# INFORMATION-THEORETICALLY SECURE COMMUNICATION UNDER CHANNEL UNCERTAINTY

A Dissertation

by

HUNG DINH LY

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

May 2012

Major Subject: Electrical Engineering

# INFORMATION-THEORETICALLY SECURE COMMUNICATION UNDER CHANNEL UNCERTAINTY

A Dissertation

by

HUNG DINH LY

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Approved by:

| | |
|---|---|
| Chair of Committee, | Tie Liu |
| Committee Members, | Serap Savari |
| | Anxiao (Andrew) Jiang |
| | Srinivas Shakkottai |
| Head of Department, | Costas N. Georghiades |

May 2012

Major Subject: Electrical Engineering

# ABSTRACT

Information-Theoretically Secure Communication Under Channel Uncertainty.

(May 2012)

Hung Dinh Ly, B.S., Posts and Telecommunications Institute of Technology;

M.S., The University of Texas at Arlington

Chair of Advisory Committee: Dr. Tie Liu

Secure communication under channel uncertainty is an important and challenging problem in physical-layer security and cryptography. In this dissertation, we take a fundamental information-theoretic view at three concrete settings and use them to shed insight into efficient secure communication techniques for different scenarios under channel uncertainty.

First, a multi-input multi-output (MIMO) Gaussian broadcast channel with two receivers and two messages: a common message intended for both receivers (i.e., channel uncertainty for decoding the common message at the receivers) and a confidential message intended for one of the receivers but needing to be kept asymptotically perfectly secret from the other is considered. A matrix characterization of the secrecy capacity region is established via a channel-enhancement argument and an extremal entropy inequality previously established for characterizing the capacity region of a degraded compound MIMO Gaussian broadcast channel.

Second, a multilevel security wiretap channel where there is one possible realization for the legitimate receiver channel but multiple possible realizations for the eavesdropper channel (i.e., channel uncertainty at the eavesdropper) is considered. A coding scheme is designed such that the number of secure bits delivered to the legitimate receiver depends on the actual realization of the eavesdropper channel. More

specifically, when the eavesdropper channel realization is weak, all bits delivered to the legitimate receiver need to be secure. In addition, when the eavesdropper channel realization is strong, a prescribed part of the bits needs to remain secure. We call such codes security embedding codes, referring to the fact that high-security bits are now embedded into the low-security ones. We show that the key to achieving efficient security embedding is to jointly encode the low-security and high-security bits. In particular, the low-security bits can be used as (part of) the transmitter randomness to protect the high-security ones.

Finally, motivated by the recent interest in building secure, robust and efficient distributed information storage systems, the problem of secure symmetrical multilevel diversity coding (S-SMDC) is considered. This is a setting where there are channel uncertainties at both the legitimate receiver and the eavesdropper. The problem of encoding individual sources is first studied. A precise characterization of the entire admissible rate region is established via a connection to the problem of secure coding over a three-layer wiretap network and utilizing some basic polyhedral structure of the admissible rate region. Building on this result, it is then shown that the simple coding strategy of separately encoding individual sources at the encoders can achieve the minimum sum rate for the general S-SMDC problem.

To my family

# ACKNOWLEDGMENTS

It has been a great pleasure to be one of the first Ph.D. students of Professor Tie Liu. Over the past five years, I have gained a deep respect for Professor Liu's principles and philosophy about life and research. The valuable research skills and knowledge that I have learned from him will be extremely useful for my future career. Without his advice, encouragement and support throughout my Ph.D. process, I would have never completed this dissertation. Thank you so much, Professor Liu.

I am deeply grateful to Professor Serap Savari, Professor Andrew Jiang and Professor Srinivas Shakkottai for serving on my committee and being supportive in the different stages of my Ph.D. studies. I would also like to thank Dr. Yufei Blankenship, Professor Yingbin Liang, Professor Scott Miller and Ananth Balasubramanian for the fruitful collaborations and encouragement. Many interesting results presented in this dissertation come from such collaborations.

My sincere thanks go to Makesh Pravin Wilson, Ananth Balasubramanian, Phong Nguyen, Cuong Huynh, Jae Won Yoo, Jinjing Jiang, Neeharika Marukala, Shuo Li, Mustafa El-Halabi, Amir Salimi, Byung-Hak Kim, Meng Zeng, Lili Zhang, Armin Banaei, Jerry Huang and my Vietnamese friends in College Station for making my Ph.D. journey enjoyable.

Finally, I am truly thankful to my parents and my parents-in-law for their endless support and encouragement. They give me all freedom to follow my heart and pursue my dream. I wish to thank my wife, Sam, for enriching my life and always supporting me. Without her love, encouragement and patience, I would have never gone this far. My lovely daughters, Linh and Giang, make every single day in my life joyful and memorable. This dissertation is dedicated to them.

TABLE OF CONTENTS

CHAPTER Page

I INTRODUCTION . . . . . 1
A. Motivation . . . . . 1
B. Prior Work . . . . . 5
C. Dissertation Outline . . . . . 10

II MULTIPLE-INPUT MULTIPLE-OUTPUT GAUSSIAN BROADCAST CHANNELS WITH COMMON AND CONFIDENTIAL MESSAGES . . . . . 12
A. Introduction . . . . . 12
B. Main Results . . . . . 16
C. Aligned MIMO Gaussian Broadcast Channel . . . . . 19
D. General MIMO Gaussian Broadcast Channel . . . . . 29
E. Numerical Examples . . . . . 33
F. Concluding Remarks . . . . . 37

III SECURITY EMBEDDING CODES . . . . . 39
A. Introduction . . . . . 39
B. Two-Level Security Wiretap Channel . . . . . 42
1. Channel Model . . . . . 42
2. Main Results . . . . . 45
3. Proof of Theorem 5 . . . . . 48
C. Gaussian Two-Level Security Wiretap Channel . . . . . 53
1. Scalar Channel . . . . . 53
2. Independent Parallel Channel . . . . . 56
D. Two-Level Security Wiretap Channel II . . . . . 60
E. Concluding Remarks . . . . . 64

IV SECURE SYMMETRICAL MULTILEVEL DIVERSITY CODING 65
A. Introduction . . . . . 65
B. Secure Symmetrical Single-Level Diversity Coding . . . . . 67
1. Problem Statement . . . . . 67
2. Main Results . . . . . 69
3. Proof of Theorem 15 . . . . . 73

CHAPTER Page

C. Secure Symmetrical Multilevel Diversity Coding . . . . . 78
1. Problem Statement . . . . . 78
2. Main Results . . . . . 80
3. Proof of the Main Results . . . . . 81
D. Concluding Remarks . . . . . 86

V CONCLUSIONS . . . . . 87

REFERENCES . . . . . 91

APPENDIX A . . . . . 96

APPENDIX B . . . . . 100

APPENDIX C . . . . . 104

APPENDIX D . . . . . 106

APPENDIX E . . . . . 108

VITA . . . . . 111

# LIST OF FIGURES


| FIGURE | | Page |
|---|---|---|
| 1 | The Shannon cipher system. | 2 |
| 2 | The wiretap channel. | 3 |
| 3 | MIMO Gaussian broadcast channel with common and confidential messages. | 13 |
| 4 | Enhanced MIMO Gaussian broadcast channel with common and confidential messages. | 23 |
| 5 | An illustration of the secrecy capacity regions of the MIMO Gaussian broadcast channel with common and confidential messages. | 35 |
| 6 | Two-level security wiretap channel. | 43 |
| 7 | Codebook structure for a coding scheme that combines rate splitting, superposition coding, (nested) binning, and prefix coding. | 49 |
| 8 | Secrecy capacity region of the scalar Gaussian two-level security wiretap channel ($a > b_1 > b_2$). For comparison, the dashed line and the dotted line are the boundary of the time-sharing and power-sharing rate regions, respectively. | 55 |
| 9 | Secrecy capacity region of the independent parallel Gaussian two-level security wiretap channel under an average total power constraint. The intersection of the dashed lines are outside the secrecy capacity region, indicating that the channel is not perfectly embeddable. | 59 |
| 10 | The rate region $\mathcal{R}(L, k, H)$ for $L = 2$ and 3. The $R_l = 0$ slices of $\mathcal{R}(3, 2, H)$ are isomorphic to $\mathcal{R}(2, 1, H)$. | 72 |
| 11 | The $(L, N, m, (R_1, \ldots, R_L))$ wiretap network. | 75 |

# CHAPTER I

# INTRODUCTION

## A. Motivation

Broadcast is a fundamental nature of wireless communication: any receiver within the transmission range can listen to the transmission and potentially decode some of the messages. With appropriate coding architecture, the broadcast nature of wireless communication can be used to the advantage of simultaneously transmitting to several receivers at high rates. On the other hand, eavesdropping also becomes easier due to the broadcast nature of wireless communication. The traditional approach to protect against eavesdropping is cryptography. There are two different cryptographic systems: secret-key cryptosystem and public-key cryptosystem [1]. Secret-key cryptosystems require a secret key shared between the sender and the receiver. Comparatively, public-key cryptosystems do not require the pre-establishment of a secret key, but are more susceptible to advanced attacks such as the man-in-the-middle attack. Both cryptosystems are based on the assumption that the eavesdropper has limited computation power and hence lack *"absolute"* security.

In 1949, Shannon introduced the notion of information-theoretic security. In his seminal paper [2], Shannon defined a secrecy system to be perfectly secure if the cipher text is statistically independent of the message. Note that this is the strongest notion of security, as observing cipher text now does not entail any information regarding the message being sent. In his cipher system, Shannon assumed that 1)

---

The journal model is *IEEE Transactions on Information Theory*.

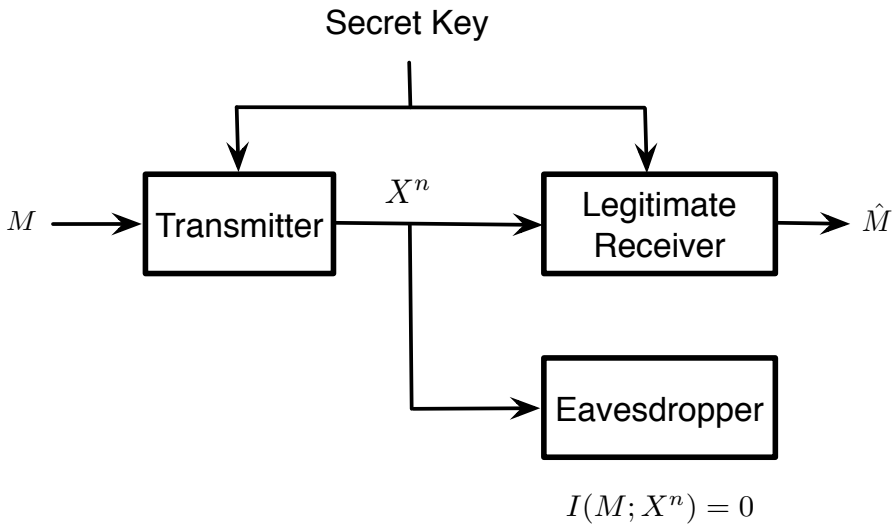



Fig. 1. The Shannon cipher system.

the transmitter and the legitimate receiver share a secret key, which is unknown to the eavesdropper; 2) transmission of the message is noiseless to both the legitimate receiver and the eavesdropper. Under these assumptions, Shannon showed that to have a perfect secrecy system, the length of the secret key should be at least as long as the length of the message being sent [2]. See Fig. 1 for an illustration of a Shannon cypher system. Shannon's result on perfect secrecy systems is certainly pessimistic. The reason for such pessimism was not clear until the work of Wyner in the 1970's. In his seminal paper [3], Wyner argued that the reason for Shannon's pessimistic result is *not* because of the strong notion of information-theoretic security, but actually due to the assumption that the transmission of the message is over *noiseless* channels. By extending the Shannon cypher system to a noisy setting, Wyner [3] considered the problem of communication over a broadcast channel with two receivers, one interpreted as legitimate receiver and the other as eavesdropper.

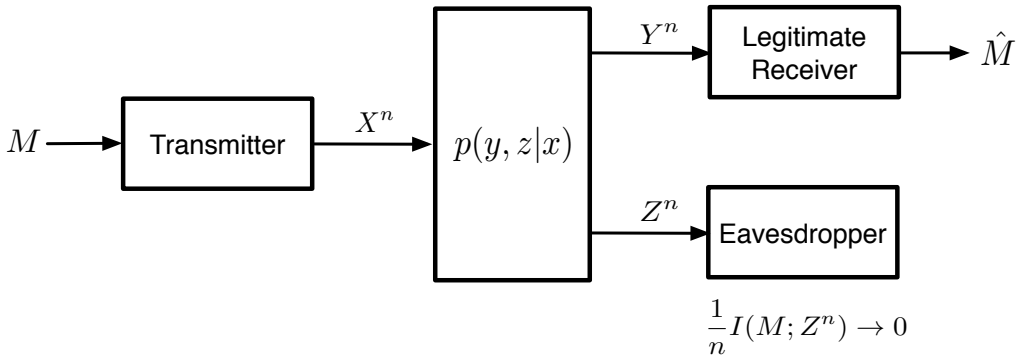



Fig. 2. The wiretap channel.

Both the legitimate receiver and the eavesdropper channels are assumed to be *known* at the transmitter. Furthermore, the eavesdropper channel is assumed to be noisier than the legitimate receiver channel. By exploring the statistical *advantage* of the legitimate receiver channel over the eavesdropper channel, one may design coding schemes that can deliver a confidential message reliably to the legitimate receiver while keeping it asymptotically perfectly secret from the eavesdropper. No secret key is needed to achieve asymptotically perfectly secure communication. This result was later extended to the general broadcast channel by Csiszár and Körner [4]. The line of research was termed as the wiretap channel; see Fig. 2 for an illustration of the basic model.

While assuming the transmitter's knowledge of the legitimate receiver channel might be reasonable (particularly when a feedback link is available), assuming that the transmitter knows the eavesdropper channel is *unrealistic* in most scenarios. This is mainly because the eavesdropper is an *adversary*, which usually has no incentive to help the transmitter to acquire its channel state information. Hence, it is critical

that physical layer security techniques are designed to withstand the *uncertainty* of the eavesdropping channel only or of both the legitimate receiver channel and the eavesdropper channel in general.

In this dissertation, we extend the basic channel model of Wyner [3] and Csiszár-Körner [4] to more complex and realistic secure communication scenarios under channel uncertainty. In particular, we take a fundamental information-theoretic view at three concrete settings and use them to shed insight into efficient secure communication techniques for different scenarios under channel uncertainty.

1. ***Broadcast channels with common and confidential messages.*** Here, in addition to the confidential message, there is also a common message intended for both receivers (i.e., channel uncertainty for decoding the common message at the receivers). This problem was first studied by Csiszár and Körner [4], who derived a single-letter expression for the capacity region. In this dissertation, our focus is on the specific MIMO communication scenario and to understand the fundamental limitation of such MIMO secret communication.

2. ***Multilevel security wiretap channel.*** This problem is motivated by the fact that assuming the transmitter's knowledge of the eavesdropper channel is, on most occasions, unrealistic. This is because the eavesdropper is an *adversary*, which usually has no incentive to feedback its channel state information to the transmitter. Hence, it is critical that communication schemes are designed to withstand the *uncertainty* of the eavesdropper channel. In this setting, we consider the communication scenario where there are *multiple* possible realizations for the eavesdropper channel. Which realization actually materializes is *unknown* to the transmitter a priori (i.e., channel uncertainty at the eavesdropper). Our goal is to design coding schemes such that the number of *secure*

bits delivered to the legitimate receiver depends on the actual realization of the eavesdropper channel. More specifically, when the eavesdropper channel realization is strong, we require part of the bits delivered to the legitimate receiver to be secure. On the other hand, when the eavesdropper channel realization is weak, all bits delivered to the legitimate receiver need to be secure. We call such codes *security embedding codes*, referring to the fact that high-security bits are now embedded into low-security ones. Our main goal here is to understand the fundamental limitations of the security embedding.

3. ***Secure symmetrical multilevel diversity coding.*** This source coding problem is motivated by recent interest on building secure, robust and efficient distributed information storage systems (e.g., storage cloud). Here, $L-N$ discrete memoryless information sources $(S_1, \ldots, S_{L-N})$ of an decreasing importance order are encoded by $L$ encoders. A legitimate receiver and an eavesdropper have access to subsets $U$ and $A$ of the encoder outputs, respectively. Which subsets $U$ and $A$ will materialize are unknown a priori at the encoders (i.e., channel uncertainties at both the legitimate receiver and the eavesdropper). However, no matter which subsets $U$ and $A$ actually occur, the $k$ most important sources $(S_1, \ldots, S_k)$ need to be perfectly reconstructable at the legitimate receiver whenever $|U| = N + k$, and all sources $(S_1, \ldots, S_{L-N})$ need to be kept perfectly secure from the eavesdropper as long as $|A| \leq N$. Our ultimate goal is to understand the fundamental limit of this secure communication scenario.

## B. Prior Work

In this section, we briefly review some basic results on the secrecy capacity and optimal encoding scheme for several classical wiretap channel settings. These re-

sults provide performance and structural benchmarks for our study in the consequent chapters. We first consider a discrete memoryless wiretap channel with transition probability $p(y, z|x)$, where $X$ is the channel input, and $Y$ and $Z$ are the channel outputs at the legitimate receiver and the eavesdropper, respectively. This communication channel is illustrated in Fig. 2. The transmitter has a message $M$, uniformly drawn from $\{1, \ldots, 2^{nR}\}$ where $n$ is the communication block length and $R$ is the rate of communication. The message $M$ is intended for the legitimate receiver, but needs to be kept asymptotically perfectly secret from the eavesdropper. Mathematically, this secrecy constraint can be written as

$$\frac{1}{n} I(M; Z^n) \to 0 \tag{1.1}$$

in the limit as communication block length $n \to \infty$, where $Z^n = (Z[1], \ldots, Z[n])$ is the collection of the channel outputs at the eavesdropper during communication. A communication rate $R$ is said to be *achievable* if there exists a sequence of codes of rate $R$ such that the message $M$ can be reliably delivered to the legitimate receiver while satisfying the asymptotic perfect secrecy constraint (1.1). The largest achievable rate is termed as the *secrecy capacity* of the channel.

A discrete memoryless wiretap channel $p(y, z|x)$ is said to be *degraded* if $X \to Y \to Z$ forms a Markov chain in that order. The secrecy capacity of a degraded wiretap channel was characterized by Wyner [3] and can be written as

$$C_s(P_{y,z|x}) = \max_{p(x)} [I(X; Y) - I(X; Z)] \tag{1.2}$$

where the maximization is over all possible input distributions $p(x)$. Later in [4], it was shown that the degradation requirement can be replaced by a weaker "more capable" condition. The scheme proposed in [3] to achieve the secrecy capacity (1.2) is *random binning*, which can be described as follows.

Consider a codebook of $2^{n(R+T)}$ codewords, each of length $n$. The codewords are partitioned into $2^{nR}$ bins, each containing $2^{nT}$ codewords. Given a message $m$ (which is uniformly drawn from $\{1, \ldots, 2^{nR}\}$), the encoder *randomly* and uniformly chooses a codeword $x^n$ in the $m$th bin and sends it through the channel. The legitimate receiver needs to decode the entire codebook (and hence recover the transmitted message $m$), so the overall rate $R + T$ cannot be too high. On the other hand, the rate $T$ of the sub-codebooks in each bin represents the amount of external randomness injected by the transmitter (transmitter randomness) into the channel and hence needs to be sufficiently large to confuse the eavesdropper. With an appropriate choice of the codebooks and the partitions of bins, it was shown in [3] that any communication rate $R$ less than the secrecy capacity (1.2) is achievable by the aforementioned random binning scheme.

For a *general* discrete memoryless wiretap channel $p(y, z|x)$ where the channel outputs $Y$ and $Z$ are *not* necessarily ordered, the random binning scheme of [3] is *not* necessarily optimal. In this case, the secrecy capacity of the channel was characterized by Csiszár and Körner [4] and can be written as

$$C_s(P_{y,z|x}) = \max_{p(v,x)} [I(V;Y) - I(V;Z)] \tag{1.3}$$

where $V$ is an auxiliary random variable satisfying the Markov chain $V \to X \to (Y, Z)$. The scheme proposed in [4] is to first *prefix* the channel input $X$ by $V$ and view $V$ as the input of the *induced* wiretap channel $p(y, z|v) = \sum_x p(y, z|x)p(x|v)$. Applying the random binning scheme of [3] to the induced wiretap channel $p(y, z|v)$ proves the achievability of rate $I(V;Y) - I(V;Z)$ for any given joint auxiliary-input distribution $p(v, x)$.

In communication engineering, communication channels are usually modeled as discrete-time channels with real input and additive white Gaussian noise. Consider a

(scalar) Gaussian wiretap channel where the channel outputs at the legitimate receiver and the eavesdropper are given by

$$\begin{aligned} Y &= \sqrt{a}X + N_1 \\ Z &= \sqrt{b}X + N_2. \end{aligned} \tag{1.4}$$

Here, $X$ is the channel input which is subject to the average power constraint

$$\frac{1}{n}\sum_{i=1}^{n}(X[i])^2 \leq P \tag{1.5}$$

$a$ and $b$ are the channel gains for the legitimate receiver and the eavesdropper channel respectively, and $N_1$ and $N_2$ are additive white Gaussian noise with zero means and *unit* variances. The secrecy capacity of the channel was characterized in [5] and can be written as

$$C_s(P, a, b) = \left[\frac{1}{2}\log(1 + aP) - \frac{1}{2}\log(1 + bP)\right]^+ \tag{1.6}$$

where $[x]^+ := \max(0, x)$. Note from (1.6) that $C_s(P, a, b) > 0$ if and only if $a > b$. That is, for the Gaussian wiretap channel (1.4), asymptotic perfect secrecy communication is possible if and only if the legitimate receiver has a larger channel gain than the eavesdropper. In this case, we can equivalently write the channel output $Z$ at the eavesdropper as a degraded version of the channel output $Y$ at the legitimate receiver, and the random binning scheme of [3] with *Gaussian* codebooks and *full* transmit power achieves the secrecy capacity of the channel.

A closely related engineering scenario consists of a bank of $L$ independent parallel scalar Gaussian wiretap channels [6]. In this scenario, the channel outputs at the legitimate receiver and the eavesdropper are given by $Y = (Y_1, \ldots, Y_L)$ and $Z =$

$(Z_1, \ldots, Z_L)$ where

$$\begin{aligned} Y_l &= \sqrt{a_l} X_l + N_{1,l} \\ Z_l &= \sqrt{b_l} X_l + N_{2,l} \end{aligned}, \quad l = 1, \ldots, L. \tag{1.7}$$

Here, $X_l$ is the channel input for the $l$th subchannel, $a_l$ and $b_l$ are the channel gains for the legitimate receiver and the eavesdropper channel respectively in the $l$th subchannel, and $N_{1,l}$ and $N_{2,l}$ are additive white Gaussian noise with zero means and *unit* variances. Furthermore, $(N_{1,l}, N_{2,l})$ are independent for $l = 1, \ldots, L$ so all $L$ subchannels are independent of each other.

Two different types of power constraints have been considered: the average individual per-subchannel power constraint

$$\frac{1}{n} \sum_{i=1}^{n} (X_l[i])^2 \leq P_l, \quad l = 1, \ldots, L \tag{1.8}$$

and the average total power constraint

$$\sum_{l=1}^{L} \left[ \frac{1}{n} \sum_{i=1}^{n} (X_l[i])^2 \right] \leq P. \tag{1.9}$$

Under the average individual per-subchannel power constraint (1.8), the secrecy capacity of the independent parallel Gaussian wiretap channel (1.7) is given by [6]

$$C_s(\{P_l, a_l, b_l\}_{l=1}^{L}) = \sum_{l=1}^{L} C_s(P_l, a_l, b_l) \tag{1.10}$$

where $C_s(P, a, b)$ is defined as in (1.6). Clearly, any communication rate less than the secrecy capacity (1.10) can be achieved by using $L$ separate scalar Gaussian wiretap codes, each for one of the $L$ subchannels. The secrecy capacity, $C_s(P, \{a_l, b_l\}_{l=1}^{L})$, under the average total power constraint (1.9) is given by

$$C_s(P, \{a_l, b_l\}_{l=1}^{L}) = \max_{(P_1, \ldots, P_L)} \sum_{l=1}^{L} C_s(P_l, a_l, b_l) \tag{1.11}$$

where the maximization is over all possible power allocations $(P_1, \ldots, P_L)$ such that $\sum_{l=1}^{L} P_l \leq P$. A waterfilling-like solution for the optimal power allocation was derived in [6, Theorem 1], which provides an efficient way to numerically calculate the secrecy capacity $C_s(P, \{a_l, b_l\}_{l=1}^{L})$. This line of wiretap channel (or physical-layer security) research has been a very active area of research in information theory. One may refer to [7] and [8] for overviews of recent progress in this field.

## C. Dissertation Outline

Secure communication under channel uncertainty is an important and challenging problem in physical-layer security and cryptography. In this dissertation, we take a fundamental information-theoretic view at three concrete settings and use them to shed insight into efficient secure communication techniques for different scenarios under channel uncertainty.

First, a multi-input multi-output (MIMO) Gaussian broadcast channel with two receivers and two messages: a common message intended for both receivers (i.e., channel uncertainty for decoding the common message at the receivers) and a confidential message intended for one of the receivers but needing to be kept asymptotically perfectly secret from the other is considered. A matrix characterization of the secrecy capacity region is established via a channel-enhancement argument and an extremal entropy inequality previously established for characterizing the capacity region of a degraded compound MIMO Gaussian broadcast channel.

Second, a multilevel security wiretap channel where there is one possible realization for the legitimate receiver channel but multiple possible realizations for the eavesdropper channel (i.e., channel uncertainty at the eavesdropper) is considered. A coding scheme is designed such that the number of secure bits delivered to the legit-

imate receiver depends on the actual realization of the eavesdropper channel. More specifically, when the eavesdropper channel realization is weak, all bits delivered to the legitimate receiver need to be secure. In addition, when the eavesdropper channel realization is strong, a prescribed part of the bits needs to remain secure. We call such codes security embedding codes, referring to the fact that high-security bits are now embedded into the low-security ones. We show that the key to achieving efficient security embedding is to jointly encode the low-security and high-security bits. In particular, the low-security bits can be used as (part of) the transmitter randomness to protect the high-security ones.

Finally, motivated by the recent interest in building secure, robust and efficient distributed information storage systems, the problem of secure symmetrical multilevel diversity coding (S-SMDC) is considered. This is a setting where there are channel uncertainties at both the legitimate receiver and the eavesdropper. The problem of encoding individual sources is first studied. A precise characterization of the entire admissible rate region is established via a connection to the problem of secure coding over a three-layer wiretap network and utilizing some basic polyhedral structure of the admissible rate region. Building on this result, it is then shown that the simple coding strategy of separately encoding individual sources at the encoders can achieve the minimum sum rate for the general S-SMDC problem.

The rest of the dissertation is organized as follows. Chapter II presents our results on the multiple-input multiple-output Gaussian broadcast channel with common and confidential messages, which was reported in [9]. Chapter III presents our results on the multilevel security wiretap channel. The results were also reported in [10]. Chapter IV presents our results on the secure symmetrical multilevel diversity coding, which were reported in [11]. Finally, in Chapter V, we summarize our main contributions in this dissertation and point out some future research directions.

# CHAPTER II

# MULTIPLE-INPUT MULTIPLE-OUTPUT GAUSSIAN BROADCAST CHANNELS WITH COMMON AND CONFIDENTIAL MESSAGES*

## A. Introduction

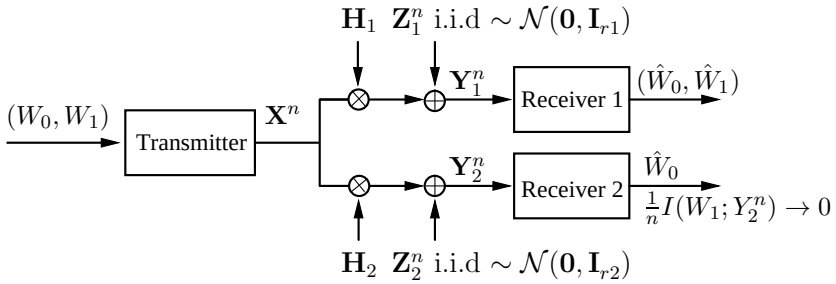
Understanding the fundamental limits of multiple-input multiple-output (MIMO) secrecy communication is an important research topic in wireless physical layer security. A basic model of MIMO secrecy communication is a MIMO Gaussian broadcast channel with two receivers, for which the channel outputs at time index $m$ are given by

$$\mathbf{Y}_k[m] = \mathbf{H}_k\mathbf{X}[m] + \mathbf{Z}_k[m], \quad k = 1, 2 \tag{2.1}$$

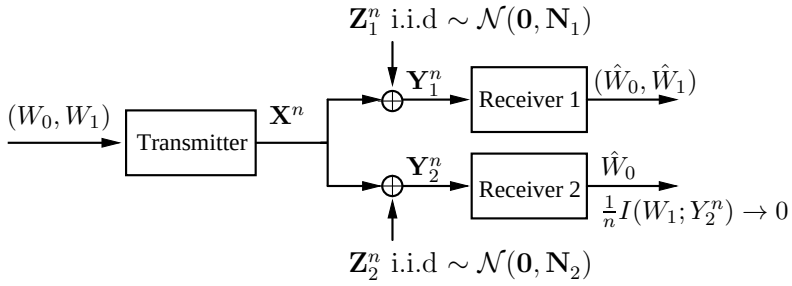
where $\mathbf{H}_k$ is the (real) channel matrix of size $r_k \times t$ for receiver $k$, and $\{\mathbf{Z}_k[m]\}_m$ is an independent and identically distributed (i.i.d.) additive vector Gaussian noise process with zero mean and identity covariance matrix. The channel input $\{\mathbf{X}[m]\}_m$ is subject to an average total power constraint:

$$\frac{1}{n}\sum_{m=1}^{n} \|\mathbf{X}[m]\|^2 \leq P. \tag{2.2}$$

The transmitter has a set of two independent messages $(W_0, W_1)$, where $W_0$ is a common message intended for both receivers 1 and 2, and $W_1$ is a confidential message intended for receiver 1 but needing to be kept secret from receiver 2. *The




(a) The general case




(b) The aligned case

Fig. 3. MIMO Gaussian broadcast channel with common and confidential messages.

confidentiality of message $W_1$ at receiver 2 is measured using the information-theoretic criterion [3, 4]:

$$\frac{1}{n} I(W_1; \mathbf{Y}_2^n) \to 0 \tag{2.3}$$

where $\mathbf{Y}_2^n := (\mathbf{Y}_2[1], \ldots, \mathbf{Y}_2[n])$, and the limit is taken as the block length $n \to \infty$. An illustration of this communication scenario is shown in Figure 3(a). The goal is to characterize the entire rate region $\mathcal{C}_s(\mathbf{H}_1, \mathbf{H}_2, P)$ that includes all rate pairs $(R_0, R_1)$ that can be achieved by any coding scheme. In this chapter, we term $\mathcal{C}_s(\mathbf{H}_1, \mathbf{H}_2, P)$ as the *secrecy capacity region* despite the fact that $W_0$ is not a confidential message.

