

New Results on Multiple-Input Multiple-Output Broadcast Channels with Confidential Messages

Ruoheng Liu, Tie Liu, H. Vincent Poor, and Shlomo Shamai (Shitz)

Abstract—This paper presents two new results on multiple-input multiple-output (MIMO) Gaussian broadcast channels with confidential messages. First, the problem of the MIMO Gaussian wiretap channel is revisited. A matrix characterization of the capacity-equivocation region is provided, which extends the previous result on the secrecy capacity of the MIMO Gaussian wiretap channel to the general, possibly imperfect secrecy setting. Next, the problem of MIMO Gaussian broadcast channels with two receivers and three independent 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 secret from the other, is considered. A precise characterization of the capacity region is provided, generalizing the previous results which considered only two out of three possible messages.

Index Terms—Multiple-input multiple-output (MIMO) communication, wiretap channel, capacity-equivocation region, broadcast channel, confidential message

I. INTRODUCTION

Information-theoretic security has been a very active area of research recently. (See [1] and [2] for overviews of recent progress in this field.) In particular, significant progress has been made in understanding the fundamental limits of multiple-input multiple-output (MIMO) secret communication. More specifically, the secrecy capacity of the MIMO Gaussian wiretap channel was characterized in [3]–[7]. The works [8] and [9] considered the problem of MIMO Gaussian broadcast channels with two confidential messages, each intended for one receiver but needing to be kept asymptotically perfectly secret from the other, and provided a precise characterization of the capacity region. The capacity region of the MIMO Gaussian broadcast channel with two receivers and two independent messages, a common message intended for both receivers and a confidential message intended for one of the receivers but

This research was supported by the National Science Foundation under Grant CNS-09-05398, CCF-08-45848 and CCF-09-16867, by the Air Force Office of Scientific Research under Grant FA9550-08-1-0480, by the European Commission in the framework of the FP7 Network of Excellence in Wireless Communications NEWCOM++, and by the Israel Science Foundation. The material in this paper was presented in part at the IEEE International Symposium on Information Theory (ISIT), Austin, TX, June 2010.

Ruoheng Liu is with Alcatel-Lucent, Murray Hill, NJ 07974, USA (email: ruoheng.liu@alcatel-lucent.com).

Tie Liu is with the Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843, USA (e-mail: tieliu@tamu.edu).

H. Vincent Poor is with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA (e-mail: poor@princeton.edu).

Shlomo Shamai (Shitz) is with the Department of Electrical Engineering, Technion-Israel Institute of Technology, Technion City, Haifa 32000, Israel (e-mail: sshlomo@ee.technion.ac.il).

needing to be kept asymptotically perfectly secret from the other, was characterized in [10].

This paper presents two new results on MIMO Gaussian broadcast channels with confidential messages¹:

- 1) The problem of the MIMO Gaussian wiretap channel is revisited. A matrix characterization of the *capacity-equivocation* region is provided, which extends the result of [6] on the secrecy capacity of the MIMO Gaussian wiretap channel to the general, possibly imperfect secrecy setting.
- 2) The problem of MIMO Gaussian broadcast channels with two receivers and *three* independent messages, a common message intended for both receivers, and two mutually confidential messages each intended for one of the receivers but needing to be kept asymptotically perfectly secret from the other, is considered. A precise characterization of the capacity region is provided, generalizing the results of [9] and [10] which considered only two out of three possible messages.

Notation. Vectors and matrices are written in bold letters. All vectors by default are column vectors. The identity matrices are denoted by \mathbf{I} , where a subscript may be used to indicate the size of the matrix to avoid possible confusion. The transpose of a matrix \mathbf{A} is denoted by \mathbf{A}^\top , and the trace of a square matrix \mathbf{A} is denoted by $\text{Tr}(\mathbf{A})$. Finally, we write $\mathbf{A} \preceq \mathbf{B}$ (or, equivalently, $\mathbf{B} \succeq \mathbf{A}$) whenever $\mathbf{B} - \mathbf{A}$ is positive semidefinite.

II. THE CAPACITY-EQUIVOCATION REGION OF THE MIMO GAUSSIAN WIRETAP CHANNEL

A. Channel Model

Consider a MIMO Gaussian broadcast channel with two receivers, one of which is a legitimate receiver and the other is an eavesdropper. The received signals at time index m are given by

$$\begin{aligned} \mathbf{Y}[m] &= \mathbf{H}_r \mathbf{X}[m] + \mathbf{W}_r[m] \\ \mathbf{Z}[m] &= \mathbf{H}_e \mathbf{X}[m] + \mathbf{W}_e[m] \end{aligned} \quad (1)$$

where \mathbf{H}_r and \mathbf{H}_e are (real) channel matrices at the legitimate receiver and the eavesdropper respectively, and $\{\mathbf{W}_r[m]\}_m$ and $\{\mathbf{W}_e[m]\}_m$ are independent and identically distributed (i.i.d.) additive vector Gaussian noise processes with zero means and *identity* covariance matrices.

¹The main results of this paper were initially posted on the arXiv website in January 2010 [11] and were subsequently reported at the 2010 IEEE International Symposium on Information Theory [12], [13]. Similar results were independently reported by Ekrem and Ulukus in [14] and [15].

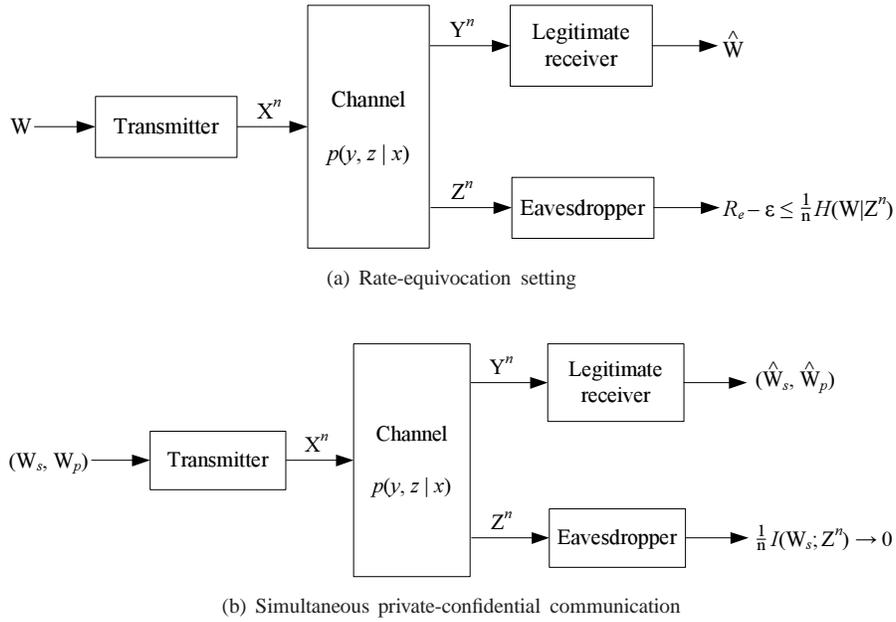


Fig. 1. Wiretap channel.

The transmitter has a single message W , which is uniformly distributed over $\{1, \dots, 2^{nR}\}$ where R is the *rate* of communication. The goal of communication is to deliver W reliably to the legitimate receiver while keeping it information-theoretically secure from the eavesdropper. Following the classical work [16], [17], for every $\epsilon > 0$ it is required that

$$\frac{1}{n} H(W|Z^n) \geq R_e - \epsilon \quad (2)$$

for sufficiently large n , where n is the block length of communication, $\mathbf{Z}^n := (\mathbf{Z}[1], \dots, \mathbf{Z}[n])$, and R_e represents the predetermined level of security of message W at the eavesdropper known as *equivocation*. The *capacity-equivocation* region is the set of rate-equivocation pairs (R, R_e) that can be achieved by *any* coding scheme. In the literature, this communication scenario is usually known as the rate-equivocation setting of the MIMO Gaussian *wiretap* channel; see Fig. 1(a) for an illustration.

Csiszár and Körner [17] studied the rate-equivocation setting of a general discrete memoryless wiretap channel. A single-letter expression for the capacity-equivocation region was derived [17, Theorem 1], which can be written as the set of nonnegative rate-equivocation pairs (R, R_e) satisfying

$$\begin{aligned} R_e &\leq \min\{R, I(V; Y|U) - I(V; Z|U)\} \\ R &\leq I(V; Y) \end{aligned} \quad (3)$$

for some $p(u, v, x, y, z) = p(u)p(v|u)p(x|v)p(y, z|x)$. Here, $p(y, z|x)$ is the transition probability of the discrete memoryless wiretap channel, and U and V are two *auxiliary* random variables. In theory, a computable expression for the capacity-equivocation region can be obtained by evaluating the single-letter expression (3) for the MIMO Gaussian wiretap channel (1). However, such an evaluation is generally difficult due to the presence of the auxiliary random variables U and V .

Several recent works [3]–[7] studied the special case where

the equivocation R_e is set to equal the communication rate R . In this case, the secrecy constraint (2) can be equivalently written as

$$\frac{1}{n} I(W; \mathbf{Z}^n) \leq \epsilon \quad (4)$$

i.e., message W needs to be asymptotically *perfectly* secure from the eavesdropper. Under the asymptotic perfect secrecy constraint (2), the maximum rate of communication is called the *secrecy* capacity. For the MIMO Gaussian wiretap channel (1), a matrix characterization of the secrecy capacity was obtained in [3]–[5] under an average total power constraint and in [6] and [7] under a more general *matrix* power constraint. Similar matrix characterizations of the capacity-equivocation region, however, were *unknown*.

