X_1}\overline{P}_{U_2|X_2}$ and functions $\phi_k(\cdot,\cdot)$ such that $Y_k = \phi_k(U_1,U_2)$ and $\mathbb{E}_{\overline{P}}[d_k(X_k,Y_k)] < D_k$. Note that $U_1 - X_1 - X_2 - U_2$ forms a Markov chain under $\overline{P}$. We must show that any rate pair (R_1,R_2) satisfying $R_1 > I(X_1;U_1)$ and $R_2 > I(X_2;U_2|U_1)$ is achievable.

As expected, the decoder will use a lossy representation of one source as side information to assist reconstruction of the other source. We can choose an $R_2' < I(U_1;U_2)$ such that $R_2 + R_2' > I(X_2;U_2)$. Here R_2' corresponds to the rate of a virtual message M_2' which is produced by Encoder 2 but not physically transmitted to the receiver. This will play the role of the index of the codeword in the bin in a traditional covering and random-binning proof.

First we will use the likelihood encoder derived from $\overline{P}_{X_1U_1}$ and a random codebook $\{{u_1}^n(m_1)\}$ generated according to $\overline{P}_{U_1}$ for Encoder 1. Then we will use the likelihood encoder derived from $\overline{P}_{X_2U_2}$ and another random codebook $\{{u_2}^n(m_2, m_2')\}$ generated according to $\overline{P}_{U_2}$ for Encoder 2. The decoder will use the transmitted message M_1 to decode ${U_1}^n$, as in the point-to-point case, and use the transmitted message M_2 along with the decoded ${U_1}^n$ to decode M_2' as $\hat{M}_2'$, as in the Wyner-Ziv case, and reproduce $u_2^n(M_2, \hat{M}_2')$. Finally, the decoder outputs the reconstructions ${Y_k}^n$ according to the symbol-by-symbol functions $\phi_k(\cdot,\cdot)$ of ${U_1}^n$ and ${U_2}^n$.

The distribution induced by the encoders and decoder is

$$\mathbf{P}_{{X_1}^n{X_2}^n{U_1}^n M_1 M_2 M_2' \hat{M}_2' {Y_1}^n {Y_2}^n} = P_{{X_1}^n{X_2}^n}\mathbf{P}_1\mathbf{P}_2 \tag{4.38}$$

where

$$\begin{aligned}
& \mathbf{P}_1(m_1, {u_1}^n|{x_1}^n) \\
\triangleq\ & \mathbf{P}_{M_1|{X_1}^n}(m_1|{x_1}^n)\mathbf{P}_{{U_1}^n|M_1}({u_1}^n|m_1) && (4.39)\\
\triangleq\ & \mathbf{P}_{LE1}(m_1|{x_1}^n)\mathbf{P}_{D1}({u_1}^n|m_1) && (4.40)
\end{aligned}$$

and

$$\begin{aligned}
& \mathbf{P}_2(m_2, m_2', \hat{m}_2', {y_1}^n, {y_2}^n|{x_2}^n, {u_1}^n) \\
\triangleq\ & \mathbf{P}_{M_2M_2'|{X_2}^n}(m_2, m_2'|{x_2}^n)\mathbf{P}_{\hat{M}_2'|M_2{U_1}^n}(\hat{m}_2'|m_2, {u_1}^n) \\
& \prod_{k=1,2} P_{{Y_k}^n|{U_1}^n M_2 \hat{M}_2'}({y_k}^n|{u_1}^n, m_2, \hat{m}_2') && (4.41)\\
\triangleq\ & \mathbf{P}_{LE2}(m_2, m_2'|{x_2}^n)\mathbf{P}_{D2}(\hat{m}_2'|m_2, {u_1}^n) \\
& \prod_{k=1,2} \mathbf{P}_{\Phi,k}({y_k}^n|{u_1}^n, m_2, \hat{m}_2'), && (4.42)
\end{aligned}$$

where $\mathbf{P}_{LE1}$ and $\mathbf{P}_{LE2}$ are the likelihood encoders; $\mathbf{P}_{D1}$ is the first part of the decoder that does a codeword lookup on $\mathcal{C}_1^{(n)}$; $\mathbf{P}_{D2}$ is the second part of the decoder that decodes m_2' as $\hat{m}_2'$; and $\mathbf{P}_{\Phi,k}({y_k}^n|{u_1}^n, m_2, \hat{m}_2')$ is the third part of the decoder that reconstructs the source sequences.

We now restate the behavior of the encoders and decoder, as components of the induced distribution.

Codebook generation: We independently generate 2^{nR_1} sequences in ${\mathcal{U}_1}^n$ according to $\prod_{t=1}^n \overline{P}_{U_1}(u_{1t})$ and index them by $m_1 \in [1 : 2^{nR_1}]$, and independently generate $2^{n(R_2+R_2')}$ sequences in ${\mathcal{U}_2}^n$ according to $\prod_{t=1}^n \overline{P}_{U_2}(u_{2t})$ and index them by $(m_2, m_2') \in [1 : 2^{nR_2}] \times [1 : 2^{nR_2'}]$. We use $\mathcal{C}_1^{(n)}$ and $\mathcal{C}_2^{(n)}$ to denote the two random codebooks, respectively.

Encoders: The first encoder $\mathbf{P}_{LE1}(m_1|{x_1}^n)$ is the likelihood encoder according to $\overline{P}_{{X_1}^n{U_1}^n}$ and $\mathcal{C}_1^{(n)}$. The second encoder $\mathbf{P}_{LE2}(m_2, m_2'|{x_2}^n)$ is the likelihood encoder according to $\overline{P}_{{X_2}^n{U_2}^n}$ and $\mathcal{C}_2^{(n)}$.

Decoder: First, let $\mathbf{P}_{D1}({u_1}^n|m_1)$ be a $\mathcal{C}_1^{(n)}$ codeword lookup decoder. Then, let $\mathbf{P}_{D2}(\hat{m}_2'|m_2, {u_1}^n)$ be a good channel decoder with respect to the sub-codebook $\mathcal{C}_2^{(n)}(m_2) = \{{u_2}^n(m_2, a)\}_a$ and the memoryless channel $\overline{P}_{U_1|U_2}$. Last, define ${\phi_k}^n({u_1}^n, {u_2}^n)$ as the concatenation $\{\phi_k(u_{1t}, u_{2t})\}_{t=1}^n$ and set the decoders $\mathbf{P}_{\Phi,k}$ to be the deterministic functions

$$\mathbf{P}_{\Phi,k}({y_k}^n|{u_1}^n, m_2, \hat{m}_2') \triangleq \mathbb{1}\{{y_k}^n = {\phi_k}^n({u_1}^n, {U_2}^n(m_2, \hat{m}_2'))\}. \tag{4.43}$$

Analysis: We will need the following distributions: the induced distribution $\mathbf{P}$ and auxiliary distributions $\mathbf{Q}_1$ and $\mathbf{Q}_1^*$. The general idea of the proof is as follows: Encoder 1 makes $\mathbf{P}$ and $\mathbf{Q}_1$ close in total variation. Distribution $\mathbf{Q}_1^*$ (random only with respect to the second codebook $\mathcal{C}_2^{(n)}$) is the expectation of $\mathbf{Q}_1$ over the random codebook $\mathcal{C}_1^{(n)}$. This is really the key step in the proof. By considering the expectation of the distribution with respect to $\mathcal{C}_1^{(n)}$, we effectively remove Encoder 1 from the problem and turn the message from Encoder 1 into memoryless side information at the decoder. Hence, the two distortions (averaged over $\mathcal{C}_1^{(n)}$) under $\mathbf{P}$ are roughly the same as the distortions under $\mathbf{Q}_1^*$, which is a much simpler distribution. We then recognize $\mathbf{Q}_1^*$ as precisely $\mathbf{P}$ in (4.10) from the Wyner-Ziv proof of the previous section, with a source pair (X_1, X_2), a pair of reconstructions (Y_1, Y_2) and U_1 as the side information.

1) The auxiliary distribution $\mathbf{Q}_1$ takes the following form:

$$\mathbf{Q}_{1\,{X_1}^n{X_2}^n{U_1}^n M_1 M_2 M_2' \hat{M}_2' {Y_1}^n {Y_2}^n} = \mathbf{Q}_{1\,M_1{U_1}^n{X_1}^n{X_2}^n}\mathbf{P}_2 \tag{4.44}$$

where

$$\begin{aligned} & \mathbf{Q}_{1M_1{U_1}^n{X_1}^n{X_2}^n}(m_1, {u_1}^n, {x_1}^n, {x_2}^n) \\ = \; & \frac{1}{2^{nR_1}} \mathbb{1}\{{u_1}^n = {U_1}^n(m_1)\} \overline{P}_{{X_1}^n|{U_1}^n}({x_1}^n|{u_1}^n) \overline{P}_{{X_2}^n|{X_1}^n}({x_2}^n|{x_1}^n). \end{aligned} \tag{4.45}$$

Note that $\mathbf{Q}_1$ is the idealized distribution with respect to the first message, as introduced in the point-to-point case. Hence, by the same arguments, since $R_1 > I(X_1; U_1)$, using the basic soft-covering lemma (Lemma 2.1),

$$\mathbb{E}_{\mathcal{C}_1^{(n)}} \left[\| \mathbf{Q}_1 - \mathbf{P} \|_{TV} \right] \leq \epsilon_{1_n}, \tag{4.46}$$

where $\mathbf{Q}_1$ and $\mathbf{P}$ are distributions over random variables ${X_1}^n, {X_2}^n, {U_1}^n, M_1, M_2, M_2', \hat{M}_2', {Y_1}^n, {Y_2}^n$ and ϵ_{1_n} is the error term introduced from the soft-covering lemma.

2) Taking the expectation over codebook $\mathcal{C}_1^{(n)}$, we define

$$\mathbf{Q}^*_{1{X_1}^n{X_2}^n{U_1}^n M_2 M_2' \hat{M}_2' {Y_1}^n {Y_2}^n} \triangleq \mathbb{E}_{\mathcal{C}_1^{(n)}} \left[\mathbf{Q}_{1{X_1}^n{X_2}^n{U_1}^n M_2 M_2' \hat{M}_2' {Y_1}^n {Y_2}^n} \right]. \tag{4.47}$$

Note that under this definition of $\mathbf{Q}_1^*$, we have

$$\begin{aligned} & \mathbf{Q}^*_{1{X_1}^n{X_2}^n{U_1}^n M_2 M_2' \hat{M}_2' {Y_1}^n {Y_2}^n}({x_1}^n, {x_2}^n, {u_1}^n, m_2, m_2', \hat{m}_2', {y_1}^n, {y_2}^n) \\ = \; & \mathbb{E}_{\mathcal{C}_1^{(n)}} \left[\mathbf{Q}^*_{1{X_1}^n{X_2}^n{U_1}^n}({x_1}^n, {x_2}^n, {u_1}^n) \right] \mathbf{P}_2(m_2, m_2', \hat{m}_2', {y_1}^n, {y_2}^n | {x_2}^n, {u_1}^n) \qquad (4.48) \\ = \; & \overline{P}_{{X_1}^n{X_2}^n{U_1}^n}({x_1}^n, {x_2}^n, {u_1}^n) \mathbf{P}_2(m_2, m_2', \hat{m}_2', {y_1}^n, {y_2}^n | {x_2}^n, {u_1}^n), \qquad (4.49) \end{aligned}$$

where the last step can be verified using the same technique as (3.13) given in Section 3.3.

By Property 2.1(b),

$$\begin{aligned}
& \mathbb{E}_{\mathcal{C}_1^{(n)}}\left[\mathbb{E}_{\mathbf{P}}\left[d_k({X_k}^n, {Y_k}^n)\right]\right] \\
\leq\ & \mathbb{E}_{\mathcal{C}_1^{(n)}}\left[\mathbb{E}_{\mathbf{Q}_1}[d_k({X_k}^n, {Y_k}^n)]\right] + d_{kmax}\epsilon_{1n} && (4.50)\\
=\ & \mathbb{E}_{\mathcal{C}_1^{(n)}}\left[\sum_{{x_k}^n, {y_k}^n} \mathbf{Q}_{1{X^n}{Y^n}}({x_k}^n, {y_k}^n) d_k({x_k}^n, {y_k}^n)\right] + d_{kmax}\epsilon_{1n} && (4.51)\\
=\ & \sum_{{x_k}^n, {y_k}^n} \mathbb{E}_{\mathcal{C}_1^{(n)}}[\mathbf{Q}_{1{X^n}{Y^n}}({x_k}^n, {y_k}^n)] d_k({x_k}^n, {y_k}^n) + d_{kmax}\epsilon_{1n} && (4.52)\\
=\ & \sum_{{x_k}^n, {y_k}^n} \mathbf{Q}^*_{1{X^n}{Y^n}}({x_k}^n, {y_k}^n) d_k({x_k}^n, {y_k}^n) + d_{kmax}\epsilon_{1n} && (4.53)\\
=\ & \mathbb{E}_{\mathbf{Q}_1^*}\left[d_k({X_k}^n, {Y_k}^n)\right] + d_{kmax}\epsilon_{1n}. && (4.54)
\end{aligned}$$

Note that $\mathbf{Q}_1^*$ is exactly of the form of the induced distribution $\mathbf{P}$ in the Wyner-Ziv proof of the previous section, with the inconsequential modification that there are two reconstructions and two distortion functions. Thus, by (4.19) through (4.30), we obtain

$$\begin{aligned}
& \mathbb{E}_{\mathcal{C}_2^{(n)}}\left[\mathbb{E}_{\mathbf{Q}_1^*}\left[d_k({X_k}^n, {Y_k}^n)\right]\right] \\
\leq\ & \mathbb{E}_{\overline{P}}\left[d_k(X_k, Y_k)\right] + d_{kmax}(\epsilon_{2n} + \delta_n), && (4.55)
\end{aligned}$$

where ϵ_{2n} and δ_n are error terms introduced from the soft-covering lemma and channel decoding, respectively.

Finally, taking expectation over $\mathcal{C}_1^{(n)}$ and using (4.54) and (4.55),

$$\begin{aligned}
& \mathbb{E}_{\mathcal{C}_2^{(n)}}\left[\mathbb{E}_{\mathcal{C}_1^{(n)}}\left[\mathbb{E}_{\mathbf{P}}\left[d_k({X_k}^n, {Y_k}^n)\right]\right]\right] \\
\leq\ & \mathbb{E}_{\mathcal{C}_2^{(n)}}\left[\mathbb{E}_{\mathbf{Q}_1^*}\left[d_k({X_k}^n, {Y_k}^n)\right] + d_{kmax}\epsilon_{1n}\right] && (4.56)\\
\leq\ & \mathbb{E}_{\overline{P}}\left[d_k(X_k, Y_k)\right] + d_{kmax}\epsilon_{1n} + d_{kmax}(\epsilon_{2n} + \delta_n), && (4.57)
\end{aligned}$$

where (4.56) follows from (4.54); and (4.57) follows from (4.54) and (4.55). Taking the limit on both sides gives:

$$\limsup_{n\to\infty} \mathbb{E}_{\mathcal{C}_2^{(n)}}\left[\mathbb{E}_{\mathcal{C}_1^{(n)}}\left[\mathbb{E}_{\mathbf{P}}\left[d_k({X_k}^n, {Y_k}^n)\right]\right]\right] \leq D_k \tag{4.58}$$

■

Remark 3. *Note that the proof above uses the proof of Wyner-Ziv achievability from the previous section. To do the entire proof step by step, we would define a total of three auxiliary distributions, which would be the* $\mathbf{Q}_1$ *used in the proof, as well as* $\mathbf{Q}_2^{(1)}$ *and* $\mathbf{Q}_2^{(2)}$ *defined below for completeness. The steps outlined above show how to relate the induced distribution* $\mathbf{P}$ *to* $\mathbf{Q}_1$ *and its expectation* $\mathbf{Q}_1^*$*. This effectively converts the message from Encoder 1 into memoryless side information at the decoder. The omitted steps, as seen in the previous section, relate* $\mathbf{Q}_1^*$ *to* $\mathbf{Q}_2^{(1)}$ *through the soft-covering lemma and* $\mathbf{Q}_2^{(1)}$ *to* $\mathbf{Q}_2^{(2)}$ *through reliable channel decoding. The expected value of* $\mathbf{Q}_2^{(2)}$ *over codebooks is the desired distribution* $\overline{P}$*. For reference, the omitted auxiliary distributions are*

$$\begin{aligned}
& \mathbf{Q}_{2M_2M_2'U_2{}^nX_2{}^nX_1{}^nU_1{}^n}(m_2, m_2', u_2{}^n, x_2{}^n, x_1{}^n, u_1{}^n) \\
= \; & \frac{1}{2^{n(R_2+R_2')}} \mathbb{1}\{u_2{}^n = U_2{}^n(m_2, m_2')\} \overline{P}_{X_2{}^n|U_2{}^n}(x_2{}^n|u_2{}^n) \\
& \overline{P}_{X_1{}^nU_1{}^n|X_2{}^n}(x_1{}^n, u_1{}^n|x_2{}^n),
\end{aligned} \tag{4.59}$$

which is of the same structure as the idealized distribution described in Fig. 4.2, and

$$\begin{aligned}
\mathbf{Q}_2^{(1)}{}_{X_1{}^nX_2{}^nU_1{}^nM_2M_2'\hat{M}_2'Y_1{}^nY_2{}^n} \triangleq \; & \mathbf{Q}_{2X_1{}^nX_2{}^nU_1{}^nM_2M_2'}(x_1{}^n, x_2{}^n, u_1{}^n, m_2, m_2') \\
& \mathbf{P}_{D2}(\hat{m}_2'|m_2, u_1{}^n) \prod_{k=1,2} \mathbf{P}_{\Phi,k}(y_k{}^n|u_1{}^n, m_2, \hat{m}_2')
\end{aligned} \tag{4.60}$$

$$\begin{aligned}
\mathbf{Q}_2^{(2)}{}_{X_1{}^nX_2{}^nU_1{}^nM_2M_2'\hat{M}_2'Y_1{}^nY_2{}^n} \triangleq \; & \mathbf{Q}_{2X_1{}^nX_2{}^nU_1{}^nM_2M_2'}(x_1{}^n, x_2{}^n, u_1{}^n, m_2, m_2') \\
& \mathbf{P}_{D2}(\hat{m}_2'|m_2, u_1{}^n) \prod_{k=1,2} \mathbf{P}_{\Phi,k}(y_k{}^n|u_1{}^n, m_2, m_2').
\end{aligned} \tag{4.61}$$

Remark 4. *To see how this is a simpler proof than the traditional joint typicality encoder proof, recall from [10] that to bound the different error events, we would need the regular covering lemma, the conditional typicality lemma, the Markov lemma, and the mutual packing lemma, some of which are quite involving to verify. With the likelihood encoder, all we need is the soft-covering lemma and Lemma 4.1.*

4.5 Summary

In this chapter, we have used the likelihood encoder to obtain achievability results for multiuser lossy source coding problems. The simplicity of the analysis is accentuated when used for distributed source coding because it bypasses the need for a Markov lemma of any form and it avoids the technical complications that can arise in analyzing the decoder whenever random binning is involved in lossy compression. Although we only demonstrate with two cases, the Wyner-Ziv and the Berger-Tung settings, it is believed that the likelihood encoder and its corresponding analysis can achieve other best known source coding results. A highlight in the achievability proof for the Wyner-Ziv setting is that we are able to apply the channel coding result directly without the need for a packing lemma. This becomes an important feature in proving secrecy results in the next chapters.

Chapter 5

Rate-Distortion Based Security in the Noiseless Wiretap Channel

5.1 Introduction

In this chapter, we investigate secrecy in source coding problems from a rate-distortion approach. We first review Shannon's formulation of perfect secrecy in lossy compression using a shared secret key, where the secrecy performance is measured by a quantity called "equivocation". Then we introduce Yamamoto's rate-distortion based formulation of the same communication system. We refer to this model as the naive formulation, because it does not ensure a strong secure communication system. However, this naive formulation remains an important game-theoretic setting. In particular, the model captures the essence of a system where the legitimate receiver and eavesdropper are each only given one attempt to estimate the source. Next, we apply this naive secrecy formulation to physical layer security where instead of a shared secret key, the legitimate receiver and the eavesdropper have access to side information that is correlated with the source.

At the end of the chapter, we strengthen the formulation by causally disclosing the source realization to the eavesdropper during decoding. It turns out this modification not only provides a stable secure communication system, but also fully generalizes the equivocation formulation. Although these two metrics, equivocation and distortion, appear

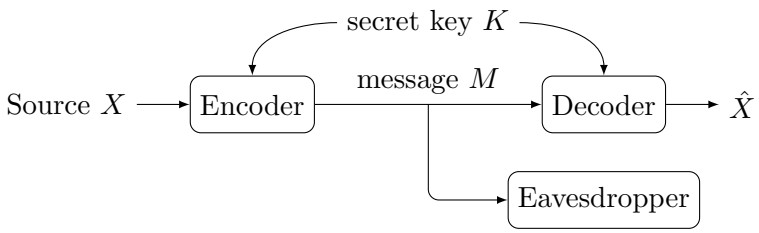

Figure 5.1: The Shannon cipher system.

to be completely unrelated at a first glance, with careful choice of distortion function, equivocation becomes a special case under the causal disclosure formulation.

5.2 Secure Source Coding Via Secret Key

5.2.1 The Shannon Cipher System and Perfect Secrecy

The concept of perfect secrecy was first introduced by Shannon in "Communication Theory of Secrecy Systems" [1], in which the secrecy system in Fig. 5.1 was studied. The transmitter has a source X. The legitimate receiver aims to decode the source losslessly. The encoder and decoder share some common randomness, secret key K.

The system is considered **perfectly secure** if the source and the encrypted message received by the eavesdropper are statistically independent. This can be quantified by the conditional entropy $H(X|M)$. We can therefore formally define perfect secrecy as follows.

Definition 5.1. *The Shannon cipher system is perfectly secure if*

$$\mathbb{P}[\hat{X} \neq X] = 0 \tag{5.1}$$

$$H(X|M) = H(X). \tag{5.2}$$

This is a very strong notion of secrecy. An important result under perfect secrecy is that the number of secret key bits required needs to be at least the entropy of the source. In other words, if we would efficiently and losslessly compress the source X into a bit stream of length l, the secret key bits needs to be at least the same length l to guarantee perfect secrecy. This can be achieved by using a "one-time pad".

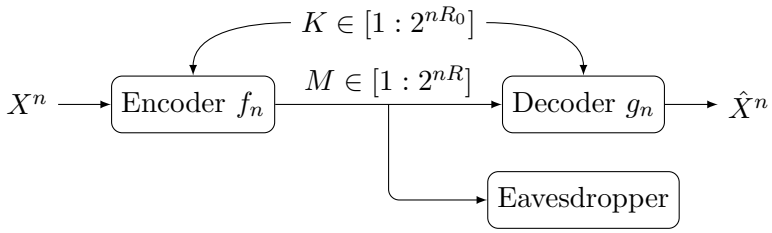

Figure 5.2: The Shannon cipher system with a sequence of source symbols.

The use of conditional entropy for measuring secrecy was also considered in the original work on the wiretap channel in [7] and [30]. When a sequence of source symbols X^n is involved Fig. 5.2, instead of directly using the conditional entropy itself, this quantity is normalized over the blocklength $\frac{1}{n}H(X^n|M)$, which is referred as "equivocation rate" in the literature.

Consider the setup of an i.i.d. source sequence X^n distributed according to $\prod_{t=1}^{n} P_X(x_t)$ with secret key K satisfying the following constraints:

- Encoder $f_n : \mathcal{X}^n \times \mathcal{K} \mapsto \mathcal{M}$ (possibly stochastic)
- Legitimate receiver decoder $g_n : \mathcal{M} \times \mathcal{K} \mapsto \hat{\mathcal{X}}^n$ (possibly stochastic)
- Compression rate: R, i.e. $|\mathcal{M}| = 2^{nR}$
- Secret key rate: R_0, i.e. $|\mathcal{K}| = 2^{nR_0}$
- Lossless reconstruction at the legitimate receiver:

$$\mathbb{P}[\hat{X}^n \neq X^n] \to_n 0 \tag{5.3}$$

- Equivocation at the eavesdropper

$$\liminf_{n\to\infty} \frac{1}{n} H(X^n|M) \geq H(X). \tag{5.4}$$

Definition 5.2. *A rate pair (R, R_0) is achievable under perfect secrecy if there exists a sequence of rate (R, R_0) encoders and decoders (f_n, g_n) such that*

$$\mathbb{P}[\hat{X}^n \neq X^n] \to_n 0, \tag{5.5}$$

$$\liminf_{n\to\infty} \frac{1}{n} H(X^n|M) \geq H(X). \tag{5.6}$$

Theorem 5.1 (Shannon [1])**.** *A rate pair (R, R_0) is achievable under perfect secrecy if and only if*

$$R \geq H(X), \tag{5.7}$$

$$R_0 \geq H(X). \tag{5.8}$$

5.2.2 Naive Rate-Distortion Based Secrecy

We first consider the simplest rate-distortion based secrecy formulation of a noiseless wiretap channel. This is essentially the same setting as the Shannon cipher system with a sequence of source symbols, except the secrecy here is measured by a distortion function instead of equivocation. This type of secrecy setting was introduced by Yamamoto [2], where upper and lower bounds on the tradeoff between the rate of secret key and the eavesdropper's distortion were established. The problem was solved in [3]. We now formally summarize the problem setup and its main result.

We want to determine the rate-distortion region for a secrecy system with an i.i.d. source sequence distributed according to $\prod_{t=1}^{n} P_X(x_t)$ satisfying the following constraints:

- Encoder $f_n : \mathcal{X}^n \times \mathcal{K} \mapsto \mathcal{M}$ (possibly stochastic)
- Legitimate receiver decoder: $g_n : \mathcal{M} \times \mathcal{K} \mapsto \hat{\mathcal{X}}^n$ (possibly stochastic)
- Eavesdropper decoder: $P_{Z^n|M}$
- Compression rate: R, i.e. $|\mathcal{M}| = 2^{nR}$
- Secret key rate: R_0, i.e. $|\mathcal{K}| = 2^{nR_0}$.

The system performance is measured according the following metrics:

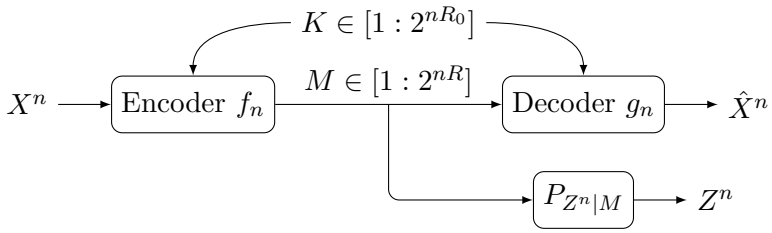

Figure 5.3: Naive setup for rate-distortion based secrecy.

- Lossless reconstruction for the legitimate receiver:

$$\mathbb{P}[\hat{X}^n \neq X^n] \to_n 0 \tag{5.9}$$

- Minimum average distortion for the eavesdropper:

$$\liminf_{n\to\infty} \min_{P_{Z^n|M}} \mathbb{E}\left[d(X^n, Z^n)\right] \geq D. \tag{5.10}$$

Definition 5.3. *The rate distortion triple (R, R_0, D) is achievable if there exists a sequence of rate (R, R_0) encoders and decoders (f_n, g_n) such that*

$$\mathbb{P}[\hat{X}^n \neq X^n] \to_n 0 \tag{5.11}$$

and

$$\liminf_{n\to\infty} \min_{P_{Z^n|M}} \mathbb{E}\left[d(X^n, Z^n)\right] \geq D. \tag{5.12}$$

The above mathematical formulation is illustrated in Fig. 5.3.

The main result is summarized in the following theorem.

Theorem 5.2. *The closure of achievable rate-distortion triple* (R, R_0, D) *is given by the following region:*

$$\begin{aligned} R &\geq H(X), && (5.13)\\ R_0 &\geq 0, && (5.14)\\ D &\leq \min_z \mathbb{E}[d(X,z)]. && (5.15) \end{aligned}$$

The original proof can be found in [3]. Here we make a quick comment. The converse is straightforward from lossless compression and the fact that the eavesdropper's estimate of the source cannot be worse than its a-priori estimation based only on the source distribution. To show achievability, a simpler way (compared to the scheme given in [3]) would be using the likelihood encoder with its corresponding analysis.

5.3 Secure Source Coding with Side Information at the Decoders

In this section, we investigate the physical layer security of a noiseless wiretap channel with side information at the decoders [31].

The wire-tap channel with side information at the decoders has been previously investigated. It was studied in [32] under an equivocation constraint at the eavesdropper and a complete characterization of the rate-distortion-equivocation region was derived. A related problem with coded side information was studied in [33]. However, using equivocation as the description of secrecy does not capture how much distortion will occur if the eavesdropper is forced to reconstruct the source. In this work, both the legitimate receiver and the eavesdropper's reconstructions of the source are measured by distortion. Furthermore, the eavesdropper is assumed to make the best use of its side information along with the encoded message. This setting can also be interpreted as a game-theoretic model where the two receivers are playing a zero-sum game and each one is required to output a sequence that is closest to the source sequence being transmitted.

It was shown in the previous section that a secret key with any strictly positive rate can force the eavesdropper's reconstruction of the source to be as bad as if it knows only the source distribution, i.e. the distortion under perfect secrecy. This result suggests, if instead of a shared secret key, the decoders have access to different side information, we should be able to force the eavesdropper's reconstruction of the source to have the distortion under perfect secrecy as long as the legitimate receiver's side information is somewhat stronger than the eavesdropper's side information with respect to the source. This is indeed the case, which will be formally stated herein. However, in the more general case, the legitimate receiver may not have the stronger side information. Can a positive distortion still be forced upon the eavesdropper? We show in this section that we can encode the source in favor of the legitimate receiver's side information so that the eavesdropper can only make limited use of the encoded message even with the help of its side information.

5.3.1 Problem Formulation

We want to determine the rate-distortion region for a secrecy system with an i.i.d. source and two side information sequences (X^n, B^n, W^n) distributed according to $\prod_{t=1}^{n} P_{XBW}(x_t, b_t, w_t)$ satisfying the following constraints:

- Encoder $f_n : \mathcal{X}^n \mapsto \mathcal{M}$ (possibly stochastic);
- Legitimate receiver decoder $g_n : \mathcal{M} \times \mathcal{B}^n \mapsto \mathcal{Y}^n$ (possibly stochastic);
- Eavesdropper decoder $P_{Z^n|MW^n}$;
- Compression rate: R, i.e. $|\mathcal{M}| = 2^{nR}$.

The system performance is measured according to the following distortion metrics:

- Average distortion for the legitimate receiver:

$$\limsup_{n\to\infty} \mathbb{E}[d_b(X^n, Y^n)] \leq D_b \tag{5.16}$$

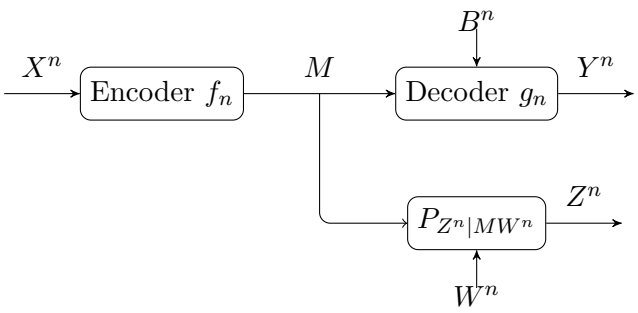

Figure 5.4: Secrecy system setup with side information at the decoders.

- Minimum average distortion for the eavesdropper:

$$\liminf_{n\to\infty} \min_{P_{Z^n|MW^n}} \mathbb{E}[d_w(X^n, Z^n)] \geq D_w \tag{5.17}$$

Note that d_b and d_w can be the same or different distortion measures.

Definition 5.4. *The rate-distortion triple (R, D_b, D_w) is achievable if there exists a sequence of rate R encoders and decoders (f_n, g_n) such that*

$$\limsup_{n\to\infty} \mathbb{E}[d_b(X^n, Y^n)] \leq D_b \tag{5.18}$$

and

$$\liminf_{n\to\infty} \min_{P_{Z^n|MW^n}} \mathbb{E}[d_w(X^n, Z^n)] \geq D_w. \tag{5.19}$$

The above mathematical formulation is illustrated in Fig. 5.4.