In their seminar work [4], Csiszár and Körner considered the discrete memoryless case of the problem. A single-letter expression of the secrecy capacity region was given as the set of nonnegative rate pairs $(R_0, R_1)$ satisfying

$$\begin{aligned} R_0 &\leq \min\left[I(U;Y_1), I(U;Y_2)\right] \\ R_1 &\leq I(V;Y_1|U) - I(V;Y_2|U) \end{aligned} \tag{2.4}$$

for some $p(u,v,x,y_1,y_2) = p(u)p(v|u)p(x|v)p(y_1,y_2|x)$, where $p(y_1,y_2|x)$ is the transition probability of the discrete memoryless broadcast channel. Thus, in principle, the secrecy capacity region $\mathcal{C}_s(\mathbf{H}_1, \mathbf{H}_2, P)$ can be computed by evaluating the Csiszár-Körner region (2.4) for the MIMO Gaussian broadcast channel (2.1).

However, directly evaluating (2.4) for the MIMO Gaussian broadcast channel (2.1) appears difficult due to the presence of the auxiliary variables $U$ and $V$. Consider, for example, the special case where the common message $W_0$ is absent, i.e., $R_0 = 0$. Let $U$ be deterministic in (2.4). Then, the maximum of $R_1$ can be determined by solving the optimization program

$$\max_{p(x,v)} \left[I(V;Y_1) - I(V;Y_2)\right]. \tag{2.5}$$

In literature, the problem of communicating a confidential message over a MIMO Gaussian broadcast channel is termed as the MIMO Gaussian wiretap channel problem. Characterizing the secrecy capacity of the MIMO Gaussian wiretap channel has been an active area of research in recent years. However, despite intensive effort [12, 13, 14, 15, 16], determining the secrecy capacity of the MIMO Gaussian wiretap channel via *directly* solving the optimization program (2.5) remains intractable.

Recently, Khisti and Wornell [14] and Oggier and Hassibi [15] studied the MIMO Gaussian wiretap channel problem and proposed an *indirect* approach to solve the optimization program (2.5). The main idea was to compute an upper bound on the

secrecy capacity by considering a fictitious MIMO Gaussian wiretap channel in which the legitimate receiver has access to both received signals $\{\mathbf{Y}_1[m]\}_m$ and $\{\mathbf{Y}_2[m]\}_m$. For any fixed correlation between the additive noise $\mathbf{Z}_1[m]$ and $\mathbf{Z}_2[m]$, Khisti and Wornell [14] and Oggier and Hassibi [15] showed that *Gaussian* random binning *without* prefix coding is optimal for the fictitious channel. Comparing the upper bound (minimized over all possible correlations between $\mathbf{Z}_1[m]$ and $\mathbf{Z}_2[m]$) with the achievable secrecy rate by choosing a *Gaussian* $V = \mathbf{X}$ in the objective function of (2.5) established an exact matrix characterization of the secrecy capacity. However, matching the upper and lower bounds requires complicated matrix analysis, which makes the approach difficult to extend to the more general scenario with both common and confidential messages.

More recently, Liu and Shamai [16] presented an alternative, simpler characterization of the secrecy capacity of the MIMO Gaussian wiretap channel. Compared with the work of [14] and [15], there are two key differences in the argument of [16]

1. Instead of the average total power constraint (2.2), [16] considered the more general matrix power constraint:

$$\frac{1}{n}\sum_{m=1}^{n}\left(\mathbf{X}[m]\mathbf{X}^{\mathrm{T}}[m]\right) \preceq \mathbf{S} \tag{2.6}$$

   where $\mathbf{S}$ is a positive semidefinite matrix, and "$\preceq$" denotes "less than or equal to" in the positive semidefinite ordering between real symmetric matrices.

2. Different from the Sato-like [17] argument of [14] and [15], the upper bound on the secrecy capacity in [16] was obtained by considering an *enhanced* MIMO Gaussian wiretap channel that has the *same* secrecy capacity as the original wiretap channel. Channel-enhancement argument was first introduced by Weingarten et al. [18] to characterize the *private message* capacity region of the

MIMO Gaussian broadcast channel; [16] was the first to apply this argument to MIMO *secrecy* communication problems.

The main goal of this chapter is to *adapt* the channel-enhancement argument of [16] to the more general problem of MIMO Gaussian broadcast channel with both common and confidential messages. Our main result is that for the MIMO Gaussian broadcast channel (2.1), a jointly *Gaussian* $(U, V, \mathbf{X})$ with $V = \mathbf{X}$ is *optimal* for the Csiszár-Körner region (2.4). This establishes a matrix characterization of the secrecy capacity region of the MIMO Gaussian broadcast channel under a matrix power constraint.

The rest of the chapter is organized as follows. In Section B, we summarize the main results of the chapter. In Section C, we consider the special case of the MIMO Gaussian broadcast channel (2.1) in which the channel matrices $\mathbf{H}_1$ and $\mathbf{H}_2$ are square and invertible, and use a channel-enhancement argument to characterize the secrecy capacity region. In Section D, we broaden the result of Section C, via a limiting argument, to the general case, and characterize the secrecy capacity region of the general MIMO Gaussian broadcast channel. We provide some numerical examples to illustrate the main results of the chapter in Section E. Finally, in Section F, we conclude the chapter with some remarks.

## B. Main Results

The following theorem summarizes the secrecy capacity region of the MIMO Gaussian broadcast channel with common and confidential messages under a matrix power constraint.

**Theorem 1.** *The secrecy capacity region* $\mathcal{C}_s(\mathbf{H}_1, \mathbf{H}_2, \mathbf{S})$ *of the MIMO Gaussian broadcast channel* (2.1) *with messages* $W_0$ *(intended for both receivers 1 and 2) and* $W_1$

*(intended for receiver 1 but needing to be kept asymptotically perfectly secret from receiver 2) under the matrix power constraint* (2.6) *is given by the set of all nonnegative rate pairs* $(R_0, R_1)$ *satisfying*

$$\begin{aligned} R_0 &\leq \min\left(\tfrac{1}{2}\log\left|\tfrac{\mathbf{H}_1\mathbf{S}\mathbf{H}_1^{\mathrm{T}}+\mathbf{I}_{r_1}}{\mathbf{H}_1\mathbf{B}\mathbf{H}_1^{\mathrm{T}}+\mathbf{I}_{r_1}}\right|, \tfrac{1}{2}\log\left|\tfrac{\mathbf{H}_2\mathbf{S}\mathbf{H}_2^{\mathrm{T}}+\mathbf{I}_{r_2}}{\mathbf{H}_2\mathbf{B}\mathbf{H}_2^{\mathrm{T}}+\mathbf{I}_{r_2}}\right|\right) \\ R_1 &\leq \tfrac{1}{2}\log\left|\mathbf{H}_1\mathbf{B}\mathbf{H}_1^{\mathrm{T}}+\mathbf{I}_{r_1}\right| - \tfrac{1}{2}\log\left|\mathbf{H}_2\mathbf{B}\mathbf{H}_2^{\mathrm{T}}+\mathbf{I}_{r_2}\right| \end{aligned} \tag{2.7}$$

*for some* $0 \preceq \mathbf{B} \preceq \mathbf{S}$. *Here,* $\mathbf{I}_{r_k}$ *denotes the identity matrix of size* $r_k \times r_k$.

As mentioned previously, the MIMO Gaussian wiretap channel problem can be considered as a special case here with the common rate $R_0 = 0$. We have thus recovered the main result of [16], restated below as a corollary.

**Corollary 2** ([16])**.** *The secrecy capacity* $C_s(\mathbf{H}_1, \mathbf{H}_2, \mathbf{S})$ *of the MIMO Gaussian broadcast channel* (2.1) *with a confidential message messages* $W$ *(intended for receiver 1 but needing to be kept asymptotically perfectly secret from receiver 2) under the matrix power constraint* (2.6) *is given by*

$$C_s(\mathbf{H}_1, \mathbf{H}_2, \mathbf{S}) = \max_{0\preceq\mathbf{B}\preceq\mathbf{S}} \left(\frac{1}{2}\log\left|\mathbf{H}_1\mathbf{B}\mathbf{H}_1^{\mathrm{T}}+\mathbf{I}_{r_1}\right| - \frac{1}{2}\log\left|\mathbf{H}_2\mathbf{B}\mathbf{H}_2^{\mathrm{T}}+\mathbf{I}_{r_2}\right|\right). \tag{2.8}$$

In engineering practice, it is particularly relevant to consider the average total power constraint. The following corollary summarizes the secrecy capacity region of the MIMO Gaussian broadcast channel with common and confidential messages under an average total power constraint. The result is a simple consequence of [18, Lemma 1].

**Corollary 3.** *The secrecy capacity region* $\mathcal{C}_s(\mathbf{H}_1, \mathbf{H}_2, P)$ *of the MIMO Gaussian broadcast channel* (2.1) *with messages* $W_0$ *(intended for both receivers 1 and 2) and* $W_1$ *(intended for receiver 1 but needing to be kept asymptotically perfectly secret from receiver 2) under the average total power constraint* (2.2) *is given by the set of all*

*nonnegative rate pairs* $(R_0, R_1)$ *satisfying*

$$\begin{aligned} R_0 &\leq \min\left[\tfrac{1}{2}\log\left|\tfrac{\mathbf{H}_1(\mathbf{B}_1+\mathbf{B}_2)\mathbf{H}_1^{\mathrm{T}}+\mathbf{I}_{r_1}}{\mathbf{H}_1\mathbf{B}_1\mathbf{H}_1^{\mathrm{T}}+\mathbf{I}_{r_1}}\right|, \tfrac{1}{2}\log\left|\tfrac{\mathbf{H}_2(\mathbf{B}_1+\mathbf{B}_2)\mathbf{H}_2^{\mathrm{T}}+\mathbf{I}_{r_2}}{\mathbf{H}_2\mathbf{B}_1\mathbf{H}_2^{\mathrm{T}}+\mathbf{I}_{r_2}}\right|\right] \\ R_1 &\leq \tfrac{1}{2}\log\left|\mathbf{H}_1\mathbf{B}_1\mathbf{H}_1^{\mathrm{T}}+\mathbf{I}_{r_1}\right| - \tfrac{1}{2}\log\left|\mathbf{H}_2\mathbf{B}_1\mathbf{H}_2^{\mathrm{T}}+\mathbf{I}_{r_2}\right| \end{aligned} \tag{2.9}$$

*for some positive semidefinite matrices* $\mathbf{B}_1$ *and* $\mathbf{B}_2$ *with* $\mathrm{Tr}(\mathbf{B}_1+\mathbf{B}_2) \leq P$.

The achievability proof of Theorem 1 follows from the Csiszár-Körner region (2.4) by letting $U$ be a $t$-dimensional Gaussian vector with zero mean and covariance matrix $\mathbf{S}-\mathbf{B}$ and $V = \mathbf{X} = U + G$, where $G$ is a $t$-dimensional Gaussian vector with zero mean and covariance matrix $\mathbf{B}$ and is independent of $U$. Note that prefix coding is *not* needed in communicating the confidential message $W_1$ even though the corresponding eavesdropper channel may not be degraded with respect to the legitimate receiver channel.

The converse of Theorem 1 follows from an adaptation of the channel-enhancement argument of [16] with the following two new ingredients:

1. To obtain an enhanced MIMO Gaussian broadcast channel that has the *same* weighted secrecy sum-capacity as the original channel, we need to split receiver 1 into two *virtual* receivers: one as the legitimate receiver for the confidential message $W_1$, and the other as one of the intended receivers for the common message $W_0$. Only the legitimate receiver for the confidential message $W_1$ is enhanced in the proof.

2. With only a confidential message, in [16], the matrix characterization of the secrecy capacity of the enhanced channel was obtained via the worst noise result of Diggavi and Cover [19]. With both common and confidential messages, characterizing the secrecy capacity region of the enhanced channel becomes more involved. In our proof, we resort to an extremal entropy inequality which was

first proved by Weingarten et al. [20] for characterizing the capacity region of a degraded *compound* MIMO Gaussian broadcast channel.

The details of the proof are provided in the next two sections.

## C. Aligned MIMO Gaussian Broadcast Channel

In this section, we prove Theorem 1 for the special case where the channel matrices $\mathbf{H}_1$ and $\mathbf{H}_2$ are square and invertible. In this case, multiplying both sides of (2.1) by $\mathbf{H}_k^{-1}$, the channel model can be equivalently written as

$$\mathbf{Y}_k[m] = \mathbf{X}[m] + \mathbf{Z}_k[m], \qquad k = 1, 2 \tag{2.10}$$

where $\{\mathbf{Z}_k[m]\}_m$ is an i.i.d. additive vector Gaussian noise process with zero mean and covariance matrix

$$\mathbf{N}_k = \mathbf{H}_k^{-1}\mathbf{H}_k^{-\mathrm{T}}.$$

Following [18], we will term the channel model (2.10) as the *aligned* MIMO Gaussian broadcast channel (see Figure 3(b)) and (2.1) as the *general* MIMO Gaussian broadcast channel. The main result of this section is summarized in the following theorem.

**Theorem 4.** *The secrecy capacity region* $\mathcal{C}_s(\mathbf{N}_1, \mathbf{N}_2, \mathbf{S})$ *of the aligned MIMO Gaussian broadcast channel* (2.10) *with messages* $W_0$ *(intended for both receivers 1 and 2) and* $W_1$ *(intended for receiver 1 but needing to be kept asymptotically perfectly secret from receiver 2) under the matrix power constraint* (2.6) *is given by the set of all nonnegative rate pairs* $(R_0, R_1)$ *satisfying*

$$\begin{aligned} R_0 &\leq \min\left(\tfrac{1}{2}\log\left|\tfrac{\mathbf{S}+\mathbf{N}_1}{\mathbf{B}+\mathbf{N}_1}\right|, \tfrac{1}{2}\log\left|\tfrac{\mathbf{S}+\mathbf{N}_2}{\mathbf{B}+\mathbf{N}_2}\right|\right) \\ R_1 &\leq \tfrac{1}{2}\log\left|\tfrac{\mathbf{B}+\mathbf{N}_1}{\mathbf{N}_1}\right| - \tfrac{1}{2}\log\left|\tfrac{\mathbf{B}+\mathbf{N}_2}{\mathbf{N}_2}\right| \end{aligned} \tag{2.11}$$

*for some* $0 \preceq \mathbf{B} \preceq \mathbf{S}$.

*Proof.* Let $G$ be a $t$-dimensional Gaussian vector with zero mean and covariance matrix $\mathbf{B}$. Then, the achievability of (2.11) can be obtained from the Csiszár-Körner region (2.4) by letting $U$ be a $t$-dimensional Gaussian vector with zero mean and covariance matrix $\mathbf{S} - \mathbf{B}$ and $V = \mathbf{X} = U + G$, where $U$ and $G$ are assumed to be independent. We therefore concentrate on proving the converse result.

To show that any achievable secrecy rate pair $(R_0, R_1)$ for the aligned MIMO Gaussian broadcast channel (2.10) must satisfy (2.11) for some $0 \preceq \mathbf{B} \preceq \mathbf{S}$, we may assume, without loss of generality, that the matrix power constraint $\mathbf{S} \succ 0$. For the case where $\mathbf{S} \succeq 0$ but $|\mathbf{S}| = 0$, let $\theta = \mathsf{Rank}(\mathbf{S}) < t$. We can define an *equivalent* aligned MIMO Gaussian broadcast channel with $\theta$ transmit and receive antennas and a new covariance matrix power constraint that is strictly positive definite. Hence, we can convert the case where $\mathbf{S} \succeq 0$, $|\mathbf{S}| = 0$ to the case where $\mathbf{S} \succ 0$ with the same secrecy capacity region. See [18, Lemma 2] for a formal presentation of this argument.

For the case where $\mathbf{S} \succ 0$, we shall consider proof by contradiction as follows. Assume that $(R_0^o, R_1^o)$ is an achievable secrecy rate pair for the aligned MIMO Gaussian broadcast channel (2.10) that lies *outside* the rate region (2.11). Since $(R_0^o, R_1^o)$ is achievable, $R_0^o$ can be bounded from above as

$$R_0^o \leq \min\left(\frac{1}{2}\log\left|\frac{\mathbf{S}+\mathbf{N}_1}{\mathbf{N}_1}\right|, \frac{1}{2}\log\left|\frac{\mathbf{S}+\mathbf{N}_2}{\mathbf{N}_2}\right|\right) = R_0^{max}. \tag{2.12}$$

Moreover, if $R_1^o = 0$, then $R_0^{max}$ can be achieved by letting $\mathbf{B} = 0$ in (2.11). Therefore,

we can write $R_1^o = R_1^* + \delta$ for some $\delta > 0$, where $R_1^*$ is given by

$$\begin{array}{rl} \max_{\mathbf{B}} & \frac{1}{2}\log\left|\frac{\mathbf{B}+\mathbf{N}_1}{\mathbf{N}_1}\right| - \frac{1}{2}\log\left|\frac{\mathbf{B}+\mathbf{N}_2}{\mathbf{N}_2}\right| \\ \text{subject to} & \frac{1}{2}\log\left|\frac{\mathbf{S}+\mathbf{N}_1}{\mathbf{B}+\mathbf{N}_1}\right| \geq R_0^o \\ & \frac{1}{2}\log\left|\frac{\mathbf{S}+\mathbf{N}_2}{\mathbf{B}+\mathbf{N}_2}\right| \geq R_0^o \\ & 0 \preceq \mathbf{B} \preceq \mathbf{S}. \end{array} \tag{2.13}$$

The above optimization program can be rewritten in the following standard form:

$$\begin{array}{rrcl} \min_{\mathbf{B}} & \frac{1}{2}\log\left|\frac{\mathbf{B}+\mathbf{N}_2}{\mathbf{N}_2}\right| - \frac{1}{2}\log\left|\frac{\mathbf{B}+\mathbf{N}_1}{\mathbf{N}_1}\right| & & \\ \text{subject to} & R_0^o - \frac{1}{2}\log\left|\frac{\mathbf{S}+\mathbf{N}_1}{\mathbf{B}+\mathbf{N}_1}\right| & \leq & 0 \\ & R_0^o - \frac{1}{2}\log\left|\frac{\mathbf{S}+\mathbf{N}_2}{\mathbf{B}+\mathbf{N}_2}\right| & \leq & 0 \\ & -\mathbf{B} & \preceq & 0 \\ & \mathbf{B}-\mathbf{S} & \preceq & 0 \end{array} \tag{2.14}$$

which has one semidefinite variable, $\mathbf{B}$, constrained by both scalar and semidefinite inequalities. This is in fact an optimization problem with generalized constraints in the form of semidefinite inequalities [21, p. 267]. Therefore, the Karush-Kuhn-Tucker (KKT) condition states that the derivative of the Lagrangian

$$\begin{array}{rcl} \mathcal{L} & = & \left(\frac{1}{2}\log\left|\frac{\mathbf{B}+\mathbf{N}_2}{\mathbf{N}_2}\right| - \frac{1}{2}\log\left|\frac{\mathbf{B}+\mathbf{N}_1}{\mathbf{N}_1}\right|\right) + \sum_{k=1}^{2}\mu_k\left(R_0^o - \frac{1}{2}\log\left|\frac{\mathbf{S}+\mathbf{N}_k}{\mathbf{B}+\mathbf{N}_k}\right|\right) \\ & & +\mathrm{Tr}\left((-\mathbf{B})\mathbf{M}_1\right) + \mathrm{Tr}\left((\mathbf{B}-\mathbf{S})\mathbf{M}_2\right) \end{array} \tag{2.15}$$

must vanish at an optimal solution $\mathbf{B}^*$.[1] Here, $\mathbf{M}_k$, $k = 1, 2$, are positive semidefinite

[1] As this optimization problem is not necessarily convex, a set of constraint qualifications (CQs) should be verified to make sure that the KKT conditions indeed hold. The CQs stated in [18, Appendix D] hold in a trivial manner for this optimization program.

matrices such that

$$\mathbf{B}^*\mathbf{M}_1 = 0 \tag{2.16}$$

$$(\mathbf{S}-\mathbf{B}^*)\mathbf{M}_2 = 0 \tag{2.17}$$

and $\mu_k \geq 0$, $k=1,2$, with equality if

$$\frac{1}{2}\log\left|\frac{\mathbf{S}+\mathbf{N}_k}{\mathbf{B}^*+\mathbf{N}_k}\right| > R_0^o.$$

We immediately have

$$\mu_k R_0^o = \frac{\mu_k}{2}\log\left|\frac{\mathbf{S}+\mathbf{N}_k}{\mathbf{B}^*+\mathbf{N}_k}\right|, \quad k=1,2. \tag{2.18}$$

Taking derivative of the Lagrangian in (2.15) over $\mathbf{B}$, the KKT condition can be written as

$$\nabla_{\mathbf{B}}\left(\frac{1}{2}\log\left|\frac{\mathbf{B}+\mathbf{N}_2}{\mathbf{N}_2}\right| - \frac{1}{2}\log\left|\frac{\mathbf{B}+\mathbf{N}_1}{\mathbf{N}_1}\right| + \sum_{k=1}^{2}\mu_k\left(R_0^o - \frac{1}{2}\log\left|\frac{\mathbf{S}+\mathbf{N}_k}{\mathbf{B}+\mathbf{N}_k}\right|\right)\right)$$
$$-\mathbf{M}_1+\mathbf{M}_2 = 0$$

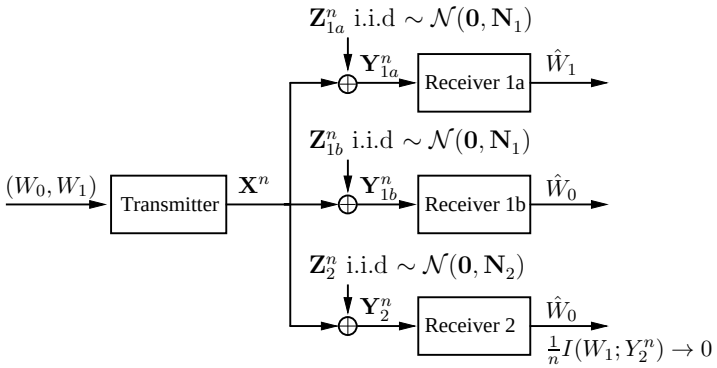
which gives

$$\frac{1}{2}(\mathbf{B}^*+\mathbf{N}_1)^{-1}+\mathbf{M}_1 = \frac{\mu_1}{2}(\mathbf{B}^*+\mathbf{N}_1)^{-1} + \frac{\mu_2+1}{2}(\mathbf{B}^*+\mathbf{N}_2)^{-1}+\mathbf{M}_2. \tag{2.19}$$

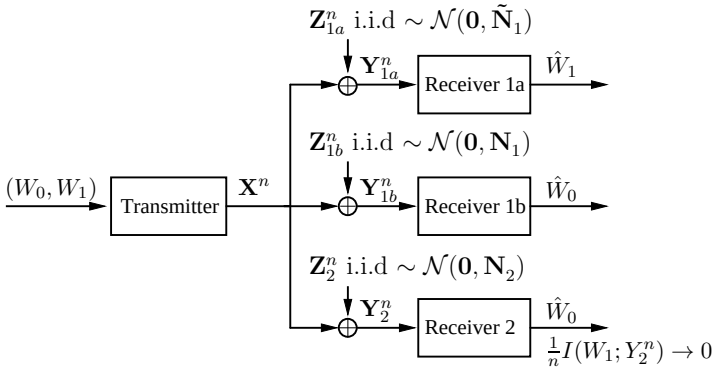
By (2.13) and (2.18), we have

$$\begin{aligned} R_1^o + (\mu_1+\mu_2)R_0^o &= \frac{1}{2}\log\left|\frac{\mathbf{B}^*+\mathbf{N}_1}{\mathbf{N}_1}\right| - \frac{1}{2}\log\left|\frac{\mathbf{B}^*+\mathbf{N}_2}{\mathbf{N}_2}\right| \\ &\quad + \sum_{k=1}^{2}\left(\frac{\mu_k}{2}\log\left|\frac{\mathbf{S}+\mathbf{N}_k}{\mathbf{B}^*+\mathbf{N}_k}\right|\right) + \delta. \end{aligned} \tag{2.20}$$

Next, we shall find a contradiction to (2.20) by showing that for *any* achievable




(a) An equivalent view of the aligned MIMO Gaussian broadcast channel shown in Figure 3(b)




(b) The enhanced channel

Fig. 4. Enhanced MIMO Gaussian broadcast channel with common and confidential messages.

secrecy rate pair $(R_0, R_1)$,

$$R_1 + (\mu_1 + \mu_2) R_0 \leq \frac{1}{2} \log \left| \frac{\mathbf{B}^* + \mathbf{N}_1}{\mathbf{N}_1} \right| - \frac{1}{2} \log \left| \frac{\mathbf{B}^* + \mathbf{N}_2}{\mathbf{N}_2} \right| + \sum_{k=1}^{2} \left( \frac{\mu_k}{2} \log \left| \frac{\mathbf{S} + \mathbf{N}_k}{\mathbf{B}^* + \mathbf{N}_k} \right| \right).$$

We divide our proof into three steps.

**Step 1: Split receiver 1 into two virtual receivers.**

Consider the following aligned MIMO Gaussian broadcast channel with three

receivers:

$$\begin{aligned} \mathbf{Y}_{1a}[m] &= \mathbf{X}[m] + \mathbf{Z}_{1a}[m] \\ \mathbf{Y}_{1b}[m] &= \mathbf{X}[m] + \mathbf{Z}_{1b}[m] \\ \mathbf{Y}_{2}[m] &= \mathbf{X}[m] + \mathbf{Z}_{2}[m] \end{aligned} \tag{2.21}$$

where $\{\mathbf{Z}_{1a}[m]\}_m$, $\{\mathbf{Z}_{1b}[m]\}_m$ and $\{\mathbf{Z}_{2}[m]\}_m$ are i.i.d. additive vector Gaussian noise processes with zero means and covariance matrices $\mathbf{N}_1$, $\mathbf{N}_1$ and $\mathbf{N}_2$, respectively. Suppose that the transmitter has two independent messages $W_0$ and $W_1$, where $W_0$ is intended for both receivers 1b and 2 and $W_1$ is intended for receiver 1a but needs to be kept secret from receiver 2. The confidentiality of message $W_1$ at receiver 2 is measured using the information-theoretic criterion (2.3). See Figure 4(a) for an illustration of this communication scenario.

Note that both receivers 1a and 1b in the aligned MIMO Gaussian broadcast channel (2.21) have the same noise covariance matrices as receiver 1 in the aligned MIMO Gaussian broadcast channel (2.10), and receiver 2 in the aligned MIMO Gaussian broadcast channel (2.21) has the same noise covariance matrix as receiver 2 in the aligned MIMO Gaussian broadcast channel (2.10). Therefore, any achievable secrecy rate pair $(R_0, R_1)$ for the aligned MIMO Gaussian broadcast channel (2.21) can also be achieved by the *same* coding scheme for the aligned MIMO Gaussian broadcast channel (2.10), and vice versa. Thus, the aligned MIMO Gaussian broadcast channel (2.21) has the *same* secrecy capacity region as the aligned MIMO Gaussian broadcast channel in (2.10) under the same power constraints.

