# Transmission of Common, Public and Confidential Messages in Broadcast Channels with Multiple Antennas

Ersen Ekrem Sennur Ulukus
Department of Electrical and Computer Engineering
University of Maryland, College Park, MD 20742
*ersen@umd.edu* *ulukus@umd.edu*

***Abstract*— We study the Gaussian multiple-input multiple-output (MIMO) wiretap channel, which consists of a transmitter, a legitimate user, and an eavesdropper. In this channel, the transmitter sends a common message to both the legitimate user and the eavesdropper. Moreover, the legitimate user receives a private message, which is desired to be kept hidden as much as possible from the eavesdropper. We obtain the entire capacity-equivocation region of the Gaussian MIMO wiretap channel. This region contains all achievable common message, private message, and private message's equivocation rates. This capacity-equivocation region is equal to the capacity region of a Gaussian MIMO broadcast channel where the transmitter sends a common message to both the legitimate user and the eavesdropper, a public message to the legitimate user on which there is no secrecy constraint, and a confidential message to the legitimate user which needs to kept perfectly secret from the eavesdropper.**

## I. Introduction

We consider the Gaussian multiple-input multiple-output (MIMO) wiretap channel, which consists of a transmitter, a legitimate user, and an eavesdropper. In this channel, the transmitter sends a common message to both the legitimate user and the eavesdropper in addition to a private message which is directed to only the legitimate user. There is a secrecy concern regarding this private message in the sense that the private message needs to be kept secret as much as possible from the eavesdropper. The secrecy of the private message is measured by its equivocation at the eavesdropper.

Here, we obtain the capacity-equivocation region of the Gaussian MIMO wiretap channel. This region contains all achievable rate triples $(R_0, R_1, R_e)$, where $R_0$ denotes the common message rate, $R_1$ denotes the private message rate, and $R_e$ denotes the private message's equivocation (secrecy) rate. In fact, this region is known in a single-letter form due to [1]. In this work, we show that jointly Gaussian auxiliary random variables and channel input are sufficient to evaluate this single-letter description for the capacity-equivocation region of the Gaussian MIMO wiretap channel. We prove the sufficiency of the jointly Gaussian auxiliary random variables and channel input by using channel enhancement [2] and an extremal inequality from [3]. In our proof, we also use the equivalence between the Gaussian MIMO wiretap channel and the Gaussian MIMO wiretap channel with *public* messages [4, Problem 33-c], [5]. In the latter channel model, the transmitter has three messages, a common, a confidential, and a public message. The common message is sent to both the legitimate user and the eavesdropper, while the confidential and public messages are directed to only the legitimate user. Here, the confidential message needs to be transmitted in perfect secrecy, whereas there is no secrecy constraint on the public message. Since the Gaussian MIMO wiretap channel and the Gaussian MIMO wiretap channel with public messages are equivalent, i.e., there is a one-to-one correspondence between the capacity regions of these two models, in our proof, we obtain the capacity region of the Gaussian MIMO wiretap channel with public messages, which, in turn, gives us the capacity-equivocation region of the Gaussian MIMO wiretap channel.

Our result subsumes the following previous findings about the capacity-equivocation region of the Gaussian MIMO wiretap channel: i) The secrecy capacity of this channel, i.e., $\max R_1$ when $R_0 = 0, R_e = R_1$, is obtained in [6], [7] for the general case, and in [8] for the 2-2-1 case. ii) The common and confidential rate region under perfect secrecy, i.e., $(R_0, R_1)$ region with $R_e = R_1$, is obtained in [9]. iii) The capacity-equivocation region without a common message, i.e., $(R_1, R_e)$ region with $R_0 = 0$, is obtained in [5]. iv) The capacity region of the Gaussian MIMO broadcast channel with degraded message sets without a secrecy concern, i.e., $(R_0, R_1)$ region with no consideration on $R_e$, is obtained in [10]. Here, we obtain the entire $(R_0, R_1, R_e)$ region.

## II. Discrete Memoryless Wiretap Channels

The discrete memoryless wiretap channel consists of a transmitter, a legitimate user and an eavesdropper. The channel transition probability is $p(y, z|x)$, where $x \in \mathcal{X}$ is the channel input, $y \in \mathcal{Y}$ is the legitimate user's observation, and $z \in \mathcal{Z}$ is the eavesdropper's observation. We consider the following scenario: The transmitter sends a common message to both the legitimate user and the eavesdropper, and a private message to the legitimate user which is desired to be kept hidden as much as possible from the eavesdropper.

An $(n, 2^{nR_0}, 2^{nR_1})$ code for this channel consists of two message sets $\mathcal{W}_j = \{1, \ldots, 2^{nR_j}\}$, $j = 0, 1$, one encoder at the transmitter $f : \mathcal{W}_0 \times \mathcal{W}_1 \rightarrow \mathcal{X}^n$, one decoder at

This work was supported by NSF Grants CCF 04-47613, CCF 05-14846, CNS 07-16311 and CCF 07-29127.

the legitimate user $g_u : \mathcal{Y}^n \to \mathcal{W}_0 \times \mathcal{W}_1$, and one decoder at the eavesdropper $g_e : \mathcal{Z}^n \to W_0$. The probability of error is defined as $P_e^n = \max\{P_{e,u}^n, P_{e,e}^n\}$, where $P_{e,u}^n = \Pr[g_u(Y^n) \neq (W_0, W_1)], P_{e,e}^n = \Pr[g_e(Z^n) \neq W_0]$, and $W_j$ is a uniformly distributed random variable in $\mathcal{W}_j$, $j = 0, 1$. The secrecy of the legitimate user's private message is measured by its equivocation at the eavesdropper [1], [11]. A rate triple $(R_0, R_1, R_e)$ is said to be achievable if there exists an $(n, 2^{nR_0}, 2^{nR_1})$ code such that $\lim_{n\to\infty} P_e^n = 0$, and

$$R_e = \lim_{n\to\infty} \frac{1}{n} H(W_1|W_0, Z^n) \tag{1}$$

The capacity-equivocation region of the discrete memoryless wiretap channel, $\mathcal{C}$, is defined as the convex closure of all achievable rate triples $(R_0, R_1, R_e)$. $\mathcal{C}$ is given as follows [1].