For the special case of lossless compression between the transmitter and the legitimate receiver, we make the following definition.

Definition 5.5. *A rate-distortion pair (R, D_w) is achievable if there exists a sequence of encoders and decoders (f_n, g_n) such that*

$$\mathbb{P}\left[X^n \neq Y^n\right] \to_n 0 \tag{5.20}$$

and

$$\liminf_{n\to\infty} \min_{P_{Z^n|M,W^n}} \mathbb{E}[d_w(X^n, Z^n)] \geq D_w. \tag{5.21}$$

Less Noisy and More Capable Side Information

Definition 5.6. *The side information B is **strictly** less noisy than the side information W with respect to X if*

$$I(V;B) > I(V;W)$$

for all V such that $V - X - (B,W)$ and $I(V;B) > 0$.

Definition 5.7. *The side information B is **strictly** more capable than the side information W with respect to X if*

$$I(X;B) > I(X;W).$$

5.3.2 Inner Bound

Theorem 5.3. *A rate-distortion triple (R, D_b, D_w) is achievable if*

$$R > I(V;X|B) \tag{5.22}$$

$$D_b \geq \mathbb{E}[d_b(X,Y)] \tag{5.23}$$

$$D_w \leq \min_{z(u,w)} \mathbb{E}[d_w(X, Z(U,W))] \tag{5.24}$$

$$I(V;B|U) > I(V;W|U) \tag{5.25}$$

for some $P_{UVXBW} = P_{XBW}P_{V|X}P_{U|V}$, where $Y = \phi(V,B)$ for some function $\phi(\cdot,\cdot)$.

Theorem 5.3 involves two auxiliary variables U and V that are correlated with the source X in a Markov chain relationship. The variable V can be understood as the lossy representation of X that is communicated efficiently using random binning to the intended receiver, which will be used with the side information B to estimate X, just as in the setting without an eavesdropper which was pioneered by [27]. The purpose of the auxiliary variable U is to provide secrecy similar to the way secrecy is achieved in [32]. The side information at the intended receiver must be better than that of the eavesdropper (as measured by

mutual information with V) in order to prevent decoding of V. The variable U (if needed) is given away to all parties as the first layer of a superposition code in order to generate this condition for V.

We now give the achievability proof of Theorem 5.3 using the soft-covering lemmas. We apply the same proof technique using the likelihood encoder as introduced in Chapter 3 with the modification of using a superposition codebook.

The source is encoded into four messages M_p, M_p', M_s and M_s', where M_p and M_s are transmitted and M_p' and M_s' are virtual messages that are not physically transmitted, but will be recovered with small error at the legitimate receiver with the help of the side information. On the other hand, M_p and M_p' play the role of public messages, which both the legitimate receiver and the eavesdropper will decode; M_s and M_s' index a codeword that is kept secret from the eavesdropper, which only the legitimate receiver can make sense of with its own side information.

The $\overline{P}$ notation is used in the same way as in the previous chapters and P is used to denote the system induced distribution. Note that $\overline{P}_{XBW} = P_{XBW}$.

Proof. Fix a distribution $\overline{P}_{UVXBW} = \overline{P}_{XBW}\overline{P}_{V|X}\overline{P}_{U|V}$ satisfying

$$I(V;B|U) > I(V;W|U), \tag{5.26}$$

$$\mathbb{E}_{\overline{P}}[d_b(X,\phi(V,B))] \leq D_b, \tag{5.27}$$

$$\min_{z(u,w)} \mathbb{E}_{\overline{P}}[d_w(X,Z(U,W))] \geq D_w, \tag{5.28}$$

and fix rates R_p, R_p', R_s, R_s' such that

$$R_p + R_p' > I(U;X), \tag{5.29}$$

$$R_p' < I(U;B), \tag{5.30}$$

$$R_s + R_s' > I(X;V|U), \tag{5.31}$$

$$I(V;W|U) < R_s' < I(V;B|U). \tag{5.32}$$

The distribution induced by the encoder and decoder is

$$\begin{aligned} & \mathbf{P}(x^n, b^n, w^n, m_p, m_p', m_s, m_s', \hat{m}_p', \hat{m}_s', y^n) \\ \triangleq \; & P_{X^n B^n W^n}(x^n, b^n, w^n) \mathbf{P}_{LE}(m_p, m_p', m_s, m_s'|x^n) \\ & \mathbf{P}_D(\hat{m}_p', \hat{m}_s'|m_p, m_s, b^n) \mathbf{P}_\Phi(y^n|m_p, \hat{m}_p', m_s, \hat{m}_s', b^n), \end{aligned} \tag{5.33}$$

where $\mathbf{P}_{LE}(m_p, m_p', m_s, m_s'|x^n)$ is the source encoder; $\mathbf{P}_D(\hat{m}_p', \hat{m}_s'|m_p, m_s, b^n)$ is the first part of the decoder that estimates m_p' and m_s' as $\hat{m}_p'$ and $\hat{m}_s'$; $\mathbf{P}_\Phi(y^n|m_p, \hat{m}_p', m_s, \hat{m}_s', b^n)$ is the second part of the decoder that reconstructs the source sequence.

Codebook generation: We independently generate $2^{n(R_p+R_p')}$ sequences in $\mathcal{U}^n$ according to $\prod_{t=1}^n \overline{P}_U(u_t)$ and index by $(m_p, m_p') \in [1 : 2^{nR_p}] \times [1 : 2^{nR_p'}]$. We use $\mathcal{C}_U^{(n)}$ to denote this random codebook. For each $(m_p, m_p') \in [1 : 2^{nR_p}] \times [1 : 2^{nR_p'}]$, we independently generate $2^{n(R_s+R_s')}$ sequences in $\mathcal{V}^n$ according to $\prod_{t=1}^n \overline{P}_{V|U}(v_t|u_t(m_p, m_p'))$ and index by (m_p, m_p', m_s, m_s'), $(m_s, m_s') \in [1 : 2^{nR_s}] \times [1 : 2^{nR_s'}]$. We use $\mathcal{C}_V^{(n)}(m_p, m_p')$ to denote this random codebook.

Encoder: The encoder $\mathbf{P}_{LE}(m_p, m_p', m_s, m_s'|x^n)$ is a likelihood encoder that chooses M_p, M_p', M_s, M_s' stochastically according to the following probability:

$$\mathbf{P}_{LE}(m|x^n) = \frac{\mathcal{L}(m|x^n)}{\sum_{\bar{m} \in \mathcal{M}} \mathcal{L}(\bar{m}|x^n)} \tag{5.34}$$

where $m = (m_p, m_p', m_s, m_s')$, $\mathcal{M} = [1 : 2^{nR_p}] \times [1 : 2^{nR_p'}] \times [1 : 2^{nR_s}] \times [1 : 2^{nR_s'}]$, and

$$\mathcal{L}(m|x^n) = \overline{P}_{X^n|V^n}(x^n|v^n(m)). \tag{5.35}$$

Decoder: The decoder has two parts. Let $\mathbf{P}_D(\hat{m}_p', \hat{m}_s'|m_p, m_s, b^n)$ be a good channel decoder with respect to the superposition sub-codebook $\{v^n(m_p, a_p, m_s, a_s)\}_{a_p, a_s}$ and the memoryless channel $\overline{P}_{B|V}$. For the second part of the decoder, fix a function $\phi(\cdot, \cdot)$. Define $\phi^n(v^n, b^n)$ as the concatenation $\{\phi(v_t, b_t)\}_{t=1}^n$ and set the decoder $\mathbf{P}_\Phi$ to be the deterministic

function

$$\begin{aligned} & \mathbf{P}_{\Phi}(y^n|m_p, \hat{m}'_p, m_s, \hat{m}'_s, b^n) \\ \triangleq \;& \mathbb{1}\{y^n = \phi^n(v^n(m_p, \hat{m}'_p, m_s, \hat{m}'_s), b^n)\}. \end{aligned} \tag{5.36}$$

Analysis: We examine the distortions at the two receivers one at a time. To analyze the distortion at the legitimate receiver, we will consider four distributions, the induced distribution $\mathbf{P}$, two approximating distributions $\mathbf{Q}^{(1)}$ and $\mathbf{Q}^{(2)}$, and an auxiliary distribution $\mathbf{Q}'$ that helps with the analysis. The idea is to show that 1) the system has nice behavior for distortion under $\mathbf{Q}^{(2)}$; and 2) $\mathbf{P}$ and $\mathbf{Q}^{(2)}$ are close in total variation (on average over the random codebook) through $\mathbf{Q}^{(1)}$. To analyze the distortion at the eavesdropper, we will consider the induced distribution $\mathbf{P}$ together with an auxiliary distribution $\tilde{\mathbf{Q}}$.

Distortion at the Legitimate Receiver

This part of the proof follows the same idea of the achievability proof for the Wyner-Ziv setting using the likelihood encoder given in Section 4.3.2.

The approximating distributions $\mathbf{Q}^{(1)}$ and $\mathbf{Q}^{(2)}$ are defined through an idealized distribution $\mathbf{Q}$ of the structure given in Fig. 5.5. This idealized distribution $\mathbf{Q}$ can be written as

$$\begin{aligned} & \mathbf{Q}_{X^n B^n W^n M_p M'_p M_s M'_s U^n V^n}(x^n, b^n, w^n, m_p, m'_p, m_s, m'_s, u^n, v^n) \\ = \;& Q_{M_p M'_p M_s M'_s}(m_p, m'_p, m_s, m'_s) \mathbf{Q}_{U^n|M_p M'_p}(u^n|m_p, m'_p) \mathbf{Q}_{V^n|U^n M_s M'_s}(v^n|u^n, m_s, m'_s) \\ & \mathbf{Q}_{X^n B^n W^n|M_p M'_p M_s M'_s}(x^n, b^n, w^n|m_p, m'_p, m_s, m'_s) \end{aligned} \tag{5.37}$$

$$\begin{aligned} = \;& \frac{1}{2^{n(R_p+R'_p+R_s+R'_s)}} \mathbb{1}\{u^n = U^n(m_p, m'_p)\} \mathbb{1}\{v^n = V^n(m_p, m'_p, m_s, m'_s)\} \\ & \overline{P}_{X^n B^n W^n|V^n}(x^n, b^n, w^n|V^n(m_p, m'_p, m_s, m'_s)) \end{aligned} \tag{5.38}$$

$$\begin{aligned} = \;& \frac{1}{2^{n(R_p+R'_p+R_s+R'_s)}} \mathbb{1}\{u^n = U^n(m_p, m'_p)\} \mathbb{1}\{v^n = V^n(m_p, m'_p, m_s, m'_s)\} \\ & \prod_{t=1}^{n} \overline{P}_{X|V}(x_t|v_t) \overline{P}_{BW|X}(b_t, w_t|x_t), \end{aligned} \tag{5.39}$$

where (5.39) follows from the Markov relation $V - X - BW$.

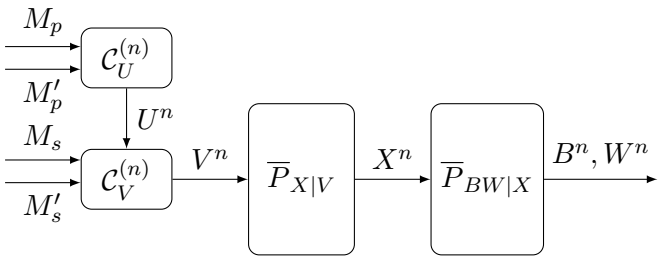

Figure 5.5: Idealized distribution $\mathbf{Q}$ via a superposition codebook and memoryless channels $\overline{P}_{X|V}$ and $\overline{P}_{BW|X}$.

Note that the encoder $\mathbf{P}_{LE}$ satisfies

$$\mathbf{P}_{LE}(m_p, m_p', m_s, m_s'|x^n) = \mathbf{Q}_{M_p M_p' M_s M_s'|X^n}(m_p, m_p', m_s, m_s'|x^n). \tag{5.40}$$

Furthermore, it can be verified with the same technique used in Section 3.3 that the idealized distribution $\mathbf{Q}$ satisfies

$$\begin{aligned} & \mathbb{E}_{\mathcal{C}^{(n)}}\left[\mathbf{Q}_{X^n B^n W^n U^n V^n}(x^n, b^n, w^n, u^n, v^n)\right] \\ = \;& \overline{P}_{X^n B^n W^n U^n V^n}(x^n, b^n, w^n, u^n, v^n), \end{aligned} \tag{5.41}$$

where $\mathbb{E}_{\mathcal{C}^{(n)}}[\cdot]$ denotes $\mathbb{E}_{\mathcal{C}_U^{(n)}}\left[\mathbb{E}_{\mathcal{C}_V^{(n)}}[\cdot]\right]$.

We now define the distributions $\mathbf{Q}^{(1)}$ and $\mathbf{Q}^{(2)}$ via the idealized distribution $\mathbf{Q}$ as follows:

$$\begin{aligned} & \mathbf{Q}^{(1)}_{X^n B^n W^n U^n V^n M_p M_p' M_s M_s' \hat{M}_p' \hat{M}_s'}(x^n, b^n, w^n, u^n, v^n, m_p, m_p', m_s, m_s', \hat{m}_p', \hat{m}_s') \\ \triangleq \;& \mathbf{Q}_{X^n B^n W^n M_p M_p' M_s M_s' U^n V^n}(x^n, b^n, w^n, m_p, m_p', m_s, m_s', u^n, v^n) \\ & \mathbf{P}_D(\hat{m}_p', \hat{m}_s'|m_p, m_s, b^n)\mathbf{P}_\Phi(y^n|m_p, \hat{m}_p', m_s, \hat{m}_s') \end{aligned} \tag{5.42}$$

$$\begin{aligned} & \mathbf{Q}^{(2)}_{X^n B^n W^n U^n V^n M_p M_p' M_s M_s' \hat{M}_p' \hat{M}_s'}(x^n, b^n, w^n, u^n, v^n, m_p, m_p', m_s, m_s', \hat{m}_p', \hat{m}_s') \\ \triangleq \;& \mathbf{Q}_{X^n B^n W^n M_p M_p' M_s M_s' U^n V^n}(x^n, b^n, w^n, m_p, m_p', m_s, m_s', u^n, v^n) \\ & \mathbf{P}_D(\hat{m}_p', \hat{m}_s'|m_p, m_s, b^n)\mathbf{P}_\Phi(y^n|m_p, m_p', m_s, m_s'). \end{aligned} \tag{5.43}$$

Notice that the distributions $\mathbf{Q}^{(1)}$ and $\mathbf{Q}^{(2)}$ differ only in $\mathbf{P}_\Phi$. From (5.41), it can be shown that the distortion under distribution $\mathbf{Q}^{(2)}$ averaged over the random codebook is given by the following:

$$\begin{aligned}
& \mathbb{E}_{\mathcal{C}^{(n)}}\left[\mathbb{E}_{\mathbf{Q}^{(2)}}[d_b(X^n,Y^n)]\right] \\
= & \sum_{x^n,v^n,b^n} \mathbb{E}_{\mathcal{C}^{(n)}}\left[\mathbf{Q}_{X^nV^nB^n}(x^n,v^n,b^n)\right] d_b(x^n,\phi^n(v^n,b^n)) && (5.44)\\
= & \sum_{x^n,v^n,b^n} \overline{P}_{X^nV^nB^n}(x^n,v^n,b^n) d_b(x^n,\phi^n(v^n,b^n)) && (5.45)\\
= & \mathbb{E}_{\overline{P}}\left[d_b(X,Y)\right]. && (5.46)
\end{aligned}$$

Define the auxiliary distribution $\mathbf{Q}'$ on a subset of the variables as

$$\mathbf{Q}'_{M_pM'_pX^n}(m_p,m'_p,x^n) \triangleq \frac{1}{2^{n(R_p+R'_p)}}\overline{P}_{X^n|U^n}(x^n|U^n(m_p,m'_p)). \tag{5.47}$$

Since $R_s+R'_s > I(X;V|U)$, applying the generalized superposition soft-covering lemma 2.2, we have

$$\mathbb{E}_{\mathcal{C}^{(n)}}\left[\left\|\mathbf{Q}_{M_pM'_pX^n}-\mathbf{Q}'_{M_pM'_pX^n}\right\|_{TV}\right] \le e^{-\gamma_2 n} \triangleq \epsilon_{2n}. \tag{5.48}$$

Also since $R_p+R'_p > I(U;X)$, applying the basic soft-covering lemma (Lemma 2.1), we have

$$\mathbb{E}_{\mathcal{C}^{(n)}}\left[\left\|P_{X^n}-\mathbf{Q}'_{X^n}\right\|_{TV}\right] \le e^{-\gamma_1 n} \triangleq \epsilon_{1n}. \tag{5.49}$$

Using Property 2.1(b), (5.49), and (5.48), we obtain

$$\mathbb{E}_{\mathcal{C}^{(n)}}\left[\|\mathbf{Q}_{X^n}-P_{X^n}\|_{TV}\right] \le \epsilon_{1n}+\epsilon_{2n} \triangleq \epsilon_{3n}. \tag{5.50}$$

Therefore, by definitions of $\mathbf{P}$ and $\mathbf{Q}^{(1)}$ and Property 2.1(c), we have

$$\mathbb{E}_{\mathcal{C}^{(n)}}\left[\left\|\mathbf{P}-\mathbf{Q}^{(1)}\right\|_{TV}\right] \le \epsilon_{3n} \tag{5.51}$$

where the distributions are taken over $X^n B^n W^n M_p M'_p M_s M'_s \hat{M}'_p \hat{M}'_s Y^n$.

On the one hand, we need to apply the Wyner-Ziv technique to complete the distortion bound at the legitimate receiver. Since $R'_p < I(U;B)$ and $R'_s < I(V;B|U)$, the codebooks are randomly generated, and M'_p and M'_s are uniformly distributed under $\mathbf{Q}$, it is well known that the maximum likelihood decoder (as well as a variety of other decoders) will drive the error probability to zero as n goes to infinity. This can be seen from Fig. 5.5, by identifying for fixed M_p and M_s, that M'_p and M'_s are the messages to be transmitted over the memoryless channel $\overline{P}_{B|V}$ with the superposition codebook. Specifically,

$$\mathbb{E}_{\mathcal{C}^{(n)}}\left[\mathbb{P}_{\mathbf{Q}^{(1)}}\left[(\hat{M}'_p, \hat{M}'_s) \neq (M'_p, M'_s)\right]\right] \leq \delta_n \to_n 0. \tag{5.52}$$

Using Lemma 4.1, it can be shown that

$$\begin{aligned} & \mathbb{E}_{\mathcal{C}^{(n)}}\left[\left\| \mathbf{Q}^{(1)}_{X^n B^n W^n M_p \hat{M}'_p M_s \hat{M}'_s} - \mathbf{Q}^{(2)}_{X^n B^n W^n M_p M'_p M_s M'_s} \right\|_{TV}\right] \\ \leq\ & \mathbb{E}_{\mathcal{C}^{(n)}}\left[\mathbb{P}_{\mathbf{Q}^{(1)}}\left[(\hat{M}'_p, \hat{M}'_s) \neq (M'_p, M'_s)\right]\right] \qquad (5.53) \\ \leq\ & \delta_n. \qquad (5.54) \end{aligned}$$

Hence, by (5.46), (5.51) and (5.54) and Property 2.1(a) and (b), we obtain

$$\begin{aligned} & \mathbb{E}_{\mathcal{C}^{(n)}}\left[\mathbb{E}_{\mathbf{P}}[d_b(X^n, Y^n)]\right] \\ \leq\ & \mathbb{E}_{\overline{P}}[d_b(X,Y)] + d_{bmax}(\epsilon_{3n} + \delta_n) \qquad (5.55) \\ \leq\ & D_b + d_{bmax}(\epsilon_{3n} + \delta_n). \qquad (5.56) \end{aligned}$$

This completes the distortion analysis at the legitimate receiver.

Distortion at the Eavesdropper

To evaluate the enforced distortion at the eavesdropper with the best possible decoder, we will consider two distributions: the system induced distribution $\mathbf{P}$ and an auxiliary

distribution $\tilde{\mathbf{Q}}^{(i)}$ defined as

$$\begin{aligned} & \tilde{\mathbf{Q}}^{(i)}_{M_pM_p'M_sM_s'U^nXW^n}(m_p, m_p', m_s, m_s', u^n, x, w^n) \\ \triangleq \; & \frac{1}{2^{n(R_p+R_p'+R_s+R_s')}} 1\{u^n = U^n(m_p, m_p')\} \\ & \prod_{t=1}^{n} \overline{P}_{W|U}(w_t|U_t(m_p, m_p'))\overline{P}_{X|WU}(x|w_i, U_i(m_p, m_p')). \end{aligned} \tag{5.57}$$

Note that under $\tilde{\mathbf{Q}}^{(i)}$, we have the Markov relation

$$X - U_i(M_p, M_p')W_i - M_pM_p'M_sM_s'W^n. \tag{5.58}$$

The auxiliary distribution $\tilde{\mathbf{Q}}^{(i)}$ has the following property:

$$\mathbb{E}_{\mathcal{C}_U^{(n)}}\left[\tilde{\mathbf{Q}}^{(i)}_{U^nW^nX}(u^n, w^n, x)\right] = \prod_{t=1}^{n} \overline{P}_U(u_t)\overline{P}_{W|U}(w_t|u_t)\overline{P}_{X|WU}(x|w_i, u_i). \tag{5.59}$$

Recall that under distribution $\mathbf{Q}$, for fixed $M_s = m_s$,

$$\begin{aligned} & \mathbf{Q}_{M_pM_p'M_s'W^nX_i|M_s}(m_p, m_p', m_s', w^n, x_i|m_s) \\ = \; & \frac{1}{2^{n(R_p+R_p'+R_s')}} \overline{P}_{W^n|V^n}(w^n|V^n(m_p, m_p', m_s, m_s')) \\ & \overline{P}_{X|WVU}(x_i|w_i, V_i(m_p, m_p', m_s, m_s'), U_i(m_p, m_p')) \end{aligned} \tag{5.60}$$

Since $R_s' > I(V; W|U)$, by applying the superposition soft-covering lemma 2.2, we have for fixed m_s,

$$\mathbb{E}_{\mathcal{C}^{(n)}}\left[\left\|\tilde{\mathbf{Q}}^{(i)}_{M_pM_p'W^nX} - \mathbf{Q}_{M_pM_p'W^nX_i}\right\|_{TV}\right] \leq e^{-\gamma_4 n} \triangleq \epsilon_{4n}. \tag{5.61}$$

Averaging over M_s, we have

$$\mathbb{E}_{\mathcal{C}^{(n)}}\left[\left\|\tilde{\mathbf{Q}}^{(i)}_{M_pM_p'M_sW^nX} - \mathbf{Q}_{M_pM_p'M_sW^nX_i}\right\|_{TV}\right] \leq \epsilon_{4n}, \tag{5.62}$$

and by Property 2.1(b), (5.51) and (5.62),

$$\mathbb{E}_{\mathcal{C}^{(n)}}\left[\left\|\tilde{\mathbf{Q}}^{(i)}_{M_pM_p'M_sW^nX}-\mathbf{P}_{M_pM_p'M_sW^nX_i}\right\|_{TV}\right]\leq\epsilon_{3n}+\epsilon_{4n}\triangleq\epsilon_{5n}. \tag{5.63}$$

Also note that, since $R_p+R_p'>0$, we can invoke Lemma 2.2 by identifying

$$(R_1,R_2,U,V,X,Z)\leftarrow(0,R_p+R_p',\varnothing,U,\varnothing,U), \tag{5.64}$$

where the left side symbols represents the symbols from Lemma 2.2. This gives us

$$\mathbb{E}_{\mathcal{C}^{(n)}}\left[\left\|\tilde{\mathbf{Q}}^{(i)}_{u_i(M_p,M_p')}-\overline{P}_U\right\|_{TV}\right]\leq e^{-\gamma_6 n}\triangleq\epsilon_{6n}. \tag{5.65}$$

Combining (5.56), (5.63) and (5.65), we get

$$\begin{aligned}
&\mathbb{E}_{\mathcal{C}^{(n)}}\Bigg[\sum_{i=1}^{n}\left\|\mathbf{P}_{M_pM_p'M_sW^nX_i}-\tilde{\mathbf{Q}}^{(i)}_{M_pM_p'M_sW^nX}\right\|_{TV}\\
&\quad+\sum_{i=1}^{n}\left\|\tilde{\mathbf{Q}}^{(i)}_{u_i(M_p,M_p')}-\overline{P}_U\right\|_{TV}+\left|\mathbb{E}_{\mathbf{P}}[d_b(X^n,Y^n)]-D_b\right|\Bigg]\\
\leq\;& n\epsilon_{5n}+n\epsilon_{6n}+d_{bmax}(\epsilon_{3n}+\delta_n) &(5.66)\\
\leq\;& ne^{-n\min(\gamma_1,\gamma_2,\gamma_4,\gamma_6)}+d_{bmax}(\epsilon_{3n}+\delta_n) &(5.67)\\
\triangleq\;& \epsilon_n\to_n 0. &(5.68)
\end{aligned}$$

Therefore, there exists a codebook under which

$$\sum_{i=1}^{n}\left\|P_{M_pM_p'M_sW^nX_i}-\tilde{Q}^{(i)}_{M_pM_p'M_sW^nX}\right\|_{TV}\leq\epsilon_n, \tag{5.69}$$

$$\sum_{i=1}^{n}\left\|\tilde{Q}^{(i)}_{u_i(M_p,M_p')}-\overline{P}_U\right\|_{TV}\leq\epsilon_n, \tag{5.70}$$

and

$$\mathbb{E}_P[d_b(X^n,Y^n)]\leq D_b+\epsilon_n. \tag{5.71}$$

Finally, the distortion at the eavesdropper can be lower bounded by

$$\begin{aligned}
& \min_{z^n(m_p,m_s,w^n)} \mathbb{E}_P\left[d_w(X^n, z^n(M_p, M_s, W^n))\right] \\
\geq\ & \min_{z^n(m_p,m_p',m_s,w^n)} \mathbb{E}_P\left[d_w(X^n, z^n(M_p, M_p', M_s, W^n))\right] && (5.72)\\
=\ & \frac{1}{n}\sum_{i=1}^{n} \min_{z_i(m_p,m_p',m_s,w^n)} \mathbb{E}_P\left[d_w(X_i, z_i(M_p, M_p', M_s, W^n))\right] && (5.73)\\
\geq\ & \frac{1}{n}\sum_{i=1}^{n} \min_{z_i(m_p,m_p',m_s,w^n)} \mathbb{E}_{\tilde{Q}^{(i)}}\left[d_w(X, z_i(M_p, M_p', M_s, W^n))\right] - \epsilon_n d_{wmax} && (5.74)\\
=\ & \frac{1}{n}\sum_{i=1}^{n} \min_{z(u,w)} \mathbb{E}_{\tilde{Q}^{(i)}}\left[d_w(X, z(u_i(M_p, M_p'), W_i))\right] - \epsilon_n d_{wmax} && (5.75)\\
\geq\ & \frac{1}{n}\sum_{i=1}^{n} \min_{z(u,w)} \mathbb{E}_{\overline{P}}\left[d_w(X, z(U, W))\right] - 2\epsilon_n d_{wmax} && (5.76)
\end{aligned}$$

where (5.75) uses the Markov relation under $\tilde{Q}^{(i)}$ given in (5.58), and (5.76) uses $\left\|\tilde{Q}^{(i)}_{u_i(M_p,M_p')} - \overline{P}_U\right\|_{TV} \leq \epsilon_n$ from (5.70) and the fact that

$$\tilde{Q}^{(i)}_{W_iX|U_i}(w_i, x|u_i) = \overline{P}_{W|U}(w_i|u_i)\overline{P}_{X|WU}(x|w_i, u_i) \tag{5.77}$$

from (5.57).

This completes the distortion analysis at the eavesdropper. □

5.3.3 Outer Bound

A tight outer bound is not attained and hence, the optimality of Theorem 5.3 is not yet known. A trivial outer bound is stated as follows for completeness.

Theorem 5.4. *If a rate-distortion triple (R, D_b, D_w) is achievable, then*

$$R \geq I(V; X|B) \tag{5.78}$$

$$D_b \geq \mathbb{E}[d_b(X, Y)] \tag{5.79}$$

$$D_w \leq \min_{z(w)} \mathbb{E}[d_w(X, z(W))] \tag{5.80}$$

for some $P_{VXBW} = P_{XBW}P_{V|X}$, where $Y = \phi(V, B)$ for some function $\phi(\cdot,\cdot)$.

Proof. To get (5.78) and (5.79), we just need to apply the Wyner-Ziv converse; and to get (5.80), observe that the reconstruction cannot be worse than the symbol-by-symbol estimation of X^n from W^n without using M. □

5.3.4 Special Cases

Less Noisy Side Information

Corollary 5.1. *If the legitimate receiver has **strictly** less noisy side information than the eavesdropper, the converse of Theorem 5.4 is tight.*

Proof. To see the achievability, we just need to set the U in Theorem 5.3 to be $\varnothing$. □

Note that the strictly less noisy condition meets the inequality in Theorem 5.3. Corollary 5.1 covers the case of degraded side information at the eavesdropper, i.e. $X-B-W$, except for the corner case where $I(X;W) = I(X;B)$.

Lossless Compression

When the legitimate receiver must reconstruct the source sequence losslessly, we have the following inner bound.

Corollary 5.2. (R, D_w) *is achievable if*

$$R > H(X|B) \tag{5.81}$$

$$D_w \leq \min_{z(u,w)} \mathbb{E}[d_w(X, z(U,W))] \tag{5.82}$$

$$I(X;B|U) > I(X;W|U) \tag{5.83}$$

for some $P_{UXBW} = P_{XBW}P_{U|X}$.

Proof. This is consistent with Theorem 5.3 by setting $V = X$ and that the additional proof required for lossless recovery follows naturally from the construction of the achievability scheme for Theorem 5.3. □

Corollary 5.3. *If the legitimate receiver has strictly more capable side information than the eavesdropper with respect to the source, then the rate-distortion pair* (R, D_w) *is achievable*

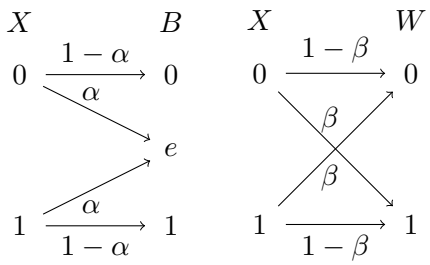

Figure 5.6: Side information B and W correlated with source X

if and only if

$$R \geq H(X|B) \tag{5.84}$$

$$D_w \leq \min_{z(w)} \mathbb{E}[d_w(X, z(W))]. \tag{5.85}$$

5.3.5 Example

We give an example for the lossless compression case with Hamming distortion measure for the eavesdropper.

Let X^n be an i.i.d. $Bern(p)$ source, and let B^n and W^n be side information obtained through a binary erasure channel (BEC) and binary symmetric channel (BSC), respectively, i.e.

$$P_X(0) = 1 - P_X(1) = 1 - p, \tag{5.86}$$

$$P_{B|X}(e|x) = \alpha, \tag{5.87}$$

$$P_{W|X}(1 - x|x) = \beta. \tag{5.88}$$

This is illustrated in Fig. 5.6. This type of side information was also considered in [34], but only with a $Bern(\frac{1}{2})$ source.

We consider a generic discrete auxiliary random variable U that takes values on $1, ..., |\mathcal{U}|$ with $\overline{P}_U(i) = u_i$ and $\overline{P}_{X|U}(0|i) = \delta_i$, $\overline{P}_{X|U}(1|i) = 1 - \delta_i$. It can be shown that the distortion D_w takes the following form. By applying Corollary 5.2, we can obtain the following theorem.