B. Main Results

The main result of this section is a matrix characterization of the capacity-equivocation region of the MIMO Gaussian wiretap channel. More specifically, consider the MIMO Gaussian wiretap channel (1) under the matrix power constraint

$$\frac{1}{n} \sum_{m=1}^n (\mathbf{X}[m] \mathbf{X}^T[m]) \preceq \mathbf{S} \quad (5)$$

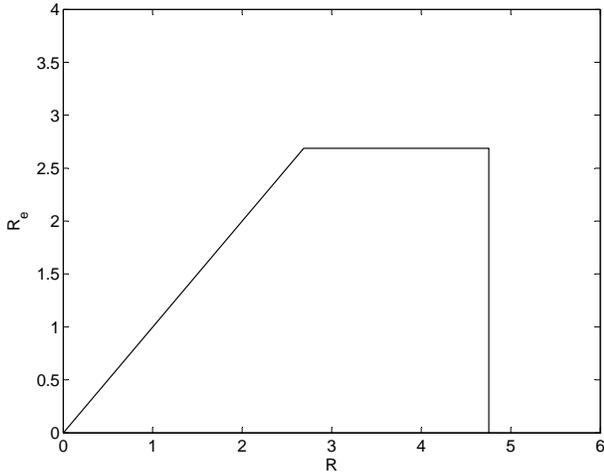
where \mathbf{S} is a positive semidefinite matrix. Let

$$C(\mathbf{S}, \mathbf{H}_r) = \frac{1}{2} \log |\mathbf{I} + \mathbf{H}_r \mathbf{S} \mathbf{H}_r^T| \quad (6)$$

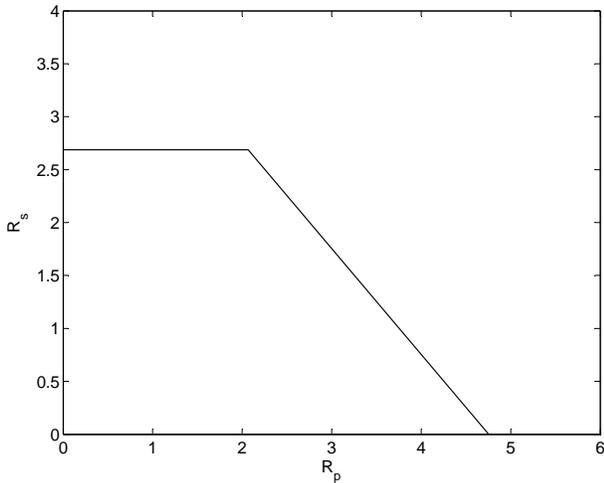
be the Shannon capacity of a MIMO Gaussian point-to-point channel with channel matrix \mathbf{H}_r and under the matrix power constraint (5), and let

$$C_s(\mathbf{S}, \mathbf{H}_r, \mathbf{H}_e) = \max_{0 \preceq \mathbf{B} \preceq \mathbf{S}} \frac{1}{2} \log \left| \frac{\mathbf{I} + \mathbf{H}_r \mathbf{B} \mathbf{H}_r^T}{\mathbf{I} + \mathbf{H}_e \mathbf{B} \mathbf{H}_e^T} \right| \quad (7)$$

be the secrecy capacity of a MIMO Gaussian wiretap channel with legitimate receiver and eavesdropper channel matrices \mathbf{H}_r



(a) Capacity-equivocation region



(b) Private-confidential message capacity region

Fig. 2. MIMO Gaussian wiretap channel under matrix power constraint.

and \mathbf{H}_e respectively and under the matrix power constraint (5) [6], [7]. We then have the following result.

Theorem 1: The capacity-equivocation region of the MIMO Gaussian wiretap channel (1) under the matrix power constraint (5) is given by the set of nonnegative rate-equivocation pairs (R, R_e) satisfying

$$\begin{aligned} R_e &\leq \min\{R, C_s(\mathbf{S}, \mathbf{H}_r, \mathbf{H}_e)\} \\ R &\leq C(\mathbf{S}, \mathbf{H}_r) \end{aligned} \quad (8)$$

where $C(\mathbf{S}, \mathbf{H}_r)$ and $C_s(\mathbf{S}, \mathbf{H}_r, \mathbf{H}_e)$ are defined as in (6) and (7), respectively.

Fig. 2(a) illustrates the capacity-equivocation region of a MIMO Gaussian wiretap channel with channel matrices

$$\mathbf{H}_r = \begin{pmatrix} 1.8 & 2.0 \\ 1.0 & 3.0 \end{pmatrix} \quad \text{and} \quad \mathbf{H}_e = \begin{pmatrix} 3.3 & 1.3 \\ 2.0 & -1.5 \end{pmatrix}$$

(which yields a *nondegraded* wiretap channel) and matrix power constraint

$$\mathbf{S} = \begin{pmatrix} 5.0 & 1.25 \\ 1.25 & 10.0 \end{pmatrix}.$$

The capacity-equivocation region of the MIMO Gaussian wiretap channel under an average total power constraint is summarized in the following corollary. The result is a direct consequence of Theorem 1 and [18, Lemma 1].

Corollary 1: The capacity-equivocation region of the MIMO Gaussian wiretap channel (1) under the average total power constraint

$$\frac{1}{n} \sum_{m=1}^n (\mathbf{X}[m]^T \mathbf{X}[m]) \leq P \quad (9)$$

is given by the set of nonnegative rate-equivocation pairs (R, R_e) satisfying

$$\begin{aligned} R_e &\leq \min\{R, C_s(\mathbf{S}, \mathbf{H}_r, \mathbf{H}_e)\} \\ R &\leq C(\mathbf{S}, \mathbf{H}_r) \end{aligned} \quad (10)$$

for some $\mathbf{S} \succeq 0$, $\text{Tr}(\mathbf{S}) \leq P$.

C. Proof of the Main Results

Next, we prove Theorem 1. As mentioned previously, directly evaluating the single-letter expression (3) for the MIMO Gaussian wiretap channel (1) is difficult due to the presence of the auxiliary random variables. We thus resort to an *indirect* approach that connects the rate-equivocation setting of a MIMO Gaussian wiretap channel to the problem of simultaneously communicating private and confidential messages.

The problem of simultaneously communicating private and confidential messages over a discrete memoryless wiretap channel is illustrated in Fig. 1(b). Here, the transmitter has a private message W_p , which is uniformly distributed over $\{1, \dots, 2^{nR_p}\}$, and a confidential message W_s , which is uniformly distributed over $\{1, \dots, 2^{nR_s}\}$. The confidential message W_s is intended for the legitimate receiver but needs to be kept asymptotically *perfectly* secret from the eavesdropper. That is, for any $\epsilon > 0$ it is required that

$$\frac{1}{n} I(W_s; Z^n) \leq \epsilon \quad (11)$$

for sufficiently large block length n . The private message W_p is also intended for the legitimate receiver, but is *not* subject to any secrecy constraint. The *private-confidential* message capacity region is the set of private-confidential rate pairs (R_p, R_s) that can be achieved by *any* coding scheme.

The following lemma provides a single-letter characterization of the private-confidential message capacity region of the discrete memoryless wiretap channel.

Lemma 1: The private-confidential message capacity region of the discrete memoryless wiretap channel $p(y, z|x)$ is given by the set of nonnegative private-confidential rate pairs (R_p, R_s) satisfying

$$\begin{aligned} R_s &\leq I(V; Y|U) - I(V; Z|U) \\ R_s + R_p &\leq I(V; Y) \end{aligned} \quad (12)$$

for some $p(u, v, x, y, z) = p(u)p(v|u)p(x|v)p(y, z|x)$, where U and V are auxiliary random variables.

The achievability part of the lemma can be proved by considering a coding scheme that combines superposition coding, random binning, and rate splitting. In particular, part of the private message will be used in the binning scheme

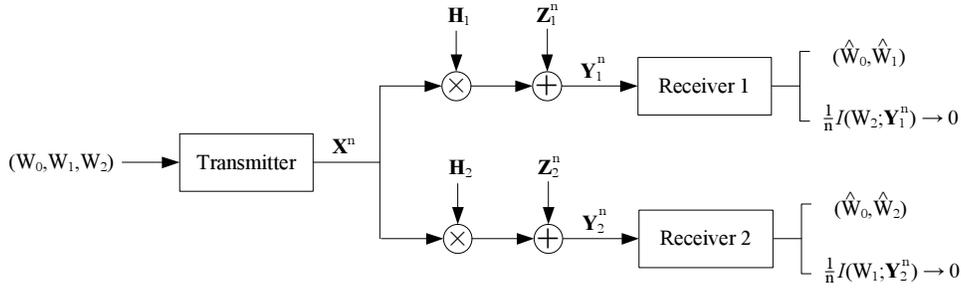


Fig. 3. MIMO Gaussian broadcast channel with common and confidential messages.

to protect the confidential message against the eavesdropper. The converse proof follows standard information-theoretic argument. The details of the proof are deferred to Appendix A.

A simple inspection of the capacity-equivocation region (3) and the private-confidential message capacity region (12) reveals the following interesting fact:

Fact 1: A nonnegative rate pair $(R, R_e) = (R_p + R_s, R_s)$ is an achievable rate-equivocation pair for a discrete memoryless wiretap channel if and only if (R_p, R_s) is an achievable private-confidential rate pair for the same channel.

The “if” part of the fact is easy to verify: Simply use the *same* code for both communication scenarios and view (W_p, W_s) as the single message W for the rate-equivocation setting. Note that

$$\begin{aligned} \frac{1}{n}H(W|Z^n) &= \frac{1}{n}H(W_p, W_s|Z^n) \\ &\geq \frac{1}{n}H(W_s|Z^n) \\ &\geq R_s - \epsilon \\ &= R_e - \epsilon. \end{aligned}$$

Thus, the same code satisfying the secrecy constraint (11) for simultaneous private-confidential communication also satisfies the secrecy constraint (2) for the rate-equivocation setting. The “only if” part of the fact comes as a mild surprise, as in the rate-equivocation setting which part of message is secure does not need to be specified *a priori* and may even depend on the realization of the channel noise. We note here that the above interesting fact was first mentioned in [19, pp. 411–412] without proof.