**Theorem 1 ([1, Theorem 1])** *The capacity-equivocation region of the discrete memoryless wiretap channel $\mathcal{C}$ is given by the union of rate triples $(R_0, R_1, R_e)$ satisfying*

$$0 \leq R_e \leq \min\{I(V;Y|U) - I(V;Z|U), R_1\} \tag{2}$$

$$R_0 + R_1 \leq I(V;Y|U) + \min\{I(U;Y), I(U;Z)\} \tag{3}$$

$$R_0 \leq \min\{I(U;Y), I(U;Z)\} \tag{4}$$

*for some $U, V, X$ such that $U \to V \to X \to Y, Z$.*

We now provide an alternative description for $\mathcal{C}$, which arises as the capacity region of a different, however related, scenario for the discrete memoryless wiretap channel. In this scenario, the transmitter has three messages, $W_0, W_p, W_s$, where $W_0$ is sent to both the legitimate user and the eavesdropper, and $W_s, W_p$ are sent only to the legitimate user. Here, $W_s$ needs to be sent in perfect secrecy, i.e., it needs to satisfy

$$\lim_{n\to\infty} \frac{1}{n} I(W_s; Z^n, W_0) = 0 \tag{5}$$

and there is no secrecy constraint on the *public* message $W_p$. We call the corresponding channel model the discrete memoryless wiretap channel with *public* messages [4], [5].

A rate triple $(R_0, R_p, R_s)$ is said to be achievable for this channel model if there exists an $(n, 2^{nR_0}, 2^{nR_p}, 2^{nR_s})$ code such that $\lim_{n\to\infty} P_e^n = 0$ and (5) is satisfied. The capacity region $\mathcal{C}_p$ of the discrete memoryless wiretap channel with *public* messages is defined as the convex closure of all achievable rate triples $(R_0, R_p, R_s)$. The following lemma shows the equivalence between $\mathcal{C}$ and $\mathcal{C}_p$.

**Lemma 1** $(R_0, R_p, R_s) \in \mathcal{C}_p$ *iff* $(R_0, R_s + R_p, R_s) \in \mathcal{C}$.

The proof of this lemma as well as the proofs of the other results that are omitted here can be found in the journal version of this paper [12]. Using Lemma 1 and Theorem 1, we can express $\mathcal{C}_p$ as stated in the following theorem.

**Theorem 2** *The capacity region of the discrete memoryless wiretap channel with public messages $\mathcal{C}_p$ is given by the union of rate triples $(R_0, R_p, R_s)$ satisfying*

$$0 \leq R_s \leq I(V;Y|U) - I(V;Z|U) \tag{6}$$

$$R_0 + R_p + R_s \leq I(V;Y|U) + \min\{I(U;Y), I(U;Z)\} \tag{7}$$

$$R_0 \leq \min\{I(U;Y), I(U;Z)\} \tag{8}$$

*for some $(U, V, X)$ such that $U \to V \to X \to Y, Z$.*

## III. Gaussian MIMO Wiretap Channel

The Gaussian MIMO wiretap channel is defined by

$$\mathbf{Y} = \mathbf{H}_Y \mathbf{X} + \mathbf{N}_Y \tag{9}$$

$$\mathbf{Z} = \mathbf{H}_Z \mathbf{X} + \mathbf{N}_Z \tag{10}$$

where $\mathbf{X}$ is the channel input, $\mathbf{Y}$ is the legitimate user's observation, $\mathbf{Z}$ is the eavesdropper's observation, $\mathbf{H}_Y, \mathbf{H}_Z$ are the channel gain matrices. $\mathbf{N}_Y, \mathbf{N}_Z$ are Gaussian with covariance matrices $\mathbf{\Sigma}_Y, \mathbf{\Sigma}_Z$, respectively, which are strictly positive-definite. There is a covariance constraint on $\mathbf{X}$:

$$E\left[\mathbf{X}\mathbf{X}^\top\right] \preceq \mathbf{S} \tag{11}$$

where $\mathbf{S} \succeq \mathbf{0}$. The capacity-equivocation region of the Gaussian MIMO wiretap channel, $\mathcal{C}(\mathbf{S})$, is given as follows.

**Theorem 3** *The capacity-equivocation region of the Gaussian MIMO wiretap channel $\mathcal{C}(\mathbf{S})$ is given by the union of rate triples $(R_0, R_1, R_e)$ satisfying*

$$0 \leq R_e \leq \frac{1}{2}\log\frac{|\mathbf{H}_Y\mathbf{K}\mathbf{H}_Y^\top + \mathbf{\Sigma}_Y|}{|\mathbf{\Sigma}_Y|} - \frac{1}{2}\log\frac{|\mathbf{H}_Z\mathbf{K}\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{12}$$

$$R_0 + R_1 \leq \frac{1}{2}\log\frac{|\mathbf{H}_Y\mathbf{K}\mathbf{H}_Y^\top + \mathbf{\Sigma}_Y|}{|\mathbf{\Sigma}_Y|} + \frac{1}{2}\min\left\{\log\frac{|\mathbf{H}_Y\mathbf{S}\mathbf{H}_Y^\top + \mathbf{\Sigma}_Y|}{|\mathbf{H}_Y\mathbf{K}\mathbf{H}_Y^\top + \mathbf{\Sigma}_Y|}, \log\frac{|\mathbf{H}_Z\mathbf{S}\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z|}{|\mathbf{H}_Z\mathbf{K}\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z|}\right\} \tag{13}$$

$$R_0 \leq \frac{1}{2}\min\left\{\log\frac{|\mathbf{H}_Y\mathbf{S}\mathbf{H}_Y^\top + \mathbf{\Sigma}_Y|}{|\mathbf{H}_Y\mathbf{K}\mathbf{H}_Y^\top + \mathbf{\Sigma}_Y|}, \log\frac{|\mathbf{H}_Z\mathbf{S}\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z|}{|\mathbf{H}_Z\mathbf{K}\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z|}\right\} \tag{14}$$

*for some positive semi-definite matrix $\mathbf{K}$ such that $\mathbf{K} \preceq \mathbf{S}$.*

We obtain an alternative statement for Theorem 3 by considering the Gaussian MIMO wiretap channel with *public* messages. The capacity region of this scenario is denoted by $\mathcal{C}_p(\mathbf{S})$, and is obtained by using Lemma 1 and Theorem 3 as follows.