Theorem 5.5. *(R, D_w) is achievable for the BEC-BSC side information with Hamming distortion $d_w(\cdot,\cdot)$ if*

$$\begin{aligned} R &\geq \alpha h(p) \\ D_w &\leq \max_{\{u_i,\delta_i\}_{i=1}^3} \sum_{i=1}^3 u_i \min(\delta_i, 1-\delta_i, \beta) \\ &\quad s.t. \quad 0 \leq u_i, \delta_i \leq 1 \\ &\quad \sum_{i=1}^3 u_i = 1 \\ &\quad \sum_{i=1}^3 u_i \delta_i = 1 - p \\ &\quad \sum_{i=1}^3 u_i [(1-\alpha) h(\delta_i) - h(\delta_i * \beta)] + h(\beta) \geq 0 \end{aligned}$$

where $h(\cdot)$ denotes the binary entropy function.

We plot the distortion at the eavesdropper as a function of the source distribution p for fixed α and β in Fig. 5.7 and Fig. 5.8, where the outer bounds are calculated from Theorem 5.4.

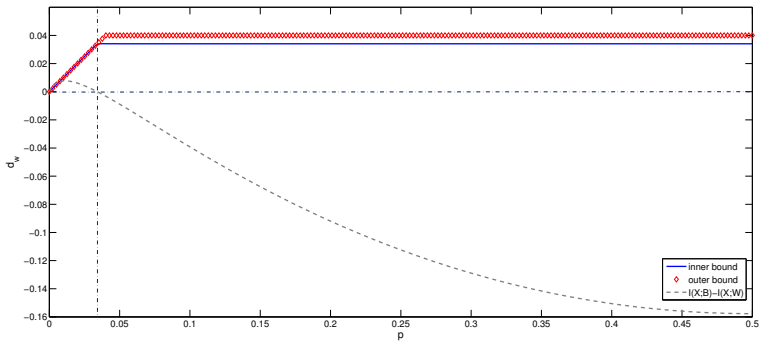

Figure 5.7: Distortion at the eavesdropper as a function of source distribution p with $\alpha = 0.4$, $\beta = 0.04$.

In Fig. 5.7, when the legitimate receiver's side information is more capable than the eavesdropper's side information with respect to the source, distortion equivalent to perfect secrecy at the eavesdropper is achieved; when the eavesdropper's side information is more capable than the legitimate receiver, with our encoding scheme, we achieve a positive

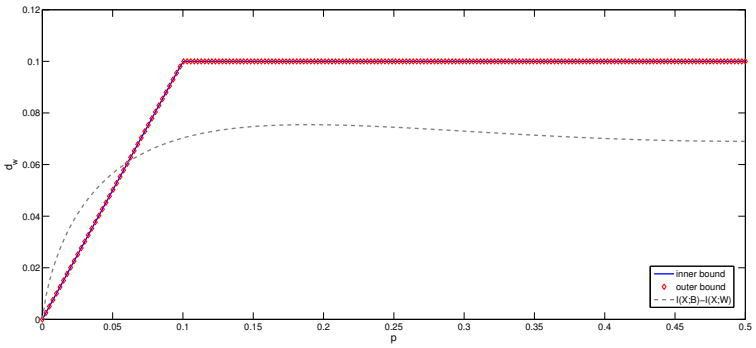

Figure 5.8: Distortion at the eavesdropper as a function of source distribution p with $\alpha = 0.4$, $\beta = 0.1$.

distortion at the eavesdropper with no additional cost on the compression rate to ensure lossless decoding at the legitimate receiver. It is worth noting that our scheme encodes the source so that it favors the side information for the legitimate receiver even if the legitimate receiver's side information is less capable, as opposed to using the regular Wyner-Ziv (Slepian-Wolf) encoding scheme that gives the same compression rate but no distortion at the eavesdropper.

In Fig. 5.8, since the legitimate receiver's side information is always more capable than the eavesdropper's side information, it is a direct application of Corollary 5.3 and distortion equivalent to perfect secrecy is ensured.

5.4 Secure Source Coding with Causal Disclosure

In this section, we make the connection between equivocation and distortion as metrics for secrecy. We first illustrate why the naive formulation in Section 5.2.2 is not a good metric for secrecy by using the "one-bit secrecy" example given in [6].

Consider an i.i.d. source X^n with $X_i \sim Bern(\frac{1}{2})$. K is one bit of shared secrect key used to encrypt X^n in the following way:

$$Y_i = X_i \oplus K. \tag{5.89}$$

Upon receiving Y^n the legitimate receiver can decode with the shared secret key K. Under Hamming distortion, it is easy to see that the eavesdropper's best strategy is to output $Z^n = Y^n$, yielding an average distortion of $\frac{1}{2}$. This is indeed the maximum possible average distortion. However, this is a vulnerable secrecy model because the eavesdropper knows that X^n can only be one of the two candidate sequences.

In the above example, the eavesdropper is able to decode the entire sequence accurately after observing the first symbol realization. Motivated by this observation, [4] [5] and [6] formulate the rate-distortion based secrecy setting with causal disclosure, where the eavesdropper has access to the past realization of the source sequence. It is also shown in [6] that the equivocation metric becomes a special case of the distortion metric with causal source disclosure by choosing the distortion function to be log-loss. Here we recap the main result under this setting.

5.4.1 Problem Formulation

We want to determine the rate-distortion region for a secrecy system with an i.i.d. source sequence X^n distributed according to $\prod_{t=1}^{n} P_X(x_t)$ satisfying the following constraints:

- Encoder $f_n : \mathcal{X}^n \times \mathcal{K} \mapsto \mathcal{M}$ (possibly stochastic)
- Legitimate receiver decoder $g_n : \mathcal{M} \times \mathcal{K} \mapsto \mathcal{Y}^n$ (possibly stochastic)
- Eavesdropper decoder $\{P_{Z_t|MX^{t-1}}\}_{t=1}^{n}$
- Compression rate: R, i.e. $|\mathcal{M}| = 2^{nR}$
- Secret key rate: R_0, i.e. $|\mathcal{K}| = 2^{nR_0}$.

The system performance is measured according to the following distortion metrics:

- Average distortion for the legitimate receiver:

$$\limsup_{n\to\infty} \mathbb{E}\left[d_b(X^n, Y^n)\right] \leq D_b \tag{5.90}$$

- Minimum average distortion for the eavesdropper:

$$\liminf_{n\to\infty} \min_{\{P_{Z_t|MX^{t-1}}\}_{t=1}^{n}} \mathbb{E}\left[d_e(X^n, Z^n)\right] \geq D_e. \tag{5.91}$$

Definition 5.8. *The rate-distortion quadruple (R, R_0, D_b, D_e) is achievable if there exists a sequence of rate (R, R_0) encoders and decoders (f_n, g_n) such that*

$$\limsup_{n\to\infty} \mathbb{E}\left[d_b(X^n, Y^n)\right] \leq D_b \tag{5.92}$$

and

$$\liminf_{n\to\infty} \min_{\{P_{Z_t|MX^{t-1}}\}_{t=1}^{n}} \mathbb{E}\left[d_e(X^n, Z^n)\right] \geq D_e. \tag{5.93}$$

The above mathematical formulation is illustrated in Fig. 5.9.

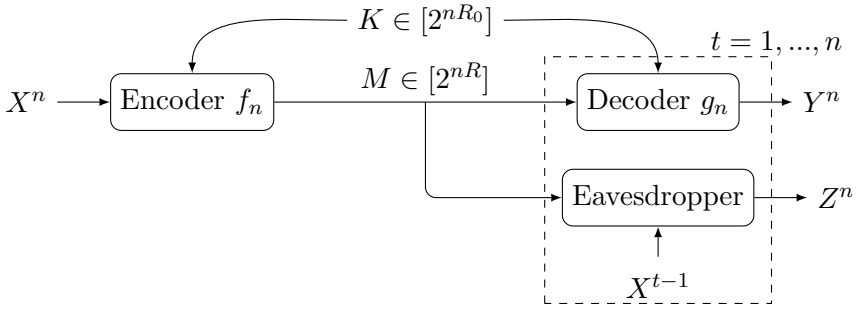

Figure 5.9: Rate-distortion based secrecy system setup with shared secret key and causal source disclosure.

For the special case of lossless compression at the legitimate receiver, we make the following definition.

Definition 5.9. *A rate-distortion triple (R, R_0, D_e) is achievable if there exists a sequence of rate (R, R_0) encoders and decoders (f_n, g_n) such that*

$$\mathbb{P}[X^n \neq Y^n] \to_n 0 \tag{5.94}$$

and

$$\liminf_{n\to\infty} \min_{\{P_{Z_t|MX^{t-1}}\}_{t=1}^{n}} \mathbb{E}\left[d_e(X^n, Z^n)\right] \geq D_e. \tag{5.95}$$

5.4.2 Main Results

The main results are summarized in the following theorem. The proofs are found in the original paper [6] and not presented here.

Theorem 5.6. *The rate-distortion quadruple* (R, R_0, D_b, D_e) *is achievable if and only if*

$$\begin{aligned} R &\geq I(X;Y) && (5.96)\\ R_0 &\geq I(X;Y|U) && (5.97)\\ D_b &\geq \mathbb{E}[d_b(X, \phi(Y))] && (5.98)\\ D_e &\leq \min_{z(u)} \mathbb{E}[d_e(X, z(U))] && (5.99) \end{aligned}$$

for some distribution $P_X P_{Y|X} P_{U|Y}$ *and some function* $\phi(\cdot)$.

For the special case of lossless compression, we have the following corollary.

Corollary 5.4. *The rate-distortion triple* (R, R_0, D_e) *is achievable if and only if*

$$\begin{aligned} R &\geq H(X) && (5.100)\\ R_0 &\geq H(X|U) && (5.101)\\ D_e &\leq \min_{z(u)} \mathbb{E}[d_e(X, z(U))] && (5.102) \end{aligned}$$

for some distribution $P_X P_{U|X}$.

5.4.3 Equivocation

We now examine Theorem 5.6 by setting $d_e(\cdot,\cdot)$ to the log-loss function defined as

$$d_e(x, z) = \log \frac{1}{z(x)} \tag{5.103}$$

where z is a probability distribution on $\mathcal{X}$, and $z(x)$ denotes the probability of $x \in \mathcal{X}$ according to $z \in \Delta_{\mathcal{X}}$. Therefore, the distortion at the eavesdropper can be written as

$$\begin{aligned}
&\min_{\{P_{Z_t|MX^{t-1}}\}_{t=1}^n} \mathbb{E}\left[\frac{1}{n}\sum_{t=1}^n d_e(X_t, Z_t)\right] \\
&= \frac{1}{n}\sum_{t=1}^n \min_{P_{Z|MX^{t-1}}} \mathbb{E}\left[d_e(X_t, Z)\right] && (5.104)\\
&= \frac{1}{n}\sum_{t=1}^n \min_{P_{Z|MX^{t-1}}} \mathbb{E}\left[\log\frac{1}{Z(X_t)}\right] && (5.105)\\
&= \frac{1}{n}\sum_{t=1}^n H(X_t|MX^{t-1}) && (5.106)\\
&= \frac{1}{n}H(X^n|M) && (5.107)
\end{aligned}$$

where (5.106) is due to Lemma 5.1 stated below.

Lemma 5.1. *Fix a pair of random variables (X, Y) and let $\mathcal{Z} = \Delta_{\mathcal{X}}$. Then*

$$H(X|Y) = \min_{Z: X-Y-Z} \mathbb{E}\left[\log\frac{1}{Z(X)}\right] \tag{5.108}$$

where $z(x)$ is the probability of x according to z.

Proof. If $X - Y - Z$, then

$$\begin{aligned}
&\mathbb{E}\left[\log\frac{1}{Z(X)}\right] \\
&= \mathbb{E}\left[\log\frac{1}{P_{X|Y}(X|Y)}\right] + \mathbb{E}\left[\log\frac{P_{X|Y}(X|Y)}{Z(X)}\right] && (5.109)\\
&= H(X|Y) + \sum_{y,z} P_{YZ}(y,z) D(P_{X|Y=y}||z) && (5.110)\\
&\geq H(X|Y) && (5.111)
\end{aligned}$$

where equality holds if $z = P_{X|Y=y}$ for all (y, z). □

The above observation shows that equivocation $\frac{1}{n}H(X^n|M)$ is nothing but a special case under the distortion metric with causal source disclosure.

5.4.4 Binary Source

In this section, we illustrate the result from causal source disclosure for the lossless case given by Corollary 5.4 with a $Bern(p)$ i.i.d. source sequence and Hamming distortion.

Consider the setup given by Fig. 5.9 and Definition 5.9. The source distribution is particularized to $X_t \sim Bern(p)$. For distortion, we use Hamming distortion for the eavesdropper:

$$d(x, x') = d_e(x, x') \triangleq \mathbb{1}\{x \neq x'\}. \tag{5.112}$$

The optimal achievable region is solved in [6] reproduced as follows.

Theorem 5.7. *The optimal (R, R_0, D_e) region for $Bern(p)$ source and Hamming distortion is given by*

$$R \geq H(X) \tag{5.113}$$

$$D_e \leq D_L(R_0) \tag{5.114}$$

where

$$D_L(R_0) = \min\{f(R_0), p, 1-p\}, \tag{5.115}$$

where the function $f(\cdot)$ is defined as the linear interpolation of the points $(\log n, \frac{n-1}{n})$, for $n \in \mathbb{N}$.

5.4.5 Gaussian Source

In this section, we investigate the application of the general results from causal source disclosure, namely, Theorem 5.6 and Corollary 5.4 to a Gaussian i.i.d. source sequence and squared error distortion.

Consider the setup given by Fig. 5.9 and Definition 5.8, 5.9. The source distribution is particularized to Gaussian distribution, $X_t \sim \mathcal{N}(\mu_0, \sigma_0^2)$. For distortion, we use normalized

squared error distortion for both the legitimate receiver and the eavesdropper:

$$d(x,x') = d_b(x,x') = d_e(x,x') \triangleq \frac{1}{\sigma_0^2}(x'-x)^2. \tag{5.116}$$

We want to solve for the region stated in Theorem 5.6 for our choice of source distribution and distortion measure. For convenience, instead of looking at the entire region, we work with its boundary – distortion-rate functions. Also, here we examine a joint payoff function by combining the two distortion functions as the following:

$$\pi(x,y,z) \triangleq \frac{1}{\sigma_0^2}[(z-x)^2 - (y-x)^2]. \tag{5.117}$$

Note that (5.117) compares the squared error distortions of the legitimate receiver and the eavesdropper. If the distance between the eavesdropper's symbol z and the original source symbol x is greater than that of the legitimate receiver's symbol y and x, we have a positive payoff; otherwise, we get a negative payoff. Similarly, the payoff of sequences is defined as the average of per letter payoff:

$$\pi(x^n,y^n,z^n) \triangleq \frac{1}{n}\sum_{t=1}^{n}\pi(x_t,y_t,z_t). \tag{5.118}$$

We rewrite the region in Theorem 5.6 for the above modifications as the optimal payoff function:

$$\Pi(R,R_0) = \max_{P_{YU|X}\in\mathcal{P}} \min_{z(u)} \mathbb{E}\left[\pi(X,Y,z(U))\right] \tag{5.119}$$

$$\mathcal{P} = \left\{ \begin{array}{l} P_{YU|X}: \\ X-Y-U \\ R_0 \geq I(X;Y|U) \\ R \geq I(X;Y) \end{array} \right\}, \tag{5.120}$$

where $\Pi(R,R_0)$ is the maximum payoff that is achievable with rates (R,R_0). To specialize this result to the Gaussian case, we must optimize over the choice of distribution $P_{YU|X}$. It is often the case for Gaussian problems that the choice of jointly Gaussian auxiliary random

variables is optimal. However, because the legitimate receiver and the eavesdropper are playing the game competitively instead of collaboratively, it turns out that a joint Gaussian distribution does as poorly as if no auxiliary random variable is used.

Let us first make the following observation:

$$\begin{aligned} & \Pi(R, R_0) \\ = & \max_{P_{YU|X}(y,u|x)\in\mathcal{P}} \min_{z(u)} \frac{1}{\sigma_0^2}\mathbb{E}[(z(U)-X)^2-(Y-X)^2] \qquad (5.121) \\ = & \frac{1}{\sigma_0^2} \max_{P_{YU|X}\in\mathcal{P}} \Bigg[\sum_{x,u} P_{U|X}(u|x)P_X(x)(x-\mathbb{E}[X|U=u])^2 \\ & -\sum_{x,y} P_{Y|X}(y|x)P_X(x)(y-x)^2 \Bigg] \qquad (5.122) \end{aligned}$$

where (5.122) comes from the fact that the conditional mean is the minimum mean squared error (MMSE) estimator. Here we are using $\sum$ and $\int$ interchangebly for convenience because it is not clear whether Y and U are discrete or not at this stage.

The optimal payoff for this problem is only solved completely for $R_0 \geq 1$ bit. But before explaining the optimal payoff, we first discuss two suboptimal solutions.

A. Jointly Gaussian

Theorem 5.8. *The solution to* (5.119) *for a Gaussian source is*

$$\Pi(R, R_0) = 1 - \exp\left(-2\min(R_0, R)\right) \qquad (5.123)$$

when P_{XYU} is constrained to be a jointly Gaussian distribution.

The proof can be found in [35] and is not presented here.

Note that Theorem 5.8 implies that for a jointly Gaussian distribution P_{XYU}, choosing the auxiliary random variable U correlated with X and Y does not improve the payoff from an uncorrelated U. In this case, U does not give out any information about X and therefore the distortion between the source and the eavesdropper is kept to a maximum as if under perfect secrecy. However, the rate-distortion tradeoff between the source and the legitimate receiver is limited by the secret key rate. Is it possible to achieve a higher payoff by another

choice of $P_{YU|X}$? Next we show how a simple Gaussian quantization can provide a better solution that is independent of the key rate R_0 under certain conditions.

B. Gaussian Quantization

Let us consider the following construction. X is quantized symmetrically about its mean with uniform intervals T as shown in Fig. 5.10 so that $Y \triangleq nT, n \triangleq \arg\min_{k\in\mathbb{Z}} |kT - X|$, and $U = |Y|$. With this construction, Y is a function of X and U is a function of Y. The reason for choosing such a symmetric quantization is that, to maintain a high distortion between the source and the eavesdropper in (5.122), we want to keep $\mathbb{E}[X|U = u]$ unbiased for all u.

Then the two constraints in (5.119) become

$$R_0 \geq I(X;Y|U) = H(Y|U) = s \text{ bits}, s < 1 \tag{5.124}$$

$$R \geq I(X;Y) = H(Y). \tag{5.125}$$

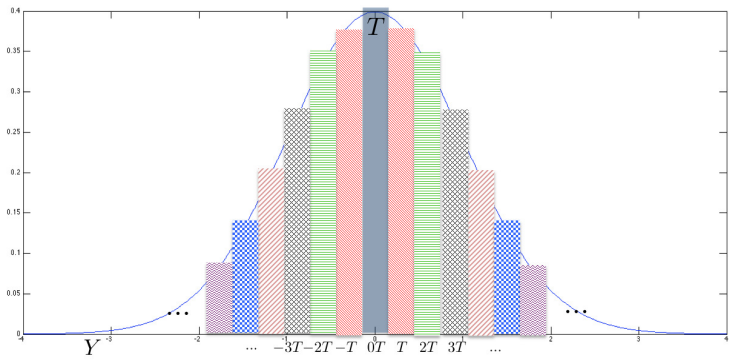

Figure 5.10: Symmetric quantization of the Gaussian random variable X with uniform interval T.

Here we apply the operational meaning of differential entropy from Theorem 9.3.1 of [9] to get

$$H(Y) + \log T \quad \to \quad h(X), \text{ as } T \to 0, \tag{5.126}$$

where $h(X)$ denotes the differential entropy of X. Recall that the differential entropy of a Gaussian random variable is $h(X) = \frac{1}{2}\log(2\pi e\sigma_0^2)$. Therefore, for $R_0 \geq 1$ bit, as $T \to 0$,

a sufficient condition for (5.125) is $T \geq \sqrt{2\pi e}\sigma_0 \exp(-R)$. The distortion between the source and the eavesdropper under this Gaussian quantization scheme can be asymptotically calculated as follows:

$$\begin{aligned} D^{\Delta}(R) &= \int_{-\infty}^{\infty} \sum_{y} P_{Y|X}(y|x) \frac{1}{\sqrt{2\pi}\sigma_0} e^{-\frac{x^2}{2\sigma_0^2}} (y-x)^2 dx & (5.127) \\ &= \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}\sigma_0} e^{-\frac{x^2}{2\sigma_0^2}} (nT-x)^2 dx & (5.128) \\ &\leq \frac{\pi e}{2} \sigma_0^2 \exp(-2R). & (5.129) \end{aligned}$$

Summarizing the above analysis, we have

$$\Pi(R, R_0) \geq 1 - \frac{\pi e}{2} 2^{-2R} \text{ for } R_0 \geq 1 \text{ bit and } R \to \infty. \tag{5.130}$$

With Gaussian quantization, even though we sacrifice a constant factor on the distortion between the source and the legitimate receiver, the overall payoff is no longer governed by the key rate R_0 given that $R_0 \geq 1$ bit. This illustrates that the joint Gaussian distribution does not achieve optimal payoff. Next, we provide a construction for Y and U that achieves maximum payoff under certain conditions.

Optimal Payoff for $R_0 \geq 1$ bit

Theorem 5.9. *If the key rate $R_0 \geq 1$ bit, the optimal secrecy rate-payoff function for an i.i.d. Gaussian source is given by*

$$\Pi(R, R_0) = 1 - 2^{-2R}. \tag{5.131}$$

Proof. To see the converse, observe that by relaxing the constraints in (5.119) and evaluating (5.122), we have

$$\max_{P_{YU|X}} \sum_{u,x} P_{U|X}(u|x) P_X(x) (x - \mathbb{E}[X|U=u])^2 = \sigma_0^2 \tag{5.132}$$

$$\min_{P_{YU|X}: I(X;Y) \leq R} \sum_{x,y} P_{Y|X}(y|x) P_X(x) (y-x)^2 = \sigma_0^2 2^{-2R} \tag{5.133}$$

where (5.133) comes from the distortion rate function $d(R)$ of a Gaussian source. To show the achievability, we choose $P_{YU|X}$ as follows. Y is chosen such that X and Y are zero-mean jointly Gaussian. $U \triangleq |Y|$ and $V \triangleq sgn(Y)$, where $sgn(Y)$ is a binary variable indicating the sign of Y. Observe that U, V together gives Y. By this construction, we have

$$I(X;Y|U) \;=\; I(X;V|U) \;<\; 1 \text{ bit}. \tag{5.134}$$

Therefore, given that $R_0 \geq 1$ bit, the constraint $R_0 \geq I(X;Y|U)$ is automatically satisfied from (5.134). In addition, $\mathbb{E}[X|U=u] = \frac{1}{2}\mathbb{E}[X|Y=u] + \frac{1}{2}\mathbb{E}[X|Y=-u] = 0$ for all u due to symmetry. The payoff achieves $1 - 2^{-2R}$. □

The optimization problem (5.119) for the case $R_0 < 1$ bit involves the coupling of two terms in (5.122). We next present a special case for this regime using a Gaussian quantizer.

Gaussian Quantizer Special Case

We now address a special structure of the system with causal source disclosure. A symbol-by-symbol quantization of the source sequence is performed before the transmission and the legitimate receiver in this system happens to reproduce the scalar quantization of the source at the decoder. That is, we are restricting to a subset $\mathcal{B}_n$ of all valid encoder and decoder pairs (f_n, g_n).

Let $\hat{X}_t \sim \hat{p}_0$ be the conditional mean of a uniform quantization of X_t as in Fig. 5.10, i.e. $\hat{X}_t = \mathbb{E}[X_t|\text{Quantization bin of } X_t]$, and $\hat{M}$ be the encoded message to be transmitted. Let the optimal payoff function under such restriction be $\Pi^{\Delta}(R, R_0)$. The following lemma indicates that revealing the causal realization of the original source is equivalent to revealing the causal realization of the quantized version of the source in the eavesdropper's estimate.

Lemma 5.2.

$$X_t - (\hat{M}, \hat{X}^{t-1}) - X^{t-1} \tag{5.135}$$

for all $t = 1, ..., n$.

This can be verified by observing that $X^t - \hat{X}^t - \hat{M}$. Therefore, we can alternatively analyze the performance of the system in Fig. 5.11. This model is defined formally as the following.

Definition 5.10. *The rate-distortion triple* (R, R_0, D) *is achievable if*

$$\mathbb{P}[\hat{Y}^n \neq \hat{X}^n] \to_n 0, \tag{5.136}$$

and

$$\liminf_{n\to\infty} \sup_{(f_n,g_n)\in\mathcal{B}_n} \min_{\{P_{\hat{Z}_t|\hat{M}\hat{X}^{t-1}}\}_{t=1}^n} \mathbb{E}\left[\frac{1}{n}\sum_{t=1}^{n}(\hat{Z}_t - \hat{X}_t)^2\right] \geq D. \tag{5.137}$$

Lemma 5.3.

$$X_t - \hat{X}_t - (\hat{M}, \hat{X}^{t-1}) \tag{5.138}$$

for all $t = 1, ..., n$.

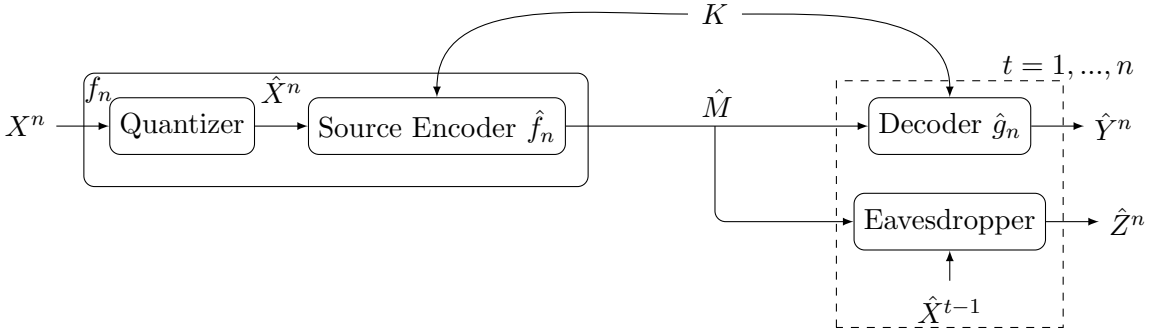

Figure 5.11: An alternative model in which quantization is performed before lossless compression.

Now by applying Corollary 5.4, we have that (R, R_0, D) is achievable iff

$$D \leq D_{\hat{p}_0}(R, R_0) \triangleq \max_{P_{\hat{U}|\hat{X}}\in\mathcal{Q}} \min_{\hat{z}(\hat{u})} \mathbb{E}[(\hat{z}(\hat{U}) - \hat{X})^2], \tag{5.139}$$

where $\hat{X} \sim \hat{p}_0$ and

$$\mathcal{Q} = \{P_{\hat{U}|\hat{X}} : R \geq H(\hat{X}), R_0 \geq H(\hat{X}|\hat{U})\}. \tag{5.140}$$

If we fix (R, R_0) and suppose $P_{\hat{U}|\hat{X}} \in \mathcal{Q}$ is the corresponding distribution that achieves $D_{\hat{p}_0}(R, R_0)$,

$$\mathcal{Z}_n \triangleq \{P_{Z_t|\hat{M}X^{t-1}}\}_{t=1}^n, \tag{5.141}$$

$$\hat{\mathcal{Z}}_n \triangleq \{P_{\hat{Z}_t|\hat{M}\hat{X}^{t-1}}\}_{t=1}^n, \tag{5.142}$$

then we have the following inequalities:

$$\begin{aligned}
& \sigma_0^2 \Pi^{\Delta}(R, R_0) \\
= & \lim_{n\to\infty} \sup_{\mathcal{B}_n} \min_{\mathcal{Z}_n} \frac{1}{n} \sum_{t=1}^n \mathbb{E}[(Z_t - X_t)^2] - \mathbb{E}[(X_t - \hat{Y}_t)^2] && (5.143)\\
= & \lim_{n\to\infty} \sup_{\mathcal{B}_n} \min_{\hat{\mathcal{Z}}_n} \frac{1}{n} \sum_{t=1}^n \mathbb{E}[(\hat{Z}_t - X_t)^2] - \mathbb{E}[(X_t - \hat{Y}_t)^2] && (5.144)\\
= & \lim_{n\to\infty} \sup_{\mathcal{B}_n} \min_{\hat{\mathcal{Z}}_n} \frac{1}{n} \sum_{t=1}^n \mathbb{E}[(\hat{Z}_t - \hat{X}_t)^2] + \mathbb{E}[(\hat{X}_t - X_t)^2] \\
& + 2\mathbb{E}\left[\mathbb{E}[(\hat{Z}_t - \hat{X}_t)(\hat{X}_t - X_t)|\hat{X}_t]\right] - \mathbb{E}[(X_t - \hat{Y}_t)^2] && (5.145)\\
= & \lim_{n\to\infty} \sup_{\mathcal{B}_n} \min_{\hat{\mathcal{Z}}_n} \frac{1}{n} \sum_{t=1}^n \mathbb{E}[(\hat{Z}_t - \hat{X}_t)^2] + \frac{1}{n} \sum_{t=1}^n \mathbb{E}[(\hat{X}_t - X_t)^2] - \mathbb{E}[(X_t - \hat{Y}_t)^2] && (5.146)\\
= & D_{\hat{p}_0}(R, R_0). && (5.147)
\end{aligned}$$

Here, (5.143) follows by definition of $\Pi^{\Delta}(R, R_0)$; (5.144) follows from Lemma 5.2; (5.145) follows from law of total expectation; (5.146) follows from Lemma 5.3; and (5.147) follows by Definition 5.10. Summarizing the analysis in this section, we have the following theorem.

Theorem 5.10. $\Pi^{\Delta}(R, R_0) = \frac{1}{\sigma_0^2} D_{\hat{p}_0}(R, R_0)$.

$D_{\hat{p}_0}(R, R_0)$ can be calculated as a linear program (LP).

Numerical Result

We compare the Gaussian quantization scheme with the jointly Gaussian scheme. Even though in Gaussian quantization, we gave only an analytical lower bound on the payoff as a function of the rates as $R \to \infty$, here we propose a numerical scheme that can evaluate the achievable secrecy rate-payoff for arbitary R and R_0. The choice of the random variable Y is the same and $U \triangleq n \mod N$, where N is some positive integer. Intuitively, U is a coarser quantizer of X. Here we greedily obtain an achievable lower bound by sequentially solving for the optimal T that satisfies $R \geq I(X;Y)$ and the optimal N that satisfies $R_0 \geq I(X;Y|U)$. The payoff of the optimal scheme for $R_0 \geq 1$ bit is also computed for low R_0 for comparison. These results are shown in Fig. 5.12, which shows that the Gaussian quantization choice outperforms the jointly Gaussian choice in the payoff as a function of R_0 for a fixed R. The quantization upper bound is numerically obtained by solving the LP. Note that even though Theorem 5.10 gives a tight bound, the implementation of LP requires that the eavesdropper's reconstruction fall in the same quantization alphabet.

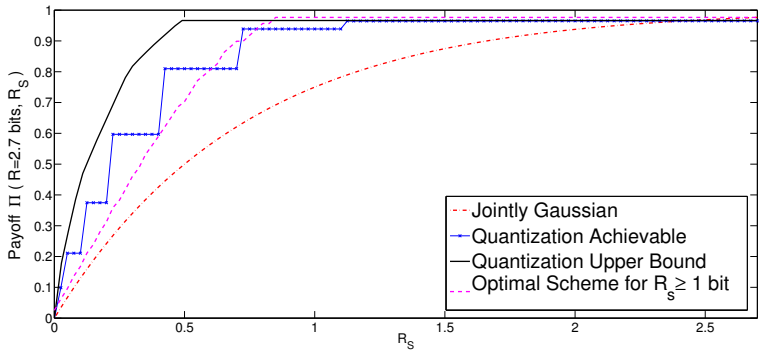

Figure 5.12: Payoff as a function of key rate R_s for fixed $R = 2.7$ bits.

5.5 Summary

In this chapter, we have considered three main rate-distortion based secrecy settings: the naive formulation with shared secret key, the naive formulation with side information at the decoders, and the stronger formulation with causal source disclosure.