**Step 2: Construct an enhanced channel.**

Let $\tilde{\mathbf{N}}_1$ be a real symmetric matrix satisfying

$$\frac{1}{2}(\mathbf{B}^* + \tilde{\mathbf{N}}_1)^{-1} = \frac{1}{2}(\mathbf{B}^* + \mathbf{N}_1)^{-1} + \mathbf{M}_1. \tag{2.22}$$

Following [18, Lemma 11], we have

$$0 \prec \tilde{\mathbf{N}}_1 \preceq \mathbf{N}_1 \tag{2.23}$$

and

$$\left|\frac{\mathbf{B}^* + \tilde{\mathbf{N}}_1}{\tilde{\mathbf{N}}_1}\right| = \left|\frac{\mathbf{B}^* + \mathbf{N}_1}{\mathbf{N}_1}\right|. \tag{2.24}$$

Moreover, substitute (2.22) into (2.19) and we have

$$\frac{1}{2}(\mathbf{B}^* + \tilde{\mathbf{N}}_1)^{-1} = \frac{\mu_1}{2}(\mathbf{B}^* + \mathbf{N}_1)^{-1} + \frac{\mu_2 + 1}{2}(\mathbf{B}^* + \mathbf{N}_2)^{-1} + \mathbf{M}_2. \tag{2.25}$$

Note that $(\mathbf{B}^* + \mathbf{N}_1)^{-1}$, $(\mathbf{B}^* + \mathbf{N}_2)^{-1}$ and $\mathbf{M}_2$ are all positive semidefinite so we have

$$\frac{1}{2}(\mathbf{B}^* + \tilde{\mathbf{N}}_1)^{-1} \succeq \frac{1}{2}(\mathbf{B}^* + \mathbf{N}_2)^{-1}$$

and hence

$$\tilde{\mathbf{N}}_1 \preceq \mathbf{N}_2. \tag{2.26}$$

Now consider the following enhanced MIMO Gaussian broadcast channel (see Figure 4(b)):

$$\begin{aligned} \tilde{\mathbf{Y}}_{1a}[m] &= \mathbf{X}[m] + \tilde{\mathbf{Z}}_{1a}[m] \\ \mathbf{Y}_{1b}[m] &= \mathbf{X}[m] + \mathbf{Z}_{1b}[m] \\ \mathbf{Y}_2[m] &= \mathbf{X}[m] + \mathbf{Z}_2[m] \end{aligned} \tag{2.27}$$

where $\{\tilde{\mathbf{Z}}_{1a}[m]\}_m$, $\{\mathbf{Z}_{1b}[m]\}_m$ and $\{\mathbf{Z}_2[m]\}_m$ are i.i.d. additive vector Gaussian noise processes with zero mean and covariance matrix $\tilde{\mathbf{N}}_1$, $\mathbf{N}_1$ and $\mathbf{N}_2$, respectively. Note from (2.23) that $\tilde{\mathbf{N}}_1 \preceq \mathbf{N}_1$. We conclude that the secrecy capacity region of the enhanced MIMO Gaussian broadcast channel (2.27) is at least as large as the secrecy capacity region of the aligned MIMO Gaussian broadcast channel (2.21) under the same power constraints.

**Step 3: Bound from above the weighted secrecy sum-capacity of the**

**enhanced channel.**

Note from (2.23) and (2.26) that

$$0 \prec \tilde{\mathbf{N}}_1 \preceq \{\mathbf{N}_1, \mathbf{N}_2\}. \tag{2.28}$$

Thus, in the enhanced MIMO Gaussian broadcast channel (2.27), the received signals $\mathbf{Y}_{1b}[m]$ and $\mathbf{Y}_2[m]$ are (stochastically) degraded with respect to the received signal $\mathbf{Y}_{1a}[m]$. In the following proposition, we shall consider the discrete memoryless case of the enhanced channel (2.27) and provide a single-letter characterization of the secrecy capacity region.

**Proposition 1.** *Consider a discrete memoryless broadcast channel with transition probability $p(\tilde{y}_{1a}, y_{1b}, y_2|x)$ and messages $W_0$ (intended for both receivers 1b and 2) and $W_1$ (intended for receiver 1a but needs to be kept confidential from receiver 2). If both*

$$X \to \tilde{Y}_{1a} \to Y_{1b} \quad \textit{and} \quad X \to \tilde{Y}_{1a} \to Y_2$$

*form Markov chains in their respective order, then the secrecy capacity region of this channel is given by the set of nonnegative rate pairs $(R_0, R_1)$ satisfying*

$$\begin{aligned} R_0 &\leq \min\left[I(U;Y_{1b}), I(U;Y_2)\right] \\ R_1 &\leq I(X;\tilde{Y}_{1a}|U) - I(X;Y_2|U) \end{aligned} \tag{2.29}$$

*for some $p(u, x, \tilde{y}_{1a}, y_{1b}, y_2) = p(u)p(x|u)p(\tilde{y}_{1a}, y_{1b}, y_2|x)$.*

*Proof.* The achievability of (2.29) follows from a coding scheme that combines superposition coding [22] and random binning [3]. The converse proof follows from the steps similar to those in the converse proof in [4]. The details of the converse proof are provided in Appendix A. □

**Remark 1.** *Prefix coding is no longer needed due to the preexisting Markov relation*

$X \to \tilde{Y}_{1a} \to Y_2$.

Next, to evaluate the single-letter expression (2.29) for the enhanced MIMO Gaussian broadcast channel (2.27), we shall recall an extremal entropy inequality which is a special case of [20, Corollary 4].

**Proposition 2** ([20]). *Let $\tilde{\mathbf{Z}}_{1a}$, $\mathbf{Z}_{1b}$ and $\mathbf{Z}_2$ be $t$-dimensional Gaussian vectors with zero means and covariance matrices $\tilde{\mathbf{N}}_1$, $\mathbf{N}_1$ and $\mathbf{N}_2$, respectively. Assume that $\tilde{\mathbf{N}}_1$, $\mathbf{N}_1$ and $\mathbf{N}_2$ are ordered as in* (2.28). *Let $\mathbf{S}$ be a $t \times t$ positive definite matrix. If there exists a $t \times t$ real symmetric matrix $\mathbf{B}^*$ such that $0 \preceq \mathbf{B}^* \preceq \mathbf{S}$ and satisfying*

$$\begin{aligned} \tfrac{1}{2}(\mathbf{B}^* + \tilde{\mathbf{N}}_1)^{-1} &= \tfrac{\mu\lambda}{2}(\mathbf{B}^* + \mathbf{N}_1)^{-1} + \tfrac{\mu(1-\lambda)}{2}(\mathbf{B}^* + \mathbf{N}_2)^{-1} + \mathbf{M}_2 \\ (\mathbf{S} - \mathbf{B}^*)\mathbf{M}_2 &= 0 \end{aligned}$$

*for some positive semidefinite matrix $\mathbf{M}_2$ and real scalars $\mu \geq 0$ and $0 \leq \lambda \leq 1$, then*

$$\begin{aligned} h(\mathbf{X}+\tilde{\mathbf{Z}}_{1a}|U) - \mu\lambda h(\mathbf{X} + \mathbf{Z}_{1b}|U) - \mu(1-\lambda)h(\mathbf{X} + \mathbf{Z}_2|U) \\ \leq \frac{1}{2}\log|2\pi e(\mathbf{B}^* + \tilde{\mathbf{N}}_1)| - \frac{\mu\lambda}{2}\log|2\pi e(\mathbf{B}^* + \mathbf{N}_1)| \\ - \frac{\mu(1-\lambda)}{2}\log|2\pi e(\mathbf{B}^* + \mathbf{N}_2)| \end{aligned}$$

*for any $(\mathbf{X}, U)$ independent of $(\tilde{\mathbf{Z}}_{1a}, \mathbf{Z}_{1b}, \mathbf{Z}_2)$ such that $E[\mathbf{X}\mathbf{X}^{\mathrm{T}}] \preceq \mathbf{S}$.*

We are now ready to bound from above the weighted secrecy sum-capacity of the enhanced channel (2.27). By Proposition 1, for any achievable secrecy rate pair

$(R_0, R_1)$ for the enhanced channel (2.27) we have

$$\begin{aligned}
&R_1 + (\mu_1+\mu_2)R_0 \\
&\quad \le I(\mathbf{X};\tilde{\mathbf{Y}}_{1a}|U) - I(\mathbf{X};\mathbf{Y}_2|U) + (\mu_1+\mu_2)\min\left[I(U;\mathbf{Y}_{1b}), I(U;\mathbf{Y}_2)\right] \\
&\quad \le I(\mathbf{X};\tilde{\mathbf{Y}}_{1a}|U) - I(\mathbf{X};\mathbf{Y}_2|U) + \left[\mu_1 I(U;\mathbf{Y}_{1b}) + \mu_2 I(U;\mathbf{Y}_2)\right] \\
&\quad = h(\mathbf{Z}_2) - h(\tilde{\mathbf{Z}}_{1a}) + \mu_1 h(\mathbf{X}+\mathbf{Z}_{1b}) + \mu_2 h(\mathbf{X}+\mathbf{Z}_2) \\
&\qquad\quad + \left[h(\mathbf{X}+\tilde{\mathbf{Z}}_{1a}|U) - \mu_1 h(\mathbf{X}+\mathbf{Z}_{1b}|U) - (\mu_2+1)h(\mathbf{X}+\mathbf{Z}_2|U)\right] \\
&\quad \le \frac{1}{2}\log\left|2\pi e\mathbf{N}_2\right| - \frac{1}{2}\log\left|2\pi e\tilde{\mathbf{N}}_1\right| + \sum_{k=1}^{2}\left[\frac{\mu_k}{2}\log\left|2\pi e(\mathbf{S}+\mathbf{N}_k)\right|\right] \\
&\qquad\quad + \left[h(\mathbf{X}+\tilde{\mathbf{Z}}_{1a}|U) - \mu_1 h(\mathbf{X}+\mathbf{Z}_{1b}|U) - (\mu_2+1)h(\mathbf{X}+\mathbf{Z}_2|U)\right] \qquad (2.30)
\end{aligned}$$

where the last inequality follows from the facts that

$$\begin{aligned}
h(\tilde{\mathbf{Z}}_{1a}) &= \frac{1}{2}\log\left|2\pi e\tilde{\mathbf{N}}_1\right|, \\
h(\mathbf{Z}_2) &= \frac{1}{2}\log\left|2\pi e\mathbf{N}_2\right|, \\
h(\mathbf{X}+\mathbf{Z}_{1b}) &\le \frac{1}{2}\log\left|2\pi e(\mathbf{S}+\mathbf{N}_1)\right|,
\end{aligned}$$

and

$$h(\mathbf{X}+\mathbf{Z}_2) \le \frac{1}{2}\log\left|2\pi e(\mathbf{S}+\mathbf{N}_2)\right|.$$

Let $\mu = \mu_1+\mu_2+1$ and $\lambda = \mu_1/(\mu_1+\mu_2+1)$. We obtain from (2.25) (and Proposition 2)

$$\begin{aligned}
&h(\mathbf{X}+\tilde{\mathbf{Z}}_{1a}|U) - \mu_1 h(\mathbf{X}+\mathbf{Z}_{1b}|U) - (\mu_2+1)h(\mathbf{X}+\mathbf{Z}_2|U) \\
&\quad \le \frac{1}{2}\log\left|2\pi e(\mathbf{B}^*+\tilde{\mathbf{N}}_1)\right| - \frac{\mu_1}{2}\log\left|2\pi e(\mathbf{B}^*+\mathbf{N}_1)\right| \\
&\qquad - \frac{\mu_2+1}{2}\log\left|2\pi e(\mathbf{B}^*+\mathbf{N}_2)\right|. \qquad (2.31)
\end{aligned}$$

Substituting (2.31) into (2.30), we have

$$\begin{aligned}
&R_1 + (\mu_1+\mu_2)R_0 \\
&\quad\le \frac{1}{2}\log|2\pi e\mathbf{N}_2| - \frac{1}{2}\log\left|2\pi e\tilde{\mathbf{N}}_1\right| + \sum_{k=1}^{2}\left[\frac{\mu_k}{2}\log|2\pi e(\mathbf{S}+\mathbf{N}_k)|\right] \\
&\qquad\quad + \left[\frac{1}{2}\log\left|2\pi e(\mathbf{B}^*+\tilde{\mathbf{N}}_1)\right| - \frac{\mu_1}{2}\log|2\pi e(\mathbf{B}^*+\mathbf{N}_1)|\right. \\
&\qquad\quad \left. -\frac{\mu_2+1}{2}\log|2\pi e(\mathbf{B}^*+\mathbf{N}_2)|\right] \\
&\quad= \frac{1}{2}\log\left|\frac{\mathbf{B}^*+\tilde{\mathbf{N}}_1}{\tilde{\mathbf{N}}_1}\right| - \frac{1}{2}\log\left|\frac{\mathbf{B}^*+\mathbf{N}_2}{\mathbf{N}_2}\right| + \sum_{k=1}^{2}\left[\frac{\mu_k}{2}\log\left|\frac{\mathbf{S}+\mathbf{N}_k}{\mathbf{B}^*+\mathbf{N}_k}\right|\right] \\
&\quad= \frac{1}{2}\log\left|\frac{\mathbf{B}^*+\mathbf{N}_1}{\mathbf{N}_1}\right| - \frac{1}{2}\log\left|\frac{\mathbf{B}^*+\mathbf{N}_2}{\mathbf{N}_2}\right| + \sum_{k=1}^{2}\left[\frac{\mu_k}{2}\log\left|\frac{\mathbf{S}+\mathbf{N}_k}{\mathbf{B}^*+\mathbf{N}_k}\right|\right] \qquad (2.32)
\end{aligned}$$

for any achievable secrecy rate pair $(R_0, R_1)$ for the enhanced MIMO Gaussian broadcast channel (2.27). Here, the last equality follows from (2.24).

Finally, combining Steps 1 and 2, we conclude that any achievable secrecy rate pair for the original aligned MIMO Gaussian broadcast channel (2.10) is also achievable for the enhanced MIMO Gaussian broadcast channel (2.27). Thus, (2.32) holds for any achievable secrecy rate pair $(R_0, R_1)$ for the original aligned MIMO Gaussian broadcast channel (2.10). Since $\delta > 0$, this contradicts (2.20). Therefore, any achievable secrecy rate pair $(R_0, R_1)$ for the aligned MIMO Gaussian broadcast channel (2.10) must satisfy (2.11) for some $0 \preceq \mathbf{B} \preceq \mathbf{S}$. This is the desired converse result, which completes the proof of the theorem. □

## D. General MIMO Gaussian Broadcast Channel

In this section, we Theorem 1 by extending the secrecy capacity result of Theorem 4 on the aligned MIMO Gaussian broadcast channel to the general MIMO broadcast channel. As mentioned in Section A, the achievability of the rate region (2.7) can

be obtained from the Csiszár-Körner region (2.4) with proper choice of input and auxiliary variables $(U, V, \mathbf{X})$. We therefore concentrate on proving the converse part of the theorem. Also as mentioned previously, the case when both channel matrices $\mathbf{H}_1$ and $\mathbf{H}_2$ are square and invertible can be easily transformed into an aligned MIMO Gaussian broadcast channel and thus has been proved by Theorem 4. Our goal next is to *approximate* a general MIMO Gaussian broadcast channel with an aligned MIMO Gaussian broadcast channel.

Without loss of generality, we assume that the channel matrices $\mathbf{H}_1$ and $\mathbf{H}_2$ are square (but *not* necessarily invertible). If that is not the case, we can apply singular value decomposition (SVD) to show that there exists an equivalent channel that has $t \times t$ square channel matrices and the same secrecy capacity region as the original channel [18, Section V-B].

Using SVD, we can write the channel matrices as

$$\mathbf{H}_k = \mathbf{U}_k \mathbf{\Lambda}_k \mathbf{V}_k^{\mathrm{T}}, \quad k = 1, 2$$

where $\mathbf{U}_k$ and $\mathbf{V}_k$ are $t \times t$ unitary matrices, and $\mathbf{\Lambda}_k$ is diagonal. We now define a new MIMO Gaussian broadcast channel:

$$\overline{\mathbf{Y}}_k[m] = \overline{\mathbf{H}}_k \mathbf{X}[m] + \mathbf{Z}_k[m] \quad k = 1, 2 \tag{2.33}$$

where

$$\overline{\mathbf{H}}_k = \mathbf{U}_k(\mathbf{\Lambda}_k + \alpha \mathbf{I}_t)\mathbf{V}_k^{\mathrm{T}}$$

for some $\alpha > 0$. Note that the MIMO Gaussian broadcast channel (2.33) does have invertible channel matrices. By Theorem 4, the secrecy capacity, $C_s(\overline{\mathbf{H}}_1, \overline{\mathbf{H}}_2, \mathbf{S})$, under the matrix power constraint (2.6) is given by the set of all nonnegative rate pairs

$(R_0, R_1)$ satisfying

$$\begin{aligned} R_0 &\leq \min\left(\tfrac{1}{2}\log\left|\frac{\overline{\mathbf{H}}_1\mathbf{S}\overline{\mathbf{H}}_1^{\mathrm{T}}+\mathbf{I}_{r_1}}{\overline{\mathbf{H}}_1\mathbf{B}\overline{\mathbf{H}}_1^{\mathrm{T}}+\mathbf{I}_{r_1}}\right|, \tfrac{1}{2}\log\left|\frac{\overline{\mathbf{H}}_2\mathbf{S}\overline{\mathbf{H}}_2^{\mathrm{T}}+\mathbf{I}_{r_2}}{\overline{\mathbf{H}}_2\mathbf{B}\overline{\mathbf{H}}_2^{\mathrm{T}}+\mathbf{I}_{r_2}}\right|\right) \\ R_1 &\leq \tfrac{1}{2}\log\left|\overline{\mathbf{H}}_1\mathbf{B}\overline{\mathbf{H}}_1^{\mathrm{T}}+\mathbf{I}_{r_1}\right| - \tfrac{1}{2}\log\left|\overline{\mathbf{H}}_2\mathbf{B}\overline{\mathbf{H}}_2^{\mathrm{T}}+\mathbf{I}_{r_2}\right| \end{aligned}$$

for some $0 \preceq \mathbf{B} \preceq \mathbf{S}$.

Further note that we can write $\mathbf{H}_k = \mathbf{D}_k\overline{\mathbf{H}}_k$ where

$$\mathbf{D}_k = \mathbf{U}_k\mathbf{\Lambda}_k(\mathbf{\Lambda}_k + \alpha\mathbf{I}_t)^{-1}\mathbf{U}_k^{\mathrm{T}}.$$

Since $\mathbf{D}_k^2 \prec \mathbf{I}_t$, we have [20, Definition 1]

$$\mathbf{X} \to \overline{\mathbf{Y}}_k \to \mathbf{Y}_k \tag{2.34}$$

forms a Markov chain for $k = 1, 2$. Therefore, both receivers 1 and 2 receive a better signal in the new channel (2.33) than in the original channel (2.1). Note that receiver 2 also plays the role of an eavesdropper for the confidential message $W_1$. Therefore, unlike the private message problem considered in [18], enhancing both receivers in the channel does *not* necessarily lead to an increase in the secrecy capacity region. In the following, however, we show that

$$\mathcal{C}_s(\mathbf{H}_1, \mathbf{H}_2, \mathbf{S}) \subseteq \mathcal{C}_s(\overline{\mathbf{H}}_1, \overline{\mathbf{H}}_2, \mathbf{S}) + \mathcal{O}(\mathbf{H}_2, \overline{\mathbf{H}}_2, \mathbf{S}) \tag{2.35}$$

where

$$\mathcal{O}(\mathbf{H}_2, \overline{\mathbf{H}}_2, \mathbf{S}) := \left\{(0, R_1) : 0 \leq R_1 \leq \frac{1}{2}\log\left|\overline{\mathbf{H}}_2\mathbf{S}\overline{\mathbf{H}}_2^{\mathrm{T}}+\mathbf{I}_t\right| - \frac{1}{2}\log\left|\mathbf{H}_2\mathbf{S}\mathbf{H}_2^{\mathrm{T}}+\mathbf{I}_t\right|\right\}$$

Let $(R_0, R_1)$ be an achievable secrecy rate pair for the MIMO Gaussian broadcast channel (2.1). By the result of Csiszár and Körner [4], there exists a collection of input and auxiliary variables $(U, V, \mathbf{X})$ satisfying the Markov relation $U \to V \to \mathbf{X}$ such

that

$$\begin{aligned} R_0 &\leq \min\left[I(U;\mathbf{Y}_1), I(U;\mathbf{Y}_2)\right] \\ R_1 &\leq I(V;\mathbf{Y}_1|U) - I(V;\mathbf{Y}_2|U). \end{aligned}$$

Also by the result of Csiszár and Körner [4], the secrecy rate pair $(\overline{R}_0, \overline{R}_1)$ given by

$$\begin{aligned} \overline{R}_0 &= \min\left[I(U;\overline{\mathbf{Y}}_1), I(U;\overline{\mathbf{Y}}_2)\right] \\ \overline{R}_1 &= I(V;\overline{\mathbf{Y}}_1|U) - I(V;\overline{\mathbf{Y}}_2|U) \end{aligned}$$

is achievable for the MIMO Gaussian broadcast channel (2.33). By the Markov relation (2.34), we have

$$I(U;\mathbf{Y}_k) \leq I(U;\overline{\mathbf{Y}}_k),$$

$$I(V;\mathbf{Y}_k|U) \leq I(V;\overline{\mathbf{Y}}_k|U),$$

and

$$I(\mathbf{X};\mathbf{Y}_k|U,V) \leq I(\mathbf{X};\overline{\mathbf{Y}}_k|U,V)$$

for $k = 1, 2$. Hence, we have

$$R_0 - \overline{R}_0 \leq \min\left[I(U;\mathbf{Y}_1), I(U;\mathbf{Y}_2)\right] - \min\left[I(U;\overline{\mathbf{Y}}_1), I(U;\overline{\mathbf{Y}}_2)\right] \leq 0 \qquad (2.36)$$

and

$$\begin{aligned}
R_1 - \overline{R}_1 &\leq I(V;\mathbf{Y}_1|U) - I(V;\mathbf{Y}_2|U) - \big[I(V;\overline{\mathbf{Y}}_1|U) - I(V;\overline{\mathbf{Y}}_2|U)\big] \\
&= I(V;\overline{\mathbf{Y}}_2|U) - I(V;\mathbf{Y}_2|U) - \big[I(V;\overline{\mathbf{Y}}_1|U) - I(V;\mathbf{Y}_1|U)\big] \\
&\leq I(V;\overline{\mathbf{Y}}_2|U) - I(V;\mathbf{Y}_2|U) \\
&= I(U,V;\overline{\mathbf{Y}}_2) - I(U,V;\mathbf{Y}_2) - \big[I(U;\overline{\mathbf{Y}}_2) - I(U;\mathbf{Y}_2)\big] \\
&\leq I(U,V;\overline{\mathbf{Y}}_2) - I(U,V;\mathbf{Y}_2) \\
&= I(\mathbf{X};\overline{\mathbf{Y}}_2) - I(\mathbf{X};\mathbf{Y}_2) - \big[I(\mathbf{X};\overline{\mathbf{Y}}_2|U,V) - I(\mathbf{X};\mathbf{Y}_2|U,V)\big] \\
&\leq I(\mathbf{X};\overline{\mathbf{Y}}_2) - I(\mathbf{X};\mathbf{Y}_2) \\
&= I(\mathbf{X};\overline{\mathbf{Y}}_2|\mathbf{Y}_2) \qquad (2.37) \\
&\leq \max_{0\preceq\mathbf{B}\preceq\mathbf{S}} \left(\frac{1}{2}\log\left|\overline{\mathbf{H}}_2\mathbf{B}\overline{\mathbf{H}}_2^{\mathrm{T}} + \mathbf{I}_t\right| - \frac{1}{2}\log\left|\mathbf{H}_2\mathbf{B}\mathbf{H}_2^{\mathrm{T}} + \mathbf{I}_t\right|\right) \qquad (2.38) \\
&= \frac{1}{2}\log\left|\overline{\mathbf{H}}_2\mathbf{S}\overline{\mathbf{H}}_2^{\mathrm{T}} + \mathbf{I}_t\right| - \frac{1}{2}\log\left|\mathbf{H}_2\mathbf{S}\mathbf{H}_2^{\mathrm{T}} + \mathbf{I}_t\right| \qquad (2.39)
\end{aligned}$$

where (2.37) follows from the Markov relation (2.34), (2.38) follows from a well-known inequality due to Thomas [23, Lemma 1], and (2.39) follows from the fact that $\mathbf{H}_2^{\mathrm{T}}\mathbf{H}_2 \prec \overline{\mathbf{H}}_2^{\mathrm{T}}\overline{\mathbf{H}}_2$. Combining (2.36) and (2.39) established the set relationship (2.35).

Finally, let $\alpha \downarrow 0$ on both sides of (2.35). Note that $\overline{\mathbf{H}}_k \to \mathbf{H}_k$ for $k = 1, 2$, so $\mathcal{C}_s(\overline{\mathbf{H}}_1, \overline{\mathbf{H}}_2, \mathbf{S})$ converges to the rate region (2.7) and $\mathcal{O}(\mathbf{H}_2, \overline{\mathbf{H}}_2, \mathbf{S}) \to \{(0,0)\}$. We thus have proved the desired converse result and completed the proof of the theorem.

## E. Numerical Examples

In this section, we illustrate the results of Theorem 1 and Corollary 3 by numerical examples. Note that finding the boundaries of the secrecy capacity regions $\mathcal{C}_s(\mathbf{H}_1, \mathbf{H}_2, \mathbf{S})$ and $\mathcal{C}_s(\mathbf{H}_1, \mathbf{H}_2, P)$ as expressed in (2.7) and (2.9) involves solving *nonconvex* optimization programs and hence is nontrivial. Following the work in [25], we can rewrite the

expressions (2.7) and (2.9) such that the optimization program for finding the boundaries of $\mathcal{C}_s(\mathbf{H}_1, \mathbf{H}_2, \mathbf{S})$ and $\mathcal{C}_s(\mathbf{H}_1, \mathbf{H}_2, P)$ become tractable for the case where each of the receivers is equipped with only one receive antenna, i.e., $r_k = 1$ for $k = 1, 2$. As we limit the discussion in this section to the single receive antenna case, the channel matrices $\mathbf{H}_k$ become the $1 \times t$ channel vectors $\mathbf{h}_k$, $k = 1, 2$.

To compute the secrecy capacity region $\mathcal{C}_s(\mathbf{h}_1, \mathbf{h}_2, \mathbf{S})$, consider re-parameterizing $(R_0, R_1)$ using $(\alpha, \gamma_0)$ as

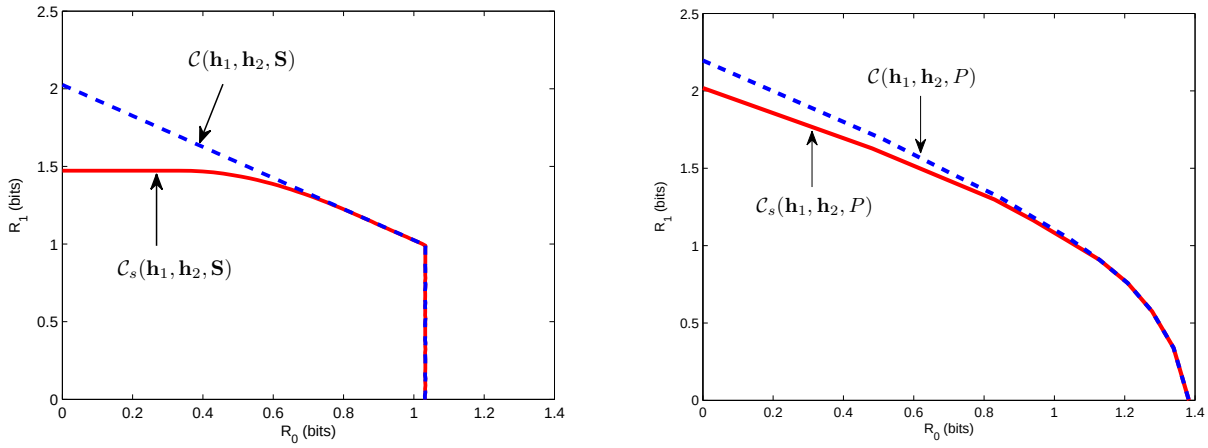
$$\begin{aligned} R_0 &= \tfrac{1}{2}\log(1 + \alpha\gamma_0) \\ R_1 &= \tfrac{1}{2}\log(1 + \alpha(1 - \gamma_0)). \end{aligned} \tag{2.40}$$

Thus, to see whether a particular secrecy rate pair $(R_0, R_1)$ is inside $\mathcal{C}_s(\mathbf{h}_1, \mathbf{h}_2, \mathbf{S})$ as expressed in (2.7), one may check, instead, whether there exists a positive semidefinite matrix $\mathbf{B}$ which satisfies the set of constraints:

$$\begin{aligned} \mathbf{h}_1(\mathbf{S} - \mathbf{B})\mathbf{h}_1^{\mathrm{T}} &\geq \alpha\gamma_0(\mathbf{h}_1\mathbf{B}\mathbf{h}_1^{\mathrm{T}} + 1) \\ \mathbf{h}_2(\mathbf{S} - \mathbf{B})\mathbf{h}_2^{\mathrm{T}} &\geq \alpha\gamma_0(\mathbf{h}_2\mathbf{B}\mathbf{h}_2^{\mathrm{T}} + 1) \\ \mathbf{h}_1\mathbf{B}\mathbf{h}_1^{\mathrm{T}} - \mathbf{h}_2\mathbf{B}\mathbf{h}_2^{\mathrm{T}} &\geq \alpha(1 - \gamma_0)(\mathbf{h}_2\mathbf{B}\mathbf{h}_2^{\mathrm{T}} + 1) \\ \mathbf{B} &\preceq \mathbf{S}. \end{aligned} \tag{2.41}$$

Note that all the constraints in (2.41) are linear in $\mathbf{B}$. Hence, whether there exists a feasible solution can be examined using standard semidefinite programming techniques (i.e., `CVX`, a package for specifying and solving convex programs [24]). Note from (2.40) that both $R_0$ and $R_1$ increase as $\alpha$ increases. Therefore, for a fixed $\gamma_0$, a boundary point of $\mathcal{C}_s(\mathbf{h}_1, \mathbf{h}_2, \mathbf{S})$ can be found by searching over the maximum $\alpha$ such that the set of constraints in (2.41) admits a feasible solution. Sweeping over $\gamma_0 \in [0, 1]$ gives all the boundary points of $\mathcal{C}_s(\mathbf{h}_1, \mathbf{h}_2, \mathbf{S})$.

