Multi-Receiver Wiretap Channel With Public and Confidential Messages

Ersen Ekrem, *Student Member, IEEE*, and Sennur Ulukus, *Member, IEEE*

***Abstract*—We study the multi-receiver wiretap channel (MR-WC) with public and confidential messages. In this channel, there is a transmitter that wishes to communicate with two legitimate users in the presence of an external eavesdropper. The transmitter sends a pair of public and confidential messages to each legitimate user. While there are no secrecy constraints on the public messages, confidential messages need to be transmitted in perfect secrecy. We study the discrete memoryless MR-WC as well as its Gaussian multi-input multi-output (MIMO) counterpart. First, we propose an inner bound for the general, not necessarily degraded, discrete memoryless MR-WC by using Marton's inner bound and rate splitting in conjunction with superposition coding and binning. Second, we specialize this inner bound for the degraded discrete memoryless case. This specialized form of the inner bound can be obtained by using superposition coding and binning only. Next, we obtain an outer bound for the capacity region of the degraded channel, which matches the inner bound for some special cases. Third, we consider the degraded Gaussian MIMO channel, and show that, to evaluate both the inner and outer bounds, considering only jointly Gaussian auxiliary random variables and channel input is sufficient. Similar to the discrete memoryless case, for the Gaussian MIMO case as well, these bounds match for some special cases.**

***Index Terms*—Capacity region, Gaussian multi-input multi-output (MIMO) channel, multi-receiver wiretap channel (MR-WC), public and confidential messages.**

I. Introduction

We study the multi-receiver wiretap channel (MR-WC) (see Fig. 1), which is a generalization of the wiretap channel introduced by Wyner [1] to a broadcast setting. In the MR-WC, different from the basic wiretap channel in [1] and [2], there are multiple legitimate users who would like to have secure communications with the transmitter in the presence of an external eavesdropper. Previously, [3]–[6] studied the MR-WC for the scenario, where the transmitter sends a *confidential* message to each legitimate user that needs to be kept perfectly secret from the eavesdropper. For this scenario, [3]–[5] obtained the capacity region of the *degraded* discrete memoryless MR-WC (see Fig. 2), and [6] obtained the capacity region of the general, *not necessarily degraded*, Gaussian multi-input multi-output (MIMO) MR-WC.

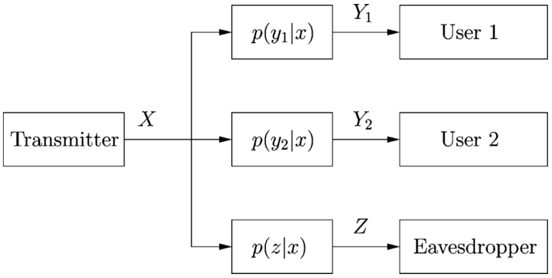

Fig. 1. MR-WC.

In this paper, we study the MR-WC for the scenario, where the transmitter sends a pair of *public* and *confidential* messages to each legitimate user. While there are no secrecy concerns on the public messages, confidential messages need to be transmitted in perfect secrecy. We call the channel model arising from this scenario the MR-WC with public and confidential messages. This scenario can be viewed as a generalization of the works on the MR-WC in [3]–[6], where there were no public messages.

First, we consider the general, not necessarily degraded, discrete memoryless MR-WC, and propose an inner bound for its capacity region. We obtain this inner bound by using Marton's inner bound [7] and rate splitting in conjunction with superposition coding and binning. This inner bound generalizes the previous inner bound for the MR-WC in [3]–[5] which do not consider public messages. In particular, our inner bound generalizes this previous inner bound by first incorporating public messages, and second using Marton's inner bound and rate splitting in addition to superposition coding and binning, the latter two of which were sufficient to obtain the inner bound in [3]–[5].

Second, we consider the degraded discrete memoryless MR-WC and obtain an inner bound for its capacity region by specializing the inner bound we obtained for the general case. This specialized form of the inner bound can be obtained by an achievable scheme that combines superposition coding [8] and binning. Next, we propose an outer bound for the capacity region of the degraded discrete memoryless channel. Although these inner and outer bounds do not match in general, there are cases where they match and, hence, provide the capacity region. In particular, when we specialize these inner and outer bounds by setting either the public message rate of the second legitimate user (weak user) or the confidential message rate of the first legitimate user (strong user) to zero, they match providing the exact capacity region for these two scenarios.

Manuscript received June 02, 2011; revised February 13, 2012; accepted November 21, 2012. Date of publication January 25, 2013; date of current version March 13, 2013. This work was supported by the National Science Foundation under Grants CCF 07-29127, CNS 09-64632, CCF 09-64645, and CCF 10-18185. This paper was presented in part at the 48th Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, September 29–October 1, 2010.

E. Ekrem was with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742 USA. He is now with Qualcomm, Santa Clara, CA 95051 USA (e-mail: ersen@umd.edu).

S. Ulukus is with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742 USA (e-mail: ulukus@umd.edu).

Communicated by S. A. Jafar, Associate Editor for Communications.

Digital Object Identifier 10.1109/TIT.2013.2238655

Moreover, when we set the rates of both of the public messages to zero, these inner and outer bounds match recovering the secrecy capacity region of the degraded discrete memoryless channel obtained in [3]–[5].

Third, we consider the degraded Gaussian MIMO instance of this channel model. This generalizes our work in [6], where we consider the general, not necessarily degraded, Gaussian MIMO channel only with confidential messages. For the degraded Gaussian MIMO channel, we show that it is sufficient to consider jointly Gaussian auxiliary random variables and channel input for the evaluation of both the inner and outer bounds we proposed for the degraded discrete memoryless channel. We prove the sufficiency of Gaussian auxiliary random variables and channel input by using the de Bruijn identity [9], a differential relationship between the differential entropy and the Fisher information matrix, in conjunction with the properties of the Fisher information matrix. Similar to the degraded discrete case, for the degraded Gaussian case as well, although these inner and outer bounds do not match in general, there are cases where they coincide and, hence, provide the capacity region. In particular, the inner and outer bounds for the degraded Gaussian MIMO channel completely match giving us the exact capacity region, when either the public message rate of the second legitimate user (weak user) or the confidential message rate of the first legitimate user (strong user) is zero. Moreover, these inner and outer bounds match for the secrecy capacity region of the degraded Gaussian MIMO channel, which we obtain by setting the rates of both public messages to zero [6], [10].