For the naive formulation with shared secret key, the problem has been solved completely: a secret key of a positive rate is necessary and sufficient to force the maximum possible distortion to the eavesdropper.

For the naive formulation with side information at decoders, we have obtained an inner and an outer bound. The results show that even if the legitimate receiver has a weaker side information, a positive distortion can still be enforced to the eavesdropper with a proper encoding. Although exact bounds have been obtained for several special cases, the outer bound for arbitrarily correlated side information is not tight, which suggests an interesting direction for future work.

For the stronger formulation with causal source disclosure, the general result is complete. Its relation to equivocation has been discussed and it has been proved mathematically that equivocation is a special case of the rate-distortion approach. Two examples of common sources and distortion metrics, binary source under Hamming distortion and Gaussian source under squared error distortion, have been studied in detail.

Chapter 6

Source-Channel Security in the Noisy Wiretap Channel

6.1 Introduction

Unlike the point-to-point communication system, separating the encodings of source compression and channel coding is in general not optimal in a multi-terminal setting. Building upon the secrecy models proposed in Chapter 5, we extend them to joint source-channel settings by allowing noisy channels.

In this chapter, we start by considering operationally separate source-channel coding in the context of secrecy. It turns out for the naive secrecy formulation, operationally separate source-channel coding is optimal. However, under the strong formulation, where the source is causally disclosed to the eavesdropper during decoding, separation does not hold. This motivates us to explore more efficient ways of conducting source-channel coding. Recent work [8] on hybrid coding provides a new approach for joint source-channel coding. Furthermore, the analysis of hybrid coding aligns nicely with the likelihood encoder.

6.2 Operational Separate Source-Channel Security

6.2.1 Naive Formulation

Problem Setup

A source node has an independent and i.i.d. sequence S^k that it intends to transmit over a memoryless broadcast channel $P_{YZ|X}$ such that a legitimate receiver can reliably decode the source sequence, while keeping the distortion between an eavesdropper and the source as high as possible. The source sequence S^k is mapped to the channel input sequence X^n through a source-channel encoder. Upon receiving Y^n, the legitimate receiver makes an estimate $\hat{S}^k$ of the original source sequence S^k. Similarly, the eavesdropper also makes an estimate $\check{S}^k$ of S^k upon receiving Z^n.

The input of the system is an i.i.d. source sequence S^k distributed according to $\prod_{j=1}^{k} P_S(s_j)$ and the channel is a memoryless broadcast channel $\prod_{t=1}^{n} P_{YZ|X}(y_t, z_t|x_t)$. The source-channel coding model satisfies the following constraints:

- Encoder $f_{k,n} : \mathcal{S}^k \mapsto \mathcal{X}^n$ (possibly stochastic);
- Legitimate receiver decoder $g_{k,n} : \mathcal{Y}^n \mapsto \hat{\mathcal{S}}^k$ (possibly stochastic);
- Eavesdropper decoders $P_{\check{S}^k|Z^n}$;
- Communication rate: $R = \frac{k}{n}$, i.e. symbol/channel use.

The system performance is measured by the error probability at the legitimate receiver and a distortion metric $d(\cdot, \cdot)$ at the eavesdropper as follows:

- Lossless compression for the legitimate receiver:

$$\mathbb{P}\left[S^k \neq \hat{S}^k\right] \to_k 0 \tag{6.1}$$

- Minimum average distortion for the eavesdropper:

$$\liminf_{k\to\infty} \min_{P_{\check{S}^k|Z^n}} \mathbb{E}[d(S^k, \check{S}^k)] \geq D. \tag{6.2}$$

Definition 6.1. *For a given distortion function $d(\cdot,\cdot)$, a rate distortion pair (R, D) is achievable if there exists a sequence of encoder and decoder pairs $(f_{k,n}, g_{k,n})$ such that*

$$\frac{k}{n} = R,$$

$$\mathbb{P}\left[S^k \neq \hat{S}^k\right] \to_k 0,$$

and

$$\liminf_{k\to\infty} \min_{P_{\check{S}^k|Z^n}} \mathbb{E}\left[d(S^k, \check{S}^k)\right] \geq D.$$

Note that the rate-distortion pair (R, D) captures the tradeoff between the communication rate for reliable transmission and the eavesdropper's distortion, which is different from rate-distortion theory in the traditional sense.

The above mathematical formulation is illustrated in Fig. 6.7.

The average distortion achieved by guesses based only on the prior distribution of the source Δ, is defined as

$$\Delta \triangleq \min_a \mathbb{E}[d(S, a)]. \tag{6.3}$$

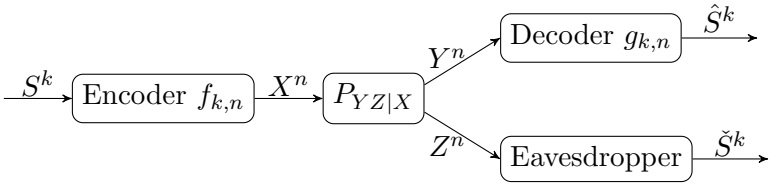

Figure 6.1: Source-channel secrecy system setup at the eavesdropper.

Main Results

We first make some general observations about the communication between the transmitter and the legitimate receiver, as well as the communication between the transmitter and the eavesdropper. If the eavesdropper is not present, the transmitter and receiver can communicate losslessly at any rate lower than $R_0 \triangleq \frac{\max_X I(X;Y)}{H(S)}$ because separate source-channel coding is optimal for point-to-point communication. Ideally, we want to force maximum

average distortion Δ upon the eavesdropper. But higher distortion to the eavesdropper may come at the price of a lower communication rate to the legitimate receiver.

As for physical layer secrecy of a memoryless broadcast channel, the result for transmitting two messages, one confidential and one public, from Csiszár and Körner [30] has been known for many decades. In their work, weak secrecy was considered. This result was strengthened in [36] by considering strong secrecy. The same rate region was obtained in [36], however the metric for secrecy is stronger. In our work, the source-channel coding schemes we propose operationally separate source and channel coding that requires dividing the bit sequence produced by source coding into two messages which are then processed by the channel coding. The channel coding part functions in a way that is similar to [30] or [36], except that the public message in those works is not required to be decoded in our case, and we refer to that message as the "non-confidential" message.

We now state the rate-distortion result for general source-channel coding with an i.i.d. source sequence and a discrete memoryless broadcast channel $P_{YZ|X}$. In the following theorem, we will see that the source sequence can be delivered almost losslessly to the legitimate receiver at a rate arbitarily close to R_0 while the distortion to the eavesdropper is kept at Δ, as long as the secrecy capacity is positive.

Theorem 6.1. *For an i.i.d. source sequence S^k and memoryless broadcast channel $P_{YZ|X}$, if there exists $W - X - YZ$ such that $I(W;Y) - I(W;Z) > 0$, then (R, D) is achievable if and only if*

$$R < \frac{\max_X I(X;Y)}{H(S)}, \tag{6.4}$$

$$D \leq \Delta, \tag{6.5}$$

where Δ was defined in (6.3)*.*

Remark: The requirement $I(W;Y) - I(W;Z) > 0$ implies the existence of a secure channel with a positive rate, i.e. the eavesdropper's channel is not less noisy than the intended receiver's channel. So instead of demanding a high secure transmission rate with perfect secrecy to accommodate the description of the source, we need only to ensure the

existence of a secure channel with positive rate. This will suffice to ensure that the eavesdropper's distortion is maximal.

The converse is straightforward. Each of the inequalities (6.4) and (6.5) is true individually for any channel and source, (6.4) by channel capacity coupled by optimality of source-channel separation, and (6.5) by definition.

Achievability

The idea for achievability is to operationally separate the source and channel coding (see Fig. 6.2). The source encoder compresses the source and splits the resulting message into a confidential message and a non-confidential message. A channel encoder is concatenated digitally with the source encoder so that the channel delivers both the confidential and non-confidential messages reliably to the legitimate receiver and keeps the confidential message secret from the eavesdropper, as in [30]. The overall source-channel coding rate will have the following form: $R = \frac{k}{n} = \frac{k}{\log|\mathcal{M}|} \cdot \frac{\log|\mathcal{M}|}{n} = \frac{R_{ch}}{R_{src}}$, where $|\mathcal{M}|$ is the total cardinality of the confidential and the non-confidential messages; R_{ch} and R_{src} are the channel coding and source coding rates, respectively.

Let us look at two models that will help us establish the platform for showing the achievability of Theorem 6.1.

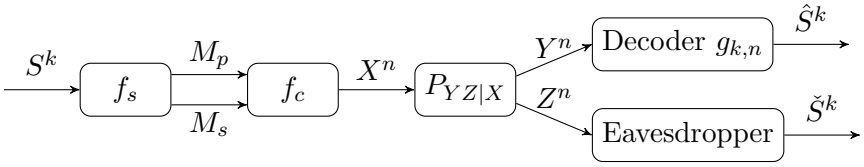

Figure 6.2: Operationally separate source-channel coding: the confidential and non-confidential messages satisfy $M_s \in [1 : 2^{kR'_s} = 2^{nR_s}]$ and $M_p \in [1 : 2^{kR'_p} = 2^{nR_p}]$.

A. Channel Coding and Strong Secrecy

Consider a memoryless broadcast channel $P_{YZ|X}$ and a communication system with a confidential message M_s and a non-confidential message M_p that must allow the intended receiver to decode both M_s and M_p while keeping the eavesdropper from learning anything about M_s. Problems like this were first studied by Csiszár and Körner [30] in 1978, as an extension of Wyner's work in [7]. However, their model and our model differ in that

the second receiver in their setting is required to decode the public message M_p. The mathematical formulation and result of our channel model is stated below. We focus on the message pairs (M_s, M_p) whose distribution satisfies the following:

$$P_{M_s|M_p=m_p}(m_s) \quad = \quad 2^{-nR_s} \tag{6.6}$$

for all (m_s, m_p). Later we will show that a source encoder can always prepare the input messages to the channel in this form.

Definition 6.2. *An (R_s, R_p, n) channel code consists of a channel encoder f_c (possibly stochastic) and a channel decoder g_c such that*

$$f_c : \mathcal{M}_s \times \mathcal{M}_p \mapsto \mathcal{X}^n$$

and

$$g_c : \mathcal{Y}^n \mapsto \mathcal{M}_s \times \mathcal{M}_p$$

where $|\mathcal{M}_s| = 2^{nR_s}$ and $|\mathcal{M}_p| = 2^{nR_p}$.

Definition 6.3. *The rate pair (R_s, R_p) is achievable under **weak secrecy** if for all (M_s, M_p) satisfying (6.6), there exists a sequence of (R_s, R_p, n) channel codes such that*

$$\mathbb{P}\left[(M_s, M_p) \neq (\hat{M}_s, \hat{M}_p)\right] \to_n 0 \tag{6.7}$$

and

$$\frac{1}{n} I(M_s; Z^n | M_p) \to_n 0. \tag{6.8}$$

Note that because the eavesdropper may completely or partially decode M_p, the secrecy requirement is modified accordingly to consider $I(M_s; Z^n|M_p)$ instead of $I(M_s; Z^n)$. To guarantee true secrecy of M_s, we want to make sure that even if M_p is given to the eavesdropper, there is no information leakage of M_s, because $I(M_s; Z^n|M_p) = I(M_s; Z^n M_p)$ if M_s and M_p are independent.

Theorem 6.2. *A rate pair (R_s, R_p) is achievable under weak secrecy if*

$$R_s \leq I(W;Y|V) - I(W;Z|V), \tag{6.9}$$

$$R_p \leq I(V;Y) \tag{6.10}$$

for some $V - W - X - YZ$.

The proof is given in Appendix 6.5.5. Let us denote the above region as $\mathcal{R}$. We now strengthen the result by considering strong secrecy introduced in [37]. Later we will use strong secrecy to connect the operationally separate source and channel encoders.

Definition 6.4. *The rate pair (R_s, R_p) is achievable under* ***strong secrecy*** *if for all (M_s, M_p) satisfying* (6.6)*, there exists a sequence of (R_s, R_p, n) channel codes such that*

$$\mathbb{P}[(M_p, M_s) \neq (\hat{M}_s, \hat{M}_p)] \to_n 0 \tag{6.11}$$

and

$$I(M_s; Z^n|M_p) \to_n 0. \tag{6.12}$$

In general, weak secrecy does not necessarily imply that strong secrecy is also achievable; however, in this particular setting we have the following claim:

Theorem 6.3. *A rate pair (R_s, R_p) achievable under weak secrecy is also achievable under strong secrecy.*

The following two lemmas will assist the proof of Theorem 6.3 by providing a sufficient condition for satisfying the secrecy constraint $I(M_s; Z^n|M_p) \to_n 0$.

Lemma 6.1. *If*

$$\left\| P_{Z^n|M_p=m_p} P_{M_s|M_p=m_p} - P_{Z^n M_s|M_p=m_p} \right\|_{TV} \leq \epsilon \leq \frac{1}{2}, \tag{6.13}$$

then

$$I(M_s; Z^n | M_p = m_p) \leq -\epsilon \log \frac{\epsilon}{|\mathcal{M}_s|}. \tag{6.14}$$

The proof of Lemma 6.1 is provided in Appendix 6.5.1.

Lemma 6.2. *If for every (m_s, m_p), there exists a measure θ_{m_p} on $\mathcal{Z}^n$ such that*

$$\left\| P_{Z^n | M_p = m_p M_s = m_s} - \theta_{m_p} \right\|_{TV} \leq \epsilon_n \tag{6.15}$$

then

$$I(M_s; Z^n | M_p) \to_n 0 \tag{6.16}$$

where $\epsilon_n = 2^{-n\beta}$ for some $\beta > 0$.

A proof of Lemma 6.2 is given in Appendix 6.5.2.

If there exist channel codes such that $\mathbb{P}\left[(M_s, M_p) \neq (\hat{M}_s, \hat{M}_p)\right] \to_n 0$ and measure θ_{m_p} for all (m_s, m_p) such that $||P_{Z^n | M_p = m_p M_s = m_s} - \theta_{m_p}||_{TV} \leq \epsilon_n$, then Theorem 6.3 follows immediately. The existence of such a code and measure is assured by the same codebook construction and choice of measure as in [36].

B. Source Coding

Here we consider a source coding model in which the transmitter has an i.i.d. source sequence S^k. A source encoder is needed to prepare S^k by encoding it into a pair of messages (M_s, M_p) that satisfies $P_{M_s | M_p = m_p}(m_s) = 2^{-kR'_s} = 2^{-nR_s}$. Note that this condition is enforced only for the purpose of channel coding so that the messages generated by the source encoder satisfy (6.6) to be a valid channel input.

Definition 6.5. *An (R'_s, R'_p, k) source code consists of an encoder f_s and a decoder g_s such that*

$$f_s : \mathcal{S}^k \mapsto \mathcal{M}_s \times \mathcal{M}_p$$

$$g_s : \mathcal{M}_s \times \mathcal{M}_p \mapsto \mathcal{S}^k$$

where $|\mathcal{M}_s| = 2^{kR'_s}$ *and* $|\mathcal{M}_p| = 2^{kR'_p}$.

Definition 6.6. *A rate distortion triple* (R'_s, R'_p, D) *is achievable under a given distortion measure* $d(\cdot,\cdot)$ *if there exists a sequence of* (R'_s, R'_p, k) *source codes such that*

$$\mathbb{P}\left[S^k \neq g_s(f_s(S^k))\right] \to_k 0 \tag{6.17}$$

and the message pair generated by the source encoder satisfies $P_{M_s|M_p=m_p}(m_s) = 2^{-kR'_s}$ *and for all* $P_{Z^n|M_sM_p}$ *such that* $I(M_s; Z^n|M_p) \to_n 0$

$$\liminf_{k\to\infty} \min_{\check{s}^k(z^n)} \mathbb{E}\left[d(S^k, \check{s}^k(Z^n))\right] \geq D. \tag{6.18}$$

Theorem 6.4. (R'_s, R'_p, D) *is achievable if*

$$R'_s > 0, \tag{6.19}$$

$$R'_s + R'_p > H(S), \tag{6.20}$$

and

$$D \leq \Delta. \tag{6.21}$$

The general idea for achievability is to consider the ϵ-typical S^k sequences and partition them into bins of equal size so that each bin contains sequences of the same type. The identity M_p of the bin is revealed to all parties, but the identity M_s of each sequence inside a bin is perfectly protected.[1] Each such partition is treated as a codebook. It was shown in [3] that, for the noiseless case in which the eavesdropper is given m_p instead of z^n, the distortion averaged over all such codebooks achieves the maximum average distortion Δ as $k \to \infty$ and therefore there must exist one partition that achieves Δ. In order to transition

[1]Strictly speaking, the source encoder may violate the condition (6.6) on $(k+1)^{|\mathcal{S}|}$ number of bins, because $(k+1)^{|\mathcal{S}|}$ is an upper bound on the number of types of a sequence of length k. However, this is just a very small (polynomial in k) number of bins compared with the total number (roughly $2^{kH(S)}$) of bins. Therefore, for this small portion of "bad" bins that violate (6.6), we can just let the source encoder declare an error on the confidential message M_s and construct a dummy M_s uniformly given the bin index m_p. This will contribute only an ϵ factor to the error probability.

from the result in [3] to our claim in Theorem 6.4, we only need to show

$$\min_{\check{s}^k(z^n)} \mathbb{E}\left[d^k(S^k, \check{s}^k(Z^n))\right] \geq \min_{\check{s}^k(m_p)} \mathbb{E}\left[d^k(S^k, \check{s}^k(M_p))\right] - 2\delta'(\epsilon). \tag{6.22}$$

Proof. First, observe that

$$\min_{\check{s}^k(\cdot)} \mathbb{E}\left[d^k(S^k, \check{s}^k(\cdot))\right] = \frac{1}{k}\sum_{i=1}^{k} \min_{\check{s}(i,\cdot)} \mathbb{E}\left[d(S_i, \check{s}(i,\cdot))\right]. \tag{6.23}$$

Next, we claim the channel output sequence z^n does not provide the eavesdropper anything more than m_p and therefore

$$\min_{\check{s}(i,z^n)} \mathbb{E}\left[\frac{1}{k}\sum_{i=1}^{k} d(S_i, \check{s}(i, Z^n))\right] \geq \min_{\check{s}(i,m_p)} \mathbb{E}\left[\frac{1}{k}\sum_{i=1}^{k} d(S_i, \check{s}(i, M_p))\right] - 2\delta'(\epsilon). \tag{6.24}$$

The analysis is similar to that in [38], but for the sake of clarity, we present the complete proof of (6.24) in Appendix 6.5.3. Here strong secrecy comes into play. It is also pointed out within the proof in Appendix 6.5.3 that $I(M_s; Z^n|M_p) \to_n 0$ is needed.

Finally, combining (6.24) with (6.23) gives us the desired result. □

C. Achievability Proof of Theorem 6.1

We are now ready to complete the achievability proof of Theorem 6.1 using Theorems 6.2 and Theorem 6.4 by concatenating the channel encoder with the source encoder.

Fix $\nu \geq \epsilon > 0$. Fix P_S. Let ${R_s}' = 2\nu$, ${R_p}' = H(S) - \nu$ and ${R}' = {R_s}' + {R_p}'$. We apply the same codebook construction and encoding scheme as in B by partioning the ϵ-typical S^k sequences into $2^{k{R_p}'}$ bins and inside each bin we have $2^{k{R_s}'}$ sequences so that $\mathbb{P}[S^k \neq g_s(f_s(S^k))] \leq \epsilon$. Recall that all the sequences inside one bin are of the same type, so it is guaranteed that

$$P_{M_s|M_p=m_p}(m_s) = \frac{1}{|\mathcal{M}_s|} = \frac{1}{2^{kR'_s}} \tag{6.25}$$

for all m_p, m_s, which implies $I(M_s; M_p) = 0$.

Let R_s and R_p be the channel rates. R_p is seen as a function of R_s on the boundary of the region given in Theorem 6.2 and this is denoted by $R_p(R_s)$. Suppose $\max_{(R_s,R_p)\in\mathcal{R}} R_s > 0$, i.e. there exists $W-X-YZ$ such that $I(W;Y)-I(W;Z)>0$ (justified in Appendix 6.5.4). $R_p(R_s)$ is continuous and non-increasing. Thus, R_p achieves its maximum at $R_s = 0$, which would be the channel capacity $\max_X I(X;Y)$ of $P_{Y|X}$ for reliable transmission. By the continuity of $R_p(R_s)$, $(R_s, R_p) = (2\nu\frac{k}{n}, R_p(0)-\delta(\nu))$ is achievable under strong secrecy, i.e. $\mathbb{P}[(M_s, M_p) \neq (\hat{M}_s, \hat{M}_p)] \leq \epsilon$ and $I(M_s; Z^n|M_p) \leq \epsilon$, where $\delta(\nu)\to 0$ as $\nu \to 0$.

From the above good channel code under strong secrecy we have $P_{Z^n|M_sM_p}$ such that $I(M_s; Z^n|M_p) \to_n 0$. Therefore, we can apply Theorem 6.4 to achieve

$$\min_{\check{s}^k(z^n)} \mathbb{E}\left[d^k(S^k, \check{s}^k(Z^n))\right] \to_k D. \tag{6.26}$$

The error probability is bounded by the sum of the error probabilities from the source coding and channel coding parts, i.e. $\mathbb{P}\left[S^k \neq \hat{S}^k\right] < 2\epsilon$. Finally, we verify the total transmission rate to complete the proof:

$$\begin{aligned} R &= \frac{k}{n} = \frac{R_s + R_p}{R_s' + R_p'} && (6.27)\\ &= \frac{R_p(0) - \delta(\nu) + 2R\nu}{H(S)+\nu} && (6.28)\\ &\geq \frac{R_p(0)-\delta(\nu)}{H(S)+\nu} && (6.29)\\ &\xrightarrow{\nu\to 0} \frac{\max_X I(X;Y)}{H(S)}. && (6.30) \end{aligned}$$

6.2.2 With Causal Source Disclosure at the Eavesdropper

Problem Setup

Now we consider a variation of the problem considered in Section 6.2.1. We want to determine conditions for a joint source-channel secrecy system that guarantee reliable communication to the legitimate receiver while a certain level of distortion can be forced on the eavesdropper. The input of the system is an i.i.d. source sequence S^k distributed according to $\prod_{j=1}^k P_S(s_j)$ and the channel is a memoryless broadcast channel $\prod_{t=1}^n P_{YZ|X}(y_t, z_t|x_t)$.

The source realization is causally disclosed to the eavesdropper during decoding. The source-channel coding model satisfies the following constraints:

- Encoder $f_{k,n} : \mathcal{S}^k \mapsto \mathcal{X}^n$ (possibly stochastic);
- Legitimate receiver decoder $g_{k,n} : \mathcal{Y}^n \mapsto \hat{\mathcal{S}}^k$ (possibly stochastic);
- Eavesdropper decoders $\{P_{\check{S}_j|Z^n S^{j-1}}\}_{j=1}^k$;
- Communication reate: $R = \frac{k}{n}$, i.e. symbol/channel use.

The system performance is measured by the error probability at the legitimate receiver and a distortion metric $d(\cdot, \cdot)$ as follows:

- Lossless compression for the legitimate receiver:

$$\mathbb{P}\left[S^k \neq \hat{S}^k\right] \to_k 0 \tag{6.31}$$

- Minimum average distortion for the eavesdropper:

$$\liminf_{k\to\infty} \min_{\{P_{\check{S}_j|Z^n S^{j-1}}\}_{j=1}^k} \mathbb{E}[d(S^k, \check{S}^k)] \geq D.$$

Definition 6.7. *For a given distortion function $d(\cdot, \cdot)$, a rate distortion pair (R, D) is achievable if there exists a sequence of encoder/decoder pairs $f_{k,n}$ and $g_{k,n}$ such that*

$$\frac{k}{n} = R,$$

$$\mathbb{P}\left[S^k \neq \hat{S}^k\right] \to_k 0,$$

and

$$\liminf_{k\to\infty} \min_{\{P_{\check{S}_j|Z^n S^{j-1}}\}_{j=1}^k} \mathbb{E}[d(S^k, \check{S}^k)] \geq D.$$

The above mathematical formulation is illustrated in Fig. 6.7.

Main Results

We give an inner bound and an outer bound stated as follows.

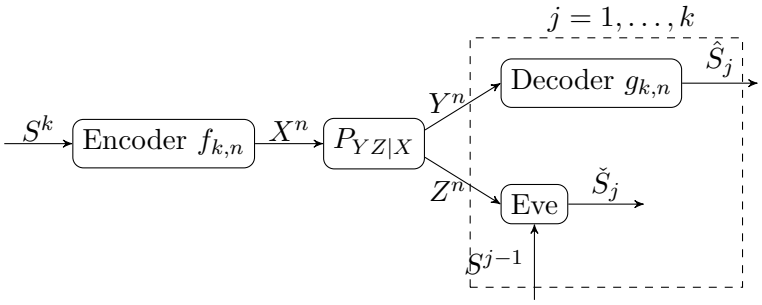

Figure 6.3: Joint source-channel secrecy system setup with causal source disclosure at the eavesdropper

Theorem 6.5. *A rate distortion pair* (R, D) *is achievable if*

$$R \leq \min\left(\frac{I(V;Y)}{I(S;U)}, \frac{I(W;Y|V) - I(W;Z|V)}{H(S|U)}\right), \tag{6.32}$$

$$D \leq \min_{\phi(u)} \mathbb{E}\left[d(S, \phi(U))\right] \tag{6.33}$$

for some distribution $P_S P_{U|S} P_V P_{W|V} P_{X|W} P_{YZ|X}$.

Theorem 6.6. *If a rate distortion pair* (R, D) *is achievable, then*

$$R \leq \min\left(\frac{I(W;Y)}{H(S)}, \frac{I(W;Y|V) - I(W;Z|V)}{H(S|U)}\right) \tag{6.34}$$

$$D \leq \min_{\phi(u)} \mathbb{E}\left[d(S, \phi(U))\right] \tag{6.35}$$

for some distribution $P_S P_{U|S} P_V P_{W|V} P_{X|W} P_{YZ|X}$.

Achievability

The method for showing the achievability part given in Theorem 6.5 follows the same procedures as the case without causal source disclosure. Again, we divide the problem into a channel coding part and a source coding part. However, the major difference here is that unlike the case without causal disclosure, only weak secrecy from the channel coding part is required.

A. Channel Coding and Weak Secrecy

The input to the encoder is again a pair of messages (M_p, M_s) destined for the channel

decoder, with M_p representing a public message and M_s a secure message. The channel decoder outputs the pair $(\hat{M}_p, \hat{M}_s)$. We allow the channel encoder to use private randomization. We use the same definition given in Definition 6.2 for a channel code.

We make a further technical requirement (cf. [30]) for the channel input. That is, conditioned on M_p, M_s is almost uniform. To be precise, we require

$$\max_{m_p, m_s, m_s'} \frac{\mathbb{P}[M_s = m_s | M_p = m_p]}{\mathbb{P}[M_s = m_s' | M_p = m_p]} \leq 2^{n\delta_n} \tag{6.36}$$

to hold for some $\delta_n \to_n 0$. The source encoder we employ will produce message pairs (M_p, M_s) that satisfy this condition, regardless of the source distribution.

Definition 6.8. *The rate pair (R_s, R_p) is achievable under weak secrecy if for all (M_s, M_p) satisfying* (6.36)*, there exists a sequence of (R_s, R_p, n) channel codes such that*

$$\mathbb{P}\left[(M_s, M_p) \neq (\hat{M}_s, \hat{M}_p)\right] \to_n 0 \tag{6.37}$$

and

$$\frac{1}{n} I(M_s; Z^n M_p) \to_n 0. \tag{6.38}$$

Theorem 6.7. *The pair (R_p, R_s) is achievable if*

$$\begin{aligned} R_p &\leq I(V;Y) && (6.39)\\ R_s &\leq I(W;Y|V) - I(W;Z|V) && (6.40) \end{aligned}$$

for some $P_V P_{W|V} P_{X|W} P_{YZ|X}$.

The proof of Theorem 6.7 is provided in Appendix 6.5.5.

B. Source Coding

Under the same definition for a source code given in Definition 6.5, we make the following modifications.

Definition 6.9. *A rate distortion triple* (R'_s, R'_p, D) *is achievable under a given distortion measure* $d(\cdot,\cdot)$ *if there exists a sequence of* (R'_s, R'_p, k) *source codes such that*

$$\mathbb{P}\left[S^k \neq g_s(f_s(S^k))\right] \to_k 0 \tag{6.41}$$

and the message pair generated by the source encoder satisfies (6.36) *for every* n*, and for all* $P_{Z^n|M_sM_p}$ *such that* $\frac{1}{n}I(M_s; Z^n|M_p) \to_n 0$

$$\liminf_{k\to\infty} \min_{\{\check{s}_j(z^n, s^{j-1})\}_{j=1}^k} \mathbb{E}\left[\frac{1}{k}\sum_{j=1}^k d(S_j, \check{s}_j(Z^n, S^{j-1}))\right] \geq D. \tag{6.42}$$

Theorem 6.8. *A rate distortion triple* (R'_s, R'_p, D) *is achievable if*

$$\begin{aligned} R'_p &> I(S;U) && (6.43)\\ R'_s &> H(S|U) && (6.44)\\ D &\leq \min_{\phi(u)} \mathbb{E}[d(S, \phi(U))] && (6.45) \end{aligned}$$

for some $P_S P_{U|S}$*.*

The main idea in the proof of Theorem 6.8 is to use the public message to specify a sequence U^k that is correlated with S^k, and use the secure message to encode the supplement that is needed to fully specify the source sequence. The source encoder is defined in such a way that, conditioned on the public message M_p, the adversary views the source as if it were generated by passing U^k through a memoryless channel $P_{S|U}$. With this perspective, the past S^{j-1} will no longer help the adversary; the eavesdropper's best strategy is to choose a function that maps U_j to $\check{S}_j$.

Below is a crucial lemma that shows how the weak secrecy provided by a good channel code is used in analyzing the payoff. The result of this lemma is that we can view the eavesdropper as having full knowledge of M_p and S^{j-1} and no knowledge of M_s, which fulfills our goal of creating a secure channel and a public channel. We show that, from the eavesdropper's perspective, knowledge of (Z^n, S^{j-1}) is no more helpful than (M_p, S^{j-1}) in easing the distortion.

Lemma 6.3. *If $P_{M_pM_s}$ satisfies* (6.36) *for every n, and $P_{Z^n|M_pM_s}$ such that $\frac{1}{n}I(M_s;Z^n|M_p)\to_n 0$, then for all $\epsilon>0$,*

$$\begin{aligned}&\min_{\check{s}(j,s^{j-1},z^n)}\mathbb{E}\left[\frac{1}{k}\sum_{j=1}^{k}d\left(S_j,\check{s}(j,S^{j-1},Z^n)\right)\right]\\ \geq\ &\min_{\check{s}(j,s^{j-1},m_p)}\mathbb{E}\left[\frac{1}{k}\sum_{j=1}^{k}d\left(S_j,\check{s}(j,S^{j-1},M_p)\right)\right]-\delta(\epsilon)\end{aligned}\tag{6.46}$$

for sufficiently large n, where $\delta(\epsilon)\to 0$ as $\epsilon\to 0$.

The proof is provided in Appendix 6.5.6.

Now we have all the elements to prove Theorem 6.8. Again, we use the likelihood encoder together with the analysis using the soft-covering lemmas.

Proof. We follow the convention of using P to denote the system induced distribution and replace the single-letter distributions with $\overline{P}$. Note that $P_S=\overline{P}_S$.

Fix a distribution $\overline{P}_{SU}=\overline{P}_S\overline{P}_{U|S}$ satisfying

$$\min_{\phi(u)}\mathbb{E}[d(S,\phi(U))]\geq D\tag{6.47}$$

and fix rates R_p', R_s' such that

$$R_p' > I(S;U),\tag{6.48}$$

$$R_s' > H(S|U)\tag{6.49}$$

under $\overline{P}_{SU}$.