Similarly, to compute the secrecy capacity region $\mathcal{C}_s(\mathbf{h}_1, \mathbf{h}_2, P)$, we consider the




(a) The matrix power constraint

(b) The average total power constraint

Fig. 5. An illustration of the secrecy capacity regions of the MIMO Gaussian broadcast channel with common and confidential messages.

set of constraints for a pair of positive semidefinite matrices $(\mathbf{B}_1, \mathbf{B}_2)$:

$$\begin{aligned} \mathbf{h}_1\mathbf{B}_2\mathbf{h}_1^{\mathrm{T}} &\geq \alpha\gamma_0(\mathbf{h}_1\mathbf{B}_1\mathbf{h}_1^{\mathrm{T}} + 1) \\ \mathbf{h}_2\mathbf{B}_2\mathbf{h}_2^{\mathrm{T}} &\geq \alpha\gamma_0(\mathbf{h}_2\mathbf{B}_1\mathbf{h}_2^{\mathrm{T}} + 1) \\ \mathbf{h}_1\mathbf{B}_1\mathbf{h}_1^{\mathrm{T}} - \mathbf{h}_2\mathbf{B}_1\mathbf{h}_2^{\mathrm{T}} &\geq \alpha(1-\gamma_0)(\mathbf{h}_2\mathbf{B}_1\mathbf{h}_2^{\mathrm{T}} + 1) \\ \mathrm{Tr}(\mathbf{B}_1 + \mathbf{B}_2) &\leq P. \end{aligned} \tag{2.42}$$

Again, all the constraints in (2.42) are linear in $(\mathbf{B}_1, \mathbf{B}_2)$ so whether there exists a feasible solution can be examined using standard semidefinite programming techniques [24]. Therefore, for a fixed $\gamma_0$, a boundary point of $\mathcal{C}_s(\mathbf{h}_1, \mathbf{h}_2, P)$ can be found by searching over the maximum $\alpha$ such that the set of constraints in (2.42) admits a feasible solution. Sweeping over $\gamma_0 \in [0, 1]$ gives all the boundary points of $\mathcal{C}_s(\mathbf{h}_1, \mathbf{h}_2, P)$.

Figure 5 plots the secrecy capacity regions $\mathcal{C}_s(\mathbf{h}_1, \mathbf{h}_2, \mathbf{S})$ and $\mathcal{C}_s(\mathbf{h}_1, \mathbf{h}_2, P)$ for the

channel vectors $\mathbf{h}_1 = [2 \;\; 0.4]$ and $\mathbf{h}_2 = [0.4 \;\; 1]$ and power constraints

$$\mathbf{S} = \begin{bmatrix} 3.3333 & 1.2346 \\ 1.2346 & 1.6667 \end{bmatrix}$$

and $P = \mathrm{Tr}(\mathbf{S}) = 5$. For comparison, in Figure 5, we have also plotted the capacity regions of the same MIMO Gaussian broadcast channel with a common message $W_0$ intended for both receiver 1 and 2 and a private message $W_1$ intended only for receiver 1 (but without any secrecy constraints). This problem is known as the MIMO Gaussian broadcast channel with degraded message sets [25, 26]. As shown in [25], the capacity region, $\mathcal{C}(\mathbf{h}_1, \mathbf{h}_2, \mathbf{S})$, under the matrix power constraint (2.6) is given by[2]

$$\mathcal{C}(\mathbf{h}_1, \mathbf{h}_2, \mathbf{S}) = \mathcal{R}_1(\mathbf{h}_1, \mathbf{S}) \cap \mathcal{R}_2(\mathbf{h}_1, \mathbf{h}_2, \mathbf{S})$$

where $\mathcal{R}_1(\mathbf{h}_1, \mathbf{S})$ is given by the nonnegative rate pairs $(R_0, R_1)$ satisfying

$$R_0 + R_1 \leq \frac{1}{2} \log(\mathbf{h}_1 \mathbf{S} \mathbf{h}_1^{\mathrm{T}} + 1),$$

and $\mathcal{R}_2(\mathbf{h}_1, \mathbf{h}_2, \mathbf{S})$ is given by the nonnegative rate pairs $(R_0, R_1)$ satisfying

$$\begin{aligned} R_0 &\leq \tfrac{1}{2} \log \left( \tfrac{\mathbf{h}_2 \mathbf{S} \mathbf{h}_2^{\mathrm{T}} + 1}{\mathbf{h}_2 \mathbf{B} \mathbf{h}_2^{\mathrm{T}} + 1} \right) \\ R_1 &\leq \tfrac{1}{2} \log(\mathbf{h}_1 \mathbf{B} \mathbf{h}_1^{\mathrm{T}} + 1) \end{aligned}$$

for some $0 \preceq \mathbf{B} \preceq \mathbf{S}$. Similarly, the capacity region, $\mathcal{C}(\mathbf{h}_1, \mathbf{h}_2, P)$, under the average total power constraint (2.2) is given by

$$\mathcal{C}(\mathbf{h}_1, \mathbf{h}_2, P) = \mathcal{R}_1(\mathbf{h}_1, P) \cap \mathcal{R}_2(\mathbf{h}_1, \mathbf{h}_2, P)$$

[2] As shown in [25], this result holds for the general MIMO Gaussian broadcast channel, not just for the single receive antenna case.

where $\mathcal{R}_1(\mathbf{h}_1, P)$ is given by the nonnegative rate pairs $(R_0, R_1)$ satisfying

$$R_0 + R_1 \leq \frac{1}{2}\log(P\|\mathbf{h}_1\|^2 + 1),$$

and $\mathcal{R}_2(\mathbf{h}_1, \mathbf{h}_2, P)$ is given by the nonnegative rate pairs $(R_0, R_1)$ satisfying

$$\begin{aligned} R_0 &\leq \tfrac{1}{2}\log\left(\tfrac{\mathbf{h}_2(\mathbf{B}_1+\mathbf{B}_2)\mathbf{h}_2^{\mathrm{T}}+1}{\mathbf{h}_2\mathbf{B}_1\mathbf{h}_2^{\mathrm{T}}+1}\right) \\ R_1 &\leq \tfrac{1}{2}\log(\mathbf{h}_1\mathbf{B}_1\mathbf{h}_1^{\mathrm{T}}+1) \end{aligned}$$

for some $\mathbf{B}_1 \succeq 0$, $\mathbf{B}_2 \succeq 0$ and $\mathrm{Tr}(\mathbf{B}_1 + \mathbf{B}_2) \leq P$. The boundaries of the rate regions $\mathcal{R}_2(\mathbf{h}_1, \mathbf{h}_2, \mathbf{S})$ and $\mathcal{R}_2(\mathbf{h}_1, \mathbf{h}_2, P)$ can be computed similarly to those of $\mathcal{C}_s(\mathbf{h}_1, \mathbf{h}_2, \mathbf{S})$ and $\mathcal{C}_s(\mathbf{h}_1, \mathbf{h}_2, P)$, respectively. As expected, for any given common rate $R_0$, the maximum secrecy rate is less than (or equal to) the maximum private rate due to the additional secrecy constraint at receiver 2.

## F. Concluding Remarks

This chapter considered the problem of the MIMO Gaussian broadcast channel with two receivers and two messages: a common message intended for both receivers, and a confidential message intended for one of the receivers but needing to be kept asymptotically perfectly secure from the other. A matrix characterization of the secrecy capacity region is established via a channel enhancement argument. The enhanced channel is constructed by first splitting the receiver that decodes both messages into two virtual receivers and then enhancing only the virtual receiver that decodes the confidential message. The secrecy capacity region of the enhanced channel is characterized using an extremal entropy inequality previously established for characterizing the capacity region of a degraded compound MIMO Gaussian broadcast channel.

After the initial submission of our paper [9], [27] and [28] considered the problem of the MIMO Gaussian broadcast channel with two receivers and three messages:

a common message intended for both receivers, and two confidential messages each intended for one of the receivers but needing to be kept asymptotically perfectly secure from the other. A matrix characterization of the secrecy capacity region was established, which generalized the main results of our paper. It is worth mentioning that the set of techniques developed/applied in our paper, more specifically receiver splitting and the extremal entropy inequality in Proposition 2, was also used in [27] and [28] in proving their converse results.

# CHAPTER III

# SECURITY EMBEDDING CODES*

## A. Introduction

A basic model of physical layer security, as discussed in Chapter I, is a broadcast channel [3, 4] with two receivers, a legitimate receiver and an eavesdropper. Both the legitimate receiver and the eavesdropper channels are assumed to be *known* at the transmitter. By exploring the statistical difference between the legitimate receiver and the eavesdropper channel, one may design coding schemes that can deliver a message reliably to the legitimate receiver while keeping it asymptotically perfectly secret from the eavesdropper.

While assuming the transmitter's knowledge of the legitimate receiver channel might be reasonable (particularly when a feedback link is available), assuming that the transmitter knows the eavesdropper channel is *unrealistic* in most scenarios. This is mainly because the eavesdropper is an *adversary*, which usually has no incentive to help the transmitter to acquire its channel state information. Hence, it is critical that physical layer security techniques are designed to withstand the *uncertainty* of the eavesdropper channel.

In this chapter, we consider a communication scenario where there are *multiple* possible realizations for the eavesdropper channel. Which realization will actually occur is *unknown* to the transmitter. *Our goal is to design coding schemes such that

the number of *secure* bits delivered to the legitimate receiver depends on the *actual* realization of the eavesdropper channel. More specifically, when the eavesdropper channel realization is weak, *all* bits delivered to the legitimate receiver need to be secure. In addition, when the eavesdropper channel realization is strong, a *prescribed part* of the bits needs to *remain* secure. We call such codes *security embedding codes*, referring to the fact that high-security bits are now embedded into the low-security ones. We envision that such codes are naturally useful for the secrecy communication scenarios where information bits are *not* created equal: some of them have more security priorities than the others and hence require stronger security protection during communication. For example, in real wireless communication systems, control plane signals have higher secrecy requirements than data plane transmissions, and signals that carry users' identities and cryptographic keys require stronger security protections than the other signals.

A key question that we consider is at what expense one may allow part of the bits to enjoy additional security protections. Note that a "naive" security embedding scheme is to design two separate secrecy codes to provide two different levels of security protections, and apply them to two separate parts of the information bits via *time sharing*. In this scheme, the high-security bits are protected using a stronger secrecy code and hence are communicated at a lower rate. The overall communication rate is a *convex* combination of the low-security bit rate and the high-security bit rate and hence is lower than the low-security bit rate. Another simple scheme for security embedding is *power sharing* [29], where the transmitted signal is given by the *superposition* of two secrecy codes separately designed to protect the low-security and high-security bits. Though generally better than the time-sharing scheme, the overall rate of communication for the power-sharing scheme is still lower than that when all bits delivered are lower-security ones.

The main result of this chapter is to show that it is possible to have a significant portion of the information bits enjoying additional security protections *without* sacrificing the overall rate of communication. This further justifies the name "security embedding," as now having part of the information bits enjoying additional security protections is only an added bonus. More specifically, in this chapter, we call a secrecy communication scenario *embeddable* if a *nonzero* fraction of the information bits can enjoy additional security protections without sacrificing the overall communication rate, and we call it *perfectly embeddable* if the high-security bits can be communicated at *full* rate (as if the low-security bits do not exist) without sacrificing the overall communication rate. The key to achieving efficient security embedding is to *jointly* encode the low-security and high-security bits (as opposed to separate encoding as in the time- and power-sharing schemes). In particular, the low-security bits can be used as (part of) the *transmitter randomness* to protect the high-security bits (when the eavesdropper channel realization is strong); this is the key feature of our proposed security embedding codes.

Our definition of security embedding and proposed coding schemes are mainly motivated by the special case where there are *no* secrecy constraints on the "low-security" bits. In this case, the problem of security embedding reduces to the problem of simultaneously communicating a private message and a confidential message, for which the secrecy capacity region was established in [30, p. 411] and [31]. Our main technical contribution in this chapter is to extend the setting of [30, p. 411] and [31] to the general case where both low-security and high-security bits are subject to (different) asymptotic perfect secrecy constraints.

The rest of the chapter is organized as follows. In Section B, an information-theoretic formulation of the security embedding problem is presented, which we term as the *two-level security wiretap channel*. A coding scheme that combines rate split-

ting, superposition coding, nested binning, and channel prefixing is proposed and is shown to achieve the secrecy capacity region of the channel in several scenarios. Based on the results of Section B, in Section C we study the engineering communication models with real channel input and additive white Gaussian noise, and show that both scalar and independent parallel Gaussian (under an individual per-subchannel average power constraint) two-level security wiretap channels are *perfectly embeddable*. In Section D, we extend the results of Section B to the *wiretap channel II* setting of Ozarow and Wyner [32], and show that two-level security wiretap channels II are also *perfectly embeddable*. Finally, in Section E, we conclude the chapter with some remarks.

## B. Two-Level Security Wiretap Channel

### 1. Channel Model

Consider a discrete memoryless broadcast channel with three receivers and transition probability $p(y, z_1, z_2|x)$. The receiver that receives the channel output $Y$ is a legitimate receiver. The receivers that receive the channel outputs $Z_1$ and $Z_2$ represent two possible realizations of an eavesdropper. Assume that the channel output $Z_2$ is *degraded* with respect to the channel output $Z_1$, i.e., $X \to Z_1 \to Z_2$ forms a Markov chain in that order, so $Z_1$ represents a stronger realization of the eavesdropper than $Z_2$.

The transmitter has two independent messages: a high-security message $M_1$ uniformly drawn from $\{1, \ldots, 2^{nR_1}\}$ and a low-security message $M_2$ uniformly drawn from $\{1, \ldots, 2^{nR_2}\}$ where $n$ is the block length, and $R_1$ and $R_2$ are the corresponding rates of communication. Both messages $M_1$ and $M_2$ are intended for the legitimate receiver, and need to be kept asymptotically perfectly secure when the eavesdropper

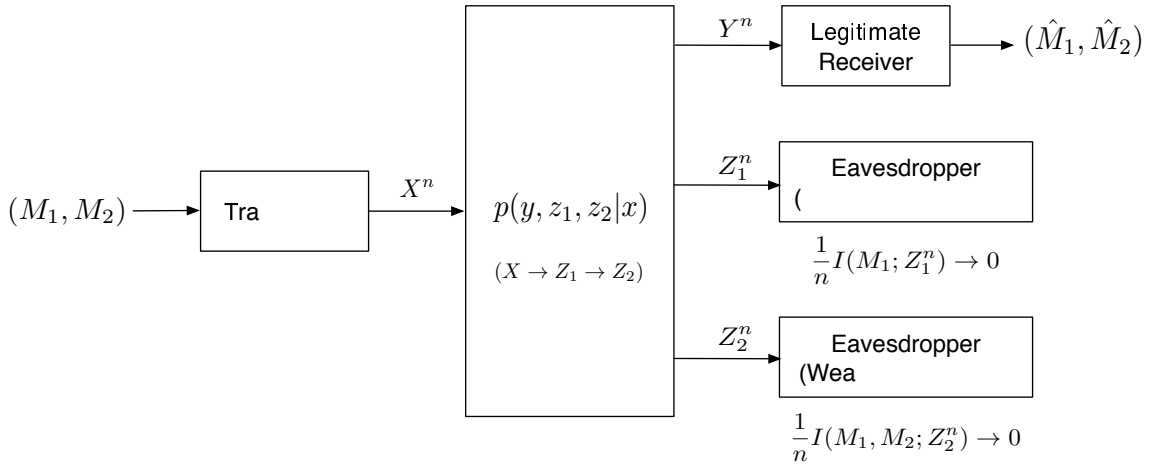



Fig. 6. Two-level security wiretap channel.

realization is weak, i.e.,

$$\frac{1}{n} I(M_1, M_2; Z_2^n) \to 0 \tag{3.1}$$

in the limit as $n \to \infty$. In addition, when the eavesdropper realization is strong, the high-security message $M_1$ needs to remain asymptotically perfectly secure, i.e.,

$$\frac{1}{n} I(M_1; Z_1^n) \to 0 \tag{3.2}$$

in the limit as $n \to \infty$. A rate pair $(R_1, R_2)$ is said to be *achievable* if there is a sequence of codes of rate pair $(R_1, R_2)$ such that both messages $M_1$ and $M_2$ can be reliably delivered to the legitimate receiver while satisfying the asymptotic perfect secrecy constraints (3.1) and (3.2). The collection of all possible achievable rate pairs is termed as the *secrecy capacity region* of the channel. Fig. 6 illustrates this communication scenario, which we term as *two-level security wiretap channel*.

The above setting of two-level security wiretap channel is closely related to the traditional wiretap channel setting of [3, 4]. More specifically, without the additional

secrecy constraint (3.2) on the high-security message $M_1$, we can simply view the messages $M_1$ and $M_2$ as a single (low-security) message $M$ with rate $R_1 + R_2$. In this case, the problem reduces to communicating the message $M$ over the traditional wiretap channel with transition probability $p(y, z_2|x) = \sum_{z_1} p(y, z_1, z_2|x)$, and the maximum achievable $R_1 + R_2$ is given by $C_s(P_{y,z_2|x})$. Similarly, without needing to communicate the low-security message $M_2$ (i.e., $R_2 = 0$), the basic secrecy constraint (3.1) reduces to $(1/n)I(M_1; Z_2^n) \to 0$, which is implied by the additional secrecy constraint (3.2) due to the assumption that $Z_2$ is degraded with respect to $Z_1$. In this case, the problem reduces to communicating the high-security message $M_1$ over the traditional wiretap channel with transition probability $p(y, z_1|x) = \sum_{z_2} p(y, z_1, z_2|x)$, and the maximum achievable $R_1$ is given by $C_s(P_{y,z_1|x})$. We thus have the following simple observation.

**Fact 1.** *A two-level security wiretap channel $p(y, z_1, z_2|x)$ where $Z_2$ is degraded with respect to $Z_1$ is* embeddable *if there exists a sequence of codes with rate pair $(R_1, R_2)$ such that $R_1 + R_2 = C_s(P_{y,z_2|x})$ and $R_1 > 0$, and it is* perfectly embeddable *if there exists a sequence of codes with rate pair $(R_1, R_2)$ such that $R_1 + R_2 = C_s(P_{y,z_2|x})$ and $R_1 = C_s(P_{y,z_1|x})$.*

An important special case of the two-level security wiretap channel problem considered here is when the channel output $Z_2$ is a *constant* signal. In this case, the secrecy constraint (3.1) becomes *obsolete*, and the low-security message $M_2$ becomes a *private* message without being subject to any secrecy constraints. The problem of simultaneously communicating a private message and a confidential message over a discrete memoryless wiretap channel was considered in [30, p. 411] and [31], where a single-letter characterization of the secrecy capacity region was established. For the *general* two-level security wiretap channel problem that we consider here, both

high-security message $M_1$ and the low-security message $M_2$ are subject to asymptotic perfect secrecy constraints, which makes the problem much more involved.

## 2. Main Results

The following theorem provides a *sufficient* condition for establishing the achievability of a rate pair for the discrete memoryless two-level security wiretap channel.

**Theorem 5.** *Consider a discrete memoryless two-level security wiretap channel with transition probability $p(y, z_1, z_2|x)$ where $Z_2$ is degraded with respect to $Z_1$. A nonnegative pair $(R_1, R_2)$ is an achievable rate pair of the channel if it satisfies*

$$\begin{aligned} R_1 &\leq I(V;Y|U) - I(V;Z_1|U) \\ \textit{and} \quad R_1 + R_2 &\leq I(V;Y|S) - I(V;Z_2|S) \end{aligned} \tag{3.3}$$

*for some joint distribution $p(s, u, v, x)$, where $S$, $U$ and $V$ are auxiliary random variables satisfying the Markov chain $S \to U \to V \to X \to (Y, Z_1, Z_2)$.*

A proof of the theorem is provided in Section 3. Note that to show that every rate pair that satisfies (3.3) is achievable, we only need to consider the case where $I(U;Y|S) \geq I(U;Z_2|S)$. This can be seen as follows. Assuming that $I(U;Y|S) \leq I(U;Z_2|S)$, we have

$$\begin{aligned} &I(V;Y|S) - I(V;Z_2|S) \\ &\quad = I(V;Y|U) - I(V;Z_2|U) + [I(U;Y|S) - I(U;Z_2|S)] \qquad (3.4) \\ &\quad \leq I(V;Y|U) - I(V;Z_2|U). \qquad (3.5) \end{aligned}$$

It follows that every rate pair that satisfies (3.3) must satisfy

$$\begin{aligned} R_1 &\leq I(V;Y|U) - I(V;Z_1|U) \\ \text{and} \quad R_1 + R_2 &\leq I(V;Y|U) - I(V;Z_2|U) \end{aligned} \tag{3.6}$$

which is a special case of (3.3) by setting $S = U$ so that $I(U;Y|S) = I(U;Z_2|S) = 0$.

To show that every rate pair that satisfies (3.3) for which $I(U;Y|S) \geq I(U;Z_2|S)$ is achievable, we shall consider a coding scheme that combines rate splitting, superposition coding, nested binning, and channel prefixing. In particular, (part of) the low-security message $M_2$ will be used as (part of) the transmitter randomness to protect the high-security message $M_1$ (when the eavesdropper channel realization is strong). See Section 3 for the details of the proof.

Combining Theorem 5 with Fact 1, we have the following sufficient conditions for establishing that a two-level security wiretap channel is (perfectly) embeddable. The conditions are stated in terms of the existence of a joint auxiliary-input distribution.

**Corollary 6.** *A two-level security wiretap channel $p(y, z_1, z_2|x)$ where $Z_2$ is degraded with respect to $Z_1$ is* embeddable *if there exists a joint distribution $p(s, u, v, x)$ satisfying the Markov chain $S \to U \to V \to X \to (Y, Z_1, Z_2)$ and such that*

$$\begin{aligned} I(V;Y|S) - I(V;Z_2|S) &= C_s(P_{y,z_2|x}) \\ \textit{and} \quad I(V;Y|U) - I(V;Z_1|U) &> 0 \end{aligned} \tag{3.7}$$

*and it is* perfectly embeddable *if there exists a joint distribution $p(s, u, v, x)$ satisfying the Markov chain $S \to U \to V \to X \to (Y, Z_1, Z_2)$ and such that*

$$\begin{aligned} I(V;Y|S) - I(V;Z_2|S) &= C_s(P_{y,z_2|x}) \\ \textit{and} \quad I(V;Y|U) - I(V;Z_1|U) &= C_s(P_{y,z_1|x}). \end{aligned} \tag{3.8}$$

Assume that $Y$ is *less noisy* than $Z_2$, i.e., $I(U;Y) \geq I(U;Z_2)$ for any random variable $U$ satisfying the Markov chain $U \to X \to (Y, Z_2)$. In this case, we have a *precise* characterization of the secrecy capacity region as summarized in the following theorem.

**Theorem 7.** *Consider a discrete memoryless two-level security wiretap channel with*

*transition probability* $p(y, z_1, z_2|x)$ *where* $Z_2$ *is degraded with respect to* $Z_1$ *and* $Y$ *is less noisy than* $Z_2$. *The secrecy capacity region of the channel is given by the set of all nonnegative pairs* $(R_1, R_2)$ *that satisfy*

$$\begin{aligned} R_1 &\leq I(V;Y|U) - I(V;Z_1|U) \\ \textit{and} \quad R_1 + R_2 &\leq I(V;Y) - I(V;Z_2) \end{aligned} \tag{3.9}$$

*for some joint distribution* $p(u, v, x)$, *where* $U$ *and* $V$ *are auxiliary random variables satisfying the Markov chain* $U \to V \to X \to (Y, Z_1, Z_2)$.

The forward part of the theorem follows directly from Theorem 5 by setting $S$ to be constant. The converse part of the theorem is proved in Appendix B, which mainly involves identifying a choice for the auxiliary random variables $U$ and $V$. Note that when the channel output $Z_2$ is constant, the conditions that $Z_2$ is degraded with respect to $Z_1$ and $Y$ is less noisy than $Z_2$ are trivially met by any channel outputs $(Y, Z_1)$. In this case, Theorem 7 recovers the results of [30, p. 411] and [31] on simultaneously communicating a private message and a confidential message over a discrete memoryless wiretap channel.

Assume, instead, that $Y$ is less noisy than $Z_1$. Given that $Z_2$ is degraded with respect to $Z_1$, this implies that $Y$ is also less noisy than $Z_2$. In this case, we have

$$\begin{aligned} &I(V;Y|U) - I(V;Z_1|U) \\ &\quad = I(V;Y) - I(V;Z_1) - [I(U;Y) - I(U;Z_1)] && (3.10) \\ &\quad \leq I(V;Y) - I(V;Z_1) && (3.11) \\ &\quad = I(X;Y) - I(X;Z_1) - [I(X;Y|V) - I(X;Z_1|V)] && (3.12) \\ &\quad \leq I(X;Y) - I(X;Z_1) && (3.13) \end{aligned}$$

and

$$\begin{aligned} & I(V;Y) - I(V;Z_2) \\ & \quad = I(X;Y) - I(X;Z_2) - [I(X;Y|V) - I(X;Z_2|V)] \qquad (3.14) \\ & \quad \leq I(X;Y) - I(X;Z_1) \qquad (3.15) \end{aligned}$$

where (3.11) and (3.13) are due to the fact that $Y$ is less noisy than $Z_1$, and (3.15) is due to the fact that $Y$ is less noisy than $Z_2$. Thus, without loss of generality, we may set $V = X$ and $U$ to be constant in (3.9), which leads to a simpler characterization of the secrecy capacity region that does not involve any auxiliary random variables. We summarize this result in the following theorem.

**Theorem 8.** *Consider a discrete memoryless two-level security wiretap channel with transition probability $p(y, z_1, z_2|x)$ where $Z_2$ is degraded with respect to $Z_1$ and $Y$ is less noisy than $Z_1$. The secrecy capacity region of the channel is given by the set of all nonnegative pairs $(R_1, R_2)$ that satisfy*

$$\begin{aligned} R_1 &\leq I(X;Y) - I(X;Z_1) \\ \textit{and} \quad R_1 + R_2 &\leq I(X;Y) - I(X;Z_2) \end{aligned} \qquad (3.16)$$

*for some input distribution $p(x)$.*

## 3. Proof of Theorem 5

As mentioned previously in Section 2, to prove Theorem 5, we only need to consider the case where $I(U;Y|S) \geq I(U;Z_2|S)$. To show that every rate pair $(R_1, R_2)$ that satisfies (3.3) for which $I(U;Y|S) \geq I(U;Z_2|S)$ is achievable, we shall consider a coding scheme that combines rate splitting, superposition coding, (nested) binning, and prefix coding. Our code construction relies on a random-coding argument, which can be described as follows.

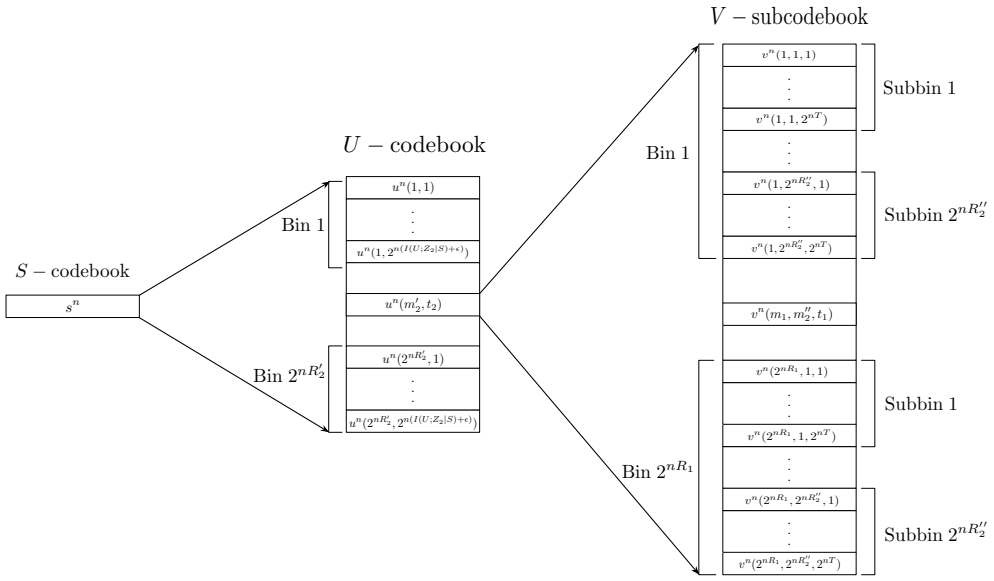



Fig. 7. Codebook structure for a coding scheme that combines rate splitting, superposition coding, (nested) binning, and prefix coding.

Fix a joint auxiliary-input distribution $p(s)(u|s)p(v|u)p(x|v)$ with $I(U;Y|S) \geq I(U;Z_2|S)$ and $\epsilon > 0$. Split the low-security message $M_2$ into two independent submessages $M_2'$ and $M_2''$ with rates $R_2'$ and $R_2''$, respectively.

*Codebook generation.* Our entire codebook consists of three layers: the $S$-codebook as the bottom layer, the $U$-codebook as the middle layer, and the $V$-codebook as the top layer. The $S$-codebook consists of a single length-$n$ sequence $s^n$, generated according to an $n$-product of $p(s)$.