II. Discrete Memoryless MR-WCs

Discrete memoryless MR-WCs consist of a transmitter, two legitimate users, and an eavesdropper. The channel is memoryless with a transition probability $p(y_1, y_2, z|x)$, where $X \in \mathcal{X}$ is the channel input, and $Y_1 \in \mathcal{Y}_1$, $Y_2 \in \mathcal{Y}_2$, $Z \in \mathcal{Z}$ denote the channel outputs of the first legitimate user, the second legitimate user, and the eavesdropper, respectively. We consider the scenario in which, the transmitter sends a pair of public and confidential messages to each legitimate user. While there are no secrecy constraints on the public messages, the confidential messages need to be transmitted in perfect secrecy. We call the channel model arising from this scenario the MR-WC with public and confidential messages.

An $(n, 2^{nR_{p1}}, 2^{nR_{s1}}, 2^{nR_{p2}}, 2^{nR_{s2}})$ code for this channel consists of four message sets, $\mathcal{W}_{p1} = \{1, \ldots, 2^{nR_{p1}}\}$, $\mathcal{W}_{s1} = \{1, \ldots, 2^{nR_{s1}}\}$, $\mathcal{W}_{p2} = \{1, \ldots, 2^{nR_{p2}}\}$, $\mathcal{W}_{s2} = \{1, \ldots, 2^{nR_{s2}}\}$, one encoder at the transmitter $f : \mathcal{W}_{p1} \times \mathcal{W}_{s1} \times \mathcal{W}_{p2} \times \mathcal{W}_{s2} \rightarrow \mathcal{X}^n$, and one decoder at each legitimate user $g_j : \mathcal{Y}_j^n \rightarrow \mathcal{W}_{pj} \times \mathcal{W}_{sj}$, for $j = 1, 2$. The probability of error is defined as $P_e^n = \max\{P_{e,1}^n, P_{e,2}^n\}$, where $P_{e,j}^n = \Pr[g_j(Y_j^n) \neq (W_{pj}, W_{sj})]$, for $j = 1, 2$, and W_{p1}, W_{s1}, W_{p2}, W_{s2} are uniformly distributed random variables in $\mathcal{W}_{p1}$, $\mathcal{W}_{s1}$, $\mathcal{W}_{p2}$, $\mathcal{W}_{s2}$, respectively. A rate tuple $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ is said to be achievable if there exists an $(n, 2^{nR_{p1}}, 2^{nR_{s1}}, 2^{nR_{p2}}, 2^{nR_{s2}})$ code which satisfies $\lim_{n\rightarrow\infty} P_e^n = 0$ and

$$\lim_{n\rightarrow\infty} \frac{1}{n} I(W_{s1}, W_{s2}; Z^n) = 0 \tag{1}$$

which implies

$$\lim_{n\rightarrow\infty} \frac{1}{n} I(W_{sj}; Z^n) = 0, \ j = 1, 2. \tag{2}$$

The capacity region of the MR-WC with public and confidential messages, $\mathcal{C}$ is defined as the convex closure of all achievable rate tuples $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$.

A. General Channels

We first consider the general, not necessarily degraded, discrete memoryless MR-WC with public and confidential messages, and propose the following inner bound for its capacity region.

Theorem 1: An achievable rate region for the discrete memoryless MR-WC with public and confidential messages is given by the union of rate tuples $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ satisfying

$$R_{s1} \leq \min_{j=1,2} I(U; Y_j|Q) + I(V_1; Y_1|U) - I(U, V_1; Z|Q) \tag{3}$$

$$R_{s2} \leq \min_{j=1,2} I(U; Y_j|Q) + I(V_2; Y_2|U) - I(U, V_2; Z|Q) \tag{4}$$

$$\begin{aligned}\sum_{j=1}^{2} R_{sj} \leq \min_{j=1,2} & I(U; Y_j|Q) + I(V_1; Y_1|U) + I(V_2; Y_2|U) \\ & - I(V_1; V_2|U) - I(U, V_1, V_2; Z|Q)\end{aligned} \tag{5}$$

$$R_{s1} + R_{p1} \leq \min_{j=1,2} I(U; Y_j) + I(V_1; Y_1|U) \tag{6}$$

$$R_{s2} + R_{p2} \leq \min_{j=1,2} I(U; Y_j) + I(V_2; Y_2|U) \tag{7}$$

$$\begin{aligned}\sum_{j=1}^{2} R_{sj} + R_{p1} \leq \min_{j=1,2} & I(U; Y_j) + I(V_1; Y_1|U) + I(V_2; Y_2|U) \\ & - I(V_2; Z|U)\end{aligned} \tag{8}$$

$$\begin{aligned}\sum_{j=1}^{2} R_{sj} + R_{p1} \leq \min_{j=1,2} & I(U; Y_j) + 2I(V_1; Y_1|U) + I(V_2; Y_2|U) \\ & - I(V_1; V_2|U) - I(V_1, V_2; Z|U)\end{aligned} \tag{9}$$

$$\begin{aligned}\sum_{j=1}^{2} R_{sj} + R_{p2} \leq \min_{j=1,2} & I(U; Y_j) + I(V_1; Y_1|U) + I(V_2; Y_2|U) \\ & - I(V_1; Z|U)\end{aligned} \tag{10}$$

$$\begin{aligned}\sum_{j=1}^{2} R_{sj} + R_{p2} \leq \min_{j=1,2} & I(U; Y_j) + I(V_1; Y_1|U) + 2I(V_2; Y_2|U) \\ & - I(V_1; V_2|U) - I(V_1, V_2; Z|U)\end{aligned} \tag{11}$$

$$\begin{aligned}\sum_{j=1}^{2} R_{sj} + R_{pj} \leq \min_{j=1,2} & I(U; Y_j) + I(V_1; Y_1|U) + I(V_2; Y_2|U) \\ & - I(V_1; V_2|U)\end{aligned} \tag{12}$$

$$0 \leq \min_{j=1,2} I(U; Y_j|Q) - I(U; Z|Q) \tag{13}$$

$$0 \leq I(V_1; Y_1|U) - I(V_1; Z|U) \tag{14}$$

$$0 \leq I(V_2; Y_2|U) - I(V_2; Z|U) \tag{15}$$

$$\begin{aligned}0 \leq & I(V_1; Y_1|U) + I(V_2; Y_2|U) - I(V_1; V_2|U) \\ & - I(V_1, V_2; Z|U)\end{aligned} \tag{16}$$

for some Q, U, V_1, V_2 such that $p(q, u, v_1, v_2, x, y_1, y_2, z) = p(q, u)p(v_1, v_2, x|u)p(y_1, y_2, z|x)$.