**Theorem 4** *The capacity region of the Gaussian MIMO wiretap channel with public messages $\mathcal{C}_p(\mathbf{S})$ is given by the union of rate triples $(R_0, R_p, R_s)$ satisfying*

$$0 \leq R_s \leq \frac{1}{2}\log\frac{|\mathbf{H}_Y\mathbf{K}\mathbf{H}_Y^\top + \mathbf{\Sigma}_Y|}{|\mathbf{\Sigma}_Y|} - \frac{1}{2}\log\frac{|\mathbf{H}_Z\mathbf{K}\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{15}$$

$$R_0 + R_p + R_s \leq \frac{1}{2}\log\frac{|\mathbf{H}_Y\mathbf{K}\mathbf{H}_Y^\top + \mathbf{\Sigma}_Y|}{|\mathbf{\Sigma}_Y|} + \frac{1}{2}\min\left\{\log\frac{|\mathbf{H}_Y\mathbf{S}\mathbf{H}_Y^\top + \mathbf{\Sigma}_Y|}{|\mathbf{H}_Y\mathbf{K}\mathbf{H}_Y^\top + \mathbf{\Sigma}_Y|}, \log\frac{|\mathbf{H}_Z\mathbf{S}\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z|}{|\mathbf{H}_Z\mathbf{K}\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z|}\right\} \tag{16}$$

$$R_0 \leq \frac{1}{2}\min\left\{\log\frac{|\mathbf{H}_Y\mathbf{S}\mathbf{H}_Y^\top+\mathbf{\Sigma}_Y|}{|\mathbf{H}_Y\mathbf{K}\mathbf{H}_Y^\top+\mathbf{\Sigma}_Y|},\log\frac{|\mathbf{H}_Z\mathbf{S}\mathbf{H}_Z^\top+\mathbf{\Sigma}_Z|}{|\mathbf{H}_Z\mathbf{K}\mathbf{H}_Z^\top+\mathbf{\Sigma}_Z|}\right\} \tag{17}$$

*for some positive semi-definite matrix* $\mathbf{K}$ *such that* $\mathbf{K}\preceq\mathbf{S}$.

Now we define a sub-class of Gaussian MIMO wiretap channels called the aligned Gaussian MIMO wiretap channel, which is obtained from (9)-(10) by setting $\mathbf{H}_Y=\mathbf{H}_Z=\mathbf{I}$,

$$\mathbf{Y}=\mathbf{X}+\mathbf{N}_Y \tag{18}$$

$$\mathbf{Z}=\mathbf{X}+\mathbf{N}_Z \tag{19}$$

Here, we prove Theorems 3 and 4 for the aligned Gaussian MIMO wiretap channel. The proof for capacity region of the general channel model in (9)-(10) can be found in [12].

### A. Capacity Region under a Power Constraint

The covariance constraint on the channel input in (11) is a general constraint that subsumes the average power constraint

$$E\left[\mathbf{X}^\top\mathbf{X}\right]=\mathrm{tr}\left(E\left[\mathbf{X}\mathbf{X}^\top\right]\right)\leq P \tag{20}$$

as a special case, see Lemma 1 and Corollary 1 of [2]. Thus, using Theorem 3, the capacity-equivocation region arising from the constraint in (20), $\mathcal{C}(P)$, can be found as follows.

**Corollary 1** *The capacity-equivocation region of the Gaussian MIMO wiretap channel subject to the constraint in (20) is given by the union of rate triples* $(R_0,R_1,R_e)$ *satisfying*

$$R_e\leq\frac{1}{2}\log\frac{|\mathbf{H}_Y\mathbf{K}_1\mathbf{H}_Y^\top+\mathbf{\Sigma}_Y|}{|\mathbf{\Sigma}_Y|}-\frac{1}{2}\log\frac{|\mathbf{H}_Z\mathbf{K}_1\mathbf{H}_Z^\top+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{21}$$

$$R_0+R_1\leq\frac{1}{2}\log\frac{|\mathbf{H}_Y\mathbf{K}_1\mathbf{H}_Y^\top+\mathbf{\Sigma}_Y|}{|\mathbf{\Sigma}_Y|}+\min\{R_{0Y}(\mathbf{K}_1,\mathbf{K}_2),R_{0Z}(\mathbf{K}_1,\mathbf{K}_2)\} \tag{22}$$

$$R_0\leq\min\{R_{0Y}(\mathbf{K}_1,\mathbf{K}_2),R_{0Z}(\mathbf{K}_1,\mathbf{K}_2)\} \tag{23}$$

*for some positive semi-definite matrices* $\mathbf{K}_1,\mathbf{K}_2$ *such that* $\mathrm{tr}(\mathbf{K}_1+\mathbf{K}_2)\leq P$*, where* $R_{0Y}(\mathbf{K}_1,\mathbf{K}_2)$ *is given by*

$$R_{0Y}(\mathbf{K}_1,\mathbf{K}_2)=\frac{1}{2}\log\frac{|\mathbf{H}_Y(\mathbf{K}_1+\mathbf{K}_2)\mathbf{H}_Y^\top+\mathbf{\Sigma}_Y|}{|\mathbf{H}_Y\mathbf{K}_1\mathbf{H}_Y^\top+\mathbf{\Sigma}_Y|} \tag{24}$$

*and* $R_{0Z}(\mathbf{K}_1,\mathbf{K}_2)$ *can be obtained from* $R_{0Y}(\mathbf{K}_1,\mathbf{K}_2)$ *by swapping the subscript* $Y$ *with* $Z$.