Given $s^n$, randomly and independently generate $2^{n(R_2'+I(U;Z_2|S)+\epsilon)}$ codewords of length $n$ according to an $n$-product of $p(u|s)$. Randomly partition the codewords into $2^{nR_2'}$ bins so each bin contains $2^{n(I(U;Z_2|S)+\epsilon)}$ codewords. Label the codewords as $u_{j,k}^n$ where $j$ denotes the bin number, and $k$ denotes the codeword number within each bin. We shall refer to the codeword collection $\{u_{j,k}^n\}_{j,k}$ as the $U$-codebook.

For each codeword $u_{j,k}^n$ in the $U$-codebook, randomly and independently generate

$2^{n(R_1+R_2''+T)}$ codewords of length $n$ according to an $n$-product of $p(v|u)$. Randomly partition the codewords into $2^{nR_1}$ bins so each bin contains $2^{n(R_2''+T)}$ codewords. Further partition each bin into $2^{nR_2''}$ subbins so each subbin contains $2^{nT}$ codewords. Label the codewords as $v^n_{j,k,l,p,q}$ where $(j,k)$ indicates the base codeword $u^n_{j,k}$ from which $v^n_{j,k,l,p,q}$ was generated, $l$ denotes the bin number, $p$ denotes the subbin number within each bin, and $q$ denotes the codeword number within each subbin. We shall refer to the codeword collection $\{v^n_{j,k,l,p,q}\}_{l,p,q}$ as the $V$-subcodebook corresponding to the base codeword $u^n_{j,k}$ and $\{v^n_{j,k,l,p,q}\}_{j,k,l,p,q}$ as the $V$-codebook.

Once all three codebooks are chosen, they are revealed to all terminals. Fig. 7 illustrates the structure of the entire codebook.

*Encoding.* To send a message triple $(m_1, m_2', m_2'')$, the transmitter *randomly* (according a uniform distribution) chooses a codeword $u^n_{m_2',t_2}$ from the $m_2'$th bin in the $U$-codebook. Once a $u^n_{m_2',t_2}$ is chosen, the transmitter looks into the corresponding $V$-subcodebook $\{v^n_{m_2',t_2,l,p,q}\}_{l,p,q}$ and *randomly* chooses a codeword $v^n_{m_2',t_2,m_1,m_2'',t_1}$ from the subbin identified by $(m_1, m_2'')$. Once a $v^n_{m_2',t_2,m_1,m_2'',t_1}$ is chosen, an input sequence $x^n$ is generated according to an $n$-product of $p(x|v)$ and is then sent through the channel. Note that the sole codeword $s^n$ in the $S$-codebook simply serves as an "averaging base" for the $U$- and $V$-codebooks and does not play any role in the encoding.

*Decoding at the legitimate receiver.* Given the channel outputs $y^n$, the legitimate receiver looks into the $U$-codebook and its $V$-subcodebooks and searches for a pair of codewords $(u^n_{j,k}, v^n_{j,k,l,p,q})$ such that $(s^n, u^n_{j,k}, v^n_{j,k,l,p,q})$ is jointly typical [33] with $y^n$. In the case when

$$R_2' + I(U;Z_2|S) + \epsilon \;<\; I(U;Y|S) \tag{3.17}$$

$$\text{and} \quad R_1 + R_2'' + T \;<\; I(V;Y|U) \tag{3.18}$$

with high probability the codeword pair selection $(u^n_{m'_2,t_2}, v^n_{m'_2,t_2,m_1,m''_2,t_1})$ is the only one that is jointly typical [33] with $y^n$.

*Security at the eavesdropper.* To analyze the security of the high-security message $M_1$ and the submessage $M''_2$ at the eavesdropper, we shall assume (for now) that both the submessage $m'_2$ and the codeword selection $u^n_{m'_2,t_2}$ are known at the eavesdropper. Note that such an assumption can only *strengthen* our security analysis. For any given codeword $u^n_{m'_2,t_2}$, the high security message $M_1$ and the submessage $M''_2$ are encoded using the corresponding $V$-subcodebook $\{v^n_{m'_2,t_2,l,p,q}\}_{l,p,q}$. In particular, each bin in the $V$-subcodebook corresponds to a message $m_1$ and contains $2^{n(R_2+T)}$ codewords, each randomly and independently generated according to an $n$-product of $p(v|u)$. For a given message $m_1$, the transmitted codeword is randomly and uniformly chosen from the corresponding bin (where the randomness is from both the submessage $M''_2$ and the transmitter's choice of $t$). Following [4], in the case when

$$R''_2 + T > I(V; Z_1|U) \tag{3.19}$$

we have

$$\frac{1}{n} I(M_1; Z_1^n, M'_2) \to 0 \tag{3.20}$$

in the limit as $n \to 0$. From (3.20), we conclude that $(1/n)I(M_1; Z_1^n) \to 0$ in the limit as $n \to \infty$. Furthermore, each subbin in the $V$-subcodebook corresponds to a message pair $(m_1, m''_2)$ and contains $2^{nT}$ codewords, each randomly and independently generated according to an $n$-product of $p(v|u)$. For a given message pair $(m_1, m''_2)$, the transmitted codeword is randomly and uniformly chosen from the corresponding subbin (where the randomness is from the transmitter's choice of $t$). Again, following [4], in the case when

$$T > I(V; Z_2|U) \tag{3.21}$$

we have

$$\frac{1}{n}I(M_1, M_2''; Z_2^n, M_2') \to 0 \tag{3.22}$$

in the limit as $n \to 0$.

To analyze the security of the submessage $M_2'$, note that each bin in the $U$-codebook corresponds to a submessage $m_2'$ and contains $2^{n(R_2'+I(U;Z_2|S)+\epsilon)}$ codewords, each randomly and independently generated according to an $n$-product of $p(u|s)$. For a given submessage $m_2'$, the codeword $u^n_{m_2',t_2}$ is randomly and uniformly chosen from the corresponding bin (where the randomness is from the transmitter's choice of $t_2$). Note from (3.21) that the rate of each $V$-subcodebook is greater than $I(V; Z_2|U)$. Following [34, Lemma 1], we have

$$\frac{1}{n}I(M_2'; Z_2^n) \to 0 \tag{3.23}$$

in the limit as $n \to \infty$. Putting together (3.22) and (3.23) and using the fact that $(M_1, M_2'')$ and $M_2'$ are independent, we have

$$\begin{aligned}
\frac{1}{n}I(M_1, M_2; Z_2^n) &= \frac{1}{n}I(M_1, M_2', M_2''; Z_2^n) && (3.24)\\
&= \frac{1}{n}I(M_2'; Z_2^n) + \frac{1}{n}I(M_1, M_2''; Z_2^n|M_2') && (3.25)\\
&= \frac{1}{n}I(M_2'; Z_2^n) + \frac{1}{n}I(M_1, M_2''; Z_2^n, M_2') && (3.26)
\end{aligned}$$

which tends to zero in the limit as $n \to \infty$.

Finally, note that the overall communicate rate $R_2$ of the low-security message $M_2$ is given by

$$R_2 = R_2' + R_2''. \tag{3.27}$$

Eliminating $T$, $R_2'$ and $R_2''$ from (3.17)–(3.19), (3.21), (3.27), and $R_2', R_2'' \geq 0$ using Fourier-Motzkin elimination, simplifying the results using the facts that 1) $I(U; Y|S) \geq I(U; Z_2|S)$ by the assumption, 2) $I(V; Z_2|U) \leq I(V; Z_1|U)$ due to the Markov chain

$(U,V) \to Z_1 \to Z_2$, and 3) $I(V;Y|U) + I(U;Y|S) = I(V,U;Y|S) = I(V;Y|S)$ and $I(V;Z_2|U) + I(U;Z_2|S) = I(V,U;Z_2|S) = I(V;Z_2|S)$ due to the Markov chain $S \to U \to V \to X \to (Y,Z_1,Z_2)$, and letting $\epsilon \to 0$, we conclude that any rate pair $(R_1,R_2)$ satisfying (3.3) for which $I(U;Y|S) \geq I(U;Z_2|S)$ is achievable. This completes the proof of Theorem 5.

## C. Gaussian Two-Level Security Wiretap Channel

### 1. Scalar Channel

Consider a discrete-time two-level security wiretap channel with real input $X$ and outputs $Y$, $Z_1$ and $Z_2$ given by

$$\begin{aligned} Y &= \sqrt{a}X + N_1 \\ Z_1 &= \sqrt{b_1}X + N_2 \\ Z_2 &= \sqrt{b_2}X + N_3 \end{aligned} \tag{3.28}$$

where $a$, $b_1$ and $b_2$ are the corresponding channel gains, and $N_1$, $N_2$ and $N_3$ are additive white Gaussian noise with zero means and unit variances. Assume that $b_1 \geq b_2$ so the channel output $Z_2$ is (stochastically) degraded with respect to $Z_1$. The channel input $X$ is subject to the average power constraint (1.5).

We term the above communication scenario as *(scalar) Gaussian two-level security wiretap channel*. The following theorem provides an explicit characterization of the secrecy capacity region.

**Theorem 9.** *Consider the (scalar) Gaussian two-level security wiretap channel* (3.28) *where* $b_1 \geq b_2$, *and the channel input* $X$ *is subject to the average power constraint* (1.5). *The secrecy capacity region of the channel is given by the collection of all*

*nonnegative pairs* $(R_1, R_2)$ *that satisfy*

$$\begin{aligned} R_1 &\leq C_s(P, a, b_1) \\ \textit{and} \quad R_1 + R_2 &\leq C_s(P, a, b_2) \end{aligned} \tag{3.29}$$

*where* $C_s(P, a, b)$ *is defined as in* (1.6).

*Proof:* Following the same argument as that for Fact 1, any achievable secrecy rate pair $(R_1, R_2)$ must satisfy (3.29). We may thus focus on the forward part of the theorem.

To show that any nonnegative pair $(R_1, R_2)$ that satisfies (3.29) is achievable, let us first consider two simple cases. First, when $b_1 \geq b_2 \geq a$, both $C_s(P, a, b_1)$ and $C_s(P, a, b_2)$ are equal to zero (c.f. definition (1.6)). So (3.29) does not include any positive rate pairs and hence there is nothing to prove. Next, when $b_1 \geq a \geq b_2$, $C_s(P, a, b_1) = 0$ and (3.29) reduces to

$$\begin{aligned} R_1 &= 0 \\ \text{and} \quad R_2 &\leq C_s(P, a, b_2). \end{aligned} \tag{3.30}$$

Since the high-security message $M_1$ does not need to be transmitted, any rate pair in this region can be achieved by using a scalar Gaussian wiretap code to encode the low-security message $M_2$. This has left us with the only case with $a \geq b_1 \geq b_2$.

For the case where $a \geq b_1 \geq b_2$, the channel output $Y$ is less noisy than $Z_1$. Thus, the achievability of any rate pair in (3.29) follows from that of (3.16) by choosing $X$ to be Gaussian with zero mean and variance $P$. This completes the proof of the theorem. □

The following corollary follows directly from the achievability of the corner point

$$(R_1, R_2) = (C_s(P, a, b_1), C_s(P, a, b_2) - C_s(P, a, b_1)) \tag{3.31}$$

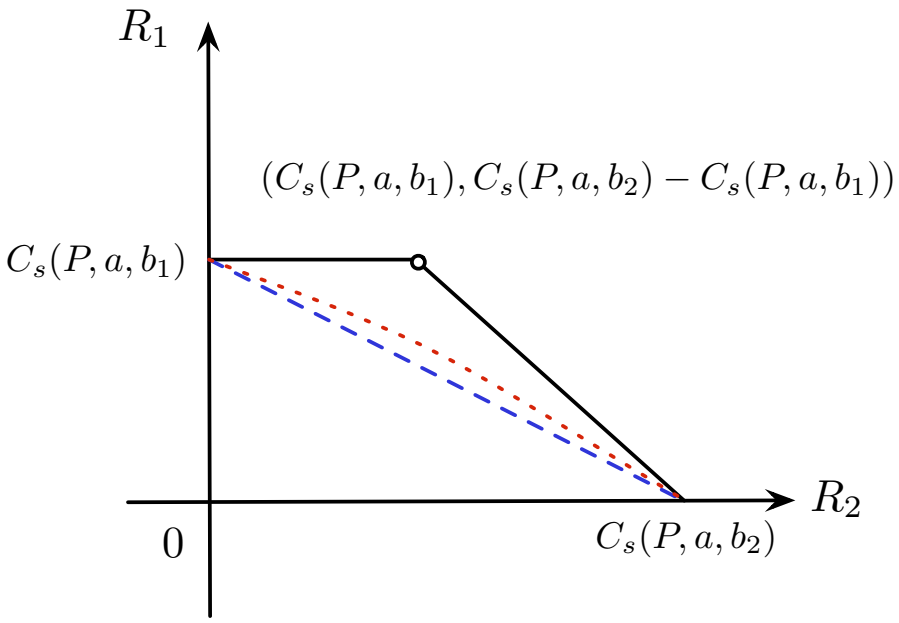



Fig. 8. Secrecy capacity region of the scalar Gaussian two-level security wiretap channel ($a > b_1 > b_2$). For comparison, the dashed line and the dotted line are the boundary of the time-sharing and power-sharing rate regions, respectively.

of (3.29) and Fact 1. (Alternatively, it can also be proved from Theorem 5 by letting $V = X$ be Gaussian with zero mean and variance $P$, $U = X \cdot 1_{\{a \le b_1\}}$, and $S = X \cdot 1_{\{a \le b_2\}}$, where $1_A$ denotes the indicator function for event $A$.)

**Corollary 10.** *Scalar Gaussian two-level security wiretap channels under an average power constraint are perfectly embeddable.*

Fig. 8 illustrates the secrecy capacity region (3.29) for the case where $a > b_1 > b_2$. Also illustrated in the figure are the rate regions that can be achieved by time-sharing and power-sharing between two secrecy codes that are separately designed for the low-security and high-security messages. The time-sharing rate region includes all nonnegative pairs $(R_1, R_2)$ below the straight line connecting the corner points

$(C_s(P, a, b_1), 0)$ and $(0, C_s(P, a, b_2))$. The power-sharing rate region [29] includes all nonnegative pairs $(R_1, R_2)$ such that

$$\begin{aligned} R_1 &\leq C_s(P_1, a, b_1) \\ R_2 &\leq C_s(P, a, b_2) - C_s(P_1, a, b_2) \end{aligned} \tag{3.32}$$

for some $P_1 \in [0, P]$. Note that the corner point (3.31) is strictly outside the time-sharing and power-sharing rate regions, illustrating the superiority of nested binning over the separate coding schemes.

### 2. Independent Parallel Channel

Consider a discrete-time two-level security wiretap channel which consists of a bank of $L$ independent parallel scalar Gaussian two-level security wiretap channels. In this model, the channel outputs are given by $Y = (Y_1, \ldots, Y_L)$, $Z_1 = (Z_{1,1}, \ldots, Z_{1,L})$ and $Z_2 = (Z_{2,1}, \ldots, Z_{2,L})$ where

$$\begin{aligned} Y_l &= \sqrt{a_1} X_l + N_{1,l} \\ Z_{1,l} &= \sqrt{b_{1,l}} X_l + N_{2,l} \qquad l = 1, \ldots, L. \\ Z_{2,l} &= \sqrt{b_{2,l}} X_l + N_{3,l}, \end{aligned} \tag{3.33}$$

Here, $X_l$ is the channel input for the $l$th subchannel, $a_l$, $b_{1,l}$ and $b_{2,l}$ are the corresponding channel gains in the $l$th subchannel, and $N_{1,l}$, $N_{2,l}$ and $N_{3,l}$ are additive white Gaussian noise with zero means and unit variances. We assume that $b_{1,l} \geq b_{2,l}$ for all $l = 1, \ldots, L$, so the channel output $Z_2$ is (stochastically) degraded with respect to $Z_1$. Furthermore, $(N_{1,l}, N_{2,l}, N_{3,l})$, $l = 1, \ldots, L$, are independent so all $L$ subchannels are independent of each other.

We term the above communication scenario as *independent parallel Gaussian two-level security wiretap channel*. The following theorem provides an explicit char-

acterization of the secrecy capacity region under an average individual per-subchannel power constraint.

**Theorem 11.** *Consider the independent parallel Gaussian two-level security wiretap channel* (3.33) *where* $b_{1,l} \geq b_{2,l}$ *for all* $l = 1, \ldots, L$*, and the channel input* $X$ *is subject to the average individual per-subchannel power constraint* (1.8)*. The secrecy capacity region of the channel is given by the collection of all nonnegative pairs* $(R_1, R_2)$ *that satisfy*

$$\begin{aligned} R_1 &\leq \textstyle\sum_{l=1}^{L} C_s(P_l, a_l, b_{1,l}) \\ \textit{and} \quad R_1 + R_2 &\leq \textstyle\sum_{l=1}^{L} C_s(P_l, a_l, b_{2,l}) \end{aligned} \tag{3.34}$$

*where* $C_s(P, a, b)$ *is defined as in* (1.6)*.*

*Proof:* We first prove the converse part of the theorem. Following the same argument as that for Fact 1, we have

$$\begin{aligned} R_1 &\leq C_s(\{P_l, a_l, b_{1,l}\}_{l=1}^{L}) \\ \text{and} \quad R_1 + R_2 &\leq C_s(\{P_l, a_l, b_{2,l}\}_{l=1}^{L}) \end{aligned} \tag{3.35}$$

for any achievable secrecy rate pair $(R_1, R_2)$. By the secrecy capacity expression (1.10) for the independent parallel Gaussian wiretap channel under an average individual per-subchannel power constraint, we have

$$\begin{aligned} C_s(\{P_l, a_l, b_{1,l}\}_{l=1}^{L}) &= \textstyle\sum_{l=1}^{L} C_s(P_l, a_l, b_{1,l}) \\ \text{and} \quad C_s(\{P_l, a_l, b_{2,l}\}_{l=1}^{L}) &= \textstyle\sum_{l=1}^{L} C_s(P_l, a_l, b_{2,l}). \end{aligned} \tag{3.36}$$

Substituting (3.36) into (3.35) proves the converse part of the theorem.

To show that any nonnegative pair $(R_1, R_2)$ that satisfies (3.34) is achievable, let us consider *independent* coding over each of the $L$ subchannels. Note that each subchannel is a scalar Gaussian two-level security wiretap channel with average power constraint $P_l$ and channel gains $(a_l, b_{1,l}, b_{2,l})$. Thus, by Theorem 9, any nonnegative

pair $(R_{1,l}, R_{2,l})$ that satisfies

$$\begin{aligned} R_{1,l} &\leq C_s(P_l, a_l, b_{1,l}) \\ \text{and} \quad R_{1,l} + R_{2,l} &\leq C_s(P_l, a_l, b_{2,l}) \end{aligned} \tag{3.37}$$

is achievable for the $l$th subchannel. The overall communication rates are given by

$$\begin{aligned} R_1 &= \textstyle\sum_{l=1}^{L} R_{1,l} \\ \text{and} \quad R_2 &= \textstyle\sum_{l=1}^{L} R_{2,l}. \end{aligned} \tag{3.38}$$

Substituting (3.37) into (3.38) proves that any nonnegative pair $(R_1, R_2)$ that satisfies (3.34) is achievable. This completes the proof of the theorem. □

Similar to the scalar case, the following corollary is an immediate consequence of Theorem 11.

**Corollary 12.** *Independent parallel Gaussian two-level security wiretap channels under an average individual per-subchannel power constraint are perfectly embeddable.*

The secrecy capacity region of the channel under an average total power constraint is summarized in the following corollary. The results follow from the well-known fact that an average total power constraint can be written as the *union* of average individual per-subchannel power constraints, where the union is over all possible power allocations among the subchannels.

**Corollary 13.** *Consider the independent parallel Gaussian two-level security wiretap channel* (3.33) *where* $b_{1,l} \geq b_{2,l}$ *for all* $l = 1, \ldots, L$*, and the channel input* $X$ *is subject to the average total power constraint* (1.9)*. The secrecy capacity region of the channel is given by the collection of all nonnegative pairs* $(R_1, R_2)$ *that satisfy*

$$\begin{aligned} R_1 &\leq \textstyle\sum_{l=1}^{L} C_s(P_l, a_l, b_{1,l}) \\ \textit{and} \quad R_1 + R_2 &\leq \textstyle\sum_{l=1}^{L} C_s(P_l, a_l, b_{2,l}) \end{aligned} \tag{3.39}$$

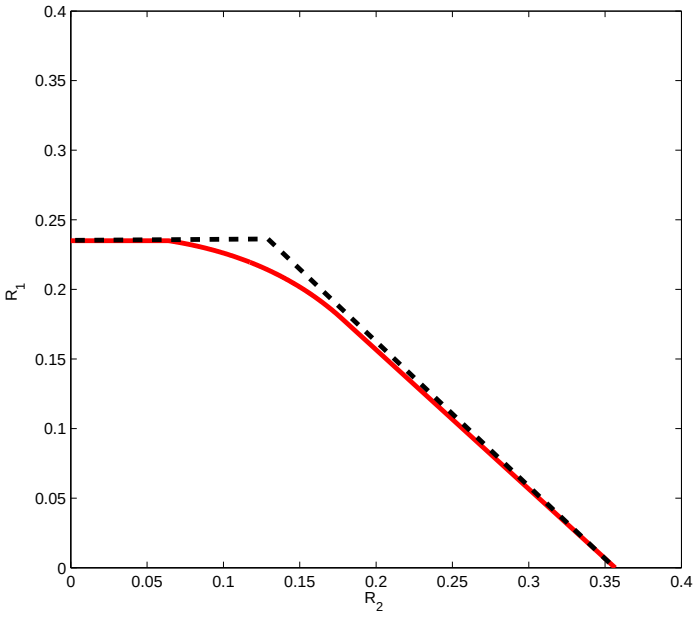



Fig. 9. Secrecy capacity region of the independent parallel Gaussian two-level security wiretap channel under an average total power constraint. The intersection of the dashed lines are outside the secrecy capacity region, indicating that the channel is not perfectly embeddable.

*for some power allocation* $(P_1, \ldots, P_L)$ *such that* $\sum_{l=1}^{L} P_l \leq P$.

Fig. 9 illustrates the secrecy capacity region with $L = 2$ subchannels where

$$a_1 = 1.000, \quad b_{1,1} = 0.800, \quad b_{2,1} = 0.100$$

$$a_2 = 1.000, \quad b_{1,2} = 0.250, \quad b_{2,2} = 0.100$$

$$\text{and} \quad P = 1.000.$$

As we can see, under the average total power constraint (1.9), the independent parallel Gaussian two-level security wiretap channel is embeddable but *not* perfectly embeddable. The reason is that the optimal power allocation $(P_1, P_2)$ that maxi-

mizes $C_s(P_1, a_1, b_{2,1}) + C_s(P_2, a_2, b_{2,2})$ is *suboptimal* in maximizing $C_s(P_1, a_1, b_{1,1}) + C_s(P_2, a_2, b_{1,2})$. By comparison, under the average individual per-subchannel power constraint (1.8), the power allocated to each of the subchannels is fixed so the channel is always perfectly embeddable.

## D. Two-Level Security Wiretap Channel II

In Chapter I we briefly summarized the known results on a classical secrecy communication setting known as wiretap channel. A closely related classical secrecy communication scenario is *wiretap channel II*, which was first studied by Ozarow and Wyner [32]. In the wiretap channel II setting, the transmitter sends a binary sequence $X^n = (X_1, \ldots, X_n)$ of length $n$ *noiselessly* to an legitimate receiver. The signal $Z^n = (Z_1, \ldots, Z_n)$ received at the eavesdropper is given by

$$Z_i = \begin{cases} X_i, & i \in S \\ e, & \text{otherwise} \end{cases} \tag{3.40}$$

where $e$ represents an erasure output, and $S$ is a subset of $\{1, \ldots, n\}$ of size $n\alpha$ representing the locations of the transmitted bits that can be accessed by the eavesdropper.

If the subset $S$ is *known* at the transmitter, a message $M$ of $n(1-\alpha)$ bits can be noiselessly communicated to the legitimate receiver through $X_{S^c} := \{X_i : \ i \in S^c\}$. Since the eavesdropper has no information regarding to $X_{S^c}$, *perfectly* secure communication is achieved *without* any coding. It is easy to see that in this scenario, $n(1-\alpha)$ is also the *maximum* number of bits that can be reliably and perfectly securely communicated through $n$ transmitted bits.

An interesting result of [32] is that for any $\epsilon > 0$, a total of $n(1-\alpha-\epsilon)$ bits can be reliably and *asymptotically perfectly* securely communicated to the legitimate receiver even when the subset $S$ is *unknown* (but with a fixed size $n\alpha$) a priori at the

transmitter. Here, by "asymptotically perfectly securely" we mean $(1/n)I(M; Z^n) \to 0$ in the limit as $n \to \infty$. Unlike the case where the subset $S$ is known a priori, coding is *necessary* when $S$ is unknown at the transmitter. In particular, [32] considered a random binning scheme that partitions the collection of all length-$n$ binary sequences into an appropriately chosen *group code* and its cosets. For the wiretap channel setting, as shown in Section B, a random binning scheme can be easily modified into a *nested* binning scheme to efficiently embed high-security bits into low-security ones. The main goal of this section is to extend this result from the classical setting of wiretap channel to wiretap channel II.

More specifically, assume that a realization of the subset $S$ has two possible sizes, $n\alpha_1$ and $n\alpha_2$, where $1 \geq \alpha_1 \geq \alpha_2 \geq 0$. The transmitter has two independent messages, the high-security message $M_1$ and the low-security message $M_2$, uniformly drawn from $\{1, \ldots, 2^{nR_1}\}$ and $\{1, \ldots, 2^{nR_2}\}$ respectively. When the size of the realization $S$ is $n\alpha_2$, both messages $M_1$ and $M_2$ need to be secure, i.e., $(1/n)I(M_1, M_2; Z^n) \to 0$ in the limit as $n \to \infty$. In addition, when the size of the realization of $S$ is $n\alpha_1$, the high-security message $M_1$ needs to remain secure, i.e., $(1/n)I(M_1; Z^n) \to 0$ in the limit as $n \to \infty$. We term this communication scenario as *two-level security wiretap channel II*, in line with our previous terminology in Section B.

By the results of [32], without needing to communicate the low-security message $M_2$, the maximum achievable $R_1$ is $1 - \alpha_1$. Without the additional secrecy constraint $(1/n)I(M_1; Z^n) \to 0$ on the high-security message $M_1$, the messages $(M_1, M_2)$ can be viewed as a single message $M$ with rate $R_1 + R_2$, and the maximum achievable $R_1 + R_2$ is $1 - \alpha_2$. The main result of this section is to show that the rate pair $(1 - \alpha_1, \alpha_1 - \alpha_2)$ is indeed achievable, from which we may conclude that two-level security wiretap channels II are *perfectly* embeddable. Moreover, perfect embedding can be achieved by a nested binning scheme that uses a *two-level* coset code. The

results are summarized in the following theorem.

**Theorem 14.** *Two-level security wiretap channels II are perfectly embeddable. Moreover, perfect embedding can be achieved by a nested binning scheme that uses a two-level coset code.*

*Proof:* Fix $\epsilon > 0$. Consider a binary parity-check matrix

$$H = \begin{bmatrix} H_1 \\ H_2 \end{bmatrix}$$

where the size of $H_1$ is $n(1-\alpha_1-\epsilon) \times n$ and the size of $H_2$ is $n(\alpha_1-\alpha_2) \times n$. Let $s_1(\cdot)$ be a one-on-one mapping between $\{1, \ldots, 2^{n(1-\alpha_1-\epsilon)}\}$ and the binary vectors of length $n(1-\alpha_1-\epsilon)$, and let $s_2(\cdot)$ be a one-on-one mapping between $M_2 \in \{1, \ldots, 2^{n(\alpha_1-\alpha_2)}\}$ and the binary vectors of length $n(\alpha_1-\alpha_2)$.

For a given message pair $(m_1, m_2)$, the transmitter randomly (according to a uniform distribution) chooses a solution $x^n$ to the linear equations

$$(x^n)^t H = (x^n)^t \begin{bmatrix} H_1 \\ H_2 \end{bmatrix} = \begin{bmatrix} s_1(m_1) \\ s_2(m_2) \end{bmatrix} \tag{3.41}$$

and sends it to the legitimate receiver.

When the parity-check matrix $H$ has *full* (row) rank, the above encoding procedure is equivalent of a nested binning scheme that partitions the collection of all length-$n$ binary sequences into bins and subbins using a two-level coset code with parity-check matrices $(H_1, H_2)$. Moreover, let $b_1, \ldots, b_n$ be the columns of $H$ and let $\Gamma \subseteq \{1, \ldots, n\}$. Define $D_2(\Gamma)$ as the dimension of the subspace spanned by $\{b_i : \ i \in \Gamma\}$ and

$$D_2^* := \min_{|\Gamma| = n(1-\alpha_2)} D_2(\Gamma). \tag{3.42}$$

When the size of the realization of $S$ is $n\alpha_2$, by [32, Lemma 4] we have

$$H(M_1, M_2|Z^n) = D_2^*. \tag{3.43}$$

Note that the low-security message $M_2$ is uniformly drawn from $\{1, \ldots, 2^{n(\alpha_1-\alpha_2)}\}$. So by (3.41), for a given high-security message $m_1$, the transmitted sequence $x^n$ is randomly chosen (according to a uniform distribution) as a solution to the linear equations $(x^n)^t H_1 = s_1(m_1)$. If we let $a_1, \ldots, a_n$ be the columns of $H_1$ and define

$$D_1^* := \min_{|\Gamma|=n(1-\alpha_1)} D_1(\Gamma) \tag{3.44}$$

where $D_1(\Gamma)$ is the dimension of the subspace spanned by $\{a_i : \ i \in \Gamma\}$, we have again from [32, Lemma 4]

$$H(M_1|Z^n) = D_1^* \tag{3.45}$$

when the size of the realization of $S$ is $n\alpha_1$.