In light of Fact 1, next we first establish a matrix characterization of the private-confidential message capacity region using the existing matrix characterization [6], [7] on the secrecy capacity of the MIMO Gaussian wiretap channel. The result will then be mapped to the rate-equivocation setting using the aforementioned equivalence between these two communication scenarios.

Lemma 2: The private-confidential message capacity region of the MIMO Gaussian wiretap channel (1) under the matrix power constraint (5) is given by the set of nonnegative private-confidential rate pairs (R_p, R_s) satisfying

$$\begin{aligned} R_s &\leq C_s(\mathbf{S}, \mathbf{H}_r, \mathbf{H}_e) \\ R_s + R_p &\leq C(\mathbf{S}, \mathbf{H}_r). \end{aligned} \quad (13)$$

Proof: Let \mathbf{B}^* be an optimal solution to the optimization problem on the right-hand side of (7). Then, the achievability

of the private-confidential rate region (13) follows from that of (12) by setting $\mathbf{V} = \mathbf{X} = \mathbf{U} + \mathbf{G}$, where \mathbf{U} and \mathbf{G} denote two independent Gaussian vectors with zero means and covariance matrices $\mathbf{S} - \mathbf{B}^*$ and \mathbf{B}^* , respectively.

The fact that $R_s \leq C_s(\mathbf{S}, \mathbf{H}_r, \mathbf{H}_e)$ for any achievable confidential rate R_s follows from the secrecy capacity result of [6] and [7] on the MIMO Gaussian wiretap channel under a matrix power constraint, by ignoring the private message W_p . The fact that $R_s + R_p \leq C(\mathbf{S}, \mathbf{H}_r)$ for any achievable private-confidential rate pair (R_p, R_s) follows from the well-known capacity result on the MIMO Gaussian point-to-point channel under a matrix power constraint, by viewing (W_p, W_s) as a single message and ignoring the asymptotic perfect secrecy constraint (11) on the confidential message W_s . ■

Remark 1: It is particularly worth mentioning the corner point (R_p, R_s) of the private-confidential message capacity region (13) as given by

$$(R_p, R_s) = (C(\mathbf{S}, \mathbf{H}_r) - C_s(\mathbf{S}, \mathbf{H}_r, \mathbf{H}_e), C_s(\mathbf{S}, \mathbf{H}_r, \mathbf{H}_e)).$$

Here, under the matrix power constraint, both messages W_s and (W_p, W_s) , viewed as a single private message, can transmit *simultaneously* at their respective *maximum* rates. In particular, transmitting an additional private message W_p does *not* incur any rate loss for communicating the confidential message W_s .

Now, Theorem 1 follows immediately from Lemma 2 and a Fourier-Motzkin elimination with $R = R_p + R_s$ and $R_e = R_s$. For comparison, the private-confidential message capacity region of the same MIMO Gaussian wiretap channel as used for Fig. 2(a) is illustrated in Fig. 2(b).

III. MIMO GAUSSIAN BROADCAST CHANNELS WITH COMMON AND CONFIDENTIAL MESSAGES

A. Channel Model

Consider a two-receiver MIMO Gaussian broadcast channel. The transmitter is equipped with t transmit antennas, and receiver k , $k = 1, 2$, is equipped with r_k receive antennas. A discrete-time sample of the channel at time m can be written as

$$\mathbf{Y}_k[m] = \mathbf{H}_k \mathbf{X}[m] + \mathbf{Z}_k[m], \quad k = 1, 2 \quad (14)$$

where \mathbf{H}_k are the (real) channel matrices of size $r_k \times t$, and $\{\mathbf{Z}_k[m]\}_m$ are i.i.d. additive vector Gaussian noise processes

with zero means and identity covariance matrices.²

As illustrated in Fig. 3, the transmitter has a common message W_0 and two independent confidential messages W_1 and W_2 . The common message W_0 is intended for both receivers. The confidential message W_k is intended for receiver k but needs to be kept asymptotically perfectly secret from the other receiver. Mathematically, for every $\epsilon > 0$ we must have

$$\frac{1}{n}I(W_1; \mathbf{Y}_2^n) \leq \epsilon \quad \text{and} \quad \frac{1}{n}I(W_2; \mathbf{Y}_1^n) \leq \epsilon \quad (15)$$

for sufficiently large block length n . Our goal here is to characterize the entire capacity region $\mathcal{C}(\mathbf{H}_1, \mathbf{H}_2, \mathbf{S}) = \{(R_0, R_1, R_2)\}$ that can be achieved by any coding scheme, where R_0, R_1 and R_2 are the communication rates corresponding to the common message W_0 and the confidential messages W_1 and W_2 , respectively.

With both confidential messages W_1 and W_2 but *without* the common message W_0 , the problem was studied in [8] for the multiple-input single-output (MISO) case and in [9] for general MIMO case. Rather surprisingly, it was shown in [9] that, under a matrix power constraint both confidential messages can be *simultaneously* communicated at their respected maximum rates. With the common message W_0 and only *one* confidential message (W_1 or W_2), the capacity region of the MIMO Gaussian wiretap channel was characterized in [10] using a channel-enhancement approach [18] and an extremal entropy inequality of Weingarten *et al.* [21].

B. Main Results

The main result of this section is a precise characterization of the capacity region of the MIMO Gaussian broadcast channel with a more complete message set that includes a common message W_0 and two independent confidential messages W_1 and W_2 .

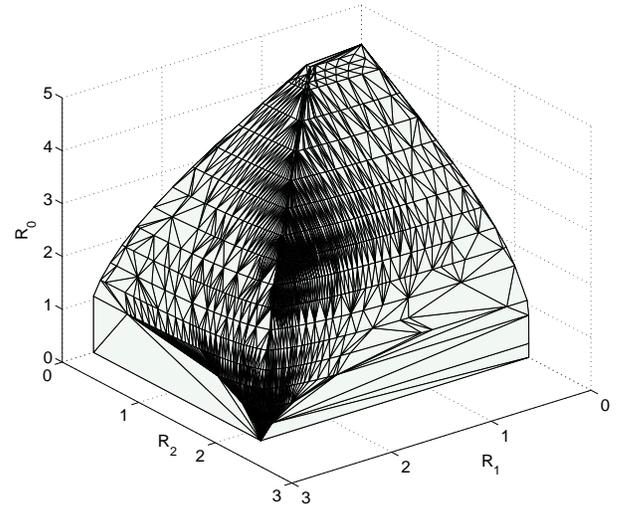
Theorem 2: The capacity region $\mathcal{C}(\mathbf{H}_1, \mathbf{H}_2, \mathbf{S})$ of the MIMO Gaussian broadcast channel (14) with a common message W_0 and two confidential messages W_1 and W_2 under the matrix power constraint (5) is given by the set of nonnegative rate triples (R_0, R_1, R_2) such that

$$\begin{aligned} R_0 &\leq \min \left\{ \frac{1}{2} \log \left| \frac{\mathbf{H}_1 \mathbf{S} \mathbf{H}_1^T + \mathbf{I}_{r_1}}{\mathbf{H}_1 (\mathbf{S} - \mathbf{B}_0) \mathbf{H}_1^T + \mathbf{I}_{r_1}} \right|, \right. \\ &\quad \left. \frac{1}{2} \log \left| \frac{\mathbf{H}_2 \mathbf{S} \mathbf{H}_2^T + \mathbf{I}_{r_2}}{\mathbf{H}_2 (\mathbf{S} - \mathbf{B}_0) \mathbf{H}_2^T + \mathbf{I}_{r_2}} \right| \right\} \\ R_1 &\leq \frac{1}{2} \log |\mathbf{I}_{r_1} + \mathbf{H}_1 \mathbf{B}_1 \mathbf{H}_1^T| - \\ &\quad \frac{1}{2} \log |\mathbf{I}_{r_2} + \mathbf{H}_2 \mathbf{B}_1 \mathbf{H}_2^T| \\ R_2 &\leq \frac{1}{2} \log \left| \frac{\mathbf{I}_{r_2} + \mathbf{H}_2 (\mathbf{S} - \mathbf{B}_0) \mathbf{H}_2^T}{\mathbf{I}_{r_2} + \mathbf{H}_2 \mathbf{B}_1 \mathbf{H}_2^T} \right| - \\ &\quad \frac{1}{2} \log \left| \frac{\mathbf{I}_{r_1} + \mathbf{H}_1 (\mathbf{S} - \mathbf{B}_0) \mathbf{H}_1^T}{\mathbf{I}_{r_1} + \mathbf{H}_1 \mathbf{B}_1 \mathbf{H}_1^T} \right| \end{aligned} \quad (16)$$

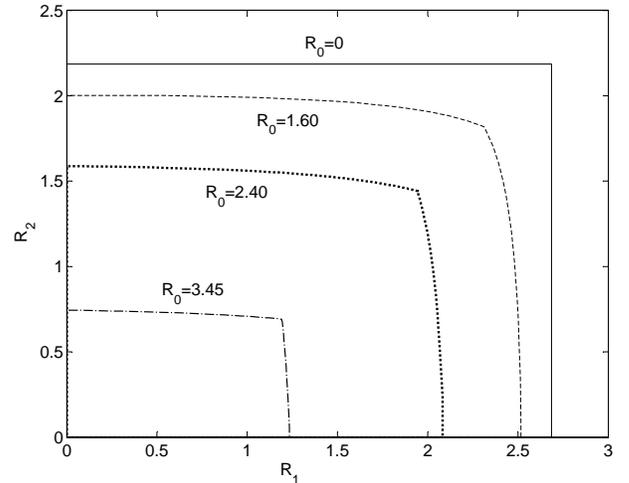
for some $\mathbf{B}_0 \succeq 0$, $\mathbf{B}_1 \succeq 0$ and $\mathbf{B}_0 + \mathbf{B}_1 \preceq \mathbf{S}$.