The distribution induced by the encoder and decoder is

$$\mathbf{P}_{S^kM_pM_s\hat{S}^k}(s^k,m_p,m_s,\hat{s}^k)=P_{S^k}(s^k)\mathbf{P}_{LE}(m_p,m_s|s^k)\mathbf{P}_D(\hat{s}^k|m_p,m_s)\tag{6.50}$$

where $\mathbf{P}_{LE}(m_p,m_s|s^k)$ is the source encoder; and $\mathbf{P}_D(\hat{s}^k|m_p,m_s)$ is the decoder that reconstructs the source sequence.

Codebook generation: We independently generate $2^{kR'_p}$ sequences in $\mathcal{U}^k$ according to $\prod_{j=1}^k \overline{P}_U(u_j)$ and index them by $m_p \in [1 : 2^{kR'_p}]$. We use $\mathcal{C}_U^{(k)}$ to denote this random codebook. For each $m_p \in [1 : 2^{kR'_p}]$, we independently generate $2^{kR'_s}$ sequences in $\mathcal{S}^k$ according to $\prod_{j=1}^k \overline{P}_{S|U}(\hat{s}_j|u_j(m_p))$ and index them by $(m_p, m_s) \in [1 : 2^{kR'_p}] \times [1 : 2^{kR'_s}]$. We use $\mathcal{C}_{\hat{S}}^{(k)}(m_p)$ to denote this random codebook.

Encoder: The encoder $\mathbf{P}_{LE}(m_p, m_s|s^k)$ is the likelihood encoder that chooses (m_p, m_s) stochastically according to the following probability:

$$\mathbf{P}_{LE}(m|s^k) = \frac{\mathcal{L}(m|s^k)}{\sum_{\bar{m}\in\mathcal{M}} \mathcal{L}(\bar{m}|s^k)} \tag{6.51}$$

where $m = (m_p, m_s)$, $\mathcal{M} = [1 : 2^{kR'_p}] \times [1 : 2^{kR'_s}]$, and

$$\begin{aligned} \mathcal{L}(m|s^k) &= \mathbb{1}\{s^k = \hat{s}^k(m)\} && (6.52)\\ &= \overline{P}_{S^k|S^k}(s^k|\hat{s}^k(m)). && (6.53) \end{aligned}$$

Decoder: The decoder is a codeword lookup decoder that simply reproduces $\hat{S}^k(m_p, m_s)$.

Analysis: We first examine the error probability at the legitimate receiver by looking at the system induced distribution $\mathbf{P}$, and auxiliary distributions $\mathbf{Q}$ and $\mathbf{Q}'$. Then we analyze the distortion at the eavesdropper through another auxiliary distribution $\tilde{\mathbf{Q}}$.

On the legitimate receiver side, let us define an idealized distribution $\mathbf{Q}$ that is of the form in the soft-covering lemma, i.e. as if the codeword $\hat{S}^k$ is passed through a noise-free memoryless channel. Formally, the idealized distribution $\mathbf{Q}$ is defined as

$$\begin{aligned} & \mathbf{Q}_{S^k M_p M_s U^k \hat{S}^k}(s^k, m_p, m_s, u^k, \hat{s}^k) \\ = \;& Q_{M_p M_s}(m_p, m_s)\mathbf{Q}_{U^k|M_p}(u^k|m_p)\mathbf{Q}_{\hat{S}^k|M_p M_s}(\hat{s}^k|m_p, m_s)\mathbf{Q}_{S^k|\hat{S}^k}(s^k|\hat{s}^k) && (6.54)\\ = \;& \frac{1}{2^{k(R'_p+R'_s)}}\mathbb{1}\{u^k = U^k(m_p)\}\mathbb{1}\{\hat{s}^k = \hat{S}^k(m_p, m_s)\}\mathbb{1}\{s^k = \hat{s}^k\} && (6.55) \end{aligned}$$

Note that the encoder $\mathbf{P}_{LE}$ and decoder $\mathbf{P}_D$ satisfy

$$\mathbf{P}_{LE}(m_p, m_s|s^k) = \mathbf{Q}_{M_pM_S|S^k}(m_p, m_s|s^k) \tag{6.56}$$

$$\mathbf{P}_D(\hat{s}^k|m_p, m_s) = \mathbf{Q}_{\hat{S}^k|M_pM_S}(\hat{s}^k|m_p, m_s). \tag{6.57}$$

Define another auxiliary distribution $\mathbf{Q}'$ on a subset of the variables as

$$\mathbf{Q}'_{M_pU^kS^k}(m_p, u^k, s^k) = \frac{1}{2^{kR'_p}} \mathbb{1}\{u^k = U^k(m_p)\} \prod_{j=1}^{k} \overline{P}_{S|U}(s_j|U_j(m_p)). \tag{6.58}$$

Since $R_s > I(S;\hat{S}|U) = H(S|U)$ under $\overline{P}$, applying the superposition soft-covering Lemma 2.2, we have for some $\gamma_2 > 0$

$$\mathbb{E}_{\mathcal{C}^{(k)}}\left[\left\|\mathbf{Q}_{M_pS^k} - \mathbf{Q}'_{M_pS^k}\right\|_{TV}\right] \leq e^{-\gamma_2 k}. \tag{6.59}$$

Also since $R_p > I(U;S)$, applying the basic soft-covering lemma (Lemma 2.1), we have for some $\gamma_1 > 0$

$$\mathbb{E}_{\mathcal{C}^{(k)}}\left[\left\|P_{S^k} - \mathbf{Q}'_{S^k}\right\|_{TV}\right] \leq e^{-\gamma_1 k}. \tag{6.60}$$

Using Property 2.1(c), (6.60) and (6.59), we obtain

$$\mathbb{E}_{\mathcal{C}^{(k)}}\left[\|P_{S^k} - \mathbf{Q}_{S^k}\|_{TV}\right] \leq e^{-\gamma_1 k} + e^{-\gamma_2 k} \triangleq \epsilon_{3k}. \tag{6.61}$$

By Property 2.1(e), (6.56) and (6.57), we have

$$\mathbb{E}_{\mathcal{C}^{(k)}}\left[\left\|\mathbf{P}_{S^kM_pM_s\hat{S}^k} - \mathbf{Q}_{S^kM_pM_s\hat{S}^k}\right\|_{TV}\right] \leq \epsilon_{3k}. \tag{6.62}$$

By construction of the idealized distribution $\mathbf{Q}$,

$$\mathbb{P}_{\mathbf{Q}}\left[\hat{S}^k \neq S^k\right] = 0. \tag{6.63}$$

Using Property 2.1(b), we obtain

$$\mathbb{P}_{\mathbf{P}}\left[\hat{S}^k \neq S^k\right] \leq \epsilon_{3k}. \tag{6.64}$$

On the eavesdropper's side, we denote the marginals of $\mathbf{Q}'$ by $\tilde{\mathbf{Q}}^{(j)}$ as follows:

$$\tilde{\mathbf{Q}}^{(j)}_{M_p U^k S^j}(m_p, u^k, s^j) = \mathbf{Q}'_{M_p U^k S^j}(m_p, u^k, s^j) \tag{6.65}$$

where $\mathbf{Q}'$ is defined in (6.58).

Therefore, by Property 2.1(c), (6.60) and (6.62), we obtain

$$\mathbb{E}_{\mathcal{C}^{(k)}}\left[\left\|\mathbf{P}_{M_p S^j} - \tilde{\mathbf{Q}}^{(j)}_{M_p S^j}\right\|_{TV}\right] \leq 2e^{-\gamma_1 k} + e^{-\gamma_2 k}. \tag{6.66}$$

Note that under $\tilde{\mathbf{Q}}^{(j)}$, we have the Markov relation

$$S_j - U_j(M_p) - M_p S^{j-1}. \tag{6.67}$$

Also note that, since $R'_p > 0$, invoking the soft-covering lemma gives us

$$\mathbb{E}_{\mathcal{C}^{(k)}}\left[\left\|\tilde{\mathbf{Q}}^{(j)}_{U_j(M_p)} - \overline{P}_U\right\|_{TV}\right] \leq e^{-\gamma_3 k} \tag{6.68}$$

for some $\gamma_3 > 0$.

Combining (6.64), (6.66) and (6.68) and the random coding argument, there exists a codebook under which

$$\mathbb{P}_P\left[\hat{S}^k \neq S^k\right] \leq \epsilon_k \tag{6.69}$$

$$\sum_{j=1}^{k}\left\|P_{M_p S^j} - \tilde{Q}^{(j)}_{M_p S^j}\right\|_{TV} \leq \epsilon_k \tag{6.70}$$

$$\sum_{j=1}^{k}\left\|\tilde{Q}_{u_j(M_p)} - \overline{P}_U\right\|_{TV} \leq \epsilon_k \tag{6.71}$$

where $\epsilon_k = \epsilon_{3k} + k(2e^{-\gamma_1 k} + e^{-\gamma_2 k}) + ke^{-\gamma_3 k}$.

Finally, the distortion at the eavesdropper can be lower bounded by the following steps:

$$\begin{aligned}
& \min_{\{\check{s}_j(z^n,s^{j-1})\}_{j=1}^k} \mathbb{E}\left[\frac{1}{k}\sum_{j=1}^k d\left(S_j, \check{s}_j(Z^n, S^{j-1})\right)\right] \\
\geq & \min_{\{\check{s}_j(m_p,s^{j-1})\}_{j=1}^k} \mathbb{E}\left[\frac{1}{k}\sum_{j=1}^k d\left(S_j, \check{s}_j(M_p, S^{j-1})\right)\right] - \delta_k & (6.72)\\
= & \frac{1}{k}\sum_{j=1}^k \min_{\check{s}_j(m_p,s^{j-1})} \mathbb{E}_P\left[d\left(S_j, \check{s}_j(M_p, S^{j-1})\right)\right] - \delta_k & (6.73)\\
\geq & \frac{1}{k}\sum_{j=1}^k \min_{\check{s}_j(m_p,s^{j-1})} \mathbb{E}_{\tilde{Q}^{(j)}}\left[d\left(S_j, \check{s}_j(M_p, S^{j-1})\right)\right] - \delta_k - \epsilon_k d_{max} & (6.74)\\
= & \frac{1}{k}\sum_{j=1}^k \min_{\phi(u)} \mathbb{E}_{\tilde{Q}^{(j)}}\left[d\left(S_j, \phi\left(u_j(M_p)\right)\right)\right] - \delta_k - \epsilon_k d_{max} & (6.75)\\
\geq & \frac{1}{k}\sum_{j=1}^k \min_{\phi(u)} \mathbb{E}_{\overline{P}}\left[d\left(S, \phi(U)\right)\right] - \delta_k - 2\epsilon_k d_{max} & (6.76)
\end{aligned}$$

where $\delta_k \to_k 0$. Eq. (6.72) follows from Lemma 6.3; (6.74) follows from (6.70); (6.75) follows from the Markov relation (6.67); and (6.76) follows from (6.71) and the fact that

$$\tilde{Q}^{(j)}_{S_j|U_j}(s_j|u_j) = \overline{P}_{S|U}(s_j|u_j). \tag{6.77}$$

□

Now we return to proving Theorem 6.5 by rate matching from the channel coding Theorem 6.7 and source coding Theorem 6.8, we can achieve

$$\begin{aligned}
R & \leq \min\left(\frac{I(V;Y)}{I(S;U)}, \frac{I(W;Y|V) - I(W;Z|V)}{H(S|U)}\right), & (6.78)\\
D & \leq \min_{\phi(u)} \mathbb{E}\left[d(S, \phi(U))\right] & (6.79)
\end{aligned}$$

for some distribution $\overline{P}_S \overline{P}_{U|S} \overline{P}_V \overline{P}_{W|V} \overline{P}_{X|W} \overline{P}_{YZ|X}$.

An Improved Inner Bound

We can strengthen the above distortion analysis by taking into account the equivocation of the public message. For source blocklength k, the equivocation of the public message

vanishes at a certain time k' due to the eavesdropper's ongoing accumulation of past source symbols $S^{k'-1}$. Before time k', the payoff is Δ, because the eavesdropper does not have enough information to decode the public message. After time k', the payoff is as given in (6.79). The transition happens at

$$k' = \frac{[I(V;Y) - I(V;Z)]^+}{I(S;U)R} k. \tag{6.80}$$

This gives us an improved achievable region stated in the following theorem.

Theorem 6.9. *A rate distortion pair (R, D) is achievable if*

$$\begin{aligned} R &\leq \min\left(\frac{I(V;Y)}{I(S;U)}, \frac{I(W;Y|V) - I(W;Z|V)}{H(S|U)}\right), && (6.81)\\ D &\leq \frac{\alpha}{R} \cdot \Delta + \left(1 - \frac{\alpha}{R}\right) \cdot \min_{\phi(u)} \mathbb{E}\left[d(S, \phi(U))\right] && (6.82) \end{aligned}$$

for some distribution $P_S P_{U|S} P_V P_{W|V} P_{X|W} P_{YZ|X}$, where $\alpha = \frac{[I(V;Y)-I(V;Z)]^+}{I(S;U)}$.

Outer Bound

Now we give the proof for Theorem 6.6.

Proof. Introduce random variables $Q_1 \sim Unif[1:k]$, $Q_2 \sim Unif[1:n]$, independent of (S^k, X^n, Y^n, Z^n). Define the random variables

$$U = (Z^n, S^{Q_1-1}, Q_1) \tag{6.83}$$

$$V = (Y^{Q_2-1}, Z_{Q_2+1}^n, Q_2) \tag{6.84}$$

$$W = (V, S^k) \tag{6.85}$$

$$S = S_{Q_1} \tag{6.86}$$

$$(X, Y, Z) = (X_{Q_2}, Y_{Q_2}, Z_{Q_2}). \tag{6.87}$$

It can be verified that $V - W - X - YZ$. First, we have

$$
\begin{aligned}
& H(S|U) \\
= \;& H(S_{Q_1}|Z^n S^{Q_1-1} Q_1) && (6.88)\\
= \;& \frac{1}{k}\sum_{j=1}^{k} H(S_j|Z^n S^{j-1}) && (6.89)\\
= \;& \frac{1}{k} H(S^k|Z^n) && (6.90)\\
= \;& \frac{1}{k} H(S^k) - \frac{1}{k} I(S^k; Z^n) && (6.91)\\
= \;& \frac{1}{k} I(S^k; Y^n) - \frac{1}{k} I(S^k; Z^n) + \frac{1}{k} H(S^k|Y^n) && (6.92)\\
\leq \;& \frac{1}{k} I(S^k; Y^n) - \frac{1}{k} I(S^k; Z^n) + \epsilon_k && (6.93)\\
= \;& \frac{1}{R}\left(\frac{1}{n} I(S^k; Y^n) - \frac{1}{n} I(S^k; Z^n)\right) + \epsilon_k && (6.94)\\
= \;& \frac{1}{R}\left(\frac{1}{n}\sum_{i=1}^{n} I(S^k; Y_i|Y^{i-1} Z_{i+1}^n) - \frac{1}{n}\sum_{i=1}^{n} I(S^k; Z_i|Y^{i-1} Z_{i+1}^n)\right) + \epsilon_k && (6.95)\\
= \;& \frac{1}{R}\left(I(W; Y|V) - I(W; Z|V)\right) + \epsilon_k && (6.96)
\end{aligned}
$$

where (6.93) follows from Fano's inequality and $\epsilon_k \to_k 0$. The step (6.95) uses the Csiszár sum identity. Next, we have

$$
\begin{aligned}
& H(S) \\
= \;& \frac{1}{R}\frac{1}{n}\left(I(S^k; Y^n) + H(S^k|Y^n)\right) && (6.97)\\
\leq \;& \frac{1}{R}\frac{1}{n}\sum_{i=1}^{n} I(S^k; Y^i|Y^{i-1}) + \epsilon_k && (6.98)\\
\leq \;& \frac{1}{R}\frac{1}{n}\sum_{i=1}^{n} I(S^k Y^{i-1} Z_{i+1}^n; Y^i) + \epsilon_k && (6.99)\\
= \;& \frac{1}{R} I(S^k Y^{Q_2-1} Z_{Q_2+1}^n; Y_{Q_2}; Y_{Q_2}|Q_2) + \epsilon_k && (6.100)\\
\leq \;& \frac{1}{R} I(W; Y) + \epsilon_k. && (6.101)
\end{aligned}
$$

Finally,

$$
\begin{aligned}
D &\leq \min_{\check{s}(j,s^{j-1},z^n)} \mathbb{E}\left[\frac{1}{k}\sum_{j=1}^{k} d\left(S_j, \check{s}(j, S^{j-1}, Z^n)\right)\right] && (6.102)\\
&= \min_{\check{s}(q_1,s^{q_1-1},z^n)} \mathbb{E}\left[d(S_{Q_1}, \check{s}(Q_1, S^{Q_1-1}, Z^n))\right] && (6.103)\\
&= \min_{\phi(u)} \mathbb{E}[d(S, \phi(U))]. && (6.104)
\end{aligned}
$$

□

6.2.3 Binary Symmetric Broadcast Channel and Binary Source

To visualize Theorem 6.1 and Theorem 6.5, we will illustrate the results with a binary symmetric broadcast channel (BSBCC) and binary source under Hamming distortion.

With the above setting, suppose $S_j \sim \text{Bern}(p)$, and the broadcast channel is binary symmetric with crossover probabilities to the intended receiver and the eavesdropper p_1 and p_2, respectively. Assume $p \leq 0.5$ and $p_1 < p_2 < 0.5$. This stochastically degraded channel can be considered physically degraded in capacity calculations because none of the mutual information quantities (or error probabilities) depend on the joint distribution. Let us make the following definitions:

$$
\begin{aligned}
&f(x) \text{ is the linear interpolation of the points}\\
&\quad \left(\log n, \frac{n-1}{n}\right), n = 1, 2, 3, ... && (6.105)\\
&d(x) \triangleq \min(f(x), 1 - \max_s P_S(s)), && (6.106)\\
&h(x) \triangleq x \log \frac{1}{x} + (1-x) \log \frac{1}{1-x}\\
&\quad \text{is the binary entropy function,} && (6.107)\\
&x_1 * x_2 \triangleq x_1 * (1-x_2) + (1-x_1) * x_2\\
&\quad \text{is the binary convolution,} && (6.108)
\end{aligned}
$$

where $P_S(\cdot)$ is the probability mass function of the random variable S. The corresponding rate-distortion regions for the cases without and with causal source disclosure are given in the following corollaries.

Corollary 6.1. *For an i.i.d. Bern(p) source sequence S^k and BSBCC with crossover probabilities p_1 and p_2,* ***without*** *causal source disclosure at the eavesdropper, (R, D) is achievable if and only if*

$$R < \frac{1-h(p_1)}{h(p)}, \tag{6.109}$$

$$D \leq p. \tag{6.110}$$

Corollary 6.2. *For an i.i.d. Bern(p) source sequence S^k and BSBCC with crossover probabilities p_1 and p_2,* ***with*** *causal source disclosure at the eavesdropper, (R, D) is achievable if*

$$R \leq \frac{h(p_2)-h(p_1)}{h(p)}, \tag{6.111}$$

$$D \leq p \tag{6.112}$$

or

$$\frac{h(p_2)-h(p_1)}{h(p)} < R \leq \frac{1-h(p_1)}{h(p)}, \tag{6.113}$$

$$D \leq \alpha' p + (1-\alpha') d\left(\frac{h(\gamma * p_1) - h(\gamma * p_2) - h(p_1) + h(p_2)}{R}\right) \tag{6.114}$$

where $\gamma \in [0, 0.5]$ solves $h(\gamma * p_2) = 1 - h(p_1) + h(p_2) - Rh(p)$ and $\alpha' = \frac{h(\gamma * p_2) - h(\gamma * p_1)}{1 - h(\gamma * p_1)}$.

These corollaries result directly from applying Theorem 6.1 and Theorem 6.5, respectively. The region given in Corollary 6.2 is calculated in a similar fashion as the region given by Theorem 7 of [38]. A numerical example with $p = 0.3$, $p_1 = 0.1$ and $p_2 = 0.2$ is plotted in Fig.6.4.

6.2.4 Applications to Multimode Fiber

Single mode fiber systems are believed to have reached their capacity limits. In particular, techniques such as wavelength-division multiplexing (WDM) and polarization-division multiplexing (PDM) have been heavily exploited in the past few years, leaving little room for further improvement in capacity [39]. Space-division multiplexing (SDM) is a promis-

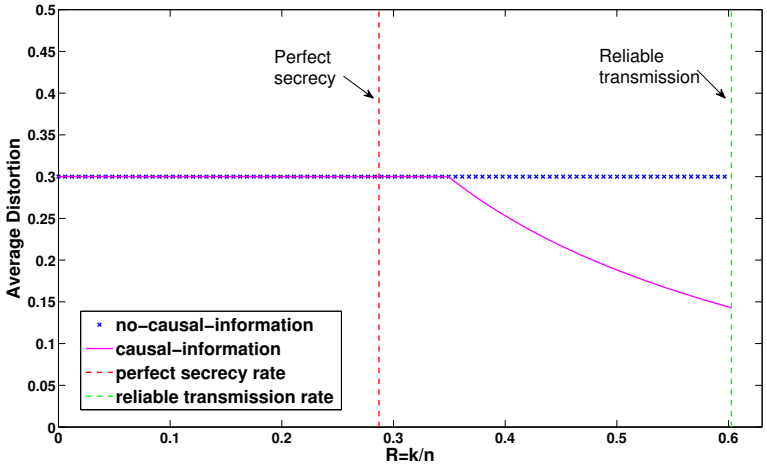

Figure 6.4: Achievable distortion-rate curves. On the horizontal axis is the symbol/channel use source-channel coding rate and on the vertical axis is the average Hamming distortion.

ing solution for meeting the growing capacity demands of optical communication networks. One way of realizing SDM is via the use of multimode fiber (MMF). While multimode transmission provides greater capacity, the security of such systems can be an issue because a wiretapper can eavesdrop upon MMF communication by simply bending the fiber [40]. MMF is a multiple-input-multiple-output (MIMO) system [39] that captures the charateristics of crosstalk among different modes. The secrecy capacity of a Gaussian MIMO broadcast channel was studied in [41], but the result cannot be applied directly to MMF because the channel is not the same. The secrecy capacity of this channel was studied in [40] where it is shown that the channel conditions required for perfect secrecy are quite demanding.

MMF Channel Model

An M-mode MMF is modeled as a memoryless MIMO channel as shown in Fig. 6.5 with input X an M-dimensional complex vector. Here M is a positive integer.

Unlike wireless MIMO which has a total power constraint, MMF channels have the following per mode power constraint averaged over n uses of the channel:

$$\frac{1}{n}\sum_{i=1}^{n}\left|X_i^{(m)}\right|^2 \leq 1 \quad \text{for all modes } m \in [1:M]. \tag{6.115}$$

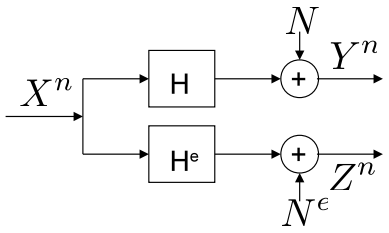

Figure 6.5: MMF channel model

More generally (as in [41]), we will consider a power constraint of the form

$$\frac{1}{n}\sum_{i=1}^{n} X_i X_i^\dagger \quad \preceq \quad Q, \tag{6.116}$$

where $Q \in \{A \in \mathcal{H}^{M\times M} : A \succeq 0, A_{ii} = 1\}$ and $\mathcal{H}$ denotes the set of Hermitian matrices. One element in this set is the identity matrix I (constraint (6.115)). We will focus on the case $Q = I$ for simplicity. A detailed discussion of the MMF channel model can be found in [39].

A. The Legitimate User Communications Model

The channel between the transmitter and the legitimate receiver $P_{Y|X}$ is complex, Gaussian, MIMO, with input $X \in \mathbb{C}^M$ as described above, and output $Y \in \mathbb{C}^M$ given by

$$Y \quad = \quad HX + N, \tag{6.117}$$

where $N \sim \mathcal{CN}(0, \sigma_N^2 I, 0)$ is M-dimensional, uncorrelated, zero-mean, complex, Gaussian noise and H is an $M \times M$ complex matrix. The legitimate receiver's channel matrix H is of the form

$$H \quad = \quad \sqrt{E_0 L}\Psi, \tag{6.118}$$

where $\Psi \in \mathbb{C}^{M\times M}$ is unitary and $E_0 L$ is a constant scalar that measures the average power of the channel. We refer to $E_0 L/\sigma_N^2$ as the SNR of the channel. The matrix Ψ, the unitary factor of the channel H, describes the modal crosstalk [39].

B. The Eavesdropper Communications Model

The channel between the transmitter and the eavesdropper $P_{Z|X}$ is also complex, Gaussian,

MIMO, with input $X \in \mathbb{C}^M$ as described above, and output $Z \in \mathbb{C}^M$ given by

$$Z = H^e X + N^e, \tag{6.119}$$

where $N^e \sim \mathcal{CN}(0, \sigma_{N^e}^2 I, 0)$ is M-dimensional uncorrelated, zero-mean, complex, Gaussian noise, and H^e is an $M \times M$ complex matrix. The eavesdropper's channel matrix H^e is of the form

$$H^e = \sqrt{E_0 L^e}\sqrt{\Phi}\Psi^e, \tag{6.120}$$

where $\Psi^e \in \mathbb{C}^{M\times M}$ is unitary, Φ is diagonal with positive entries, and $E_0 L^e$ is the average power of the eavesdropper's channel. Note that the eavesdropper has a different signal to noise ratio $\text{SNR}^e = E_0 L^e / \sigma_{N^e}^2$. The diagonal component Φ of the channel matrix H^e corresponds to the mode-dependent loss (MDL) as introduced in [39].

Main Results

We now apply the results from Section 6.2.1 and 6.2.2 to the MMF model by finding the rate distortion regions for the MMF model defined in (6.117) and (6.119) under the two scenarios [42] [43]. In this section, as before, we assume the channels are time-invariant. First of all, we will give the achievable rate region under strong secrecy (therefore also under weak secrecy).

Theorem 6.10. *The following rate region for one confidential and one non-confidential message is achievable under strong secrecy for a complex Gaussian channel:*

$$R_s \leq \log \frac{|HKH^\dagger + \sigma_N^2 I|}{|\sigma_N^2 I|} - \log \frac{|H^e K H^{e\dagger} + \sigma_{N^e}^2 I|}{|\sigma_{N^e}^2 I|} \tag{6.121}$$

$$R_p \leq \log \frac{|HQH^\dagger + \sigma_N^2 I|}{|HKH^\dagger + \sigma_N^2 I|} \tag{6.122}$$

for some K and Q, where $0 \preceq K \preceq Q$, $K \in \mathcal{H}^{M\times M}$, Q satisfies the power constraint in (6.116)*, and H and H^e are the channel gain matrices.*

Proof. According to Theorem 6.2 and 6.3,

$$R_s \leq I(W;Y|V) - I(W;Z|V) \tag{6.123}$$

$$R_p \leq I(V;Y) \tag{6.124}$$

for some $V - W - X - YZ$ and $\mathbb{E}[XX^\dagger] \preceq Q$, is an achievable rate pair.

We restrict the channel input X to be a circularly symmetric complex Gaussian vector. Let $V \sim \mathcal{CN}(0, Q-K, 0)$ and $B \sim \mathcal{CN}(0, K, 0)$ such that B and V are independent, and $W = X = V + B$. Therefore, $X \sim \mathcal{CN}(0, Q, 0)$ satisfies the power constraint. Similar to results in [41], the rate pair (R_s, R_p) satisfying inequalities (6.121) and (6.122) can be achieved. □

An immediate corollary follows directly from the above theorem.

Corollary 6.3. *The following rate pairs are achievable under strong secrecy for MMF with channel gains defined in* (6.118) *and* (6.120) *and equal full power allocation $Q = I$:*

$$R_s \leq \log \frac{|SNRK + I|}{|SNR^e \Psi^e K \Psi^{e\dagger} \Phi + I|} \tag{6.125}$$

$$R_p \leq \log \frac{|(SNR+1)I|}{|SNRK + I|} \tag{6.126}$$

for some K where $0 \preceq K \preceq I$, $K \in \mathcal{H}^{M\times M}$, $SNR = E_0 L/\sigma_N^2$ and $SNR^e = E_0 L^e/\sigma_{N^e}^2$.

With the secrecy capacity region of MMF, we can evaluate its rate distortion region (R, D) under the two extreme cases, without and with causal source disclosure at the eavesdropper's decoder respectively. For the case without causal source disclosure, we give a sufficient condition to force maximum average distortion Δ between the transmitter and the eavesdropper. For the case with causal source disclosure, we give an achievable rate-distortion region and look at the particular case of Hamming distortion.

Theorem 6.11. *For an i.i.d source sequence S^k, if*

$$\min_{j\in\{1,\ldots,M\}} \bar{\phi}_j < \frac{SNR}{SNR^e} \tag{6.127}$$

where $\bar{\phi}_j$'s are the diagonal entries of Φ, then the following rate distortion pair (R, D) is achievable ***without*** *causal source disclosure at the eavesdropper:*

$$R < \frac{M \log(SNR+1)}{H(S)} \tag{6.128}$$

$$D \leq \Delta. \tag{6.129}$$

Theorem 6.11 follows from Theorem 6.1 and Corollary 6.3. Note that (6.127) is a sufficient condition for the existence of a secure channel with strictly positive rate from the transmitter to the legitimate receiver. A discussion of this condition is provided in Appendix 6.5.7.

Theorem 6.12. *For an i.i.d. source sequence S^k and Hamming distortion, the following distortion rate curve $D(R)$ is in the achievable region* ***with*** *causal source disclosure at the eavesdropper:*

$$D = d(H(S)), \text{ if } R \leq \frac{R_s^*}{H(S)} \tag{6.130}$$

$$D = \bar{\alpha}(K)\Delta + (1-\bar{\alpha}(K))\, d\left(\frac{R_s(K)}{R}\right), \quad \text{if } \frac{R_s^*}{H(S)} < R \leq \frac{R_p^*}{H(S)} \tag{6.131}$$

where $d(\cdot)$ is as defined in (6.106)*; $\mathcal{K} \triangleq \{K \in \mathcal{H}^{M\times M}, 0 \preceq K \preceq I\}$,*

$$R_s^* = \max_{K' \in \mathcal{K}} \log \frac{|SNRK' + I|}{|SNR^e \sqrt{\Phi}\Psi^e K' \Psi^{e\dagger}\sqrt{\Phi} + I|}, \tag{6.132}$$

$$R_p^* = M \log(SNR+1), \tag{6.133}$$

$$R_s(K) = \log \frac{|SNRK + I|}{|SNR^e \sqrt{\Phi}\Psi^e K \Psi^{e\dagger}\sqrt{\Phi} + I|}, \tag{6.134}$$

$$\bar{\alpha}(K) = \frac{\bar{\beta}(K) - \bar{\gamma}(K)}{\bar{\beta}(K)}, \tag{6.135}$$

$$\bar{\beta}(K) = \log \frac{|(SNR+1)I|}{|SNRK + I|}, \tag{6.136}$$

$$\bar{\gamma}(K) = \log \frac{|SNR^e\Phi + I|}{|SNR^e \sqrt{\Phi}\Psi^e K \Psi^{e\dagger}\sqrt{\Phi} + I|}. \tag{6.137}$$

The result given in Theorem 6.12 can be derived directly from Theorem 6.5 and Corollary 6.3.

Numerical Results

In this section, we present numerical results illustrating achievable rate distortion regions of an MMF under the two information models with a time-invariant channel. Let us consider measuring the eavesdropper's distortion using Hamming distortion and a $Bern(p)$ i.i.d. source sequence. Fig. 3 shows numerical results corresponding to Theorem 6.11 and Theorem 6.12 under equal power allocation. The channels are simulated as a $4-$mode MMF with $\text{SNR} = 20dB$, $\text{SNR}^e = 10dB$, and $\text{MDL} = 20dB$.

