An Information Theoretic Approach to Provably Secure Communications

by

Jin Xu

B.E. University of Science and Technology of China, China, 2002

M.S. Institute of Automation, Chinese Academy of Sciences, China, 2005

DISSERTATION

Submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy in Electrical and Computer Engineering

in the Graduate School of Syracuse University

April 2010

Approved _____

Professor Biao Chen

Date _____

Abstract

With the rapid deployment of new wireless devices and pervasive use of wireless data and voice services, the demand for reliable and secure communications is becoming more and more urgent. The focus of this thesis is on the fundamental trade-off among throughput, reliability, and security of various wireless networks. Our study adopts the notion of provable security from an information theoretic perspective. Using equivocation to measure the confidentiality of messages, we establish, for various communication models, the fundamental rate-equivocation trade-off.

We first study capacity bounds for discrete memoryless broadcast channels with two confidential messages, which is a generalization of Csiszár and Körner's classical model. The outer bounds are proposed for the rate equivocation region of this channel model, which, together with a previously proposed inner bound, help establish the rate equivocation region of several classes of discrete memoryless broadcast channels. Furthermore, specializing to the general broadcast channel by removing the confidentiality constraint, the proposed outer bounds reduce to new capacity outer bounds for the discrete memorylesss broadcast channel.

Next, we consider another variation of Csiszár and Körner's model. The transmitter sends both a confidential message and a non-confidential message (public message) to the intended receiver. While the unintended receiver should be kept ignorant from the confidential message, we do not impose the requirement that the public message needs to be perfectly recovered by the unintended receiver. This more liberal

treatment of the non-confidential message is perhaps a more reasonable model than Csiszár and Körner's model where the non-confidential message (common message) is required to be decoded by both receivers. A single-letter characterization of the achievable rate equivocation region of this model is given and the result is then extended to the case when an extra secret key is available to the transmitter and the intended receiver.

Utilizing the developed framework of broadcast channels with confidential and public messages, we further study the problem of secure communication over a network in which each link may be noisy or noiseless. A single-source single-sink acyclic planar network is assumed, and the communication between the source and the sink is subject to non-cooperating eavesdropping on each link. Sufficient conditions, in terms of communication rates and network parameters, are found for provable secure communication. A constructive proof, which combines Shannon's key encryption, Wyner's random coding, and the Ford-Fulkerson algorithm, is provided which constitutes a readily implementable secure coding scheme for provably secure communications. The derived achievable rate equivocation region is tight when specializing to several special cases. In particular, when the communication network decouples into non-overlapping parallel links, the proposed encoding scheme is optimal, i.e., it achieves the secure communication capacity for such networks.

Acknowledgment

I am deeply indebted to my advisor, Dr. Biao Chen, for his endless support, encouragement, and personal guidance. Working closely with him throughout the last five years, I have been taught not only just his technical know-how, but also his way of conducting research and balancing various life priorities. I could never forget many late night email exchanges, the days he worked harder on my papers than myself, and the hundreds of times that I was mumbling vague ideas with him, the only one audience. All I can say is that he made my Ph.D. study experience a rewarding journey.

I would also give thanks to my committee members for carefully reviewing my thesis. They are (in alphabetic order) Dr. Hao Chen, Dr. Kevin Du, Dr. Yingbin Liang, Dr. Lixin Shen, and Dr. Pramod K. Varshney. Special thanks go to Dr. Varshney for serving on all the committees for my entire Ph.D. program: qualifying exam, proposal and defense committee. His mentoring and guidance are deeply appreciated.

I also thank my colleagues at Syracuse, including Yin Lin, Bin Liu, Xiaohu Shang, Yi Cao, Wei Liu, Kapil Borle, Minna Chen, Ge Xu and Fangfang Zhu. This work has benefited a lot from many stimulating talks and discussions with them. In addition, I am grateful to many friends at Syracuse who have made my years spent at Syracuse University so enjoyable. Special thanks to the couple, Xiaowen Lu and Min Xu, who,

from day one, were there helping me in every thing. I also like to thank Tianyun Zhang, Dr. Biao Chen's wife, for so many sweet parties held in their house and delicious dessert for our group meetings.

Finally, my most heartfelt gratitude goes to the three most special people, my father Youxiang Xu, mother Chunrong Gu, and sister Min Xu. I appreciate their deep and continuous support. This work is dedicated to them.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

The advances of today's communication networks, both wired and wireless, have dramatically improved its accessibility and affordability. As such, people have become increasingly dependent on their ability to stay connected, both in their personal and professional lives. Maintaining the integrity and security of the information flowing over the ever pervasive networks is thus of critical importance for both privacy and business or national security reasons.

Existing mechanisms to ensure the communication network security largely rely on the symmetric key and public/private key infrastructures that were developed since 1970s with the advent of computer networks. While they have been fairly successful in providing robust security performance against some common security threats, its vulnerability has also been exploited through various deliberate attacks [4]. For example, RSA-129 Factoring Challenge Project is successfully attacked in 1994;

DES system is cracked in 1997; Netscape SSL RC4 is even successfully attacked within months of its release.

These examples are not entirely surprising; these existing security schemes are based primarily on some unproven hypotheses on the difficulty of certain problems, thus in principle all of them can possibly be broken down. Even without taking into account potential advances of cryptanalysis, the exponentially increasing computing power as predicted by Moore's law kept raising the bar for data security. More importantly, the emergence of potentially new computing paradigms may completely change the entire landscape. For example, under the quantum computing regime, factoring prime numbers requires only polynomial time (i.e., Shor's algorithm). This will render the current RSA-based [5] public-key cryptographic primitives obsolete.

Therefore, it is imperative for us to give more attention to the notion of unconditional (provable) security, where we can assume that adversaries have infinite computing power. Such notion of provable security was pioneered by Claude E. Shannon in 1948 [6] from an information theoretic perspective. This thesis intends to apply this strong notion of security to more sophisticated communication systems. Contrary to existing key primitive based approaches, security is assured even if the adversary is assumed to have infinite computing power. In the following, we review related works about the information-theoretic security.

1.1 Shannon Cipher System

A Shannon cipher system, as depicted in Fig. 1.1, involves two communicating parties (Bob and Alice) and an eavesdropper (Eve). A private key K is shared by Bob and Alice that is completely unknown to Eve. Bob uses K to encrypt the secret message S into ciphertext C while Alice uses K to decipher C back to S. In information theoretic terms, perfect secrecy is said to be achieved when $H(S|C) = H(S)$ but $H(S|C, K) = 0$ where $H(\cdot)$ is the usual Shannon entropy function (see [7]). Thus, given C alone, Eve gains no information about S, while if both C and K are given (as for Alice), S can be completely recovered. Shannon established in [1] a somewhat surprising result: perfect secrecy is guaranteed only if $H(K) \geq H(S)$, i.e., the key size is at least as large as the source message.

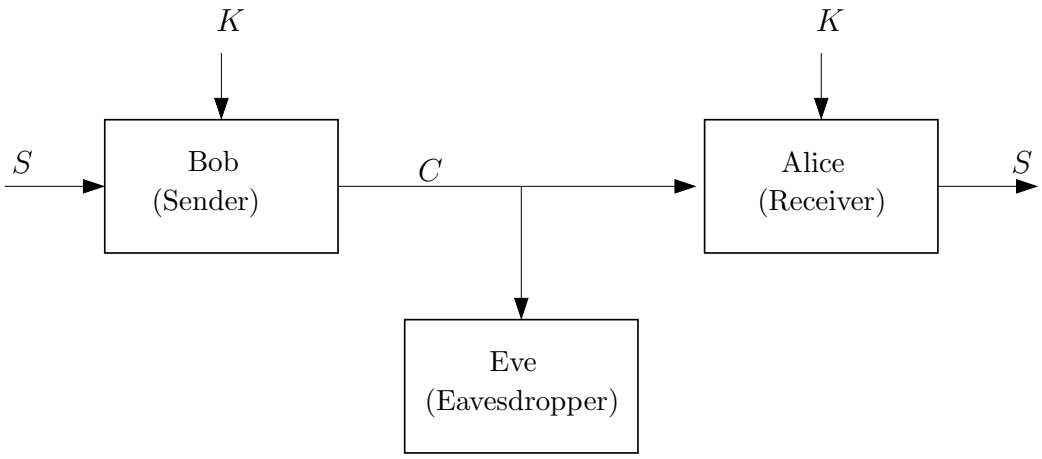


Figure 1.1: The Shannon cipher system.

Here, the notion of secrecy is in the strongest possible sense: security is inde-

pendent of any hypothesis on the intractability of certain computational problem or any assumption of limited computing power for Eve. While this establishes provable security of the so-called one-time pad, the excessive requirement on the key size essentially forebodes a negative result: any key-based encryption scheme is almost always *not* provably secure as the key size requirement precludes any hope of dynamic key exchange. It is inconceivable to be able to store infinite length private key or to have steady and secure key exchange/extraction to sustain secure communication in the digital era.

1.2 Provable Security for Noisy Channels

Although Shannon showed that a one-time pad can achieve perfect secrecy as a cryptographic encoding technique, his result appears to rule out the pursuit of absolute security in light of its excessive key requirement. Wyner in his seminal work in 1975 [2] rekindled the promise of achieving provable security in practical communication systems. The pivot lies in the very basic model assumed in Shannon's original work [1]: in Shannon's model, the encrypted message C is available error free to both intended and unintended receivers. In the context of wireless transmission, for example, this error free assumption is not realistic. Instead Wyner studied a noisy communication system that is being eavesdropped via another noisy channel. Fig. 1.2 portrays this scenario using binary symmetric broadcast channel (BSBC) models, where the two friendly users (Bob and Alice) share information over a main noisy channel (V^n is

the binary noise) and a passive eavesdropper (Eve) observes a degraded version of the information through a wiretap channel ($V^n + W^n$ is the worse noise).

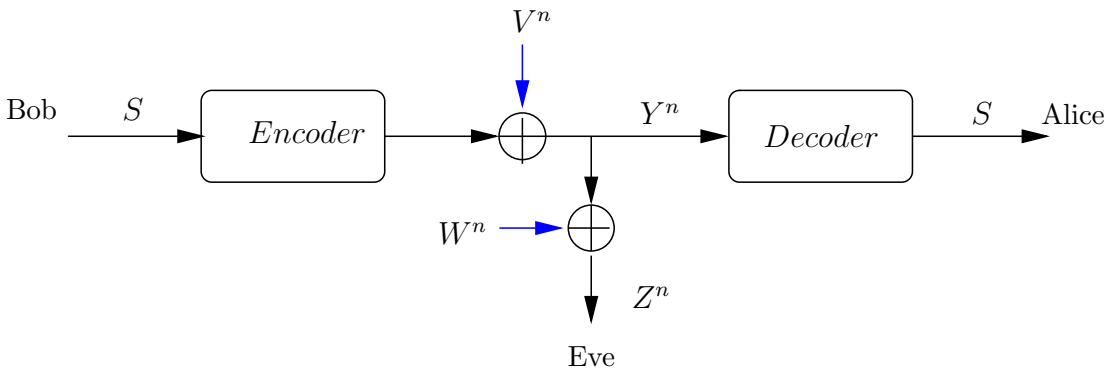


Figure 1.2: Wyner's wiretap channel model.

Wyner established in [2] that provably secure communication can indeed be achieved for communication over noisy wiretap channels *in the absence of private keys*. Wyner's breakthrough lies on its innovative use of channel coding. Instead of considering encryption and error correction as two separate function layers, Wyner adopts the random coding approach that can simultaneously achieve reliability (i.e., error correction) and security (i.e., data encryption). The key idea of random coding is to utilize the excessive channel capacity of the main channel over the wiretap channel. Since the wiretap channel is a degraded channel of the main channel, the transmitter can prudently choose a codeword of suitable rate such that it can be reliably recovered by the better (main) channel but is completely protected against the eavesdropper who sees a worse channel. This idea is illustrated pictorially in Fig. 1.3. Through information-theoretic argument, Wyner proved that if the communication rate is be-

low the so-called excess capacity between the main channel and wiretap channel, reliable and *provable* secure communication is possible through random coding.

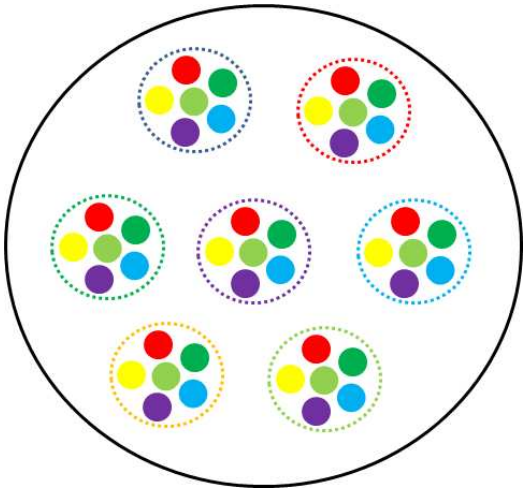
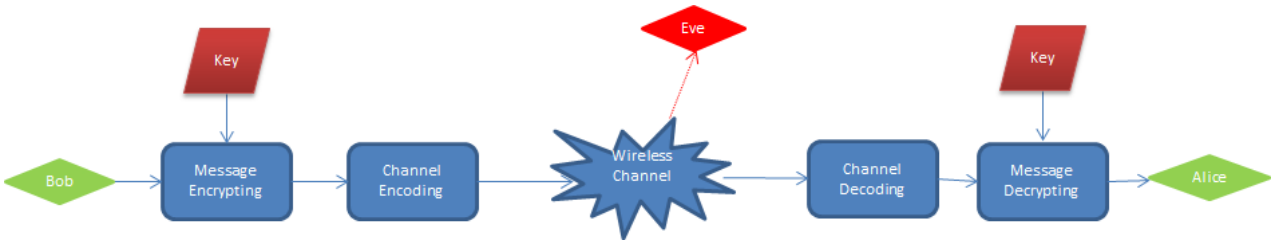


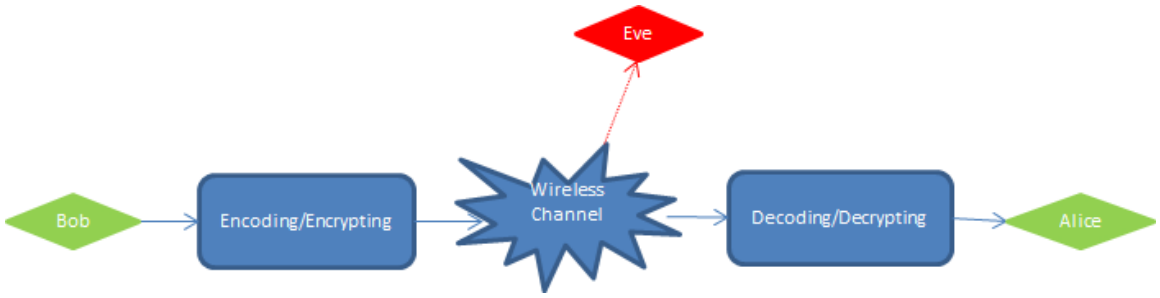
Figure 1.3: An illustration of random coding of BSBC. The main channel has better resolution so that the colors of these dots in the codebook space (i.e. the information rate) can be recovered by the main channel while the eavesdropper can't distinguish due to the worse channel.

Wyner's work pioneered research on physical layer security of wireless communication system and various extensions and generalizations to a broad range of wireless channel models have been reported in the literature (see [8] and references therein). One of the major innovative points of Wyner's approach to provable security, as alluded before, is the integration of channel coding and message encryption through the use of random coding. This contrasts with the conventional approach where data encryption is carried out at the application layer which is far above the physical layer

where channel coding is implemented. This contrast is illustrated in Fig. 1.4.



(a) Conventional layered design of secure communication



(b) Physical layer secure communication

Figure 1.4: The comparison of the conventional encryption based secure communication and the physical layer secure communication.

Wyner's model, while capturing the noisy nature of wireless medium, is somewhat restrictive because of its assumption of a degraded channel model. This assumption was later relaxed by Csiszár and Körner in their celebrated work in [3] where a general broadcast channel is studied. In their model, in addition to a confidential message that is to be protected from the unintended receiver, there is also a non-confidential message (referred to as the common message in the context of the classical broadcast channel) that is required to be decoded by both receivers. In Fig. 1.5, we summarize the difference of the three classical models studied by Shannon, Wyner and Csiszár

and Körner, respectively.

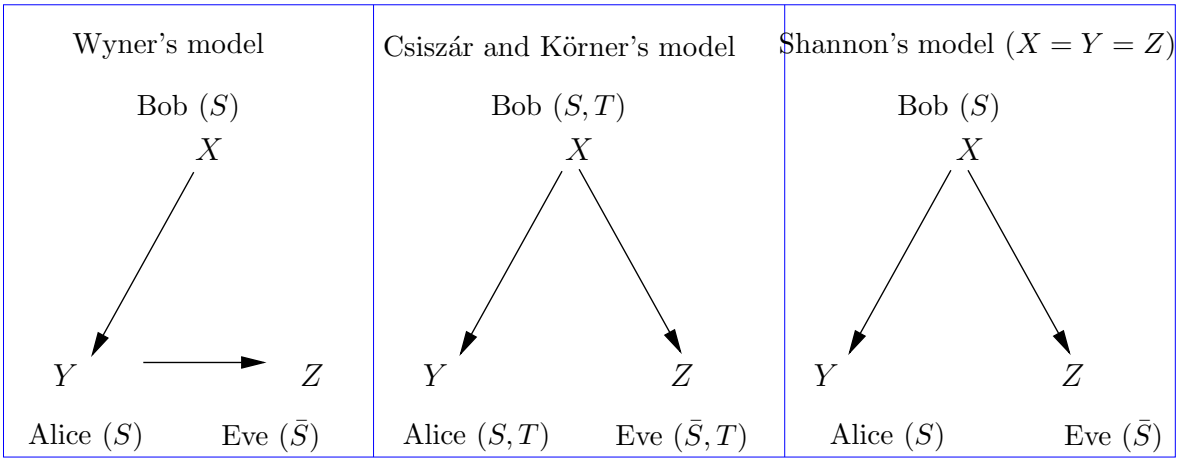


Figure 1.5: Summary of classical models studied in [1–3]. S, T are the confidential and common messages respectively; $\bar{S}$ means S is required to be protected against Eve; X, Y, Z are the channel input and outputs.

Since then, there have been considerable efforts on generalizing these studies to various multi-user channel models (see [8–24] and references therein). The obtained results are rather encouraging and our understanding of the fundamental trade-off between rate and security for many classical multi-user network models have been advanced significantly. However, the results are obtained largely for systems with a very small number of nodes and in most cases, the ways the results were derived do not provide any insight on how these trade-offs can be achieved. This is not surprising, since the characterization of communication limits of a number of wireless channel modes *without the security constraint* still remains open. This thesis makes

progress in the following two aspects. First, we study a generalization and a variation of the classical broadcast channels with confidential messages and characterize the rate-confidentiality trade-offs. Second, we consider a very general wireless or wired networks in which communications between two nodes go through multiple nodes in the network and characterize the rate-equivocation trade-off under non-cooperative eavesdropping. We now give a detailed description of this thesis below.

1.3 Outline of Thesis

The rest of the dissertation is divided into three major parts. In Chapter 2, we study a generalized Csiszár and Körner's model, namely discrete memoryless broadcast channels with confidential messages. Instead of assuming one single confidential message for one of the two users, we consider two confidential messages, and each of the two is to be decoded by its intended receiver but to be kept secret from the unintended receiver. In addition, a common message is transmitted that is to be decoded by both receivers. We propose capacity out bounds for our channel model, which, together with a previously proposed inner bound, help establish the rate equivocation region of several classes of discrete memoryless broadcast channels with two confidential messages. They include the less noisy, deterministic, and semi-deterministic broadcast channels. Furthermore, by removing the confidentiality constraint, the proposed outer bounds reduce to new capacity outer bounds for the classical discrete memory broadcast channel. The results in this chapter is also reported in [25].

In Chapter 3, we present the so-called broadcast channel with confidential and public message (BCCP) model as an alternative to the classical model of Csiszár and Körner. The difference lies on BCCP's more liberal treatment of the non-confidential message - the requirement that the unintended receiver reliably decode the non-confidential message is dropped, which results in an enlarged rate equivocation region. This is perhaps a more reasonable model than Csiszár and Körner's model where the non-confidential message is required to be decoded by both receivers. This BCCP framework is then extended to systems where a secret key is available to the intended transceiver pair, the so-called secret key enhanced BCCP model.

In Chapter 4, we further study the problem of secure communication over networks. Particularly, a single-source single-sink acyclic planar network is considered, where the single source intends to securely deliver a confidential message to the single sink through this network and each link in the network is subject to non-cooperating eavesdropping. We develop an intuitive and efficient coding scheme to achieve the secrecy, which incorporates, in a natural yet creative way, the one-time pad scheme into the Ford-Fulkerson algorithm which was developed for the celebrated Max-flow Min-cut theorem. This explicit encoding and routing scheme leads to an achievable rate equivocation region for the secure coding over network model which is shown to be tight when specializing to a network of non-overlapping parallel links.

Finally, we conclude in Chapter 5 by summarizing the main contributions of this thesis and discussing our future work.

1.4 Notations

In the following, we introduce notations which will be used throughout this thesis.

Term	Description
X	a discrete random variable
$\mathcal{X}$	the sample space of a discrete random variable X
x	a realization of a random variable X
X^n	a vector of random variables, with time from 1 to n
X_i	a random variable in time i
$X \sim p(x)$	The probability mass function of X is $p(x)$
$X \sim \mathcal{N}(\mu, \sigma^2)$	X is Gaussian distributed with mean μ and variance σ^2
$H(X)$	entropy function of X
$I(X;Y)$	mutual information between X and Y
$C(.)$	Gaussian channel capacity, $C(x) = \frac{1}{2}\log(1+x)$
$h(.)$	function, $h(\lambda) = -\lambda \log \lambda - (1-\lambda)\log(1-\lambda)$
$[.]^+$	function $[x]^+ = \max\{x, 0\}$
RV	random variable
SNR	signal to noise ratio
BSBC	binary symmetric broadcast channel
GWC	Gaussian wiretap channel
DMBC	discrete memoreless broadcast channel
DMBC-2CM	discrete memoreless broadcast channel with two confidential messages and one common message
BCCC	broadcast channel with one confidential message and one common message
BCCP	broadcast channel with one confidential message and one public message

Table 1.1: Notions used in this thesis.

Chapter 2

Capacity Bounds for Broadcast Channels with Confidential Messages

In this chapter we study a generalization of Csiszár and Körner's broadcast channel with confidential messages. Specifically, we consider a two-user broadcast channel with one common message and two confidential messages, one for each receiver. We establish outer bounds to the rate equivocation region of this channel. Our proposed outer bounds, together with a previously proposed achievable region, help establish the rate equivocation region of several classes of discrete memoryless broadcast channels with two confidential messages. Furthermore, specializing to the general broadcast channel by removing the secrecy constraint, our proposed outer bounds reduce to new capacity outer bounds for the discrete memoryless broadcast channels.

2.1 Introduction

In this chapter, we generalize Csiszár and Körner's model by considering discrete memoryless broadcast channels where each receiver needs to decode its own private message as well as a common message. We refer to this model as simply the DMBC with two confidential messages (DMBC-2CM). Fig. 2.1 illustrates the differences among the three models: Wyner's wiretap channel model, Csiszár and Körner's model, and the DMBC-2CM model. The DMBC-2CM model was first studied by Liu *et al* [21, 26] where, in the absence of a common message, the authors imposed the perfect secrecy constraint and obtained inner and outer bounds for the perfect secrecy capacity region.

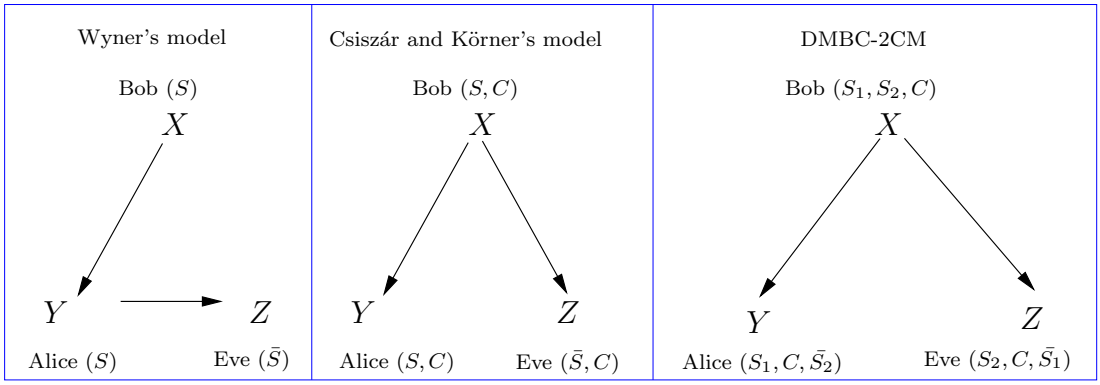


Figure 2.1: Variations to broadcast channel with confidential messages

We study capacity bounds to the rate equivocation region for the general DMBC-2CM. Our model generalizes that of [21] by including a common message. More importantly, we do not impose the perfect secrecy constraint and study instead the

general trade-off among the rates for reliable communication and the securities of confidential messages. Study of this general model allows us to unify many existing results. We first review the achievable rate equivocation region originally proposed in [27] that generalizes Csiszár and Körner's rate equivocation region in [3] where only a single confidential message is to be communicated, Liu *et al*'s achievable rate region under perfect secrecy constraint [21], and Marton and Gel'fand-Pinsker's achievable rate region for the general DMBC [28, 29]. We then describe our proposed outer bounds to the rate equivocation region of the DMBC-2CM which generalize existing outer bounds for various special cases of the DMBC-2CM. In particular, it reduces to Csiszár and Körner's rate equivocation region for the DMBC with only one confidential message and Liu *et al*'s outer bound to the capacity region with perfect secrecy. The proposed inner and outer bounds coincide for the less noisy, deterministic, and semi-deterministic DMBC-2CM, thus settle the rate equivocation region for these channels. Furthermore, in the absence of secrecy constraints, our proposed outer bounds specialize to new outer bounds to the capacity region of the general DMBC. Comparison with other outer bounds proposed in [28, 30–35] are discussed.

The rest of this chapter is organized as follows. In Section 2.2, we give the channel model and review relevant existing results. In Section 2.3, we review an achievable rate equivocation region for the DMBC-2CM and show that it coincides with various existing results under respective conditions. In Section 2.4, we present our outer bounds to the rate equivocation region of the DMBC-2CM. We prove that the outer

bound is tight for the less noisy, deterministic, and semi-deterministic DMBC-2CM. We also discuss the induced outer bound to the general DMBC and its subset relations with existing capacity outer bounds. Finally, we conclude in Section 2.5.

2.2 Problem Formulation and Previous Results

2.2.1 Problem statement

A discrete memoryless broadcast channel with confidential messages $\mathcal{K}$ is a quadruple $(\mathcal{X}, p, \mathcal{Y}_1, \mathcal{Y}_2)$, where $\mathcal{X}$ is the finite input alphabet set, $\mathcal{Y}_1$ and $\mathcal{Y}_2$ are two finite output alphabet sets, and p is the channel transition probability $p(y_1, y_2|x)$. We assume that the channels are memoryless, i.e.,

$$p(y_1^n, y_2^n|x^n) = \prod_{i=1}^{n} p(y_{1i}, y_{2i}|x_i) \tag{2.1}$$

where,

$$x^n = (x_1, \cdots, x_n) \in \mathcal{X}^n, \tag{2.2}$$

$$y_1^n = (y_{11}, \cdots, y_{1n}) \in \mathcal{Y}_1^n, \tag{2.3}$$

$$y_2^n = (y_{21}, \cdots, y_{2n}) \in \mathcal{Y}_2^n. \tag{2.4}$$

Let $\mathcal{M}_0 = \{1, 2, \cdots, M_0\}$ be the common message set, $\mathcal{M}_1 = \{1, 2, \cdots, M_1\}$ and $\mathcal{M}_2 = \{1, 2, \cdots, M_2\}$ be user 1 and user 2's private message sets, and W_0, W_1, W_2 are the respective message variables on the sets $\mathcal{M}_0, \mathcal{M}_1, \mathcal{M}_2$. We assume stochastic encoding as randomization may increase secrecy [3]. A *stochastic* encoder f with

block length n for the channel $\mathcal{K}$ is specified by $P(x^n|w_1, w_2, w_0)$, where $x^n \in \mathcal{X}^n$, $w_1 \in \mathcal{M}_1$, $w_2 \in \mathcal{M}_2$, $w_0 \in \mathcal{M}_0$ and

$$\sum_{x^n} P(x^n|w_1, w_2, w_0) = 1. \tag{2.5}$$

Here $P(x^n|w_1, w_2, w_0)$ is the probability that the message triple (w_1, w_2, w_0) is encoded as the channel input x^n. The two decoders are a pair of mappings

$$\varphi_1 : \quad \mathcal{Y}_1^n \to \mathcal{M}_1 \times \mathcal{M}_0,$$

$$\varphi_2 : \quad \mathcal{Y}_2^n \to \mathcal{M}_2 \times \mathcal{M}_0.$$

The average probabilities of decoding error of this channel are defined as

$$P_{e,1}^{(n)} \stackrel{\triangle}{=} \frac{1}{M_1 M_2 M_0} \sum_{w_1,w_2,w_0} P(\{\varphi_1(y_1^n) \neq (w_1, w_0)\}|(w_1, w_2, w_0) \text{ sent}), \tag{2.6}$$

$$P_{e,2}^{(n)} \stackrel{\triangle}{=} \frac{1}{M_1 M_2 M_0} \sum_{w_1,w_2,w_0} P(\{\varphi_2(y_2^n) \neq (w_2, w_0)\}|(w_1, w_2, w_0) \text{ sent}). \tag{2.7}$$

A rate quintuple $(R_0, R_1, R_2, R_{e1}, R_{e2})$ is said to be achievable if there exist message sets $\mathcal{M}_1$, $\mathcal{M}_2$, $\mathcal{M}_0$ and encoder-decoders $(f, \varphi_1, \varphi_2)$ such that $P_{e,1}^n \to 0$ and $P_{e,2}^n \to 0$, where for $a = 0, 1, 2$,

$$\lim_{n\to\infty} \frac{1}{n} \log ||\mathcal{M}_a|| = R_a \tag{2.8}$$

$$\lim_{n\to\infty} \frac{1}{n} H(W_1|Y_2^n) \geq R_{e1} \tag{2.9}$$

$$\lim_{n\to\infty} \frac{1}{n} H(W_2|Y_1^n) \geq R_{e2} \tag{2.10}$$

The rate equivocation region of the DMBC-2CM is the closure of the union of all achievable rate quintuples $(R_0, R_1, R_2, R_{e1}, R_{e2})$. Our objectives in this chapter are to

obtain meaningful bounds to the rate equivocation region for the DMBC-2CM and to connect our obtained bounds with prior results for various special cases of the channel model.