The proof of Theorem 1 is given in Appendix A. We obtain the achievable scheme in Theorem 1 by using Marton's coding

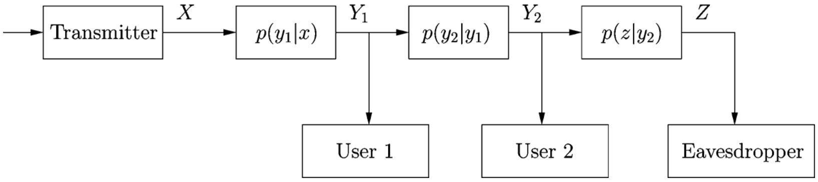

Fig. 2. Degraded MR-WC.

and rate splitting in conjunction with superposition coding and binning. Here, we provide an outline of the achievable scheme in Theorem 1 and defer the details to Appendix A. In this achievable scheme, we first divide each public message W_{pj} into three parts as W_{pj}^1, W_{pj}^2, W_{pj}^3, where the rates of the messages W_{pj}^1, W_{pj}^2, W_{pj}^3 are given by R_{pj}^1, R_{pj}^2, R_{pj}^3, respectively, and $R_{pj} = R_{pj}^1 + R_{pj}^2 + R_{pj}^3$. Similarly, we divide each confidential message W_{sj} into two parts as W_{sj}^1, W_{sj}^2, where the rates of the messages W_{sj}^1, W_{sj}^2 are given by R_{sj}^1, R_{sj}^2, respectively, and $R_{sj} = R_{sj}^1 + R_{sj}^2$. The first parts of the public messages, i.e., W_{p1}^1 and W_{p2}^1, are sent through the sequences generated by Q. The second parts of the public messages, i.e., W_{p1}^2 and W_{p2}^2, and the first parts of the confidential messages, i.e., W_{s1}^1 and W_{s2}^1, are sent through the sequences generated by U. Both legitimate receivers decode these sequences, and hence, each legitimate receiver decodes the parts of the other legitimate user's public and confidential messages. The last parts of each public message and each confidential message, i.e., W_{pj}^3 and W_{sj}^2, are encoded by the sequences generated through V_j. This encoding is performed by using Marton's coding [7]. Each legitimate receiver, after decoding Q^n and U^n, decodes the sequences V_j^n.

B. Degraded Channels

We now consider the degraded MR-WC that satisfies the following Markov chain:

$$X \to Y_1 \to Y_2 \to Z. \tag{17}$$

We first present an inner bound for the capacity region of the degraded discrete memoryless channel $\mathcal{C}$ in the following theorem.

Theorem 2: An achievable rate region, denoted by $\mathcal{R}^{\text{in}}$, for the degraded discrete memoryless MR-WC with public and confidential messages is given by the union of rate tuples $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ satisfying

$$R_{s2} \leq I(U;Y_2) - I(U;Z) \tag{18}$$

$$\sum_{j=1}^{2} R_{sj} \leq I(U;Y_2) + I(X;Y_1|U) - I(X;Z) \tag{19}$$

$$R_{p2} + R_{s2} \leq I(U;Y_2) \tag{20}$$

$$\sum_{j=1}^{2} R_{sj} + R_{p2} \leq I(U;Y_2) + I(X;Y_1|U) - I(X;Z|U) \tag{21}$$

$$\sum_{j=1}^{2} R_{pj} + R_{sj} \leq I(U;Y_2) + I(X;Y_1|U) \tag{22}$$

where (U, X) satisfy the following Markov chain:

$$U \to X \to Y_1 \to Y_2 \to Z. \tag{23}$$

The achievable rate region given by Theorem 2 can be obtained from Theorem 1 by setting $Q = \phi$, $V_2 = U$, $V_1 = X$ in Theorem 1. The achievable rate region in Theorem 2 can be shown by using superposition coding and binning. Superposition coding enables us to transmit messages of each user at a different layer, and binning enables us to ensure the protection of the confidential messages from the eavesdropper.

Now, we introduce the following outer bound for the capacity region of the degraded discrete memoryless MR-WC with public and confidential messages.

Theorem 3: The capacity region of the degraded discrete memoryless MR-WC with public and confidential messages is contained in $\mathcal{R}^{\text{out}}$ that is composed of rate tuples $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ satisfying

$$R_{s2} \leq I(U;Y_2) - I(U;Z) \tag{24}$$

$$\sum_{j=1}^{2} R_{sj} \leq I(U;Y_2) + I(X;Y_1|U) - I(X;Z) \tag{25}$$

$$R_{p2} + R_{s2} \leq I(U;Y_2) \tag{26}$$

$$\sum_{j=1}^{2} R_{pj} + R_{sj} \leq I(U;Y_2) + I(X;Y_1|U) \tag{27}$$

for some (U, X) such that U, X exhibit the following Markov chain:

$$U \to X \to Y_1 \to Y_2 \to Z. \tag{28}$$

The proof of Theorem 3 is given in Appendix C.

We note that the inner bound in Theorem 2 and the outer bound in Theorem 3 do not match in general. In fact, in Section III, we provide an example where the outer bound strictly includes the inner bound, i.e., there are rate tuples that are included in $\mathcal{R}^{\text{out}}$, but not in $\mathcal{R}^{\text{in}}$. However, there are cases for which the exact capacity region can be obtained. First, we note that the inner bound in Theorem 2 and the outer bound in Theorem 3 match when the confidential message rate of the first legitimate user is zero, i.e., $R_{s1} = 0$.