## IV. Proof of Theorem 3 for the Aligned Case

We prove Theorem 4, which implies Theorem 3 due to Lemma 1. Achievability of Theorem 4 can be shown by setting $V=\mathbf{X}$ and using jointly Gaussian $(U,V=\mathbf{X})$ in Theorem 2. Next, we provide the converse proof. To this end, we note that since $\mathcal{C}_p(\mathbf{S})$ is convex by definition, it can be characterized by solving the following optimization problem

$$f(R_0^*)=\max_{(R_0^*,R_p,R_s)\in\mathcal{C}_p(\mathbf{S})}\ \mu_pR_p+\mu_sR_s \tag{25}$$

for all $\mu_p\in[0,\infty),\mu_s\in[0,\infty)$, and all possible common message rates $R_0^*$, which is bounded as follows

$$0\leq R_0^*\leq\min\{C_Y(\mathbf{S}),C_Z(\mathbf{S})\} \tag{26}$$

where $C_Y(\mathbf{S}),C_Z(\mathbf{S})$ are the single-user capacities of the legitimate user and the eavesdropper channels, respectively:

$$C_Y(\mathbf{S})=\frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Y|}{|\mathbf{\Sigma}_Y|}\ \text{and}\ C_Z(\mathbf{S})=\frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{27}$$

We note that the optimization problem in (25) can be expressed in the following more explicit form

$$f(R_0^*)=\max_{\substack{U\to V\to\mathbf{X}\to(\mathbf{Y},\mathbf{Z})\\ E[\mathbf{X}\mathbf{X}^\top]\preceq\mathbf{S}}}\ \mu_pR_p+\mu_sR_s \tag{28}$$

$$\text{s.t.}\begin{cases}R_s\ \leq\ I(V;\mathbf{Y}|U)-I(V;\mathbf{Z}|U)\\ R_0^*+R_p+R_s\ \leq\ I(V;\mathbf{Y}|U)\\ \qquad\qquad +\min\{I(U;\mathbf{Y}),I(U;\mathbf{Z})\}\\ R_0^*\ \leq\ \min\{I(U;\mathbf{Y}),I(U;\mathbf{Z})\}\end{cases} \tag{29}$$

We also consider the Gaussian rate region $\mathcal{R}^G(\mathbf{S})$ which is given by the union of the rate triples $(R_0,R_p,R_s)$ satisfying

$$0\leq R_s\leq R_s(\mathbf{K}) \tag{30}$$

$$R_0+R_p+R_s\leq R_s(\mathbf{K})+R_p(\mathbf{K})+\min\{R_{0Y}(\mathbf{K}),R_{0Z}(\mathbf{K})\} \tag{31}$$

$$R_0\leq\min\{R_{0Y}(\mathbf{K}),R_{0Z}(\mathbf{K})\} \tag{32}$$

for some positive semi-definite matrix $\mathbf{K}$ such that $\mathbf{K}\preceq\mathbf{S}$, where $R_s(\mathbf{K}),R_p(\mathbf{K}),R_{0Y}(\mathbf{K}),R_{0Z}(\mathbf{K})$ are given as follows

$$R_s(\mathbf{K})=\frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_Y|}{|\mathbf{\Sigma}_Y|}-\frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{33}$$

$$R_p(\mathbf{K})=\frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{34}$$

$$R_{0Y}(\mathbf{K})=\frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Y|}{|\mathbf{K}+\mathbf{\Sigma}_Y|} \tag{35}$$

$$R_{0Z}(\mathbf{K})=\frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{K}+\mathbf{\Sigma}_Z|} \tag{36}$$

To provide the converse proof, i.e., to prove the optimality of jointly Gaussian $(U,V=\mathbf{X})$ for the optimization problem in (28)-(29), we will show that

$$f(R_0^*)=g(R_0^*),\quad 0\leq R_0^*\leq\min\{C_Y(\mathbf{S}),C_Z(\mathbf{S})\} \tag{37}$$

where $g(R_0^*)$ is defined as

$$g(R_0^*)=\max_{(R_0^*,R_p,R_s)\in\mathcal{R}^G(\mathbf{S})}\ \mu_pR_p+\mu_sR_s \tag{38}$$

We show (37) in two parts: A. $\mu_s\leq\mu_p$, B. $\mu_p>\mu_s$.

### A. $\mu_s\leq\mu_p$

In this case, $f(R_0^*)$ can be written as

$$f(R_0^*)=\max_{\substack{U\to V\to\mathbf{X}\to(\mathbf{Y},\mathbf{Z})\\ E[\mathbf{X}\mathbf{X}^\top]\preceq\mathbf{S}}}\ \mu_p(R_p+R_s) \tag{39}$$

$$\text{s.t.}\begin{cases}R_0^*+R_p+R_s\ \leq\ I(\mathbf{X};\mathbf{Y}|U)\\ \qquad\qquad +\min\{I(U;\mathbf{Y}),I(U;\mathbf{Z})\}\\ R_0^*\ \leq\ \min\{I(U;\mathbf{Y}),I(U;\mathbf{Z})\}\end{cases} \tag{40}$$

where we use the fact that $\mu_s\leq\mu_p$, and the secret message rate $R_s$ can be given up in favor of the private message rate $R_p$.

The optimization problem in (39)-(40) gives us the capacity region of the two-user Gaussian MIMO broadcast channel with degraded message sets, where a common message is sent to both users, and a private message, on which there is no secrecy constraint, is sent to one of the two users [13]. This optimization problem is solved in [10] by showing the optimality of jointly Gaussian $(U, \mathbf{X})$, i.e., $f(R_0^*) = g(R_0^*)$. This completes the converse proof for this case.

*B.* $\mu_p < \mu_s$

In this case, we first study the optimization problem in (38). We rewrite $g(R_0^*)$ as follows

$$g(R_0^*) = \max_{\mathbf{0} \preceq \mathbf{K} \preceq \mathbf{S}} \underbrace{\mu_p R_p + \mu_s R_s(\mathbf{K})}_{R_p} \tag{41}$$

$$\text{s.t.} \begin{cases} R_0^* + R_p \leq R_p(\mathbf{K}) + \min\{R_{0Y}(\mathbf{K}), R_{0Z}(\mathbf{K})\} \\ R_0^* \leq \min\{R_{0Y}(\mathbf{K}), R_{0Z}(\mathbf{K})\} \end{cases} \tag{42}$$

Let $(\mathbf{K}^*, R_p^*)$ be the maximizer for this optimization problem. The necessary KKT conditions for $(\mathbf{K}^*, R_p^*)$ are as follows.