The DMBC-2CM model is illustrated in Fig. 2.2. We note that in the absence of W_2, the model reduces to Csiszár and Körner's model with only one confidential message [3]. On the other hand, in the absence of confidentiality constraints (i.e., $H(W_1|Y_2^n)$ and $H(W_2|Y_1^n)$), our model reduces to the classical DMBC with two private messages and one common message [29].

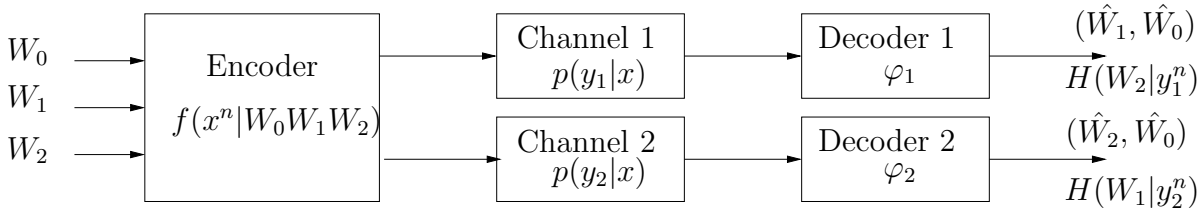


Figure 2.2: Broadcast channel with two confidential messages W_1, W_2 and one common message W_0

Before proceeding, we introduce the following definitions. Let $Z = (U, V_1, V_2, X, Y_1, Y_2)$ be a set of random variables such that $X \in \mathcal{X}$, $Y_1 \in \mathcal{Y}_1$, $Y_2 \in \mathcal{Y}_2$, and the corresponding $p(y_1, y_2|x)$ is the channel transition probability of the DMBC-2CM. Define

- $\mathcal{Q}_1$ to be the set of Z whose joint distribution factors as

$$p(u, v_1, v_2, x, y_1, y_2) = p(u, v_1, v_2)p(x|u, v_1, v_2)p(y_1, y_2|x).$$

Thus any $Z \in \mathcal{Q}_1$ satisfies the Markov chain condition $UV_1V_2 \to X \to Y_1Y_2$.

- $\mathcal{Q}_2$ to be the set of Z whose joint distribution factors as

$$p(u, v_1, v_2, x, y_1, y_2) = p(u)p(v_1, v_2|u)p(x|v_1, v_2)p(y_1, y_2|x).$$

  Thus any $Z \in \mathcal{Q}_2$ satisfies the Markov chain condition $U \to V_1V_2 \to X \to Y_1Y_2$.

- $\mathcal{Q}_3$ to be the set of Z whose joint distribution factors as

$$p(u, v_1, v_2, x, y_1, y_2) = p(v_1)p(v_2)p(u|v_1, v_2)p(x|u, v_1, v_2)p(y_1, y_2|x).$$

  $\mathcal{Q}_3$ results in the same Markov chain as $\mathcal{Q}_1$ except that V_1 and V_2 are independent of each other.

Clearly, $\mathcal{Q}_2 \subseteq \mathcal{Q}_1$ and $\mathcal{Q}_3 \subseteq \mathcal{Q}_1$.

2.2.2 Related work

In this section, we review several existing results related to the present work.

Csiszár and Körner characterized the rate equivocation region [3] for broadcast channels with a common message for both users and a single confidential message intended for one of the two users. Without loss of generality (WLOG), we assume that W_2 is absent from our model. The result is summarized below.

Proposition 1. *[3, Theorem 1] The rate equivocation region $\mathcal{R}_{CK}$ for a DMBC with one common message for both receivers and a single confidential message for the first receiver is the closed convex set consisting of those triples (R_0, R_1, R_e) for which there exist random variables $U \to V \to X \to Y_1Y_2$ such that*

$$0 \leq R_e \leq R_1 \tag{2.11}$$

$$R_e \leq I(V;Y_1|U) - I(V;Y_2|U) \tag{2.12}$$

$$R_1 + R_0 \leq I(V;Y_1|U) + \min\{I(U;Y_1), I(U;Y_2)\} \tag{2.13}$$

$$R_0 \leq \min\{I(U;Y_1), I(U;Y_2)\} \tag{2.14}$$

We note that the Markov chain condition in Proposition 1 can be relaxed, as stated below.

Lemma 1. *Let $\mathcal{R}'_{CK}$ be the convex closure of rate triples (R_1, R_e, R_0) that satisfy (2.11)-(2.14) where the random variables follow the Markov chain: $UV \to X \to Y_1Y_2$, then $\mathcal{R}_{CK} = \mathcal{R}'_{CK}$.*

Proof. $\mathcal{R}_{CK} \subseteq \mathcal{R}'_{CK}$ follows trivially from the fact that $U \to V \to X \to Y_1Y_2$ implies $UV \to X \to Y_1Y_2$. To prove $\mathcal{R}'_{CK} \subseteq \mathcal{R}_{CK}$, assume $(R_1, R_e, R_0) \in \mathcal{R}'_{CK}$ for some $UV \to X \to Y_1Y_2$. Define $U' = U$ and $V' = UV$, one can verify easily that (R_1, R_e, R_0) satisfies (2.11)-(2.14) for $U' \to V' \to X \to Y_1Y_2$, i.e., $(R_1, R_e, R_0) \in \mathcal{R}_{CK}$. □

Recently, Liu *et al* proposed an inner bound and an outer bound to the capacity region for broadcast channels with perfect-secrecy constraint on the confidential messages [21, 26]. The model in [21, 26] is in essence a DMBC-2CM without a common message. In their model, each user has its own confidential message that is to be completely protected from the other user. The proposed achievable region and outer bound are given in Propositions 2 and 3, respectively.

Proposition 2. *[21, Theorem 4] Let $\mathcal{R}_{LMSY-I}$ denote the union of all (R_1, R_2) satisfying*

$$\begin{aligned} 0 \leq R_1 &\leq I(V_1;Y_1|U) - I(V_1;Y_2|V_2U) - I(V_1;V_2|U) \\ 0 \leq R_2 &\leq I(V_2;Y_2|U) - I(V_2;Y_1|V_1U) - I(V_1;V_2|U) \end{aligned} \tag{2.15}$$

over all random variables $(U, V_1, V_2, X, Y_1, Y_2) \in \mathcal{Q}_2$. Any rate pair $(R_1, R_2) \in \mathcal{R}_{LMSY-I}$ is achievable for the DMBC-2CM without a common message and with perfect secrecy for the confidential messages, i.e., $R_0 = 0$, $R_1 = R_{e1}$, and $R_2 = R_{e2}$.

Proposition 3. *[21, Theorem 3] An outer bound to the capacity region for the DMBC-2CM without a common message and with the perfect secrecy constraint is the set of all (R_1, R_2) satisfying*

$$0 \leq R_1 \leq \min\{I(V_1;Y_1|U) - I(V_1;Y_2|U), I(V_1;Y_1|V_2U) - I(V_1;Y_2|V_2U)\} \tag{2.16}$$

$$0 \leq R_2 \leq \min\{I(V_2;Y_2|U) - I(V_2;Y_1|U), I(V_2;Y_2|V_1U) - I(V_2;Y_1|V_1U)\} \tag{2.17}$$

for some $(U, V_1, V_2, X, Y_1, Y_2) \in \mathcal{Q}_2$. We denote by $\mathcal{R}_{LMSY-O}$ this outer bound.

In the absence of the secrecy constraint, the present model reduces to the DMBC first introduced by Cover [36]. The capacity region for a DMBC is only known for some special cases (see [37] and references therein). The best achievable region for the general DMBC is given by Gel'fand and Pinsker in [29] which reduces to Marton's achievable region [28] for the DMBC in the absence of a common message. Capacity region outer bounds include Körner and Marton's outer bound [28], Liang and Kramer's outer bound [32,33], Nair and El Gamal's outer bound [30,31], Liang,

Kramer and Shamai (Shitz)'s outer bound [34], and most recently the outer bound proposed by Nair [35].

Marton in 1979 considered the DMBC in the absence of a common message and proposed the following achievable rate region [28].

Proposition 4. *[28, Theorem 2] Let $\mathcal{R}_{MT}$ be the union of non-negative rate pairs (R_1, R_2) satisfying $R_1, R_2 \geq 0$ and*

$$\begin{aligned} R_1 &\leq I(UV_1; Y_1) && (2.18)\\ R_2 &\leq I(UV_2; Y_2) && (2.19)\\ R_1 + R_2 &\leq \min\{I(U;Y_1), I(U;Y_2)\} + I(V_1;Y_1|U) + I(V_2;Y_2|U) \\ &\quad - I(V_1;V_2|U) && (2.20) \end{aligned}$$

for some $(U, V_1, V_2, X, Y_1, Y_2) \in \mathcal{Q}_1$. Then $\mathcal{R}_{MT}$ is an achievable rate region for the DMBC without a common message.

Gel'fand and Pinsker [29] generalized Marton's model by considering the DMBC with a common message. The achievable rate region they proposed is summarized below.

Proposition 5. *[29, Theorem 1] Let $\mathcal{R}_{GP}$ be the union of non-negative rate triples (R_0, R_1, R_2) satisfying*

$$\begin{aligned} R_0 &\leq \min\{I(U;Y_1), I(U;Y_2)\} && (2.21)\\ R_1 + R_0 &\leq I(V_1;Y_1|U) + \min\{I(U;Y_1), I(U;Y_2)\} && (2.22) \end{aligned}$$

$$R_2 + R_0 \leq I(V_2; Y_2|U) + \min\{I(U; Y_1), I(U; Y_2)\} \quad (2.23)$$

$$R_1 + R_2 + R_0 \leq \min\{I(U; Y_1), I(U; Y_2)\} + I(V_1; Y_1|U) + I(V_2; Y_2|U) - I(V_1; V_2|U) \quad (2.24)$$

for some $(U, V_1, V_2, X, Y_1, Y_2) \in \mathcal{Q}_1$. *Then* $\mathcal{R}_{GP}$ *is an achievable rate region for the DMBC.*

In the absence of a common message, $\mathcal{R}_{GP}$ can be shown to be equivalent to $\mathcal{R}_{MT}$ [29]. Furthermore, an equivalent definition of $\mathcal{R}_{GP}$ can be obtained by restricting $Z \in \mathcal{Q}_2$ instead of $\mathcal{Q}_1$, i.e.,

Lemma 2. *Define* $\mathcal{R}'_{GP}$ *to be the union of non-negative rate triples* (R_0, R_1, R_2) *satisfying (2.21)-(2.24) with* $Z \in \mathcal{Q}_2$, *then* $\mathcal{R}_{GP} = \mathcal{R}'_{GP}$.

The proof is similar to that for Lemma 1 and is omitted. Similarly, $\mathcal{R}_{MT}$ can also be equivalently defined using $Z \in \mathcal{Q}_2$.

Recently, a new achievable region was given by Liang and Kramer [32, 33], summarized in Proposition 6.

Proposition 6. *[33, Theorem 5] Let* $\mathcal{R}_{LKI}$ *be the union of non-negative rate triples* (R_0, R_1, R_2) *satisfying*

$$R_1 + R_0 \leq I(V_1U; Y_1) \quad (2.25)$$

$$R_2 + R_0 \leq I(V_2U; Y_2) \quad (2.26)$$

$$R_1 + R_2 + R_0 \leq \min\{I(U; Y_1), I(U; Y_2)\} + I(V_1; Y_1|U) + I(V_2; Y_2|U)$$

$$-I(V_1;V_2|U) \tag{2.27}$$

$$R_1+R_2+2R_0 \leq I(V_1U;Y_1)+I(V_2U;Y_2)-I(V_1;V_2|U) \tag{2.28}$$

for some $(U,V_1,V_2,X,Y_1,Y_2)\in\mathcal{Q}_1$. *Then* $\mathcal{R}_{LKI}$ *is an achievable rate region for the DMBC.*

While the expressions of $\mathcal{R}_{LKI}$ suggests that it may potentially enlarge the existing achievable region, it was later shown in [38] that this region is actually equivalent to $\mathcal{R}_{GP}$ in Proposition 5.

An earlier outer bound by Körner and Marton [28, Theorem 5] for the capacity region of the DMBC is subsumed by several recent outer bounds. One of the proposed outer bounds was by Liang and Kramer [32, 33], as summarized in Proposition 7.

Proposition 7. *[33, Theorem 6] If* (R_0,R_1,R_2) *is achievable, then there exists* $Z\in\mathcal{Q}_1$ *and*

$$R_0 \leq \min\{I(U;Y_1),I(U;Y_2)\}, \tag{2.29}$$

$$R_0+R_1 \leq I(V_1U;Y_1), \tag{2.30}$$

$$R_0+R_2 \leq I(V_2U;Y_2), \tag{2.31}$$

$$R_0+R_1+R_2 \leq I(X;Y_2|V_1U)+I(V_1;Y_1|U)+\min\{I(U;Y_1),I(U;Y_2)\}, \tag{2.32}$$

$$R_0+R_1+R_2 \leq I(X;Y_1|V_2U)+I(V_2;Y_2|U)+\min\{I(U;Y_1),I(U;Y_2)\}. \tag{2.33}$$

We denote this outer bound as $\mathcal{R}_{LK}$, i.e., $\mathcal{R}_{LK}$ is the union of non-negative rate triples (R_0,R_1,R_2) satisfying (2.29)-(2.33) over $Z\in\mathcal{Q}_1$. Furthermore, we can also restrict the Markov chain condition to be $Z\in\mathcal{Q}_2$, i.e.,

Lemma 3. *Define $\mathcal{R}'_{LK}$ to be the convex closure of the union of non-negative rate triples (R_0, R_1, R_2) satisfying (2.29)-(2.33) with $Z \in \mathcal{Q}_2$, then $\mathcal{R}_{LK} = \mathcal{R}'_{LK}$.*

In [30, 31], another outer bound to the capacity region of the general DMBC was given by Nair and El Gamal, as summarized in Proposition 8. This outer bound was shown to be strictly tighter than the Körner and Marton outer bound [28, Theorem 5].

Proposition 8. *[31, Theorem 2.1] If (R_0, R_1, R_2) is achievable, then there exists $Z \in \mathcal{Q}_3$ and*

$$\begin{aligned} R_0 &\leq \min\{I(U;Y_1), I(U;Y_2)\}, && (2.34)\\ R_0 + R_1 &\leq I(V_1U;Y_1), && (2.35)\\ R_0 + R_2 &\leq I(V_2U;Y_2), && (2.36)\\ R_0 + R_1 + R_2 &\leq I(V_2;Y_2|V_1U) + I(V_1U;Y_1), && (2.37)\\ R_0 + R_1 + R_2 &\leq I(V_1;Y_1|V_2U) + I(V_2U;Y_2). && (2.38) \end{aligned}$$

We denote by $\mathcal{R}_{NE}$ this new outer bound, i.e., $\mathcal{R}_{NE}$ is the union of nen-negative rate triples (R_0, R_1, R_2) satisfying (2.34)-(2.38) over $Z \in \mathcal{Q}_3$. It was shown in [39] that, in the absence of a common message ($R_0 = 0$), $\mathcal{R}_{NE}$ remains invariant if we replace $\mathcal{Q}_3$ with $\mathcal{Q}_1$.

A more recent outer bound to the capacity region for the DMBC was proposed by Liang, Kramer, and Shamai (Shitz) [34], , as summarized in Proposition 9.

Proposition 9. *[34, Theorem 1] If* (R_0, R_1, R_2) *is achievable, then there exist random variables* $(W_0, W_1, W_2, V_1, V_2, X, Y_1, Y_2)$ *whose joint distribution factors as*

$$p(w_0)p(w_1)p(w_2)p(v_1, v_2|w_0, w_1, w_2)p(x|v_1, v_2, w_0, w_1, w_2)p(y_1, y_2|x) \tag{2.39}$$

such that,

$$0 \leq R_0 \leq \min\{I(W_0; Y_1|V_1), I(W_0; Y_2|V_2)\} \tag{2.40}$$

$$R_1 \leq I(W_1; Y_1|V_1) \tag{2.41}$$

$$R_2 \leq I(W_2; Y_2|V_2) \tag{2.42}$$

$$R_0 + R_1 \leq \min\{I(W_0W_1; Y_1|V_1), I(W_1; Y_1|W_0V_1V_2) + I(W_0V_1; Y_2|V_2)\} \tag{2.43}$$

$$R_0 + R_2 \leq \min\{I(W_0W_2; Y_2|V_2), I(W_2; Y_2|W_0V_1V_2) + I(W_0V_2; Y_1|V_1)\} \tag{2.44}$$

$$R_0 + R_1 + R_2 \leq I(W_1; Y_1|W_0W_2V_1V_2) + I(W_0W_2V_1; Y_2|V_2) \tag{2.45}$$

$$R_0 + R_1 + R_2 \leq I(W_2; Y_2|W_0W_1V_1V_2) + I(W_0W_1V_2; Y_1|V_1) \tag{2.46}$$

$$R_0 + R_1 + R_2 \leq I(W_1; Y_1|W_0W_2V_1V_2) + I(W_2; Y_2|W_0V_1V_2) + I(W_0V_1V_2; Y_1) \tag{2.47}$$

$$R_0 + R_1 + R_2 \leq I(W_2; Y_2|W_0W_1V_1V_2) + I(W_1; Y_1|W_0V_1V_2) + I(W_0V_1V_2; Y_2), \tag{2.48}$$

where X *is a deterministic function of* $(W_0, W_1, W_2, V_1, V_2)$*, and* W_0, W_1, W_2 *are uniformly distributed.*

We refer to this new outer bound as $\mathcal{R}_{LKS}$.

2.3 An Achievable Rate Equivocation Region

In this section, we review an achievable rate equivocation region for the DMBC-2CM, given in Theorem 1, and first proposed by Cao and Chen in [27]. The coding scheme combines binning, superposition coding, and rate splitting. For the rate constraints, the binning approach in [40] is supplemented with superposition coding to accommodate the common message. An additional binning is introduced for achieving confidentiality of private messages. We note that this double binning technique has been used by various authors for communications involving confidential messages (see, e.g., [21, 41]).

Different from that of [21], we make explicit use of rate splitting for the two private messages in order to boost the rates R_1 and R_2. We note that this rate splitting was implicitly used in [3] (specifically, the proof of Lemma 3 in [3]). To be precise, we split the private message $W_1 \in \{1, \cdots, 2^{nR_1}\}$ into $W_{11} \in \{1, \cdots, 2^{nR_{11}}\}$ and $W_{10} \in \{1, \cdots, 2^{nR_{10}}\}$, and $W_2 \in \{1, \cdots, 2^{nR_2}\}$ into $W_{22} \in \{1, \cdots, 2^{nR_{22}}\}$ and $W_{20} \in \{1, \cdots, 2^{nR_{20}}\}$, respectively. W_{11} and W_{22} are only to be decoded by their intended receivers while W_{10} and W_{20} are to be decoded by both receivers. Notice that this rate splitting is typically used in interference channels to achieve a larger rate region as it enables interference cancellation at the receivers. It is clear that this rate splitting is prohibited if perfect secrecy is required as in [21].

The achievable rate equivocation region for the DMBC-2CM is formally stated below.

Theorem 1. *Let $\mathcal{R}_I$ be the union of all non-negative rate quintuple $(R_0, R_1, R_2, R_{e1}, R_{e2})$ satisfying*

$$\begin{aligned}
R_{e1} &\leq R_1 && (2.49)\\
R_{e2} &\leq R_2 && (2.50)\\
R_0 &\leq \min\{I(U;Y_1), I(U;Y_2)\} && (2.51)\\
R_1 + R_0 &\leq I(V_1;Y_1|U) + \min\{I(U;Y_1), I(U;Y_2)\} && (2.52)\\
R_2 + R_0 &\leq I(V_2;Y_2|U) + \min\{I(U;Y_1), I(U;Y_2)\} && (2.53)\\
R_1 + R_2 + R_0 &\leq I(V_1;Y_1|U) + I(V_2;Y_2|U) - I(V_1;V_2|U) \\
&\quad + \min\{I(U;Y_1), I(U;Y_2)\} && (2.54)\\
R_{e1} &\leq [I(V_1;Y_1|U) - I(V_1;Y_2V_2|U)]^+ && (2.55)\\
R_{e2} &\leq [I(V_2;Y_2|U) - I(V_2;Y_1V_1|U)]^+ && (2.56)
\end{aligned}$$

over all $(U, V_1, V_2, X, Y_1, Y_2) \in \mathcal{Q}_2$, where $[x]^+ = \max\{x, 0\}$. Then $\mathcal{R}_I$ is an achievable rate region for the DMBC-2CM.

The interpretation of the auxiliary variables is as follows. The auxiliary variable U represents all the common information, i.e., the triple (W_{10}, W_{20}, W_0); V_1 and V_2 represent W_{11} and W_{22} respectively.

The region $\mathcal{R}_I$ remains the same if we replace $\mathcal{Q}_2$ with $\mathcal{Q}_1$. Formally,

Lemma 4. *Define $\mathcal{R}'_I$ to be the union of all non-negative rate quintuple $(R_1, R_2, R_0, R_{e1}, R_{e2})$ satisfying (2.49)-(2.56) over $Z \in \mathcal{Q}_1$, then $\mathcal{R}_I = \mathcal{R}'_I$.*

Proof. The fact that $\mathcal{R}_I \subseteq \mathcal{R}'_I$ follows trivially from $\mathcal{Q}_2 \subseteq \mathcal{Q}_1$.

We now show $\mathcal{R}'_I \subseteq \mathcal{R}_I$. Assume $(R_1, R_2, R_0, R_{e1}, R_{e2}) \in \mathcal{R}'_I$, i.e., there exists $(U, V_1, V_2, X, Y_1, Y_2) \in \mathcal{Q}_1$ such that $(R_1, R_2, R_0, R_{e1}, R_{e2})$ satisfies (2.49)-(2.56). The proof is completed by definining $U' = U$, $V'_1 = UV_1$, and $V'_2 = UV_2$ and observe that the same $(R_1, R_2, R_0, R_{e1}, R_{e2})$ satisfies (2.49)-(2.56) for $(U', V'_1, V'_2, X, Y_1, Y_2) \in \mathcal{Q}_2$. □

This achievable rate equivocation region unifies many existing results which we enumerate below.

2.3.1 Csiszár and Körner's region

In [3], Csiszár and Körner characterized the rate equivocation region for broadcast channels with a single confidential message and a common message.

By setting $R_2 = 0$ and $R_{e2} = 0$ in Theorem 1, it is easy to see that $\mathcal{R}_I$ reduces to Csiszár and Körner's capacity region $\mathcal{R}_{CK}$ described in Proposition 1.

2.3.2 Liu et al's region

In [21], Liu *et al* proposed an achievable rate region for broadcast channel with confidential messages where there are two private message and no common message. In addition, the private messages are to be perfectly protected from the unintended receivers.

By setting $R_1 = R_{e1}$, $R_2 = R_{e2}$ and $R_0 = 0$ in Theorem 1, one can easily check that $\mathcal{R}_I$ reduces to Liu *et al*'s achievable rate region R_{LMSY-I} described in Proposition 2.

2.3.3 Gel'fand and Pinsker's region

In [29], Gel'fand and Pinkser generalized Marton's result by proposing an achievable rate region for broadcast channels with a common message. If we remove the secrecy constraints in our model by setting $R_{e1} = 0$ and $R_{e2} = 0$ in Theorem 1, we obtain an achievable rate region for the general DMBC, denoted by $\hat{\mathcal{R}}$, defined by (2.51)-(2.54) with $U \to (V_1, V_2) \to X \to (Y_1, Y_2)$. From Proposition 5 and Lemma 2, $\hat{\mathcal{R}} = \mathcal{R}_{GP}$.

The proofs in [28, 29] both use a corner point approach. A binning approach was used in [40] to prove a weakened version of [28, Theorem 2]. The proof introduced in the present chapter, by stripping out all confidentiality constraints, provides a new way to prove the general achievable rate region of the DMBC, [29, Theorem 1] and [28, Theorem 2], along the line of [40].

2.4 Outer Bounds

We now present several outer bounds to the rate equivocation region for DMBC-2CM. Define $\mathcal{R}_{O1}$ to be the union, over all $Z \in \mathcal{Q}_1$, of non-negative rate quintuple $(R_0, R_1, R_2, R_{e1}, R_{e2})$ satisfying

$$R_{e1} \leq R_1 \tag{2.57}$$

$$
\begin{aligned}
R_{e2} &\leq R_2 && (2.58)\\
R_0 &\leq \min\{I(U;Y_1), I(U;Y_2)\} && (2.59)\\
R_0 + R_1 &\leq I(V_1;Y_1|U) + \min\{I(U;Y_1), I(U;Y_2)\} && (2.60)\\
R_0 + R_2 &\leq I(V_2;Y_2|U) + \min\{I(U;Y_1), I(U;Y_2)\} && (2.61)\\
R_0 + R_1 + R_2 &\leq I(V_2;Y_2|V_1U) + I(V_1;Y_1|U) + \min\{I(U;Y_1), I(U;Y_2)\} && (2.62)\\
R_0 + R_1 + R_2 &\leq I(V_1;Y_1|V_2U) + I(V_2;Y_2|U) + \min\{I(U;Y_1), I(U;Y_2)\} && (2.63)\\
R_{e1} &\leq \min\{[I(V_1;Y_1|U) - I(V_1;Y_2|U)]^+, \\
&\qquad [I(V_1;Y_1|V_2U) - I(V_1;Y_2|V_2U)]^+\} && (2.64)\\
R_{e2} &\leq \min\{[I(V_2;Y_2|U) - I(V_2;Y_1|U)]^+, \\
&\qquad [I(V_2;Y_2|V_1U) - I(V_2;Y_1|V_1U)]^+\}. && (2.65)
\end{aligned}
$$

Similarly, define $\mathcal{R}_{O2}$ and $\mathcal{R}_{O3}$ in exactly the same fashion except with $\mathcal{Q}_1$ replaced by $\mathcal{Q}_2$ and $\mathcal{Q}_3$, respectively. We have

Theorem 2. *$\mathcal{R}_{O1}$, $\mathcal{R}_{O2}$, and $\mathcal{R}_{O3}$ are all outer bounds to the rate equivocation region of the DMBC-2CM.*

Proof. The proof that $\mathcal{R}_{O2}$ and $\mathcal{R}_{O3}$ are outer bounds is given in Section 2.6.1. That $\mathcal{R}_{O1}$ is an outer bound follows directly from Lemma 5. □

Lemma 5. $\mathcal{R}_{O3} \subseteq \mathcal{R}_{O1} = \mathcal{R}_{O2}$.

Lemma 5 can be established by simple algebra whose proof is omitted. While $\mathcal{R}_{O3}$ subsumes both $\mathcal{R}_{O1}$ and $\mathcal{R}_{O2}$, the latter expressions are often easier to use in

establishing capacity results or comparing with existing bounds. For example, it is straightforward to show that $\mathcal{R}_{O2}$ is tight for Csiszár and Körner's model [3], i.e., the DMBC with only one confidential message.

Below, we discuss various implications of Theorem 2.