Remark 2: By setting $\mathbf{B}_0 = 0$ we can recover the result of [9, Theorem 1] that includes both confidential messages W_1 and W_2 but without the common message W_0 . Similar to [9, Theorem 1], for any given \mathbf{B}_0 the upper bounds on R_1 and R_2 can be simultaneously maximized by a same \mathbf{B}_1 . In fact, the upper bounds on R_1 and R_2 in (16) are fully symmetric

²The channel model is the same as that in Section II-A. However, different notation is used here for the convenience of presentation.



(a) Capacity region $\mathcal{C}(\mathbf{H}_1, \mathbf{H}_2, \mathbf{S})$



(b) (R_1, R_2) -cross sections

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

with respect to \mathbf{H}_1 and \mathbf{H}_2 , even though it is not immediately evident from the expressions themselves.

Remark 3: By setting $\mathbf{B}_0 = \mathbf{S} - \mathbf{B}_1$ we can recover the result of [10, Theorem 1] that includes the common message W_0 and the confidential message W_1 but without the other confidential message W_2 .

Fig. 4(a) illustrates the capacity region $\mathcal{C}(\mathbf{H}_1, \mathbf{H}_2, \mathbf{S})$ for the channel matrices and the matrix power constraint as given by

$$\begin{aligned} \mathbf{H}_1 &= \begin{pmatrix} 1.8 & 2.0 \\ 1.0 & 3.0 \end{pmatrix}, \quad \mathbf{H}_2 = \begin{pmatrix} 3.3 & 1.3 \\ 2.0 & -1.5 \end{pmatrix} \\ \text{and} \quad \mathbf{S} &= \begin{pmatrix} 5.0 & 1.25 \\ 1.25 & 10.0 \end{pmatrix}. \end{aligned}$$

(The channel parameters are the same as those used for Fig. 2.) In Fig. 4(b), we have also plotted the (R_1, R_2) -cross section of $\mathcal{C}(\mathbf{H}_1, \mathbf{H}_2, \mathbf{S})$ for several given values of R_0 . Note that when $R_0 = 0$, the (R_1, R_2) -cross section is *rectangular*, implying that under a matrix power constraint, both confidential

messages W_1 and W_2 can be simultaneously transmitted at their respective maximum rates [9]. For $R_0 > 0$, however, the (R_1, R_2) -cross sections are generally non-rectangular as different boundary points on the same cross section may correspond to *different* choice of \mathbf{B}_0 .

The capacity region under an average total power constraint is summarized in the following corollary. The result is a direct consequence of Theorem 2 and [18, Lemma 1].

Corollary 2: The capacity region $\mathcal{C}(\mathbf{H}_1, \mathbf{H}_2, P)$ of the MIMO Gaussian broadcast channel (14) with a common message W_0 and two confidential messages W_1 and W_2 under the average total power constraint (9) is given by

$$\mathcal{C}(\mathbf{H}_1, \mathbf{H}_2, P) = \bigcup_{\mathbf{S} \succeq 0, \text{Tr}(\mathbf{S}) \leq P} \mathcal{C}(\mathbf{H}_1, \mathbf{H}_2, \mathbf{S}). \quad (17)$$

C. Proof of the Main Results

Next, we prove Theorem 2. Following [18], we shall focus on the canonical case in which the channel matrices \mathbf{H}_1 and \mathbf{H}_2 are square and invertible and the matrix power constraint \mathbf{S} is strictly positive definite. In this case, multiplying both sides of (14) by \mathbf{H}_k^{-1} , the MIMO Gaussian broadcast channel (14) can be equivalently written as

$$\mathbf{Y}_k[m] = \mathbf{X}_k[m] + \mathbf{Z}_k[m], \quad k = 1, 2 \quad (18)$$

where $\{\mathbf{Z}_k[m]\}_m$ are i.i.d. additive vector Gaussian noise processes with zero means and covariance matrices $\mathbf{N}_k = \mathbf{H}_k^{-1} \mathbf{H}_k^{-\top}$. Similarly, the rate region (16) can be equivalently written as

$$\begin{aligned} R_0 &\leq \min \left\{ \frac{1}{2} \log \left| \frac{\mathbf{S} + \mathbf{N}_1}{(\mathbf{S} - \mathbf{B}_0) + \mathbf{N}_1} \right|, \frac{1}{2} \log \left| \frac{\mathbf{S} + \mathbf{N}_2}{(\mathbf{S} - \mathbf{B}_0) + \mathbf{N}_2} \right| \right\} \\ R_1 &\leq \frac{1}{2} \log \left| \frac{\mathbf{B}_1 + \mathbf{N}_1}{\mathbf{N}_1} \right| - \frac{1}{2} \log \left| \frac{\mathbf{B}_1 + \mathbf{N}_2}{\mathbf{N}_2} \right| \\ R_2 &\leq \frac{1}{2} \log \left| \frac{(\mathbf{S} - \mathbf{B}_0) + \mathbf{N}_2}{\mathbf{B}_1 + \mathbf{N}_2} \right| - \frac{1}{2} \log \left| \frac{(\mathbf{S} - \mathbf{B}_0) + \mathbf{N}_1}{\mathbf{B}_1 + \mathbf{N}_1} \right|. \end{aligned} \quad (19)$$

Next, we show that the rate region (19) over all possible $\mathbf{B}_0 \succeq 0$, $\mathbf{B}_1 \succeq 0$ and $\mathbf{B}_0 + \mathbf{B}_1 \preceq \mathbf{S}$ gives the capacity region $\mathcal{C}(\mathbf{H}_1, \mathbf{H}_2, \mathbf{S})$ for the canonical MIMO Gaussian broadcast channel (18). Extensions to the general model (14) follow from the well-known limiting argument [6], [10], [18] and hence are omitted from the paper.

To prove the achievability of the rate region (19), recall that the problem of a two-receiver discrete memoryless broadcast channel with a common message and two confidential common messages was studied in [22]. There, a single-letter expression for an achievable rate region was established, which is given by the set of rate triples (R_0, R_1, R_2) such that

$$\begin{aligned} R_0 &\leq \min[I(\mathbf{U}; \mathbf{Y}_1), I(\mathbf{U}; \mathbf{Y}_2)] \\ R_1 &\leq I(\mathbf{V}_1; \mathbf{Y}_1 | \mathbf{U}) - I(\mathbf{V}_1; \mathbf{V}_2, \mathbf{Y}_2 | \mathbf{U}) \\ R_2 &\leq I(\mathbf{V}_2; \mathbf{Y}_2 | \mathbf{U}) - I(\mathbf{V}_2; \mathbf{V}_1, \mathbf{Y}_1 | \mathbf{U}) \end{aligned} \quad (20)$$

where \mathbf{U} , \mathbf{V}_1 and \mathbf{V}_2 are auxiliary random variables satisfying the Markov relation $(\mathbf{U}, \mathbf{V}_1, \mathbf{V}_2) \rightarrow \mathbf{X} \rightarrow (\mathbf{Y}_1, \mathbf{Y}_2)$. The proposed coding scheme is a natural combination of double binning [23] and superposition coding. Thus, the achievability of the rate region (19) follows from that of (20) by setting $\mathbf{V}_1 = \mathbf{U}_1 + \mathbf{F}\mathbf{U}_2$, $\mathbf{V}_2 = \mathbf{U}_2$, and $\mathbf{X} = \mathbf{U} + \mathbf{U}_1 + \mathbf{U}_2$ where \mathbf{U} , \mathbf{U}_1 and \mathbf{U}_2 are three independent Gaussian vectors with

zero means and covariance matrices \mathbf{B}_0 , \mathbf{B}_1 and $\mathbf{S} - \mathbf{B}_0 - \mathbf{B}_1$ respectively, and

$$\mathbf{F} := \mathbf{B}\mathbf{H}_1^\top (\mathbf{I}_{r_1} + \mathbf{H}_1 \mathbf{B}\mathbf{H}_1^\top)^{-1} \mathbf{H}_1.$$

To show that the rate region (19) over all possible $\mathbf{B}_0 \succeq 0$, $\mathbf{B}_1 \succeq 0$ and $\mathbf{B}_0 + \mathbf{B}_1 \preceq \mathbf{S}$ is indeed the capacity region, we shall consider proof by contradiction and resort to a channel-enhancement argument akin to that in [10].