Corollary 1: The capacity region of the degraded discrete memoryless MR-WC without the first legitimate user's confidential message is given by the union of rate triples (R_{p1}, R_{p2}, R_{s2}) satisfying

$$R_{s2} \leq I(U;Y_2) - I(U;Z) \tag{29}$$

$$R_{s2} + R_{p2} \leq I(U;Y_2) \tag{30}$$

$$R_{p1} + R_{p2} + R_{s2} \leq I(U;Y_2) + I(X;Y_1|U) \tag{31}$$

where U, X exhibit the following Markov chain:

$$U \rightarrow X \rightarrow Y_1 \rightarrow Y_2 \rightarrow Z. \quad (32)$$

Corollary 1 can be proved by setting $R_{s1} = 0$ in both Theorems 2 and 3 and eliminating the redundant bounds.

Next, we note that the inner bound in Theorem 2 and the outer bound in Theorem 3 match when the public message rate of the second legitimate user is zero, i.e., $R_{p2} = 0$.

Corollary 2: The capacity region of the degraded discrete memoryless MR-WC without the second legitimate user's public message is given by the union of rate triples (R_{p1}, R_{s1}, R_{s2}) satisfying

$$R_{s2} \leq I(U;Y_2) - I(U;Z) \quad (33)$$

$$\sum_{j=1}^{2} R_{sj} \leq I(U;Y_2) + I(X;Y_1|U) - I(X;Z) \quad (34)$$

$$R_{p1} + \sum_{j=1}^{2} R_{sj} \leq I(U;Y_2) + I(X;Y_1|U) \quad (35)$$

where U, X exhibit the following Markov chain:

$$U \rightarrow X \rightarrow Y_1 \rightarrow Y_2 \rightarrow Z. \quad (36)$$

Corollary 2 can be proved by setting $R_{p2} = 0$ in both Theorems 2 and 3 and eliminating the redundant bounds.

Corollary 2 also implies that the inner bound in Theorem 2 and the outer bound in Theorem 3 match on the secrecy capacity region of the degraded MR-WC, i.e., when the rates of both public messages R_{p1}, R_{p2} are set to zero:

Corollary 3 ([3]–[5]): The secrecy capacity region of the degraded discrete memoryless MR-WC is given by the union of rate pairs (R_{s1}, R_{s2}) satisfying

$$R_{s2} \leq I(U;Y_2) - I(U;Z) \quad (37)$$

$$R_{s1} + R_{s2} \leq I(U;Y_2) + I(X;Y_1|U) - I(X;Z) \quad (38)$$

where U, X exhibit the following Markov chain:

$$U \rightarrow X \rightarrow Y_1 \rightarrow Y_2 \rightarrow Z. \quad (39)$$

So far, we provided examples where the inner and outer bounds match when one of the rates is zero. Next, we provide an example where the inner and outer bounds match when none of the rates is zero. To this end, we note that the inner and the outer bounds can be expressed by using hyperplanes that are tangent to them

$$L^{\text{in}} = \max_{(R_{p1},R_{s1},R_{p2},R_{s2}) \in \mathcal{R}^{\text{in}}} \sum_{j=1}^{2} \mu_{pj} R_{pj} + \mu_{sj} R_{sj} \quad (40)$$

$$L^{\text{out}} = \max_{(R_{p1},R_{s1},R_{p2},R_{s2}) \in \mathcal{R}^{\text{out}}} \sum_{j=1}^{2} \mu_{pj} R_{pj} + \mu_{sj} R_{sj}. \quad (41)$$

Assume that the following condition holds:

$$\mu_{s2} > \max(\mu_{s1}, \mu_{p2}) \geq \min(\mu_{s1}, \mu_{p2}) > \mu_{p1} \quad (42)$$

$$\mu_{s2} + \mu_{p1} > \mu_{s1} + \mu_{p2}. \quad (43)$$

Under these conditions, we have

$$\begin{aligned} L^{\text{out}} = &\max_{(R_{pj},R_{sj})_{j=1}^{2} \in \mathcal{R}^{\text{out}}} \mu_{p1} \left(\sum_{j=1}^{2} R_{pj} + R_{sj} \right) \\ &+ (\mu_{s1} - \mu_{p1})(R_{s1} + R_{s2}) + (\mu_{p2} - \mu_{p1})(R_{p2} + R_{s2}) \\ &+ (\mu_{s2} + \mu_{p1} - \mu_{s1} - \mu_{p2}) R_{s2} \end{aligned} \quad (44)$$

$$\begin{aligned} = &\max_{(U,X) \in \mathcal{F}} \mu_{p1} \big[I(U;Y_2) + I(X;Y_1|U) \big] \\ &+ (\mu_{s1} - \mu_{p1}) \big[I(U;Y_2) + I(X;Y_1|U) - I(X;Z) \big] \\ &+ (\mu_{p2} - \mu_{p1}) I(U;Y_2) \\ &+ (\mu_{s2} + \mu_{p1} - \mu_{s1} - \mu_{p2}) \big[I(U;Y_2) - I(U;Z) \big] \end{aligned} \quad (45)$$

$$\begin{aligned} = &\max_{(U,X) \in \mathcal{F}} \mu_{p1} I(X;Z|U) + \mu_{s1} \big[I(X;Y_1|U) - I(X;Z|U) \big] \\ &+ \mu_{p2} I(U;Z) + \mu_{s2} \big[I(U;Y_2) - I(U;Z) \big] \end{aligned} \quad (46)$$

$$= L^{\text{in}} \quad (47)$$

where the set $\mathcal{F}$ is given by the union of (U, X) pairs that satisfy the Markov chain in (28), and (47) follows from the fact $(R_{p1}^*, R_{s1}^*, R_{p2}^*, R_{s2}^*) \in \mathcal{R}^{\text{in}}$ attains (47), and $(R_{p1}^*, R_{s1}^*, R_{p2}^*, R_{s2}^*)$ is given by

$$(R_{p1}^*, R_{s1}^*) = \big(I(X;Z|U), I(X;Y_1|U) - I(X;Z|U) \big) \quad (48)$$

$$(R_{p2}^*, R_{s2}^*) = \big(I(U;Z), I(U;Y_2) - I(U;Z) \big). \quad (49)$$

Hence, this example shows that there are parts of the capacity region where none of the rates is zero, and the inner and outer bounds match.