2.4.1 The rate equivocation region of the less noisy DMBC-2CM

For the DMBC defined in Section 2.2.1, channel 1 is said to be less noisy than channel 2 [42] if for every $V \to X \to Y_1Y_2$,

$$I(V;Y_1) \geq I(V;Y_2). \tag{2.66}$$

Furthermore, for every $U \to V \to X \to Y_1Y_2$, the above less noisy condition also implies

$$I(V;Y_1|U) \geq I(V;Y_2|U). \tag{2.67}$$

Using Theorems 1 and 2, we can establish the rate equivocation region for the less noisy DMBC-2CM as in Theorem 3.

Theorem 3. *If channel 1 is less noisy than channel 2, then the rate equivocation region for this less noisy DMBC-2CM is the set of all non-negative* $(R_0, R_1, R_2, R_{e1}, R_{e2})$ *satisfying*

$$R_{e1} \leq R_1 \tag{2.68}$$

$$R_0 + R_2 \leq I(U;Y_2) \tag{2.69}$$

$$R_0 + R_1 + R_2 \leq I(V;Y_1|U) + I(U;Y_2) \tag{2.70}$$

$$R_{e1} \leq I(V;Y_1|U) - I(V;Y_2|U) \tag{2.71}$$

$$R_{e2} = 0, \tag{2.72}$$

for some (U, V, X, Y_1, Y_2) *such that* $U \to V \to X \to Y_1Y_2$.

Proof. The achievability is established by setting $V_2 = const$ in Theorem 1 and using the conditions (2.66) and (2.67). To prove the converse, we need to show that for any rate quintuple satisfying Eqs. (2.57)-(2.65) in Theorem 2, we can find (U', V', X, Y_1, Y_2) such that $U' \to V' \to X \to Y_1Y_2$ and (2.68)-(2.72) are satisfied. This can be accomplished by using the conditions (2.66) and (2.67) in Eqs. (2.59)-(2.65) and by defining $U' = UV_2$ and $V' = UV_1V_2$ where $(U, V_1, V_2, X, Y_1, Y_2) \in \mathcal{Q}_2$ are the variables used in Theorem 2. □

The fact that $R_{e2} = 0$ is a direct consequence of the less noisy assumption: receiver 1 can always decode anything that receiver 2 can decode.

2.4.2 The rate equivocation region of the semi-deterministic DMBC-2CM

Theorem 2 also allows us to establish the rate equivocation region of the semi-deterministic DMBC-2CM. WLOG, let channel 1 be deterministic.

Theorem 4. *If* $p(y_1|x)$ *is a* $(0, 1)$ *matrix, then the rate equivocation region for this DMBC-2CM, denoted by* $\mathcal{R}_{sd}$*, is the set of all non-negative* $(R_0, R_1, R_2, R_{e1}, R_{e2})$ *sat-*

isfying

$$
\begin{aligned}
R_{e1} &\leq R_1 && (2.73)\\
R_{e2} &\leq R_2 && (2.74)\\
R_0 &\leq \min\{I(U;Y_1), I(U;Y_2)\} && (2.75)\\
R_0 + R_1 &\leq H(Y_1|U) + \min\{I(U;Y_1), I(U;Y_2)\} && (2.76)\\
R_0 + R_2 &\leq I(V_2;Y_2|U) + \min\{I(U;Y_1), I(U;Y_2)\} && (2.77)\\
R_0 + R_1 + R_2 &\leq H(Y_1|V_2U) + I(V_2;Y_2|U) + \min\{I(U;Y_1), I(U;Y_2)\} && (2.78)\\
R_{e1} &\leq H(Y_1|Y_2V_2U) && (2.79)\\
R_{e2} &\leq [I(V_2;Y_2|U) - I(V_2;Y_1|U)]^+, && (2.80)
\end{aligned}
$$

for some $(U, Y_1, V_2, X, Y_1, Y_2) \in \mathcal{Q}_2$.

Proof. The direct part of this theorem follows trivially from Theorem 1 by setting $V_1 = Y_1$.

The proof is therefore complete by showing $\mathcal{R}_{SD-O2} \subseteq \mathcal{R}_{sd}$, where $\mathcal{R}_{SD-O2}$ is the outer bound $\mathcal{R}_{O2}$ specializing to the semi-deterministic DMBC-2CM. That is, for any $Z \in \mathcal{Q}_2$ and $(R_0, R_1, R_2, R_{e1}, R_{e2})$ satisfying (2.57)-(2.65), we need to show that $(R_0, R_1, R_2, R_{e1}, R_{e2})$ also satisfies (2.73)-(2.80) when $p(y_1|x)$ is a $(0, 1)$ matrix. We note that Eqs. (2.73)-(2.75), (2.77), and (2.80) can be trivially established. That the sum-rate bound Eq. (2.76) is satisfied follows easily from Eq. (2.60) and the fact

$$H(Y_1|U) \geq I(V_1;Y_1|U). \tag{2.81}$$

The sum-rate bound for $R_0 + R_1 + R_2$ in Eqs. (2.62) and (2.63) can be re-written as

$$\begin{aligned} R_0 + R_1 + R_2 \;\leq\; & \min\{I(V_2;Y_2|V_1U) + I(V_1;Y_1|U), I(V_1;Y_1|V_2U) + I(V_2;Y_2|U)\} \\ & + \min\{I(U;Y_1), I(U;Y_2)\}. \end{aligned} \tag{2.82}$$

Thus (2.78) is satisfied since

$$H(Y_1|V_2,U) + I(V_2;Y_2|U) \geq I(V_1;Y_1|V_2U) + I(V_2;Y_2|U). \tag{2.83}$$

For Eq. (2.79), we only need to show (cf. (2.64))

$$H(Y_1|Y_2V_2U) \geq I(V_1;Y_1|V_2U) - I(V_1;Y_2|V_2U). \tag{2.84}$$

We have

$$\begin{aligned} H(Y_1|Y_2V_2U) &\geq I(V_1;Y_1|Y_2V_2U) && (2.85)\\ &= I(V_1;Y_1Y_2|V_2U) - I(V_1;Y_2|V_2U) && (2.86)\\ &\geq I(V_1;Y_1|V_2U) - I(V_1;Y_2|V_2U). && (2.87) \end{aligned}$$

The proof of Theorem 4 is therefore complete. □

Similarly, the rate equivocation region of the deterministic DMBC-2CM can be established as follows.

Theorem 5. *If $p(y_1|x)$ and $p(y_2|x)$ are both $(0,1)$ matrices, then the rate equivocation region for this deterministic DMBC-2CM is the set of all $(R_0, R_1, R_2, R_{e1}, R_{e2})$ satisfying*

$$0 \;\leq\; R_{e1} \leq R_1 \tag{2.88}$$

$$
\begin{aligned}
0 &\leq R_{e2} \leq R_2 && (2.89)\\
0 &\leq R_0 \leq \min\{I(U;Y_1), I(U;Y_2)\} && (2.90)\\
R_0 + R_1 &\leq H(Y_1|U) + \min\{I(U;Y_1), I(U;Y_2)\} && (2.91)\\
R_0 + R_2 &\leq H(Y_2|U) + \min\{I(U;Y_1), I(U;Y_2)\} && (2.92)\\
R_0 + R_1 + R_2 &\leq H(Y_1Y_2|U) + \min\{I(U;Y_1), I(U;Y_2)\} && (2.93)\\
R_{e1} &\leq H(Y_1|Y_2U) && (2.94)\\
R_{e2} &\leq H(Y_2|Y_1U), && (2.95)
\end{aligned}
$$

for some $(U, Y_1, Y_2, X, Y_1, Y_2) \in \mathcal{Q}_2$.

Proof. The direct part of this theorem follows trivially from Theorem 4 by setting $V_2 = Y_2$.

To establish the converse, we note that

$$
\begin{aligned}
H(Y_2|U) &\geq I(V_2;Y_2|U), && (2.96)\\
H(Y_1|Y_2U) &\geq H(Y_1|Y_2V_2U), && (2.97)\\
H(Y_2|Y_1U) &\geq I(V_2;Y_2|U) - I(V_2;Y_1|U), && (2.98)\\
H(Y_1Y_2|U) &= H(Y_1|Y_2U) + H(Y_2|U)\\
&\geq H(Y_1|Y_2V_2U) + H(Y_2|V_2U) - H(Y_2|V_2U) + H(Y_2|U)\\
&\geq H(Y_1|V_2U) + I(V_2;Y_2|U), && (2.99)
\end{aligned}
$$

Thus the right-hand side of Eqs. (2.77)-(2.80) in Theorem 4 are maximized by setting $V_2 = Y_2$. This completes the converse proof of Theorem 5. □

We have the following table about the classes of broadcast channel whose capacity is known for general broadcast channel and also DMBC-2CM.

	DMBC	DMBC-2CM
Inner bound	$\surd$	$\surd$
Outer bound	$\surd$	$\surd$
Capacity of More capable channel	$\surd$	?
Capacity of Less noisy channel	$\surd$	$\surd$
Capacity of Deterministic channel	$\surd$	$\surd$
Capacity of Semi-Deterministic channel	$\surd$	$\surd$
Capacity of $R_1 = 0$ or $R_2 = 0$	$\surd$	$\surd$

Table 2.1: The comparison of the known results of DMBC and DMBC-2CM.

2.4.3 Outer bound for the DMBC-2CM with perfect secrecy

By setting $R_0 = 0$, $R_{e1} = R_1$ and $R_{e2} = R_2$ in Theorem 2, we obtain outer bounds for the DMBC-2CM with perfect secrecy, denoted respectively by $\mathcal{R}_{PS-O1}$, $\mathcal{R}_{PS-O2}$, and $\mathcal{R}_{PS-O3}$ for $Z \in \mathcal{Q}_1$, $Z \in \mathcal{Q}_2$, and $Z \in \mathcal{Q}_3$. Clearly,

$$\mathcal{R}_{PS-O1} = \mathcal{R}_{PS-O2} \supseteq \mathcal{R}_{PS-O3} \tag{2.100}$$

In addition, from Proposition 3, we have

$$\mathcal{R}_{PS-O2} = \mathcal{R}_{LMSY-O}. \tag{2.101}$$

i.e., $\mathcal{R}_{PS-O2}$ coincides with Liu *et al*'s outer bound in Proposition 3. Finally, all these outer bounds are tight for the semi-deterministic DMBC-2CM with perfect secrecy.

2.4.4 New outer bounds for the general DMBC

Specializing Theorem 2 to the general DMBC, i.e, setting $R_{e1} = R_{e2} = 0$, we obtain the following outer bounds for the general DMBC.

Theorem 6. *Define $\mathcal{R}_{BC-O1}$ to be the union, over all $Z \in \mathcal{Q}_1$, of non-negative rate quintuple (R_0, R_1, R_2) satisfying*

$$R_0 \leq \min\{I(U;Y_1), I(U;Y_2)\} \tag{2.102}$$

$$R_0 + R_1 \leq I(V_1;Y_1|U) + \min\{I(U;Y_1), I(U;Y_2)\} \tag{2.103}$$

$$R_0 + R_2 \leq I(V_2;Y_2|U) + \min\{I(U;Y_1), I(U;Y_2)\} \tag{2.104}$$

$$R_0 + R_1 + R_2 \leq I(V_2;Y_2|V_1U) + I(V_1;Y_1|U) + \min\{I(U;Y_1), I(U;Y_2)\} \tag{2.105}$$

$$R_0 + R_1 + R_2 \leq I(V_1;Y_1|V_2U) + I(V_2;Y_2|U) + \min\{I(U;Y_1), I(U;Y_2)\} \tag{2.106}$$

Then $\mathcal{R}_{BC-O1}$ constitutes an outer bound to the capacity region for the DMBC.

One can establish in a similar fashion two other outer bounds for the general DMBC, denoted by $\mathcal{R}_{BC-O2}$ and $\mathcal{R}_{BC-O3}$, by replacing $\mathcal{Q}_1$ in Theorem 6 with $\mathcal{Q}_2$ and $\mathcal{Q}_3$, respectively. Similar to Lemma 5, we have

$$\mathcal{R}_{BC-O3} \subseteq \mathcal{R}_{BC-O1} = \mathcal{R}_{BC-O2}. \tag{2.107}$$

Remark 1. *It is interesting to observe that the inequalities of our outer bound $\mathcal{R}_{BC}$ are all identical to those of the existing inner bound [29], described in Proposition 5,*

except for the bound on $R_0 + R_1 + R_2$, for which there is a gap of

$$\gamma = \min\{I(V_1; V_2|Y_1U), I(V_1; V_2|Y_2U)\}. \tag{2.108}$$

Remark 2. *It is easy to show that $\mathcal{R}_{BC-O2}$ subsumes the outer bound $\mathcal{R}_{LK}$ proposed in [33, Theorem 6], by comparing Eqs. (2.103)-(2.104) with Eqs. (2.30)-(2.31).*

Remark 3. *The new outer bound $\mathcal{R}_{BC-O3}$ is also a subset of the outer bound region $\mathcal{R}_{NE}$ proposed in [31, Theorem 2.1], as described in Proposition 8. More precisely, we have*

Lemma 6. *$\mathcal{R}_{BC-O3} \subseteq \mathcal{R}_{NE}$, where the equality holds when 1) $R_0 = 0$; or 2) $R_1 = 0$; or 3) $R_2 = 0$.*

Proof. By simple algebra, one can show $\mathcal{R}_{BC-O3} \subseteq \mathcal{R}_{NE}$. The fact that $\mathcal{R}_{BC-O3} = \mathcal{R}_{NE}$ when $R_0 = 0$ can also be verified by direct substitution.

We now prove the equivalence under $R_2 = 0$, and the case for $R_1 = 0$ can be established by index swapping. With $R_2 = 0$, Eqs. (2.102)-(2.106) of $\mathcal{R}_{BC-O3}$ can be easily shown to be equivalent to

$$R_0 \leq \min\{I(U; Y_1), I(U; Y_2)\}, \tag{2.109}$$

$$R_0 + R_1 \leq I(V_1; Y_1|U) + \min\{I(U; Y_1), I(U; Y_2)\}, \tag{2.110}$$

We note this is precisely the capacity region for the DMBC with degraded message set [3, Corollary 5].

With $R_2 = 0$, $\mathcal{R}_{NE}$ in Proposition 8 reduces to

$$R_0 \leq \min\{I(U; Y_1), I(U; Y_2)\}, \tag{2.111}$$

$$R_0 + R_1 \leq I(V_1U; Y_1), \tag{2.112}$$

$$R_0 + R_1 \leq I(V_1; Y_1|V_2U) + I(UV_2; Y_2). \tag{2.113}$$

Apparently $\mathcal{R}_{BC-O3} \subseteq \mathcal{R}_{NE}$, and it remains to check $\mathcal{R}_{NE} \subseteq \mathcal{R}_{BC-O3}$. Assume $(R_0, R_1) \in \mathcal{R}_{NE}$ and $(U, V_1, V_2, X, Y_1, Y_2) \in \mathcal{Q}_3$ are the variables such that Eqs. (2.111)-(2.113) are satisfied. Consider three cases for analysis.

1. $I(U; Y_1) \leq I(U; Y_2)$. The proof of $(R_0, R_1) \in \mathcal{R}_{BC-03}$ is trivial.

2. $I(U; Y_1) \geq I(U; Y_2)$ and $I(V_2U; Y_1) \geq I(V_2U; Y_2)$.

   Define $V_1' = V_1, U' = UV_2$. From (2.111),

$$R_0 \leq \min\{I(U; Y_1), I(U; Y_2)\} \tag{2.114}$$

$$\leq \min\{I(UV_2; Y_1), I(UV_2; Y_2)\} \tag{2.115}$$

$$= \min\{I(U'; Y_1), I(U'; Y_2)\} \tag{2.116}$$

   From (2.113),

$$R_0 + R_1 \leq I(V_1; Y_1|UV_2) + I(UV_2; Y_2) \tag{2.117}$$

$$= I(V_1'; Y_1|U') + I(U'; Y_2) \tag{2.118}$$

   Thus (R_0, R_2) also satisfies (2.109) and (2.110) for $U'V_1' \to X \to Y_1Y_2$.

3. $I(U; Y_1) \geq I(U; Y_2)$ and $I(V_2U; Y_1) \leq I(V_2U; Y_2)$.

   For this case, we can always find a function $g(\cdot)$ such that

$$I(Ug(V_2); Y_1) = I(Ug(V_2); Y_2). \tag{2.119}$$

Define $V_1' = V_1, U' = Ug(V_2)$ and we can verify that (R_0, R_1) satisfies (2.109) and (2.110) for $U'V_1' \to X \to Y_1Y_2$.

The above argument completes the proof of Lemma 6.

□

Note that the conditions in Lemma 6 are only sufficient conditions, i.e., there may be other instances when the two bounds are equivalent. It is also possible that $\mathcal{R}_{BC-O3} = \mathcal{R}_{NE}$ *though we have not been successful in proving (or disapproving) it.*

Remark 4. *One can easily verify that the outer bound proposed in [34],* $\mathcal{R}_{LKS}$ *in Proposition 9, subsumes all the above outer bounds. To summarize, we have*

$$\mathcal{R}_{LKS} \subseteq \mathcal{R}_{BC-O3} \subseteq \begin{cases} \mathcal{R}_{LK} \\ \mathcal{R}_{NE} \end{cases} \tag{2.120}$$

It remains unknown if any of the above subset relations can be strict or not.

The fact that $\mathcal{R}_{LKS}$ *subsumes existing outer bounds can be attributed to the way auxiliary random variables are defined in [34]. By further splitting auxiliary random variables and isolating those corresponding to the message variables, one can keep the terms in the rate upper bounds which are otherwise dropped if only three auxiliary variables are used as in Theorem 2 or [31]. Finally, we remark that the approach in [34], modified sightly by relaxing the constraint that the codeword be a deterministic function of the auxiliary random variables, can be adopted to the problem involving secrecy constraint in a straightforward manner to obtain a new outer bound to the rate equivocation region for the DMBC-2CM.*

Remark 5. *Most recently, the outer bound $\mathcal{R}_{NE}$ is further improved in [35] by imposing an extra constraint on the auxiliary random variables*

$$I(V_1; V_2|Y_1U) = I(V_1; V_2|Y_2U). \tag{2.121}$$

This equality comes from the way the auxiliary random variables are defined within the outer bound proof, and thus it is also applicable to our outer bound $\mathcal{R}_{BC-O3}$. If this extra condition is imposed on both $\mathcal{R}_{BC-O3}$ and $\mathcal{R}_{NE}$, then the equivalence of these two outer bounds can be easily established. The obtained outer bound [35, Lemma 1] by imposing this extra constraint is shown to subsume all the above outer bounds $\mathcal{R}_{NE}$, $\mathcal{R}_{LK}$, $\mathcal{R}_{BC-O3}$, and $\mathcal{R}_{LKS}$.

2.5 Summary

In this chapter, we proposed several outer bounds for the rate equivocation region of discrete memoryless broadcast channels with two confidential messages (DMBC-2CM). Together with a previously proposed inner bound, the proposed outer bounds settle the rate equivocation region of the less noisy, deterministic, and semi-deterministic DMBC-2CM. In the absence of the equivocation constraints, the proposed outer bounds reduce to outer bounds for the general broadcast channel. General subset relations with other known outer bounds were established.

2.6 Appendix

2.6.1 Proof of the outer bounds in Theorem 2

We only prove $\mathcal{R}_{O2}$ and $\mathcal{R}_{O3}$ are outer bounds in this section. The proof of Theorem 2 is complete by the fact that $\mathcal{R}_{O1} = \mathcal{R}_{O2}$ (cf. Lemma 5).

We first define the following notations/quantities. All vectors involved are assumed to be length n.

$$X^i \triangleq (X_1, \cdots, X_i), \tag{2.122}$$

$$\tilde{X}^i \triangleq (X_i, \cdots, X_n), \tag{2.123}$$

$$\Sigma_1 = \sum_{i=1}^{n} I(\tilde{Y}_2^{i+1}; Y_{1i} | Y_1^{i-1} W_0), \tag{2.124}$$

$$\Sigma_1^* = \sum_{i=1}^{n} I(Y_1^{i-1}; Y_{2i} | \tilde{Y}_2^{i+1} W_0), \tag{2.125}$$

and (Σ_2, Σ_2^*), (Σ_3, Σ_3^*), (Σ_4, Σ_4^*) are analogously defined by replacing W_0 with W_0W_1, W_0W_2 and $W_0W_1W_2$ in Eqs. (2.124) and (2.125), respectively. In exactly the same fashion as in [3, Lemma 7], one can establish, for $a = 1, 2, 3, 4$,

$$\Sigma_a = \Sigma_a^*. \tag{2.126}$$

We begin by Fano's Lemma,

$$H(W_0W_1|Y_1^n) \leq n\epsilon_n,$$

$$H(W_0W_2|Y_2^n) \leq n\epsilon_n.$$

where $\epsilon_n \to 0$ as $n \to \infty$. Eqs. (2.57) and (2.58) follow trivially from

$$0 \le H(W_1|Y_2^n) \le H(W_1), \tag{2.127}$$

$$0 \le H(W_2|Y_1^n) \le H(W_2). \tag{2.128}$$

Next we check bound for R_0.

$$\begin{aligned}
nR_0 = H(W_0) &= I(W_0; Y_1^n) + H(W_0|Y_1^n) \\
&\le \sum_{i=1}^{n} I(W_0; Y_{1i}|Y_1^{i-1}) + n\epsilon_n && (2.129)\\
&= \sum_{i=1}^{n} (I(W_0 Y_1^{i-1}; Y_{1i}) - I(Y_1^{i-1}; Y_{1i})) + n\epsilon_n && (2.130)\\
&\le \sum_{i=1}^{n} (I(W_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Y_{1i}) - I(\tilde{Y}_2^{i+1}; Y_{1i}|Y_1^{i-1} W_0)) + n\epsilon_n && (2.131)\\
&= \sum_{i=1}^{n} I(W_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Y_{1i}) - \Sigma_1 + n\epsilon_n && (2.132)\\
&\le \sum_{i=1}^{n} I(W_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Y_{1i}) + n\epsilon_n && (2.133)\\
& && (2.134)
\end{aligned}$$

Similarly,

$$\begin{aligned}
nR_0 &\le \sum_{i=1}^{n} I(W_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Y_{2i}) - \Sigma_1^* + n\epsilon_n && (2.135)\\
&\le \sum_{i=1}^{n} I(W_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Y_{2i}) + n\epsilon_n && (2.136)
\end{aligned}$$

Therefore

$$nR_0 \le \min \left\{ \sum_{i=1}^{n} I(W_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Y_{1i}), \sum_{i=1}^{n} I(W_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Y_{2i}) \right\} + n\epsilon_n. \tag{2.137}$$

Consider the sum rate bound for $R_0 + R_1$.

$$\begin{aligned} n(R_0+R_1) = H(W_0W_1) &= H(W_0) + H(W_1|W_0) && (2.138)\\ &= H(W_0) + I(W_1;Y_1^n|W_0) + H(W_1|Y_1^nW_0) && (2.139)\\ &\le H(W_0) + I(W_1;Y_1^n|W_0) + n\epsilon_n && (2.140)\end{aligned}$$

where

$$\begin{aligned} & I(W_1;Y_1^n|W_0) && (2.141)\\ &= \sum_{i=1}^{n} I(W_1;Y_{1i}|Y_1^{i-1}W_0) && (2.142)\\ &= \sum_{i=1}^{n} (I(W_1\tilde{Y}_2^{i+1};Y_{1i}|Y_1^{i-1}W_0) - I(\tilde{Y}_2^{i+1};Y_{1i}|Y_1^{i-1}W_0W_1)) && (2.143)\\ &= \sum_{i=1}^{n} (I(W_1;Y_{1i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0) + I(\tilde{Y}_2^{i+1};Y_{1i}|Y_1^{i-1}W_0) \\ &\quad -I(\tilde{Y}_2^{i+1};Y_{1i}|Y_1^{i-1}W_0W_1)) && (2.144)\\ &= \sum_{i=1}^{n} I(W_1;Y_{1i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0) + \Sigma_1 - \Sigma_2. && (2.145)\end{aligned}$$

Combine (2.132), (2.140), and (2.145), we have

$$n(R_0+R_1) \le \sum_{i=1}^{n} I(W_0Y_1^{i-1}\tilde{Y}_2^{i+1};Y_{1i}) + \sum_{i=1}^{n} I(W_1;Y_{1i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0) - \Sigma_2 + 2n\epsilon_n. \quad (2.146)$$

On the other hand, combining (2.135), (2.140), (2.145), and (2.126) yields

$$n(R_0+R_1) \le \sum_{i=1}^{n} I(W_0Y_1^{i-1}\tilde{Y}_2^{i+1};Y_{2i}) + \sum_{i=1}^{n} I(W_1;Y_{1i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0) - \Sigma_2 + 2n\epsilon_n. \quad (2.147)$$

Thus,

$$n(R_0+R_1) \le \min\left\{\sum_{i=1}^{n} I(W_0Y_1^{i-1}\tilde{Y}_2^{i+1};Y_{1i}), \sum_{i=1}^{n} I(W_0Y_1^{i-1}\tilde{Y}_2^{i+1};Y_{2i})\right\}$$

$$+\sum_{i=1}^{n} I(W_1;Y_{1i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0) - \Sigma_2 + 2n\epsilon_n \tag{2.148}$$

$$\leq \min\left\{\sum_{i=1}^{n} I(W_0Y_1^{i-1}\tilde{Y}_2^{i+1};Y_{1i}), \sum_{i=1}^{n} I(W_0Y_1^{i-1}\tilde{Y}_2^{i+1};Y_{2i})\right\}$$
$$+\sum_{i=1}^{n} I(W_1;Y_{1i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0) + 2n\epsilon_n \tag{2.149}$$

In an analogous fashion, we can get

$$n(R_0+R_2) \leq \min\left\{\sum_{i=1}^{n} I(W_0Y_1^{i-1}\tilde{Y}_2^{i+1};Y_{1i}), \sum_{i=1}^{n} I(W_0Y_1^{i-1}\tilde{Y}_2^{i+1};Y_{2i})\right\}$$
$$+\sum_{i=1}^{n} I(W_1;Y_{2i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0) - \Sigma_3 + 2n\epsilon_n \tag{2.150}$$

$$\leq \min\left\{\sum_{i=1}^{n} I(W_0Y_1^{i-1}\tilde{Y}_2^{i+1};Y_{1i}), \sum_{i=1}^{n} I(W_0Y_1^{i-1}\tilde{Y}_2^{i+1};Y_{2i})\right\}$$
$$+\sum_{i=1}^{n} I(W_1;Y_{2i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0) + 2n\epsilon_n \tag{2.151}$$

Consider the sum rate bound for $R_0+R_1+R_2$.

$$n(R_0+R_1+R_2) = H(W_0W_1) + H(W_2|W_1W_0) \tag{2.152}$$

$$= H(W_0W_1) + I(W_2;Y_2^n|W_1,W_0) + H(W_2|Y_2^nW_0W_1) \tag{2.153}$$

$$\leq H(W_0W_1) + I(W_2;Y_2^n|W_1W_0) + n\epsilon_n, \tag{2.154}$$

$$n(R_0+R_1+R_2) = H(W_0W_2) + H(W_1|W_2W_0) \tag{2.155}$$

$$= H(W_0W_2) + I(W_1;Y_1^n|W_2W_0) + H(W_1|Y_1^nW_0W_2) \tag{2.156}$$

$$\leq H(W_0W_2) + I(W_1;Y_1^n|W_2W_0) + n\epsilon_n. \tag{2.157}$$

Following similar procedure as in (2.142)-(2.145), we can obtain

$$I(W_2;Y_2^n|W_1,W_0) = \sum_{i=1}^{n} I(W_2;Y_{2i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0W_1) + \Sigma_2^* - \Sigma_4^*. \tag{2.158}$$

$$I(W_1;Y_1^n|W_2,W_0) \;=\; \sum_{i=1}^{n} I(W_1;Y_{1i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0W_2)+\Sigma_3-\Sigma_4, \quad (2.159)$$

Combine (2.148), (2.154), (2.158), and (2.126), we get

$$\begin{aligned} n(R_0+R_1+R_2) \le\; & \min\left\{\sum_{i=1}^{n} I(W_0Y_1^{i-1}\tilde{Y}_2^{i+1};Y_{1i}), \sum_{i=1}^{n} I(W_0Y_1^{i-1}\tilde{Y}_2^{i+1};Y_{2i})\right\} \\ & +\sum_{i=1}^{n} I(W_1;Y_{1i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0)+\sum_{i=1}^{n} I(W_2;Y_{2i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0W_1) \\ & +3n\epsilon_n. \end{aligned} \quad (2.160)$$

Alternatively, combining (2.150), (2.157), (2.159), and (2.126) yields

$$\begin{aligned} n(R_0+R_1+R_2) \le\; & \min\left\{\sum_{i=1}^{n} I(W_0Y_1^{i-1}\tilde{Y}_2^{i+1};Y_{1i}), \sum_{i=1}^{n} I(W_0Y_1^{i-1}\tilde{Y}_2^{i+1};Y_{2i})\right\} \\ & +\sum_{i=1}^{n} I(W_2;Y_{2i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0)+\sum_{i=1}^{n} I(W_1;Y_{2i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0W_2) \\ & +3n\epsilon_n. \end{aligned} \quad (2.161)$$

We now consider the equivocation rate bound.

$$\begin{aligned} R_{e1} &\le H(W_1|Y_2^n) && (2.162)\\ &= H(W_1|Y_2^nW_0)+I(W_1;W_0|Y_2^n) && (2.163)\\ &\le H(W_1|W_0)-I(W_1;Y_2^n|W_0)+H(W_0|Y_2^n) && (2.164)\\ &= I(W_1;Y_1^n|W_0)-I(W_1;Y_2^n|W_0)+H(W_1|Y_1^nW_0)+H(W_0|Y_2^n) && (2.165)\\ &\le I(W_1;Y_1^n|W_0)-I(W_1;Y_2^n|W_0)+2n\epsilon_n, && (2.166)\\ R_{e1} &\le H(W_1|Y_2^n) && (2.167)\\ &= H(W_1|Y_2^nW_0W_2)+I(W_1;W_0W_2|Y_2^n) && (2.168)\\ &\le H(W_1|W_0W_2)-I(W_1;Y_2^n|W_0W_2)+H(W_0W_2|Y_2^n) && (2.169) \end{aligned}$$

$$
\begin{aligned}
&= I(W_1; Y_1^n|W_0W_2) - I(W_1; Y_2^n|W_0W_2) + H(W_1|Y_1^nW_0W_2) \\
&\quad + H(W_0W_2|Y_2^n) \qquad (2.170)\\
&\leq I(W_1; Y_1^n|W_0W_2) - I(W_1; Y_2^n|W_0W_2) + 2n\epsilon_n.. \qquad (2.171)
\end{aligned}
$$

Of the terms involved in (2.166) and (2.171), only $I(W_1; Y_2^n|W_0)$ and $I(W_1; Y_2^n|W_0W_2)$ have yet to be determined. Similar to (2.142)-(2.145), we can get

$$
\begin{aligned}
I(W_1; Y_2^n|W_0) &= \sum_{i=1}^{n} I(W_1; Y_{2i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0) + \Sigma_1^* - \Sigma_2^*, \qquad (2.172)\\
I(W_1; Y_2^n|W_0W_2) &= \sum_{i=1}^{n} I(W_1; Y_{2i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0W_2) + \Sigma_3^* - \Sigma_4^*. \qquad (2.173)
\end{aligned}
$$

Therefore we get

$$
\begin{aligned}
R_{e1} &\leq \sum_{i=1}^{n} I(W_1; Y_{1i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0) - \sum_{i=1}^{n} I(W_1; Y_{2i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0) + 2n\epsilon_n, \qquad (2.174)\\
R_{e1} &\leq \sum_{i=1}^{n} I(W_1; Y_{1i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0W_2) - \sum_{i=1}^{n} I(W_1; Y_{2i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0W_2) \\
&\quad + 2n\epsilon_n. \qquad (2.175)
\end{aligned}
$$

Bounds on R_{e2} are analogously obtained:

$$
\begin{aligned}
R_{e2} &\leq \sum_{i=1}^{n} I(W_2; Y_{2i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0) - \sum_{i=1}^{n} I(W_2; Y_{1i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0) + 2n\epsilon_n, \qquad (2.176)\\
R_{e2} &\leq \sum_{i=1}^{n} I(W_2; Y_{2i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0W_1) - \sum_{i=1}^{n} I(W_2; Y_{1i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0W_1) \\
&\quad + 2n\epsilon_n. \qquad (2.177)
\end{aligned}
$$

Let us introduce a random variable J, independent of $W_0W_1W_2X^nY_1^nY_2^n$, uniformly distributed over $\{1, \cdots, n\}$. Set

$$
\begin{aligned}
&U \triangleq W_0Y_1^{J-1}\tilde{Y}_2^{J+1}J, \quad V_1 \triangleq W_1U, \quad V_2 \triangleq W_2U,\\
&X \triangleq X_J, \qquad\qquad Y_1 \triangleq Y_{1J}, \quad Y_2 \triangleq Y_{2J}.
\end{aligned}
$$

Substituting these definitions into Eqs. (2.137), (2.149), (2.151), (2.160, (2.161), and (2.174)-(2.177), we obtain, through standard information theoretic argument, the desired bounds as in Eqs. (2.57)-(2.65). The memoryless property of the channel guarantees $U \to V_1V_2 \to X \to Y_1Y_2$. This completes the proof.