More specifically, assume that $(R_0^\dagger, R_1^\dagger, R_2^\dagger)$ is an *achievable* rate triple that lies *outside* the rate region (19) for any given $\mathbf{B}_0 \succeq 0$, $\mathbf{B}_1 \succeq 0$ and $\mathbf{B}_0 + \mathbf{B}_1 \preceq \mathbf{S}$. Since $(R_0^\dagger, R_1^\dagger, R_2^\dagger)$ is achievable, we can bound R_0^\dagger by

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

Moreover, if $R_1^\dagger = R_2^\dagger = 0$, then R_0^{\max} can be achieved by setting $\mathbf{B}_0 = \mathbf{S}$ and $\mathbf{B}_1 = 0$ in (19). Thus, by the assumption that $(R_0^\dagger, R_1^\dagger, R_2^\dagger)$ is outside the rate region (19) for any given $\mathbf{B}_0 \succeq 0$, $\mathbf{B}_1 \succeq 0$ and $\mathbf{B}_0 + \mathbf{B}_1 \preceq \mathbf{S}$, we can always find $\lambda_1 \geq 0$ and $\lambda_2 \geq 0$ such that

$$\lambda_1 R_1^\dagger + \lambda_2 R_2^\dagger = \lambda_1 R_1^* + \lambda_2 R_2^* + \rho \quad (21)$$

for some $\rho > 0$, where $\lambda_1 R_1^* + \lambda_2 R_2^*$ is given by

$$\begin{aligned} &\max_{(\mathbf{B}_0, \mathbf{B}_1)} \lambda_1 f_1(\mathbf{B}_1) + \lambda_2 f_2(\mathbf{B}_0, \mathbf{B}_1) \\ &\text{subject to } f_0(\mathbf{B}_0) \geq R_0^\dagger \\ &\mathbf{B}_0 \succeq 0 \\ &\mathbf{B}_1 \succeq 0 \\ &\mathbf{B}_0 + \mathbf{B}_1 \preceq \mathbf{S}. \end{aligned} \quad (22)$$

Here, the functions f_0 , f_1 and f_2 are defined as

$$\begin{aligned} f_0(\mathbf{B}_0) &:= \min \left\{ \frac{1}{2} \log \left| \frac{\mathbf{S} + \mathbf{N}_1}{(\mathbf{S} - \mathbf{B}_0) + \mathbf{N}_1} \right|, \right. \\ &\quad \left. \frac{1}{2} \log \left| \frac{\mathbf{S} + \mathbf{N}_2}{(\mathbf{S} - \mathbf{B}_0) + \mathbf{N}_2} \right| \right\} \\ f_1(\mathbf{B}_1) &:= \frac{1}{2} \log \left| \frac{\mathbf{B}_1 + \mathbf{N}_1}{\mathbf{N}_1} \right| - \frac{1}{2} \log \left| \frac{\mathbf{B}_1 + \mathbf{N}_2}{\mathbf{N}_2} \right| \\ \text{and } f_2(\mathbf{B}_0, \mathbf{B}_1) &:= \frac{1}{2} \log \left| \frac{(\mathbf{S} - \mathbf{B}_0) + \mathbf{N}_2}{\mathbf{B}_1 + \mathbf{N}_2} \right| \\ &\quad - \frac{1}{2} \log \left| \frac{(\mathbf{S} - \mathbf{B}_0) + \mathbf{N}_1}{\mathbf{B}_1 + \mathbf{N}_1} \right|. \end{aligned}$$

Let $(\mathbf{B}_0^*, \mathbf{B}_1^*)$ be an optimal solution to the optimization program (22). By assumption, the matrix power constraint \mathbf{S} is strictly positive definite in the canonical model. Thus, $(\mathbf{B}_0^*, \mathbf{B}_1^*)$ must satisfy the following Karush-Kuhn-Tucker (KKT) conditions:

$$\begin{aligned} (\beta_1 + \lambda_2)[(\mathbf{S} - \mathbf{B}_0^*) + \mathbf{N}_1]^{-1} + \beta_2[(\mathbf{S} - \mathbf{B}_0^*) + \mathbf{N}_2]^{-1} + \mathbf{M}_0 \\ = \lambda_2[(\mathbf{S} - \mathbf{B}_0^*) + \mathbf{N}_2]^{-1} + \mathbf{M}_2 \end{aligned} \quad (23)$$

$$\begin{aligned} (\lambda_1 + \lambda_2)(\mathbf{B}_1^* + \mathbf{N}_1)^{-1} + \mathbf{M}_1 \\ = (\lambda_1 + \lambda_2)(\mathbf{B}_1^* + \mathbf{N}_2)^{-1} + \mathbf{M}_2 \end{aligned} \quad (24)$$

$$\mathbf{M}_0 \mathbf{B}_0^* = 0, \mathbf{M}_1 \mathbf{B}_1^* = 0, \text{ and } \mathbf{M}_2(\mathbf{S} - \mathbf{B}_0^* - \mathbf{B}_1^*) = 0 \quad (25)$$

where \mathbf{M}_0 , \mathbf{M}_1 and \mathbf{M}_2 are positive semidefinite matrices, and β_k , $k = 1, 2$, are nonnegative real scalars such that $\beta_k > 0$ if

and only if

$$\frac{1}{2} \log \left| \frac{\mathbf{S} + \mathbf{N}_k}{(\mathbf{S} - \mathbf{B}_0^*) + \mathbf{N}_k} \right| = R_0^\dagger.$$

It follows that

$$\begin{aligned} & (\beta_1 + \beta_2)R_0^\dagger + \lambda_1 R_1^\dagger + \lambda_2 R_2^\dagger \\ &= \frac{\beta_1}{2} \log \left| \frac{\mathbf{S} + \mathbf{N}_1}{(\mathbf{S} - \mathbf{B}_0^*) + \mathbf{N}_1} \right| + \frac{\beta_2}{2} \log \left| \frac{\mathbf{S} + \mathbf{N}_2}{(\mathbf{S} - \mathbf{B}_0^*) + \mathbf{N}_2} \right| \\ &+ \lambda_1 \left(\frac{1}{2} \log \left| \frac{\mathbf{B}_1^* + \mathbf{N}_1}{\mathbf{N}_1} \right| - \frac{1}{2} \log \left| \frac{\mathbf{B}_1^* + \mathbf{N}_2}{\mathbf{N}_2} \right| \right) \\ &+ \lambda_2 \left(\frac{1}{2} \log \left| \frac{(\mathbf{S} - \mathbf{B}_0^*) + \mathbf{N}_2}{\mathbf{B}_1^* + \mathbf{N}_2} \right| \right. \\ &\quad \left. - \frac{1}{2} \log \left| \frac{(\mathbf{S} - \mathbf{B}_0^*) + \mathbf{N}_1}{\mathbf{B}_1^* + \mathbf{N}_1} \right| \right) + \rho. \end{aligned} \quad (26)$$

Next, we shall find a contradiction to (26) through the following three steps.

1) *Split each receiver into two virtual receivers:* Consider the following canonical MIMO Gaussian broadcast channel with four receivers:

$$\begin{aligned} \mathbf{Y}_{1a}[m] &= \mathbf{X}[m] + \mathbf{Z}_{1a}[m] \\ \mathbf{Y}_{1b}[m] &= \mathbf{X}[m] + \mathbf{Z}_{1b}[m] \\ \mathbf{Y}_{2a}[m] &= \mathbf{X}[m] + \mathbf{Z}_{2a}[m] \\ \mathbf{Y}_{2b}[m] &= \mathbf{X}[m] + \mathbf{Z}_{2b}[m] \end{aligned} \quad (27)$$

where $\{\mathbf{Z}_{1a}[m]\}$, $\{\mathbf{Z}_{1b}[m]\}$, $\{\mathbf{Z}_{2a}[m]\}$ and $\{\mathbf{Z}_{2b}[m]\}$ are i.i.d. additive vector Gaussian noise processes with zero means and covariance matrices \mathbf{N}_1 , \mathbf{N}_1 , \mathbf{N}_2 and \mathbf{N}_2 , respectively.

Suppose that the transmitter has three independent messages W_0 , W_1 and W_2 , where W_0 is intended for both receivers 1a and 2b, W_1 is intended for receiver 1a but needs to be kept asymptotically perfectly secret from receiver 2b, and W_2 is intended for receiver 2a but needs to be kept asymptotically perfectly secret from receiver 1b. Mathematically, for every $\epsilon > 0$, we must have

$$\frac{1}{n} I(W_1; \mathbf{Y}_{2b}^n) \leq \epsilon \quad \text{and} \quad \frac{1}{n} I(W_2; \mathbf{Y}_{1b}^n) \leq \epsilon \quad (28)$$

for sufficiently large block length n . Note that receivers 1a and 1b are statistically identical to receiver 1 in channel (18), so are receivers 2a and 2b to receiver 2 in channel (18). We thus conclude that the capacity region of channel (27) is the *same* as that of channel (18) under the same matrix power constraint.

2) *Construct an enhanced channel:* Let $\tilde{\mathbf{N}}$ be a real symmetric matrix satisfying

$$\tilde{\mathbf{N}} := \left(\mathbf{N}_1^{-1} + \frac{1}{\lambda_1 + \lambda_2} \mathbf{M}_1 \right)^{-1} \quad (29)$$

which implies that $\tilde{\mathbf{N}} \preceq \mathbf{N}_1$. Since $\mathbf{M}_1 \mathbf{B}_1^* = 0$, following [18, Lemma 11] we have

$$(\lambda_1 + \lambda_2)(\mathbf{B}_1^* + \tilde{\mathbf{N}})^{-1} = (\lambda_1 + \lambda_2)(\mathbf{B}_1^* + \mathbf{N}_1)^{-1} + \mathbf{M}_1$$

and

$$|\mathbf{B}_1^* + \tilde{\mathbf{N}}| |\mathbf{N}_1| = |\mathbf{B}_1^* + \mathbf{N}_1| |\tilde{\mathbf{N}}|. \quad (30)$$

Following (24), we may also obtain

$$(\lambda_1 + \lambda_2)(\mathbf{B}_1^* + \tilde{\mathbf{N}})^{-1} = (\lambda_1 + \lambda_2)(\mathbf{B}_1^* + \mathbf{N}_2)^{-1} + \mathbf{M}_2 \quad (31)$$

which implies that $\tilde{\mathbf{N}} \preceq \mathbf{N}_2$.

Consider the following enhanced aligned MIMO Gaussian broadcast channel

$$\begin{aligned} \tilde{\mathbf{Y}}_{1a}[m] &= \mathbf{X}[m] + \tilde{\mathbf{Z}}_{1a}[m] \\ \mathbf{Y}_{1b}[m] &= \mathbf{X}[m] + \mathbf{Z}_{1b}[m] \\ \tilde{\mathbf{Y}}_{2a}[m] &= \mathbf{X}[m] + \tilde{\mathbf{Z}}_{2a}[m] \\ \mathbf{Y}_{2b}[m] &= \mathbf{X}[m] + \mathbf{Z}_{2b}[m] \end{aligned} \quad (32)$$

where $\{\tilde{\mathbf{Z}}_{1a}[m]\}$, $\{\mathbf{Z}_{1b}[m]\}$, $\{\tilde{\mathbf{Z}}_{2a}[m]\}$ and $\{\mathbf{Z}_{2b}[m]\}$ are i.i.d. additive vector Gaussian noise processes with zero means and covariance matrices $\tilde{\mathbf{N}}$, \mathbf{N}_1 , $\tilde{\mathbf{N}}$ and \mathbf{N}_2 , respectively.