Next, we provide an example where the inner bound is strictly contained in the outer bound, i.e., there are rate tuples that are inside the outer bound, but outside the inner bound. To provide such an example, we again use the alternative descriptions of the inner and outer bounds by means of tangent hyperplanes as given by (40) and (41), respectively. We assume that the following condition holds:

$$\mu_{s1} > \mu_{p2} > \mu_{p1} > \mu_{s2}. \quad (50)$$

Under this condition, we have

$$\begin{aligned} L^{\text{out}} \geq &\max_{(U,X) \in \mathcal{F}} \mu_{p1} \big[I(X;Z) - \min(I(U;Y_2), I(X;Z)) \big] \\ &+ \mu_{p2} \min(I(U;Y_2), I(X;Z)) \\ &+ \mu_{s1} \big[I(U;Y_2) + I(X;Y_1|U) - I(X;Z) \big] \end{aligned} \quad (51)$$

$$\begin{aligned} L^{\text{in}} = &\max_{(U,X) \in \mathcal{F}} \mu_{p1} I(X;Z|U) + \mu_{p2} I(U;Z) \\ &+ \mu_{s1} \big[I(U;Y_2) + I(X;Y_1|U) - I(X;Z) \big] \end{aligned} \quad (52)$$

which can be shown by following the analysis in (44)–(47). The set $\mathcal{F}$ contains (U, X) pairs that satisfy the Markov chain in (28). Let us assume that (U^*, X^*) is the maximizer for (52). Hence, using (51) and (52), we have

$$L^{\text{out}} - L^{\text{in}} \geq (\mu_{p2} - \mu_{p1}) \min(I(U^*;Y_2|Z), I(X^*;Z|U^*)) \quad (53)$$

where the right-hand side of (53) can be strictly positive for certain channel models. In particular, for the degraded Gaussian model we consider in Section III, one can find (U^*, X^*) such that the right-hand side of (53) is strictly positive. This observation implies that the outer bound strictly contains the inner bound.

III. Degraded Gaussian MIMO MR-WCs

Here, we consider the degraded Gaussian MIMO MR-WC which is defined by

$$\mathbf{Y}_j = \mathbf{X} + \mathbf{N}_j, \quad j = 1,2 \tag{54}$$

$$\mathbf{Z} = \mathbf{X} + \mathbf{N}_Z \tag{55}$$

where the channel input $\mathbf{X}$ is subject to a covariance constraint $E\left[\mathbf{X}\mathbf{X}^\top\right] \preceq \mathbf{S}$ where $\mathbf{S} \succ \mathbf{0}$ and $\mathbf{N}_1, \mathbf{N}_2, \mathbf{N}_Z$ are zero-mean Gaussian random vectors with covariance matrices $\boldsymbol{\Sigma}_1, \boldsymbol{\Sigma}_2, \boldsymbol{\Sigma}_Z$, respectively.

In the degraded Gaussian MIMO MR-WC, the noise covariance matrices $\boldsymbol{\Sigma}_1, \boldsymbol{\Sigma}_2, \boldsymbol{\Sigma}_Z$ satisfy the following order:

$$\mathbf{0} \prec \boldsymbol{\Sigma}_1 \preceq \boldsymbol{\Sigma}_2 \preceq \boldsymbol{\Sigma}_Z. \tag{56}$$

In an MR-WC, since the capacity region depends only on the conditional marginal distributions of the transmitter-receiver links, but not on the entire joint distribution of the channel, the correlations among $\mathbf{N}_1, \mathbf{N}_2, \mathbf{N}_Z$ do not affect the capacity region. Thus, without changing the corresponding capacity region, we can adjust the correlation structure among these noise vectors to ensure that they satisfy the Markov chain

$$\mathbf{X} \rightarrow \mathbf{Y}_1 \rightarrow \mathbf{Y}_2 \rightarrow \mathbf{Z} \tag{57}$$

which is always possible because of our assumption about the covariance matrices in (56).

We first provide an inner bound for the capacity region of the degraded Gaussian MIMO MR-WC with public and confidential messages by using Theorem 2 as stated in the following theorem.

Theorem 4: An achievable rate region for the degraded Gaussian MIMO MR-WC with public and confidential messages is given by the union of rate tuples $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ satisfying

$$R_{s2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\boldsymbol{\Sigma}_2|}{|\mathbf{K}+\boldsymbol{\Sigma}_2|} - \frac{1}{2}\log\frac{|\mathbf{S}+\boldsymbol{\Sigma}_Z|}{|\mathbf{K}+\boldsymbol{\Sigma}_Z|} \tag{58}$$

$$\sum_{j=1}^{2} R_{sj} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\boldsymbol{\Sigma}_2|}{|\mathbf{K}+\boldsymbol{\Sigma}_2|} + \frac{1}{2}\log\frac{|\mathbf{K}+\boldsymbol{\Sigma}_1|}{|\boldsymbol{\Sigma}_1|} - \frac{1}{2}\log\frac{|\mathbf{S}+\boldsymbol{\Sigma}_Z|}{|\boldsymbol{\Sigma}_Z|} \tag{59}$$

$$R_{s2} + R_{p2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\boldsymbol{\Sigma}_2|}{|\mathbf{K}+\boldsymbol{\Sigma}_2|} \tag{60}$$

$$\sum_{j=1}^{2} R_{sj} + R_{p2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\boldsymbol{\Sigma}_2|}{|\mathbf{K}+\boldsymbol{\Sigma}_2|} + \frac{1}{2}\log\frac{|\mathbf{K}+\boldsymbol{\Sigma}_1|}{|\boldsymbol{\Sigma}_1|} - \frac{1}{2}\log\frac{|\mathbf{K}+\boldsymbol{\Sigma}_Z|}{|\boldsymbol{\Sigma}_Z|} \tag{61}$$

$$\sum_{j=1}^{2} R_{sj} + R_{pj} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\boldsymbol{\Sigma}_2|}{|\mathbf{K}+\boldsymbol{\Sigma}_2|} + \frac{1}{2}\log\frac{|\mathbf{K}+\boldsymbol{\Sigma}_1|}{|\boldsymbol{\Sigma}_1|} \tag{62}$$

where $\mathbf{K}$ is a positive semidefinite matrix satisfying $\mathbf{K} \preceq \mathbf{S}$.