In each plot, the vertical line on the right is the maximum reliable transmission rate between the transmitter and the legitimate receiver and the vertical line on the left is the maximum perfect secrecy transmission rate that can be obtained with separate source-channel coding. The horizontal line is the maximum distortion which is also the rate distortion curve from Theorem 6.11 with no causal source disclosure at the eavesdropper. The curve obtained from Theorem 6.12 shows the tradeoff between the transmission rate between the transmitter and the legitimate receiver and the distortion forced on the eavesdropper with causal source disclosure. We see in Fig. 6.6(a), $p = 0.3$, that with our source-channel coding analysis, we gain a free region for maximum distortion, as if under perfect secrecy, (from the left vertical line to the kink) because we effectively use the redundancy of the source. In Fig. 6.6(b) with $p = 0.5$, since there is no redundancy in the source, the distortion curve drops immediately after the maximum perfect secrecy rate. Note that the transmission rates are not considered beyond the right vertical lines because they are above the maximum reliable transmission rates and the legitimate receiver cannot losslesly reconstruct the source sequences.

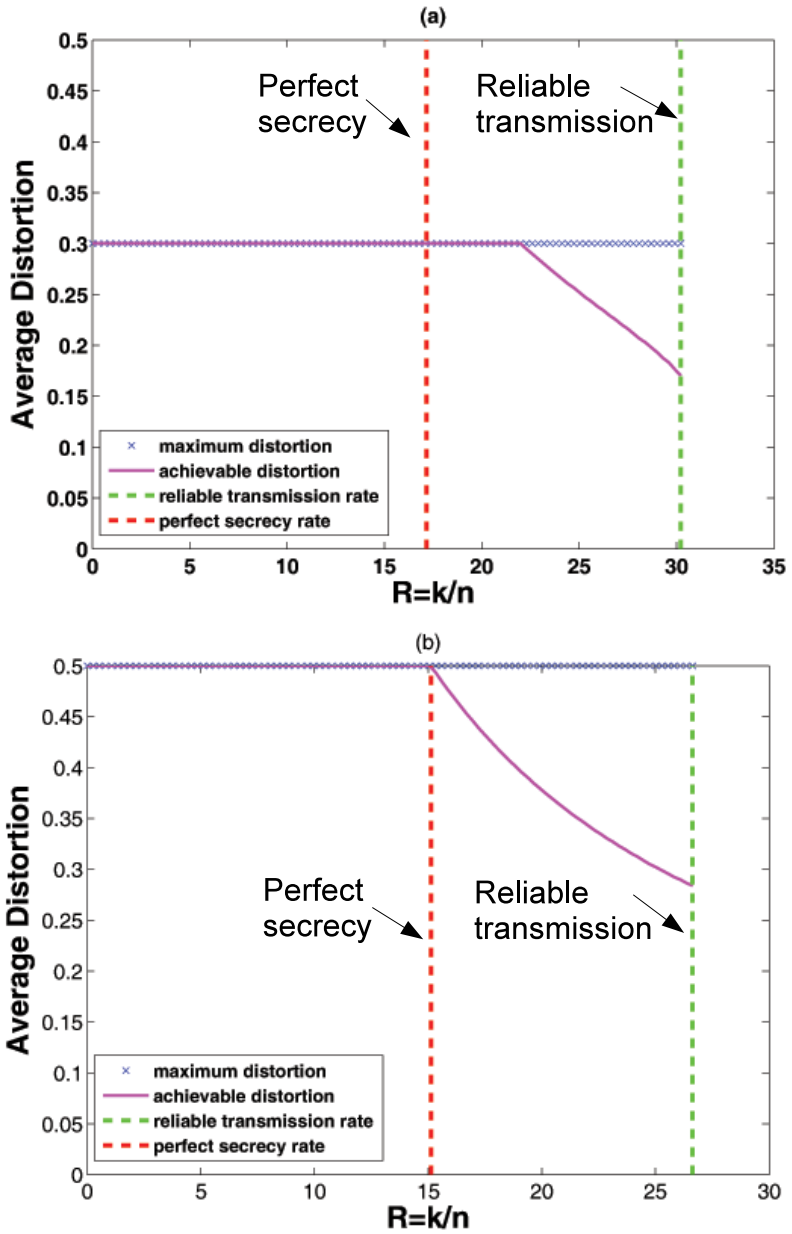

Figure 6.6: Achievable distortion-rate curves. On the left is the $Bern(0.3)$ i.i.d. source case and on the right is the $Bern(0.5)$ i.i.d. source case. On the horizontal axes are the symbol/channel use source-channel coding rate and on the vertical axes are the average Hamming distortions.

6.3 Joint Source-Channel Security

We re-approach the setting considered in Section 6.2.2. Instead of operationally separating the encodings from source compression and channel coding, we use a joint source-channel coding technique – hybrid coding to achieve better secrecy performance. The analysis relies on the likelihood encoder.

6.3.1 Problem Revisit

Although this is a revisit of the problem we have introduced in Section 6.2.2, we make a simplification here by only considering the same blocklength for the source sequence and channel input sequence. Also, we expand the problem to allow lossy reconstruction of the source at the legitimate receiver. For clarity, the problem formulation is restated as follows.

We want to determine conditions for a joint source-channel secrecy system that guarantee reliable communication to the legitimate receiver while a certain level of distortion can be forced to the eavesdropper. The input of the system is an i.i.d. source sequence S^n distributed according to $\prod_{t=1}^{n} P_S(s_t)$ and the channel is a memoryless broadcast channel $\prod_{t=1}^{n} P_{YZ|X}(y_t, z_t|x_t)$. The source realization is causally disclosed to the eavesdropper during decoding. The source-channel coding model satisfies the following constraints:

- Encoder $f_n : \mathcal{S}^n \mapsto \mathcal{X}^n$ (possibly stochastic);
- Legitimate receiver decoder $g_n : \mathcal{Y}^n \mapsto \hat{\mathcal{S}}^n$ (possibly stochastic);
- Eavesdropper decoders $\{P_{\check{S}_t|Z^n S^{t-1}}\}_{t=1}^{n}$.

The system performance is measured by a distortion metric $d(\cdot, \cdot)$ as follows:

- Average distortion for the legitimate receiver:

$$\limsup_{n\to\infty} \mathbb{E}\left[d(S^n, \hat{S}^n)\right] \leq D_b$$

- Minimum average distortion for the eavesdropper:

$$\liminf_{n\to\infty} \min_{\{P_{\check{S}_t|Z^n S^{t-1}}\}_{t=1}^{n}} \mathbb{E}[d(S^n, \check{S}^n)] \geq D_e.$$

Definition 6.10. *A distortion pair (D_b, D_e) is achievable if there exists a sequence of source-channel encoders and decoders (f_n, g_n) such that*

$$\limsup_{n\to\infty} \mathbb{E}[d(S^n, \hat{S}^n)] \leq D_b$$

and

$$\liminf_{n\to\infty} \min_{\{P_{\check{S}_t|Z^n S^{t-1}}\}_{t=1}^n} \mathbb{E}[d(S^n, \check{S}^n)] \geq D_e.$$

The above mathematical formulation is illustrated in Fig. 6.7.

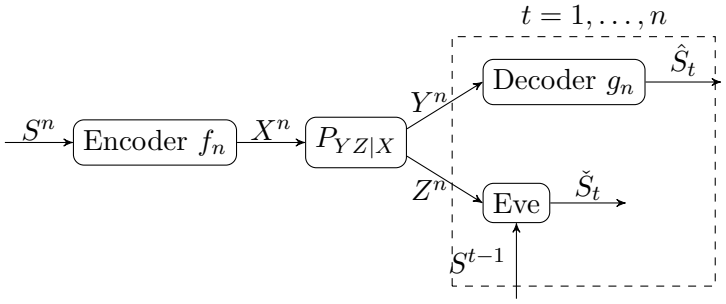

Figure 6.7: Joint source-channel secrecy system setup with causal source disclosure at the eavesdropper.

Scheme O – Operational Separate Source-Channel Coding Scheme

Although only lossless reconstruction of the source is considered in Section 6.2.2, the result can be readily generalized to the case of lossy compression as follows.

Theorem 6.13. *A distortion pair (D_b, D_e) is achievable if*

$$I(S; U_1) < I(U_2; Y) \tag{6.138}$$

$$I(S; \hat{S}|U_1) < I(V_2; Y|U_2) - I(V_2; Z|U_2) \tag{6.139}$$

$$D_b \geq \mathbb{E}\left[d(S, \hat{S})\right] \tag{6.140}$$

$$D_e \leq \eta \min_{a\in\hat{\mathcal{S}}} \mathbb{E}[d(S, a)] + (1-\eta) \min_{\psi(u_1)} \mathbb{E}[d(S, \psi(U_1))] \tag{6.141}$$

for some distribution $P_S P_{\hat{S}|S} P_{U_1|\hat{S}} P_{U_2} P_{V_2|U_2} P_{X|V_2} P_{YZ|X}$*, where*

$$\eta = \frac{[I(U_2;Y) - I(U_2;Z)]^+}{I(S;U_1)}. \tag{6.142}$$

Since the source coding and channel coding parts of the above scheme are almost independent (with some technical details), we refer to it as operationally separate source-channel coding – Scheme O.

6.3.2 Secure Hybrid Coding

Hybrid coding is a joint source-channel coding technique [8] where 1) the encoder generates a digital codeword from the analog source and selects the channel input as a symbol-by-symbol function of the codeword and the source; and 2) the decoder recovers the digital codeword from the analog channel output and selects the source estimate as a symbol-by-symbol function of the codeword and the channel output. It has been shown that this joint source-channel code is optimal at least for point-to-point communication. For the purpose of achieving secrecy, the symbol-by-symbol mapping (deterministic) to the channel input in the encoding stage is modified to be stochastic.

Scheme I – Basic Hybrid Coding

An achievability region using basic secure hybrid coding is given in the following theorem.

Theorem 6.14. *A distortion pair* (D_b, D_e) *is achievable if*

$$\begin{aligned} I(U;S) &< I(U;Y) && (6.143)\\ D_b &\geq \mathbb{E}[d(S,\phi(U,Y))] && (6.144)\\ D_e &\leq \beta \min_{\psi_0(z)} \mathbb{E}[d(S,\psi_0(Z))] + (1-\beta) \min_{\psi_1(u,z)} \mathbb{E}[d(S,\psi_1(U,Z))] && (6.145) \end{aligned}$$

where

$$\beta = \min\left\{ \frac{[I(U;Y) - I(U;Z)]^+}{I(S;U|Z)}, 1 \right\} \tag{6.146}$$

for some distribution $P_S P_{U|S} P_{X|SU} P_{YZ|X}$ *and function* $\phi(\cdot,\cdot)$.

The proof of Theorem 6.14 to be presented next uses hybrid coding combined with the likelihood encoder. The general idea is that under our choice of the encoder and decoder, the system induced distribution $\mathbf{P}$ is close in total variation distance to an idealized distribution $\mathbf{Q}$ by our construction. Therefore, by the properties of total variation, we can approximate the performance of the system under $\mathbf{P}$ by that under $\mathbf{Q}$.

Proof. The source and channel distributions $\overline{P}_S \triangleq P_S$ and $\overline{P}_{YZ|X} \triangleq P_{YZ|X}$ are given by the problem statement. Fix a joint distribution $\overline{P}_S \overline{P}_{U|S} \overline{P}_{X|SU} \overline{P}_{YZ|X}$. Again, P is reserved for the system induced distribution.

Codebook generation: We independently generate 2^{nR} sequences in $\mathcal{U}^n$ according to $\prod_{t=1}^n \overline{P}_U(u_t)$ and index them by $m \in [1 : 2^{nR}]$. We use $\mathcal{C}^{(n)}$ to denote this random codebook.

Encoder: Encoding has two steps. In the first step, a likelihood encoder $\mathbf{P}_{LE}(m|s^n)$ is used. It chooses M stochastically according to the following distribution:

$$\mathbf{P}_{LE}(m|s^n) = \frac{\mathcal{L}(m|s^n)}{\sum_{\bar{m}\in\mathcal{M}} \mathcal{L}(\bar{m}|s^n)} \tag{6.147}$$

where $\mathcal{M} = [1 : 2^{nR}]$, and

$$\mathcal{L}(m|s^n) = \overline{P}_{S^n|U^n}(s^n|u^n(m)). \tag{6.148}$$

In the second step, the encoder produces the channel input through a random transformation given by $\prod_{t=1}^n \overline{P}_{X|SU}(x_t|s_t, U_t(m))$.

Decoder: Decoding also has two steps. In the first step, let $\mathbf{P}_{D1}(\hat{m}|y^n)$ be a good channel decoder with respect to the codebook $\{u^n(a)\}_a$ and memoryless channel $\overline{P}_{Y|X}$. In the second step, fix a function $\phi(\cdot,\cdot)$. Define $\phi^n(u^n, y^n)$ as the concatenation $\{\phi(u_t, y_t)\}_{t=1}^n$ and set the decoder $\mathbf{P}_{D2}$ to be the deterministic function

$$\mathbf{P}_{D2}(\hat{s}^n|\hat{m}, y^n) \triangleq \mathbb{1}\{\hat{s}^n = \phi^n(u^n(\hat{m}), y^n)\}. \tag{6.149}$$

Analysis: We can write the system induced distribution in the following form:

$$\begin{aligned}
& \mathbf{P}_{MU^nS^nX^nY^nZ^n\hat{M}\hat{S}^n}(m, u^n, s^n, x^n, y^n, z^n, \hat{m}, \hat{s}^n) \\
\triangleq\ & \overline{P}_{S^n}(s^n)\mathbf{P}_{LE}(m|s^n)\mathbb{1}\{u^n = U^n(m)\}\prod_{t=1}^{n}\overline{P}_{X|SU}(x_t|s_t, u_t)\prod_{t=1}^{n}\overline{P}_{YZ|X}(y_t, z_t|x_t) \\
& \mathbf{P}_{D1}(\hat{m}|y^n)\mathbf{P}_{D2}(\hat{s}^n|\hat{m}, y^n). \qquad (6.150)
\end{aligned}$$

An idealized distribution $\mathbf{Q}$ is defined as follows to help with the analysis:

$$\begin{aligned}
& \mathbf{Q}_{MU^nS^nX^nY^nZ^n}(m, u^n, s^n, x^n, y^n, z^n) \\
\triangleq\ & \frac{1}{2^{nR}}\mathbb{1}\{u^n = U^n(m)\}\prod_{t=1}^{n}\overline{P}_{S|U}(s_t|u_t) \\
& \prod_{t=1}^{n}\overline{P}_{X|SU}(x_t|s_t, u_t)\prod_{t=1}^{n}\overline{P}_{YZ|X}(y_t, z_t|x_t). \qquad (6.151)
\end{aligned}$$

A. Distortion analysis at the legitimate receiver: Applying Lemma 2.1 and properties of total variation distance from Property 2.1, we have

$$\mathbb{E}_{\mathcal{C}^{(n)}}\left[\|\mathbf{P} - \mathbf{Q}\|_{TV}\right] \leq e^{-\gamma_1 n} \triangleq \epsilon_{1n} \to_n 0, \qquad (6.152)$$

where the distributions are over the random variables $MU^nS^nX^nY^nZ^n$, if

$$R > I(U; S). \qquad (6.153)$$

Using the same steps as was given in Section 4.3.2 for the analysis of Wyner-Ziv setting, it can be verified that the following holds:

$$\begin{aligned}
& \mathbb{E}_{\mathcal{C}^{(n)}}\left[\mathbb{E}_{\mathbf{P}}\left[d(S^n, \hat{S}^n)\right]\right] \\
\leq\ & \mathbb{E}_{\overline{P}}[d(S, \phi(U, Y))] + d_{max}(\epsilon_{1n} + \delta_n), \qquad (6.154)
\end{aligned}$$

if

$$R \leq I(U; Y), \qquad (6.155)$$

where $\delta_n \to_n 0$.

B. Distortion analysis at the eavesdropper: On the eavesdropper side, we make the following observation. Define an auxiliary distribution

$$\check{\mathbf{Q}}^{(i)}_{S^iZ^n}(s^i, z^n) \triangleq \prod_{t=1}^{n} \overline{P}_Z(z_t) \prod_{j=1}^{i} \overline{P}_{S|Z}(s_j|z_j) \tag{6.156}$$

and under $\check{\mathbf{Q}}^{(i)}$,

$$S_i - Z_i - Z^n S^{i-1}. \tag{6.157}$$

Recall that

$$\begin{aligned} & \mathbf{Q}_{MZ^nS^i}(m, z^n, s^i) \\ = \; & \frac{1}{2^{nR}} \prod_{t=1}^{n} \overline{P}_{Z|U}(z_t|U_t(m)) \prod_{j=1}^{i} \overline{P}_{S|ZU}(s_j|z_j, U_j(m)) \end{aligned} \tag{6.158}$$

and under $\mathbf{Q}$, the following Markov relation holds:

$$S_i - Z_i U_i(M) - Z^n S^{i-1} M. \tag{6.159}$$

Apply Lemma 2.2 with the following symbol assignment:

$$(U, V, X, Z) \leftarrow (\varnothing, U, Z, S) \tag{6.160}$$

where on the left are the variables from Lemma 2.2 and on the right are the variables from our analysis. We obtain

$$\mathbb{E}_{\mathcal{C}^{(n)}} \left[\left\| \check{\mathbf{Q}}^{(i)}_{Z^nS^i} - \mathbf{Q}_{Z^nS^i} \right\|_{TV} \right] \le e^{-\gamma_2 n} \tag{6.161}$$

for any $\beta < \frac{R - I(U;Z)}{I(S;U|Z)}$, $i \le \beta n$, where $\gamma_2 > 0$ depends on the gap $\frac{R-I(U;Z)}{I(S;U|Z)} - \beta$. Consequently,

$$\mathbb{E}_{\mathcal{C}^{(n)}} \left[\left\| \check{\mathbf{Q}}^{(i)}_{Z^nS^i} - \mathbf{P}_{Z^nS^i} \right\|_{TV} \right] \le e^{-\gamma_1 n} + e^{-\gamma_2 n}. \tag{6.162}$$

Also note that since $R > 0$, we have

$$\mathbb{E}_{\mathcal{C}^{(n)}}\left[\left\|\mathbf{Q}_{u_i(M)} - \overline{P}_U\right\|_{TV}\right] \leq e^{-\gamma_3 n}. \tag{6.163}$$

Therefore, combining (6.152), (6.338), (6.340), and (6.154), there exists a codebook $\mathcal{C}^{(n)}$ such that

$$\sum_{i=1}^{n} \|P_{MZ^nS^i} - Q_{MZ^nS^i}\|_{TV} \leq \epsilon_n \tag{6.164}$$

$$\sum_{i=1}^{n} \left\|P_{Z^nS^i} - \check{Q}^{(i)}_{Z^nS^i}\right\|_{TV} \leq \epsilon_n \tag{6.165}$$

$$\sum_{i=1}^{n} \left\|Q_{u_i(M)} - \overline{P}_U\right\|_{TV} \leq \epsilon_n \tag{6.166}$$

$$\mathbb{E}_P\left[d(S^n, \hat{S}^n)\right] \leq \mathbb{E}_{\overline{P}}\left[d(S^n, \hat{S}^n)\right] + \epsilon_n \tag{6.167}$$

where $\epsilon_n = n\left(2e^{-n\gamma_1} + e^{-n\gamma_2} + e^{-n\gamma_3}\right) + d_{max}(\epsilon_{1n} + \delta_n) \to_n 0$.

Now we can bound the distortion at the eavesdropper by breaking it down into two sections. The distortion after the time transition βn can be lower bounded by the following:

$$\begin{aligned}
&\min_{\{\psi_{1_i}(s^{i-1}, z^n)\}} \mathbb{E}_P\left[\frac{1}{k}\sum_{i=j}^{n} d(S_i, \psi_{1i}(S^{i-1}, Z^n))\right] \\
= \;& \frac{1}{k}\sum_{i=j}^{n} \min_{\psi_{1_i}(s^{i-1}, z^n)} \mathbb{E}_P\left[d(S_i, \psi_{1i}(S^{i-1}, Z^n))\right] && (6.168)\\
\geq \;& \frac{1}{k}\sum_{i=1}^{n} \min_{\psi_{1_i}(s^{i-1}, z^n, m)} \mathbb{E}_P\left[d(S_i, \psi_{1i}(S^{i-1}, Z^n, M))\right] && (6.169)\\
\geq \;& \frac{1}{k}\sum_{i=j}^{n} \min_{\psi_{1_i}(s^{i-1}, z^n, m)} \mathbb{E}_Q\left[d(S_i, \psi_{1i}(S^{i-1}, Z^n, M))\right] - \epsilon_n d_{max} && (6.170)\\
= \;& \frac{1}{k}\sum_{i=j}^{n} \min_{\psi_1(u,z)} \mathbb{E}_Q\left[d(S_i, \psi_1(u_i(M), Z_i))\right] - \epsilon_n d_{max} && (6.171)\\
\geq \;& \frac{1}{k}\sum_{i=j}^{n} \min_{\psi_1(u,z)} \mathbb{E}_{\overline{P}}\left[d(S, \psi_1(U, Z))\right] - 2\epsilon_n d_{max} && (6.172)
\end{aligned}$$

$$j = \beta n + 1 \tag{6.173}$$

$$k = (1-\beta)n \tag{6.174}$$

where (6.170) is from (6.164), (6.171) uses the Markov relation given in (6.159), and (6.172) uses (6.166) and the fact that

$$Q_{Z_i S_i|U_i}(z_i, s_i|u_i) = \overline{P}_{Z|U}(z_i|u_i)\overline{P}_{S|ZU}(s_i|z_i, u_i). \tag{6.175}$$

Similarly, we can bound the distortion before the time transition βn by the following steps:

$$\begin{aligned}
&\min_{\{\psi_{0i}(s^{i-1},z^n)\}_i} \mathbb{E}_P\left[\frac{1}{k}\sum_{i=1}^{k} d(S_i, \psi_{0i}(S^{i-1}, Z^n))\right] \\
&= \frac{1}{k}\sum_{i=1}^{k} \min_{\psi_{0i}(s^{i-1},z^n)} \mathbb{E}_P\left[d(S_i, \psi_{0i}(S^{i-1}, Z^n))\right] && (6.176)\\
&\geq \frac{1}{k}\sum_{i=1}^{k} \min_{\psi_{0i}(s^{i-1},z^n)} \mathbb{E}_{\check{Q}^{(i)}}\left[d(S_i, \psi_{0i}(S^{i-1}, Z^n))\right] - \epsilon_n d_{max} && (6.177)\\
&= \frac{1}{k}\sum_{i=1}^{k} \min_{\psi_0(z)} \mathbb{E}_{\check{Q}^{(i)}}\left[d(S_i, \psi_0(Z_i))\right] - \epsilon_n d_{max} && (6.178)\\
&= \frac{1}{k}\sum_{i=1}^{k} \min_{\psi_0(z)} \mathbb{E}_{\overline{P}}\left[d(S, \psi_0(Z))\right] - \epsilon_n d_{max} && (6.179)
\end{aligned}$$

$$k = \beta n \tag{6.180}$$

where (6.177) is from (6.165), (6.178) uses the Markov relation given in (6.325), and (6.179) uses the definition of $\check{\mathbf{Q}}$ given in (6.156).

Collecting (6.153), (6.155) and (6.167), and taking the average of the distortion at the eavesdropper over the entire blocklength n from (6.172) and (6.179) finishes the proof. □

Scheme II – Superposition Hybrid Coding

An achievability region using superposition secure hybrid coding is given in the following theorem.

Theorem 6.15. *A distortion pair (D_b, D_e) is achievable if*

$$\begin{aligned} I(V;S) &< I(UV;Y) && (6.181)\\ D_b &\geq \mathbb{E}\left[d(S,\phi(V,Y))\right] && (6.182)\\ D_e &\leq \min\{\beta,\alpha\} \min_{\psi_0(z)} \mathbb{E}\left[d(S,\psi_0(Z))\right] \\ &\quad + (\alpha - \min\{\beta,\alpha\}) \min_{\psi_1(u,z)} \mathbb{E}\left[d(S,\psi_1(U,Z))\right] \\ &\quad + (1-\alpha) \min_{\psi_2(v,z)} \mathbb{E}\left[d(S,\psi_2(V,Z))\right] && (6.183) \end{aligned}$$

where

$$\begin{aligned} \beta &= \min\left\{\frac{[I(U;Y)-I(U;Z)]^+}{I(S;U|Z)}, 1\right\} && (6.184)\\ \alpha &= \min\left\{\frac{[r_s - I(Z;V|U)]^+}{I(S;V|ZU)}, 1\right\} && (6.185)\\ r_s &= \min\{I(V;Y|U), I(UV;Y) - I(S;U)\} && (6.186) \end{aligned}$$

for some distribution $P_S P_{V|S} P_{U|V} P_{X|SUV} P_{YZ|X}$ and function $\phi(\cdot,\cdot)$.

The proof of Theorem 6.15 follows the same lines as the proof of Theorem 6.14 with the modification of using a superposition codebook and the superposition version of the soft-covering lemma. The proof is provided in Appendix 6.5.8.

Under Scheme II, the distortion at the eavesdropper can potentially experience two transitions at βn and αn due to the superposition structure of the code.

6.3.3 Scheme Comparision

The relations of Scheme O, I and II can be summarized in the following corollaries.

Corollary 6.4. *Scheme II generalizes Scheme I.*

To see this, notice that we can let $U = \varnothing$ in Theorem 6.15. In fact, Scheme II simplifies to Scheme I if $\beta \geq \alpha$.

Corollary 6.5. *Scheme O is a special case of Scheme II.*

Proof. Identify the following assignment of random variables from Theorem 6.13 to 6.15

$$U \leftarrow U_1 U_2 \tag{6.187}$$

$$V \leftarrow \hat{S} V_2. \tag{6.188}$$

Substituting this assignment to the inequalities in Theorem 6.15 for the case $\alpha > \beta$, we get

$$I(S;\hat{S}) \quad < \quad I(V_2;Y). \tag{6.189}$$

It is easy to verify that the conditions given in Theorem 6.13 satisfy (6.189).

Substituting the assignment to (6.184) and (6.185) gives us

$$\beta \quad = \quad \frac{[I(U_2;Y) - I(U_2;Z)]^+}{I(S;U_1)} = \eta \tag{6.190}$$

$$\alpha \quad = \quad 1. \tag{6.191}$$

Moreover, by the statistical independence of SU_1 and U_2V_2Z

$$\min_{\psi_0(z)} \mathbb{E}[d(S,\psi_0(Z))] \quad = \quad \min_{a} \mathbb{E}[d(S,a)] \tag{6.192}$$

$$\min_{\psi_1(u,z)} \mathbb{E}[d(S,\psi_1(U,Z))] \quad = \quad \min_{\psi_1(u_1,u_2,z)} \mathbb{E}[d(S,\psi_1(U_1,U_2,Z))] \tag{6.193}$$

$$= \quad \min_{\psi(u_1)} \mathbb{E}[d(S,\psi(U_1))]. \tag{6.194}$$

□

6.3.4 The Perfect Secrecy Outer Bound

Theorem 6.16. *If (D_b, D_e) is achievable, then*

$$I(S;U) \quad \leq \quad I(U;Y) \tag{6.195}$$

$$D_b \quad \geq \quad \mathbb{E}[d(S,\phi(U,Y))] \tag{6.196}$$

$$D_e \quad \leq \quad \min_{a \in \hat{\mathcal{S}}} \mathbb{E}[d(S,a)] \tag{6.197}$$

for some distribution $P_S P_{U|S} P_{X|SU} P_{YZ|X}$ *and function* $\phi(\cdot,\cdot)$.

This trivial outer bound can be verified by using the optimality of hybrid coding for point-to-point communication and the fact that the estimation by the eavesdropper cannot be worse than the a-priori estimation of the source. Note that (6.195) and (6.196) are no different from the requirement for point-to-point source-channel coding. But we state it this way to emphasize that hybrid coding does achieve optimality for point-to-point communication.

6.3.5 Numerical Example

The source is distributed i.i.d. according to $Bern(p)$ and the channels are binary symmetric channels with crossover probabilities $p_1 = 0$ and $p_2 = 0.3$. For simplicity, we require lossless decoding at the legitimate receiver. Hamming distance is considered for distortion at the eavesdropper.

A numerical comparison of Scheme I with Scheme O is demonstrated in Fig. 6.8. The choice of auxiliary random variable U in Scheme I is SX, which may not necessarily be the optimum choice but is good enough to outperform Scheme O. Scheme II is not numerically evaluated. However, because of Corollary 6.4 and 6.5, we know analytically that Scheme II is no worse than O or I.

6.4 Summary

In this chapter, secure source-channel coding models have been studied. We have considered two main ideas: operationally separate source-channel coding and hybrid coding. Following the trace of developing secure source coding, we have investigated compression over a noisy wiretap channel under the naive formulation without causal source disclosure and the stronger formulation with causal source disclosure at the decoder. The theoretical results have been applied to an multimode fiber channel.

We have shown that, under the naive formulation, with a general broadcast channel and any distortion measure, it is possible with an operationally separate source-channel coding scheme to send the source at the maximum rate that guarantees lossless reconstruction at

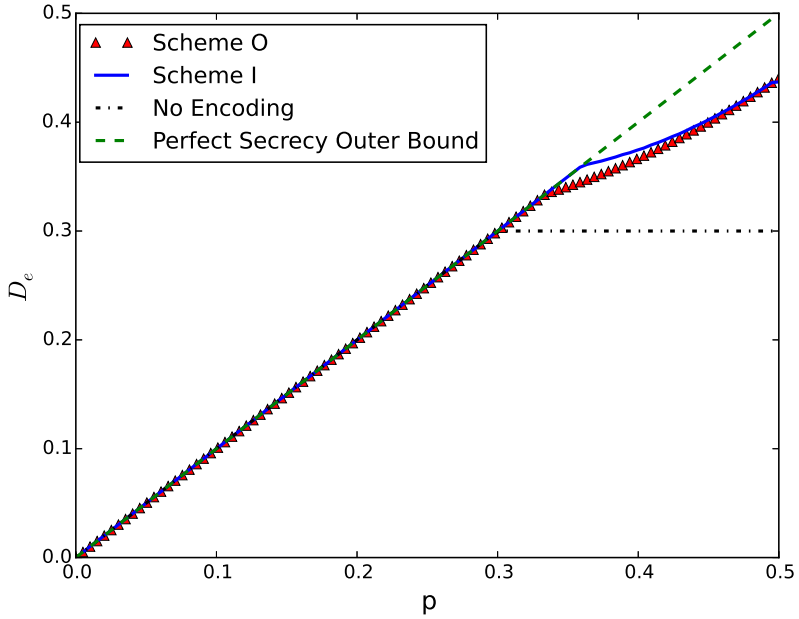

Figure 6.8: Distortion at the eavesdropper as a function of source distribution p with $p_1 = 0$, $p_2 = 0.3$.

the legitimate receiver while keeping the distortion at the eavesdropper as high as if it only has the source prior distribution. A similar result should generalize to lossy compression although this is not presented.

Under the stronger formulation with causal source disclosure to the eavesdropper, we have shown that an operational separate source-channel coding scheme is not optimal. An improvement is attained using hybrid coding. Although a simple numerical example shows that a basic hybrid coding scheme (I) can potentially outperform the operational-separate scheme (O), we have only managed to prove analytically that a superposition hybrid coding scheme can fully generalize both Scheme O and I. The direct relation between Scheme O and I, and whether Scheme II is strictly better than I are still open for further investigation. Non-trivial outer bounds are yet to be explored.