The message set configuration is the same as that for channel (27). Since $\tilde{\mathbf{N}} \preceq \{\mathbf{N}_1, \mathbf{N}_2\}$, we conclude that the capacity region of channel (32) is *at least as large* as that of channel (27) under the same matrix power constraint.

Furthermore, from (31) we have

$$\begin{aligned} & [(\mathbf{S} - \mathbf{B}_0^*) + \tilde{\mathbf{N}}](\mathbf{B}_1^* + \tilde{\mathbf{N}})^{-1} \\ &= [(\mathbf{S} - \mathbf{B}_0^*) + \mathbf{N}_2](\mathbf{B}_1^* + \mathbf{N}_2)^{-1} \end{aligned} \quad (33)$$

and hence

$$\left| \frac{(\mathbf{S} - \mathbf{B}_0^*) + \tilde{\mathbf{N}}}{\mathbf{B}_1^* + \tilde{\mathbf{N}}} \right| = \left| \frac{(\mathbf{S} - \mathbf{B}_0^*) + \mathbf{N}_2}{\mathbf{B}_1^* + \mathbf{N}_2} \right|. \quad (34)$$

Combining (23) and (31), we may obtain

$$\begin{aligned} & (\lambda_1 + \lambda_2)[(\mathbf{S} - \mathbf{B}_0^*) + \tilde{\mathbf{N}}]^{-1} \\ &= (\lambda_2 + \beta_1)[(\mathbf{S} - \mathbf{B}_0^*) + \mathbf{N}_1]^{-1} \\ &+ (\lambda_1 + \beta_2)[(\mathbf{S} - \mathbf{B}_0^*) + \mathbf{N}_2]^{-1} + \mathbf{M}_0. \end{aligned} \quad (35)$$

Substituting (30) and (34) into (26), we have

$$\begin{aligned} & (\beta_1 + \beta_2)R_0^\dagger + \lambda_1 R_1^\dagger + \lambda_2 R_2^\dagger \\ &= \frac{\beta_1}{2} \log \left| \frac{\mathbf{S} + \mathbf{N}_1}{(\mathbf{S} - \mathbf{B}_0^*) + \mathbf{N}_1} \right| + \frac{\beta_2}{2} \log \left| \frac{\mathbf{S} + \mathbf{N}_2}{(\mathbf{S} - \mathbf{B}_0^*) + \mathbf{N}_2} \right| \\ &+ \lambda_1 \left(\frac{1}{2} \log \left| \frac{(\mathbf{S} - \mathbf{B}_0^*) + \tilde{\mathbf{N}}}{\tilde{\mathbf{N}}} \right| - \frac{1}{2} \log \left| \frac{(\mathbf{S} - \mathbf{B}_0^*) + \mathbf{N}_2}{\mathbf{N}_2} \right| \right) \\ &+ \lambda_2 \left(\frac{1}{2} \log \left| \frac{(\mathbf{S} - \mathbf{B}_0^*) + \tilde{\mathbf{N}}}{\tilde{\mathbf{N}}} \right| - \frac{1}{2} \log \left| \frac{(\mathbf{S} - \mathbf{B}_0^*) + \mathbf{N}_1}{\mathbf{N}_1} \right| \right) \\ &+ \rho. \end{aligned} \quad (36)$$

3) *Outer bound the enhanced channel:* Next, we consider a discrete memoryless broadcast channel with four receivers and three independent messages and provide a single-letter outer bound on the capacity region.

Lemma 3: Consider a discrete memoryless broadcast channel $p(\tilde{y}_{1a}, y_{1b}, \tilde{y}_{2a}, y_{2b} | x)$ with four receivers and three independent messages (W_0, W_1, W_2) : W_0 is intended for both receivers 1b and 2b, W_1 is intended for receiver 1a but needs to be kept asymptotically perfectly secret from receiver 2b, and W_2 is intended for receiver 2a but needs to be kept

asymptotically perfectly secret from receiver 1b. Assume that

$$X \rightarrow \tilde{Y}_{1a} \rightarrow (Y_{1b}, Y_{2b}) \quad \text{and} \quad X \rightarrow \tilde{Y}_{2a} \rightarrow (Y_{1b}, Y_{2b})$$

form two Markov chains. Then, any achievable rate triple (R_0, R_1, R_2) must satisfy

$$\begin{aligned} R_0 &\leq \min[I(U; Y_{1b}), I(U; Y_{2b})] \\ R_1 &\leq I(X; \tilde{Y}_{1a}|U) - I(X; Y_{2b}|U) \\ R_2 &\leq I(X; \tilde{Y}_{2a}|U) - I(X; Y_{1b}|U) \end{aligned} \quad (37)$$

for some $p(u, x)$, where U is an auxiliary random variable.

The proof follows standard information-theoretic argument and is deferred to Appendix B.

Now, we can combine all previous three steps and obtain an upper bound on the weighted sum rate $(\beta_1 + \beta_2)R_0^\dagger + \lambda_1 R_1^\dagger + \lambda_2 R_2^\dagger$. By assumption, $(R_0^\dagger, R_1^\dagger, R_2^\dagger)$ is an achievable rate triple for channel (18). Then, following Lemma 3 we have

$$\begin{aligned} &(\beta_1 + \beta_2)R_0^\dagger + \lambda_1 R_1^\dagger + \lambda_2 R_2^\dagger \\ &\leq \frac{\beta_1}{2} \log |2\pi e(\mathbf{S} + \mathbf{N}_1)| + \frac{\beta_2}{2} \log |2\pi e(\mathbf{S} + \mathbf{N}_2)| \\ &\quad + \frac{\lambda_1}{2} \log \left| \frac{\mathbf{N}_2}{\tilde{\mathbf{N}}} \right| + \frac{\lambda_2}{2} \log \left| \frac{\mathbf{N}_1}{\tilde{\mathbf{N}}} \right| + \eta(\lambda_1, \lambda_2) \end{aligned} \quad (38)$$

where

$$\begin{aligned} \eta(\lambda_1, \lambda_2) &:= \lambda_1 h(\mathbf{X} + \tilde{\mathbf{Z}}_{1a}|U) + \lambda_2 h(\mathbf{X} + \tilde{\mathbf{Z}}_{2a}|U) \\ &\quad - (\lambda_2 + \beta_1)h(\mathbf{X} + \mathbf{Z}_{1b}|U) - (\lambda_1 + \beta_2)h(\mathbf{X} + \mathbf{Z}_{2b}|U). \end{aligned}$$

Note that $0 \prec \tilde{\mathbf{N}} \preceq \{\mathbf{N}_1, \mathbf{N}_2\}$, $0 \prec \mathbf{B}_0^* \preceq \mathbf{S}$, and $\mathbf{B}_0^* \mathbf{M}_0 = 0$. By [21, Corollary 4] and (35), we have

$$\begin{aligned} \eta(\lambda_1, \lambda_2) &\leq (\lambda_1 + \lambda_2) \log \left| 2\pi e(\mathbf{S} - \mathbf{B}_0^*) + \tilde{\mathbf{N}} \right| \\ &\quad - (\lambda_2 + \beta_1) \log |2\pi e(\mathbf{S} - \mathbf{B}_0^*) + \mathbf{N}_1| \\ &\quad - (\lambda_1 + \beta_2) \log |2\pi e(\mathbf{S} - \mathbf{B}_0^*) + \mathbf{N}_2|. \end{aligned} \quad (39)$$

Combining (38) and (39), we have

$$\begin{aligned} &(\beta_1 + \beta_2)R_0^\dagger + \lambda_1 R_1^\dagger + \lambda_2 R_2^\dagger \\ &\leq \frac{\beta_1}{2} \log \left| \frac{\mathbf{S} + \mathbf{N}_1}{(\mathbf{S} - \mathbf{B}_0^*) + \mathbf{N}_1} \right| + \frac{\beta_2}{2} \log \left| \frac{\mathbf{S} + \mathbf{N}_2}{(\mathbf{S} - \mathbf{B}_0^*) + \mathbf{N}_2} \right| \\ &\quad + \lambda_1 \left(\frac{1}{2} \log \left| \frac{(\mathbf{S} - \mathbf{B}_0^*) + \tilde{\mathbf{N}}}{\tilde{\mathbf{N}}} \right| - \frac{1}{2} \log \left| \frac{(\mathbf{S} - \mathbf{B}_0^*) + \mathbf{N}_2}{\mathbf{N}_2} \right| \right) \\ &\quad + \lambda_2 \left(\frac{1}{2} \log \left| \frac{(\mathbf{S} - \mathbf{B}_0^*) + \tilde{\mathbf{N}}}{\tilde{\mathbf{N}}} \right| - \frac{1}{2} \log \left| \frac{(\mathbf{S} - \mathbf{B}_0^*) + \mathbf{N}_1}{\mathbf{N}_1} \right| \right) \end{aligned}$$

which is a contradiction to (36) as $\rho > 0$. We thus conclude that the rate region (19) over all possible $\mathbf{B}_0 \succeq 0$, $\mathbf{B}_1 \succeq 0$ and $\mathbf{B}_0 + \mathbf{B}_1 \preceq \mathbf{S}$ is indeed the capacity region of the canonical MIMO Gaussian broadcast channel (18). This completes the proof of Theorem 2.