**Lemma 2** $\mathbf{K}^*$ *needs to satisfy*

$$\begin{aligned}(\mu_s - \mu_p\lambda - \beta_Y)(\mathbf{K}^* + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M} \\ = (\mu_s - \mu_p\lambda + \beta_Z)(\mathbf{K}^* + \mathbf{\Sigma}_Z)^{-1} + \mathbf{M}_S\end{aligned} \tag{43}$$

*for some positive semi-definite matrices* $\mathbf{M}, \mathbf{M}_S$ *such that* $\mathbf{K}^*\mathbf{M} = \mathbf{M}\mathbf{K}^* = \mathbf{0}, (\mathbf{S} - \mathbf{K}^*)\mathbf{M}_S = \mathbf{M}_S(\mathbf{S} - \mathbf{K}^*) = \mathbf{0}$ *and for some* $\lambda = 1 - \bar{\lambda}$ *such that it satisfies* $0 \leq \lambda \leq 1$ *and*

$$\lambda \begin{cases} = & 0 & \text{if} & R_{0Y}(\mathbf{K}^*) > R_{0Z}(\mathbf{K}^*) \\ = & 1 & \text{if} & R_{0Y}(\mathbf{K}^*) < R_{0Z}(\mathbf{K}^*) \\ \neq & 0, 1 & \text{if} & R_{0Y}(\mathbf{K}^*) = R_{0Z}(\mathbf{K}^*) \end{cases} \tag{44}$$

*and* $(\beta_Y, \beta_Z)$ *are given as follows*

$$(\beta_Y, \beta_Z) \begin{cases} = (0,0) & \text{if} & R_0^* < \min\{R_{0Y}(\mathbf{K}^*), R_{0Z}(\mathbf{K}^*)\} \\ (= 0, > 0) & \text{if} & R_0^* = R_{0Z}(\mathbf{K}^*) < R_{0Y}(\mathbf{K}^*) \\ (> 0, = 0) & \text{if} & R_0^* = R_{0Y}(\mathbf{K}^*) < R_{0Z}(\mathbf{K}^*) \\ (> 0, > 0) & \text{if} & R_0^* = R_{0Y}(\mathbf{K}^*) = R_{0Z}(\mathbf{K}^*) \end{cases} \tag{45}$$

*$R_p^*$ needs to satify*

$$R_p^* = R_p(\mathbf{K}^*) + \min\{R_{0Y}(\mathbf{K}^*), R_{0Z}(\mathbf{K}^*)\} - R_0^* \tag{46}$$

We treat three cases separately:

1) $R_0^* < \min\{R_{0Y}(\mathbf{K}^*), R_{0Z}(\mathbf{K}^*)\}$
2) $R_0^* = R_{0Y}(\mathbf{K}^*) \leq R_{0Z}(\mathbf{K}^*)$
3) $R_0^* = R_{0Z}(\mathbf{K}^*) < R_{0Y}(\mathbf{K}^*)$

*1)* $R_0^* < \min\{R_{0Y}(\mathbf{K}^*), R_{0Z}(\mathbf{K}^*)\}$*:* We have $\beta_Y = \beta_Z = 0$, see (45). Thus, the KKT condition in (43) reduces to

$$\begin{aligned}(\mu_s - \mu_p\lambda)(\mathbf{K}^* + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M} = (\mu_s - \mu_p\lambda)(\mathbf{K}^* + \mathbf{\Sigma}_Z)^{-1} \\ + \mathbf{M}_S\end{aligned} \tag{47}$$

We first note that $\mathbf{K}^*$ satisfying (47) achieves the secrecy capacity of this Gaussian MIMO wiretap channel [14], i.e.,

$$R_s^* = R_s(\mathbf{K}^*) = C_S(\mathbf{S}) \tag{48}$$

$$= \max_{\mathbf{0} \preceq \mathbf{K} \preceq \mathbf{S}} \frac{1}{2} \log \frac{|\mathbf{K} + \mathbf{\Sigma}_Y|}{|\mathbf{\Sigma}_Y|} - \frac{1}{2} \log \frac{|\mathbf{K} + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{49}$$

Next, we define a new covariance matrix $\tilde{\mathbf{\Sigma}}_Z$ as follows

$$\begin{aligned}(\mu_s - \mu_p\lambda)(\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Z)^{-1} = (\mu_s - \mu_p\lambda)(\mathbf{K}^* + \mathbf{\Sigma}_Z)^{-1} \\ + \mathbf{M}_S\end{aligned} \tag{50}$$

This new covariance matrix $\tilde{\mathbf{\Sigma}}_Z$ has some useful properties.

**Lemma 3** *We have the following facts.*

- $\tilde{\mathbf{\Sigma}}_Z \preceq \mathbf{\Sigma}_Z$ *and* $\tilde{\mathbf{\Sigma}}_Z \preceq \mathbf{\Sigma}_Y$
- $(\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Z)^{-1}(\mathbf{S} + \tilde{\mathbf{\Sigma}}_Z) = (\mathbf{K}^* + \mathbf{\Sigma}_Z)^{-1}(\mathbf{S} + \mathbf{\Sigma}_Z)$

Thus, we have

$$R_{0Z}(\mathbf{K}^*) = \frac{1}{2} \log \frac{|\mathbf{S} + \tilde{\mathbf{\Sigma}}_Z|}{|\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Z|} \tag{51}$$

$$\geq \frac{1}{2} \log \frac{|\mathbf{S} + \mathbf{\Sigma}_Y|}{|\mathbf{K}^* + \mathbf{\Sigma}_Y|} \tag{52}$$

$$= R_{0Y}(\mathbf{K}^*) \tag{53}$$

where (51) comes from the third part of Lemma 3, (52) is due to the fact that

$$\frac{|\mathbf{A} + \mathbf{B} + \mathbf{\Delta}|}{|\mathbf{B} + \mathbf{\Delta}|} \leq \frac{|\mathbf{A} + \mathbf{B}|}{|\mathbf{B}|} \tag{54}$$

for $\mathbf{A} \succeq \mathbf{0}$, $\mathbf{\Delta} \succeq \mathbf{0}$, $\mathbf{B} \succ \mathbf{0}$ by noting the second part of Lemma 3. Using (53) in (46), we find $R_p^*$ as follows

$$R_p^* = R_p(\mathbf{K}^*) + R_{0Y}(\mathbf{K}^*) - R_0^* \tag{55}$$

We also note the following

$$R_0^* + R_p^* + R_s^* = R_{0Y}(\mathbf{K}^*) + R_p(\mathbf{K}^*) + R_s(\mathbf{K}^*) \tag{56}$$