To prove $\mathcal{R}_{O3}$ is also an outer bound, we follow exactly the same procedure except that auxiliary random variables are defined differently. Specifically,

$$U \triangleq W_0 Y_1^{J-1} \tilde{Y}_2^{J+1} J, \quad V_1 \triangleq W_1, \quad V_2 \triangleq W_2.$$

Chapter 3

Broadcast Channels with Confidential and Public Messages

We consider in this chapter a variation of Csiszár and Körner's model of broadcast channels with confidential messages. The transmitter sends both a confidential message and a non-confidential message (herein termed as public message) to the intended receiver. While the unintended receiver should be kept ignorant from the confidential message, we do not impose the requirement that the public message needs to be perfectly recovered by the unintended receiver. This more liberal treatment of the non-confidential message is perhaps a more reasonable model than Csiszár and Körner's model where the non-confidential message is required to be decoded by both receivers. A single-letter characterization of the achievable rate equivocation region of this model is given, and this result is then extended to the case where an extra secret key is available to the intended transceiver pair.

3.1 Introduction

Csiszár and Körner [3] studied a general broadcast channel with two receivers. The transmitter communicates a confidential message to receiver 1, of which receiver 2 shall be kept as ignorant as possible. In addition, a common message is transmitted which is to be recovered by both receivers.

Apparently, Csiszár and Körner's model conforms to the classical broadcast channel model with both common message and private message [36], with the additional secrecy constraint imposed on receiver 2. The inclusion of common message comes from the classical model for broadcast channels; however, its meaningfulness in certain security applications is questionable, that is, the requirement that receiver 2 needs to decode the common message might not be justified in many real applications. Often times, a transmitter needs to transmit multiple messages to a receiver, some of which need to be kept confidential. However, for the messages that do not need to be kept confidential, it would be overly restrictive to require an unintended receiver to completely recover them.

Therefore, in the present chapter, we take on a more practical viewpoint and study a variation of Csiszár and Körner's model. We term this broadcast channel with confidential and public messages (BCCP). Whereas the confidential message shall be kept secret from any unintended receivers, the public message is only *required* to be decoded by the intended receiver. We do not impose any constraint on whether the unintended receiver shall decode the public message or not, even if there is no

incentive to protect the public message. As such, we use public instead of common message to differentiate from that of the classical model of Csiszár and Körner. For easy reference, we will use BCCC (broadcast channel with confidential and common messages) to refer to Csiszár and Körner's original model where the non-confidential message is to be decoded by both receivers.

Similar to the previous chapter, we illustrate in Fig. 3.1 the differences among the three models, Wyner's wiretap channel model, Csiszár and Körner's BCCC model, and our present BCCP model. As shown in Fig. 3.1, BCCP requires both confidential message S and public message T to be reliably recovered at legitimate receiver (Alice). For the unintended receiver (Eve), we only impose a constraint on the equivocation rate with respect to S, whereas in Csiszár and Körner's model, the unintended receiver also needs to decode the common message. A single letter characterization of the rate equivocation region is derived for BCCP. Our result indeed indicates that BCCP can achieve better secrecy than BCCC in the sense that given the same confidential and non-confidential rates, BCCP achieves strictly larger equivocation rate than BCCC.

The rest of the chapter is organized as follows. Section 3.2 gives the problem formulation and related work. The main result of BCCP is stated in Section 3.3, followed by discussions about major implications of the main result. The proof is given in Section 3.4. Section 3.5 discusses its extended version, secret key enhanced BCCP model. We conclude our work in Section 3.6.

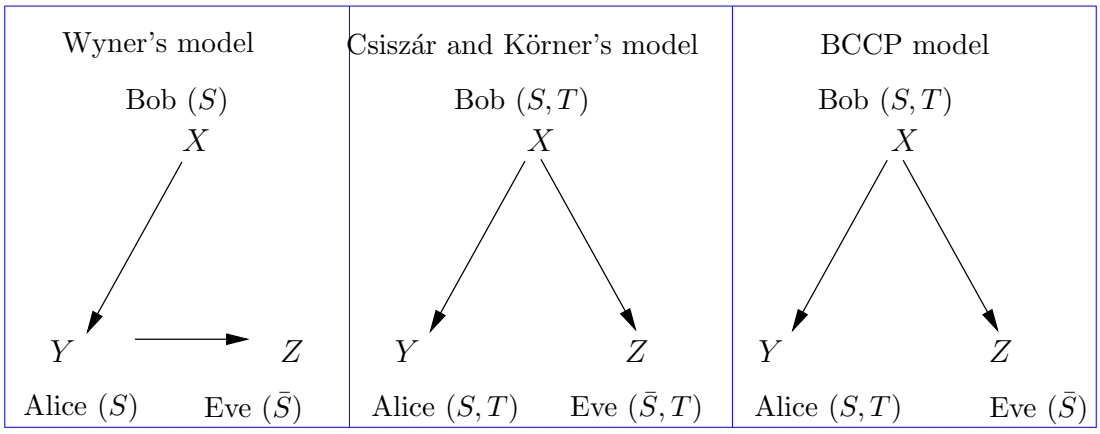


Figure 3.1: Variations to the wiretap channel

3.2 Problem Formulation and Related Work

In this section, we give a precise statement of the problem that we stated informally in the previous section and then summarize our results. Some of the notions and definitions follow closely that of [3]. Fig. 3.2 gives an illustration of the BCCP model we study in this chapter.

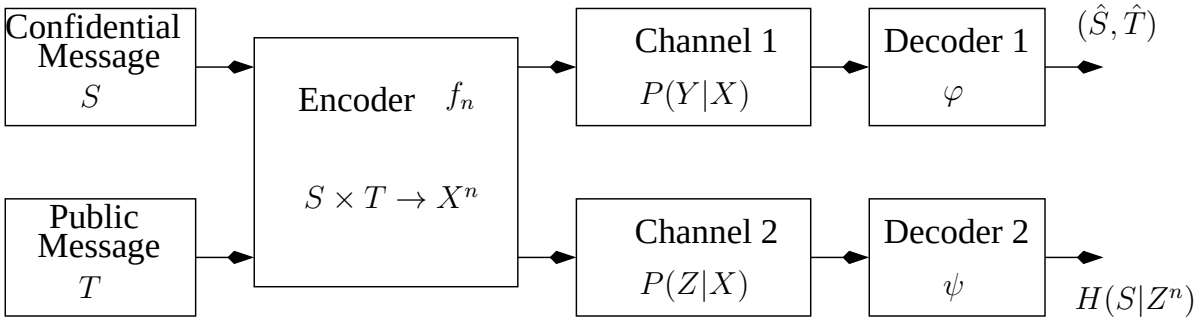


Figure 3.2: Broadcasting confidential message S and public message T.

Definition 1. *A stochastic encoder* $f : \mathcal{S} \times \mathcal{T} \to \mathcal{X}^n$ *with block length* n *for the*

BCCP is specified by a matrix of conditional probabilities $f(x^n|s,t)$, where $\mathcal{S}$ and $\mathcal{T}$ are arbitrary sets representing the possible confidential messages and public messages, and $f(x^n|s,t)$ is the probability that the message pair (s,t) is encoded as channel input x^n.

In Definition 1, we assume stochastic encoding as randomization may increase secrecy [3].

Definition 2. *The encoder-decoder (f,φ,ψ) gives rise to (n,ϵ)-transmission over the BCCP iff for every $s \in \mathcal{S}$, $t \in \mathcal{T}$, decode φ gives the correct (s,t) with probability $\geq 1-\epsilon$.*

In Definition 2, unlike [3], we do not impose any requirement for receiver 2 to recover T .

Definition 3. *(R_1, R_e, R_p) is an achievable rate triple for the BCCP iff for every $\epsilon > 0$ there exists a sequence of message sets $\mathcal{S}^n$,$\mathcal{T}^n$ and encoder-decoder (f,φ,ψ) giving rise to (n,ϵ)-transmission, such that*

$$\lim_{n\to\infty} \frac{1}{n} \log \|\mathcal{S}^n\| = R_1, \tag{3.1}$$

$$\lim_{n\to\infty} \frac{1}{n} \log \|\mathcal{T}^n\| = R_p, \tag{3.2}$$

$$\frac{1}{n} H(S^n|Z^n) \geq R_e - \epsilon, \tag{3.3}$$

where $H(S^n|Z^n)$ is evaluated under the assumption that the pair of random messages (S^n, T^n) is uniformly distributed over $\mathcal{S}^n \times \mathcal{T}^n$. The set of achievable rate triples will

be denoted by $\mathcal{R}_{BCP}$*. If* $(R_1, R_e, R_p) \in \mathcal{R}_{BCP}$*, we say that* R_1 *and* R_p *are achievable confidential and public message rates at equivocation rate* R_e*.*

Clearly, the closely related work is [3], where Csiszár and Körner characterized the rate equivocation region for BCCC, i.e., a broadcast channel with a common message for both receivers and a single confidential message intended for the intended receiver. We will revisit the idea of random coding over noisy channel (referred as to [3, Lemma 2]), which is stated below.

Proposition 10. *If* $U \to X \to YZ$ *forms a Markov chain, and* $I(X;Y|U) > I(X;Z|U)$*, then for every* n *there exists a set* $x^n_{jkl} \subset \mathcal{X}^n$ *where* $j \in \mathcal{M}_J \triangleq \{1, \ldots, M_J\}$ *and* $k \in \mathcal{M}_K \triangleq \{1, \ldots, M_K\}$ *and* $l \in \mathcal{M}_L \triangleq \{1, \ldots, M_L\}$*, with the following properties.*

1. *For each* $l \in \mathcal{M}_L$*, there exist a* U*-typical sequence* $u^n_l \in U^n$ *such that every* x^n_{jkl} *is* $X|U$*-generated by* u^n_l*. Moreover, there exist pairwise disjoint subsets* $\mathcal{B}_l \subset \mathcal{F}_{Y|U}(u^n_l)$ *resp.* $\mathcal{C}_l \subset \mathcal{F}_{Z|U}(u^n_l)$ *such that*

$$\begin{aligned} P_{Y|X}(\mathcal{B}_l|x^n_{jkl}) &\geq 1-\epsilon_n, \\ P_{Z|X}(\mathcal{C}_l|x^n_{jkl}) &\geq 1-\epsilon_n. \end{aligned}$$

2. *There exist pairwise disjoint subsets* $\mathcal{B}_{jkl} \subset \mathcal{F}_{Y|X}(x^n_{jkl})$ *and subset* $\mathcal{C}_{jkl} \subset \mathcal{F}_{Z|X}(x^n_{jkl})$*, of which those with the same index* k *are pairwise disjoint, such that*

$$\begin{aligned} P_{Y|X}(\mathcal{B}_{jkl}|x^n_{jkl}) &\geq 1-\epsilon_n, \\ P_{Z|X}(\mathcal{C}_{jkl}|x^n_{jkl}) &\geq 1-\epsilon_n. \end{aligned}$$

3. Also, as $n \to \infty$

$$\begin{aligned} \epsilon_n &\to 0 \\ \frac{1}{n}\log\|\mathcal{M}_J\| &\to I(X;Z|U), \\ \frac{1}{n}\log\|\mathcal{M}_K\| &\to I(X;Y|U) - I(X;Z|U), \\ \frac{1}{n}\log\|\mathcal{M}_L\| &\to \min(I(U;Y), I(U;Z)). \end{aligned}$$

We can see from Proposition 10 that the index l can be decoded by both Y^n and Z^n, in addition, given index k, Z^n could decode all indices j, k, l with arbitrary small error probabilities. In other words, only the part of message corresponding to index k would be kept secret.

Based on this proposition, Csiszár and Körner characterized the rate equivocation region for BCCC, summarized in Proposition 1. As illustrated in Fig. 3.3, to achieve this rate equivocation region, the essential idea is to arrange the common message bits in index l and put the rest in index j and k according to Proposition 10. The total protected bits are then $I(X;Y|U) - I(X;Z|U)$.

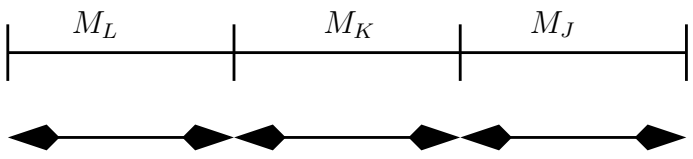


Figure 3.3: Encoding scheme of BCCC.

3.3 Main Result For The BCCP Model

Our main result is the following theorem.

Theorem 7. *$\mathcal{R}_{BCP}$ is a closed convex set consisting of those triples (R_1, R_e, R_p) for which there exist RV's $U \to V \to X \to YZ$ such that the conditional distribution of Y (resp. Z) given X is determined by channel 1 (resp. 2) and*

$$\begin{aligned} 0 &\leq R_e \leq R_1, && (3.4)\\ R_e &\leq I(V;Y|U) - I(V;Z|U), && (3.5)\\ R_1 + R_p &\leq I(V;Y|U) + \min(I(U;Y), I(U;Z)). && (3.6) \end{aligned}$$

To exhaust $\mathcal{R}_{BCP}$, it is enough to consider U and V such that

$$\begin{aligned} \|\mathcal{U}\| &\leq \|\mathcal{X}\| + 2, && (3.7)\\ \|\mathcal{V}\| &\leq \|\mathcal{X}\|^2 + 3\|\mathcal{X}\| + 2. && (3.8) \end{aligned}$$

In the following, we discuss our main result and its various special cases.

3.3.1 Comparison with Csiszár and Körner's model

In Csiszár and Körner's model, the non-confidential message needs to be reliably recovered at both receivers, which was therefore referred to as the common message. In the present model, the non-confidential message is only required to be decoded at receiver 1, the reason we term it public message.

Therefore it is intuitive that by relaxing the constraint on the non-confidential message, the achievable rate equivocation region ought to be enlarged. This can be

easily verified by comparing Theorem 7 with Proposition 1([3, Theorem 1]) where BCCC imposes the following additional constraint on the non-confidential message:

$$R_0 \leq \min\{I(U;Y), I(U;Z)\}. \tag{3.9}$$

On the other hand, if one set $R_0 = 0$ in Csiszar and Korner's BCCC model, it is easy to see that the rate R_1 is equivalent to $R_1 + R_p$ in BCCP, i.e., one can view the confidential and public messages in BCCP as splitting the confidential message in the BCCC model by setting $R_0 = 0$. Fig. 3.4 shows the typical rate region of ($R_1 + R_p$ v.s. R_e) from the main result which coincides with Fig. 1 in [3].

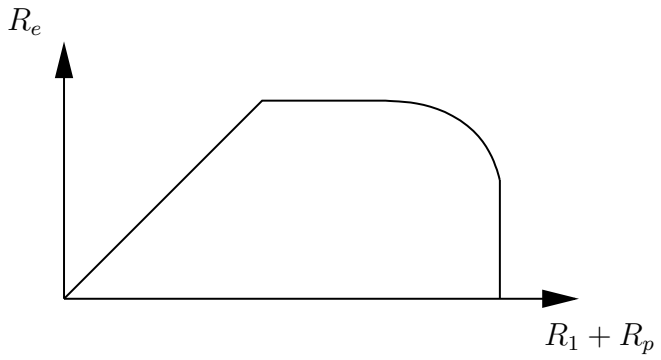


Figure 3.4: The typical rate region of ($R_1 + R_p$ vs R_e) for BCCP.

The real advantage of the BCCP model is the enhanced security of the confidential message. Before we present the generate results, let us first examine an extreme case to appreciate the advantage of relaxing the decoding requirement for receiver 2. Assume we have a less noisy channel [42] in the sense of $I(U;Z) \leq I(U;Y)$ for any $U \to X \to YZ$. Consider now we have a non-confidential rate that equals

$\max I(X;Z)$. It is clear that imposing receiver 2 to decode the non-confidential message (i.e., the BCCC model) will result in $R_1 = R_e = 0$, which can be verified easily given $U = V = X$. On the other hand, the BCCP model still can achieve $R_1 = R_e = I(X;Y) - I(X;Z)$ which is obtained by letting $U = \phi$ and $V = X$ in Theorem 7.

Denote by $C_c(R)$ and $C_p(R)$ the secrecy capacities for BCCC and BCCP at non-confidential message rate R (i.e., $R_0 = R$ for BCCC and $R_0 = R$ for BCCP). Equivalently, $C_c(R)$ is the maximum of R_1 such that (R_1, R_1, R) is achievable for BCCC while $C_p(R)$ is the maximum of R_1 such that (R_1, R_1, R) is achievable for BCCP. We have

Proposition 11. $C_c(R) \leq C_p(R)$

The proposition follows trivially from the fact that the BCCC region is a subset of BCCP region and the definition of $C_c(R)$ and $C_p(R)$.

Proposition 11 shows that it is possible that a larger secrecy capacity can be achieved given identical non-confidential message rate $R_p = R_0 = R$. The discussion about the extreme case above also indicates the improvement can be strict, i.e., the inequality in Proposition 11 can be strict. In the following, we generalize the above result to a special class of broadcast channels, namely less noisy symmetric channels. For this class of broadcast channels [11], uniform input simultaneously maximizes $I(X;Y)$, $I(X;Z)$, as well as $I(X;Y) - I(X;Z)$. Specifically, we have

Proposition 12. *For a less noisy and symmetric broadcast channel, BCCP has a*

strictly larger rate equivocation region than BCCC provided that the non-confidential message rate is positive.

Proof. From Theorem 7, the rate region for BCCP for the less noisy broadcast channel can be written as,

$$\begin{aligned} 0 &\leq R_e \leq R_1, && (3.10)\\ R_e &\leq I(X;Y) - I(X;Z), && (3.11)\\ R_1 + R_p &\leq I(X;Y). && (3.12) \end{aligned}$$

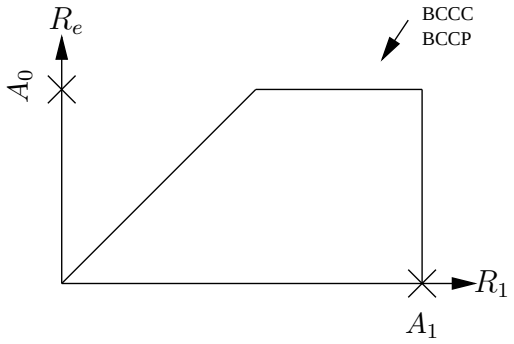
The proof is quite similar to the proof of [3, Theorem 3].

On the other hand, the rate region for BCCC reduces to

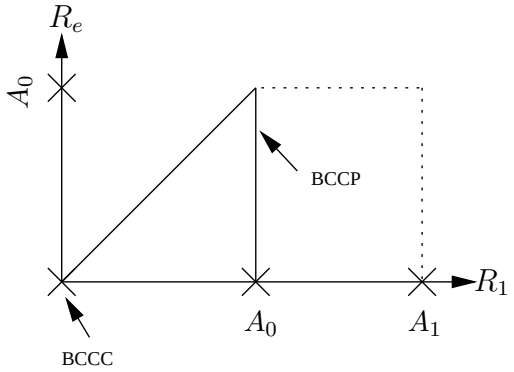
$$\begin{aligned} 0 &\leq R_e \leq R_1, && (3.13)\\ R_e &\leq I(X;Y|U) - I(X;Z|U), && (3.14)\\ R_0 &\leq I(U;Z), && (3.15)\\ R_1 + R_0 &\leq I(X;Y|U) + I(U;Z). && (3.16) \end{aligned}$$

We separate the three different cases, as illustrated in Fig. 3.5.

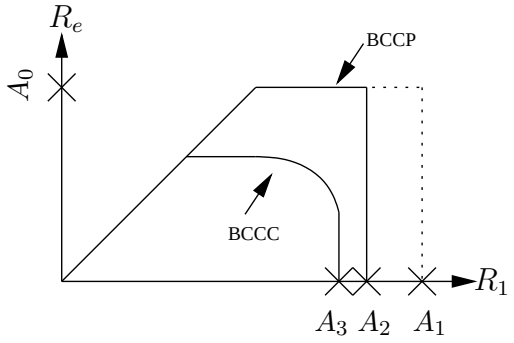
1. $R_p = R_0 = 0$. As we shall see in the next section, the rate regions for BCCC and BCCP coincide with each other. In addition, the rate region has a right angle at upper right corner instead of a curve as in Fig. 3.4. This is due to the fact that for symmetric channel $I(X;Y)$, $I(X;Z)$, and $I(X;Y) - I(X;Z)$ can achieve their respective maxima simultaneously.



(1) $R_p = R_0 = 0$



(2) $R_p = R_0 = \max(I(X;Z))$



(3) $0 < R_p = R_0 = R < \max(I(X;Z))$

Figure 3.5: BCCC and BCCP's rate regions of less noisy and symmetric broadcast channel in three cases, where $A_0 = \max(I(X;Y) - I(X;Z))$, $A_1 = \max(I(X;Y))$, $A_2 = \max(I(X;Y)) - R$, $A_3 = \max(I(X;Y|U) + I(U;Z)) - R$. In (2), the rate region for BCCC degenerates into a single point $(0, 0)$.

2. $R_p = R_0 = \max I(X;Z)$. BCCC reduces to

$$R_e = R_1 = 0.$$

When the non-confidential message rate reaches the capacity of the more noisy channel (receiver 2), the confidential message is forced to be zero even though there is positive excess capacity for receiver 1. This is due to the requirement in BCCC that receiver 2 needs to decode the non-confidential message. Transmitting confidential message will force the non-confidential message rate to back off from its maximum. For BCCP, however, one can still achieve

$$R_e = R_1 = I(X;Y) - I(X;Z)$$

For this case, the inequality in Proposition 11 is strict since $C_c(\max I(X;Z)) = 0$ while $C_p(\max I(X;Z)) = I(X;Y) - I(X;Z)$.

In addition, it should be pointed out that the public message rate R_p in BCCP can exceed the wiretap channel's capacity, i.e. $R_p \geq \max I(X;Z)$. This is another consequence of relaxing the decoding requirement to unintended receiver in the BCCP model.

3. $0 < R_p = R_0 < \max I(X;Z)$. We observe from Eq. (3.11) and Eq. (3.14) that there is always a gap $I(U;Y) - I(U;Z)$ for the R_e constraint for the two models since

$$I(X;Y) - I(X;Z) \;\; = \;\; I(X;Y|U) - I(X;Z|U)$$

$$+I(U;Y) - I(U;Z).$$

Given the less noisy assumption the BCCP's rate region is strictly larger than that of BCCC. In addition, notice that the BCCC rate region has a curve at its upper right corner instead of a right angle as BCCP because in this case $I(X;Y|U)-I(X;Z|U)$ and $I(X;Y|U)+I(U;Z)$ might not achieve their maxima simultaneously.

From the above three cases, we know that the BCCP achieves strictly larger rate region for a given positive non-confidential message rate. □

3.3.2 No public message

Now we turn to the special case of no public message ($R_p = 0$). We denote by $\mathcal{R}_{1e}$ the set of achievable rate pairs (R_1, R_e) with no public message, i.e., $(R_1, R_e) \in \mathcal{R}_{1e}$ iff $(R_1, R_e, 0) \in \mathcal{R}_{BCP}$.

Theorem 8. $(R_1, R_e) \in \mathcal{R}_{1e}$ *iff there exist* $U \to V \to X \to YZ$ *such that* $I(U;Y) \leq I(U;Z)$ *and*

$$0 \leq R_e \leq I(V;Y|U) - I(V;Z|U); \tag{3.17}$$

$$R_e \leq R_1 \leq I(V;Y). \tag{3.18}$$

Proof. Taking $R_p = 0$ in Theorem 7 we obtain that $(R_1, R_e) \in \mathcal{R}_{1e}$ iff there exist $U \to V \to X \to YZ$ such that

$$R_e \leq I(V;Y|U) - I(V;Z|U), \tag{3.19}$$

$$R_e \leq R_1 \leq I(V;Y). \tag{3.20}$$

If $I(U;Y) \leq I(U;Z)$, then Eq. (3.17) and Eq. (3.18) hold.

If $I(U;Y) \geq I(U;Z)$, we get

$$\begin{aligned} R_e &\leq I(V;Y|U) - I(V;Z|U) \\ &\leq I(V;Y|U) - I(V;Z|U) + I(U;Y) - I(U;Z) \\ &= I(V;Y) - I(V;Z), \end{aligned} \tag{3.21}$$

$$R_e \leq R_1 \leq I(V;Y). \tag{3.22}$$

In the latter case Eq. (3.17)-(3.18) are satisfied for $U = \text{const}$. □

Compare Theorem 8 with [3, Corollary 2], we see that the region is identical to that of BCCC without common message. This is not surprising; in the absence of non-confidential message, BCCP and BCCC converge to the same model with only a single confidential message.

3.3.3 Binary symmetric broadcast channel

The binary symmetric broadcast channel (BSBC) is a simple example of a degraded (hence less noisy) broadcast channel that is also symmetric.