Let $\Psi(H) = 1$ when we have either $H$ does *not* have full rank, or $D_2^* < n(1 - \alpha_2 - \epsilon) - 3/\epsilon$, or $D_1^* < n(1 - \alpha_1 - \epsilon) - 3/\epsilon$, and let $\Psi(H) = 0$ otherwise. By using a randomized argument that generates the entries of $H$ independently according to a uniform distribution in $\{0, 1\}$, we can show that there exists an $H$ with $\Psi(H) = 0$ for sufficiently large $n$ (see Appendix C for details). For such an $H$, we have from (3.43) and (3.45) that $(1/n)I(M_1, M_2; Z^n) \leq 3/(n\epsilon)$ when the size of the realization of $S$ is $n\alpha_2$, and $(1/n)I(M_1; Z^n) \leq 3/(n\epsilon)$ when the size of the realization of $S$ is $n\alpha_1$.

Letting $n \to \infty$ and $\epsilon \to 0$ (in that order) proves the achievability of the rate pair $(1 - \alpha_1, \alpha_1 - \alpha_2)$ and hence completes the proof of the theorem. $\square$

## E. Concluding Remarks

In this chapter, we considered the problem of simultaneously communicating two messages, a high-security message and a low-security message, to a legitimate receiver, referred to as the security embedding problem. An information-theoretic formulation of the problem was presented. With appropriate coding architectures, it was shown that a significant portion of the information bits can receive additional security protections without sacrificing the overall rate of communication. The key to achieving efficient embedding was to use the low-security message as part of the transmitter randomness to protect the high-security message when the eavesdropper channel realization is strong.

For the engineering communication scenarios with real channel input and additive white Gaussian noise, it was shown that the high-security message can be embedded into the low-security message at full rate without incurring any loss on the overall rate of communication for both scalar and independent parallel Gaussian channels (under an average individual per-subchannel power constraint). The scenarios with multiple transmit and receive antennas are considerably more complex and hence require further investigations.

Finally, note that even though in this chapter we have only considered providing two levels of security protections to the information bits, most of the results extend to multiple-level security in the most straightforward fashion. In the limit scenario when the security levels change continuously, the number of secure bits delivered to the legitimate receiver would depend on the realization of the eavesdropper channel even though such realizations are unknown a priori at the transmitter.

# CHAPTER IV

# SECURE SYMMETRICAL MULTILEVEL DIVERSITY CODING

## A. Introduction

Symmetrical Multilevel Diversity Coding (SMDC) is a source coding problem with $L$ independent discrete memoryless sources $(S_1, \ldots, S_L)$, where the *importance* of the sources is assumed to decrease with the subscript $l$. The sources are to be encoded by a total of $L$ encoders, where the rate of the $l$th encoder output is $R_l$. The decoder can access a subset $U \subseteq \Omega_L := \{1, \ldots, L\}$ of the encoder outputs. Which subset of the encoder outputs is available at the decoder is *unknown* a priori at the encoders. However, no matter which subset $U$ actually realizes, the sources $(S_1, \ldots, S_m)$ need to be asymptotically perfectly reconstructed at the decoder whenever $|U| \geq m$. Note that the word "symmetrical" here refers to the fact that the sources that need to be reconstructed at the decoder depend on the available subset of the encoder outputs only via its cardinality. The rate allocations at different encoders, however, can be different and are not necessarily symmetrical.

The problem of Multilevel Diversity Coding (MDC) was introduced by Roche [35] and Yeung [36] in the early 1990s. In particular, [36] considered the simple coding strategy of separately encoding different sources at the encoders, subsequently referred to as *superposition coding*. The aforementioned SMDC problem was first systematically studied in [37], where it was shown that superposition coding can achieve the minimum sum rate for the general SMDC problem (with an arbitrary total number of encoders $L$) and the entire admissible rate region with $L = 3$ encoders. The problem regarding whether superposition coding can achieve the entire admissible

rate region for the general SMDC problem, however, remained open. Finally, in a very elegant (albeit highly technical) paper [38], Yeung and Zhang resolved the open problem by positive through the so-called $\alpha$-*resolution* method.

Recent years have seen a flurry of research on information-theoretic security. See [7] and [8] for surveys of recent progress in this field. Motivated by this renewed interest, in this chapter we consider the problem of *Secure* Symmetrical Multilevel Diversity Coding (S-SMDC) in the presence of an additional eavesdropper. Specifically, a collection of $L - N$ independent discrete memoryless sources $(S_1, \ldots, S_{L-N})$ are to be encoded by a total of $L$ encoders, where the rate of the $l$th encoder output is $R_l$. A legitimate receiver and an eavesdropper can access a subset $U \subseteq \Omega_L$ and $A \subseteq \Omega_L$ of the encoder outputs, respectively. Which subsets of the encoder outputs are available at the legitimate receiver and the eavesdropper are *unknown* a priori at the encoders. However, no matter which subsets $U$ and $A$ actually occur, the sources $(S_1, \ldots, S_k)$ need to be asymptotically perfectly reconstructed at the legitimate receiver whenever $|U| \geq N + k$, and the entire collection of the sources $(S_1, \ldots, S_{L-N})$ needs to be kept *perfectly* secret from the eavesdropper as long as $|A| \leq N$. As before, the word "symmetrical" here refers to the access structure at the legitimate receiver and the eavesdropper, but not to the rate allocations at different encoders. We envision that such a communication scenario is useful for designing distributed information storage systems [35] where information retrieval needs to be both robust and secure.

As mentioned previously, separate encoding of different sources (superposition coding) can achieve the entire admissible rate region for the general SMDC problem without any secrecy constraints [38]. It is thus natural to ask whether the same separate encoding strategy would remain optimal for the general S-SMDC problems. For the classical SMDC problems without any secrecy constraints, the problem of efficient

encoding of individual sources is essentially to transmit the source over an *erasure* channel and is well understood based on the earlier work of Singleton [39]. For the S-SMDC problems, however, the problem of efficient encoding of individual sources is closely related to the problem of secure coding over a *Wiretap Network (WN)* [40], which, in its most general setting, is a very challenging problem in information-theoretic security.

The rest of the chapter is organized as follows. In Section B, we focus on the problem of encoding individual sources, i.e., Secure Symmetrical Single-level Diversity Coding (S-SSDC). By leveraging the results of [40] on secure coding over a three-layer WN and utilizing some basic polyhedral structure of the admissible rate region, we provide a precise characterization of the entire admissible rate region for the general S-SSDC problem. Building on this result, in Section C we show that superposition coding can achieve the minimum sum rate for the general S-SMDC problem. Finally, in Section D we conclude the chapter with some remarks.

## B. Secure Symmetrical Single-Level Diversity Coding

### 1. Problem Statement

Let $\{S[t]\}_{t=1}^{\infty}$ be a discrete memoryless source with time index $t$ and let $S^n := (S[1], \ldots, S[n])$. An $(L, N, m)$ S-SSDC problem consists of a set of $L$ encoders, a legitimate receiver who has access to a subset $U \subseteq \Omega_L$ of the encoder outputs, and an eavesdropper who has access to a subset $A \subseteq \Omega_L$ of the encoder outputs. Which subsets of the encoder outputs are available at the legitimate receiver and the eavesdropper are *unknown* a priori at the encoders. However, no matter which subsets $U$ and $A$ actually occur, the legitimate receiver must be able to asymptotically perfectly reconstruct the source whenever $|U| \geq m$, and the source must be kept *perfectly* secret

from the eavesdropper as long as $|A| \leq N$. Obviously, reliable and secure communication of the source is possible only when $m > N$.

Formally, an $(n, (M_1, \ldots, M_L))$ code is defined by a collection of $L$ encoding functions

$$e_l : \mathcal{S}^n \times \mathcal{K} \to \{1, \ldots, M_l\}, \quad \forall l = 1, \ldots, L \tag{4.1}$$

and decoding functions

$$d_U : \prod_{l \in U} \{1, \ldots, M_l\} \to \mathcal{S}^n, \quad \forall U \subseteq \Omega_L \text{ s.t. } |U| \geq m. \tag{4.2}$$

Here, $\mathcal{K}$ denotes the key space accessible to all $L$ encoders. There are no limitations on the size of the key space $\mathcal{K}$. However, the secret key is only shared by the encoders, but *not* with the legitimate receiver or the eavesdropper. A nonnegative rate tuple $(R_1, \ldots, R_L)$ is said to be *admissible* if for every $\epsilon > 0$, there exists, for sufficiently large block length $n$, an $(n, (M_1, \ldots, M_L))$ code such that:

- (Rate constraints)

$$\frac{1}{n} \log M_l \leq R_l + \epsilon, \quad \forall l = 1, \ldots, L; \tag{4.3}$$

- (Asymptotically perfect reconstruction at the legitimate receiver)

$$\Pr\{d_U(X_U) \neq S^n\} \leq \epsilon, \quad \forall U \subseteq \Omega_L \text{ s.t. } |U| \geq m \tag{4.4}$$

  where $X_l := e_l(S^n, K)$ is the output of the $l$th encoder, $K$ is the secret key shared by all $L$ encoders, and $X_U := \{X_l : l \in U\}$; and

- (Perfect secrecy at the eavesdropper)

$$H(S^n | X_A) = H(S^n), \qquad \forall A \subseteq \Omega_L \text{ s.t. } |A| \leq N \tag{4.5}$$

  i.e., observing the encoder outputs $X_A$ does not provide *any* information re-

garding to the source sequence $S^n$.

The *admissible rate region* $\mathcal{R}$ is the collection of *all* admissible rate tuples $(R_1, \ldots, R_L)$. The *minimum sum rate* $R_{ms}$ is defined as

$$R_{ms} := \min_{(R_1,\ldots,R_L)\in\mathcal{R}} \sum_{l=1}^{L} R_l. \tag{4.6}$$

## 2. Main Results

The following lemma provides a simple outer bound on the admissible rate region of the general S-SSDC problem. Let $\mathcal{R}(L, k, H)$ be the collection of all nonnegative rate tuples $(R_1, \ldots, R_L)$ satisfying

$$\sum_{l\in D} R_l \geq H, \quad \forall D \in \Omega_L^{(k)} \tag{4.7}$$

where $\Omega_L^{(k)}$ is the collection of all subsets of $\Omega_L$ of size $k$.

**Lemma 1.** *For any $(L, N, m)$ S-SSDC problem, the admissible rate region*

$$\mathcal{R} \subseteq \mathcal{R}(L, m - N, H(S)). \tag{4.8}$$

Lemma 1 can be proved using standard information-theoretic techniques. For completeness, a proof is included in Appendix D. The above outer bound is known to be tight in the following two special cases:

1) When $N = 0$, the $(L, N, m)$ S-SSDC problem reduces to the classical $(L, m)$ SSDC problem without any secrecy constraints, for which the admissible rate region is known [39] to be $\mathcal{R}(L, m, H(S))$.

2) With $N > 0$ but $m = N + 1$, a collection $D$ of the encoder outputs will either lead to an asymptotically perfect reconstruction of the source (whenever $|D| \geq N + 1$), or provide zero information on the source (whenever $|D| \leq N$).

In this case, the $(L, N, m)$ S-SSDC problem reduces to the classical $(L, N)$ *threshold secret sharing* problem, for which the admissible rate region is known [41, 42] to be $\mathcal{R}(L, 1, H(S))$.

The main result of this section is that the outer bound $\mathcal{R}(L, m-N, H(S))$ is in fact the admissible rate region for the *general* S-SSDC problem, as summarized in the following theorem.

**Theorem 15.** *For any $(L, N, m)$ S-SSDC problem, the admissible rate region*

$$\mathcal{R} = \mathcal{R}(L, m-N, H(S)). \tag{4.9}$$

A proof of the theorem is provided in Section 3. To show that *every* rate tuple in $\mathcal{R}(L, m-N, H(S))$ is admissible, our proof proceeds in the following two steps. First, we show that for any $(L, N, m)$ S-SSDC problem, the symmetrical rate tuple $(H(S)/(m-N), \ldots, H(S)/(m-N))$ is admissible. In our proof, this is accomplished by relating the S-SSDC problem to the problem of secure coding over a *three-layer* WN and using the result of [40, Theorem 3] on an achievable secrecy rate for the generic WN. Building on the previous result, next we show that every rate tuple in $\mathcal{R}(L, m-N, H(S))$ is admissible via an induction argument (inducting on the total number of encoders $L$) and the following polyhedral structure of $\mathcal{R}(L, k, H)$.

**Proposition 3.** *$\mathcal{R}(L, k, H)$ is a pointed polyhedron in $\mathbb{R}^L$ with the following structural properties:*

1) *The characteristic cone of $\mathcal{R}(L, k, H)$ is given by $\{(R_1, \ldots, R_L) : R_l \geq 0, \forall l = 1, \ldots, L\}$.*
2) *Among all corner points (vertices) of $\mathcal{R}(L, k, H)$, $(H/k, \ldots, H/k)$ is the* only *one with all* strictly *positive entries (if there exists any).*

*3) For any $l = 1, \ldots, L$, the $R_l = 0$ slice of $\mathcal{R}(L, k, H)$ is* isomorphic *to $\mathcal{R}(L-1, k-1, H)$. In particular, the $R_L = 0$ slice of $\mathcal{R}(L, k, H)$ is* identical *to $\mathcal{R}(L-1, k-1, H)$, i.e.,*

$$\{(R_1, \ldots, R_{L-1}) : (R_1, \ldots, R_{L-1}, 0) \in \mathcal{R}(L, k, H)\} = \mathcal{R}(L-1, k-1, H). \quad (4.10)$$

*Proof.* Property 1 follows directly from the definition of characteristic cone [43, Lecture 2]. Property 2 is due to the fact that

$$(R_1, \ldots, R_L) = (H/k, \ldots, H/k) \quad (4.11)$$

is a solution to the equations

$$\sum_{l \in D} R_l = H, \quad \forall D \in \Omega_L^{(k)}. \quad (4.12)$$

To see property 3, note that the $R_l = 0$ slice of $\mathcal{R}(L, k, H)$ is given by all nonnegative rate tuples $(R_1, \ldots, R_{l-1}, R_{l+1}, \ldots, R_L)$ satisfying

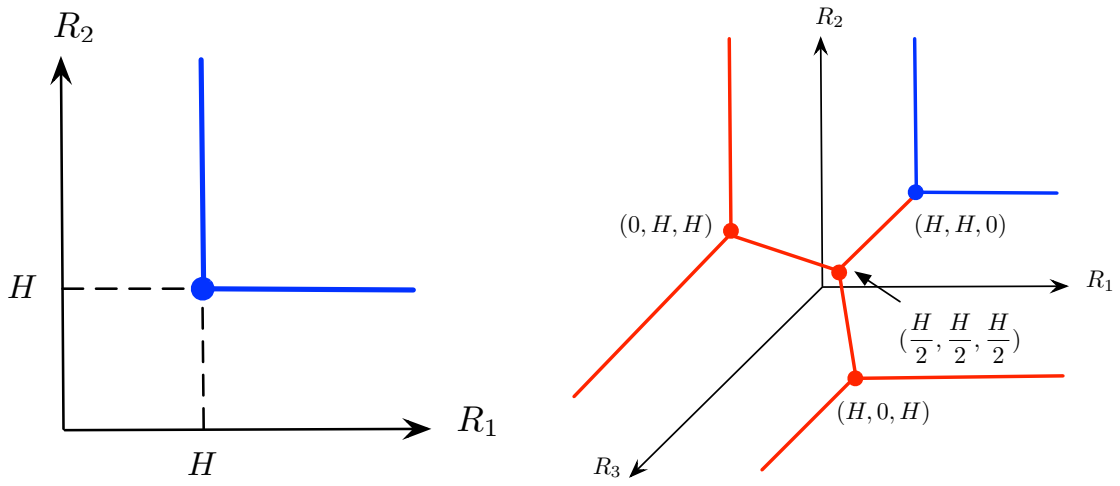
$$\sum_{d \in D} R_d \geq H, \quad \forall D \in \Omega_{L\setminus\{l\}}^{(k-1)} \cup \Omega_{L\setminus\{l\}}^{(k)} \quad (4.13)$$

where $\Omega_{L\setminus\{l\}}^{(k)}$ denotes all subsets of $\Omega_L \setminus \{l\}$ of size $k$. Since every inequality with $D \in \Omega_{L\setminus\{l\}}^{(k)}$ is dominated by every inequality with $D' \in \Omega_{L\setminus\{l\}}^{(k-1)}$ and such that $D' \subseteq D$, we have the desired property. □

Fig. 10 illustrates the above polyhedral structure of $\mathcal{R}(L, k, H)$ for $L = 2$ and 3. The following corollary summarizes the minimum sum rate for the general S-SSDC problem.

**Corollary 16.** *For any $(L, N, m)$ S-SSDC problem, the minimum sum rate*

$$R_{ms} = \frac{L}{m - N} H(S). \quad (4.14)$$




(a) $L = 2, m = 2, N = 1$ (b) $L = 3, m = 3, N = 1$

Fig. 10. The rate region $\mathcal{R}(L, k, H)$ for $L = 2$ and 3. The $R_l = 0$ slices of $\mathcal{R}(3, 2, H)$ are isomorphic to $\mathcal{R}(2, 1, H)$.

*Proof.* Let us first verify that

$$\min_{(R_1,\ldots,R_L)\in\mathcal{R}(L,k,H)} \sum_{l=1}^{L} R_l = \frac{L}{k} H. \tag{4.15}$$

For any rate tuple $(R_1, \ldots, R_L) \in \mathcal{R}(L, k, H)$, we have

$$\sum_{l\in D} R_l \geq H, \quad \forall D \in \Omega_L^{(k)}. \tag{4.16}$$

Summing over all $D \in \Omega_L^{(k)}$ gives

$$\sum_{D\in\Omega_L^{(k)}} \sum_{l\in D} R_l = \begin{pmatrix} L-1 \\ k-1 \end{pmatrix} \sum_{l=1}^{L} R_l \geq \begin{pmatrix} L \\ k \end{pmatrix} H. \tag{4.17}$$

We thus have

$$\sum_{l=1}^{L} R_l \geq \frac{\begin{pmatrix} L \\ k \end{pmatrix}}{\begin{pmatrix} L-1 \\ k-1 \end{pmatrix}} H = \frac{L}{k} H \tag{4.18}$$

for any rate tuple $(R_1, \ldots, R_L) \in \mathcal{R}(L, k, H)$. On the other hand, note that the symmetrical rate tuple

$$(H/k, \ldots, H/k) \in \mathcal{R}(L, k, H) \tag{4.19}$$

so

$$\min_{(R_1,\ldots,R_L)\in\mathcal{R}(L,k,H)} \sum_{l=1}^{L} R_l \leq \frac{L}{k} H. \tag{4.20}$$

Combining (4.18) and (4.20) completes the proof of (4.15).

Now by Theorem 15,

$$R_{ms} = \min_{(R_1,\ldots,R_L)\in\mathcal{R}} \sum_{l=1}^{L} R_l = \min_{(R_1,\ldots,R_L)\in\mathcal{R}(L,m-N,H(S))} \sum_{l=1}^{L} R_l = \frac{L}{m-N} H(S). \tag{4.21}$$

This completes the proof of the corollary. □

## 3. Proof of Theorem 15

Let us first show that the symmetrical rate tuple $(H(S)/(m-N), \ldots, H(S)/(m-N))$ is admissible by considering the following simple *source-channel separation* scheme for the $(L, N, m)$ S-SSDC problem:

- First compress the source sequence $S^n$ into a source message $W$ using a fixed-length lossless source code. It is well known [33, Chapter 3.2] that the rate $R$ of the source message $W$ can be made arbitrarily close to the entropy rate $H(S)$ for sufficiently large block length $n$.

- Next, the source message $W$ is delivered to the legitimate receiver using a secure

$$(L, N, m, (R_1, \ldots, R_L))$$

  WN code.

The problem of secure coding over a WN was formally introduced in [40]. A generic WN $(\mathcal{G}, s, \mathcal{U}, \mathcal{A})$ consists of a directed acyclic network $\mathcal{G}$, a source node $s$, a set of user nodes $\mathcal{U}$, and a collection of sets of wiretapped edges $\mathcal{A}$. Each member of $\mathcal{A}$ may be fully accessed by an eavesdropper, but no eavesdropper may access more than one member of $\mathcal{A}$. The source node has access to a message $W$, which is intended for all user nodes in $\mathcal{U}$ but needs to be kept *perfectly* secret from the eavesdroppers. The maximum achievable secrecy rate for $W$ is called the *secrecy capacity* of the WN and is denoted by $C_s(\mathcal{G}, s, \mathcal{U}, \mathcal{A})$.

An $(L, N, m, (R_1, \ldots, R_L))$ WN is a special WN with three layers of nodes: top, middle, and bottom. As illustrated in Fig. 11, the only node in the top layer is the source node $s$. There are $L$ intermediate nodes in the middle layer, each corresponding to an encoder in the $(L, N, m)$ S-SSDC problem. For each $l = 1, \ldots, L$, the source node $s$ is connected to the intermediate node $l$ by a channel $(s, l)$ with capacity $R_l$. There are

$$|\mathcal{U}| = \begin{pmatrix} L \\ m \end{pmatrix} \tag{4.22}$$

user nodes in the bottom layer, each corresponding to a possible realization of the legitimate receiver in the $(L, N, m)$ S-SSDC problem and is connected to $m$ intermediate nodes through $m$ infinite-capacity channels. Finally, the collection of sets of wiretapped edges $\mathcal{A}$ is defined as

$$\mathcal{A} := \left\{ \{(s, l) | l \in A\} : A \in \Omega_L^{(N)} \right\} \tag{4.23}$$

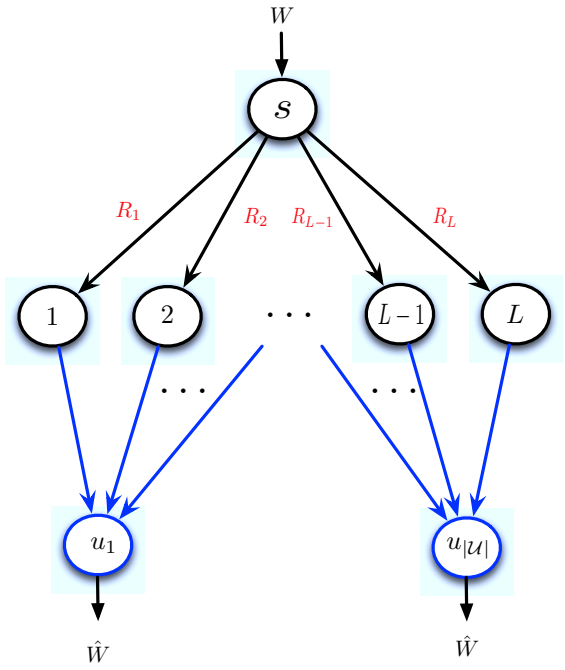



Fig. 11. The $(L, N, m, (R_1, \ldots, R_L))$ wiretap network.

where each set of wiretapped edges in $\mathcal{A}$ corresponds to a possible realization of the eavesdropper in the $(L, N, m)$ S-SSDC problem.

Based on the aforementioned connection between the $(L, N, m)$ S-SSDC problem and the problem of secure coding over the $(L, N, m, (R_1, \ldots, R_L))$ WN, we have the following simple lemma.

**Lemma 2.** *A nonnegative rate tuple $(R_1, \ldots, R_L)$ is admissible for the $(L, N, m)$ S-SSDC problem if the entropy rate of the source is less than or equal to the secrecy capacity of the $(L, N, m, (R_1, \ldots, R_L))$ WN, i.e.,*

$$H(S) \leq C_s(L, N, m, (R_1, \ldots, R_L)). \tag{4.24}$$

In general, characterizing the exact secrecy capacity of a WN can be very difficult. For a generic WN $(\mathcal{G}, s, \mathcal{U}, \mathcal{A})$, the following secrecy rate

$$R_s = \min_{u \in \mathcal{U}, A \in \mathcal{A}} [mincut(s,u) - mincut(s,A)] \tag{4.25}$$

is known [40] to be achievable. Here, $mincut(s,u)$ denotes the value of a minimum cut between the source node $s$ and the user node $u$, and $mincut(s,A)$ denotes the value of a minimum cut between the source node $s$ and the set of wiretapped edges $A$. For the $(L, N, m, (H(S)/(m-N), \ldots, H(S)/(m-N)))$ WN, it is straightforward to verify that

$$mincut(s,u) = \frac{m}{m-N} H(S), \quad \forall u \in \mathcal{U} \tag{4.26}$$

and

$$mincut(s,A) = \frac{N}{m-N} H(S), \quad \forall A \in \mathcal{A}. \tag{4.27}$$

Hence, the secrecy rate

$$R_s = \frac{m}{m-N} H(S) - \frac{N}{m-N} H(S) = H(S) \tag{4.28}$$

is achievable for the $(L, N, m, (H(S)/(m-N), \ldots, H(S)/(m-N)))$ WN. We summarize this result in the following lemma.

**Lemma 3.** *For any $(L, N, m, (H(S)/(m-N), \ldots, H(S)/(m-N)))$ WN, the secrecy capacity can be bounded from below as*

$$C_s(L, N, m, (H(S)/(m-N), \ldots, H(S)/(m-N))) \geq H(S). \tag{4.29}$$

Combining Lemmas 2 and 3 proves the admissibility of the symmetrical rate tuple $(H(S)/(m-N), \ldots, H(S)/(m-N))$.

Building on the previous result, next we show that *every* rate tuple in $\mathcal{R}(L, m-N, H(S))$ is admissible. By Proposition 3, $\mathcal{R}(L, m-N, H(S))$ is a pointed polyhedron

with the characteristic cone given by $\{(R_1, \ldots, R_L) : R_l \geq 0,\ \forall l = 1, \ldots, L\}$. Thus, to show that all rate tuples in $\mathcal{R}(L, m-N, H(S))$ are admissible, it is sufficient to show that all *corner points* of $\mathcal{R}(L, m-N, H(S))$ are admissible.

We shall consider proof by induction, where the induction is on the total number of encoders $L$. First consider the base case with $L = 2$. When $L = 2$, there is only one nontrivial $(L, N, m)$ S-SSDC problem: the $(2, 1, 2)$ S-SSDC problem. Note that the rate region $\mathcal{R}(2, 1, H(S))$ has only one corner point: the symmetrical rate pair $(H(S), H(S))$, whose admissibility has already been established. We thus conclude that every rate tuple in $\mathcal{R}(2, 1, H(S))$ is admissible for the $(2, 1, 2)$ S-SSDC problem.

Now assume that for every nontrivial $(L-1, N', m')$ S-SSDC problem, all rate tuples in $\mathcal{R}(L', m'-N', H(S))$ are admissible. Based on this assumption, next we show that all corner points of $\mathcal{R}(L, m-N, H(S))$ are admissible for the $(L, N, m)$ S-SSDC problem. We shall consider the corner points with all *strictly* positive entries (it they exist) and those with *at least one zero* entry separately:

1) By Proposition 3, the symmetrical rate tuple $(H(S)/(m-N), \ldots, H(S)/(m-N))$ is the *only* corner point of $\mathcal{R}(L, m-N, H(S))$ with all *strictly* positive entries (if it exists), whose admissibility has already been established.

2) To prove the admissibility of the corner points of $\mathcal{R}(L, m-N, H(S))$ with *at least one zero* entry, by the *symmetry* of the rate region $\mathcal{R}(L, m-N, H(S))$ we may consider without loss of generality those with $R_L = 0$. Note that if an $(n, (M_1, \ldots, M_{L-1}))$ code satisfies both asymptotically perfect reconstruction constraint (4.4) and the perfect secrecy constraint (4.5) for the $(L-1, N, m-1)$ S-SSDC problem, an $(n, (M_1, \ldots, M_{L-1}, 1))$ code with the *same* encoding functions for encoders 1 to $L-1$ (encoder $L$ uses a constant encoding function) also satisfies (trivially) both constraints for the $(L, N, m)$ S-SSDC problem.

Thus, if $(R_1, \ldots, R_{L-1})$ is an admissible rate tuple for the $(L-1, N, m-1)$ S-SSDC problem, then $(R_1, \ldots, R_{L-1}, 0)$ is also an admissible rate tuple for the $(L, N, m)$ S-SSDC problem. By the induction assumption, all rate tuples in $\mathcal{R}(L-1, m-N-1, H(S))$ are admissible for the $(L-1, N, m-1)$ problem. Combined with Proposition 3, this implies that all rate tuples in

$$\begin{aligned} \{(R_1, \ldots, R_{L-1}, 0) : (R_1, \ldots, R_{L-1}) \in \mathcal{R}(L-1, m-N-1, H(S))\} \\ = \{(R_1, \ldots, R_L) \in \mathcal{R}(L, m-N, H(S)) : R_L = 0\} \end{aligned} \tag{4.30}$$

i.e., the $R_L = 0$ slice of $\mathcal{R}(L, m-N, H(S))$, are admissible for the $(L, N, m)$ S-SSDC problem. As a special case, all corner points of $\mathcal{R}(L, m-N, H(S))$ with $R_L = 0$ are admissible for the $(L, N, m)$ S-SSDC problem.