$$= C_Y(\mathbf{S}) \tag{57}$$

Now, we show that

$$g(R_0^*) = f(R_0^*) \tag{58}$$

To this end, we assume that $g(R_0^*) < f(R_0^*)$ which implies that there exists a rate triple $(R_0^*, R_p^o, R_s^o) \in \mathcal{C}_p(\mathbf{S})$ such that

$$\mu_p R_p^* + \mu_s R_s^* < \mu_p R_p^o + \mu_s R_s^o \tag{59}$$

To prove (58), we note the following bounds

$$R_s^o \leq C_S(\mathbf{S}) = R_s^* \tag{60}$$

$$R_p^o + R_s^o \leq C_Y(\mathbf{S}) - R_0^* = R_p^* + R_s^* \tag{61}$$

where (60) comes from (49) and the fact that the rate of the confidential message, i.e., $R_s$, cannot exceed the secrecy capacity, and (61) is due to (57) and the fact that the sum rate $R_0 + R_p + R_s$ cannot exceed the legitimate user's single-user capacity. Thus, in view of $\mu_s > \mu_p$, (60)-(61) imply

$$\mu_p R_p^o + \mu_s R_s^o \leq \mu_p R_p^* + \mu_s R_s^* \tag{62}$$

which contradicts with (59); proving (58). This completes the converse proof for this case.

We now recap our converse proof for the current case. Here, we did not show the optimality of Gaussian signalling

directly, instead, we show the desired identity $g(R_0^*) = f(R_0^*)$ indirectly. First, we show that for the given common message rate $R_0^*$, we can achieve the secrecy capacity, i.e., $R_s^* = C_S(\mathbf{S})$, see (48)-(49). Hence, $(R_0^*, 0, R_s^*)$ is on the boundary of the capacity region $\mathcal{C}_p(\mathbf{S})$. Next, we show that for the given common message rate $R_0^*$, $R_p^* + R_s^*$ achieves the sum capacity of the public and confidential messages, see (56)-(57) and (61). These two findings lead to the two inequalities in (60)-(61). Finally, we use a time-sharing argument for the inequalities in (60)-(61) to obtain the desired identity $g(R_0^*) = f(R_0^*)$, which completes the proof.

*2)* $R_0^* = R_{0Y}(\mathbf{K}^*) \leq R_{0Z}(\mathbf{K}^*)$*:* We first rewrite the KKT condition in (43) as follows

$$\begin{aligned}(\mu_s - \mu_p\lambda - \mu_0\beta)(\mathbf{K}^* + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M} \\ = (\mu_s - \mu_p\lambda + \mu_0\bar{\beta})(\mathbf{K}^* + \mathbf{\Sigma}_Z)^{-1} + \mathbf{M}_S \quad (63)\end{aligned}$$

by defining $\mu_0 = \beta_Y + \beta_Z$, $\mu_0\beta = \beta_Y$, and $\mu_0\bar{\beta} = \beta_Z$. We note that if $R_{0Y}(\mathbf{K}^*) < R_{0Z}(\mathbf{K}^*)$, we have $\beta = \lambda = 1$, if $R_{0Y}(\mathbf{K}^*) = R_{0Z}(\mathbf{K}^*)$, we have $0 < \lambda < 1, 0 < \beta < 1$. The proof of these two cases are very similar, and we consider only the latter case. The other case can be proved similarly.

Similar to Section IV-B.1, here also, we prove the desired identity

$$g(R_0^*) = f(R_0^*) \quad (64)$$

by contradiction. We first assume that $g(R_0^*) < f(R_0^*)$ which implies that there exists a rate triple $(R_0^*, R_p^o, R_s^o) \in \mathcal{C}_p(\mathbf{S})$ such that

$$\mu_p R_p^* + \mu_s R_s^* < \mu_p R_p^o + \mu_s R_s^o \quad (65)$$

where we define $R_s^* = R_s(\mathbf{K}^*)$. Since the sum rate $R_0 + R_p + R_s$ needs to be smaller than the legitimate user's single user capacity, we have

$$R_0^* + R_p^o + R_s^o \leq C_Y(\mathbf{S}) \quad (66)$$

On the other hand, we have the following

$$\begin{aligned}R_0^* + R_p^* + R_s^* &= \min\{R_{0Y}(\mathbf{K}^*), R_{0Z}(\mathbf{K}^*)\} + R_p(\mathbf{K}^*) \\ &\quad + R_s(\mathbf{K}^*) \quad (67)\\ &= R_{0Y}(\mathbf{K}^*) + R_p(\mathbf{K}^*) + R_s(\mathbf{K}^*) \quad (68)\\ &= C_Y(\mathbf{S}) \quad (69)\end{aligned}$$

where (67) comes from (46), and (68) is due to our assumption that $R_0^* = R_{0Y}(\mathbf{K}^*) = R_{0Z}(\mathbf{K}^*)$. Equations (66) and (69) imply that

$$R_p^o + R_s^o \leq R_p^* + R_s^* \quad (70)$$

Next we prove that we have $R_s^o \leq R_s^*$ for the given common message rate $R_0^*$, which, in conjunction with (70), will yield a contradiction with (65); proving (64). To this end, we first define a new covariance matrix $\tilde{\mathbf{\Sigma}}_Y$ as follows

$$(\mu_s - \mu_p\lambda)(\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Y)^{-1} = (\mu_s - \mu_p\lambda)(\mathbf{K}^* + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M} \quad (71)$$

This new covariance matrix $\tilde{\mathbf{\Sigma}}_Y$ has some useful properties.