6.5 Appendix

6.5.1 Proof of Lemma 6.1

Let

$$\epsilon_{z^n} = \left\| P_{M_s|M_p=m_p} - P_{M_s|Z^n=z^n M_p=m_p} \right\|_{TV}. \tag{6.198}$$

Therefore,

$$\mathbb{E}_{P_{Z^n|M_p=m_p}}[\epsilon_{z^n}] = \left\| P_{Z^n|M_p=m_p} P_{M_s|M_p=m_p} - P_{Z^n M_s|M_p=m_p} \right\|_{TV} \leq \epsilon. \tag{6.199}$$

By Lemma 2.7 of [17],

$$|H(M_s|M_p=m_p) - H(M_s|Z^n=z^n, M_p=m_p)| \leq -\epsilon_{z^n} \log \frac{\epsilon_{z^n}}{|\mathcal{M}_s|}. \tag{6.200}$$

Note that $f(x) \triangleq -x \log x$ is concave. And by applying Jensen's inequality twice, we have

$$\begin{aligned}
& I(M_s; Z^n|M_p=m_p) \\
= \;& \left| \mathbb{E}_{P_{Z^n|M_p=m_p}}[H(M_s|M_p=m_p) - H(M_s|Z^n=z^n, M_p=m_p)] \right| && (6.201)\\
\leq \;& \mathbb{E}_{P_{Z^n|M_p=m_p}}\left[|H(M_s|M_p=m_p) - H(M_s|Z^n=z^n, M_p=m_p)| \right] && (6.202)\\
\leq \;& \mathbb{E}_{P_{Z^n|M_p=m_p}}\left[-\epsilon_{z^n} \log \frac{\epsilon_{z^n}}{|\mathcal{M}_s|} \right] && (6.203)\\
\leq \;& -\epsilon \log \frac{\epsilon}{|\mathcal{M}_s|}. && (6.204)
\end{aligned}$$

6.5.2 Proof of Lemma 6.2

Given (m_s, m_p), suppose there exists θ_{m_p} such that

$$\left\| P_{Z^n|M_p=m_p M_s=m_s} - \theta_{m_p} \right\|_{TV} \leq \epsilon_n \tag{6.205}$$

where $\epsilon_n = 2^{-n\beta}$ for some $\beta > 0$. Then we have the following:

$$
\begin{aligned}
& \left\| P_{Z^n|M_p=m_p} - \theta_{m_p} \right\|_{TV} \\
= & \sum_{z^n} \left| P_{Z^n|M_p=m_p}(z^n) - \theta_{m_p}(z^n) \right| && (6.206) \\
= & \sum_{z^n} \Bigg| \sum_{m_s} P_{M_s|M_p=m_p}(m_s) P_{Z^n|M_p=m_p M_s=m_s}(z^n) \\
& - \sum_{m_s} P_{M_s|M_p=m_p}(m_s) \theta_{m_p}(z^n) \Bigg| && (6.207) \\
= & \sum_{z^n} \left| \sum_{m_s} \frac{1}{|\mathcal{M}_s|} P_{Z^n|M_p=m_p M_s=m_s}(z^n) - \sum_{m_s} \frac{1}{|\mathcal{M}_s|} \theta_{m_p}(z^n) \right| && (6.208) \\
\leq & \sum_{z^n} \sum_{m_s} \frac{1}{|\mathcal{M}_s|} \left| P_{Z^n|M_p=m_p M_s=m_s}(z^n) - \theta_{m_p}(z^n) \right| && (6.209) \\
= & \sum_{m_s} \frac{1}{|\mathcal{M}_s|} \sum_{z^n} \left| P_{Z^n|M_p=m_p M_s=m_s}(z^n) - \theta_{m_p}(z^n) \right| && (6.210) \\
\leq & \sum_{m_s} \frac{1}{|\mathcal{M}_s|} \epsilon_n && (6.211) \\
= & \epsilon_n && (6.212)
\end{aligned}
$$

where (6.209) follows from triangle inequality and (6.211) follows from (6.205). We further have

$$
\begin{aligned}
& \left\| P_{Z^n|M_p=m_p} P_{M_s|M_p=m_p} - P_{Z^n M_s|M_p=m_p} \right\|_{TV} \\
= & \sum_{z^n} \sum_{m_s} |P_{Z^n|M_p=m_p}(z^n) P_{M_s|M_p=m_p}(m_s) \\
& - P_{Z^n|M_p=m_p M_s=m_s}(z^n) P_{M_s|M_p=m_p}(m_s)| && (6.213) \\
= & \frac{1}{|\mathcal{M}_s|} \sum_{z^n} \sum_{m_s} |P_{z^n|M_p=m_p}(z^n) - P_{Z^n|M_p=m_p M_s=m_s}(z^n)| && (6.214) \\
= & \frac{1}{|\mathcal{M}_s|} \sum_{z^n} \sum_{m_s} |P_{Z^n|M_p=m_p}(z^n) - \theta_{m_p}(z^n) + \theta_{m_p}(z^n) - P_{Z^n|M_p=m_p M_s=m_s}(z^n)| && (6.215) \\
\leq & \frac{1}{|\mathcal{M}_s|} \sum_{z^n} \sum_{m_s} \Big(\left| P_{Z^n|M_p=m_p}(z^n) - \theta_{m_p}(z^n) \right| \\
& + \left| P_{Z^n|M_p=m_p M_s=m_s}(z^n) - \theta_{m_p}(z^n) \right| \Big) && (6.216) \\
= & \frac{1}{|\mathcal{M}_s|} \sum_{m_s} \Big(\sum_{z^n} \left| P_{Z^n|M_p=m_p}(z^n) - \theta_{m_p}(z^n) \right| \\
& + \sum_{z^n} \left| P_{Z^n|M_p=m_p M_s=m_s}(z^n) - \theta_{m_p}(z^n) \right| \Big) && (6.217) \\
\leq & \frac{1}{|\mathcal{M}_s|} \sum_{m_s} (\epsilon_n + \epsilon_n) && (6.218) \\
= & 2\epsilon_n. && (6.219)
\end{aligned}
$$

By applying Lemma 6.1, we have

$$
\begin{aligned}
I(M_s; Z^n|M_p) &= \sum_{m_p} P_{M_p}(m_p) I(M_s; Z^n|M_p = m_p) && (6.220) \\
&\leq \sum_{m_p} P_{M_p}(m_p)(-2\epsilon_n \log \frac{2\epsilon_n}{|\mathcal{M}_s|}) && (6.221) \\
&\leq 2 \cdot 2^{-n\beta}(nR_s) && (6.222)
\end{aligned}
$$

where (6.222) goes to 0 as $n \to \infty$.

6.5.3 Proof of (6.24)

For each i, we have

$$\begin{aligned} I(S_i; Z^n|M_p) &\leq I(M_s S_i; Z^n|M_p) && (6.223)\\ &= I(M_s; Z^n|M_p) + I(S_i; Z^n|M_s M_p) && (6.224)\\ &\leq \epsilon && (6.225) \end{aligned}$$

for large enough n. Eq. (6.225) follows from strong secrecy of the channel and Fano's inequality. Note that weak secrecy is not sufficient to give us the desired result in our proof. We now define

$$\begin{aligned} P_i &\triangleq P_{S_i Z^n M_p} && (6.226)\\ \hat{P}_i &\triangleq P_{M_p} P_{S_i|M_p} P_{Z^n|M_p} && (6.227) \end{aligned}$$

i.e. $\bar{P}_i$ is the Markov chain $S_i - M_p - Z^n$. By Pinsker's inequality,

$$\begin{aligned} ||P_i - \hat{P}_i||_{TV} &\leq \frac{1}{\sqrt{2}} D(P_i||\hat{P}_i)^{\frac{1}{2}} && (6.228)\\ &= \frac{1}{\sqrt{2}} I(S_i; Z^n|M_p)^{\frac{1}{2}} && (6.229)\\ &\leq \sqrt{\frac{\epsilon}{2}} && (6.230) \end{aligned}$$

$$\begin{aligned} & \min_{\check{s}(i,z^n)} \mathbb{E}[d(S_i, \check{s}(i, Z^n))] \\ \geq & \min_{\check{s}(i,z^n,m_p)} \mathbb{E}[d(S_i, \check{s}(i, Z^n, M_p))] \\ \geq & \min_{\check{s}(i,z^n,m_p)} \mathbb{E}_{\hat{P}_i}[d(S_i, \check{s}(i, Z^n, M_p))] - \delta'(\epsilon) && (6.231)\\ = & \min_{\check{s}(i,m_p)} \mathbb{E}_{\hat{P}_i}[d(S_i, \check{s}(i, M_p))] - \delta'(\epsilon) && (6.232)\\ \geq & \min_{\check{s}(i,m_p)} \mathbb{E}[d(S_i, \check{s}(i, M_p))] - 2\delta'(\epsilon) && (6.233) \end{aligned}$$

where (6.231) and (6.233) use the fact that P_i and $\hat{P}_i$ are close in total variation from (6.230); and (6.232) uses the Markov relation $S_i - M_p - Z^n$ of the distribution $\hat{P}_i$. The

technical details can be found in Lemma 2 and 3 from [38]. Averaging over k, we obtain (6.24).

6.5.4 Justification of the condition $\max_{(R_s,R_p)\in\mathcal{R}} R_s > 0$

From Theorem 6.2 or 6.3, we have that

$$\max_{(R_s,R_p)\in\mathcal{R}} R_s > 0$$

is equivalent to

$$I(W;Y|V) - I(W;Z|V) \quad > \quad 0 \tag{6.234}$$

for some $V - W - X - YZ$. We claim that this can be simplified to

$$I(W;Y) - I(W;Z) \quad > \quad 0 \tag{6.235}$$

for some $W - X - YZ$.

To see (6.235) $\Rightarrow$ (6.234), we can simply let $V = \varnothing$. To see (6.234) $\Rightarrow$ (6.235), observe that if there exists $V - W - X - YZ$ such that (6.234) holds, then there has to exist at least one value v such that $I(W;Y|V=v) - I(W;Z|V=v) > 0$. We can redefine the distribution as $P_{W'X'Y'Z'} \triangleq P_{WXYZ|V=v}$. It can be verified that the Markov relation $W' - X' - Y'Z'$ holds and $P_{Y'Z'|X'} = P_{YZ|X}$.

6.5.5 Proof of Theorem 6.2 and Theorem 6.7

We provide the proof for Theorem 6.7. Since (6.36) required in Definition 6.8 is a milder condition than (6.6) required in Definition 6.3, the following proof also applies to Theorem 6.2.

Let us call the region given in Theorem 6.7 $\mathcal{R}_1$. Instead of showing $\mathcal{R}_1$ is achievable directly, we work with another region $\mathcal{R}_2$, which in fact is equivalent to $\mathcal{R}_1$.

Lemma 6.4. *The rate pair (R_p, R_s) is achievable if*

$$R_p + R_s \leq I(W;Y) - I(W;Z|V) \tag{6.236}$$

$$R_s \leq I(W;Y|V) - I(W;Z|V) \tag{6.237}$$

for some $P_V P_{W|V} P_{X|W} P_{YZ|X}$.

This region is denoted as $\mathcal{R}_2$.

Lemma 6.5.

$$\mathcal{R}_1 = \mathcal{R}_2. \tag{6.238}$$

Proof. The inclusion $\mathcal{R}_1 \subseteq \mathcal{R}_2$ is immediate. To see $\mathcal{R}_2 \subseteq \mathcal{R}_1$, fix a distribution $P_V P_{W|V} P_{X|W} P_{YZ|X}$. Viewing $\mathcal{R}_1$ as a union of rectangles, this defines a rectangle with corner point $(I(V;Y), I(W,Y|V - I(W;Z|V))) \triangleq (a,b)$. From the convexity of $\mathcal{R}_1$ and the fact that $(\max_{P_X} I(X;Y), 0) \in \mathcal{R}_1$, we see that the trapezoid $(0,0)$, $(0,b)$, (a,b), $(\max_{P_X} I(X;Y), 0)$ is included in $\mathcal{R}_1$. Since $a+b \leq \max_{P_X} I(X;Y)$, this trapezoid contains the trapezoid $(0,0)$, $(0,b)$, (a,b), $(a+b,0)$. □

The idea to show Theorem 6.7 is to include enough private randomness in the channel encoder so that the adversary effectively uses its full decoding capabilities to resolve the randomness, leaving no room to additionally decode part of the secret message. The amount of randomness required is the mutual information provided by the adversary's channel. To allow for private randomization, we augment the input to the encoder to accept a random variable K independent of all other random variables present in the system:

$$f_c : \mathcal{M}_p \times \mathcal{M}_s \times \mathcal{K} \mapsto \mathcal{X}^n. \tag{6.239}$$

First we state and prove a lemma that will grant us the existence of a certain channel code. Then we will analyze the equivocation under such a code. The proofs use strong typicality, which is defined as follows.

Definition 6.11. *Fix a distribution P_X. For $\epsilon > 0$, the ϵ-typical set is defined by*

$$T_\epsilon^n(X) \triangleq \{x^n \in \mathcal{X}^n : |P_{x^n}(x) - P_X(x)| < \epsilon, \forall x \in \mathcal{X}\} \tag{6.240}$$

where $P_{x^n}(x) = \frac{1}{n}\sum_{i=1}^n \mathbb{1}\{x_i = x\}$ is the empirical distribution of the sequence x^n.

Lemma 6.6. *Let $(R_p, R_s) \in \mathcal{R}_2$. Then, for all $\epsilon > 0$, there exists (n, f_c, g_c, h) (where $h : \mathcal{Z}^n \mapsto \mathcal{K}$) such that*

- $\mathbb{P}\left[(M_p, M_s) \neq (\hat{M}_p, \hat{M}_s)\right] < \epsilon$
- $\mathbb{P}\left[h(Z^n) \neq K | M_p = m_p, M_s = m_s\right] < \epsilon$
- *f_c can be written as the composition of $f_1 : \mathcal{W}^n \mapsto \mathcal{X}^n$ with $f_2 : \mathcal{M}_p \times \mathcal{M}_s \times \mathcal{K} \mapsto \mathcal{W}^n_{|T_\epsilon}$, where f_2 is injective and $\mathcal{W}^n_{|T_\epsilon} = \{w^n \in \mathcal{W}^n : w^n \in T_\epsilon^n(W)\}$.*

The second requirement says that the adversary can decode the private randomness K it is given the public and the private message; this is not necessary operationally but will aid in the analysis. The third requirement is technical.

Proof. Fix $P_V P_{W|V} P_{X|W}$ and $\epsilon > 0$. Choose R_p and R_s such that they satisfy (6.236) and (6.237). Let $R_k = I(W; Z|V) - \delta(\epsilon)$ and $K \sim Unif[1 : 2^{nR_k}]$; $\delta(\epsilon)$ to be determined later, is such that $\delta(\epsilon) \to 0$ as $\epsilon \to 0$.

Codebook generation: We independently generate 2^{nR_p} sequences in $\mathcal{V}^n$ according to $\prod_{i=1}^n P_V(v_i)$ and index by $m_p \in [1 : 2^{nR_p}]$. We use $\mathcal{C}_V^{(n)}$ to denote this random codebook. For each $m_p \in [1 : 2^{nR_p}]$, we independently generate $2^{n(R_s+R_k)}$ sequences in $\mathcal{W}^n$ according to $\prod_{i=1}^n P_{W|V}(w_i|v_i(m_p))$ and index by (m_p, m_s, k), $(m_s, k) \in [1 : 2^{nR_s}] \times [1 : 2^{nR_k}]$. We use $\mathcal{C}_W^{(n)}(m_p)$ to denote this random codebook.

Encoder f_c: To send (m_p, m_s, k), pass $w^n(m_p, m_s, k)$ through the memoryless channel $P_{X|V}$. If the output $x^n \notin T_\epsilon^n(X)$, declare an error; otherwise send x^n through the broadcast channel.

Decoder g_c: Find the unique (m_p, m_s, k) such that $(v^n(m_p), w^n(m_p, m_s, k), y^n) \in T_\epsilon^n(V, W, Y)$. Otherwise, declare an error.

Decoder h: Given m_p and m_s, find the unique k such that $(w^n(m_p, m_s, k), z^n) \in T_\epsilon^n(W, Z)$. Otherwise, declare an error.

Analysis: Without loss of generality, we can assume $M_s = M_p = K = 1$. Denoting the event that any error occurs by $\mathcal{E}$, it can be verified that $\mathbb{P}[\mathcal{E}] = \mathbb{P}[\mathcal{E}|M_s = 1, M_p = 1, K = 1]$. Define the following error events:

$$\begin{aligned}
\mathcal{E}_f &= \{(V^n(1), W^n(1,1,1)) \notin T_\epsilon^n(V, W)\} && (6.241)\\
\mathcal{E}_{g1} &= \{(V^n(1), W^n(1,1,1), Y^n) \notin T_\epsilon^n(V, W, Y)\} && (6.242)\\
\mathcal{E}_{g2} &= \{(V^n(m_p), W^n(m_p, m_s, k), Y^n) \in T_\epsilon^n(V, W, Y) \text{ for some } (m_s, k) \neq (1, 1)\} && (6.243)\\
\mathcal{E}_g &= \mathcal{E}_{g1} \cup \mathcal{E}_{g2} && (6.244)\\
\mathcal{E}_{h1} &= \{(V^n(1), W^n(1,1,1), Z^n) \notin T_\epsilon^n(V, W, Z)\} && (6.245)\\
\mathcal{E}_{h2} &= \{(V^n(1), W^n(1,1,k), Z^n) \in T_\epsilon^n(V, W, Z) \text{ for some } k \neq 1\} && (6.246)\\
\mathcal{E}_h &= \mathcal{E}_{h1} \cup \mathcal{E}_{h2}. && (6.247)
\end{aligned}$$

By the law of large numbers, $\mathbb{P}[\mathcal{E}_f] < \epsilon$ for sufficiently large n. By the law of large numbers and the packing lemma, $\mathbb{P}[\mathcal{E}_g] < \epsilon$ for sufficiently large n as long as we have

$$\begin{aligned}
R_s + R_k &< I(W; Y|V) - \delta(\epsilon) && (6.248)\\
R_p + R_s + R_k &< I(V, W; Y) - \delta(\epsilon). && (6.249)
\end{aligned}$$

By the law of large numbers and the packing lemma, $\mathbb{P}[\mathcal{E}_h] < \epsilon$ for sufficiently large n as long as we have

$$R_k < I(W; Z|V) - \delta(\epsilon). \quad (6.250)$$

Therefore, with all the rate restrictions satisfied, we use the union bound to obtain

$$\mathbb{P}[\mathcal{E}] \leq \mathbb{P}[\mathcal{E}_f] + \mathbb{P}[\mathcal{E}_g] + \mathbb{P}[\mathcal{E}_h] < 3\epsilon \quad (6.251)$$

for sufficiently large n.

Applying the random coding argument, there must exist a codebook that meets the above requirement. Finally, we address the range restriction and the injectivity of f_2. This is satisfied if we throw away the worst half of our codebook, knowing that this reduces the rate a negligible amount while maintaining negligible probability of error. □

Lemma 6.7. *If (X, Y) are random variables distributed such that*

$$\max_{x,y,y'} \frac{\mathbb{P}[Y = y|X = x]}{\mathbb{P}[Y = y'|X = x]} \leq 2^{\alpha} \tag{6.252}$$

then

$$H(Y|X) \geq \log |\mathcal{Y}| - \alpha. \tag{6.253}$$

Proof. Let $x \in \mathcal{X}$. There exists $y^* \in \mathcal{Y}$ such that $P_{Y|X}(y^*|x) \leq \frac{1}{|\mathcal{Y}|}$. For all $y \in \mathcal{Y}$,

$$\begin{aligned}
\log |\mathcal{Y}| &\leq \log \frac{1}{P_{Y|X}(y^*|x)} && (6.254)\\
&= \log \left(\frac{1}{P_{Y|X}(y|x)} \frac{P_{Y|X}(y|x)}{P_{Y|X}(y^*|x)} \right) && (6.255)\\
&\leq \log \left(\frac{1}{P_{Y|X}(y|x)} 2^{\alpha} \right) && (6.256)\\
&= \log \frac{1}{P_{Y|X}(y|x)} + \alpha. && (6.257)
\end{aligned}$$

Taking expectation of both sides, we have the inequality. □

We are now ready to prove Lemma 6.4.

Proof. Let $\epsilon > 0$. With the existence of the channel code from Lemma 6.6 in hand, we analyze the quantity $\frac{1}{n}H(M_s|Z^nM_p)$ by writing

$$\begin{aligned}
& H(M_s|Z^nM_p) \\
= \;& H(M_sZ^n|M_p) - H(Z^n|M_p) && (6.258)\\
= \;& H(M_sZ^nW^n|M_p) - H(W^n|M_sM_pZ^n) - H(Z^n|M_p) && (6.259)\\
= \;& H(M_sW^n|M_p) + H(Z^n|M_sM_pW^n) - H(W^n|M_sM_pZ^n) - H(Z^n|M_p) && (6.260)\\
\geq \;& H(W^n|M_p) + H(Z^n|W^n) - H(W^n|M_sM_pZ^n) - H(Z^n|M_p) && (6.261)
\end{aligned}$$

and bounding each of the terms in (6.261) individually.

By condition (6.36) and Lemma 6.7, we have

$$\begin{aligned}
\frac{1}{n}H(W^n|M_p) &\geq \frac{1}{n}\log|\mathcal{M}_s||\mathcal{K}| - \delta_n && (6.262)\\
&= R_s + R_k - \delta_n && (6.263)
\end{aligned}$$

by observing the following fact:

$$\begin{aligned}
& \mathbb{P}[W^n = w^n|M_p = m_p] \\
= \;& \sum_{(m_s,k)} \mathbb{P}[(M_s,K) = (m_s,k)|M_p = m_p] \\
& \mathbb{P}[W^n = w^n|(M_p,M_s,K) = (m_p,m_s,k)] && (6.264)\\
= \;& \sum_{(m_s,k):f_2(m_p,m_s,k)=w^n} \mathbb{P}[K=k]\mathbb{P}[M_s = m_s|M_p = m_p] && (6.265)\\
= \;& 2^{-nR_k}\mathbb{P}[M_s = m_s|M_p = m_p]. && (6.266)
\end{aligned}$$

To bound the second term, note that for large enough n,

$$\begin{aligned}
& \frac{1}{n} H(Z^n|W^n = w^n) \\
= \; & \frac{1}{n} \sum_{i=1}^{n} H(Z|W = w_i) && (6.267) \\
= \; & \frac{1}{n} \sum_{w \in \mathcal{W}} n P_{w^n}(w) H(Z|W = w) && (6.268) \\
\geq \; & \sum_{w \in \mathcal{W}} (P_W(w) - \epsilon) H(Z|W = w) && (6.269) \\
= \; & H(Z|W) - \delta(\epsilon). && (6.270)
\end{aligned}$$

Taking expectations on both sides gives us

$$\frac{1}{n} H(Z^n|W^n) \geq H(Z|W) - \delta(\epsilon). \tag{6.271}$$

To bound the third term, by Fano's inequality and the second requirement in Lemma 6.6, we have

$$\frac{1}{n} H(W^n|M_p M_s Z^n) \leq \epsilon_n. \tag{6.272}$$

To bound the last term, we define the following function:

$$\hat{z}^n(m_p, z^n) = \begin{cases} z^n \text{ if } (z^n, v^n(m_p)) \in T_\epsilon^n(V, Z) \\ \text{arbitrary } z^n \in T_\epsilon^n(Z|v^n(m_p)) \text{ o.w.} \end{cases} \tag{6.273}$$

Note that

$$\frac{1}{n} H(Z^n|M_p) \leq \frac{1}{n} H(Z^n|\hat{Z}^n M_p) + \frac{1}{n} H(\hat{Z}^n|M_p). \tag{6.274}$$

Since $\mathbb{P}[Z^n \neq \hat{Z}^n | M_p = m_p] < \epsilon$, we can apply Fano's inequality to $\frac{1}{n} H(Z^n | \hat{Z}^n M_p)$. Furthermore,

$$\begin{aligned} \frac{1}{n} H(\hat{Z}^n | M_p) &= \frac{1}{n} \mathbb{E}[H(Z^n | \hat{M_p} = m_p)] && (6.275) \\ &\leq \frac{1}{n} \mathbb{E}[\log |T_\epsilon^n(Z|v^n(M_p))|] && (6.276) \\ &\leq H(Z|V) + \delta_1(\epsilon). && (6.277) \end{aligned}$$

Putting it all together, we have

$$\begin{aligned} & \frac{1}{n} H(M_s | Z^n M_p) \\ \geq & \frac{1}{n} \left(nR_s + I(W; Z|V) + H(Z|W) - H(Z|V) \right) - \delta_2(\epsilon) && (6.278) \\ = & R_s - \delta_2(\epsilon) && (6.279) \end{aligned}$$

for sufficiently large n, where $\delta_2(\epsilon) \to 0$ as $\epsilon \to 0$. Or equivalently,

$$\frac{1}{n} I(M_s; Z^n | M_p) \to_n 0. \tag{6.280}$$

□

6.5.6 Proof of Lemma 6.3

Let $\epsilon > 0$. Introduce the random variable $Q \sim Unif[1:k]$, independent of all other random variables present. First, we have

$$\begin{aligned}
& I(S_Q; Z^n | M_p S^{Q-1} Q) \\
= \; & \frac{1}{k} \sum_{j=1}^{k} I(S_j; Z^n | M_p S^{j-1}) && (6.281) \\
= \; & \frac{1}{k} I(S^k; Z^n | M_p) && (6.282) \\
\leq \; & \frac{1}{k} I(M_s S^k; Z^n | M_p) && (6.283) \\
= \; & \frac{1}{k} I(M_s; Z^n | M_p) + \frac{1}{k} I(S^k; Z^n | M_p M_s) && (6.284) \\
= \; & \frac{1}{k} I(M_s; Z^n | M_p) && (6.285) \\
= \; & \frac{1}{R} \frac{1}{n} I(M_s; Z^n | M_p) && (6.286) \\
< \; & \epsilon && (6.287)
\end{aligned}$$

for sufficiently large n.

Next, denote

$$P = P_{S^Q Z^n M_p Q} \tag{6.288}$$

and define the following distribution:

$$\hat{P} = P_{M_p S^{Q-1} Q} P_{S_Q | M_p S^{Q-1} Q} P_{Z^n | M_p S^{Q-1} Q}. \tag{6.289}$$

That is, $\hat{P}$ is the Markov chain $S_Q - M_p S^{Q-1} Q - Z^n$. Now, using Pinsker's inequality, we have

$$\begin{aligned}
\left\| P - \hat{P} \right\|_{TV} \; & \leq \; D(P||\hat{P})^{\frac{1}{2}} && (6.290) \\
& = \; I(S_Q; Z^n | M_p S^{Q-1} Q)^{\frac{1}{2}} && (6.291) \\
& < \; \sqrt{\epsilon}. && (6.292)
\end{aligned}$$

Finally, we have

$$\begin{aligned}
& \min_{\check{s}(j,s^{j-1},z^n)} \mathbb{E}\left[\frac{1}{k}\sum_{j=1}^{k} d\left(S_j, \check{s}(j, S^{j-1}, Z^n)\right)\right] \\
\geq & \min_{\check{s}(j,s^{j-1},z^n,m_p)} \mathbb{E}\left[\frac{1}{k}\sum_{j=1}^{k} d\left(S_j, \check{s}(j, S^{j-1}, Z^n, M_p)\right)\right] && (6.293)\\
= & \min_{\check{s}(j,s^{j-1},z^n,m_p)} \mathbb{E}\left[d\left(S_Q, \check{s}(Q, S^{Q-1}, Z^n, M_p)\right)\right] && (6.294)\\
\geq & \min_{\check{s}(j,s^{j-1},z^n,m_p)} \mathbb{E}_{\hat{P}}\left[d\left(S_Q, \check{s}(Q, S^{Q-1}, Z^n, M_p)\right)\right] - \delta(\epsilon) && (6.295)\\
= & \min_{\check{s}(j,s^{j-1},m_p)} \mathbb{E}_{\hat{P}}\left[d\left(S_Q, \check{s}(Q, S^{Q-1}, M_p)\right)\right] - \delta(\epsilon) && (6.296)\\
\geq & \min_{\check{s}(j,s^{j-1},m_p)} \mathbb{E}\left[d\left(S_Q, \check{s}(Q, S^{Q-1}, M_p)\right)\right] - 2\delta(\epsilon) && (6.297)\\
= & \min_{\check{s}(j,s^{j-1},m_p)} \mathbb{E}\left[\frac{1}{k}\sum_{j=1}^{k} d\left(S_j, \check{s}(j, S^{j-1}, M_p)\right)\right] - 2\delta(\epsilon) && (6.298)
\end{aligned}$$

where (6.295) and (6.297) are by Property 2.1 (b); and (6.296) follows from the Markov relation under $\hat{P}$.

6.5.7 Sufficient condition on Theorem 6.11

From Theorem 6.1 and Corollary 6.3, we know that a sufficient condition for the eavesdropper's channel not being less noisy than the intended receiver's channel is

$$\max_{K\in\mathcal{H}^{M\times M}, 0\preceq K\preceq I} \frac{|\mathrm{SNR}K + I|}{|\mathrm{SNR}^e \Psi^e K \Psi^{e\dagger}\Phi + I|} > 1. \tag{6.299}$$

However, (6.299) is computationally difficult to verify. If we restrict K to be of the form $K = \Psi^{e\dagger}\Lambda\Psi^e$ where Λ is diagonal with diagonal entries $\lambda_i \in [0,1]$, then (6.299) has a much simpler form:

$$\frac{\prod_{i=1}^{M}(1+\mathrm{SNR}\lambda_i)}{\prod_{i=1}^{M}(1+\mathrm{SNR}^e\lambda_i\bar{\phi}_i)} > 1. \tag{6.300}$$

Therefore, if there exists a $j \in \{1,...,M\}$ such that $\bar{\phi}_j < \frac{\mathrm{SNR}}{\mathrm{SNR}^e}$, we can choose $\lambda_j = 1$ and $\lambda_i = 0$ for $i \neq j$ to satisfy (6.300).

6.5.8 Proof of Theorem 6.15

We first provide an adapted version of the superposition soft-covering lemma that is needed in the following analysis.

Lemma 6.8. *(**Superposition soft-covering**, [11]) Given a joint distribution P_{UVX}, let $\mathcal{C}_U^{(n)}$ be a random codebook of 2^{nR_1} sequences in $\mathcal{U}^n$, each drawn independently according to $\prod_{t=1}^n P_U(u_t)$ and indexed by $m_1 \in [1 : 2^{nR_1}]$. For each m_1, let $\mathcal{C}_V^{(n)}(m_1)$ be a random codebook of 2^{nR_2} sequences in $\mathcal{V}^n$, each drawn independently according to $\prod_{t=1}^n P_{V|U}(v_t|u_t(m_1))$ and indexed by $(m_1, m_2) \in [1 : 2^{nR_2}]$. Denote by $\mathbf{P}_{X^n}$ the output distribution induced by selecting an index pair (m_1, m_2) uniformly at random and applying $U^n(m_1)$ and $V^n(m_1, m_2)$ to the memoryless channel specified by $P_{X|UV}$. If*

$$\begin{aligned} R_1 &> I(U;X) && (6.301)\\ R_2 &> I(UV;X) - H(U) && (6.302)\\ R_1 + R_2 &> I(UV;X) && (6.303) \end{aligned}$$

then

$$\mathbb{E}_{\mathcal{C}^{(n)}}\left[\left\|\mathbf{P}_{X^n} - \prod_{t=1}^n P_X\right\|_{TV}\right] \leq e^{-\gamma n} \to_n 0, \tag{6.304}$$

for some $\gamma > 0$.

Now we begin the proof of Theorem 6.15.

The source and channel distributions $\overline{P}_S \triangleq P_S$ and $\overline{P}_{YZ|X} \triangleq P_{YZ|X}$ are given by the problem statement. Fix a joint distribution $\overline{P}_S\overline{P}_{V|S}\overline{P}_{U|V}\overline{P}_{X|SUV}\overline{P}_{YZ|X}$.

Codebook generation: We independently generate 2^{nR_p} sequences in $\mathcal{U}^n$ according to $\prod_{t=1}^n \overline{P}_U(u_t)$ and index them by $m_p \in [1 : 2^{nR_p}]$. We use $\mathcal{C}_U^{(n)}$ to denote this random codebook. For each $m_p \in [1 : 2^{nR_p}]$, we independently generate 2^{nR_s} sequences in $\mathcal{V}^n$ according to $\prod_{t=1}^n \overline{P}_{V|U}(v_t|u_t(m_p))$ and index them by (m_p, m_s), $m_s \in [1 : 2^{nR_s}]$. We use $\mathcal{C}_V^{(n)}(m_p)$ to denote this random codebook.