Combining Steps 1 and 2 proves that all corner points of $\mathcal{R}(L, m-N, H(S))$ are admissible. We thus conclude that all rate tuples in $\mathcal{R}(L, m-N, H(S))$ are admissible. This completes the induction step and hence the proof of the theorem.

## C. Secure Symmetrical Multilevel Diversity Coding

### 1. Problem Statement

Let $\{S_1[t], \ldots, S_{L-N}[t]\}_{t=1}^{\infty}$ be a collection of $L-N$ independent discrete memoryless sources with time index $t$ and let $S_k^n := (S_k[1], \ldots, S_k[n])$. An $(L, N)$ S-SMDC problem consists of a set of $L$ encoders, a legitimate receiver who has access to a subset $U$ of the encoder outputs, and an eavesdropper who has access to a subset $A$ of the encoder outputs. Which subsets of the encoder outputs are available at the legitimate receiver and the eavesdropper are *unknown* a priori at the encoders. However, no matter which subsets $U$ and $A$ actually occur, the legitimate receiver must be able to asymptotically perfectly reconstruct the sources $(S_1, \ldots, S_k)$ whenever $|U| = N + k$,

and all sources $(S_1, \ldots, S_{L-N})$ must be kept perfectly secure from the eavesdropper as long as $|A| \leq N$.

Formally, an $(n, (M_1, \ldots, M_L))$ code is defined by a collection of $L$ encoding functions

$$e_l : \prod_{k=1}^{L-N} \mathcal{S}_k^n \times \mathcal{K} \to \{1, \ldots, M_l\}, \quad \forall l = 1, \ldots, L \tag{4.31}$$

and decoding functions

$$d_U : \prod_{l \in U} \{1, \ldots, M_l\} \to \prod_{k=1}^{|U|-N} \mathcal{S}_k^n, \quad \forall U \subseteq \Omega_L \text{ s.t. } |U| \geq N+1. \tag{4.32}$$

Here, $\mathcal{K}$ is the key space accessible to all $L$ encoders. A nonnegative rate tuple $(R_1, \ldots, R_L)$ is said to be *admissible* if for every $\epsilon > 0$, there exits, for sufficiently large block length $n$, an $(n, (M_1, \ldots, M_L))$ code such that:

- (Rate constraints)

$$\frac{1}{n} \log M_l \leq R_l + \epsilon, \quad \forall l = 1, \ldots, L; \tag{4.33}$$

- (Asymptotically perfect reconstruction at the legitimate receiver)

$$\Pr\{d_U(X_U) \neq (S_1^n, \ldots, S_{|U|-N}^n)\} \leq \epsilon, \quad \forall U \subseteq \Omega_L \text{ s.t. } |U| \geq N+1 \tag{4.34}$$

  where $X_l := e_l((S_1^n, \ldots, S_{L-N}^n), K)$ is the output of the $l$th encoder, $K$ is the secret key shared by all $L$ encoders, and $X_U := \{X_l : l \in U\}$; and

- (Perfect secrecy at the eavesdropper)

$$H(S_1^n, \ldots, S_{L-N}^n | X_A) = H(S_1^n, \ldots, S_{L-N}^n), \quad \forall A \subseteq \Omega_L \text{ s.t. } |A| \leq N \tag{4.35}$$

  i.e., observing the encoder outputs $X_A$ does not provide *any* information regarding to the source sequences $(S_1^n, \ldots, S_{L-N}^n)$.

## 2. Main Results

Motivated by the success of [36, 37, 38] on the classical SMDC problem without any secrecy constraints, here we focus on superposition coding where the output of the $l$th encoder $X_l$ is given by

$$X_l = \left(X_l^{(1)}, \ldots, X_l^{(L-N)}\right) \tag{4.36}$$

and $X_l^{(k)}$ is the coded message for source $S_k$ at the $l$th encoder using an $(L, N, N+k)$ S-SSDC code. Note here that all sources are encoded *separately* at the encoders, and there is *no* coding across different sources. Thus, if $(R_1^{(k)}, \ldots, R_L^{(k)})$ is an admissible rate tuple for the $(L, N, N+k)$ S-SSDC problem with source $S_k$, then the rate tuple

$$(R_1, \ldots, R_L) = \left(\sum_{k=1}^{L-N} R_1^{(k)}, \ldots, \sum_{k=1}^{L-N} R_L^{(k)}\right) \tag{4.37}$$

is admissible for the $(L, N)$ S-SMDC problem.

By Corollary 16, the minimum sum rate for the $(L, N, N+k)$ S-SSDC problem with source $S_k$ is given by $(L/k)H(S_k)$. It follows that $\sum_{k=1}^{L-N}(L/k)H(S_k)$ is the minimum sum rate that can be achieved by superposition coding for the $(L, N)$ S-SMDC problem. The main result of this section is that $\sum_{k=1}^{L-N}(L/k)H(S_k)$ is in fact the minimum sum rate that can be achieved by *any* coding scheme for the $(L, N)$ S-SMDC problem. Thus, superposition coding is optimal in terms of achieving the minimum sum rate for the general S-SMDC problem. We summarize this result in the following theorem.

**Theorem 17.** *Superposition coding can achieve the minimum sum rate for the general $(L, N)$ S-SMDC problem, which is given by*

$$R_{ms} = \sum_{k=1}^{L-N} \frac{L}{k} H(S_k). \tag{4.38}$$

A proof of the theorem is provided in Section 3. The proof uses an induction argument and is built on the classical subset inequality of Han [33, Chapter 17.6] and the following key proposition.

**Proposition 4.** *For any $(n, (M_1, \ldots, M_L))$ code that satisfies both asymptotically perfect reconstruction constraint* (4.34) *and the perfect secrecy constraint* (4.35)*, we have*

$$H(X_D|S_1^n, \ldots, S_{k-1}^n, X_A) \geq nH(S_k) + H(X_D|S_1^n, \ldots, S_k^n, X_A) - n\delta_k(n, \epsilon) \tag{4.39}$$

*where*

$$\delta_k(n, \epsilon) := 1/n + \epsilon \sum_{\alpha=1}^{k} \log |\mathcal{S}_\alpha| \tag{4.40}$$

*for any $A \in \Omega_L^{(N)}$ and $D \in \Omega_L^{(k)}$ such that $A \cap D = \emptyset$ and any $k = 1, \ldots, L - N$.*

## 3. Proof of the Main Results

Let us first prove Proposition 4. Since $|A| = N$, $|D| = k$, and $A \cap D = \emptyset$, we have $|D \cup A| = N + k$. For any $(n, (M_1, \ldots, M_L))$ code that satisfies both asymptotically perfect reconstruction constraint (4.34) and the perfect secrecy constraint (4.35), we have by Fano's inequality

$$H(S_1^n, \ldots, S_k^n|X_D, X_A) \leq n\delta_k(n, \epsilon) \tag{4.41}$$

and

$$H(S_1^n, \ldots, S_k^n|X_A) = H(S_1^n, \ldots, S_k^n). \tag{4.42}$$

Thus,

$$
\begin{aligned}
& H(X_D|S_1^n,\ldots,S_{k-1}^n,X_A)+n\delta_k(n,\epsilon) \\
&\quad \geq\ H(X_D|S_1^n,\ldots,S_{k-1}^n,X_A)+H(S_1^n,\ldots,S_k^n|X_D,X_A) && (4.43)\\
&\quad \geq\ H(X_D|S_1^n,\ldots,S_{k-1}^n,X_A)+H(S_k^n|S_1^n,\ldots,S_{k-1}^n,X_D,X_A) && (4.44)\\
&\quad =\ H(X_D,S_k^n|S_1^n,\ldots,S_{k-1}^n,X_A) && (4.45)\\
&\quad =\ H(S_k^n|S_1^n,\ldots,S_{k-1}^n,X_A)+H(X_D|S_1^n,\ldots,S_k^n,X_A) && (4.46)\\
&\quad =\ H(S_1^n,\ldots,S_k^n|X_A)-H(S_1^n,\ldots,S_{k-1}^n|X_A) \\
&\qquad\quad +H(X_D|S_1^n,\ldots,S_k^n,X_A) && (4.47)\\
&\quad =\ H(S_1^n,\ldots,S_k^n)-H(S_1^n,\ldots,S_{k-1}^n|X_A) \\
&\qquad\quad +H(X_D|S_1^n,\ldots,S_k^n,X_A) && (4.48)\\
&\quad \geq\ H(S_1^n,\ldots,S_k^n)-H(S_1^n,\ldots,S_{k-1}^n)+H(X_D|S_1^n,\ldots,S_k^n,X_A) && (4.49)\\
&\quad =\ H(S_k^n|S_1^n,\ldots,S_{k-1}^n)+H(X_D|S_1^n,\ldots,S_k^n,X_A) && (4.50)\\
&\quad =\ H(S_k^n)+H(X_D|S_1^n,\ldots,S_k^n,X_A) && (4.51)\\
&\quad =\ nH(S_k)+H(X_D|S_1^n,\ldots,S_k^n,X_A) && (4.52)
\end{aligned}
$$

where (4.43) follows from (4.41), (4.48) follows from (4.42), (4.49) follows from the fact that conditioning reduces entropy, (4.51) follows from the fact that the sources $S_1,\ldots,S_k$ are mutually independent, and (4.52) follows from the fact that the source $S_k$ is memoryless. Moving $n\delta_k(n,\epsilon)$ to the right-hand side of the inequality completes the proof of Proposition 4.

Building on the result of Proposition 4, next let us show that for any $(n,(M_1,\ldots,M_L))$ code that satisfies both asymptotically perfect reconstruction constraint (4.34) and

the perfect secrecy constraint (4.35) and any $\alpha = 1, \ldots, L-N$, we have

$$\sum_{l=1}^{L} H(X_l) \geq \sum_{k=1}^{\alpha} \frac{nL}{k} H(S_k) + \Delta_\alpha - \sum_{k=1}^{\alpha} nL\delta_k(n,\epsilon) \tag{4.53}$$

where

$$\Delta_\alpha := \frac{L}{\begin{pmatrix} L \\ N \end{pmatrix} \begin{pmatrix} L-N \\ \alpha \end{pmatrix}} \sum_{A \in \Omega_L^{(N)}} \sum_{D \in \Omega_{L\setminus A}^{(\alpha)}} \frac{H(X_D | S_1^n, \ldots, S_\alpha^n, X_A)}{\alpha}. \tag{4.54}$$

We shall consider proof by induction, where the induction is on $\alpha$. First consider the base case with $\alpha = 1$. Let $A \in \Omega_L^{(N)}$ and let $l \in \Omega_L \setminus A$. Applying Proposition 4 with $k = 1$, we have

$$H(X_l) \geq nH(S_1) + H(X_l | S_1^n, X_A) - n\delta_1(n,\epsilon). \tag{4.55}$$

Averaging (4.55) over all $l \in \Omega_L \setminus A$ and all $A \in \Omega_L^{(N)}$, we have

$$\frac{1}{\begin{pmatrix} L \\ N \end{pmatrix} \begin{pmatrix} L-N \\ 1 \end{pmatrix}} \sum_{A \in \Omega_L^{(N)}} \sum_{l \in \Omega_L \setminus A} H(X_l) \geq nH(S_1) + \frac{1}{L}\Delta_1 - n\delta_1(n,\epsilon). \tag{4.56}$$

Note that

$$\frac{1}{\begin{pmatrix} L \\ N \end{pmatrix} \begin{pmatrix} L-N \\ 1 \end{pmatrix}} \sum_{A \in \Omega_L^{(N)}} \sum_{l \in \Omega_L \setminus A} H(X_l) = \frac{1}{L} \sum_{l=1}^{L} H(X_l). \tag{4.57}$$

We thus have

$$\sum_{l=1}^{L} H(X_l) \geq nLH(S_1) + \Delta_1 - nL\delta_1(n,\epsilon) \tag{4.58}$$

which completes the proof of the base case.

Now assume that (4.53) holds for $\alpha - 1$ for some $2 \leq \alpha \leq L - N$. Based on

this assumption, next we show that (4.53) also holds for $\alpha$. By the classical subset inequality of Han [33, Chapter 17.6], for any $A \in \Omega_L^{(N)}$ we have

$$\begin{aligned} &\frac{1}{\left(\begin{array}{c} L-N \\ \alpha-1 \end{array}\right)} \sum_{D\in\Omega_{L\setminus A}^{(\alpha-1)}} \frac{H(X_D|S_1^n,\ldots,S_{\alpha-1}^n,X_A)}{\alpha-1} \\ &\qquad \geq \frac{1}{\left(\begin{array}{c} L-N \\ \alpha \end{array}\right)} \sum_{D\in\Omega_{L\setminus A}^{(\alpha)}} \frac{H(X_D|S_1^n,\ldots,S_{\alpha-1}^n,X_A)}{\alpha}. \end{aligned} \tag{4.59}$$

It follows that

$$\Delta_{\alpha-1} \geq \frac{L}{\left(\begin{array}{c} L \\ N \end{array}\right)\left(\begin{array}{c} L-N \\ \alpha \end{array}\right)} \sum_{A\in\Omega_L^{(N)}} \sum_{D\in\Omega_{L\setminus A}^{(\alpha)}} \frac{H(X_D|S_1^n,\ldots,S_{\alpha-1}^n,X_A)}{\alpha}. \tag{4.60}$$

By Proposition 4, for any $A \in \Omega_L^{(N)}$ and any $D \in \Omega_{L\setminus A}^{(\alpha)}$ we have

$$H(X_D|S_1^n,\ldots,S_{\alpha-1}^n,X_A) \geq nH(S_\alpha) + H(X_D|S_1^n,\ldots,S_\alpha^n,X_A) - n\delta_n(\alpha,\epsilon). \tag{4.61}$$

Substituting (4.61) into (4.60) gives

$$\begin{aligned} \Delta_{\alpha-1} &\geq \frac{L}{\left(\begin{array}{c} L \\ N \end{array}\right)\left(\begin{array}{c} L-N \\ \alpha \end{array}\right)} \sum_{A\in\Omega_L^{(N)}} \sum_{D\in\Omega_{L\setminus A}^{(\alpha)}} \\ &\qquad \frac{nH(S_\alpha) + H(X_D|S_1^n,\ldots,S_\alpha^n,X_A) - n\delta_\alpha(n,\epsilon)}{\alpha} \qquad (4.62) \\ &= \frac{nL}{\alpha}H(S_\alpha) + \Delta_\alpha - nL\delta_\alpha(n,\epsilon). \qquad (4.63) \end{aligned}$$

By the induction assumption,

$$\begin{aligned}
\sum_{l=1}^{L} H(X_l) &\geq \sum_{k=1}^{\alpha-1} \frac{nL}{k} H(S_k) + \Delta_{\alpha-1} - \sum_{k=1}^{\alpha-1} nL\delta_k(n,\epsilon) && (4.64)\\
&\geq \sum_{k=1}^{\alpha-1} \frac{nL}{k} H(S_k) + \left( \frac{nL}{\alpha} H(S_\alpha) + \Delta_\alpha - nL\delta_\alpha(n,\epsilon) \right) \\
&\qquad - \sum_{k=1}^{\alpha-1} nL\delta_k(n,\epsilon) && (4.65)\\
&= \sum_{k=1}^{\alpha} \frac{nL}{k} H(S_k) + \Delta_\alpha - \sum_{k=1}^{\alpha} nL\delta_k(n,\epsilon). && (4.66)
\end{aligned}$$

This completes the proof of the induction step and hence (4.53).

Finally, let $\alpha = L - N$ in (4.53). For any admissible rate tuple $(R_1, \ldots, R_L)$ and any $\epsilon > 0$, we have

$$\begin{aligned}
n \sum_{l=1}^{L} (R_l + \epsilon) &\geq \sum_{l=1}^{L} H(X_l) && (4.67)\\
&\geq \sum_{k=1}^{L-N} \frac{nL}{k} H(S_k) + \Delta_{L-N} - \sum_{k=1}^{L-N} nL\delta_k(n,\epsilon) && (4.68)\\
&\geq \sum_{k=1}^{L-N} \frac{nL}{k} H(S_k) - \sum_{k=1}^{L-N} nL\delta_k(n,\epsilon) && (4.69)
\end{aligned}$$

where (4.69) follows from the fact that $\Delta_{L-N} \geq 0$. Divide both sides of (4.69) by $n$ and let $n \to \infty$ and $\epsilon \to 0$. Note that $\delta_k(n,\epsilon) \to 0$ in the limit as $n \to \infty$ and $\epsilon \to 0$ for all $k = 1, \ldots, L - N$. We thus have

$$\sum_{l=1}^{L} R_l \geq \sum_{k=1}^{L-N} \frac{L}{k} H(S_k) \qquad (4.70)$$

for any admissible rate tuple $(R_1, \ldots, R_L)$. This completes the proof of Theorem 17.

## D. Concluding Remarks

This chapter considered the problem of S-SMDC, which is a natural (perhaps also the simplest) extension of the classical SMDC problem [35, 36, 37, 38] to the secrecy communication setting. First, the problem of encoding individual sources, i.e., the S-SSDC problem, was studied. A precise characterization of the entire admissible rate region was established via a connection to the problem of secure coding over a three-layer WN [40] and utilizing some basic polyhedral structure of the admissible rate region. Building on this result, it was then shown that the simple coding strategy of separately encoding individual sources at the encoders (superposition coding) can achieve the minimum sum rate for the general S-SMDC problem.

# CHAPTER V

# CONCLUSIONS

Secure communication under channel uncertainty is an important and challenging problem in physical-layer security and cryptography. In this dissertation, we take a fundamental information-theoretic view at three concrete settings and use them to shed insight into efficient secure communication techniques for different scenarios under channel uncertainty.

First, a multi-input multi-output (MIMO) Gaussian broadcast channel with two receivers and two messages: a common message intended for both receivers (i.e., channel uncertainty for decoding the common message at the receivers) and a confidential message intended for one of the receivers but needing to be kept asymptotically perfectly secret from the other is considered. A matrix characterization of the secrecy capacity region is established via a channel-enhancement argument and an extremal entropy inequality previously established for characterizing the capacity region of a degraded compound MIMO Gaussian broadcast channel.

Second, a multilevel security wiretap channel where there is one possible realization for the legitimate receiver channel but multiple possible realizations for the eavesdropper channel (i.e., channel uncertainty at the eavesdropper) is considered. A coding scheme is designed such that the number of secure bits delivered to the legitimate receiver depends on the actual realization of the eavesdropper channel. More specifically, when the eavesdropper channel realization is weak, all bits delivered to the legitimate receiver need to be secure. In addition, when the eavesdropper channel realization is strong, a prescribed part of the bits needs to remain secure. We call

such codes security embedding codes, referring to the fact that high-security bits are now embedded into the low-security ones. We show that the key to achieving efficient security embedding is to jointly encode the low-security and high-security bits. In particular, the low-security bits can be used as (part of) the transmitter randomness to protect the high-security ones.

Finally, motivated by the recent interest in building secure, robust and efficient distributed information storage systems, the problem of secure symmetrical multilevel diversity coding (S-SMDC) is considered. This is a setting where there are channel uncertainties at both the legitimate receiver and the eavesdropper. The problem of encoding individual sources is first studied. A precise characterization of the entire admissible rate region is established via a connection to the problem of secure coding over a three-layer wiretap network and utilizing some basic polyhedral structure of the admissible rate region. Building on this result, it is then shown that the simple coding strategy of separately encoding individual sources at the encoders can achieve the minimum sum rate for the general S-SMDC problem.

Several topics are worthy of future research. First, in Chapter III, it was shown that the high-security message can be embedded into the low-security message at full rate without incurring any loss on the overall rate of communication for both scalar and independent parallel Gaussian channels (under an average individual per-subchannel power constraint). The scenarios with multiple transmit and receive antennas are considerably more complex and hence require further investigations.

Second, in Chapter III, we consider secure communication with one legitimate receiver and one eavesdropper having multiple possible realizations. Which eavesdropper channel realization will occur is *unknown* to the transmitter. The number of *secure* bits delivered to the legitimate receiver depends on the actual realization of the eavesdropper channel. In many applications, however, security needs to be guar-

anteed in that all bits delivered to the legitimate receiver need to be secure, no matter which eavesdropper channel realization materializes. This communication scenario is captured by a compound wiretap channel model [44], which can be viewed as a wiretap channel with one legitimate receiver and multiple eavesdroppers. The transmitter wishes to transmit information to the legitimate receiver but keep it secret from *all* eavesdroppers. When all the eavesdropper channels are degraded with respect to the legitimate receiver channel, the secrecy capacity of this channel is known [44]. Without the degradedness assumption, however, the secrecy capacity of the compound wiretap channel remains *unknown* in general. In [45], Liu *et al.* characterized the secrecy capacity of the parallel Gaussian compound wiretap channel. The proposed coding scheme in [45] to achieve the secrecy capacity is binning over a *product* codebook, which is very specific for the parallel setting and hard to extend to the more general MIMO setting. In [46], we proposed an alternative simple coding schemes combining the security embedding codes with secure network coding. Generalizing our coding schemes to MIMO settings may be worthy to investigate.

Lastly, based on the result of Theorem 17 in Chapter IV (and the fact that superposition coding can achieve the entire admissible rate region for the classical SMDC problems without secrecy constraints), it is very tempting to conjecture that superposition coding can in fact achieve the entire admissible rate region for the general S-SMDC problem. In Appendix E, we verify that this is indeed the case for the simplest nontrivial S-SMDC problem: the $(3, 1)$ S-SMDC problem. Our proof relies on an *explicit* characterization of the superposition coding rate region via a Fourier-Motzkin elimination procedure. The optimality of superposition coding is then established by carefully using the results of Proposition 4.

Extending such a proof strategy to the general $(L, N)$ S-SMDC problem, however, faces a number of challenges. To begin with, the complexity of Fourier-Motzkin

elimination procedure grows unboundedly as the total number of encoders $L$ increases. Thus, establishing an explicit characterization of the superposition coding rate region for the general $(L, N)$ S-SMDC problem appears to be very difficult. An alternative strategy is to look for an *implicit* characterization of the superposition coding rate region using *optimal $\alpha$-resolutions*, similar to that [38] for the classical SMDC problem without any secrecy constraints. In fact, note from Theorem 15 that the admissible rate region of an $(L, N, m)$ S-SSDC problem depends on the parameters $N$ and $m$ only via its difference $m - N$. As mentioned previously in Section B, when $N = 0$, the $(L, N, m)$ S-SSDC problem reduces to the classical $(L, m)$ SSDC problem without any secrecy constraints. Thus, the admissible rate region of the $(L, N, N + k)$ S-SSDC problem with source $S_k$ is *identical* to that of the classical $(L, k)$ SSDC problem with the same source. As a result, the superposition coding rate region of the $(L, N)$ S-SMDC problem with sources $(S_1, \ldots, S_{L-N})$ is *identical* to the superposition coding rate region of the classical SMDC problem with a total of $L$ encoders and sources $(S_1, \ldots, S_L)$ where the entropy rate of the source $H(S_l) = 0$ for $l = L - N + 1, \ldots, L$. Based on this observation, the $\alpha$-resolution characterization of the superposition coding rate region for the general SMDC problem can be directly translated to the S-SMDC problem. It remains to see whether the properties provided in [38] on optimal $\alpha$-resolutions are sufficient for establishing the optimality of superposition coding for the general S-SMDC problem. This problem is currently under our investigations.

# REFERENCES

[1] C. Kaufman, R. Perlman, and M. Speciner, *Network Security: Private Communication in a Public World*, 2nd Edition. New Jersey: Prentice Hall, 2002.

[2] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp 656–715, 1949.

[3] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[4] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Info. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[5] S. K. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Info. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.

[6] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," in *Proc. 44th Annu. Allerton Conf. Communication, Control and Computing*, Monticello, IL, Sep. 2006.

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

[8] R. Liu and W. Trappe, Eds, *Securing Wireless Communications at the Physical Layer*. New York: Springer Verlag, 2010.

[9] H. D. Ly, T. Liu, and Y. Liang, "Multiple-input multiple-output Gaussian broadcast channels with common and confidential messages," *IEEE Trans. Info. Theory*, vol. 56, no. 11, pp. 5477-5487, Nov. 2010.

[10] H. D. Ly, T. Liu, and Y. Blankenship, "Security embedding codes," *IEEE Trans. Info. Forensics and Security*, vol. 7, no. 1, pp. 148-159, Feb. 2012.

[11] A. Balasubramanian, H. D. Ly, S. Li, T. Liu, and S. L. Miller, "Secure symmetrical multilevel diversity coding," *IEEE Trans. Info. Theory*, submitted for publication, May 2011.

[12] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel," *IEEE Trans. Info. Theory*, vol. 55, no. 9, Sep. 2009.

[13] A. Khisti, G. W. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," in *Proc. IEEE Int. Symp. Inform. Theory*, Nice, France, Jun. 2007.

[14] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas: The MIMOME channel," *IEEE Trans. Info. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[15] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. IEEE Int. Symp. Info. Theory*, Toronto, Canada, Jul. 2008.

[16] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Info. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[17] H. Sato, "An outer bound to the capacity region of broadcast channels," *IEEE Trans. Info. Theory*, vol. IT-24, no. 3, pp. 374–377, May 1978.

[18] H. Weingarten, Y. Steinberg, and S. Shamai (Shitz), "The capacity region of the Gaussian multiple-input-multiple-output broadcast channel," *IEEE Trans. Info. Theory*, vol. 52, no. 9, pp. 3936–3964, Sep. 2006.

[19] S. N. Diggavi and T. M. Cover, "The worst additive noise under a covariance constraint," *IEEE Trans. Info. Theory*, vol. 47, no. 7, pp. 3072–3081, Nov. 2001.

[20] H. Weingarten, T. Liu, S. Shamai (Shitz), Y. Steinberg, and P. Viswanath, "The capacity region of the degraded multiple-input multiple-output compound broadcast channel," *IEEE Trans. Info. Theory*, vol. 55, no. 11, pp. 5011–5023, Nov. 2009.

[21] S. Boyd and L. Vandenberghe, *Convex Optimization*. New York: Cambridge University Press, 2004.

[22] P. P. Bergman, "Random coding theorem for broadcast channels with degraded components," *IEEE Trans. Info. Theory*, vol. IT-19, no. 3, pp. 197–207, Mar. 1973.

[23] J. A. Thomas, "Feedback can at most double Gaussian multiple access channel capacity," *IEEE Trans. Info. Theory*, vol. IT-33, no. 5, pp. 711–716, Sep. 1987.

[24] M. Grant and S. Boyd, *CVX: Matlab software for disciplined convex programming*. Available: `http://stanford.edu/~boyd/cvx`, Feb. 2009.

[25] H. Weingarten, Y. Steinberg, and S. Shamai (Shitz), "On the capacity region of the multi-antenna broadcast channel with common messages," in *Proc. IEEE Int. Symp. Info. Theory*, Seattle, WA, Jul. 2006.

[26] J. Körner and K. Marton, "General broadcast channels with degraded message sets," *IEEE Trans. Info. Theory*, vol. IT-23, no. 1, pp. 60–64, Jan. 1977.

[27] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz), "MIMO Gaussian broadcast channels with confidential and common messages," in *Proc. IEEE Int. Symp. Inf. Theory*, Austin, TX, Jun. 2010.

[28] E. Ekrem and S. Ulukus, "Gaussian MIMO broadcast channels with common and confidential messages," in *Proc. IEEE Int. Symp. Inf. Theory*, Austin, TX, Jun. 2010.

[29] Y. Liang, L. Lai, H. V. Poor, and S. Shamai (Shitz), "The broadcast approach to fading wiretap channels," in *Proc. IEEE Inf. Theory Workshop*, Taormina, Sicily, Italy, Oct. 2009.

[30] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Budapest, Hungary: Academic Press, 1982.

[31] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz), "New results on multiple-input multiple-output Gaussian broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, submitted for publication. Available: `http://arxiv.org/abs/1101.2007`

[32] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," *Bell Syst. Tech. J.*, vol. 63, no. 10, pp. 2135–2157, Dec. 1984.

[33] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd Edition, New York: Wiley, 2006.

[34] Y. K. Chia and A. El Gamal, "3-receiver broadcast channels with common and confidential messages," *IEEE Trans. Inf. Theory*, submitted for publication. Available: `http://arxiv.org/abs/0910.1407`

[35] J. R. Roche, "Distributed information storage," *Ph.D. Dissertation*, Stanford University, Stanford, CA, Mar. 1992.

[36] R. W. Yeung, "Multilevel diversity coding with distortion," *IEEE Trans. Inf. Theory*, vol. 41, pp. 412–422, Mar. 1995.

[37] J. R. Roche, R. W. Yeung, and K. P. Hau, "Symmetrical multilevel diversity coding," *IEEE Trans. Inf. Theory*, vol. 43, pp. 1059–1064, May 1997.

[38] R. W. Yeung and Z. Zhang, "On symmetrical multilevel diversity coding," *IEEE Trans. Inf. Theory*, vol. 45, pp. 609–621, Mar. 1999.

[39] R. C. Singleton, "Maximum distance $q$-nary codes," *IEEE Trans. Inf. Theory*, vol. IT-10, pp. 116–118, Apr. 1964.

[40] N. Cai and R. W. Yeung, "Secure network coding on a wiretap network," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 424-435, Jan. 2011.

[41] A. Shamir, "How to share a secret," *Comm. ACM*, vol. 22, pp. 612–613, Nov. 1979.

[42] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. National Computer Conference*, New York, NY, Jun. 1979, vol. 48, pp. 313–317.