The achievable rate region given in Theorem 4 can be obtained by evaluating the achievable rate region in Theorem 2 for the degraded Gaussian MIMO MR-WC by using the following selection for $\mathbf{U}$, $\mathbf{X}$: 1) $\mathbf{U}$ is a zero-mean Gaussian random vector with covariance matrix $\mathbf{S}-\mathbf{K}$, 2) $\mathbf{X} = \mathbf{U} + \mathbf{U}'$ where $\mathbf{U}'$ is a zero-mean Gaussian random vector with covariance matrix $\mathbf{K}$, and is independent of $\mathbf{U}$. We note that besides this jointly Gaussian $(\mathbf{U}, \mathbf{X})$ selection, there might be other possible $(\mathbf{U}, \mathbf{X})$ selections which may yield a larger region than the one obtained by using jointly Gaussian $(\mathbf{U}, \mathbf{X})$. However, we show that jointly Gaussian $(\mathbf{U}, \mathbf{X})$ selection is sufficient to evaluate the achievable rate region in Theorem 2 for the degraded Gaussian MIMO MR-WC. This sufficiency result is stated in the following theorem.

Theorem 5: For the degraded Gaussian MIMO MR-WC, the achievable rate region in Theorem 2 is exhausted by jointly Gaussian $(\mathbf{U}, \mathbf{X})$. In particular, for any non-Gaussian $(\mathbf{U}, \mathbf{X})$, there exists a Gaussian $(\mathbf{U}^G, \mathbf{X}^G)$ which yields a larger region than the one obtained by using the non-Gaussian $(\mathbf{U}, \mathbf{X})$.

Next, we provide an outer bound for the capacity region of the degraded Gaussian MIMO MR-WC. This outer bound can be obtained by evaluating the outer bound given in Theorem 3 for the degraded Gaussian MIMO MR-WC. This evaluation is tantamount to finding the optimal $(\mathbf{U}, \mathbf{X})$ which exhausts the outer bound in Theorem 3 for the degraded Gaussian MIMO MR-WC. We show that jointly Gaussian $(\mathbf{U}, \mathbf{X})$ is sufficient to exhaust the outer bound in Theorem 3 for the degraded Gaussian MIMO channel. The corresponding outer bound is stated in the following theorem.

Theorem 6: The capacity region of the degraded Gaussian MIMO MR-WC is contained in the union of rate tuples $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ satisfying

$$R_{s2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\boldsymbol{\Sigma}_2|}{|\mathbf{K}+\boldsymbol{\Sigma}_2|} - \frac{1}{2}\log\frac{|\mathbf{S}+\boldsymbol{\Sigma}_Z|}{|\mathbf{K}+\boldsymbol{\Sigma}_Z|} \tag{63}$$

$$\sum_{j=1}^{2} R_{sj} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\boldsymbol{\Sigma}_2|}{|\mathbf{K}+\boldsymbol{\Sigma}_2|} + \frac{1}{2}\log\frac{|\mathbf{K}+\boldsymbol{\Sigma}_1|}{|\boldsymbol{\Sigma}_1|} - \frac{1}{2}\log\frac{|\mathbf{S}+\boldsymbol{\Sigma}_Z|}{|\boldsymbol{\Sigma}_Z|} \tag{64}$$

$$R_{s2} + R_{p2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\boldsymbol{\Sigma}_2|}{|\mathbf{K}+\boldsymbol{\Sigma}_2|} \tag{65}$$

$$\sum_{j=1}^{2} R_{sj} + R_{pj} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\boldsymbol{\Sigma}_2|}{|\mathbf{K}+\boldsymbol{\Sigma}_2|} + \frac{1}{2}\log\frac{|\mathbf{K}+\boldsymbol{\Sigma}_1|}{|\boldsymbol{\Sigma}_1|} \tag{66}$$

where $\mathbf{K}$ is a positive semidefinite matrix satisfying $\mathbf{K} \preceq \mathbf{S}$.

The proofs of Theorems 5 and 6 are given in Appendix D. We prove Theorems 5 and 6 by using the de Bruijn identity [9], a differential relationship between differential entropy and the Fisher information matrix, in conjunction with the properties of the Fisher information matrix. In particular, to prove Theorem 5, we consider the region in Theorem 2, and show that for any non-Gaussian $(\mathbf{U}, \mathbf{X})$, there exists a Gaussian $(\mathbf{U}^G, \mathbf{X}^G)$ which yields a larger region than the one that is obtained by evaluating the region in Theorem 2 with the non-Gaussian $(\mathbf{U}, \mathbf{X})$. We note that this proof of Theorem 5 implies the proof of Theorem 6. In particular, since the region in Theorem 2 includes all the constraints involved in the outer bound given in Theorem 3, the proof of Theorem 5 reveals that for any non-Gaussian $(\mathbf{U}, \mathbf{X})$, there exists a Gaussian $(\mathbf{U}^G, \mathbf{X}^G)$ which yields a larger region than the one that is obtained by evaluating the region in Theorem 3 with the non-Gaussian $(\mathbf{U}, \mathbf{X})$.

The inner bound in Theorem 4 and the outer bound in Theorem 6 do not match in general. However, similar to the discrete memoryless case in Section II-B, here also we can specialize the inner and outer bounds for the cases 1) $R_{s1} = 0$, 2) $R_{p2} = 0$, and 3) $R_{p1} = R_{p2} = 0$, where they match, yielding the capacity region. These three cases correspond to the extension of Corollaries 1, 2, 3 to the degraded Gaussian MIMO model. Finally, we note that the case $R_{p1} = R_{p2} = 0$ gives us the secrecy capacity region of the degraded Gaussian MIMO model, and in fact, the secrecy capacity region of the general, not necessarily degraded, Gaussian MIMO model is known due to [6].

IV. Conclusion

We study the MR-WC with public and confidential messages. We first consider the general, not necessarily degraded, discrete memoryless channel, and provide an inner bound for its capacity region by using Marton's coding and rate splitting in conjunction with superposition coding and binning. Second, we specialize this inner bound to the degraded case, where superposition coding and binning are sufficient to obtain this specialized form of the inner bound. We also provide an outer bound for the capacity region of the degraded case. We show that there are cases where these bounds match providing the capacity region. Third, we consider the degraded Gaussian MIMO MR-WC. We show that, to evaluate the proposed inner and outer bounds for the Gaussian MIMO case, it is sufficient to consider only jointly Gaussian auxiliary random variables and channel input. Similar to the discrete degraded case, for the degraded Gaussian MIMO case also, these bounds match for certain cases.