Given a BSBC with crossover probabilities p_1 and p_2, $0 < p_1 < p_2 < 1/2$, we can view X, Y, Z as the inputs and outputs of the cascaded binary symmetric channels with $X \to Y \to Z$. For less noisy channel, we have

$$0 \leq R_e \leq R_1,$$

$$\begin{aligned} R_e &\leq I(X;Y) - I(X;Z), \\ R_1 + R_p &\leq I(X;Y). \end{aligned}$$

$I(X;Y)$ achieves its maximum $1 - h(p_1)$ at $P(X = 1) = P(X = 0) = 1/2$, where $h(\cdot)$ is defined as $h(\lambda) = -\lambda \log \lambda - (1 - \lambda) \log(1 - \lambda)$.

For any arbitrary $P(X)$,

$$\begin{aligned} I(X;Y) - I(X;Z) &= H(Y) - H(Y|X) \\ &\quad -[H(Z) - H(Z|X)] \\ &= h(p_2) - h(p_1) + H(Y) - H(Z) \\ &\leq h(p_2) - h(p_1). \end{aligned}$$

The last inequality follows from the well-known fact (see [43]) that the entropy of the output of a binary symmetric channel, i.e. $H(Z)$, is no smaller than the entropy of the input, $H(Y)$.

Now that $I(X;Y)$ and $I(X;Y) - I(X;Z)$ are simultaneously maximized at $P(X = 1) = P(X = 0) = 1/2$, we conclude that, for BSBC, $\mathcal{R}_{BCP}$ is given as

$$\begin{aligned} 0 &\leq R_e \leq R_1, \\ R_e &\leq h(p_2) - h(p_1), \\ R_1 + R_p &\leq 1 - h(p_1). \end{aligned}$$

From this example, it is clear that R_p can be as large as $1 - h(p_1)$ whereas for the BCCC model, the non-confidential message rate $R_0 \leq 1 - h(p_2)$. Furthermore, if the

non-confidential message rate is set at $1 - h(p_2)$, it can be easily verified that for the BCCC model, $R_1 = R_e = 0$ whereas for the BCCP model $R_1 = R_e = h(p_2) - h(p_1)$ can be achieved.

3.3.4 Gaussian channel

Our main result can also be extended to the Gaussian case as follows.

Theorem 9. *For the Gaussian BCCP, $\mathcal{R}_{BCP}$ is a set consisting of those triples (R_1, R_e, R_p) satisfying*

$$\begin{aligned} 0 &\leq R_e \leq R_1, && (3.23) \\ R_e &\leq C\left(\frac{P}{N_1}\right) - C\left(\frac{P}{N_2}\right), && (3.24) \\ R_1 + R_p &\leq C\left(\frac{P}{N_1}\right), && (3.25) \end{aligned}$$

where the noises of channel 1 and 2 are both independently and identically distributed (i.i.d.) Gaussian sequences with variances N_1 and N_2 respectively, with $N_1 \leq N_2$. The power constraint of the channel input is $\mathrm{E}(X^2) \leq P$. $C(\cdot)$ is defined as $C(x) = \frac{1}{2}\log(1+x)$.

3.3.5 The source-channel matching problem

Our main results in the above sections pertain to a channel coding problem. The problem of source channel matching can be treated in a similar fashion as that of [3].

Consider two memoryless sources with alphabets $\mathcal{S}$ and $\mathcal{T}$, i.e., let $S_1T_1, S_2T_2, \cdots$

be i.i.d. pairs of RV's (but S_i and T_i need not be independent). Assume that block-to-block encoding is used: a (k, n)-encoder is a (stochastic) encoder in the sense of Definition 1 with block length n and message sets (S^k, T^k).

Definition 4. *The source pair S, T is (R, Δ)-transmissible over the BCCP, where $R > 0$, $\Delta \geq 0$, iff for every $\epsilon > 0$ there exist a (k, n)-encoder f and decoders φ, ψ such that*

$$\begin{aligned} \frac{k}{n} &\geq R - \epsilon, \\ \frac{1}{k} H(S^k | Z^n) &\geq \Delta - \epsilon, \\ \mathrm{E}\left[\frac{1}{k} d_H\left(S^k T^k, \varphi(Y^n)\right)\right] &\leq \epsilon. \end{aligned}$$

We shall refer to R as the rate of source-channel matching.

Theorem 10. *In order that the source pair S, T be (R, Δ)-transmissible over the BCCP, it is necessary and sufficient that*

$$(RH(S), R\Delta, RH(T|S)) = (R_1, R_e, R_p) \in \mathcal{R}_{BCP}.$$

Proof. It is similar to the proof in [3, Theorem 3] by replacing $(RH(S|T), R\Delta, RH(T))$ with $(RH(S), R\Delta, RH(T|S)$. □

3.3.6 The model with three classes of messages

We can also generalize the result to transmitting three messages: confidential message with rate R_1, common message with rate R_0 and public message with rate R_p, which is defined as follows.

Definition 5. *(R_1, R_e, R_0, R_p) is an achievable rate quadruple for broadcast channels with confidential, common, and public messages* iff *for every $\epsilon > 0$ and sufficiently large n there exists a sequence of message sets $\mathcal{S}^n$,$\mathcal{T}_1^n$,$\mathcal{T}_2^n$ and encoder-decoder (f, φ, ψ) giving rise to (n, ϵ)-transmission, such that*

$$\begin{aligned}
\lim_{n\to\infty} \frac{1}{n} \log \|\mathcal{S}^n\| &= R_1, \\
\lim_{n\to\infty} \frac{1}{n} \log \|\mathcal{T}_1^n\| &= R_0, \\
\lim_{n\to\infty} \frac{1}{n} \log \|\mathcal{T}_2^n\| &= R_p, \\
\frac{1}{n} H(S^n|Z^n) &\geq R_e - \epsilon.
\end{aligned}$$

The definition of (n, ϵ_n) transmission in Definition 5 is now amended by requiring that both receivers correctly recover the common message T_1^n with probability $\geq 1 - \epsilon_n$.

The following theorem describes the rate equivocation region for the generalized model, whose proof is omitted as it can be directly constructed by combining the proofs for BCCC and BCCP models.

Theorem 11. *The rate equivocation region $\mathcal{R}_{3msg}$ is a closed convex set consisting of those quadruples (R_1, R_e, R_0, R_p) for which there exist RV's $U \to V \to X \to YZ$ such that the conditional distribution of Y (resp. Z) given X is determined by channel 1 (resp. 2) and*

$$\begin{aligned}
0 &\leq R_e \leq R_1, \\
R_e &\leq I(V;Y|U) - I(V;Z|U),
\end{aligned}$$

$$
\begin{aligned}
R_1 + R_0 + R_p &\leq I(V;Y|U) + \min(I(U;Y), I(U;Z)), \\
0 &\leq R_0 \leq \min(I(U;Y), I(U;Z)).
\end{aligned}
$$

Apparently this theorem constitutes a generalization of the results of both BCCP and BCCC.

3.4 Proof of Theorem 7

The direct part proof of Theorem 7 utilizes Lemma 2 in [3] (as repeated in Proposition 10), and the essential idea is to split the messages bits into three indices M_J, M_K, M_L as shown in Fig. 3.6, where

$$
\begin{aligned}
\frac{1}{n}\log\|M_L\| &= \min(I(U;Y), I(U;Z)) - \epsilon; \\
\frac{1}{n}\log\|M_K\| &= I(X;Y|U) - I(X;Z|U) - \epsilon, \\
\frac{1}{n}\log\|M_J\| &= I(X;Z|U) - \epsilon.
\end{aligned}
$$

As discussed before, M_K will be kept completely secret and thus part of confidential message bits are put into M_K to achieve equivocation rate, and the rest confidential message and also total public message bits are put into M_J and M_L in order to be transmitted to the legitimate receiver correctly. We skip the details here except to point out that our proof, as in [3], also relies on the convexity argument: we first establish the achievability of a subset of $\mathcal{R}_{BCP}$ and then generalize it to the entire $\mathcal{R}_{BCP}$ through a simple convexity argument.

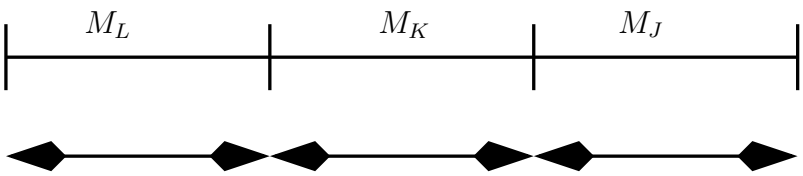


Figure 3.6: Encoding scheme of direct part proof.

The converse proof is similar to that in Section 2.6.1. Let us assume the existence of encoder-decoders (f, φ, ψ) giving rise to (n, ϵ_n)-transmission over the BCCP. By Fano's Lemma we have

$$\frac{1}{n}H(ST|Y^n) \leq \eta_n.$$

where $\eta_n \to 0$ if $\epsilon_n \to 0$. We shall show the existence of random variables $U \to V \to X \to YZ$ such that

$$\begin{aligned} R_e &\leq I(V;Y|U) - I(V;Z|U) + \eta_n, \\ R_1 + R_p &\leq I(V;Y|U) + \min(I(U;Y), I(U;Z)) + \eta_n. \end{aligned}$$

Note that Eq. (3.4) is readily established from the fact that $H(S|Z^n) \leq H(S)$ and the definition in Eq. (3.1) and (3.3).

First,

$$\begin{aligned} n(R_1 + R_p) &= H(ST) \\ &\leq I(ST;Y^n) + n\eta_n \end{aligned} \tag{3.26}$$

For R_e, we have

$$nR_e \leq H(S|Z^n)$$

$$\begin{aligned} &\leq H(ST|Z^n) \\ &\leq I(ST;Y^n) - I(ST;Z^n) + n\eta_n. \end{aligned} \tag{3.27}$$

Defining $Y^i = (Y_1, \cdots, Y_i)$, $\tilde{Z}^i = (Z_i, \cdots, Z_n)$, similar as the converse proof in [3], we have

$$\begin{aligned} I(ST;Y^n) &= \sum_{i=1}^{n} I(ST;Y_i|Y^{i-1}\tilde{Z}^{i+1}) + \Sigma_1 - \Sigma_2, \\ I(ST;Z^n) &= \sum_{i=1}^{n} I(ST;Z_i|Y^{i-1}\tilde{Z}^{i+1}) + \Sigma_1^* - \Sigma_2^*, \end{aligned}$$

where

$$\begin{aligned} \Sigma_1 &= \sum_{i=1}^{n} I(\tilde{Z}^{i+1};Y_i|Y^{i-1}), \\ \Sigma_1^* &= \sum_{i=1}^{n} I(Y^{i-1};Z_i|\tilde{Z}^{i+1}), \\ \Sigma_2 &= \sum_{i=1}^{n} I(\tilde{Z}^{i+1};Y_i|Y^{i-1}TS), \\ \Sigma_2^* &= \sum_{i=1}^{n} I(Y^{i-1};Z_i|\tilde{Z}^{i+1}TS). \end{aligned}$$

By [3, Lemma 7], we know

$$\begin{aligned} \Sigma_1 &= \Sigma_1^*, \\ \Sigma_2 &= \Sigma_2^*. \end{aligned}$$

Furthermore,

$$\begin{aligned} \Sigma_1 &= \sum_{i=1}^{n} I(\tilde{Z}^{i+1};Y_i|Y^{i-1}) \leq \sum_{i=1}^{n} I(\tilde{Z}^{i+1}Y^{i-1};Y_i), \\ \Sigma_1^* &= \sum_{i=1}^{n} I(Y^{i-1};Z_i|\tilde{Z}^{i+1}) \leq \sum_{i=1}^{n} I(\tilde{Z}^{i+1}Y^{i-1};Z_i). \end{aligned}$$

Let us introduce an RV J, which is independent of (S, T, X^n, Y^n, Z^n) and uniformly distributed over $\{1, \cdots, n\}$. Set

$$U \triangleq Y^{J-1}\tilde{Z}^{J+1}J, \quad V \triangleq UST, \quad X \triangleq X_J,$$
$$Y \triangleq Y_J, \qquad\qquad Z \triangleq Z_J.$$

Then we have

$$\frac{1}{n}\left(I(ST;Y^n) - I(ST;Z^n)\right) = I(V;Y|U) - I(V;Z|U); \tag{3.28}$$
$$\frac{1}{n}\Sigma_1 = \frac{1}{n}\Sigma_1^* \leq \min(I(U;Y), I(U;Z)). \tag{3.29}$$

Substituting Eq. (3.28)-(3.29) into Eq. (3.26)-(3.27), we have

$$\begin{aligned} R_e &\leq I(V;Y|U) - I(V;Z|U) + \eta_n, \\ R_1 + R_p &\leq I(V;Y|U) + \min(I(U;Y), I(U;Z)) + \eta_n. \end{aligned}$$

Using the memoryless property of the channel, it is straightforward to verify that $U \to V \to X \to YZ$ and that the conditional distribution of Y and Z given X coincide with the corresponding channel matrices. The converse proof is complete.

The support lemma [44, Page 310] is invoked to prove that the region $\mathcal{R}_{BCP}$ is not altered if the alphabet sizes of U, V are bounded as in Eqs. (3.7) and (3.8) (similar to [3, Appendix]).

3.5 Secret Key Enhanced BCCP Model

In this section, we extend the BCCP model to systems where a secret key, K, with a key rate R_k, is available to the intended transceiver pair. The key enhanced BCCP model is illustrated in Fig. 3.7.

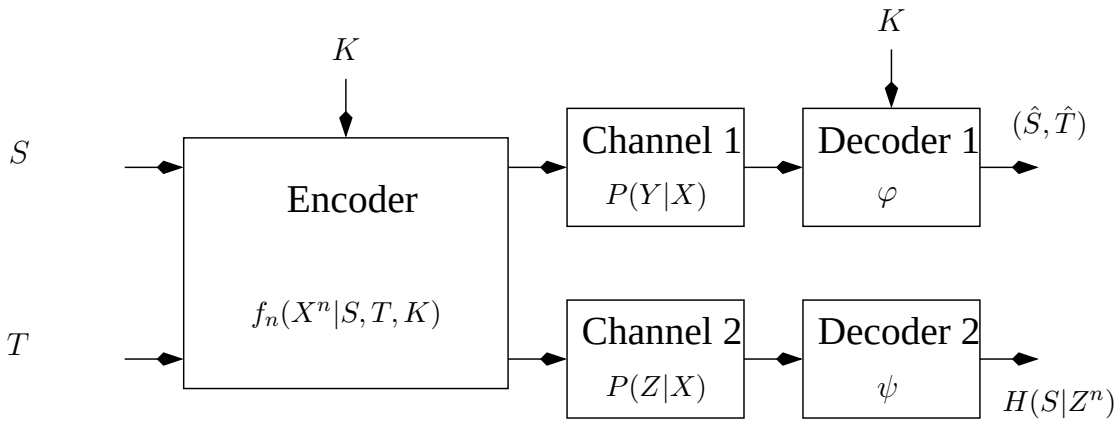


Figure 3.7: Key enhanced BCCP model.

Closely related to the present model is the so-called rate-distortion theory for the Shannon cipher system studied by Yamamoto [45]. In [45], in addition to having a secret key known to the transmitter and the intended receiver, the main channel is assumed to be less noisy than the wire-tap channel, and a single confidential source is to be communicated to the main receiver. The encoding scheme essentially concatenates three codes: one to attain the ordinary rate distortion function, a random code for the wire-tap channel, and the Shannon cipher's modulo addition encoding. It was shown in [45] that the security contributions from that of the random wire-tap

encoding and the secret key are additive.

In this section, we consider the general discrete memoryless broadcast channel instead of the less noisy channel. In addition, a non-confidential message is also to be transmitted along with the confidential message. On the other hand, we only consider the channel coding problem; therefore arbitrarily small error probability is imposed for recovering the messages at the receiver instead of a general distortion constraint. Our result indicates that for this channel coding problem for the general model, the effects of random encoding and secret key are still additive, as reflected in the expression for the equivocation rate. The additive contribution to the equivocation rate suggests that secret key can be used to enhance the secrecy capacity attained via the wire-tap encoding. Furthermore, in the worst event that the receiver 2 sees a less noisy channel than receiver 1, positive secrecy rate is still possible if the key rate is sufficiently large.

The rate equivocation region of secret key enhanced BCCP is described in the following theorem.

Theorem 12. *Assume R_k is the secret key rate. The rate equivocation region $\mathcal{R}_{SP}$ is a closed convex set consisting of rate triples (R_1, R_p, R_e) for which there exist random variables $U \to V \to X \to YZ$ such that the conditional distribution of Y (respectively Z) given X is determined by channel 1 (respectively 2) and*

$$0 \leq R_e \leq R_1, \tag{3.30}$$

$$R_e \leq [I(V;Y|U) - I(V;Z|U)]^+ + R_k, \tag{3.31}$$

$$R_1 + R_p \leq I(V;Y|U) + \min(I(U;Y), I(U;Z)), \tag{3.32}$$

where $[\cdot]^+$ is defined as $[x]^+ = \max\{x, 0\}$.

The direct part of Theorem 12 can be proved, as with [45], by concatenation of two codes: Csiszár and Körner's random channel code [3] and Shannon's modulo addition code [1], [46]. The converse proof follows along the similar line as that for the BCCP model in Section 3.4 (or see [47, 48]). We will omit the detailed proof as the model is in fact a special case of what to be studied in the next chapter.

From Theorem 12, one can see that the secret key does not affect the rate constraints for R_c and R_p. This is due to the reasonable assumption that the key K is independent of the channel and the information sources. The enhancement of secrecy due to the presence of key is in an additive manner, as measured by the equivocation rate, i.e., Eq. (3.31). Consider, for example, an extreme case in which channel 2 is less noisy than channel 1. For such a case, $R_e = 0$ for the classical BCCP; however, for BCCP with a secret key, a positive R_e can still be attained if the key rate $R_k > 0$.

This result also coincides with various existing results, which is discussed in the following subsections.

3.5.1 Shannon cipher system

In [1] Shannon assumed that both the intended receiver and an eavesdropper have an uncorrupted copy of the encrypted message. By setting $Y = Z = X$, the channels become noiseless and our model reduces to Shannon's cipher system. From Theorem 12,

we have

$$\begin{aligned} 0 &\leq R_e \leq R_1, && (3.33)\\ R_e &\leq R_k, && (3.34)\\ R_1 + R_p &\leq I(V;X|U) + I(U;X) = I(V;X). && (3.35) \end{aligned}$$

If perfect secrecy is required, i.e. $R_1 = R_e$, then we have $R_1 = R_e \leq R_k$ and correspondingly $H(S) \leq H(K)$. Notice that the condition $H(S) \leq H(K)$ is precisely the same as that obtained in [1] for Shannon cipher system.

3.5.2 Yamamoto's model

Our model considers a channel coding problem, while Yamamoto's model [45] considered a source-channel coding problem, that is, [45] is concerned with the transmissibility of a source sequence instead of a message set. To be concrete, we introduce the following definition from [45].

Definition 6. *[45, Definition 1]: (R, R'_k, D, h) is achievable if for any $\epsilon \geq 0$ and sufficiently large K and N, there exists a code (f, ϕ) satisfying*

$$\begin{aligned} \frac{N}{K} &\leq R + \epsilon,\\ \mathrm{E}d^{(K)}(S^K, \hat{S}^K) &\leq D + \epsilon,\\ \frac{1}{K}\log \mathcal{M}^k &\leq R'_k + \epsilon,\\ \frac{1}{K}H(S^K|Z^N) &\geq h - \epsilon. \end{aligned}$$

We note again that [45] deals with a single message source (i.e., no public message is considered) hence only a single rate R is needed. Since for the BCCP model, receiver 1 is to recover message arbitrarily reliably, this is equivalent to having $D = 0$, hence $R(D) = H(S)$. Similar to the source-channel matching part [3, Theorem 2], we have

Proposition 13. *The source rate quadruple* $(R, R'_k, 0, h)$ *is admissible* iff

$$\left(\frac{H(S)}{R}, \frac{h}{R}, \frac{R'_k}{R}\right) = (R_1, R_e, R_k) \in \mathcal{R}_{S1e}, \tag{3.36}$$

where $\mathcal{R}_{S1e}$ *is the achievable rate region for key-assisted BCCP with no public message, i.e.,* $(R_1, R_e) \in \mathcal{R}_{S1e}$ iff $(R_1, R_e, 0) \in \mathcal{R}_{SP}$.

Moreover, it is also assumed in [45] that channel 1 is less noisy than channel 2. Specializing Theorem 12 to this model, we have

Proposition 14. *If channel 1 is less noisy than channel 2 then* $(R_1, R_e) \in \mathcal{R}_{S1e}$ iff *there exist* X, Y, Z *such that*

$$0 \leq R_e \leq I(X;Y) - I(X;Z) + R_k, \tag{3.37}$$

$$R_e \leq R_1 \leq I(X;Y). \tag{3.38}$$

Proof. It is also quite similar to the proof of [3, Theorem 3]. □

From Proposition 13 and Proposition 14, it is straightforward to show that Proposition 14 coincides with Yamamoto's result [45, Theorem 1] with $D = 0$ which we repeat below.

Proposition 15. $(R, R'_k, D = 0, h)$ *is admissible* iff *there exist r.v's X,Y, and Z that satisfy*

$$I(X;Y)R \geq H(S), \tag{3.39}$$

$$R'_k \geq [h - \{I(X;Y) - I(X;Z)\}R]^+. \tag{3.40}$$

3.6 Summary

We revisited the problem of broadcasting both a confidential and a non-confidential message for discrete memoryless broadcast channels. The present model differs from the classical model of Csiszár and Körner in that the non-confidential message need not be reliably recovered at receiver 2. A single letter characterization of the rate equivocation region was provided. By relaxing the constraint on the non-confidential message, the new approach improves the equivocation rate for the confidential message compared with the classical model. Furthermore, this BCCP framework was also extended to systems where a secret key is available to the intended transceiver pair. The results reveal that the secret key and the random coding technique for broadcast channels with confidential messages contribute to the secrecy of the confidential message in an additive manner.

More interestingly, this more liberal treatment of the non-confidential message might be a more reasonable model and can be applied to various secure communication models which are otherwise not attainable using the classical BCCC model.

Finally, we would like to point out that upon concluding this work, the author discovered that a special case of this BCCP model was discussed in [44, Problem 4.33(c), Chapter 3, Section 4]. There, perfect secrecy of the confidential message is required and the result is consistent with our result when specializing Theorem 7 to the case of $R_1 = R_e$.

Chapter 4

Secure Coding Over Networks

In this chapter we study the problem of secure communication over networks in which each link may be noisy or noiseless. Specially, a single-source single-sink acyclic planar network is assumed, and the communication between the source and the sink is subject to non-cooperating eavesdropping on each link. A constructive proof, which combines Shannon's key encryption, Wyner's random coding, and the Ford-Fulkerson algorithm, is presented which constitutes a readily implementable secure coding scheme for provably secure communications. This explicit encoding and routing scheme leads to an achievable rate equivocation region for the secure coding over network model, which is shown to be tight when specializing to a network of non-overlapping parallel links.

4.1 Introduction

The BCCP framework, proposed in Chapter 3, enlarges the rate equivocation of the classical BCCC model of Csiszár and Körner. Perhaps more significantly, the more liberal treatment of the non-confidential message makes it more readily applicable to complex communication networks. One simple example is illustrated in Fig. 4.1, where communication is conducted over two independent sub-channels, and each sub-channel is subject to a non-cooperating eavesdropper: Eve 1 or Eve 2, which do not communicate with each other. To understand how it works, we note that in the Shannon cipher system, the secret key needs to be kept secret from the eavesdropper as it also has access to the encrypted message. However, given the independence between the key and the confidential message, if an eavesdropper only has access to the secret key but without any knowledge of the encrypted message, complete secrecy is still attained. Thus the simple achievable scheme for the motivating example is to communicate a secret key K on link 1 while transmit the key-encrypted message $S \oplus K$ on link 2, as depicted in Fig. 4.1. Protection against eavesdropping on link 2 is attributed to the provable security of one-time pad. On the other hand, the eavesdropper on link 1 has only access to the key but not the encrypted message hence is also completely ignorant of the message. We comment here that similar observation was made to motivate the so-called secure network coding in [13] where communication between a single source and multiple sinks is conducted over a noiseless network.

This intuitively simple idea can be applied to a more general setting which we

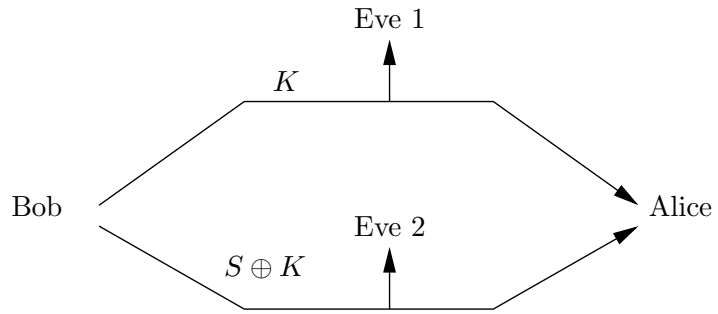


Figure 4.1: A motivating example of secure communication over multiple links.

consider in this chapter, namely secure communication over noisy/noiseless networks where each link can be modeled as a wiretap channel. This is illustrated in Fig. 4.2 where the eavesdroppers do not cooperate, i.e., the eavesdroppers do not communicate with each other. A practically more meaningful yet equivalent interpretation is that communication is subject to link eavesdropping yet the location of the eavesdropper is unknown. Thus to measure the security of this system, the equivocation rates over every link need to be considered simultaneously. For this model with the assumption of acyclic single-source single-sink planar graph, we obtain an achievable rate equivocation region, which is shown to be tight when specializing to several special cases. A more important contribution is the explicit coding and bit routing scheme that combines the classical Ford-Fulkerson algorithm [49] for Max-flow Min-cut network flow, the one-time pad scheme, and the random coding to achieve the desired rate equivocation rate-tuple.

Closely related to the present model is the so-called secure network coding problem, first introduced in [13] and further developed in [50, 51]. The model used in [13]

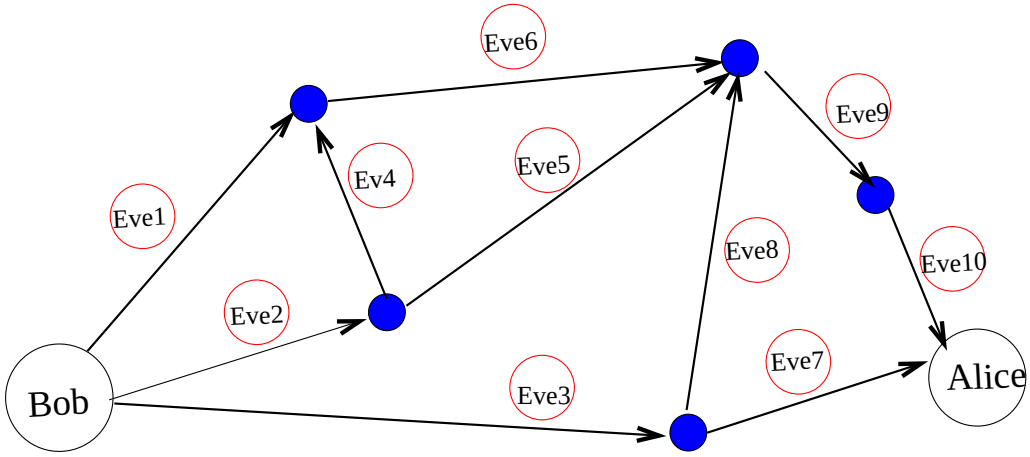


Figure 4.2: An example of network with non-cooperating eavesdropping

is a multi-graph network, where the noiseless network with unit capacity edges is used to multicast information to multiple sinks. An adversary is assumed to have access to an intact copy of information communicated over a subset of edges. The collection of those subsets are known to the designer. For this multicast model, the existence of such a secure linear network code is proved in [13]. With an additional constraint on the edge subsets, more efficient algorithms to construct the secure network code were proposed in [50, 51]. However, the network coding scheme proposed in [50, 51] do not directly apply to the unicast model with eavesdropping on individual link due to the added constraint on the edge subsets. In addition, the secure coding scheme proposed in the present work is much more efficient to implement and intuitive to understand.

This work is also a generalized model of Yamamoto's work on secret sharing system [10,46,52], where two parallel broadcast channels with degradedness assumption were

studied. There were also some recent about parallel/compound wiretap channels [16, 53, 54]. The model used there however is drastically different: it was assumed in [16, 53, 54] that a single adversary can simultaneously eavesdrop all parallel links whereas we assume non-cooperating eavesdropping in which each link is subject to individual eavesdropping.

The rest of the chapter is organized as follows. Section 4.2 gives the problem formulation and reviews related results. The main theorem for noiseless case is given in Section 4.3, along with discussions about its major implications. Section 4.4 gives the proof where an explicit code construction and a network routing scheme are provided. It is then generalized to noisy case in Section 4.5. Section 4.6 discusses an interesting special case, parallel links. We conclude in Section 4.7.

4.2 Problem Formulation and Related Work

Fig. 4.2 illustrates the model studied in this chapter. We give detailed description below.