Remark 4: Note that in the enhanced channel (32), both legitimate receivers 1a and 2a have the *same* noise covariance matrices. This fact greatly simplified the capacity analysis of the enhanced channel and is key to the success of the proposed channel enhancement approach. We mention here that the same technique was also used in [24] to derive the sum-private-v.s.-common message capacity region of the MIMO Gaussian broadcast channel.

IV. CONCLUDING REMARKS

In this paper we have presented two new results on MIMO Gaussian broadcast channels with confidential messages, leading to a more comprehensive understanding of the fundamental limits of MIMO secret communication.

First, a matrix characterization of the capacity-equivocation region of the MIMO Gaussian wiretap channel has been obtained, generalizing the previous results [3]–[7] which dealt only with the secrecy capacity of the channel. The result has been obtained via an interesting connection between the rate-equivocation setting and simultaneous private-confidential communication over a discrete memoryless wiretap channel, which allows a matrix characterization of the entire capacity-equivocation region based on the existing characterization of secrecy capacity for the MIMO Gaussian wiretap channel.

Next, the problem of MIMO Gaussian wiretap channels with two receivers and three independent messages, a common message intended for both receivers, and two mutually confidential messages each intended for one of the receivers but needing to be kept asymptotically perfect secure from the other, has been considered. A precise characterization of the capacity region has been obtained via a channel-enhancement argument, which is a natural extension of the channel-enhancement arguments of [9] and [24].

APPENDIX A PROOF OF LEMMA 1

We first prove the achievability part of the lemma by considering a coding scheme that combines superposition coding, random binning, and rate splitting. Fix $p(u)p(v|u)p(x|v)$. Split the private message W_p into two independent submessages W_p' and W_p'' .

Codebook generation. Fix $\delta > 0$. Randomly and independently generate $2^{n(R_p + \delta)}$ codewords of length n according to p_U^n . Label each of the codewords as u_j^n , where j is the codeword number. We will refer to the codeword collection $\{u_j^n\}_j$ as the U -codebook.

For each codeword u_j^n in the U -codebook, randomly and independently generate $2^{n(R_s + R_p' + T)}$ codewords of length n according to $\prod_{i=1}^n p_{V|U=u_j[i]}$. Randomly partition the codewords into 2^{nR_s} bins so that each bin contains $2^{n(R_p' + T)}$ codewords. Further partition each bin into $2^{nR_p''}$ sub-bins so that each sub-bin contains 2^{nT} codewords. Label each of the codewords as $v_{j,k,l,t}^n$ where k denotes the bin number, l denotes the sub-bin number within each bin, and t denotes the codeword number within each sub-bin. We will refer to the codeword collection $\{v_{j,k,l,t}^n\}_{k,l,t}$ as the V -subcodebook corresponding to u_j^n . Fig. 5 illustrates the overall codebook structure.

Encoding. To send a message triple (w_s, w_p', w_p'') , the transmitter first chooses the codeword $u_{w_p'}^n$ from the U -codebook. Next, the transmitter looks into the V -subcodebook corresponding to $u_{w_p'}^n$ and *randomly* (according to a uniform distribution) chooses a codeword $v_{w_p', w_s, w_p'', t}^n$ from the w_p'' th sub-bin of the w_s th bin. Once a $v_{w_p', w_s, w_p'', t}^n$ is chosen, an input sequence x^n is generated according to $\prod_{i=1}^n p_{X|V=v_{w_p', w_s, w_p'', t}[i]}$ and is then sent through the channel.

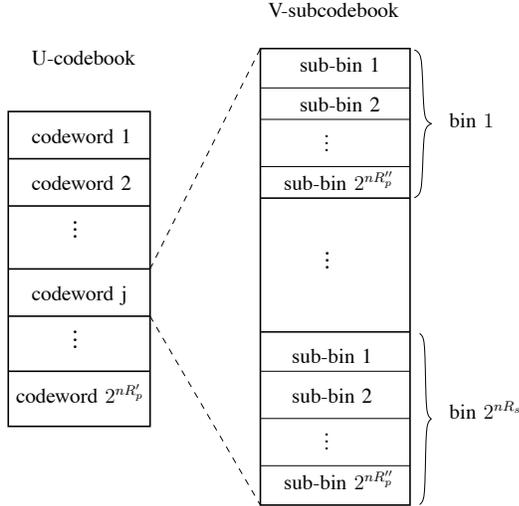


Fig. 5. Codebook structure.

Decoding at receiver 1. Given y_1^n , receiver 1 looks into the codebooks U and V and searches for a pair of codewords $(u_j^n, v_{j,k,l,t}^n)$ that are jointly typical with y_1^n . In the case when

$$R'_p < I(U; Y) \quad (40)$$

$$\text{and } R_s + R''_p + T < I(V; Y|U) \quad (41)$$

with high probability the transmitted codeword pair $(u_{w_p}^n, v_{w_p, w_s, w_p, t}^n)$ is the only one that is jointly typical with y_1^n .

Security at receivers 2 and 3. Fix $\epsilon > 0$. In the case when

$$R''_p + T > I(V; Z|U) \quad (42)$$

we have [17, Theorem 1]

$$\frac{1}{n} I(W_s; Z^n | W'_p) \leq \epsilon \quad (43)$$

for sufficiently large n . Since W_s and W'_p are independent, we have from (43) that

$$\begin{aligned} \frac{1}{n} I(W_s; Z^n) &\leq \frac{1}{n} I(W_s; Z^n, W'_p) \\ &= \frac{1}{n} I(W_s; Z^n | W'_p) \\ &\leq \epsilon \end{aligned}$$

i.e., the message W_s is asymptotically perfectly secure at the eavesdropper.

To summarize, for any given $p(u)p(v|u)p(x|v)$ and any $T \geq 0$, any rate triple (R_s, R'_p, R''_p) that satisfies (40)–(42) is achievable. Note that

$$R_p = R'_p + R''_p. \quad (44)$$

Eliminating T , R'_p and R''_p from (40)–(42) and (44) using Fourier-Motzkin elimination, we may conclude that any rate pair (R_s, R_p) satisfying (12) is achievable.

To prove the converse part of the lemma, we first consider an upper bound on the confidential message rate R_s . The perfect

secrecy condition (11) implies that for every $\epsilon > 0$,

$$H(W_s | Z^n) \geq H(W_s) - n\epsilon. \quad (45)$$

On the other hand, Fano's inequality [20, Ch. 2.11] implies that for every $\epsilon_0 > 0$,

$$\begin{aligned} H(W_s, W_p | Y^n) &\leq \epsilon_0 \log \left[2^{n(R_s + R_p)} - 1 \right] + h(\epsilon_0) \\ &:= n\delta. \end{aligned} \quad (46)$$

Applying (45) and (46), we have

$$\begin{aligned} nR_s &= H(W_s) \\ &\leq [H(W_s | Z^n) + n\epsilon] + [n\delta - H(W_s, W_p | Y^n)] \\ &\leq H(W_s, W_p | Z^n) - H(W_s, W_p | Y^n) + n(\epsilon + \delta). \end{aligned} \quad (47)$$

By the chain rule of the mutual information [20, Ch. 2.5],

$$\begin{aligned} n(R_s - \epsilon - \delta) &\leq I(W_s, W_p; Y^n) - I(W_s, W_p; Z^n) \\ &= \sum_{i=1}^n [I(W_s, W_p; Y_i | Y^{i-1}) \\ &\quad - I(W_s, W_p; Z_i | Z_{i+1}^n)] \\ &= \sum_{i=1}^n [I(W_s, W_p; Y_i | Y^{i-1}, Z_{i+1}^n) \\ &\quad - I(W_s, W_p; Z_i | Y^{i-1}, Z_{i+1}^n)] \end{aligned} \quad (48)$$

where the last equality follows from [17, Lemma 7]. Let

$$U_i := (Y^{i-1}, Z_{i+1}^n) \quad \text{and} \quad V_i := (W_s, W_p, U_i) \quad (49)$$

and we have from (48) that

$$n(R_s - \epsilon - \delta) \leq \sum_{i=1}^n [I(V_i; Y_i | U_i) - I(V_i; Z_i | U_i)]. \quad (50)$$

Next, we consider an upper bound on the sum private-confidential message rate $R_s + R_p$. By (46),

$$\begin{aligned} n(R_s + R_p) &= H(W_s, W_p) \\ &\leq I(W_s, W_p; Y^n) - n\delta. \end{aligned} \quad (51)$$

Applying the chain rule of the mutual information [20, Ch. 2.5], we have

$$\begin{aligned} n(R_s + R_p - \delta) &\leq \sum_{i=1}^n I(W_s, W_p; Y_i | Y^{i-1}) \\ &\leq \sum_{i=1}^n I(W_s, W_p, Y^{i-1}, Z_{i+1}^n; Y_i) \\ &= \sum_{i=1}^n I(V_i; Y_i). \end{aligned} \quad (52)$$

Applying the standard single-letterization procedure (e.g., see [20, Ch. 14.3]) to (50) and (52), we have the desired converse result for Lemma 1.