Appendix A
Proof of Theorem 1

We first consider a more general scenario than the scenario introduced in Section II-A, where the transmitter sends a pair of common public and confidential messages to the legitimate users in addition to a pair of public and confidential messages intended to each legitimate user. Thus, in this case, the transmitter has the message tuple $(W_{p0}, W_{s0}, W_{p1}, W_{s1}, W_{p2}, W_{s2})$, where the common public message W_{p0} and the common confidential message W_{s0} are sent to both legitimate users, and a pair of public and confidential messages (W_{pj}, W_{sj}) are sent to the jth legitimate user, $j = 1, 2$.[1] There is no secrecy concern on the public messages $\{W_{pj}\}_{j=0}^2$ while the confidential messages $\{W_{sj}\}_{j=0}^2$ need to be transmitted in perfect secrecy

$$\lim_{n\to\infty} \frac{1}{n} I(W_{s0}, W_{s1}, W_{s2}; Z^n) = 0. \tag{67}$$

Next, we prove an achievable rate region for the more general scenario we just introduced.

We fix the joint distribution $p(q, u, v_1, v_2, x, y_1, y_2, z) = p(q, u)p(v_1, v_2, x|u)p(y_1, y_2, z|x)$. Next, we divide the common public message W_{p0} into two parts as $W_{p0} = (\tilde{W}_{p0}, \tilde{\tilde{W}}_{p0})$, where the rate of $\tilde{W}_{p0}$ is $\tilde{R}_{p0}$, and the rate of $\tilde{\tilde{W}}_{p0}$ is $\tilde{\tilde{R}}_{p0}$. We use rate splitting for the common public message because due to [2], we know that rate splitting might enhance the achievable public and confidential message rate pairs even for the single legitimate user case.

Codebook Generation:

1) Generate $2^{n\tilde{R}_{p0}}$ length-n sequences q^n through $p(q^n) = \prod_{i=1}^n p(q_i)$, and index them as $q^n(\tilde{w}_{p0})$, where $\tilde{w}_{p0} \in \{1, \ldots, 2^{n\tilde{R}_{p0}}\}$.
2) For each $q^n(\tilde{w}_{p0})$ sequence, generate $2^{n(\tilde{\tilde{R}}_{p0}+R_{s0}+\Delta_0)}$ length-n sequences u^n through $p(u^n|q^n) = \prod_{i=1}^n p(u_i|q_i)$, and index them as $u^n(\tilde{w}_{p0}, \tilde{\tilde{w}}_{p0}, w_{s0}, d_0)$, where $\tilde{\tilde{w}}_{p0} \in \{1, \ldots, 2^{n\tilde{\tilde{R}}_{p0}}\}$, $w_{s0} \in \{1, \ldots, 2^{nR_{s0}}\}$, $d_0 \in \{1, \ldots, 2^{n\Delta_0}\}$.
3) For each $u^n(\tilde{w}_{p0}, \tilde{\tilde{w}}_{p0}, w_{s0}, d_0)$ sequence, generate $2^{n(R_{pj}+R_{sj}+\Delta_j+L_j)}$ length-n sequences v_j^n through $p(v_j^n|u^n) = \prod_{i=1}^n p(v_{ji}|u_i)$, and index them as $v_j^n(\tilde{w}_{p0}, \tilde{\tilde{w}}_{p0}, w_{s0}, d_0, w_{pj}, w_{sj}, d_j, l_j)$, where $w_{pj} \in \{1, \ldots, 2^{nR_{pj}}\}$, $w_{sj} \in \{1, \ldots, 2^{nR_{sj}}\}$, $d_j \in \{1, \ldots, 2^{n\Delta_j}\}$, $l_j \in \{1, \ldots, 2^{nL_j}\}$.

Encoding: Assume $(w_{p0}, w_{s0}, w_{p1}, w_{s1}, w_{p2}, w_{s2})$ is the message to be transmitted. Randomly pick d_0, d_1, d_2. Next, we find an (l_1, l_2) pair such that the corresponding sequence tuple (q^n, u^n, v_1^n, v_2^n) is jointly typical. Due to mutual covering lemma [11], if L_1, L_2 satisfy

$$L_1 + L_2 \geq I(V_1; V_2|U) \tag{68}$$

with high probability, there will be at least one such l_1, l_2 pair.

Decoding: The jth legitimate user decodes $(w_{p0}, w_{s0}, d_0, w_{pj}, w_{sj}, d_j)$ in two steps. In the first step, it decodes (w_{p0}, w_{s0}, d_0) by looking for the unique (q^n, u^n) pair such that (q^n, u^n, y_j^n) is jointly typical. In the second step, given that (w_{p0}, w_{s0}, d_0) is decoded correctly in the first step, the jth legitimate user decodes (w_{sj}, w_{pj}, d_j) by looking for the unique (q^n, u^n, v_j^n) tuple such that (q^n, u^n, v_j^n, y_j^n) is jointly typical. If the following conditions are satisfied:

$$R_{p0} + R_{s0} + \Delta_0 \leq \min_{j=1,2} I(U; Y_j) \tag{69}$$

$$\tilde{\tilde{R}}_{p0} + R_{s0} + \Delta_0 \leq I(U; Y_1|Q) \tag{70}$$

$$R_{p1} + R_{s1} + \Delta_1 + L_1 \leq I(V_1; Y_1|U) \tag{71}$$

$$\tilde{\tilde{R}}_{p0} + R_{s0} + \Delta_0 \leq I(U; Y_2|Q) \tag{72}$$

$$R_{p2} + R_{s2} + \Delta_2 + L_2 \leq I(V_2; Y_2|U) \tag{73}$$

both legitimate users decode their messages with vanishingly small probability of error.