**Lemma 4** *We have the following facts.*

- $\tilde{\mathbf{\Sigma}}_Y \preceq \mathbf{\Sigma}_Y$ *and* $\tilde{\mathbf{\Sigma}}_Y \preceq \mathbf{\Sigma}_Z$
- $(\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Y)^{-1}\tilde{\mathbf{\Sigma}}_Y = (\mathbf{K}^* + \mathbf{\Sigma}_Y)^{-1}\mathbf{\Sigma}_Y$

Using this new covariance matrix, we define $\tilde{\mathbf{Y}}$ as

$$\tilde{\mathbf{Y}} = \mathbf{X} + \tilde{\mathbf{N}}_Y \quad (72)$$

where $\tilde{\mathbf{N}}_Y$ is a Gaussian random vector with covariance matrix $\tilde{\mathbf{\Sigma}}_Y$. Due to the first statement of Lemma 4, we have the following Markov chain

$$U \to V \to \mathbf{X} \to \tilde{\mathbf{Y}} \to \mathbf{Y}, \mathbf{Z} \quad (73)$$

We next study the following optimization problem

$$\begin{aligned}L &= \max_{(R_0,R_p,R_s)\in\mathcal{C}_p(\mathbf{S})} \mu_0 R_0 + (\mu_s - \mu_p\lambda)R_s \\ &= \max_{\substack{U\to V\to\mathbf{X}\to(\mathbf{Y},\mathbf{Z}) \\ E[\mathbf{X}\mathbf{X}^\top]\preceq\mathbf{S}}} \mu_0 \min\{I(U;\mathbf{Y}), I(U;\mathbf{Z})\} \\ &\qquad + (\mu_s - \mu_p\lambda)\left[I(V;\mathbf{Y}|U) - I(V;\mathbf{Z}|U)\right] \quad (74)\end{aligned}$$

Since we assume $(R_0^*, R_p^o, R_s^o) \in \mathcal{C}_p(\mathbf{S})$, we have the following lower bound for (74)

$$\mu_0 R_0^* + (\mu_s - \mu_p\lambda)R_s^o \leq L \quad (75)$$

Now we solve the optimization problem in (74) as follows

$$\begin{aligned}L &\leq \max_{\substack{U\to V\to\mathbf{X}\to(\mathbf{Y},\mathbf{Z}) \\ E[\mathbf{X}\mathbf{X}^\top]\preceq\mathbf{S}}} \mu_0\bar{\beta}I(U;\mathbf{Z}) + \mu_0\beta I(U;\mathbf{Y}) \\ &\qquad + (\mu_s - \mu_p\lambda)\left[I(V;\mathbf{Y}|U) - I(V;\mathbf{Z}|U)\right] \quad (76)\\ &\leq \max_{\substack{U\to\mathbf{X}\to(\mathbf{Y},\mathbf{Z}) \\ E[\mathbf{X}\mathbf{X}^\top]\preceq\mathbf{S}}} \mu_0\bar{\beta}I(U;\mathbf{Z}) + \mu_0\beta I(U;\mathbf{Y}) \\ &\qquad + (\mu_s - \mu_p\lambda)\left[I(\mathbf{X};\tilde{\mathbf{Y}}|U) - I(\mathbf{X};\mathbf{Z}|U)\right] \quad (77)\\ &\leq \frac{\mu_0\bar{\beta}}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{K}^*+\mathbf{\Sigma}_Z|} + \frac{\mu_0\beta}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Y|}{|\mathbf{K}^*+\mathbf{\Sigma}_Y|} \\ &\quad + \frac{\mu_s-\mu_p\lambda}{2}\left[\log\frac{|\mathbf{K}^*+\tilde{\mathbf{\Sigma}}_Y|}{|\tilde{\mathbf{\Sigma}}_Y|} - \log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|}\right] \quad (78)\\ &= \mu_0\bar{\beta}R_{0Z}(\mathbf{K}^*) + \mu_0\beta R_{0Y}(\mathbf{K}^*) \\ &\quad + \frac{\mu_s-\mu_p\lambda}{2}\left[\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Y|}{|\mathbf{\Sigma}_Y|} - \log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|}\right] \quad (79)\\ &= \mu_0\bar{\beta}R_{0Z}(\mathbf{K}^*) + \mu_0\beta R_{0Y}(\mathbf{K}^*) + (\mu_s-\mu_p\lambda)R_s(\mathbf{K}^*) \quad (80)\\ &= \mu_0 R_0^* + (\mu_s-\mu_p\lambda)R_s^* \quad (81)\end{aligned}$$

where (76) comes from the fact that $0 < \beta = 1 - \bar{\beta} < 1$, (77) is due to the Markov chain in (73), (78) can be obtained by using the analysis in [9, eqns (30)-(32)], (79) comes from the third part of Lemma 4, and (81) is due to our assumption that $R_0^* = R_{0Y}(\mathbf{K}^*) = R_{0Z}(\mathbf{K}^*)$. Thus, (81) implies

$$L \leq \mu_0 R_0^* + (\mu_s - \mu_p\lambda)R_s^* \quad (82)$$

Comparing (75) and (82) yields

$$R_s^o \leq R_s^* \quad (83)$$

Using (70) and (83) and noting $\mu_s > \mu_p$, we can get

$$\mu_p R_p^o + \mu_s R_s^o \leq \mu_p R_p^* + \mu_s R_s^* \tag{84}$$

which contradicts with (65); proving (64). This completes the converse proof for this case.

Now we recap our proof for the current case. Similar to Section IV-B.1, here also, we prove the optimality of Gaussian signalling indirectly, i.e., we show the desired identity $g(R_0^*) = f(R_0^*)$ indirectly. First, we show that for the given common message rate $R_0^*$, $R_s^* + R_p^*$ achieves the sum capacity of the public and confidential messages, see (70). Secondly, we show that $(R_0^*, 0, R_s^*)$ is also on the boundary of the capacity region $\mathcal{C}_p(\mathbf{S})$ by obtaining (82). These two findings give us the inequalities in (70) and (83). Finally, we use a time-sharing argument for these two inequalities in (70) and (83) to establish $g(R_0^*) = f(R_0^*)$, which completes the proof.