[43] C. Chekuri, *Lecture Notes on Combinatorial Optimization*. University of Illinois, Urbana-Champaign, IL. Available: `http://www.cs.illinois.edu/class/sp10/cs598csc/`

[44] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz), "Compound wiretap channels," in *Proc. 45th Annu. Allerton Conf. Communication, Control and Computing* Monticello, IL, Sep. 2007.

[45] T. Liu, V. Prabhakaran, and S. Vishwanath, "The secrecy capacity of a class of parallel Gaussian compound wiretap channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, Canada, Jul. 2008.

[46] H. D. Ly, T. Liu, and Y. Blankenship, "Security embedding codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Austin, TX, Jun. 2010.

# APPENDIX A

## THE CONVERSE PART OF PROPOSITION 1

In this appendix, we prove the converse part of Proposition 1. Here, we use $X_i^j$ to denote the vector $(X[i], X[i+1], \ldots, X[j])$, and when $i = 1$, we further simplify the notation by using $X^j$ to denote the vector $(X[1], X[2], \ldots, X[j])$. We also use $X_i$ to denote $X[i]$.

We consider a $\left(2^{nR_0}, 2^{nR_1}, n\right)$ code with the average block error probability $P_e^{(n)}$. Then we have the following joint probability distribution

$$p(w_0, w_1, x^n, \tilde{y}_{1a}^n, y_{1b}^n, y_2^n) = p(w_0)p(w_1)p(x^n|w_0w_1)\prod_{i=1}^{n}[p(\tilde{y}_{1ai}|x_i)p(y_{1bi}y_{2i}|\tilde{y}_{1ai})]. \quad \text{(A.1)}$$

By Fano's inequality, we have

$$H(W_0|Y_{1b}^n) \leq nR_0P_e^{(n)} + 1 := n\delta_{1n} \quad \text{(A.2)}$$

$$H(W_0|Y_2^n) \leq nR_0P_e^{(n)} + 1 := n\delta_{1n} \quad \text{(A.3)}$$

$$H(W_1|\tilde{Y}_{1a}^n) \leq nR_1P_e^{(n)} + 1 := n\delta_{2n} \quad \text{(A.4)}$$

where $\delta_{1n}, \delta_{2n} \to 0$ if $P_e^{(n)} \to 0$.

We define the following auxiliary random variable:

$$U_i := (W_0, \tilde{Y}_{1a}^{i-1}) \quad \text{(A.5)}$$

which satisfies the Markov chain relationship

$$U_i \to X_i \to (\tilde{Y}_{1ai}, Y_{1bi}, Y_{2i}).$$

We first bound $R_0$ as follows.

$$\begin{aligned} nR_0 = H(W_0) &\leq I(W_0; Y_{1b}^n) + n\delta_{1n} && \text{(A.6)} \\ &= \sum_{i=1}^{n} I(W_0; Y_{1bi}|Y_{1b}^{i-1}) + n\delta_{1n} \\ &\leq \sum_{i=1}^{n} I(W_0, \tilde{Y}_{1a}^{i-1}; Y_{1bi}|Y_{1b}^{i-1}) + n\delta_{1n} \\ &\leq \sum_{i=1}^{n} I(W_0, \tilde{Y}_{1a}^{i-1}, Y_{1b}^{i-1}; Y_{1bi}) + n\delta_{1n} \\ &\leq \sum_{i=1}^{n} I(W_0, \tilde{Y}_{1a}^{i-1}; Y_{1bi}) + n\delta_{1n} && \text{(A.7)} \\ &\leq \sum_{i=1}^{n} I(U_i; Y_{1bi}) + n\delta_{1n} && \text{(A.8)} \end{aligned}$$

where (A.6) follows from Fano's inequality (A.2), and (A.7) follows from the degradedness condition, i.e., $(W_0, Y_{1bi}) \to \tilde{Y}_{1a}^{i-1} \to Y_{1b}^{i-1}$. We can follow the steps similar to those in (A.6)-(A.8) with $Y_{1b}$ being replaced by $Y_2$, and obtain the following bound

$$nR_0 \leq \sum_{i=1}^{n} I(U_i; Y_{2i}) + n\delta_{1n}. \quad \text{(A.9)}$$

We now bound $nR_1$ and obtain

$$
\begin{aligned}
nR_1 &= H(W_1|Y_2^n) && \text{(A.10)}\\
&= H(W_1|W_0, Y_2^n) + I(W_1; W_0|Y_2^n)\\
&\leq H(W_1|W_0, Y_2^n) + n\delta_{1n}\\
&= I(W_1; \tilde{Y}_{1a}^n|W_0, Y_2^n) + H(W_1|W_0, Y_2^n, \tilde{Y}_{1a}^n) + n\delta_{1n}\\
&\leq I(W_1; \tilde{Y}_{1a}^n|W_0, Y_2^n) + n\delta_{2n} + n\delta_{1n} && \text{(A.11)}\\
&\leq I(W_1, X^n; \tilde{Y}_{1a}^n|W_0, Y_2^n) + n\delta_{2n} + n\delta_{1n}\\
&= I(X^n; \tilde{Y}_{1a}^n|W_0, Y_2^n) + n\delta_{2n} + n\delta_{1n} && \text{(A.12)}\\
&= H(X^n|W_0, Y_2^n) - H(X^n|W_0, Y_2^n, \tilde{Y}_{1a}^n) + n\delta_{2n} + n\delta_{1n}\\
&= H(X^n|W_0, Y_2^n) - H(X^n|W_0, \tilde{Y}_{1a}^n) + n\delta_{2n} + n\delta_{1n} && \text{(A.13)}\\
&= I(X^n; \tilde{Y}_{1a}^n|W_0) - H(X^n; Y_2^n|W_0) + n\delta_{2n} + n\delta_{1n}\\
&= \sum_{i=1}^{n} \Big[ I(X^n; \tilde{Y}_{1ai}|\tilde{Y}_{1a}^{i-1}, W_0) - I(X^n; Y_{2i}|Y_2^{i-1}, W_0) \Big] + n\delta_{2n} + n\delta_{1n}\\
&= \sum_{i=1}^{n} \Big[ H(\tilde{Y}_{1ai}|\tilde{Y}_{1a}^{i-1}, W_0) - H(\tilde{Y}_{1ai}|\tilde{Y}_{1a}^{i-1}, W_0, X^n)\\
&\qquad - H(Y_{2i}|Y_2^{i-1}, W_0) + H(Y_{2i}|Y_2^{i-1}, W_0, X^n) \Big] + n\delta_{2n} + n\delta_{1n}\\
&\leq \sum_{i=1}^{n} \Big[ H(\tilde{Y}_{1ai}|\tilde{Y}_{1a}^{i-1}, W_0) - H(\tilde{Y}_{1ai}|\tilde{Y}_{1a}^{i-1}, W_0, X_i)\\
&\qquad - H(Y_{2i}|\tilde{Y}_{1a}^{i-1}, Y_2^{i-1}, W_0) + H(Y_{2i}|Y_2^{i-1}, W_0, X_i) \Big] + n\delta_{2n} + n\delta_{1n} && \text{(A.14)}\\
&\leq \sum_{i=1}^{n} \Big[ H(\tilde{Y}_{1ai}|\tilde{Y}_{1a}^{i-1}, W_0) - H(\tilde{Y}_{1ai}|\tilde{Y}_{1a}^{i-1}, W_0, X_i)\\
&\qquad - H(Y_{2i}|\tilde{Y}_{1a}^{i-1}, W_0) + H(Y_{2i}|\tilde{Y}_{1a}^{i-1}, W_0, X_i) \Big] + n\delta_{2n} + n\delta_{1n} && \text{(A.15)}\\
&= \sum_{i=1}^{n} \Big[ I(X_i; \tilde{Y}_{1ai}|U_i) - I(X_i; Y_{2i}|U_i) \Big] + n\delta_{2n} + n\delta_{1n} && \text{(A.16)}
\end{aligned}
$$

where (A.10) follows from perfect secrecy condition, (A.11) follows from Fano's in-

equality, (A.12) follows from the Markov chain $(W_0, W_1) \to (X^n, Y_2^n) \to \tilde{Y}_{1a}^n$, (A.13) follows from the degradedness condition, i.e., $(X^n, W_0) \to \tilde{Y}_{1a}^n \to Y_2^n$, (A.14) follows from the Markov chain relationship $(\tilde{Y}_{1a}^{i-1}, W_0, X^n) \to X_i \to \tilde{Y}_{1ai}$ and conditioning does not increase entropy, and (A.15) follows from the Markov chain relationships $(Y_{2i}, W_0) \to \tilde{Y}_{1a}^{i-1} \to Y_2^{i-1}$ and $(Y_2^{i-1}, \tilde{Y}_{1a}^{i-1}, W_0) \to X_i \to Y_{2i}$.

The single-letter outer bound can be obtained by letting $J$ be a time-sharing variable uniformly distributed over $\{1, \ldots, n\}$, and define $U = (U_J, J)$, $X = X_J$, $\tilde{Y}_{1a} = \tilde{Y}_{1aJ}$, $Y_{1b} = Y_{1bJ}$, and $Y_2 = Y_{2J}$.

# APPENDIX B

## PROOF OF THEOREM 7

Assume that the channel output $Y$ is less noisy than $Z_2$. To show that in this case the sufficient condition (3.9) is also necessary, let $(R_1, R_2)$ be an achievable rate pair. By Fano's inequality [33] and the asymptotic perfect secrecy constraints (3.1) and (3.2), there exists a sequence of codes (indexed by the block length $n$) of rate pair $(R_1, R_2)$ such that

$$\begin{aligned} H(M_1, M_2|Y^n) &\leq n\epsilon_n/2 && \text{(B.1)} \\ I(M_1; Z_1^n) &\leq n\epsilon_n/2 && \text{(B.2)} \\ \text{and} \quad I(M_1, M_2; Z_2^n) &\leq n\epsilon_n/2 && \text{(B.3)} \end{aligned}$$

where $\epsilon_n \to 0$ in the limit as $n \to \infty$.

Let $M := (M_1, M_2)$, $Y^{i-1} := (Y[1], \ldots, Y[i-1])$, $Z_{1,i+1}^n := (Z_1[i+1], ..., Z_1[n])$, and $Z_{2,i+1}^n := (Z_2[i+1], ..., Z_2[n])$. By (B.1) and (B.2), we have

$$\begin{aligned} n(R_1 - \epsilon_n) &= H(M_1) - n\epsilon_n && \text{(B.4)} \\ &\leq H(M_1) - [I(M_1; Z_1^n) + H(M_1, M_2|Y^n)] && \text{(B.5)} \\ &= H(M_1|Z_1^n) - H(M_1, M_2|Y^n) && \text{(B.6)} \\ &\leq H(M_1, M_2|Z_1^n) - H(M_1, M_2|Y^n) && \text{(B.7)} \\ &= I(M_1, M_2; Y^n) - I(M_1, M_2; Z_1^n) && \text{(B.8)} \\ &= I(M; Y^n) - I(M; Z_1^n) && \text{(B.9)} \\ &= \sum_{i=1}^{n} \left[ I(M; Y[i]|Y^{i-1}) - I(M; Z_1[i]|Z_{1,i+1}^n) \right] && \text{(B.10)} \\ &= \sum_{i=1}^{n} \left[ I(M; Y[i]|Y^{i-1}, Z_{1,i+1}^n) - I(M; Z_1[i]|Y^{i-1}, Z_{1,i+1}^n) \right] && \text{(B.11)} \end{aligned}$$

where (B.11) follows from the well-known Csiszár-Körner sum equality [4]. Similarly, by (B.1), (B.3), and the Csiszár-Körner sum equality [4], we may also obtain

$$n(R_1 + R_2 - \epsilon_n) \leq \sum_{i=1}^{n} \left[ I(M; Y[i]|Y^{i-1}, Z_{2,i+1}^n) - I(M; Z_2[i]|Y^{i-1}, Z_{2,i+1}^n) \right]. \quad \text{(B.12)}$$

Further note that

$$\begin{aligned}
& I(M; Y[i]|Y^{i-1}, Z_{2,i+1}^n) - I(M; Z_2[i]|Y^{i-1}, Z_{2,i+1}^n) \\
&= I(M, Y^{i-1}, Z_{2,i+1}^n; Y[i]) - I(M, Y^{i-1}, Z_{2,i+1}^n; Z_2[i]) \\
&\quad - \left[ I(Y^{i-1}, Z_{2,i+1}^n; Y[i]) - I(Y^{i-1}, Z_{2,i+1}^n; Z_2[i]) \right] && \text{(B.13)} \\
&= I(M, Y^{i-1}, Z_{2,i+1}^n, Z_{1,i+1}^n; Y[i]) - I(M, Y^{i-1}, Z_{2,i+1}^n, Z_{1,i+1}^n; Z_2[i]) \\
&\quad - \left[ I(Z_{1,i+1}^n; Y[i]|M, Y^{i-1}, Z_{2,i+1}^n) - I(Z_{1,i+1}^n; Z_2[i]|M, Y^{i-1}, Z_{2,i+1}^n) \right] \\
&\quad - \left[ I(Y^{i-1}, Z_{2,i+1}^n; Y[i]) - I(Y^{i-1}, Z_{2,i+1}^n; Z_2[i]) \right] && \text{(B.14)} \\
&\leq I(M, Y^{i-1}, Z_{2,i+1}^n, Z_{1,i+1}^n; Y[i]) - I(M, Y^{i-1}, Z_{2,i+1}^n, Z_{1,i+1}^n; Z_2[i]) && \text{(B.15)} \\
&= I(M, Y^{i-1}, Z_{1,i+1}^n; Y[i]) + I(Z_{2,i+1}^n; Y[i]|M, Y^{i-1}, Z_{1,i+1}^n) \\
&\quad - \left[ I(M, Y^{i-1}, Z_{1,i+1}^n; Z_2[i]) + I(Z_{2,i+1}^n; Z_2[i]|M, Y^{i-1}, Z_{1,i+1}^n) \right] && \text{(B.16)} \\
&= I(M, Y^{i-1}, Z_{1,i+1}^n; Y[i]) - I(M, Y^{i-1}, Z_{1,i+1}^n; Z_2[i]) && \text{(B.17)}
\end{aligned}$$

where (B.15) is due to the fact that $Y$ is less noisy than $Z_2$ so we have

$$\begin{aligned}
I(Z_{1,i+1}^n; Y[i]|M, Y^{i-1}, Z_{2,i+1}^n) &\geq I(Z_{1,i+1}^n; Z_2[i]|M, Y^{i-1}, Z_{2,i+1}^n) && \text{(B.18)} \\
\text{and} \quad I(Y^{i-1}, Z_{2,i+1}^n; Y[i]) &\geq I(Y^{i-1}, Z_{2,i+1}^n; Z_2[i]) && \text{(B.19)}
\end{aligned}$$

and (B.17) is due to the Markov chain $Z_{2,i+1}^n \to (M, Y^{i-1}, Z_{1,i+1}^n) \to (Y[i], Z_2[i])$ so we have

$$I(Z_{2,i+1}^n; Y[i]|M, Y^{i-1}, Z_{1,i+1}^n) = I(Z_{2,i+1}^n; Z_2[i]|M, Y^{i-1}, Z_{1,i+1}^n) = 0. \quad \text{(B.20)}$$

Substituting (B.17) into (B.12), we have

$$n(R_1 + R_2 - \epsilon_n) \leq \sum_{i=1}^{n} \left[ I(M, Y^{i-1}, Z_{1,i+1}^n; Y[i]) - I(M, Y^{i-1}, Z_{1,i+1}^n; Z_2[i]) \right]. \quad \text{(B.21)}$$

Define $U[i] := (Y^{i-1}, Z_{1,i+1}^n)$, and $V[i] := (U[i], M)$. We can rewrite (B.11) and (B.21) as

$$n(R_1 - \epsilon_n) \leq \sum_{i=1}^{n} \left[ I(V[i]; Y[i]|U[i]) - I(V[i]; Z_1[i]|U[i]) \right] \quad \text{(B.22)}$$

$$\text{and} \quad n(R_1 + R_2 - \epsilon_n) \leq \sum_{i=1}^{n} \left[ I(V[i]; Y[i]) - I(V[i]; Z_2[i]) \right]. \quad \text{(B.23)}$$

Let $Q$ be a standard time-sharing variable [33], and let $U := (U[Q], Q)$, $V := (V[Q], Q)$, $X := X[Q]$, $Y := Y[Q]$, $Z_1 := Z_1[Q]$, $Z_2 := Z_2[Q]$. We have from (B.22) and (B.23)

$$\begin{aligned}
& n(R_1 - \epsilon_n) \\
& \quad \leq n \left[ I(V[Q]; Y[Q]|U[Q], Q) - I(V[Q]; Z_1[Q]|U[Q], Q) \right] && \text{(B.24)} \\
& \quad = n \left[ I(V[Q], Q; Y[Q]|U[Q], Q) - I(V[Q], Q; Z_1[Q]|U[Q], Q) \right] && \text{(B.25)} \\
& \quad = n \left[ I(V; Y|U) - I(V; Z_1; |U) \right] && \text{(B.26)} \\
& \text{and} \quad n(R_1 + R_2 - \epsilon_n) \\
& \quad \leq n \left[ I(V[Q]; Y[Q]|Q) - I(V[Q]; Z_2[Q]|Q) \right] && \text{(B.27)} \\
& \quad = n \left[ I(V[Q], Q; Y[Q]) - I(V[Q], Q; Z_2[Q]) \right] \\
& \qquad - n \left[ I(Q; Y[Q]) - I(Q; Z_2[Q]) \right] && \text{(B.28)} \\
& \quad \leq n \left[ I(V[Q], Q; Y[Q]) - I(V[Q], Q; Z_2[Q]) \right] && \text{(B.29)} \\
& \quad = n \left[ I(V; Y) - I(V; Z_2) \right] && \text{(B.30)}
\end{aligned}$$

where (B.29) is due to the fact that $Y$ is less noisy than $Z_2$ so we have

$$I(Q; Y[Q]) \geq I(Q; Z_2[Q]). \tag{B.31}$$

Divide both sides of (B.26) and (B.30) by $n$ and then let $n \to \infty$. The proof is complete by noting that the channel is memoryless, so we have $U[i] \to V[i] \to X[i] \to (Y[i], Z_1[i], Z_2[i])$ for all $i = 1, \ldots, n$.

# APPENDIX C

## EXISTENCE OF AN $H$ WITH $\Psi(H) = 0$

To show that there exists a parity-check matrix $H$ such that $\Psi(H) = 0$, it is sufficient to show that $\mathbb{E}\Psi(H) < 1$ where $\mathbb{E}X$ denotes the expectation of a random variable $X$.

Let

$$\Psi_0(H) := \begin{cases} 1, & \text{rank}(H) < n(1 - \alpha_2 - \epsilon) \\ 0, & \text{otherwise} \end{cases} \tag{C.1}$$

and

$$\Psi_i(H, \Gamma) := \begin{cases} 1, & D_i(\Gamma) < n(1 - \alpha_i - \epsilon) - 3/\epsilon \\ 0, & \text{otherwise,} \end{cases} \qquad i = 1, 2. \tag{C.2}$$

By the union bound,

$$\mathbb{E}\Psi(H) \leq \mathbb{E}\Psi_0(H) + \sum_{i=1}^{2} \sum_{\substack{\Gamma \subseteq \{1,\ldots,n\} \\ |\Gamma| = n\alpha_i}} \mathbb{E}\Psi_i(H, \Gamma). \tag{C.3}$$

Following [32, Lemma 6], we have

$$\mathbb{E}\Psi_0(H) \leq \frac{n(1 - \alpha_2 - \epsilon)2^{-n(\alpha_2+\epsilon)}}{1 - 2^{-n(\alpha_2+\epsilon)}} < \frac{1}{2} \tag{C.4}$$

for sufficiently large $n$. Furthermore, by [32, Lemma 5], for any $\Gamma \subseteq \{1, \ldots, n\}$ such that $|\Gamma| = n\alpha_i$, we have

$$\mathbb{E}\Psi_i(H, \Gamma) \leq 2^{-3n+n(1-\alpha_i-\epsilon)} \leq 2^{-2n}. \tag{C.5}$$

Since the total number of different subsets of $\{1, \ldots, n\}$ is $2^n$, we have

$$\sum_{i=1}^{2} \sum_{\substack{\Gamma \subseteq \{1,\ldots,n\} \\ |\Gamma| = n\alpha_i}} \mathbb{E}\Psi_i(H, \Gamma) \leq 2 \cdot 2^n \cdot 2^{-2n} = 2^{-n+1} < \frac{1}{2} \tag{C.6}$$

for any $n > 2$. Substituting (C.4) and (C.6) into (C.3) proves that $\mathbb{E}\Psi(H) < 1$ for sufficiently large $n$, and hence the existence of a parity-check matrix $H$ such that $\Psi(H) = 0$.

# APPENDIX D

## PROOF OF LEMMA 1

Let $D \in \Omega_L^{(m-N)}$ and let $A \in \Omega_{L\setminus D}^{(N)}$. Since $A \cap D = \emptyset$, we have $|D \cup A| = N + (m - N) = m$. For any $(n, (M_1, \ldots, M_L))$ code that satisfies both asymptotically perfect reconstruction constraint (4.4) and the perfect secrecy constraint (4.5), we have by Fano's inequality

$$H(S^n|X_D, X_A) \leq n\delta(n, \epsilon) \tag{D.1}$$

where

$$\delta(n, \epsilon) = 1/n + \epsilon \log |\mathcal{S}| \tag{D.2}$$

and

$$H(S^n|X_A) = H(S^n). \tag{D.3}$$

For any admissible rate tuple $(R_1, \ldots, R_L)$ and any $\epsilon > 0$, we have

$$\begin{aligned}
n \sum_{l \in D} (R_l + \epsilon) &\geq \sum_{l \in D} H(X_l) && \text{(D.4)}\\
&\geq H(X_D) && \text{(D.5)}\\
&\geq H(X_D|X_A) && \text{(D.6)}\\
&\geq H(X_D|X_A) + H(S^n|X_D, X_A) - n\delta(n, \epsilon) && \text{(D.7)}\\
&= H(X_D, S^n|X_A) - n\delta(n, \epsilon) && \text{(D.8)}\\
&= H(S^n|X_A) + H(X_D|S^n, X_A) - n\delta(n, \epsilon) && \text{(D.9)}\\
&\geq H(S^n|X_A) - n\delta(n, \epsilon) && \text{(D.10)}\\
&= H(S^n) - n\delta(n, \epsilon) && \text{(D.11)}\\
&= nH(S) - n\delta(n, \epsilon) && \text{(D.12)}
\end{aligned}$$

where (D.5) follows from the independence bound on entropy, (D.6) follows from the fact that conditioning reduces entropy, (D.7) follows from (D.1), (D.11) follows from (D.3), and (D.12) follows from the fact that the source $S$ is memoryless. Divide both sides of (D.12) by $n$ and let $n \to \infty$ and $\epsilon \to 0$. Note that $\delta(n, \epsilon) \to 0$ in the limit as $n \to \infty$ and $\epsilon \to 0$. We have from (D.12) that

$$\sum_{l \in D} R_l \geq H(S), \quad \forall D \in \Omega_L^{(m-N)}. \tag{D.13}$$

This completes the proof of Lemma 1.

# APPENDIX E

## THE ADMISSIBLE RATE REGION OF THE $(3,1)$ S-SMDC PROBLEM

In this appendix, we show that superposition coding can achieve the entire admissible rate region for the $(3,1)$ S-SMDC problem (the simplest nontrivial S-SMDC problem). The result is summarized in the following theorem.

**Theorem 18.** *Superposition coding can achieve the entire admissible rate region for the* $(3,1)$ *S-SMDC problem, which is given by the collection of all rate triples* $(R_1, R_2, R_3)$ *satisfying*

$$\begin{aligned} R_1 &\geq H(S_1) \\ R_2 &\geq H(S_1) \\ R_3 &\geq H(S_1) \\ R_1 + R_2 &\geq 2H(S_1) + H(S_2) \\ R_2 + R_3 &\geq 2H(S_1) + H(S_2) \\ R_3 + R_1 &\geq 2H(S_1) + H(S_2). \end{aligned} \tag{E.1}$$

*Proof. Achievability.* Consider the superposition coding scheme that separately encodes the sources $S_1$ and $S_2$ using the $(3,1,2)$ and $(3,1,3)$ S-SSDC codes, respectively. By Theorem 15, the admissible rate region for the $(3,1,2)$ S-SSDC problem is given by all rate triples $(R_1^{(1)}, R_2^{(1)}, R_3^{(1)})$ satisfying

$$\begin{aligned} R_1^{(1)} &\geq H(S_1) \\ R_2^{(1)} &\geq H(S_1) \\ R_3^{(1)} &\geq H(S_1) \end{aligned} \tag{E.2}$$

and the admissible rate region for the $(3,1,3)$ S-SSDC problem is given by all rate

triples $(R_1^{(2)}, R_2^{(2)}, R_3^{(2)})$ satisfying

$$\begin{aligned} R_1^{(2)} &\geq 0 \\ R_2^{(2)} &\geq 0 \\ R_3^{(2)} &\geq 0 \\ R_1^{(2)} + R_2^{(2)} &\geq H(S_2) \\ R_2^{(2)} + R_3^{(2)} &\geq H(S_2) \\ R_3^{(2)} + R_1^{(2)} &\geq H(S_2). \end{aligned} \tag{E.3}$$

Following (4.37), all rate triples $(R_1, R_2, R_3)$ as given by

$$R_l = R_l^{(1)} + R_l^{(2)}, \quad \forall l = 1, 2, 3 \tag{E.4}$$

are admissible via superposition coding. Using Fourier-Motzkin elimination to eliminate $R_l^{(k)}$, $l = 1, 2, 3$ and $k = 1, 2$, from (E.2)–(E.4), we obtain the explicit characterization of the superposition coding rate region for the $(3, 1)$ S-SMDC problem as expressed by (E.1).

*The converse.* Next, we establish the optimality of superposition coding by proving that every inequality in (E.1) must hold for *all* admissible rate triples $(R_1, R_2, R_3)$ for the $(3, 1)$ S-SMDC problem. Let

$$a \oplus b := \begin{cases} a + b, & \text{if } a + b \leq 3 \\ a + b - 3, & \text{otherwise.} \end{cases} \tag{E.5}$$

For any admissible rate triple $(R_1, R_2, R_3)$, any $l = 1, 2, 3$, and any $\epsilon > 0$, we have

$$\begin{aligned} n(R_l + \epsilon) &\geq H(X_l) && \text{(E.6)} \\ &\geq H(X_l|X_{l\oplus 1}) && \text{(E.7)} \\ &\geq nH(S_1) + H(X_l|S_1^n, X_{l\oplus 1}) - n\delta_1(n,\epsilon) && \text{(E.8)} \\ &\geq nH(S_1) - n\delta_1(n,\epsilon) && \text{(E.9)} \end{aligned}$$

and

$$\begin{aligned} & n(R_l + R_{l\oplus 1} + 2\epsilon) \\ &\geq H(X_l) + H(X_{l\oplus 1}) && \text{(E.10)} \\ &\geq H(X_l|X_{l\oplus 1}) + H(X_{l\oplus 1}|X_{l\oplus 2}) && \text{(E.11)} \\ &\geq 2nH(S_1) + H(X_l|S_1^n, X_{l\oplus 1}) + H(X_{l\oplus 1}|S_1^n, X_{l\oplus 2}) - 2n\delta_1(n,\epsilon) && \text{(E.12)} \\ &\geq 2nH(S_1) + H(X_l|S_1^n, X_{l\oplus 1}, X_{l\oplus 2}) + H(X_{l\oplus 1}|S_1^n, X_{l\oplus 2}) \\ &\quad -2n\delta_1(n,\epsilon) && \text{(E.13)} \\ &= 2nH(S_1) + H(X_l, X_{l\oplus 1}|S_1^n, X_{l\oplus 2}) - 2n\delta_1(n,\epsilon) && \text{(E.14)} \\ &\geq 2nH(S_1) + (nH(S_2) + H(X_l, X_{l\oplus 1}|S_1^n, S_2^n, X_{l\oplus 2}) - n\delta_2(n,\epsilon)) \\ &\quad -2n\delta_1(n,\epsilon) && \text{(E.15)} \\ &\geq 2nH(S_1) + nH(S_2) - n\delta_2(n,\epsilon) - 2n\delta_1(n,\epsilon). && \text{(E.16)} \end{aligned}$$

Here, (E.7), (E.11) and (E.13) follow from the fact that conditioning reduces entropy, and (E.8), (E.12) and (E.15) follow from Proposition 4. Dividing both sides of (E.9) and (E.16) by $n$ and letting $n \to \infty$ and $\epsilon \to 0$ complete the proof of the converse part of the theorem. □

# VITA

Hung Dinh Ly is receiving his Ph.D. degree in electrical engineering from Texas A&M University, College Station, in May 2012. Prior to that, he received his M.S. degree in electrical engineering from the University of Texas at Arlington in 2007 and his B.S. degree in electronics and telecommunications engineering from the Posts and Telecommunications Institute of Technology, Hanoi, Vietnam, in 2002.

From 2002 to 2005, Hung Ly was a lecturer with the Posts and Telecommunications Institute of Technology, Hanoi, Vietnam. During the summer of 2010, he was a research intern with the Wireless R&D division, Huawei Technologies, Rolling Meadows, Illinois, USA. Upon graduation he will be joining Qualcomm Corporate R&D in San Diego as a senior systems engineer. His research interests include information theory, wireless communication and signal processing.

Hung Ly can be contacted at Department of Electrical and Computer Engineering, Texas A&M University, 214 Zachry Engineering Center, College Station, Texas 77843-3128.