- The pair $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ is called a directed graph, where $\mathcal{V}$ and $\mathcal{E}$ are the node set and the edge set of $\mathcal{G}$, respectively. Denote by $Out(v)$ and $In(v)$ the edge sets flowing into and out of the node v, respectively.

- The node set $\mathcal{V}$ contains a source node u and a sink node d. The messages S and T are encoded at node u and then transmitted through the network to d.

Both S and T are required to be reliably decoded at node d, and S needs to be kept confidential from all eavesdroppers.

- The links in the network are subject to non-cooperating eavesdropping. We model each link as a general discrete memoryless broadcast channel, $p(y_{io}z_{io}|x_{io})$ for each $(i,o) \in \mathcal{E}$, where z_{io} is the observation of the eavesdropper and y_{io} is the observation for the legitimate node o. The network is noiseless if each DMBC (i,o) satisfies $x_{io} = y_{io} = z_{io}$. Otherwise, the network is said to be noisy.

The achievable rate tuple $(R_c, R_p, R_{e,io})$, $(i,o) \in \mathcal{E}$, is defined as follows.

Definition 7. *The encoder-decoder (f, f_r, φ), $r \in \mathcal{V}$, $r \neq u, d$, gives rise to (n,ϵ)-transmission over the network $\mathcal{G}$* iff *for every $s \in \mathcal{S}$, $t \in \mathcal{T}$, the encoder $f : \mathcal{S} \times \mathcal{T} \rightarrow (X_i^n, i \in Out(u))$, mapping at each individual node $f_r : (Y_i^n, i \in In(r)) \rightarrow (X_i^n, i \in Out(r))$, and the decoder $\varphi : (Y_i^n, i \in In(d)) \rightarrow \mathcal{S} \times \mathcal{T}$, give the correct (s,t) at the sink node with probability $\geq 1 - \epsilon$.*

We note that the encoder-decoder defined above also include all mappings at intermediate nodes.

Definition 8. *$(R_c, R_p, R_{e,io})$, $(i,o) \in \mathcal{E}$ is an achievable rate tuple for the network* iff *there exists encoder-decoder (f, f_r, φ) for the message sets $\mathcal{S}^n$,$\mathcal{T}^n$ giving rise to (n, ϵ_n)-transmission with $\epsilon_n \rightarrow 0$, such that for $(i,o) \in \mathcal{E}$*

$$\lim_{n\rightarrow\infty} \frac{1}{n} \log \|\mathcal{S}^n\| \;\; = \;\; R_c, \tag{4.1}$$

$$\lim_{n\to\infty} \frac{1}{n} \log \|\mathcal{T}^n\| = R_p, \tag{4.2}$$

$$\lim_{n\to\infty} \frac{1}{n} H(S^n|Z_{io}^n) \geq R_{e,io}; \tag{4.3}$$

Here, R_c is the confidential message rate transmitted over the network between the source node and the sink node; R_p is the key rate and the key itself is transmitted along with the confidential message through the network, which is in essence the public message described in the previous chapter; the equivocation rate $R_{e,io}$ measures the ignorance of the eavesdropper on link (i, o) with respect to the confidential message; $R_{e,io} = R_c$ implies perfect secrecy against the eavesdropper on link (i, o). Here we comment that, since each link in the network is subject to non-cooperating eavesdropping, we need to consider equivocation rates for all links in the network.

4.2.1 Related Work

The network model is related to that of [13], where, instead of a single sink, they studied the problem of multicasting information securely to multiple destinations D against eavesdropping $\mathcal{A}$. $\mathcal{A}$ is a collection of edge sets and the eavesdropper has complete access to one of the edge sets, while his/her choice is unknown to the transmitter. [13, Theorem 2] specifies the conditions under which it is possible to obtain an admissible linear network code to achieve perfect secrecy. The existence of such code is hard to verify directly from [13, Theorem 2]; instead, a more explicit sufficient condition is given in [13, Theorem 3], and repeated below.

Proposition 16. *[13, Theorem 3] The message S has $n-k$ bits and the independent random key has k bits. Let $\mathcal{G}^* = (\mathcal{V}, \mathcal{E}^*)$, where $\mathcal{E}^* \subset \mathcal{E}$, be a subgraph of $\mathcal{G}$ satisfying the following:*

1. *For any destination $d \subset D$, there are n disjoint paths in $\mathcal{G}^*$ from the source node u to the sink node d ,where the paths are unit-capacity.*

2. *For any $A \subset \mathcal{A}$, there are at most k disjoint paths in $\mathcal{G}^*$ from the source node u to the channels in $A \subset \mathcal{E}^*$.*

If such a subgraph $\mathcal{G}^*$ exists, then there exists an admissible network code to transmit the message S with perfect secrecy.

The noiseless case of the present model is also related to the celebrated Max-flow Min-cut theorem [49, 55] in network flow. Assume that each link in the network is noiseless with capacity C_{io}, $(i,o) \in \mathcal{E}$. The Max-flow Min-cut theorem can be stated as follows.

Proposition 17. *The maximal throughput C_G of a network $\mathcal{G}$, i.e., the network capacity, is*

$$C_G = \min_{Cut} \sum_{(i,o)\in(IO)^l_{cut}} C_{io},$$

where Cut is defined as a cut of this network [56], which splits the node set $\mathcal{V}$ into two disjoint subsets: a source subset $\mathcal{U}_{Cut}$ and a sink subset $\mathcal{D}_{Cut}$, where $u \in \mathcal{U}_{Cut}$ and $d \in \mathcal{D}_{Cut}$; $(IO)^l_{cut}$ is defined as the edge set for this given cut Cut, where for $j = 1, 2, \cdots, l$, $(i,o)_{cut,j} \in \mathcal{E}, i_{cut,j} \in \mathcal{U}_{Cut}, o_{cut,j} \in \mathcal{D}_{Cut}$.

4.3 Noiseless Case

We first consider a simple yet important case when each link in the network is noiseless and each eavesdropper has a verbatim copy of the message transmitted over the corresponding link. As such, random coding will not be useful. Instead, we will exploit the route diversity in the network in order to achieve the desired security: the fact that the source may have multiple independent routes to the destination allows the sender to encode the message in such a way that for an adversary that eavesdrops on a single link, it will gain no information about what is transmitted. One logical step is to use the Ford-Fulkerson algorithm for maximum network flow to obtain a information transmission path set and then appropriately encrypted the messages transmitted over this path set. However, different paths may share the common links and protection against eavesdropping over those shared links needs to be carefully devised. In the following, we give an achievable rate region, obtained by imposing an additional constraint on the structure of the network. Specifically, we assume a planar graph [56], meaning that the graph can be drawn on the plane in such a way that its edges intersect only at their nodes. This assumption simplifies the proof and is also a meaningful model to describe real computer or communication networks.

Theorem 13. *The rate tuple for a planar graph network,* $(R_c, R_p, R_{e,io})$, $(i,o) \in \mathcal{E}$, *is achievable,* if *there exist auxiliary numbers* r_{io} *such that*

$$r_{io} \;\leq\; C_{io}, \tag{4.4}$$

$$0 \leq r_{io} \leq R_c + R_p, \tag{4.5}$$

$$0 \leq R_{e,io} \leq R_c, \tag{4.6}$$

$$0 \leq R_c + R_p \leq \min_{Cut} \sum_{(i,o)\in(IO)^l_{cut}} r_{io}, \tag{4.7}$$

$$R_{e,io} \leq R_c + R_p - r_{io}. \tag{4.8}$$

We can provide intuitive interpretation of Theorem 13 below.

1. r_{io} can be viewed as the bits transmitted via the present edge (i, o).

2. Eq. (4.4) is natural as the transmitted bits can not exceed the present edge's capacity.

3. The transmitted bits come from the confidential and public messages and thus can not exceed the total rate, which results in Eq. (4.5).

4. Eq. (4.6) is obvious as the equivocation rate $R_{e,io}$ can not exceed the confidential message rate R_c itself.

5. Eq. (4.7) implies that total throughput can not exceed the network capacity according to the celebrated Max-flow Min-cut Theorem.

6. Eq. (4.8) implies that $R_{e,io}$ is bounded by the bits which are not transmitted via the present edge (i, o). To be more precise, the rate $R_c + R_p - r_{io}$ can be further split into two parts: the first part is the confidential message not transmitted via the present edge (i, o), which is automatically kept perfectly secret from the wiretapper of edge (i, o); the second part comes from the public message that

is not transmitted via the link (i, o) which will serve as a secret key for the bits transmitted via (i, o).

Applying perfect secrecy constraint for all links, i.e., $R_{e,io} = R_c$ for all $(i, o) \in \mathcal{E}$, the rate region reduces to the following.

Proposition 18. *A rate pair (R_c, R_p) can attain perfect secrecy* if

$$0 \leq R_c + R_p \leq \min_{Cut} \sum_{(i,o)\in(IO)^l_{cut}} r_{io}, \tag{4.9}$$

$$r_{io} \leq C_{io}, \tag{4.10}$$

$$r_{io} \leq R_p, \tag{4.11}$$

which can be simplified as

$$0 \leq R_c + R_p \leq \min_{Cut} \sum_{(i,o)\in(IO)^l_{cut}} \min(C_{io}, R_p).$$

We defer the proof of Theorem 13 to Section 4.4; the achievability proof provides an intuitive secure coding scheme that is rather easy to implement and intuitive to understand. In the following, we discuss various special cases of our main result.

4.3.1 Without secrecy constraint

Not surprisingly, in the absence of secrecy constraint, Theorem 13 reduces to the well-known Max-flow Min-cut theorem for a single-source single-sink network (see Proposition 17), where $R_c + R_p$ represents the entire throughput of the network. Thus the coding scheme would indeed achieve optimal throughput in the absence

of secrecy constraint. Our result actually provides an alternative expression of the Max-flow Min-cut theorem,

$$0 \leq r_{io} \leq R_c + R_p; \tag{4.12}$$

$$r_{io} \leq C_{io}, \tag{4.13}$$

$$0 \leq R_c + R_p \leq \min_{Cut} \sum_{(i,o)\in(IO)^l_{cut}} r_{io}. \tag{4.14}$$

4.3.2 Relationship with Cai and Yeung's result

We comment that Proposition 18 is in fact consistent with the result in [13] (as repeated in Proposition 16).

Specializing Proposition 16 to the network with only one single sink and restricting each wiretap edge set $A \in \mathcal{A}$ to correspond to each individual link in the network, the subgraph concept in Proposition 16 coincides with that of the auxiliary number r_{io} in Proposition 18[1]. This implies Eq. (4.10). Now that the network has totally $\min_{Cut} \sum_{(i,o)\in(IO)^l_{cut}} r_{io}$ disjoint paths each with unit capacity, it is therefore easy to show that conditions 1) and 2) in Proposition 16 also coincide with Eqs. (4.9) and (4.11).

Therefore, the result of Proposition 18 is consistent with that of [13, Theorem 3] when reduced to a single sink case. However, as we shall see from the following achievability proof, different from [13, Theorem 3] where sufficient condition for the existence of a network code is addressed, we will provide an explicit and simple code

[1]The idea of auxiliary numbers was first introduced in Yamamoto's treatment of secret sharing communication systems [52].

construction for secure communication over networks.

4.4 Achievability Proof

In the following, we give the proof of Theorem 13. Our proof utilizes the so-called reduced network concept (illustrated in Fig. 4.3(b)), as a result of applying the Ford-Fulkerson algorithm. The encryption and bit routing on the reduced graph occur over virtually parallel paths (reminiscent that of [48]). The remaining difficulty is to deal with the case when common edges are shared by neighboring paths. This is accomplished by the way encoded bits are distributed to the paths and the associated entropy property (c.f. Lemma 7).

4.4.1 Revisit the Ford-Fulkerson algorithm

Prior to the achievability proof, we first revisit the Ford-Fulkerson algorithm which was used for the achievability proof of the Max-flow Min-cut theorem. We begin with some definitions.

Definition 9. *In a directed graph $\mathcal{G}$, a* Path *is a sequence of edges $e_1, e_2, \cdots, e_l$ such that $e_1 \in Out(u), e_l \in In(d)$, and for $1 < i < l$ there exist $r_i \in \mathcal{V}$ such that $e_i \in In(r_i)$ and $e_{i+1} \in Out(r_i)$.*

Definition 10. *Two paths* share *an edge or node if this edge or node is contained by two paths. Two paths are* different *if one path contains no less than one edge that is*

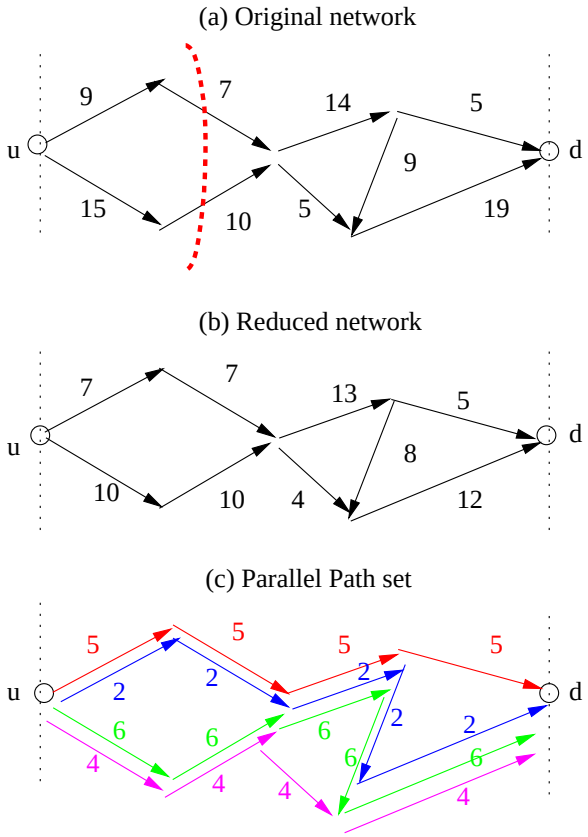


Figure 4.3: An example illustrating the achievability proof.

not shared by the other path. A path with flow amount f *means that each edge of this path has flow* f *and thus an information flow with total amount* f *can go through this pipeline path from* u *to* d*.*

The Ford-Fulkerson algorithm is stated below.

1. Set $i = 1$.

2. Find *any* path from the source node to the sink node that has a strictly positive flow capacity remaining in each edge. If there is no such path left, exit.

3. Determine f_i, the maximum flow along this path, which will be equal to the smallest flow amount on any edge in the path (the bottleneck edge).

4. Store this path as $Path_i$ with flow amount f_i.

5. Subtract f_i from the remaining flow capacity in the forward direction for each edge in the path. Add f_i to the remaining flow capacity in the backwards direction for each edge in the path.

6. Set $i = i + 1$. Go to step 2).

The Ford-Fulkerson algorithm is a 'greedy' approach to find a set of paths such that on termination, the sum of the flows along those paths gives the maximal total flow between the source and the sink nodes. This path set constitutes the so-called *reduced network*, which has the following properties.

1. The graph of the reduced network is the same as that of the original network except possibly that some edges of the original network are missing (with 0 flow amount).

2. Each edge in the reduced network has a flow amount equal to or less than the capacity of the corresponding edge in the original network.

3. The sum flow amounts of the input and output edges of any node in the reduced network are equal. The sum flow amount from the source subset to the sink subset for any cut in the reduced network is equal to the min-cut value of the original network.

The following proof utilizes this reduced network.

4.4.2 Proof of Theorem 13

In this present section, we adopt an algorithmic approach to prove the achievability of Theorem 13. As we shall see, the proof itself provides an explicit and efficient method comprising of encoding, decoding, and bit routing for secure communication over a noiseless network.

To simplify the proof, we assume that the plane graph is bounded in the 2D plane, as illustrated in Fig. 4.3. The result can be extended to unbounded case by a simple manipulation of the bit sequences. For convenience, we introduce a virtual edge $In(u)$ flowing into the source node u and a virtual edge $Out(d)$ flowing out of the sink node d for this bounded graph.

We construct a code according to the following three steps.

Step 1 Convert the uniformly distributed message variables S^n and T^n into i.i.d. Bernoulli($\frac{1}{2}$) binary sequences $\mathbf{b} : b_1, \cdots, b_{nR_c}$ and $\mathbf{k} : k_1, \cdots, k_{nR_p}$.

Step 2 Pre-process the bit sequences $\mathbf{b}$ and $\mathbf{k}$ by modulo addition.

Step 3 Assign the processed bits to the paths in the reduced network in a proper way to ensure reliable and secure delivery to the destination.

Step 1 converts the present problem to binary case where one-time pad can be easily implemented by XOR (or modulo 2 addition). Steps 2 and 3 are further elaborated

below.

Step 2 The modulo 2 sum of the two binary sequences $\mathbf{b}, \mathbf{k}$ results in the encoded bit sequence $\mathbf{c}$ defined as,

$$\begin{aligned}\{c_1, c_2, \cdots, c_{nR_c+nR_p}\} &= \{k_1, \cdots, k_{nR_p}, b_1 \oplus k_1, b_2 \oplus k_2, \cdots, b_{nR_p} \oplus k_{nR_p}, \\ &\quad b_{nR_p+1} \oplus k_1, b_{nR_p+2} \oplus k_2, \cdots, b_{nR_c-1} \oplus k_{(nR_c-1)_{nR_p}}, \\ &\quad b_{nR_c} \oplus k_{(nR_c)_{nR_p}}\}\end{aligned}$$

where $(a)_b$ denotes a modulo b. Thus $\mathbf{c}$ is a length $n(R_p + R_c)$ sequence with the header bits, i.e., the first nR_p bits, corresponding to the public message bits (key bits) and the rest of the sequence obtained by repeatedly (if $R_p < R_c$) using the key bits $\mathbf{k}$ to encrypt (modulo 2 sum) the confidential message bits $\mathbf{b}$. If $R_p \geq R_c$, each key bit will be used at most once in the encryption process. The encoded sequence has the following property.

Lemma 7. *The conditional entropy of* $\mathbf{b}$ *given any contiguous length-r* ($r \leq n(R_c + R_p)$) *segment of the bit sequence* $\mathbf{c}$*, say,* $c_j, c_{j+1}, \cdots, c_{j+r-1}$*, satisfies*

$$H(\mathbf{b}|c_j, c_{j+1}, \cdots, c_{j+r-1}) = \min(nR_c, n(R_c + R_p) - r).$$

Lemma 7 can be easily proved by simple calculation, which is given in the appendix (Section 4.8.1).

Step 3 Due to Lemma 7, the desired secrecy, Eq. (4.8), is attained as long as it can be guaranteed that any bit sequence assigned to every link in the network is a contiguous segment from $\mathbf{c}$. Essentially, the solution is to construct a set of virtually

parallel paths in the network, which should also achieve the maximal throughput. This is illustrated in Fig. 4.3(c). Given such a virtually parallel path set, assigning the bit sequence **c** successively to those paths would automatically achieve the rate equivocation region described in Theorem 13.

In order to study the virtually parallel path set, we give the formal definition of the path *order* for the bounded plane graph.

Definition 11. *A path A is* higher *in order than a path B* iff *for any node r shared by A, B, the input and output edges of A, B at node r are* clockwise *ordered as $\{A_i, A_o, B_o, B_i\}$. Conversely, a path A is* lower *than a path B* iff *the edges are ordered as $\{B_i, B_o, A_o, A_i\}$. The paths A and B are said to* crossover *(i.e.,* unordered*) if the path A is neither* higher *nor* lower *than the path B. Thus, for an ordered path set, there exists no crossover path pair in the set.*

The examples are shown in Fig. 4.4. Alternatively, two paths are ordered (parallel) if there exists a line in the plane connecting the source and sink that separates these two paths.

Definition 12. *An edge $e = (i, o)$ is* higher *than a path A* iff *there exist a path B in the network, which contains the edge e and is higher than A.*

With the above definitions, we have the following lemmas.

Lemma 8. *An ordered path set (from the highest path to the lowest path) can be constructed for information flow in a bounded plane graph, if the flow amount is no more than the min-cut value of this graph.*

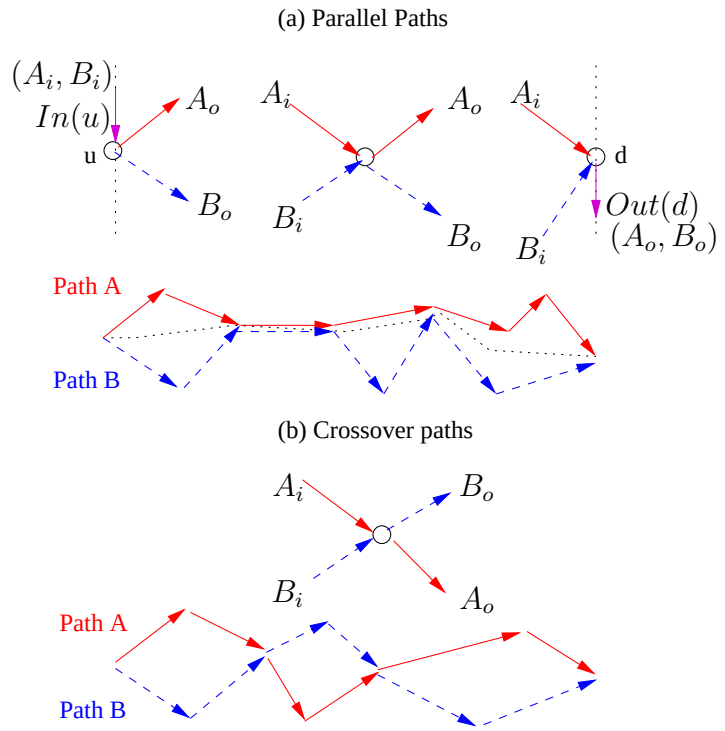


Figure 4.4: Examples for parallel and crossover path

Lemma 9. *Only the paths with successive order can share common edges, i.e., $Path_i$ and $Path_k$ can not share any edge which is not contained in $Path_j$ when $i < j < k$.*

Lemma 8 can be proved by a slight modification of the Ford-Fulkerson algorithm while Lemma 9 can be established by definition. The proofs are illustrated in the appendix (Sections 4.8.2 and 4.8.3).

To complete the coding scheme, we would assign the bit sequence $\{c_1, c_2, \cdots, c_{nR_c+nR_p}\}$ to the ordered path set successively. This achieves the min-cut value according to Lemma 8; as such, Eq. (4.4, 4.5, 4.7) hold. Then by Lemma 9, it can be shown that bits flowing in each edge $(i, o) \in \mathcal{E}$ would be a contiguous segment of the bit sequence, say, $c_j, c_{j+1}, \cdots, c_{j+nr'_{io}-1}$, where $r'_{io} \leq r_{io}$. Finally by Lemma 7, we can ensure that

the equivocation rate with $\min(nR_c, n(R_c+R_p)-nr'_{io}) \geq \min(nR_c, n(R_c+R_p)-nr_{io})$ bits can be obtained for link (i,o), which means Eqs. (4.6, 4.8) are satisfied. This completes the proof of Theorem 13.

4.5 Noisy Case

The following result is for the case where the links in the network are noisy, which generalizes Theorem 13.

Theorem 14. *The rate tuple for a planar graph network,* $(R_c, R_p, R_{e,io})$, $(i,o) \in \mathcal{E}$, *is achievable,* if *there exist auxiliary numbers* r_{io} *and random variables* $U_{io} \to V_{io} \to X_{io} \to Y_{io}Z_{io}$ *such that*

$$\begin{aligned} 0 &\leq r_{io} \leq R_c + R_p, && (4.15)\\ 0 &\leq R_{e,io} \leq R_c, && (4.16)\\ 0 &\leq R_c + R_p \leq \min_{Cut} \sum_{(i,o)\in(IO)^l_{cut}} r_{io}, && (4.17)\\ r_{io} &\leq I(V_{io};Y_{io}|U_{io}) + \min(I(U_{io};Y_{io}), I(U_{io};Z_{io})), && (4.18)\\ R_{e,io} &\leq [I(V_{io};Y_{io}|U_{io}) - I(V_{io};Z_{io}|U_{io})]^+ + R_c + R_p - r_{io}. && (4.19) \end{aligned}$$

From Eq. (4.19), we can see that each individual equivocation rate $R_{e,io}$ is now bounded by the sum of the excess capacity $[I(V_{io};Y_{io}|U_{io}) - I(V_{io};Z_{io}|U_{io})]^+$ of the main channel over the wiretap channel in DMBC (i,o) and the bits $R_c+R_p-r_{io}$ which are not transmitted via the present DMBC. This implies that our presented routing

scheme for noiseless network and random coding over noisy channel contribute to the equivocation rate in an additive manner.

4.5.1 Proof of Theorem 14: noisy case

With noisy links in the network, we propose a decode-and-forward coding scheme to achieve the rate equivocation region stated in Theorem 14. Specifically, we shall apply random coding over the wiretap channel (see [3] or Section 3.4) for each edge, and the intermediate relay nodes are required to decode and then re-encode the transmitted message bits, where the bits assignment over each edge is according to the noiseless routing scheme presented in the previous section.

For each edge, we use random coding for the corresponding bit sequence transmitted over the current link, i.e., r_{io}. Then Eqs. (4.15) and (4.17) are satisfied due to the decode-forward scheme and the noiseless routing scheme, and Eq. (4.18) is established since the random coding scheme is applied to each edge.

It remains to check Eq. (4.19), and the other inequalities in Theorem 14 are straightforward to prove. Before applying random coding, we first convert the assigned bit sequence. For simplicity, assume that an edge (i, o) is required to transmit $S_1' = (b_1 \oplus k, b_2 \oplus k)$. This sequence is then converted to the sequence, $S_1'' = (b_1 \oplus k, b_2 \oplus b_1)$ as they are one-one correspondence. We then apply random coding to the sequence by protecting the $b_1 \oplus b_2$ part, as illustrated in Fig. 4.5.

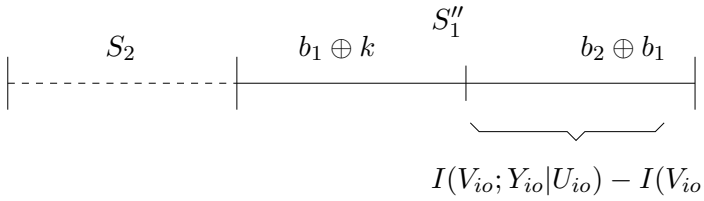


Figure 4.5: A simple example illustrating the decode-and-forward and random coding scheme.

Thus by defining $S_1 = (b_1, b_2)$ and $S = (S_1, S_2)$ we have,

$$\begin{aligned}
H(S|Z_{io}^n) &= H(S_1, S_2|Z_{io}^n) \\
&= H(S_1|Z_{io}^n) + H(S_2|S_1, Z_{io}^n) \\
&\overset{(1)}{=} H(S_1|Z_{io}^n) + H(S_2) \\
&= H(S_1'', S_1|Z_{io}^n) - H(S_1''|S_1 Z_{io}^n) + H(S_2) \\
&= H(S_1''|Z_{io}^n) + H(S_1|S_1'', Z_{io}^n) - H(S_1''|S_1 Z_{io}^n) + H(S_2) \\
&\overset{(2)}{=} H(S_1''|Z_{io}^n) + H(S_1|S_1'') - H(S_1''|S_1 Z_{io}^n) + H(S_2) \\
&\overset{(3)}{=} H(S_1''|Z_{io}^n) - H(S_1''|S_1 Z_{io}^n) + H(S_2, S_1|S_1'') \\
&\overset{(4)}{=} H(S_1''|Z_{io}^n) - H(S_1''|S_1 Z_{io}^n) + n(R_p + R_c - r_{io}) \\
&\overset{(5)}{\geq} H(S_1''|Z_{io}^n) + n(R_p + R_c - r_{io}) - \epsilon_n \\
&\overset{(6)}{\geq} n(I(V_{io}; Y_{io}|U_{io}) - I(V_{io}; Z_{io}|U_{io})) + n(R_p + R_c - r_{io}) - \epsilon_n.
\end{aligned}$$

(1) and (3) hold since S_2 is independent of S_1 and K and thus also independent of S_1'' and Z_{io}^n.

(2) holds since $S_1 \to S_1'' \to Z_{io}^n$ forms a Markov chain.

(4) holds since $H(S_2, S_1|S_1'') = H(S_2, S_1|S_1') = n(R_p + R_c - r_{io})$ by Lemma 7.

(5) holds due to the random coding property (Proposition 10) that $Z_{io}^n S_1$ can determine S_1'' with an arbitrarily small error probability.

(6) holds since $\frac{1}{n}H(S_1''|Z_{io}^n) \geq I(V_{io};Y_{io}|U_{io}) - I(V_{io};Z_{io}|U_{io})$ as proved in the direct part proof in [3].

From the above analysis, we know the random coding and key encryption can contribute to the equivocation in an additive manner. This completes the proof of noisy case.

4.6 Special Case: Parallel Links

When specializing the network to one that is composed of m parallel paths, we can prove that the achievable region described in Theorem 14 is indeed tight. Here the *parallel path network* concept is defined as that the Ford-Fulkerson algorithm can lead to a reduced network in which no two paths share a common edge. A special case of such network is one in which all intermediate nodes (i.e., except for the source and sink nodes) has only one incoming edge and one outgoing edge, as illustrated in Fig. 4.6.