*3) $R_0^* = R_{0Z}(\mathbf{K}^*) < R_{0Y}(\mathbf{K}^*)$:* We have $\lambda = \beta_Y = 0$, see (44)-(45). Hence, the KKT condition in (43) reduces to

$$\mu_s(\mathbf{K}^* + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M} = (\mu_s + \beta_Z)(\mathbf{K}^* + \mathbf{\Sigma}_Z)^{-1} + \mathbf{M}_S \tag{85}$$

Here we prove the desired identity $g(R_0^*) = f(R_0^*)$ directly. To this end, we define a new covariance matrix $\tilde{\mathbf{\Sigma}}_Y$ as follows

$$\mu_s(\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Y)^{-1} = \mu_s(\mathbf{K}^* + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M} \tag{86}$$

This new covariance matrix $\tilde{\mathbf{\Sigma}}_Y$ has the same useful properties with the one defined in (71), which are given in Lemma 4. Using this new covariance matrix $\tilde{\mathbf{\Sigma}}_Y$, we define $\tilde{\mathbf{Y}}$ as

$$\tilde{\mathbf{Y}} = \mathbf{X} + \tilde{\mathbf{N}}_Y \tag{87}$$

where $\tilde{\mathbf{N}}_Y$ is a Gaussian random vector with covariance matrix $\tilde{\mathbf{\Sigma}}_Y$. Due to the first statement of Lemma 4, we have the following Markov chain

$$U \to V \to \mathbf{X} \to \tilde{\mathbf{Y}} \to \mathbf{Y}, \mathbf{Z} \tag{88}$$

Next, we study the following optimization problem

$$L = \max_{(R_0, R_p, R_s) \in \mathcal{C}_p(\mathbf{S})} (\mu_p + \beta_Z) R_0 + \mu_p R_p + \mu_s R_s \tag{89}$$

We note the following lower bound for (89)

$$(\mu_p + \beta_Z) R_0^* + f(R_0^*) \leq L \tag{90}$$

We next obtain the maximum for (89). To this end, we obtain an explicit form for this optimization problem as follows.

**Lemma 5** *For $\mu_s > \mu_p$, we have*

$$L = \max_{\substack{U \to V \to \mathbf{X} \to (\mathbf{Y}, \mathbf{Z}) \\ E[\mathbf{X}\mathbf{X}^\top] \preceq \mathbf{S}}} (\mu_p + \beta_Z) \min\{I(U;\mathbf{Y}), I(U;\mathbf{Z})\} + \mu_p I(V;\mathbf{Z}|U) + \mu_s \left[I(V;\mathbf{Y}|U) - I(V;\mathbf{Z}|U)\right] \tag{91}$$

We now consider the maximization in (91) as follows

$$L \leq \max_{\substack{U \to V \to \mathbf{X} \to (\mathbf{Y}, \mathbf{Z}) \\ E[\mathbf{X}\mathbf{X}^\top] \preceq \mathbf{S}}} (\mu_p + \beta_Z) I(U;\mathbf{Z}) + \mu_p I(V;\mathbf{Z}|U) + \mu_s \left[I(V;\mathbf{Y}|U) - I(V;\mathbf{Z}|U)\right] \tag{92}$$

$$\leq \max_{\substack{U \to \mathbf{X} \to (\mathbf{Y}, \mathbf{Z}) \\ E[\mathbf{X}\mathbf{X}^\top] \preceq \mathbf{S}}} (\mu_p + \beta_Z) I(U;\mathbf{Z}) + \mu_p I(\mathbf{X};\mathbf{Z}|U) + \mu_s \left[I(\mathbf{X};\tilde{\mathbf{Y}}|U) - I(\mathbf{X};\mathbf{Z}|U)\right] \tag{93}$$

$$= (\mu_p + \beta_Z) R_0^* + \mu_p R_p^* + \mu_s R_s^* \tag{94}$$

$$= (\mu_p + \beta_Z) R_0^* + g(R_0^*) \tag{95}$$

where (92) is due to $\min\{a, b\} \leq a$, (93) comes from the Markov chain in (88), (94) can be shown by using Lemma 4 and the extremal inequality in [3, Corollary 4]. Comparison of (95) and (90) reveals $g(R_0^*) = f(R_0^*)$, which completes the converse proof for this case.

## V. Conclusions

We study the Gaussian MIMO wiretap channel, and obtain its entire capacity-equivocation region. To this end, we first establish an equivalence between the original definition of the wiretap channel and the wiretap channel with public messages. We obtain capacity regions for both cases. In particular, we show the sufficiency of jointly Gaussian auxiliary random variables and channel input to evaluate the single-letter description of the capacity-equivocation region due to [1]. We prove this by using channel enhancement [2] and an extremal inequality from [3].

## References


[1] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, IT-24(3):339–348, May 1978.

[2] H. Weingarten, Y. Steinberg, and S. Shamai (Shitz). The capacity region of the Gaussian multiple-input multiple-output broadcast channel. *IEEE Trans. Inf. Theory*, 52(9):3936–3964, Sep. 2006.

[3] 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. Inf. Theory*, 55(11):5011–5023, Nov. 2009.

[4] I. Csiszar and J. Korner. *Information theory: Coding theorems for discrete memoryless systems*. Academic, 1982.

[5] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz). The capacity-equivocation region of the MIMO Gaussian wiretap channel. In *IEEE ISIT*, Jun. 2010.

[6] F. Oggier and B. Hassibi. The secrecy capacity of the MIMO wiretap channel. Submitted to *IEEE Trans. Inf. Theory*, Oct. 2007. Also available at [arXiv:0710.1920].

[7] A. Khisti and G. Wornell. Secure transmission with multiple antennas II: The MIMOME channel. *IEEE Trans. Inf. Theory*, to appear. Also available at http://allegro.mit.edu/bin/pubs-search.php.

[8] S. Shafiee, N. Liu, and S. Ulukus. Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel. *IEEE Trans. Inf. Theory*, 55(9):4033–4039, Sep. 2009.

[9] H. D. Ly, T. Liu, and Y. Liang. Multiple-input multiple-output Gaussian broadcast channels with common and confidential messages. Submitted to *IEEE Trans. Inf. Theory*, Jul. 2009. Also available at http://www.ece.tamu.edu/∼tieliu/publications.html.

[10] H. Weingarten, Y. Steinberg, and S. Shamai (Shitz). On the capacity region of the multi-antenna broadcast channel with common messages. In *IEEE ISIT*, Jul. 2006.

[11] A. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54(8):1355–1387, Jan. 1975.

[12] E. Ekrem and S. Ulukus. Capacity-equivocation region of the Gaussian MIMO wiretap channel. Submitted to *IEEE Trans. Inf. Theory*, May 2010. Also available at [arXiv:1005.0419].

[13] J. Korner and K. Marton. General broadcast channels with degraded message sets. *IEEE Trans. Inf. Theory*, 23(1):60–64, Jan. 1977.

[14] T. Liu and S. Shamai (Shitz). A note on the secrecy capacity of the multi-antenna wiretap channel. *IEEE Trans. Inf. Theory*, 55(6):2547–2553, Jun. 2009.