Encoder: Encoding has two steps. In the first step, a likelihood encoder $\mathbf{P}_{LE}(m_p, m_s|s^n)$ is used. It chooses (M_p, M_s) stochastically according to the following probability:

$$\mathbf{P}_{LE}(m|s^n) = \frac{\mathcal{L}(m|s^n)}{\sum_{\bar{m}\in\mathcal{M}} \mathcal{L}(\bar{m}|s^n)} \tag{6.305}$$

where $m = (m_p, m_s)$, $\mathcal{M} = [1 : 2^{nR_p}] \times [1 : 2^{nR_s}]$, and

$$\mathcal{L}(m|s^n) = \overline{P}_{S^n|V^n}(s^n|v^n(m)). \tag{6.306}$$

In the second step, the encoder produces the channel input through a random transformation given by

$$\prod_{t=1}^{n} \overline{P}_{X|SUV}(x_t|s_t, U_t(m_p), V_t(m_p, m_s)). \tag{6.307}$$

Decoder: Decoding also has two steps. In the first step, let $\mathbf{P}_{D1}(\hat{m}_p, \hat{m}_s|y^n)$ be a good channel decoder with respect to the superposition codebook $\{v^n(a_p, a_s)\}_{a_p,a_s}$ and memoryless channel $\overline{P}_{Y|X}$. In the second step, fix a function $\phi(\cdot,\cdot)$. Define $\phi^n(v^n, y^n)$ as the concatenation $\{\phi(v_t, y_t)\}_{t=1}^n$ and set the decoder $\mathbf{P}_{D2}$ to be the deterministic function

$$\mathbf{P}_{D2}(\hat{s}^n|\hat{m}_p, \hat{m}_s, y^n) \triangleq \mathbb{1}\{\hat{s}^n = \phi^n(v^n(\hat{m}_p, \hat{m}_s), y^n)\}. \tag{6.308}$$

Analysis: We can write the system induced distribution in the following form:

$$\begin{aligned}
& \mathbf{P}_{M_pM_sU^nV^nS^nX^nY^nZ^n\hat{M}_p\hat{M}_s\hat{S}^n}(m_p, m_s, u^n, v^n, s^n, x^n, y^n, z^n, \hat{m}_p, \hat{m}_s, \hat{s}^n) \\
= \; & \overline{P}_{S^n}(s^n)\mathbf{P}_{M_pM_s|S^n}(m_p, m_s|s^n)\mathbb{1}\{u^n = U^n(m_p)\}\mathbb{1}\{v^n = V^n(m_p, m_s)\} \\
& \prod_{t=1}^{n} \overline{P}_{X|SUV}(x_t|s_t, u_t, v_t) \prod_{t=1}^{n} \overline{P}_{YZ|X}(y_t, z_t|x_t) \\
& \mathbf{P}_{\hat{M}_p\hat{M}_s|Y^n}(\hat{m}_p, \hat{m}_s|y^n)\mathbf{P}_{\hat{S}^n|\hat{M}_p\hat{M}_sY^n}(\hat{s}^n|\hat{m}_p, \hat{m}_s, y^n) \qquad (6.309) \\
= \; & \overline{P}_{S^n}(s^n)\mathbf{P}_{LE}(m_p, m_s|s^n)\mathbb{1}\{u^n = U^n(m_p)\}\mathbb{1}\{v^n = V^n(m_p, m_s)\} \\
& \prod_{t=1}^{n} \overline{P}_{X|SUV}(x_t|s_t, u_t, v_t) \prod_{t=1}^{n} \overline{P}_{YZ|X}(y_t, z_t|x_t) \\
& \mathbf{P}_{D_1}(\hat{m}_p, \hat{m}_s|y^n)\mathbf{P}_{D_2}(\hat{s}^n|\hat{m}_p, \hat{m}_s, y^n) \qquad (6.310)
\end{aligned}$$

where the encoding and decoding have been highlighted with color for easy reading.

To help with the analysis, we define an idealized distribution $\mathbf{Q}$ as follows:

$$\begin{aligned}
& \mathbf{Q}_{M_p M_s U^n V^n S^n X^n Y^n Z^n}(m_p, m_s, u^n, v^n, s^n, x^n, y^n, z^n) \\
= \; & \frac{1}{2^{n(R_p+R_s)}} \mathbb{1}\{u^n = U^n(m_p)\} \mathbb{1}\{v^n = V^n(m_p, m_s)\} \prod_{t=1}^{n} \overline{P}_{S|UV}(s_t|u_t, v_t) \\
& \prod_{t=1}^{n} \overline{P}_{X|SUV}(x_t|s_t, u_t, v_t) \prod_{t=1}^{n} \overline{P}_{YZ|X}(y_t, z_t|x_t). \qquad (6.311)
\end{aligned}$$

Using standard techniques discussed in Section 3.3 (3.10)-(3.13), it can be shown the following properties hold:

$$\begin{aligned}
& \mathbb{E}_{\mathcal{C}^{(n)}} \left[\mathbf{Q}_{U^n V^n S^n X^n Y^n Z^n}(u^n, v^n, s^n, x^n, y^n, z^n) \right] \\
= \; & \overline{P}_{U^n V^n S^n X^n Y^n Z^n}(u^n, v^n, s^n, x^n, y^n, z^n) \qquad (6.312)
\end{aligned}$$

Using the superposition soft-covering lemma 6.8, we have

$$\mathbb{E}_{\mathcal{C}^{(n)}} \left[\left\| \mathbf{Q}_{S^n} - \overline{P}_{S^n} \right\|_{TV} \right] \leq e^{-\gamma_1 n}. \qquad (6.313)$$

if

$$R_p > I(S;U) \qquad (6.314)$$

$$R_p + R_s > I(UV;S) = I(V;S) \qquad (6.315)$$

From (6.313) and Property 2.1(d), we have

$$\mathbb{E}_{\mathcal{C}^{(n)}} \left[\| \mathbf{Q} - \mathbf{P} \|_{TV} \right] \leq e^{-\gamma_1 n} \triangleq \epsilon_{1n} \qquad (6.316)$$

where the distributions are across random variables $U^n V^n S^n X^n Y^n Z^n$.

Define

$$\mathbf{Q}^{(1)} = \mathbf{Q}\mathbf{P}_{D1}(\hat{m}_p, \hat{m}_s|y^n)\mathbf{P}_{D2}(\hat{s}^n|\hat{m}_p, \hat{m}_s, y^n), \tag{6.317}$$

$$\mathbf{Q}^{(2)} = \mathbf{Q}\mathbf{P}_{D1}(\hat{m}_p, \hat{m}_s|y^n)\mathbf{P}_{D2}(\hat{s}^n|m_p, m_s, y^n). \tag{6.318}$$

Applying channel coding result, a good channel decoder $\mathbf{P}_{D1}$ will drive the error probability

$$\mathbb{E}_{\mathcal{C}^{(n)}}\left[\mathbb{P}_{\mathbf{Q}^{(1)}}\left[(\hat{M}_p, \hat{M}_s) \neq (M_p, M_s)\right]\right] \leq \delta_n \to_n 0$$

if

$$R_s \leq I(V;Y|U) \tag{6.319}$$

$$R_p + R_s \leq I(UV;Y). \tag{6.320}$$

Again using standard techniques discussed in Section 4.3.2 (4.21)-(4.28), it can be shown that

$$\mathbb{E}_{\mathcal{C}^{(n)}}\left[\left\|\mathbf{Q}^{(1)} - \mathbf{Q}^{(2)}\right\|_{TV}\right] \leq \delta_n \tag{6.321}$$

and therefore,

$$\begin{aligned} & \mathbb{E}_{\mathcal{C}^{(n)}}\left[\mathbb{E}_{\mathbf{P}}\left[d(S^n, \hat{S}^n)\right]\right] \\ \leq\ & \mathbb{E}_{\mathcal{C}^{(n)}}\left[\mathbb{E}_{\mathbf{Q}^{(2)}}\left[d(S^n, \hat{S}^n)\right]\right] + d_{max}(\epsilon_{1n} + \delta_n) \qquad (6.322) \\ =\ & \mathbb{E}_{\overline{P}}[d(S, \phi(V, Y))] + d_{max}(\epsilon_{1n} + \delta_n). \qquad (6.323) \end{aligned}$$

On the other hand, we need to analyze the performance of the eavesdropper. We define an auxiliary distribution

$$\begin{aligned}
&\tilde{\mathbf{Q}}^{(i)}_{M_pS^iZ^n}(m_p, s^i, z^n) \\
= \;& \frac{1}{2^{nR_p}} \prod_{t=1}^{n} \overline{P}_{Z|U}(z_t|U_t(m_p)) \prod_{j=1}^{i} \overline{P}_{S|ZU}(s_j|z_j, U_j(m_p)).
\end{aligned} \tag{6.324}$$

Observe that under $\tilde{\mathbf{Q}}^{(i)}$,

$$S_i - U_i(M_p)Z_i - M_pM_sZ^nS^{i-1}. \tag{6.325}$$

Recall that

$$\begin{aligned}
&\mathbf{Q}_{M_pM_sZ^nS^i}(m_p, m_s, z^n, s^i) \\
= \;& \frac{1}{2^{n(R_p+R_s)}} \prod_{t=1}^{n} \overline{P}_{Z|UV}(z_t|U_t(m_p), V_t(m_p, m_s)) \\
& \prod_{j=1}^{i} \overline{P}_{S|ZUV}(s_j|z_j, U_j(m_p), V_j(m_p, m_s)).
\end{aligned} \tag{6.326}$$

Applying the soft-covering lemma, we have

$$\mathbb{E}_{\mathcal{C}^{(n)}} \left[\left\| \tilde{\mathbf{Q}}^{(i)}_{M_pZ^nS^i} - \mathbf{Q}_{M_pZ^nS^i} \right\|_{TV} \right] \leq e^{-\gamma_3 n} \tag{6.327}$$

for any $\alpha < \frac{R_s - I(Z;V|U)}{I(S;V|ZU)}$, $i \leq \alpha n$, where $\gamma_3 > 0$ depends on the gap $\frac{R_s - I(Z;V|U)}{I(S;V|ZU)} - \alpha$.

This implies that

$$\mathbb{E}_{\mathcal{C}^{(n)}} \left[\left\| \tilde{\mathbf{Q}}^{(i)}_{M_pZ^nS^i} - \mathbf{P}_{M_pZ^nS^i} \right\|_{TV} \right] \leq e^{-\gamma_1 n} + e^{-\gamma_3 n}. \tag{6.328}$$

Also note that, since $R_p > 0$, we have

$$\mathbb{E}_{\mathcal{C}^{(n)}} \left[\left\| \tilde{\mathbf{Q}}^{(i)}_{u_i(M_p)} - \overline{P}_U \right\|_{TV} \right] \leq e^{-\gamma_2 n}. \tag{6.329}$$

For later reference, we also make the following observation. Since $R_s > 0$, we have

$$\mathbb{E}_{\mathcal{C}^{(n)}}\left[\left\|\mathbf{Q}_{u_i(M_p)v_i(M_p,M_s)} - \overline{P}_{UV}\right\|_{TV}\right] \leq e^{-\gamma_5 n}. \tag{6.330}$$

We now focus on the case $\alpha > \beta$.

Similarly, we define another auxiliary distribution

$$\begin{aligned} & \check{\mathbf{Q}}^{(i)}_{S^i Z^n}(s^i, z^n) \\ = & \prod_{t=1}^{n} \overline{P}_Z(z_t) \prod_{j=1}^{i} \overline{P}_{S|Z}(s_j|z_j) \end{aligned} \tag{6.331}$$

and under $\check{\mathbf{Q}}^{(i)}$,

$$S_i - Z_i - Z^n S^{i-1}. \tag{6.332}$$

Again recall that

$$\begin{aligned} & \tilde{\mathbf{Q}}^{(i)}_{M_p Z^n S^i}(m_p, z^n, s^i) \\ = & \frac{1}{2^{nR_p}} \prod_{t=1}^{n} \overline{P}_{Z|U}(z_t|U_t(m_p)) \prod_{j=1}^{i} \overline{P}_{S|ZU}(s_j|z_j, U_j(m_p)). \end{aligned} \tag{6.333}$$

Applying the soft-covering lemma, we have

$$\mathbb{E}_{\mathcal{C}^{(n)}}\left[\left\|\check{\mathbf{Q}}^{(i)}_{Z^n S^i} - \tilde{\mathbf{Q}}^{(i)}_{Z^n S^i}\right\|_{TV}\right] \leq e^{-\gamma_4 n} \tag{6.334}$$

for any $\beta < \frac{R - I(U;Z)}{I(S;U|Z)}$, $i \leq \beta n$, where $\gamma_4 > 0$ depends on the gap $\frac{R - I(U;Z)}{I(S;U|Z)} - \beta$.

This implies that

$$\Rightarrow \mathbb{E}_{\mathcal{C}^{(n)}}\left[\left\|\check{\mathbf{Q}}^{(i)}_{Z^n S^i} - \mathbf{P}_{Z^n S^i}\right\|_{TV}\right] \leq e^{-\gamma_1 n} + e^{-\gamma_3 n} + e^{-\gamma_4 n} \tag{6.335}$$

Based on the above analysis, there exists a codebook $\mathcal{C}^{(n)}$ such that

$$\sum_{i=1}^{n} \left\| P_{M_p Z^n S^i} - \tilde{Q}^{(i)}_{M_p Z^n S^i} \right\|_{TV} \leq \epsilon_n \tag{6.336}$$

$$\sum_{i=1}^{n} \left\| P_{M_p M_s Z^n S^i} - Q_{M_p M_s Z^n S^i} \right\|_{TV} \leq \epsilon_n \tag{6.337}$$

$$\sum_{i=1}^{n} \left\| P_{Z^n S^i} - \check{Q}^{(i)}_{Z^n S^i} \right\|_{TV} \leq \epsilon_n \tag{6.338}$$

$$\sum_{i=1}^{n} \left\| \tilde{Q}^{(i)}_{u_i(M_p)} - \overline{P}_U \right\|_{TV} \leq \epsilon_n \tag{6.339}$$

$$\sum_{i=1}^{n} \left\| Q_{u_i(M_p), v_i(M_p, M_s)} - \overline{P}_{UV} \right\|_{TV} \leq \epsilon_n \tag{6.340}$$

$$\mathbb{E}_P \left[d(S^n, \hat{S}^n) \right] \leq \mathbb{E}_{\overline{P}} \left[d(S^n, \hat{S}^n) \right] + \epsilon_n \tag{6.341}$$

where

$$\epsilon_n = n \left(3e^{-n\gamma_1} + e^{-n\gamma_2} + 2e^{-n\gamma_3} + e^{-n\gamma_4} + e^{-n\gamma_5} \right) + d_{max}(\epsilon_{1n} + \delta_n). \tag{6.342}$$

Now we evaluate the distortion at the eavesdropper. According to the above analysis, the eavesdropper will experience up to two transitions during the entire blocklength n, one at βn where the public message M_p becomes visible to the eavesdropper and one at αn where the secret message M_s also becomes visible. We next give a lower bound on the distortion for each period of the blocklength by considering before and after αn, and before and after βn.

Before αn and After βn

$$\min_{\{\psi_{1i}(s^{i-1},z^n)\}} \mathbb{E}_P \left[\frac{1}{k} \sum_{i=j_1}^{j_2} d(S_i, \psi_{1i}(S^{i-1}, Z^n)) \right]$$

$$= \frac{1}{k} \sum_{i=j_1}^{j_2} \min_{\psi_{1i}(s^{i-1},z^n)} \mathbb{E}_P \left[d(S_i, \psi_{1i}(S^{i-1}, Z^n)) \right] \tag{6.343}$$

$$\geq \frac{1}{k} \sum_{i=j_1}^{j_2} \min_{\psi_{1i}(s^{i-1},z^n,m_p)} \mathbb{E}_P \left[d(S_i, \psi_{1i}(S^{i-1}, Z^n, M_p)) \right] \tag{6.344}$$

$$\geq \frac{1}{k} \sum_{i=j_1}^{j_2} \min_{\psi_{1i}(s^{i-1},z^n,m_p)} \mathbb{E}_{\tilde{Q}^{(i)}} \left[d(S_i, \psi_{1i}(S^{i-1}, Z^n, M_p)) \right] - \epsilon_n d_{max} \tag{6.345}$$

$$= \frac{1}{k} \sum_{i=j_1}^{j_2} \min_{\psi_1(u,z)} \mathbb{E}_{\tilde{Q}^{(i)}} \left[d(S_i, \psi_1(u_i(M_p), Z_i)) \right] - \epsilon_n d_{max} \tag{6.346}$$

$$\geq \frac{1}{k} \sum_{i=j_1}^{j_2} \min_{\psi_1(U,Z)} \mathbb{E}_{\overline{P}} \left[d(S, \psi_1(U, Z)) \right] - 2\epsilon_n d_{max} \tag{6.347}$$

$$k = \alpha n - \beta n + 1 \tag{6.348}$$

$$j_1 = \beta n + 1 \tag{6.349}$$

$$j_2 = \alpha n \tag{6.350}$$

where (6.345) is from (6.336), (6.346) uses the Markov relation under $\tilde{Q}^{(i)}$ given in (6.325), and (6.347) uses (6.339) and the fact that

$$\tilde{Q}^{(i)}_{Z_i S_i | U_i}(z_i, s_i | u_i) = \overline{P}_{Z|U}(z_i|u_i) \overline{P}_{S|ZU}(s_i|z_i, u_i).$$

After αn

Since

$$\begin{aligned}
& \mathbf{Q}_{M_p M_s Z^n S^i}(m_p, m_s, z^n, s^i) \\
= \; & \frac{1}{2^{n(R_p+R_s)}} \prod_{t=1}^{n} \overline{P}_{Z|UV}(z_t|U_t(m_p), V_t(m_p, m_s)) \\
& \prod_{j=1}^{i} \overline{P}_{S|ZUV}(s_j|z_j, U_j(m_p), V_j(m_p, m_s))
\end{aligned} \tag{6.351}$$

we have under $\mathbf{Q}$

$$S_i - U_i(M_p)V_i(M_p, M_s)Z_i - M_p M_s Z^n S^{i-1}. \tag{6.352}$$

We can now bound the distortion after αn:

$$\begin{aligned}
& \min_{\{\psi_{2i}(z^n, s^{i-1})\}_i} \mathbb{E}_P \left[\frac{1}{k} \sum_{i=j}^{n} d(S_i, \psi_{2i}(Z^n, S^{i-1})) \right] \\
= \; & \frac{1}{k} \sum_{i=j}^{n} \min_{\psi_{2i}(z^n, s^{i-1})} \mathbb{E}_P \left[d(S_i, \psi_{2i}(Z^n, S^{i-1})) \right] && (6.353) \\
\geq \; & \frac{1}{k} \sum_{i=j}^{n} \min_{\psi_{2i}(z^n, s^{i-1}, m_p, m_s)} \mathbb{E}_P \left[d(S_i, \psi_{2i}(Z^n, S^{i-1}, M_p, M_s)) \right] && (6.354) \\
\geq \; & \frac{1}{k} \sum_{i=j}^{n} \min_{\psi_{2i}(z^n, s^{i-1}, m_p, m_s)} \mathbb{E}_Q \left[d(S_i, \psi_{2i}(Z^n, S^{i-1}, M_p, M_s)) \right] - \epsilon_n d_{max} && (6.355) \\
= \; & \frac{1}{k} \sum_{i=j}^{n} \min_{\psi_2(U,V,Z)} \mathbb{E}_Q \left[d(S_i, \psi_2(U_i(M_p), V_i(M_p, M_s), Z_i)) \right] - \epsilon_n d_{max} && (6.356) \\
\geq \; & \min_{\psi_2(U,V,Z)} \mathbb{E}_{\overline{P}} \left[d(S, \psi_2(U, V, Z)) \right] - 2\epsilon_n d_{max} && (6.357)
\end{aligned}$$

$$k = (1 - \alpha)n \tag{6.358}$$

$$j = \alpha n + 1 \tag{6.359}$$

where (6.357) follows from (6.340) and the fact that

$$Q_{S_iZ_i|U_iV_i}(s_i, z_i|u_i, v_i) = \overline{P}_{SZ|UV}(s_i, z_i|u_i, v_i).$$

Before βn

$$\begin{aligned}
&\min_{\{\psi_{0i}(s^{i-1},z^n)\}_i} \mathbb{E}_P \left[\frac{1}{k}\sum_{i=1}^{k} d(S_i, \psi_{0i}(S^{i-1}, Z^n))\right] \\
= \;& \frac{1}{k}\sum_{i=1}^{k} \min_{\psi_{0i}(s^{i-1},z^n)} \mathbb{E}_P \left[d(S_i, \psi_{0i}(S^{i-1}, Z^n))\right] && (6.360)\\
\geq \;& \frac{1}{k}\sum_{i=1}^{k} \min_{\psi_{0i}(s^{i-1},z^n)} \mathbb{E}_{\check{Q}^{(i)}} \left[d(S_i, \psi_{0i}(S^{i-1}, Z^n))\right] - \epsilon_n d_{max} && (6.361)\\
= \;& \frac{1}{k}\sum_{i=1}^{k} \min_{\psi_0(z)} \mathbb{E}_{\check{Q}^{(i)}} \left[d(S_i, \psi_0(Z_i))\right] - \epsilon_n d_{max} && (6.362)\\
= \;& \frac{1}{k}\sum_{i=1}^{k} \min_{\psi_0(z)} \mathbb{E}_{\overline{P}} \left[d(S, \psi_0(Z))\right] - \epsilon_n d_{max} && (6.363)
\end{aligned}$$

$$k = \beta n. \tag{6.364}$$

Gathering (6.314), (6.315), (6.319) and (6.320), and applying Fourier-Motzkin elimination give us the inequalities in Theorem 6.15. Recall (6.341) and average the distortion at the eavesdropper over the three sections of the blocklength. This finishes the proof for $\alpha > \beta$.

For the case of $\alpha \leq \beta$, we can modify the proof accordingly and it can be shown that the eavesdropper begins to decode the public message at θn, where

$$\theta = \frac{R_p + R_s - I(UV; Z)}{I(UV; S|Z)}. \tag{6.365}$$

Choosing the best $R_p + R_s$ gives us

$$\theta = \min\left\{\frac{[I(UV; Y) - I(UV; Z)]^+}{I(UV; S|Z)}, 1\right\}. \tag{6.366}$$

The analysis of the distortion at the eavesdropper before and after the time transition θn is the same as that for the other case. By the Markov relation $S - V - U$, this gives us the following achievable region for the case $\alpha \leq \beta$:

$$\begin{aligned} I(UV;S) &< I(UV;Y) && (6.367)\\ D_b &\geq \mathbb{E}\left[d(S,\phi(UV,Y))\right] && (6.368)\\ D_e &\leq \theta \min_{\psi_0(z)} \mathbb{E}\left[d(S,\psi_0(Z))\right] + (1-\theta) \min_{\psi_2(uv,z)} \mathbb{E}\left[d(S,\psi_2(UV,Z))\right]. && (6.369) \end{aligned}$$

Note that UV only appear together in these expressions, which simplifies to Scheme I.

Rewriting the regions for the case $\alpha > \beta$ and $\alpha \leq \beta$ gives us the region in Theorem 6.15.

Chapter 7

Conclusion

We have introduced a new tool – the likelihood encoder, for analyzing source coding problems. Applying this tool to classical source coding settings yields simple achievability proofs. New results in rate-distortion based secrecy systems are obtained under various formulations. The direct extensions have been discussed for each particular setting at the end of the corresponding chapters and will not be repeated here. We next point out some limitations of our overall work and suggest some future directions for possible improvement and further investigation.

The analysis we provide for the achievability scheme based on a likelihood encoder relies on the soft-covering lemmas and properties of total variation distance. Although the soft-covering lemmas are known to be asymptotically efficient, their non-asymptotic performance is only upper bounded and the bound is believed to be not tight. A more careful examination of the proofs for the soft-covering lemmas is required for tightening the bound. This is not conducted in this thesis and is a key step for improving the error exponent derived for the likelihood encoder.

On the secrecy side, the achievability using the likelihood encoder depends on the superposition soft-covering lemma, which has this phase transition as stated in the lemma itself: the system induced distribution can only be approximated by the idealized distribution with our desired properties up to some proportion of the entire blocklength. As a consequence, this leads to achievability results with phase transitions under causal source disclosure in joint source-channel coding problems. It is unclear how this can be avoided

as the optimal solution typically does not have this kind of structure. Yet this does not exclude the possibility for optimality of such structure since the outer bound may also not be tight.

This thesis has focused primarily on achievability results, in both lossy compression and secrecy. Except for some cases in which we have matching inner and outer bounds, we did not provide any new approaches to the converse proofs. However, we hope our novelty in showing achievability results has provided some interesting insights and motivated more work in related fields.

Bibliography

[1] C. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.

[2] H. Yamamoto, "Rate-distortion theory for the shannon cipher system," *IEEE Transactions on Information Theory*, vol. 43, no. 3, pp. 827–835, May 1997.

[3] C. Schieler and P. Cuff, "Secrecy is cheap if the adversary must reconstruct," in *Proc. 2012 IEEE International Symposium on Information Theory Proceedings (ISIT)*, July 2012, pp. 66–70.

[4] P. Cuff, "Using a secret key to foil an eavesdropper," in *Proc. 48th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Sept. 2010, pp. 1405–1411.

[5] ——, "A framework for partial secrecy," in *Proc. 2010 IEEE Global Telecommunications Conference (GLOBECOM 2010)*, Dec. 2010, pp. 1–5.

[6] C. Schieler and P. Cuff, "Rate-distortion theory for secrecy systems," *IEEE Transactions on Information Theory*, vol. 60, no. 12, pp. 7584–7605, Dec. 2014.

[7] A. D. Wyner, "The common information of two dependent random variables," *IEEE Transactions on Information Theory*, vol. 21, no. 2, pp. 163–179, 1975.

[8] P. Minero, S. H. Lim, and Y.-H. Kim, "Hybrid coding: An interface for joint source-channel coding and network communication," *arXiv preprint arXiv:1306.0530*, 2013.

[9] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. John Wiley & Sons, 2012.

[10] A. El Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge University Press, 2011.

[11] P. Cuff, "Distributed channel synthesis," *IEEE Transactions on Information Theory*, vol. 59, no. 11, pp. 7071–7096, Nov. 2013.

[12] T. Han and S. Verdú, "Approximation theory of output statistics," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 752–772, 1993.

[13] C. E. Shannon, "A mathematical theory of communication," *Bell Sys. Tech. Journal*, vol. 27, pp. 379–423, 623–656, 1948.

[14] ——, "Coding theorems for a discrete source with a fidelity criterion," *IRE National Convention Record, Part 4*, pp. 142–163, 1959.

[15] P. Cuff and E. C. Song, "The likelihood encoder for source coding," in *Proc. 2013 IEEE Information Theory Workshop (ITW)*, Sept. 2013, pp. 1–2.

[16] M. H. Yassaee, M. R. Aref, and A. Gohari, "A technique for deriving one-shot achievability results in network information theory," in *Proc. 2013 IEEE International Symposium on Information Theory (ISIT)*, July 2013, pp. 1287–1291.

[17] I. Csiszar and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Cambridge University Press, 2011.

[18] M. H. Yassaee, M.-R. Aref, and A. Gohari, "Achievability proof via output statistics of random binning," in *Proc. 2012 IEEE International Symposium on Information Theory (ISIT)*, July 2012, pp. 1044–1048.

[19] ——, "Non-asymptotic output statistics of random binning and its applications," *arXiv preprint arXiv:1303.0695*, 2013.

[20] D. Slepian and J. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inf. Theory*, vol. 19, no. 4, pp. 471–480, July 1973.

[21] T. Cover, "A proof of the data compression theorem of slepian and wolf for ergodic sources (corresp.)," *IEEE Trans. Inf. Theory*, vol. 21, no. 2, pp. 226–228, Mar. 1975.

[22] E. C. Song, P. Cuff, and H. V. Poor, "The likelihood encoder for lossy source compression," in *Proc. 2014 IEEE International Symposium on Information Theory (ISIT)*, June 2014, pp. 2042–2046.

[23] ——, "The likelihood encoder for lossy compression," *CoRR*, vol. abs/1408.4522, 2014. [Online]. Available: http://arxiv.org/abs/1408.4522

[24] A. Lapidoth and S. Tinguely, "Sending a bivariate gaussian over a gaussian mac," *IEEE Transactions on Information Theory*, vol. 56, no. 6, pp. 2714–2752, June 2010.

[25] P. Cuff, H. H. Permuter, and T. M. Cover, "Coordination capacity," *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4181–4206, Sept. 2010.

[26] J. Jeon, "A generalized typicality for abstract alphabets," *arXiv preprint arXiv:1401.6728*, 2014.

[27] A. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Transactions on Information Theory*, vol. 22, no. 1, pp. 1–10, 1976.

[28] S.-Y. Tung, "Multiterminal source coding," Ph.D. dissertation, Cornell University, Ithaca, NY, May 1978.

[29] T. Berger, "Multiterminal source coding," *The Information Theory Approach to Communications*, vol. 229, pp. 171–231, 1977.

[30] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[31] E. C. Song, P. Cuff, and H. V. Poor, "A rate-distortion based secrecy system with side information at the decoders," in *Proc. 52th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Oct. 2014.

[32] J. Villard and P. Piantanida, "Secure lossy source coding with side information at the decoders," in *Proc. 48th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Sept. 2010, pp. 733–739.

[33] D. Gündüz, E. Erkip, and H. V. Poor, "Secure lossless compression with side information," in *Proc. IEEE Information Theory Workshop (ITW)*, May 2008, pp. 169–173.

[34] J. Villard, P. Piantanida, and S. Shamai, "Secure transmission of sources over noisy channels with side information at the receivers," *IEEE Transactions on Information Theory*, vol. 60, no. 1, pp. 713–739, Jan. 2014.

[35] E. C. Song, P. Cuff, and H. V. Poor, "A bit of secrecy for gaussian source compression," in *Proc. 2013 IEEE International Symposium on Information Theory (ISIT)*, July 2013, pp. 2567–2571.

[36] R. F. Wyrembelski and H. Boche, "Strong secrecy in compound broadcast channels with confidential messages," in *Proc. 2012 IEEE International Symposium on Information Theory (ISIT)*, July 2012, pp. 76–80.

[37] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Advances in Cryptology EUROCRYPT 2000*, ser. Lecture Notes in Computer Science, B. Preneel, Ed. Springer Berlin Heidelberg, 2000, vol. 1807, pp. 351–368. [Online]. Available: http://dx.doi.org/10.1007/3-540-45539-6_24

[38] C. Schieler, E. C. Song, P. Cuff, and H. V. Poor, "Source-channel secrecy with causal disclosure," in *Proc. 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Oct. 2012, pp. 968–973.

[39] P. J. Winzer and G. J. Foschini, "Mimo capacities and outage probabilities in spatially multiplexed optical transport systems," *Opt. Express*, vol. 19, no. 17, pp. 16 680–16 696, Aug 2011. [Online]. Available: http://www.opticsexpress.org/abstract.cfm?URI=oe-19-17-16680

[40] K. Guan, P. J. Winzer, and E. Soljanin, "Information-theoretic security in space-division multiplexed fiber optic networks," in *Proc. European Conference and Exhibition on Optical Communication.* Optical Society of America, 2012, p. Tu.3.C.4. [Online]. Available: http://www.opticsinfobase.org/abstract.cfm?URI=ECEOC-2012-Tu.3.C.4

[41] H. D. Ly, T. Liu, and Y. Liang, "Multiple-input multiple-output gaussian broadcast channels with common and confidential messages," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5477–5487, 2010.

[42] E. C. Song, E. Soljanin, P. Cuff, H. V. Poor, and K. Guan, "Rate-distortion-based physical layer secrecy with applications to multimode fiber," *IEEE Transactions on Communications*, vol. 62, no. 3, pp. 1080–1090, Mar. 2014.

[43] K. Guan, E. C. Song, E. Soljanin, P. J. Winzer, and A. M. Tulino, "Physical layer security in space-division multiplexed fiber optic communications," in *Proc. 2012 Conference Record of the Forty Sixth Asilomar Conference on Signals, Systems and Computers (ASILOMAR)*, Nov. 2012, pp. 654–658.