APPENDIX B
PROOF OF LEMMA 3

The perfect secrecy condition (28) implies that for every $\epsilon > 0$,

$$H(W_1|Y_{2b}^n) \geq H(W_1) - n\epsilon \quad (53a)$$

$$\text{and } H(W_2|Y_{1b}^n) \geq H(W_2) - n\epsilon. \quad (53b)$$

On the other hand, Fano's inequality [20, Chapter 2.11] implies that for every $\epsilon_0 > 0$,

$$\begin{aligned} \max[H(W_0|Y_{1b}^n), H(W_0|Y_{2b}^n)] \\ \leq \epsilon_0 \log(2^{nR_0} - 1) + h(\epsilon_0) := n\delta_0 \end{aligned} \quad (54a)$$

$$\begin{aligned} H(W_1|\tilde{Y}_{1a}^n) \\ \leq \epsilon_0 \log(2^{nR_1} - 1) + h(\epsilon_0) := n\delta_1 \end{aligned} \quad (54b)$$

$$\begin{aligned} \text{and } H(W_2|\tilde{Y}_{2a}^n) \\ \leq \epsilon_0 \log(2^{nR_2} - 1) + h(\epsilon_0) := n\delta_2. \end{aligned} \quad (54c)$$

Let

$$U_i := (W_0, Y_{1b}^{i-1}, Y_{2b,i+1}^n) \quad (55)$$

which satisfies the Markov chain

$$U_i \rightarrow X_i \rightarrow (\tilde{Y}_{1a}, \tilde{Y}_{2a}, Y_{1b}, Y_{2b}). \quad (56)$$

We first bound R_0 based on (54a) as follows:

$$\begin{aligned} nR_0 &= H(W_0) \\ &\leq I(W_0; Y_{1b}^n) + n\delta_0 \\ &= \sum_{i=1}^n I(W_0; Y_{1b,i} | Y_{1b}^{i-1}) + n\delta_0 \\ &\leq \sum_{i=1}^n I(W_0, Y_{1b}^{i-1}, Y_{2b,i+1}^n; Y_{1b,i}) + n\delta_0 \\ &= \sum_{i=1}^n I(U_i; Y_{1b,i}) + n\delta_0. \end{aligned} \quad (57)$$

Similarly, we have

$$\begin{aligned} nR_0 &\leq I(W_0; Y_{2b}^n) + n\delta_0 \\ &= \sum_{i=1}^n I(W_0; Y_{2b,i} | Y_{2b,i+1}^n) + n\delta_0 \\ &\leq \sum_{i=1}^n I(W_0, Y_{1b}^{i-1}, Y_{2b,i+1}^n; Y_{2b,i}) + n\delta_0 \\ &= \sum_{i=1}^n I(U_i; Y_{2b,i}) + n\delta_0. \end{aligned} \quad (58)$$

Next, we bound R_1 based on (53a) and (54b) as follows:

$$\begin{aligned} nR_1 &= H(W_1) \\ &\leq [H(W_1|Y_{2b}^n) + n\epsilon] + [n\delta_1 - H(W_1|\tilde{Y}_{1a}^n)] \\ &= H(W_1|W_0, Y_{2b}^n) + I(W_1; W_0|Y_{2b}^n) - H(W_1|\tilde{Y}_{1a}^n) \\ &\quad + n(\epsilon + \delta_1) \\ &\leq H(W_1|W_0, Y_{2b}^n) + H(W_0|Y_{2b}^n) - H(W_1|W_0, \tilde{Y}_{1a}^n) \\ &\quad + n(\epsilon + \delta_1). \end{aligned} \quad (59)$$

Substituting (54b) into (59), we may obtain

$$\begin{aligned} nR_1 &\leq H(W_1|W_0, Y_{2b}^n) - H(W_1|W_0, \tilde{Y}_{1a}^n) \\ &\quad + n(\epsilon + \delta_0 + \delta_1) \\ &= I(W_1; \tilde{Y}_{1a}^n|W_0) - I(W_1; Y_{2b}^n|W_0) \\ &\quad + n(\epsilon + \delta_0 + \delta_1). \end{aligned} \quad (60)$$

Applying [17, Lemma 7], (60) can be rewritten as

$$\begin{aligned} nR_1 &\leq \sum_{i=1}^n [I(W_1; \tilde{Y}_{1a,i}|W_0, \tilde{Y}_{1a}^{i-1}, Y_{2b,i+1}^n) \\ &\quad - I(W_1; Y_{2b,i}|W_0, \tilde{Y}_{1a}^{i-1}, Y_{2b,i+1}^n)] + n(\epsilon + \delta_0 + \delta_1) \\ &\leq \sum_{i=1}^n [I(X_i; \tilde{Y}_{1a,i}|W_0, \tilde{Y}_{1a}^{i-1}, Y_{2b,i+1}^n) \\ &\quad - I(X_i; Y_{2b,i}|W_0, \tilde{Y}_{1a}^{i-1}, Y_{2b,i+1}^n)] + n(\epsilon + \delta_0 + \delta_1) \end{aligned} \quad (61)$$

where (61) follows from the Markov chain

$$W_1 \rightarrow X_i \rightarrow \tilde{Y}_{1a,i} \rightarrow Y_{2b,i}.$$

Moreover, due to the Markov chain

$$(W_0, \tilde{Y}_{1a,i}, Y_{2b,i+1}^n) \rightarrow \tilde{Y}_{1a}^{i-1} \rightarrow Y_{1b}^{i-1} \quad (62)$$

we can further bound R_1 as

$$\begin{aligned} nR_1 &\leq \sum_{i=1}^n [I(X_i; \tilde{Y}_{1a,i}|W_0, \tilde{Y}_{1a}^{i-1}, Y_{1b}^{i-1}, Y_{2b,i+1}^n) \\ &\quad - I(X_i; Y_{2b,i}|W_0, \tilde{Y}_{1a}^{i-1}, Y_{1b}^{i-1}, Y_{2b,i+1}^n)] \\ &\quad + n(\epsilon + \delta_0 + \delta_1) \\ &= \sum_{i=1}^n [I(X_i; \tilde{Y}_{1a,i}|U_i, \tilde{Y}_{1a}^{i-1}) \\ &\quad - I(X_i; Y_{2b,i}|U_i, \tilde{Y}_{1a}^{i-1})] + n(\epsilon + \delta_0 + \delta_1) \quad (63) \\ &= \sum_{i=1}^n [I(X_i; \tilde{Y}_{1a,i}|U_i) - I(X_i; Y_{2b,i}|U_i)] \\ &\quad - [I(\tilde{Y}_{1a}^{i-1}; \tilde{Y}_{1a,i}|U_i) - I(\tilde{Y}_{1a}^{i-1}; Y_{2b,i}|U_i)] \\ &\quad + n(\epsilon + \delta_0 + \delta_1) \\ &\leq \sum_{i=1}^n [I(X_i; \tilde{Y}_{1a,i}|U_i) - I(X_i; Y_{2b,i}|U_i)] \\ &\quad + n(\epsilon + \delta_0 + \delta_1) \end{aligned} \quad (64)$$

where (63) follows from the definition of U_i in (55), and (64) follows from the fact that $Y_{2b,i}$ is degraded with respect to $\tilde{Y}_{1a,i}$ so $I(\tilde{Y}_{1a}^{i-1}; Y_{2b,i}|U_i) \leq I(\tilde{Y}_{1a}^{i-1}; \tilde{Y}_{1a,i}|U_i)$.

Following the same steps as those in (59)–(64), we may obtain

$$\begin{aligned} nR_2 &\leq \sum_{i=1}^n [I(X_i; \tilde{Y}_{2a,i}|U_i) \\ &\quad - I(X_i; Y_{1b,i}|U_i)] + n(\epsilon + \delta_0 + \delta_2). \end{aligned} \quad (65)$$

Finally, applying the standard single-letterization procedure (e.g., see [20, Chapter 14.3]) to (57), (58), (64) and (65) proves the desired result (37) for Lemma 3.

REFERENCES

- [1] Y. Liang, H. V. Poor, and S. Shamai (Shitz), *Information Theoretic Security*. Dordrecht, The Netherlands: Now Publisher, 2009.
- [2] R. Liu and W. Trappe, Eds, *Securing Wireless Communications at the Physical Layer*. New York: Springer Verlag, 2010.
- [3] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, July 2010.
- [4] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, No. 11, pp. 5515–5532, Nov. 2010.
- [5] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, to appear.
- [6] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, June 2009.
- [7] R. Bustin, R. Liu, H. V. Poor, and S. Shamai (Shitz), "An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel," *EURASIP Journal on Wireless Communications and Networking*, 2009.
- [8] R. Liu and H. V. Poor, "Secrecy capacity region of a multi-antenna Gaussian broadcast channel with confidential messages," *IEEE Trans. Inf. Theory*, vol. 55, no. 3, pp. 1235–1249, Mar. 2009.
- [9] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz), "Multiple-input multiple-output Gaussian broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4215–4227, Sep. 2010.
- [10] H. D. Ly, T. Liu, and Y. Liang, "Multiple-input multiple-output Gaussian broadcast channels with common and confidential messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5477–5487, Nov. 2010.
- [11] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz), "MIMO Gaussian broadcast channels with confidential and common messages," Available online at <http://arxiv.org/abs/1001.2806>
- [12] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz), "The capacity-equivocation region of the MIMO Gaussian wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Austin, Texas, June 2010.
- [13] 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, Texas, June 2010.
- [14] E. Ekrem and S. Ulukus, "Capacity region of Gaussian MIMO broadcast channels with common and confidential messages," *IEEE Trans. Inf. Theory*, submitted Feb. 2010.
- [15] E. Ekrem and S. Ulukus, "Capacity-equivocation region of the Gaussian MIMO wiretap channel," *IEEE Trans. Inf. Theory*, submitted May 2010.
- [16] A. D. Wyner, "The wire-tap channel," *Bell Sys. Tech. Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
- [17] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, 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. Inf. Theory*, vol. 52, no. 9, pp. 3936–3964, Sep. 2006.
- [19] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Budapest: Academic Press, 1982.
- [20] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: John Wiley & Sons, Inc., 1991.
- [21] 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*, vol. 55, no. 11, pp. 5011–5023, Nov. 2009.
- [22] J. Xu, Y. Cao, and B. Chen, "Capacity bounds for broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 4529–4542, Oct. 2009.
- [23] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493–2507, June 2008.
- [24] H. Weingarten, *Multiple-Input Multiple-Output Broadcast Systems*. Ph.D. Thesis, Dept. of Electrical Engineering, Technion-Israel Institute of Technology, 2008.