For simplicity, we introduce a different notation for an edge (i, o) in a parallel path network. Given a m parallel path network, we define the link set in the jth parallel path as $I_j = (1_j, 2_j, \cdots, L_j)$, $j \in (1, 2, \cdots, m)$. Thus a valid cut for this network is $Cut : (i_j), j = 1, 2, \cdots, m$ with $i_j \in I_j$.

Theorem 15. *The rate tuple for a m parallel path network, (R_c, R_p, R_{e,i_j}), $i_j \in I_j$*

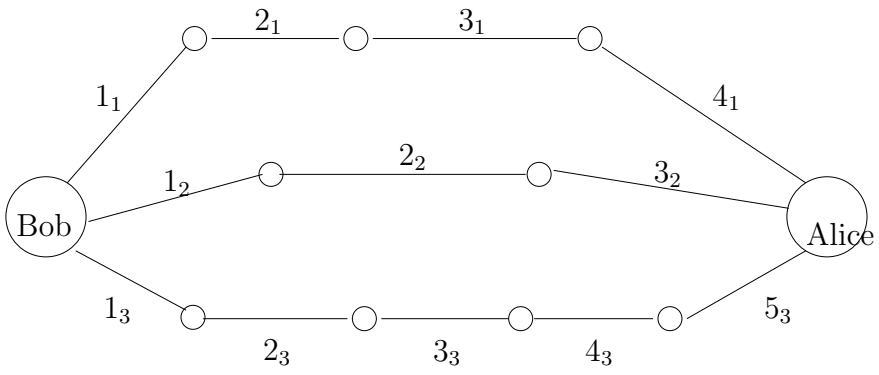


Figure 4.6: An example of $m = 3$ parallel path network, where i_j means the ith link of the jth path.

with $j \in (1, 2, \cdots, m)$*, is achievable,* iff *there exist auxiliary numbers* r_{i_j} *and random variables* $U_{i_j} \to V_{i_j} \to X_{i_j} \to Y_{i_j} Z_{i_j}$ *such that*

$$\begin{aligned}
0 &\leq r_{i_j} \leq R_c + R_p, \\
0 &\leq R_{e,i_j} \leq R_c, \\
0 &\leq R_c + R_p \leq \min_{Cut} \sum_{j=1}^{m} r_{i_j}, \\
r_{i_j} &\leq I(V_{i_j}; Y_{i_j}|U_{i_j}) + \min(I(U_{i_j}; Y_{i_j}), I(U_{i_j}; Z_{i_j})), \\
R_{e,i_j} &\leq [I(V_{i_j}; Y_{i_j}|U_{i_j}) - I(V_{i_j}; Z_{i_j}|U_{i_j})]^+ + R_c + R_p - r_{i_j},
\end{aligned}$$

Proof. The direct part is proved by specializing Theorem 14 to the parallel path network. The converse proof is in the appendix (Section 4.8.4). □

4.6.1 The m parallel channel model

In this subsection, we further specialize the m parallel path network to m parallel channel model, which is illustrated in Fig. 4.7. The difference with an m parallel

path network is that we now assume each path consists of a single hop channel between the source and the sink with no intermediate nodes. Studying this m parallel

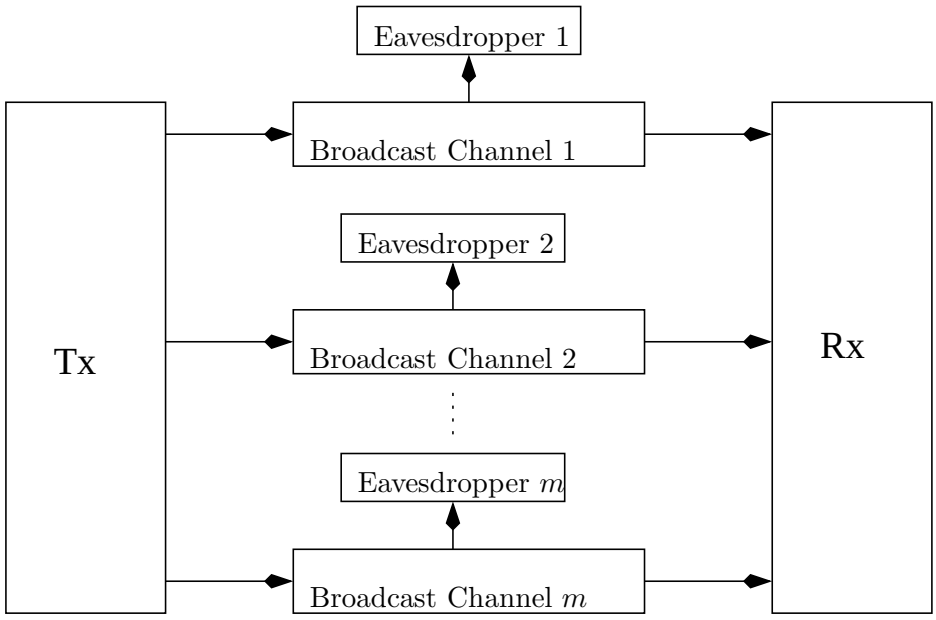


Figure 4.7: The m parallel channel model.

channel model is of great interest as it accurately models many existing systems. One example is in a wideband system, e.g., a multi-band multi-carrier system whereas the eavesdropper is limited to a narrowband receiver. Thus the rate equivocation region of the parallel channel model can shed light on any advantages that such systems may offer and what is its potentially optimal coding scheme.

Denote by $\mathcal{R}_m$ as the rate equivocation region of the m channel system. Specializing Theorem 15 to the m parallel channel model, we have the following theorem.

Theorem 16. $(R_c, R_p, R_{e1}, \cdots, R_{em}) \in \mathcal{R}_m$ iff *for* $j \in (1, 2, \cdots, m)$ *there exist aux-*

iliary numbers r_j and random variables $U_j \to V_j \to X_j \to Y_jZ_j$ such that the conditional distribution of Y_j (respectively Z_j) given X_j is determined by corresponding channel and

$$\begin{aligned} 0 &\leq R_c + R_p \leq \sum_{j=1}^{m} r_j, && (4.20)\\ 0 &\leq R_{ej} \leq R_c, && (4.21)\\ 0 &\leq r_j \leq R_c + R_p, && (4.22)\\ r_j &\leq I(V_j;Y_j|U_j) + \min(I(U_j;Y_j), I(U_j;Z_j)), && (4.23)\\ R_{ej} &\leq [I(V_j;Y_j|U_j) - I(V_j;Z_j|U_j)]^+ + R_c + R_p - r_j. && (4.24) \end{aligned}$$

4.6.2 Noiseless channels

By assuming noiseless channels in Theorem 16, we can obtain the rate equivocation region for a system with multiple parallel noiseless channels, each with capacity C_j, $j = 1, \cdots, m$.

Proposition 19. *For a noiseless m parallel channel model, $\mathcal{R}_m$ is a closed convex set consisting of rate tuples (R_c, R_p, R_{ej}), $j = 1, \cdots, m$, satisfying*

$$\begin{aligned} 0 &\leq R_c + R_p \leq \sum_{j=1}^{m} r_j, && (4.25)\\ 0 &\leq R_{ej} \leq R_c, && (4.26)\\ 0 &\leq r_j \leq R_c + R_p, && (4.27)\\ r_j &\leq C_j, && (4.28)\\ R_{ej} &\leq R_c + R_p - r_j. && (4.29) \end{aligned}$$

For perfect secrecy system, i.e., by setting $R_{ej} = R_c$ for $j = 1, \cdots, m$, we have the following result.

Proposition 20. *A rate pair (R_c, R_p) can attain perfect secrecy if and only if*

$$0 \leq R_c + R_p \leq \sum_{j=1}^{m} \min(C_j, R_p).$$

Consider now the problem of maximizing R_c, i.e., one want to maximize

$$R_c = \sum_{j=1}^{m} \min(C_j, R_p) - R_p$$

over all non-negative R_p. It is easy to show that R_c would be a piecewise linear and concave function of R_p. This is illustrated in Fig. 4.8.

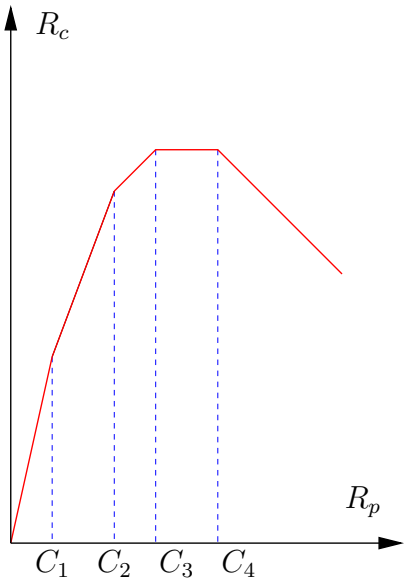


Figure 4.8: R_c vs R_p figure with four parallel channels, whose capacities are $0 \leq C_1 \leq C_2 \leq C_3 \leq C_4$. The maximum perfectly secure throughput is $\max R_c = C_1 + C_2 + C_3$.

As a result, for the m channel case, the maximum perfectly secure throughput

can be attained using the following simple scheme. Set $R_p = \max_j\{C_j\}$, i.e., choose the link with the largest capacity to transfer the public message. All other $m-1$ links implement the one-time pad scheme where the secret key comes from the public message, achieving a total secure throughput of

$$\max R_c = \sum_{i=1}^{m} C_i - \max_j\{C_j\} \tag{4.30}$$

Perfect secrecy comes from the condition that $R_p = \max_j\{C_j\} \geq C_j$ for $j = 1, \cdots, m$. As with the two channel case, R_p serves precisely the role of the secret key for the $m-1$ channels that implement the one-time pad scheme. More interestingly, this simple and intuitive scheme is actually shown to be optimal, according to Theorem 16.

4.6.3 Gaussian channel

The result can also be extended to the case of parallel Gaussian broadcast channels. Such model describes, for example, a multiband frequency hopped orthogonal frequency-division multiplexing (OFDM) system where a eavesdropper with a narrowband receiver can not simultaneously monitor the entire frequency band. The signal model for the jth sub-channel is,

$$\begin{aligned} Y_j^n &= X_j^n + G_{Yj}^n, \\ Z_j^n &= X_j^n + G_{Zj}^n, \end{aligned}$$

where the noise vectors G_{Yj}^n, G_{Zj}^n are independently and identically distributed with $G_{Yji} \sim \mathcal{N}(0, N_{1j})$ and $G_{Zji} \sim \mathcal{N}(0, N_{2j})$ respectively, with $i = 1, \cdots, n$. We assume,

for now, individual power constraint for each sub-channel:

$$\frac{1}{n}\sum_{i=1}^{n}\mathrm{E}(X_{ji}) \leq P_j.$$

Define $C(\cdot)$ as

$$C\left(x\right) = \frac{1}{2}\log\left(1+x\right),$$

the rate equivocation region is given in the following proposition.

Proposition 21. *For a Gaussian m sub-channel system, $\mathcal{R}_m$ is a closed convex set consisting of those rate groups (R_c, R_p, R_{ej}) satisfying,*

$$\begin{aligned}
0 &\leq R_c + R_p \leq \sum_{j=1}^{m} r_j, && (4.31)\\
0 &\leq R_{ej} \leq R_c, && (4.32)\\
0 &\leq r_j \leq R_c + R_p, && (4.33)\\
r_j &\leq C\left(\frac{P_j}{N_{1j}}\right), && (4.34)\\
R_{ej} &\leq \left[C\left(\frac{P_j}{N_{1j}}\right) - C\left(\frac{P_j}{N_{2j}}\right)\right]^{+} + R_c + R_p - r_j. && (4.35)
\end{aligned}$$

Consider now the total power constraint case, i.e.,

$$\sum_{j=1}^{m}\frac{1}{n}\sum_{i=1}^{n}\mathrm{E}(X_{ji}) \leq P. \tag{4.36}$$

The interesting problem is to study the optimal power allocation strategy to achieve the maximum perfectly secure throughput R_c subject to the total power constraint (Eq. (4.36)). We now prove that this is a convex optimization problem.

Proposition 22. *For a Gaussian m sub-channel system with a total power constraint, finding the optimal power allocation that achieves maximum perfectly secure throughput can be reduced to the following convex optimization problem,*

$$\begin{aligned} \max_{\boldsymbol{P}} \quad & \left(\sum_{j=1}^{m} C\left(\frac{P_j}{N_{1j}}\right) - \max_j C\left(\frac{P_j}{N'_{2j}}\right)\right) \\ \textit{subject to} \quad & \sum_{j=1}^{m} P_j \le P \end{aligned} \tag{4.37}$$

where

$$N'_{2j} \triangleq \max(N_{1j}, N_{2j}), \quad \boldsymbol{P} \triangleq (P_1, \cdots, P_m).$$

Proof. Set $R_{ej} = R_c$ in Proposition 21, the maximal R_c can be expressed as

$$\begin{aligned} \max_{R_p,\mathbf{P}} R_c &= \max_{R_p,\mathbf{P}} \sum_{j=1}^{m} \left(\min\left(C\left(\frac{P_j}{N_{1j}}\right), \left[C\left(\frac{P_j}{N_{1j}}\right) - C\left(\frac{P_j}{N_{2j}}\right)\right]^+ + R_p\right)\right) - R_p \\ &= \max_{R_p,\mathbf{P}} \sum_{j=1}^{m} \left(\min\left(C\left(\frac{P_j}{N_{1j}}\right), C\left(\frac{P_j}{N_{1j}}\right) - C\left(\frac{P_j}{N'_{2j}}\right) + R_p\right)\right) - R_p \\ &= \max_{\mathbf{P}} \max_{R_p} \left(\sum_{j=1}^{m} \left(\min\left(C\left(\frac{P_j}{N_{1j}}\right), C\left(\frac{P_j}{N_{1j}}\right) - C\left(\frac{P_j}{N'_{2j}}\right) + R_p\right)\right) - R_p\right) \\ &= \max_{\mathbf{P}} \max_{R_p} \left(\sum_{j=1}^{m} \left(C\left(\frac{P_j}{N_{1j}}\right) - C\left(\frac{P_j}{N'_{2j}}\right)\right) + \sum_{j=1}^{m} \min\left(C\left(\frac{P_j}{N'_{2j}}\right), R_p\right) - R_p\right) \\ &\overset{(1)}{=} \max_{\mathbf{P}} \left(\sum_{j=1}^{m} \left(C\left(\frac{P_j}{N_{1j}}\right) - C\left(\frac{P_j}{N'_{2j}}\right)\right) + \sum_{j=1}^{m} C\left(\frac{P_j}{N'_{2j}}\right) - \max_j C\left(\frac{P_j}{N'_{2j}}\right)\right) \\ &= \max_{\mathbf{P}} \left(\sum_{j=1}^{m} C\left(\frac{P_j}{N_{1j}}\right) - \max_j C\left(\frac{P_j}{N'_{2j}}\right)\right), \end{aligned}$$

where (1) follows from the result for the noiseless case (c.f. Eq. (4.30)), i.e., for the maximization problem

$$\max_{R_p} \left(\sum_{j=1}^{m} \min\left(C\left(\frac{P_j}{N'_{2j}}\right), R_p\right) - R_p\right),$$

the optimal solution corresponds to

$$R_p = \max_j C_j = \max_j C\left(\frac{P_j}{N'_{2j}}\right)$$

and the obtained maximum is

$$\sum_{j=1}^{m} C\left(\frac{P_j}{N'_{2j}}\right) - \max_j C\left(\frac{P_j}{N'_{2j}}\right).$$

Thus it remains to maximize the following objective function,

$$\sum_{j=1}^{m} C\left(\frac{P_j}{N_{1j}}\right) - \max_j C\left(\frac{P_j}{N'_{2j}}\right).$$

To prove the concavity of this objective function,

$$\begin{aligned}
& \sum_{j=1}^{m} C\left(\frac{P_j}{N_{1j}}\right) - \max_j C\left(\frac{P_j}{N'_{2j}}\right) \\
= & \sum_{j=1}^{m}\left(C\left(\frac{P_j}{N_{1j}}\right) - C\left(\frac{P_j}{N'_{2j}}\right)\right) + \sum_{j=1}^{m} C\left(\frac{P_j}{N'_{2j}}\right) - \max_j C\left(\frac{P_j}{N'_{2j}}\right) \\
= & \sum_{j=1}^{m}\left(C\left(\frac{P_j}{N_{1j}}\right) - C\left(\frac{P_j}{N'_{2j}}\right)\right) + \min\left\{\sum_{i=1}^{m-1} C\left(\frac{P_{j_i}}{N'_{2j_i}}\right)\middle| 1 \le j_1 \le j_2, \cdots, j_{m-1} \le m\right\}
\end{aligned}$$

where,

- $C\left(\frac{P_j}{N_{1j}}\right) - C\left(\frac{P_j}{N'_{2j}}\right)$ is concave by directly computing the second order derivative.

  Thus

  $$\sum_{j=1}^{m}\left(C\left(\frac{P_j}{N_{1j}}\right) - C\left(\frac{P_j}{N'_{2j}}\right)\right)$$

  is also concave.

- $\sum_{i=1}^{m-1} C\left(\frac{P_{j_i}}{N'_{2j_i}}\right)$ is a concave function of $\mathbf{P}$, and due to the fact that pointwise minimum preserves the concavity [57, Chapter 3], we know

  $$\min\left\{\sum_{i=1}^{m-1} C\left(\frac{P_{j_i}}{N'_{2j_i}}\right)\middle| 1 \le j_1 \le j_2, \cdots, j_{m-1} \le m\right\}$$

is also concave.

Since the above objective function is concave in the power constraint vector $\mathbf{P}$ and the parameter $\mathbf{P}$ is also defined on the convex set specified by Eq. (4.36), the optimization problem is thus a convex optimization problem. □

Therefore, the standard optimization algorithms [57] can be applied to efficiently find the global optimum of the power allocation strategy.

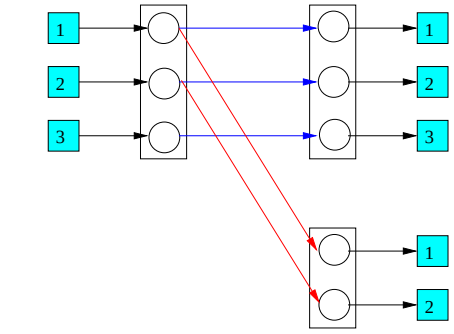
4.6.4 Illustration using the deterministic model

In this subsection, we use deterministic models to illustrate the above results for the BCCP model, the key enhanced BCCP model, and the m sub-channel model under the Gaussian channel assumption. This illustration is largely inspired by recent work reported in [58–60] and are used to give intuitive explanation on how the rate equivocation region can be attained.

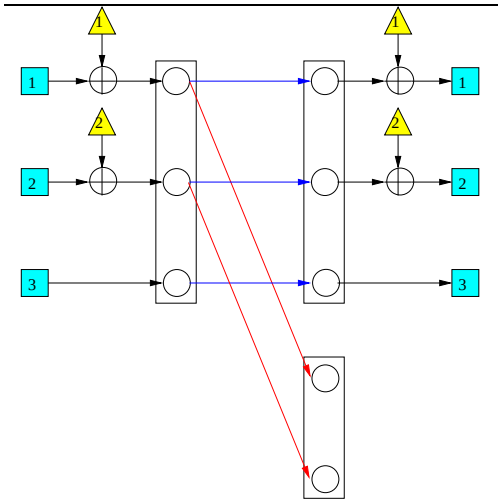
Using the approximation of capacity by channel gain under high SNR regime [59], we have the approximated capacities for the Gaussian channels,

$$C_i \approx n_i \leftrightarrow \lceil \log SNR_i \rceil, \quad i = 1, 2.$$

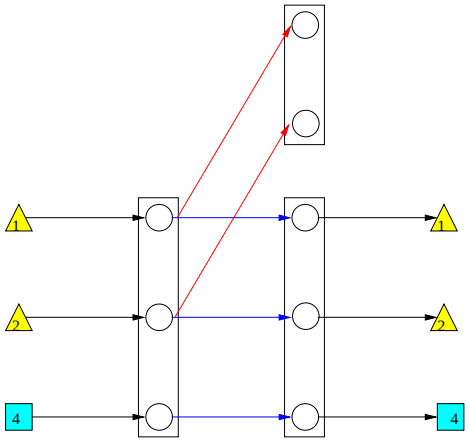
The deterministic model for a Gaussian wiretap channel (GWC) is illustrated in Fig. 4.9(a), where the main channel capacity is $n_1 = 3$ and the wiretap channel capacity is $n_2 = 2$. Now that three bits of the confidential message (Square #1-3) are to be transmitted via this broadcast channel, Fig. 4.9(a) shows that the two most

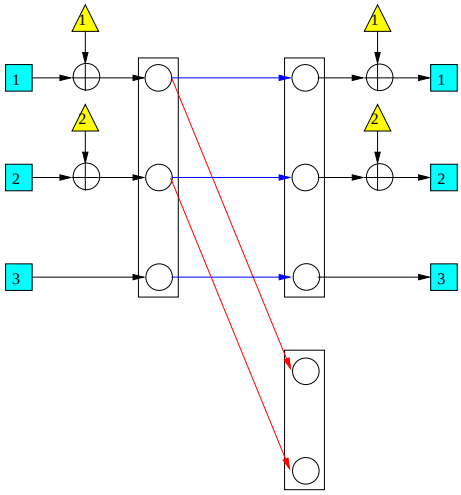


(a) GWC



(b) key enhanced GWC





(c) Gaussian m sub-channel system

Figure 4.9: Pictorial representation of the deterministic model for GWC, key enhanced GWC, and Gaussian m sub-channel system.

significant bits (MSB) (Square #1-2) can be decoded by the wiretap channel, while the one least significant bit (LSB) (Square #3) can not be seen since it falls below the noise level at the wiretapper. Thus, one bit information is totally protected from the wiretapper. The achieved secrecy capacity is $n_1 - n_2 = 1$, which coincides with the theoretical result of the Gaussian wiretap channel [9], i.e., the secrecy capacity is the difference between the capacities of the main channel and the wiretap channel.

Fig. 4.9(b) represents the secret key enhanced Gaussian wiretap channel. Assume a 2 bit secret key (Triangle #1-2) is known to the transmitter and the legitimate receiver, but unknown to the wiretapper. If, for each transmission, we pre-process the 2 MSB (Square #1-2) by a modulo 2 sum operation with the 2 bit secret key, then these 3 bits are all unknown for the wiretap. Thus, a total of 3 bits are kept secret against the wiretapper. The secrecy capacity is $n_1 - n_2 + R_p = 3$, thus the effect of the secret key on the equivocation rate is in an additive manner.

Fig. 4.9(c) illustrates a two parallel sub-channel system. Suppose two identical GWCs are available, with $n_1 = 3$ and $n_2 = 2$. Only two secret bits per channel use can be obtained, one from each sub-channel, if we communicate independently over these two parallel channels. However, if there are in addition two bit public message (Triangle #1-2), then a total of two bits can be completely protected against any of the the two wiretapper (but not both). To illustrate how to attain this four bit secrecy rate, from Fig. 4.9(c), one bit confidential message (Square #4) and two bit public message (Triangle #1-2) are transmitted via channel 1. The wiretapper of

channel 1 does not know any information about the confidential message since the 1 bit confidential message is the LSB and falls below the noise level for the wiretapper. For channel 2, all three bits are communicated as the confidential message: the LSB is protected due to channel noise while the two MSB (Square #1-2) are encrypted using the two bits of public message. Thus the two bit public message, transmitted via channel 1, serves as a secret key for channel 2. In summary, a total of six bit throughput is achieved during each transmission, of which two bits correspond to a public message and four bits correspond to a confidential message that is completely protected from each individual wiretapper.

4.7 Summary

In this chapter, we studied secure communication over a single-source single-sink acyclic planar network with possibly noiseless or noisy links. An achievable rate equivocation region was derived which admits a constructive proof approach. The result is consistent with that of secure network coding in [13]. On the other hand, our achievability proof provides a secure communication scheme that is both intuitive and easy to implement. The achievable rate equivocation region also reduces to known result for various special cases. In particular, when the communication network reduces to non-overlapping parallel links, the proposed encoding scheme is optimal. The specific coding scheme to achieve the maximal perfectly secure throughput was also discussed for both noiseless and Gaussian m sub-channel systems.

4.8 Appendix

4.8.1 Proof of Lemma 7

For simplicity, we only consider a sequence

$$\{k_{j+1}, k_{j+2}, \cdots, k_{nR_p}, b_1 \oplus k_1, b_2 \oplus k_2, \cdots, b_{nR_p} \oplus k_{nR_p},$$
$$b_{nR_p+1} \oplus k_1, b_{nR_p+2} \oplus k_2, \cdots, b_{nR_p+i} \oplus k_i\},$$

which is a quite general segment sequence. The derivation of its conditional entropy is shown as in Eq. (4.38). Following the similar light, we can prove Lemma 7 is true for any other possible segments.

$$\begin{aligned}
& H(b_1, \cdots, b_{nR_c} | k_{j+1}, \cdots, k_{nR_p}, b_1 \oplus k_1, \cdots, b_{nR_p} \oplus k_{nR_p}, \\
& b_{nR_p+1} \oplus k_1, \cdots, b_{nR_p+i} \oplus k_i) \\
= \; & H(b_{nR_p+i+1}, \cdots, b_{nR_c} | k_{j+1}, \cdots, k_{nR_p}, b_1 \oplus k_1, \cdots, b_{nR_p} \oplus k_{nR_p}, \\
& b_{nR_p+1} \oplus k_1, \cdots, b_{nR_p+i} \oplus k_i) \\
& + H(b_1, \cdots, b_{nR_p+i} | b_{nR_p+i+1}, \cdots, b_{nR_c}, k_{j+1}, \cdots, j_{nR_p}, b_1 \oplus k_1, \cdots, b_{nR_p} \oplus k_{nR_p}, \\
& b_{nR_p+1} \oplus k_1, \cdots, b_{nR_p+i} \oplus k_i) \\
= \; & nR_c - nR_p - i + H(b_1, \cdots, b_{nR_p+i} | k_{j+1}, \cdots, k_{nR_p}, b_1 \oplus k_1, \cdots, b_{nR_p} \oplus k_{nR_p}, \\
& b_{nR_p+1} \oplus k_1, \cdots, b_{nR_p+i} \oplus k_i) \\
= \; & nR_c - nR_p - i + H(b_1, \cdots, b_j | k_{j+1}, \cdots, k_{nR_p}, b_1 \oplus k_1, \cdots, b_{nR_p} \oplus k_{nR_p}, \\
& b_{nR_p+1} \oplus k_1, \cdots, b_{nR_p+i} \oplus k_i) \\
& + H(b_{j+1}, \cdots, b_{nR_p+i} | b_1, \cdots, b_j, k_{j+1}, \cdots, k_{nR_p}, b_1 \oplus k_1, \cdots, b_{nR_p} \oplus k_{nR_p},
\end{aligned}$$

$$
\begin{aligned}
& b_{nR_p+1} \oplus k_1, \cdots, b_{nR_p+i} \oplus k_i) \\
= \; & nR_c - nR_p - i + H(b_1, \cdots, b_j | k_{j+1}, \cdots, k_{nR_p}, b_1 \oplus k_1, \cdots, b_{nR_p} \oplus k_{nR_p}, \\
& b_{nR_p+1} \oplus k_1, \cdots, b_{nR_p+i} \oplus k_i) \\
= \; & nR_c - nR_p - i + j = n(R_c + R_p) - r. \qquad (4.38)
\end{aligned}
$$

4.8.2 Proof of Lemma 8

To prove Lemma 8, an iterative algorithm is applied to construct the ordered path set. Its main idea is to carefully bookkeep the flows assigned to the *ordered* paths from the source node to the sink node. This is in essence a modified version of the Ford-Fulkerson algorithm for finding network capacity.

We assume that the flows' amounts assigned to the edges are already determined to achieve the network capacity, i.e., we only need to consider the reduced network as a result of applying the Ford-Fulkerson algorithm to the original network. We then apply the following iterative algorithm to this reduced network.

1. Set $i = 1$.

2. Find the highest path from the source node to the sink node, which is higher than all other edges in the network. If there is no such path left, exit. The steps for finding the highest path are,

   (a) Initializing, set the virtual edge $In(u)$ as e_i, and the source node u as r.

(b) Let e_i be the start edge, find the closest output edge e_o from the edge set $Out(r)$ according to the clockwise order at node r. Store e_i, e_o and r.

(c) If the edge $e_o = Out(d)$, exit; otherwise, set $e_i = e_o$, $r = Endnode(e_o)$ and go to step (b).

3. Determine f_i, the maximum flow along this path, which will be equal to the smallest flow amount on any edge in the path (the bottleneck edge).

4. Store this path as $Path_i$ with flow amount f_i. Subtract f_i from the remaining flow amount for each edge in the path. Delete the edges with 0 flow amount.

5. Set $i = i + 1$. Go to step 2.

The above algorithm is to re-organize the reduced network into an ordered path set, thus it completes the proof of Lemma 8. We point out that there is no need of flow increasing on backward direction as in the original Ford-Fulkerson algorithm, as we are already dealing with the reduced network.

4.8.3 Proof of Lemma 9

We prove Lemma 9 by contradiction. Assume that Lemma 9 is wrong and $Path_i, Path_k$ can share one edge e which is not contained in $Path_j$ with $i < j < k$. Then e is higher than $Path_j$ since $Path_i$ containing edge e is higher than $Path_j$. On the other hand, e is lower than $Path_j$ as $Path_k$ is lower than $Path_j$. Thus e is contained in $Path_j$, which contradict the assumption.

4.8.4 Converse proof of Theorem 15

In this subsection we prove the converse part of Theorem 15. We shall show that, for any admissible rate quadruple (R_c, R_p, R_{e,i_j}), $i_j \in I_j$ for any $j \in (1, 2, \cdots, m)$, there exist auxiliary numbers r_{i_j} and auxiliary random variables $U_{i_j} \to V_{i_j} \to X_{i_j} \to Y_{i_j} Z_{i_j}$, $j = 1, 2, \cdots, m$, such that

$$\begin{aligned} R_{e,i_j} &\leq [I(V_{i_j}; Y_{i_j}|U_{i_j}) - I(V_{i_j}; Z_{i_j}|U_{i_j})]^+ + R_c + R_p - r_{i_j} + \epsilon & (4.39) \\ r_{i_j} &\leq I(V_{i_j}; Y_{i_j}|U_{i_j}) + \min(I(U_{i_j}; Y_{i_j}), I(U_{i_j}; Z_{i_j})) + \epsilon & (4.40) \\ R_c + R_p &\leq \sum_{j=1}^{m} r_{i_j} + \epsilon & (4.41) \\ r_{i_j} &\leq R_c + R_p + \epsilon & (4.42) \\ R_{e,i_j} &\leq R_c + \epsilon. & (4.43) \end{aligned}$$

By Fano's Lemma, we have

$$\frac{1}{n} H(ST|Y_{L_1}^n, Y_{L_2}^n, \cdots, Y_{L_m}^n) \leq \epsilon.$$

By the geometry of parallel path network and the standard functional dependence graphs argument [61], we know for $i_j \leq L_j$ with $j \in (1, 2, \cdots, m)$,

$$ST \to Y_{i_1}^n, Y_{i_2}^n, \cdots, Y_{i_m}^n \to Y_{L_1}^n, Y_{L_2}^n, \cdots, Y_{L_m}^n$$

forms a Markov chain, thus

$$\frac{1}{n} H(ST|Y_{i_1}^n, Y_{i_2}^n, \cdots, Y_{i_m}^n) \leq \frac{1}{n} H(ST|Y_{L_1}^n, Y_{L_2}^n, \cdots, Y_{L_m}^n) \leq \epsilon.$$

Furthermore, due to the parallel path network property, for the different paths, $j \neq$

k, $Y_{i_j}Z_{i_j} \rightarrow ST \rightarrow Y_{i_k}Z_{i_k}$ is also shown to be a Markov chain by the functional dependence graphs argument.[2]

Now define r_{i_j}, $i_j \in I_j$ for any $j \in (1, 2, \cdots, m)$, as

$$nr_{i_j} \triangleq I(ST; Y_{i_j})$$

.

Hence,

$$\begin{aligned} r_{i_j} &= \frac{1}{n} I(ST; Y_{i_j}) \leq \frac{1}{n} H(ST) \leq R_c + R_p + \epsilon, \\ R_{e,i_j} &\leq \frac{1}{n} H(S|Z_{i_j}^n) \leq \frac{1}{n} H(S) \leq R_c + \epsilon. \end{aligned}$$

Thus the last two inequalities of Eqs. (4.42)-(4.43) are established.

Since for the different paths, $j \neq k$, $Y_{i_j}Z_{i_j} \rightarrow ST \rightarrow Y_{i_k}Z_{i_k}$ forms a Markov chain, we then have

$$\begin{aligned} I(ST; Y_{i_1}) &= I(ST, Y_{i_2}, Y_{i_3}, \cdots, Y_{i_m}; Y_{i_1}) \\ &= I(ST; Y_{i_1}|Y_{i_2}, Y_{i_3}, \cdots, Y_{i_m}) + I(Y_{i_1}; Y_{i_2}, Y_{i_3}, \cdots, Y_{i_m}) \\ &\geq I(ST; Y_{i_1}|Y_{i_2}, Y_{i_3}, \cdots, Y_{i_m}) \\ &= H(ST) - H(ST|Y_{i_1}, Y_{i_2}, Y_{i_3}, \cdots, Y_{i_m}) - I(ST; Y_{i_2}, Y_{i_3}, \cdots, Y_{i_m}). \end{aligned}$$

Thus by induction, Eq. (4.41) holds, as

$$n \sum_{j=1}^{m} r_{i_j} = \sum_{j=1}^{m} I(ST; Y_{i_j})$$

[2]We comment here that for a general networks, such Markov chain is not established, which is the main reason we can not have a converse proof for Theorem 14.

$$\geq H(ST) - H(ST|Y_{i_1}, Y_{i_2}, \cdots, Y_{i_m})$$

$$\geq n(R_c + R_p) - n\epsilon.$$

Furthermore, the following inequalities can be obtained:

$$\begin{aligned} H(S|Z_{l_j}^n) &\leq H(ST|Z_{l_j}^n) = H(ST) - I(ST; Z_{l_j}^n) \\ &= I(ST; Y_{l_j}^n) - I(ST; Z_{l_j}^n) + H(ST|Y_{l_j}^n) \\ &= I(ST; Y_{l_j}^n) - I(ST; Z_{l_j}^n) + H(ST) - I(ST; Y_{l_j}^n) \\ &= I(ST; Y_{l_j}^n) - I(ST; Z_{l_j}^n) + n(R_c + R_p) - nr_{l_j}; \qquad (4.44) \\ I(ST; Y_{l_j}^n) &= \sum_{i=1}^{n} I(ST; Y_{l_j i}|Y_{l_j}^{i-1}\tilde{Z}_{l_j}^{i+1}) + \sum_{i=1}^{n} I(\tilde{Z}_{l_j}^{i+1}; Y_{l_j i}|Y_{l_j}^{i-1}) \\ &\quad - \sum_{i=1}^{n} I(\tilde{Z}_{l_j}^{i+1}; Y_{l_j i}|Y_{l_j}^{i-1}TS). \qquad (4.45) \end{aligned}$$

The following steps are similar to the converse proof in Section 2.6.1. Define $Y_{l_j}^i = (Y_{l_j 1}, \cdots, Y_{l_j i})$, $\tilde{Z_{l_j}}^i = (Z_{l_j i}, \cdots, Z_{l_j n})$, we have

$$\begin{aligned} I(ST; Y_{l_j}^n) &= \sum_{i=1}^{n} I(ST; Y_{l_j i}|Y_{l_j}^{i-1}\tilde{Z}_{l_j}^{i+1}) + \Sigma_{l_j} - \Sigma_{2,l_j}, \qquad (4.46) \\ I(ST; Z_{l_j}^n) &= \sum_{i=1}^{n} I(ST; Z_{l_j i}|Y_{l_j}^{i-1}\tilde{Z}_{l_j}^{i+1}) + \Sigma_{l_j}^* - \Sigma_{2,l_j}^*, \qquad (4.47) \end{aligned}$$

where,

$$\begin{aligned} \Sigma_{l_j} &= \sum_{i=1}^{n} I(\tilde{Z}_{l_j}^{i+1}; Y_{l_j i}|Y_{l_j}^{i-1}), \\ \Sigma_{l_j}^* &= \sum_{i=1}^{n} I(Y_{l_j}^{i-1}; Z_{l_j i}|\tilde{Z}_{l_j}^{i+1}), \\ \Sigma_{2,l_j} &= \sum_{i=1}^{n} I(\tilde{Z}_{l_j}^{i+1}; Y_{l_j i}|Y_{l_j}^{i-1}TS), \end{aligned}$$

$$\Sigma^*_{2,l_j} = \sum_{i=1}^{n} I(Y_{l_j}^{i-1}; Z_{l_j i}|\tilde{Z}_{l_j}^{i+1}TS).$$

From [3, Lemma 7], we know

$$\Sigma_{l_j} = \Sigma^*_{l_j},$$

$$\Sigma_{2,l_j} = \Sigma^*_{2,l_j}.$$

Thus

$$I(ST; Y_{l_j}^n) = \sum_{i=1}^{n} I(ST; Y_{l_j i}|Y_{l_j}^{i-1}\tilde{Z}_{l_j}^{i+1}) + \Sigma_{l_j} - \Sigma_{2,l_j} \quad (4.48)$$

$$= \sum_{i=1}^{n} I(ST; Y_{l_j i}|Y_{l_j}^{i-1}\tilde{Z}_{l_j}^{i+1}) + \Sigma^*_{l_j} - \Sigma_{2,l_j}, \quad (4.49)$$

$$\Sigma_{l_j} = \sum_{i=1}^{n} I(\tilde{Z}_{l_j}^{i+1}; Y_{l_j i}|Y_{l_j}^{i-1}) \le \sum_{i=1}^{n} I(\tilde{Z}_{l_j}^{i+1}Y_{l_j}^{i-1}; Y_{l_j i}), \quad (4.50)$$

$$\Sigma^*_{l_j} = \sum_{i=1}^{n} I(Y_{l_j}^{i-1}; Z_{l_j i}|\tilde{Z}_{l_j}^{i+1}) \le \sum_{i=1}^{n} I(\tilde{Z}_{l_j}^{i+1}Y_{l_j}^{i-1}; Z_{l_j i}). \quad (4.51)$$

Let us introduce a random variable J, independent of $(S, T, X_{l_j}^n, Y_{l_j}^n, Z_{l_j}^n)$ and uniformly distributed over $\{1, \cdots, n\}$. By setting

$$U_{l_j} \triangleq Y_{l_j}^{J-1}\tilde{Z}_{l_j}^{J+1}J, \quad V_{l_j} \triangleq U_{l_j}ST, \quad X_{l_j} \triangleq X_{l_j J},$$

$$Y_{l_j} \triangleq Y_{l_j J}, \qquad Z_{l_j} \triangleq Z_{l_j J},$$

we get Eqs. (4.52) and (4.53) by combining Eqs. (4.46)-(4.51),

$$\frac{1}{n}\left(I(ST; Y_{l_j}^n) - I(ST; Z_{l_j}^n)\right) = I(V_{l_j}; Y_{l_j}|U_{l_j}) - I(V_{l_j}; Z_{l_j}|U_{l_j}), \quad (4.52)$$

$$\frac{1}{n}I(ST; Y_{l_j}) \le I(V_{l_j}; Y_{l_j}|U_{l_j}) + \min(I(U_{l_j}; Y_{l_j}), I(U_{l_j}; Z_{l_j})) \quad (4.53)$$

Substituting Eqs. (4.52) and (4.53) into Eqs. (4.44) and (4.45), we have

$$\frac{1}{n}H(S|Z_{l_j}^n) \le I(V_{l_j}; Y_{l_j}|U_{l_j}) - I(V_{l_j}; Z_{l_j}|U_{l_j}) + R_c + R_p - r_{l_j},$$

$$\frac{1}{n}I(ST;Y^n) \leq I(V_{l_j};Y_{l_j}|U_{l_j}) + \min(I(U_{l_j};Y_{l_j}), I(U_{l_j};Z_{l_j})).$$

Thus Eqs. (4.39)-(4.40) hold for any l_j. This completes the converse proof of Theorem 15.

Chapter 5

Conclusions and Future Work

5.1 Conclusions

This thesis studied secure communication from an information theoretic perspective. First, we considered capacity bounds for discrete memoryless broadcast channels with two confidential messages. Several capacity outer bounds were proposed which, together with a previously proposed inner bound, help establish the rate equivocation region of several classes of broadcast channels. In addition, by removing the confidentiality constraint, the proposed outer bounds reduce to new capacity outer bounds for the classical discrete memoryless broadcast channel. Then, we studied the broadcast channel with confidential and public messages (BCCP) model. Its more liberal treatment of the non-confidential message - the requirement that the unintended receiver reliably decode the non-confidential message is dropped - results in an enlarged rate equivocation region. This BCCP framework was also extended to systems where a

secret key is available to the intended transceiver pair. Applying this key enhanced BCCP model, we further studied the problem of secure communication over a network in which each link is subject to non-cooperating eavesdropping. A single-source single-sink acyclic planar network was considered, and the achievable rate equivocation region was established through an algorithmic approach. It combines Shannon's key encryption, Wyner's random coding and the Ford-Fulkerson algorithm, and is readily applicable to real communication networks.

5.2 Future Work

The proposed coding scheme over networks deals with a particular, yet widely popular class of networks and is very promising to find applications in many practical systems. It also lays out a foundation for further exploration to account for more sophisticated threats and complex networks. We discuss two such extensions below: (1) extending to active adversaries, (2) extending to networks with interference at nodes.

5.2.1 Active Adversary

We first consider an extension to active threat, i.e., the adversary not only can intercept information communicated over a link or a node, but may be able to alter the information. The model is illustrated in Fig. 5.1.

An intuitive approach is to treat the signal alteration as a type of channel error occurring in communication systems. As such, it is reasonable to consider the use of

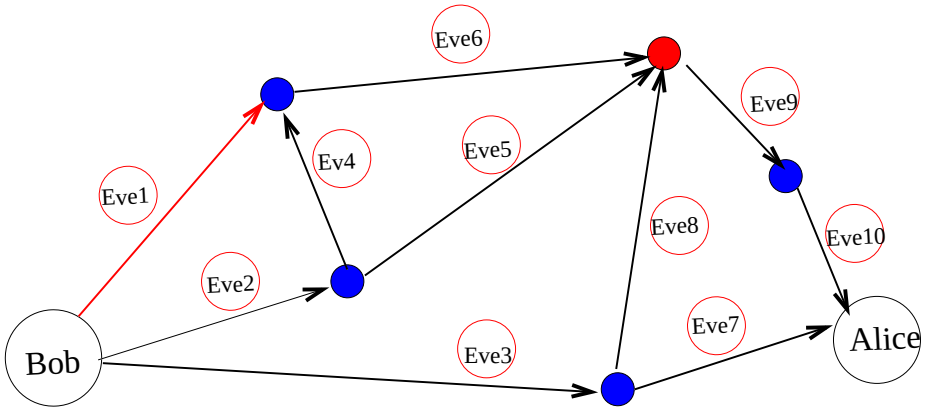


Figure 5.1: An example of network with malicious link/node (red marked ones)

error correction coding approach in dealing with this kind of active attacks.

Information theory [6] tells us that for any given channels, it is possible to construct error-correcting codes in which the likelihood of failure is arbitrarily low as long as the communication rate is below the capacity. Therefore, if the attacking pattern (i.e., error probability distribution) of the malicious adversary is known, it is easy to construct error-correcting codes to ensure that data is transmitted through the network. However, different from the usual transmission with errors occurring at temporally random instances, the data alteration occurs at random nodes in the network because of unknown adversary location. Thus protection is against errors occurring in the space domain; as such, redundancy need to be introduced in the space domain. This was also introduced by Yeung and Cai in [62, 63] in the context of network coding with active adversary and this approach can be adopted to tackle the threat considered herein.

5.2.2 Networks with Interference

Our present results considered the orthogonal transmission, i.e., the node receives the signals from different links without interfering amongst themselves. However, when applying it to wireless systems, the broadcast nature of wireless transmissions renders such orthogonal transmission assumption too simplistic. The problem becomes exceedingly hard in the presence of interference and not much is known for such a setup, illustrated in Fig. 5.2.

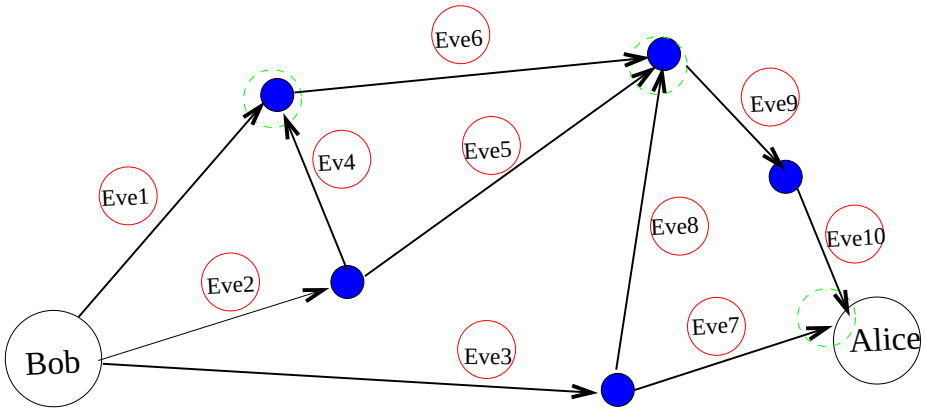


Figure 5.2: An example of network with interference, where the dashed green circles on the nodes represent that the signals received at those nodes are interfering with each other.

The main difficulties in dealing with arbitrary relay networks are (1) the broadcast nature of wireless communications, (2) the fact that signals from simultaneously transmitting nodes interfere with one another at other nodes. These give rise to complex signal interactions making the understanding of wireless networks difficult. The

signal interaction, however, also provides opportunities for secure communication, e.g., facilitating the generation of secret keys among communicating nodes. Studying the secure scheme of this model is of great interest and also challenge.

Bibliography

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 565–715, Oct. 1949.

[2] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54(8), pp. 1355–1387, 1975.

[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24(3), pp. 339–348, May 1978.

[4] S. Levy, *Crypto*, Allen Lane, 2001.

[5] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[6] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, pp. 379–423, 623–656, Jul. and Oct. 1948.

[7] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, Wiley, New York, 1991.

[8] Y. Liang, H. V. Poor, and S. Shamai (Shitz), *Information Theoretic Security*, Now Publisher, Delft, The Netherlands, 2009.

[9] S. K. Leung-Yan-Cheong and M. E. Hellman, "The gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, pp. 451–456, Jul. 1978.

[10] H. Yamamoto, "Coding theorem for secret sharing communication systems with two noisy channels," *IEEE Transactions on Information Theory*, vol. 35(3), pp. 572–578, May 1989.

[11] M. Van Dijk, "On a special class of broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 43(2), pp. 712–714, Mar. 1997.

[12] Y. Oohama, "Coding for relay channels with confidential messages," in *Proc. IEEE Information Theory Workshop*, Cairns, Australia, Sep. 2001.

[13] N. Cai and R. W. Yeung, "Secure network coding," in *Proc. IEEE International Symposium on Information Theory*, Jun. 2002.

[14] P. Moulin and J. O'Sullivan, "Information-theoretic analysis of information hiding," *IEEE Transactions on Information Theory*, vol. 49(3), pp. 563–593, Mar. 2003.

[15] I. Csiszar and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Transactions on Information Theory*, vol. 50(12), pp. 3047–3061, Dec. 2004.

[16] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," in *Proc. Allerton Conference on Communication, Control and Computing*, Monticello, IL, Sep. 2006.

[17] Y. Liang, H. V. Poor, and S. Shamai(Shitz), "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54(6), pp. 2470–2492, Jun. 2008.

[18] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J-M. Merolla, "Applications of ldpc codes to the wiretap channel," *IEEE Transactions on Information Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[19] S. Shafiee, N. Liu, , and S. Ulukus, "Towards the secrecy capcity of the gaussian mimo wiretap channel: the 2-2-1 channel," *IEEE Transactions on Information Theory*, vol. 55(9), pp. 4033–4039, Sep. 2009.

[20] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security. Information Theory," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[21] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy capacity regions," *IEEE Transactions on Information Theory*, Jun. 2008.

[22] Y. Liang and H. V. Poor, "Generalized multiple access channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 54(3), pp. 976–1002, Mar. 2008.

[23] L. Lai and H. El Gamal, "The relay-eavesdropper channel: cooperation for secrecy," *IEEE Transactions on Information Theory*, vol. 54(9), pp. 4005–4019, Sep. 2008.

[24] E. Tekin and A. Yener, "The general gaussian multiple access and two-way wiretap channels: achievable rates and cooperative jamming," *IEEE Transactions on Information Theory*, vol. 54(6), pp. 2735–2751, Jun. 2008.

[25] J. Xu, Y. Cao, and B. Chen, "Capacity bounds for broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 55, pp. 4529–4542, Oct. 2009.

[26] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interfernce and broadcst channels with confidential messages," in *Proc. Allerton conference on Communication, Control and Computing*, Sep. 2006.

[27] Y. Cao and B. Chen, "An achievable rate region for discrete memoryless broadcast channels with confidential messages," in *Proc. IEEE International Symposium on Information Theory*, Jun. 2008.

[28] K. Marton, "A coding theorem for the discrete memoryless broadcast channel," *IEEE Transactions on Information Theory*, vol. 25, pp. 306–311, May 1979.

[29] S. I. Gel'fand and M. S. Pinsker, "Capacity of a broadcast channel with one deterministic component," *Probl. Inform. Transm.*, vol. 16(1), pp. 17–25, Jan.–Mar. 1980.

[30] C. Nair and A. El Gamal, "An outer bound to the capacity region of the broadcast channel," in *Proc. IEEE International Symposium on Information Theory*, Seattle, WA, Jul. 2006.

[31] C. Nair and A. El Gamal, "An outer bound to the capacity region ofthe broadcast channel," *IEEE Transactions on Information Theory*, vol. 53(1), pp. 350–355, Jan. 2007.

[32] Y. Liang and G. Kramer, "Capacity theorems for cooperative relay broadcast channels," in *Proc. Annual Conference on Information Sciences and Systems*, Princeton, NJ, Mar. 2006.

[33] Y. Liang and G. Kramer, "Capacity theorems for cooperative relay broadcast channels," *IEEE Transactions on Information Theory*, vol. 53(10), pp. 3517–3535, Oct. 2007.

[34] Y. Liang, G. Kramer, and S. Shamai (Shitz), "Capacity outer bounds for broadcast channels," in *Proc. IEEE Information Theory Workshop*, Porto, Portugal, May 2008.

[35] C. Nair, "An outer bound for 2-receiver discrete memoryless broadcast channels," *Available at http://arxiv.org/abs/0807.3593*, Jul. 2008.

[36] T. M. Cover, "Broadcast channels," *IEEE Transactions on Information Theory*, vol. 18, pp. 2–4, Jan. 1972.

[37] T. M. Cover, "Comments on broadcast channels," *IEEE Transactions on Information Theory*, vol. 44(6), pp. 2524–2530, Oct. 1998.

[38] Y. Liang, G. Kramer, and H. V. Poor, "Equivalence of two inner bounds on the capacity region of the broadcast channel," in Proc. Allerton Conference on Communication, Control, and Computing, Monticello, IL, Sep. 2008.

[39] C. Nair and V. Wang, "On the inner and outer bounds for 2-receiver discrete memoryless broadcast channels," in *Proc. Information Theory and Application Workshop*, San Diego, CA, Jan. 2008.

[40] A. El Gamal and E.C. van der Meulen, "A proof of marton's coding theorem for the discrete memoryless broadcast channel," *IEEE Transactions on Information Theory*, vol. 27(1), pp. 120–122, Jan. 1981.

[41] Y. Chen and A. J. Han Vinck, "Wiretap channel with side information," in Proc. IEEE International Symposium on Information Theory, Seattle, WA, Jul. 2006.

[42] J. Korner and K. Marton, "Comparison of two noisy channels," *Topics in Information Theory*, pp. 411–423, Keszthely(Hungary), 1975.

[43] A. D. Wyner and J. Ziv, "A theorem on the entropy of certain binary sequences and applications: Part i," *IEEE Transactions on Information Theory*, vol. 19, pp. 769–772, Nov. 1973.

[44] I. Csiszar and J. Korner, "Information theory: Coding theorems for discrete memoryless systems," *New York: Academic*, 1981.

[45] H. Yamamoto, "Rate-distortion theory for the shannon cipher system," *IEEE Transactions on Information Theory*, vol. 43(3), pp. 827–835, May 1997.

[46] H. Yamamoto, "Information theory in cryptology," *IEICE Trans.*, vol. E74(9), pp. 2456–2464, Sep. 1991.

[47] J. Xu and B. Chen, "Broadcast confidential and public message," in *Proc. Conference on Information Sciences and systems*, Princeton, NJ, Mar. 2008.

[48] J. Xu and B. Chen, "On secure multi-channel communication systems," in *Proc. IEEE Military Communications Conference*, San Diego, CA, Nov. 2008.

[49] L. K. Ford and D. K. Fulkerson, *Flows in Networks*, Princeton University Press, Princeton, New Jersey, 1962.

[50] J. Feldman, T. Malkin, C. Stein, and R. A. Servedio, "On the capacity of secure network coding," in *Proc. Allerton Conference on Communication, Control and Computing*, Sep. 2004.

[51] S. El Rouayheb and E. Soljanin, "On Wiretap Networks II," in *Proc. IEEE International Symposium on Information Theory*, Jun. 2007.

[52] H. Yamamoto, "On secret sharing communication systems with two or three channels," *IEEE Transactions on Information Theory*, vol. 32, pp. 387–393, May 1986.

[53] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz), "Compound wiretap channels," in *Proc. Allerton Conference on Communication, Control and Computing*, Monticello, IL, Sep. 2007.

[54] T. Liu, V. Prabhakaran, and S. Vishwanath), "The secrecy capacity of a class of parallel Gaussian compound wiretap channels," in *Proc. IEEE International Symposium on Information Theory*, Toronto, Canada, Jul. 2008.

[55] P. Elias, A. Feinstein, and C. E. Shannon, "Note on maximum flow through a network," *IRE Transactions on Information Theory IT-2*, pp. 117–119, 1956.

[56] B. Bollobas, *Graph Theory, An Introductory Course*, New York:Springer-Verlag, 1979.

[57] S. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge University Press, 2004.

[58] D. Tse, "A deterministic model for wireless channels and its applications," in *Proc. IEEE Information Theory Workshop*, Lake Tahoe, Sep. 2007.

[59] S. Avestimehr, S. Diggavi, and D. Tse, "A deterministic approach to wireless relay networks," in *Proc. Allerton Conference on Communication, Control and Computing*, Monticello, IL, Sep. 2007.

[60] V. Prabhakaran, S. Diggavi, and D. Tse, "Broadcasting with common messages: a deterministic approach," in *Proc. Allerton Conference on Communication, Control and Computing*, Monticello, IL, Sep. 2007.

[61] G. Kramer, "Capacity results for the discrete memoryless network," *IEEE Transactions on Information Theory*, vol. 49(1), pp. 4–21, Jan. 2003.

[62] R. W. Yeung and N. Cai, "Network error correction, Part I: Basic concepts and upper bounds," *Communications in Information and Systems*, vol. 6, no. 1, pp. 19–36, 2006.

[63] N. Cai and R. W. Yeung, "Network error correction, Part II: Lower bounds," *Communications in Information and Systems*, vol. 6, no. 1, pp. 37–54, 2006.

VITA

NAME OF AUTHOR: Jin Xu

MAJOR: Electrical and Computer Engineering

EDUCATION:

Ph.D.	April 2010 (expected)	Syracuse University, Syracuse, NY
M.S.	July 2005	Institute of Automation, Chinese Academy of Sciences, China
B.E.	July 2002	University of Science and Technology of China, China

PUBLICATIONS:

Journal Articles

1. J. Xu, X. Shang, B. Chen, and H. V. Poor, "Parallel Discrete Memoryless Interference Channels Under Strong Interference: Seperability and Capacity Region Results," *in Preparation.*

2. J. Xu and B. Chen,"Secure Coding over Networks", *in Preparation.*

3. J. Xu, Y. Cao, and B. Chen, "Capacity bounds for broadcast channels with confidential messages", *IEEE Transactions on Information Theory*, vol. 55, pp. 4529-4542, Oct 2009.

Conference Proceedings

1. J. Xu, X. Shang, B. Chen, and H. V. Poor, "Parallel Discrete Memoryless Interference Channels Under Strong Interference: Seperability and Capacity Region Results," *Proc. IEEE Information Theory Workshop (ITW)*, Cairo, Egypt, Jan. 2010.

2. J. Xu and B. Chen, "Secure coding over networks," *Proc. IEEE International Symposium on Information Theory (ISIT)*, Seoul, Korea, June-July 2009.

3. J. Xu and B. Chen, "An outer bound to the rate-equivocation region of broadcast channels with two confidential messages," *Proc. IEEE Global Communications Conference (GLOBECOM)*, New Orleans, LA, Dec. 2008.

4. J. Xu and B. Chen, "On secure multi-channel communication systems," *Proc. IEEE Military Communications Conference (MILCOM)*, San Diego, CA, Nov. 2008.

5. J. Xu and B. Chen, "Broadcast confidential and public messages," *Proc. Annual Conference on Information Sciences and Systems (CISS)*, Princeton, NJ, March 2008.

6. J. Xu, B. Chen, and B. Himed, "A GLRT based STAP for the range dependent problem," *Proc. IEEE IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, Hawaii, April 2007.

AWARDS AND HONORS

- Nunan Poster Department Winner, Syracuse University , Apr. 2009
- Teaching Assistantship, Syracuse University, Jan. 2007 - May. 2007
- Research Assistantship, Syracuse University, Sep. 2005 - Jan. 2010