[1] The inner bound in Theorem 1 can also be obtained by using rate splitting for $\{W_{pj}, W_{sj}\}_{j=1}^2$ as mentioned in Section II-A. Here, we introduce a pair of common messages $\{W_{p0}, W_{s0}\}$, because the corresponding scenario results in an achievable scheme that encompasses the one obtained by using rate splitting.

Equivocation Computation: We now show that the proposed coding scheme satisfies the perfect secrecy requirement on the confidential messages given by (67). We start as follows:

$$\begin{aligned}
&H(W_{s0}, W_{s1}, W_{s2}|Z^n) \geq H(W_{s0}, W_{s1}, W_{s2}|Z^n, Q^n)\\
&= H(W_{s0}, W_{s1}, W_{s2}, \tilde{\tilde{W}}_{p0}, W_{p1}, W_{p2}, D_0, D_1, D_2|Z^n, Q^n)\\
&\quad - H(\tilde{\tilde{W}}_{p0}, W_{p1}, W_{p2}, D_0, D_1, D_2|Z^n, Q^n, W_{s0}, W_{s1}, W_{s2}) &(74)\\
&= H(W_{s0}, W_{s1}, W_{s2}, \tilde{\tilde{W}}_{p0}, W_{p1}, W_{p2}, D_0, D_1, D_2|Q^n)\\
&\quad - I(W_{s0}, W_{s1}, W_{s2}, \tilde{\tilde{W}}_{p0}, W_{p1}, W_{p2}, D_0, D_1, D_2; Z^n|Q^n)\\
&\quad - H(\tilde{\tilde{W}}_{p0}, W_{p1}, W_{p2}, D_0, D_1, D_2|Z^n, Q^n, W_{s0}, W_{s1}, W_{s2}) &(75)\\
&= H(W_{s0}, W_{s1}, W_{s2}) + H(\tilde{\tilde{W}}_{p0}, W_{p1}, W_{p2}, D_0, D_1, D_2)\\
&\quad - I(W_{s0}, W_{s1}, W_{s2}, \tilde{\tilde{W}}_{p0}, W_{p1}, W_{p2}, D_0, D_1, D_2; Z^n|Q^n)\\
&\quad - H(\tilde{\tilde{W}}_{p0}, W_{p1}, W_{p2}, D_0, D_1, D_2|Z^n, Q^n, W_{s0}, W_{s1}, W_{s2}) &(76)\\
&= H(W_{s0}, W_{s1}, W_{s2}) + n\left(\tilde{\tilde{R}}_{p0} + \sum_{j=1}^{2} R_{pj} + \sum_{k=0}^{2} \Delta_k\right)\\
&\quad - I(W_{s0}, W_{s1}, W_{s2}, \tilde{\tilde{W}}_{p0}, W_{p1}, W_{p2}, D_0, D_1, D_2; Z^n|Q^n)\\
&\quad - H(\tilde{\tilde{W}}_{p0}, W_{p1}, W_{p2}, D_0, D_1, D_2|Z^n, Q^n, W_{s0}, W_{s1}, W_{s2}) &(77)\\
&= H(W_{s0}, W_{s1}, W_{s2}) + n\left(\tilde{\tilde{R}}_{p0} + \sum_{j=1}^{2} R_{pj} + \sum_{k=0}^{2} \Delta_k\right)\\
&\quad - I(U^n, V_1^n, V_2^n; Z^n|Q^n)\\
&\quad - H(\tilde{\tilde{W}}_{p0}, W_{p1}, W_{p2}, D_0, D_1, D_2|Z^n, Q^n, W_{s0}, W_{s1}, W_{s2}) &(78)\\
&\geq H(W_{s0}, W_{s1}, W_{s2}) + n\left(\tilde{\tilde{R}}_{p0} + \sum_{j=1}^{2} R_{pj} + \sum_{k=0}^{2} \Delta_k\right)\\
&\quad - n(I(U, V_1, V_2; Z|Q) + \gamma_{1n})\\
&\quad - H(\tilde{\tilde{W}}_{p0}, W_{p1}, W_{p2}, D_0, D_1, D_2|Z^n, Q^n, W_{s0}, W_{s1}, W_{s2}) &(79)
\end{aligned}$$

where (76) and (77) follow from the facts that the messages W_{s0}, W_{s1}, W_{s2}, $\tilde{\tilde{W}}_{p0}$, W_{p1}, W_{p2}, D_0, D_1, D_2 are independent among themselves, uniformly distributed, and also are independent of Q^n, (78) stems from the fact that given the codewords (Q^n, U^n, V_1^n, V_2^n), $(W_{s0}, W_{s1}, W_{s2}, \tilde{\tilde{W}}_{p0}, W_{p1}, W_{p2}, D_0, D_1, D_2)$ and Z^n are independent, and (79) comes from the fact that

$$I(U^n, V_1^n, V_2^n; Z^n|Q^n) \leq nI(U, V_1, V_2; Z|Q) + n\gamma_{1n} \quad (80)$$

where $\gamma_{1n} \to 0$ as $n \to \infty$. The bound in (80) can be shown by following the analysis in [12]. Next, we consider the conditional entropy term in (79). To this end, we introduce the following lemma.

Lemma 1: We have

$$H\left(\{W_{pj}, D_j\}_{j=1}^{2}|Z^n, Q^n, \{W_{sj}\}_{j=0}^{2}, \tilde{\tilde{W}}_{p0}, D_0\right) \leq n\gamma_{2n} \quad (81)$$

where $\gamma_{2n} \to 0$ as $n \to \infty$, if the following conditions are satisfied:

$$\begin{aligned}
\sum_{j=1}^{2} R_{pj} + \Delta_j + L_j &\leq I(V_1, V_2; Z|U) + I(V_1; V_2|U) &(82)\\
R_{p1} + \Delta_1 + L_1 &\leq I(V_1; Z, V_2|U) &(83)\\
R_{p2} + \Delta_2 + L_2 &\leq I(V_2; Z, V_1|U). &(84)
\end{aligned}$$

The proof of Lemma 1 is given in Appendix B. This lemma implies the following.

Corollary 4: We have

$$H(\tilde{\tilde{W}}_{p0}, D_0|Z^n, Q^n, W_{s0}, W_{s1}, W_{s2}) \leq n\gamma_{3n} \quad (85)$$

where $\gamma_{3n} \to 0$ as $n \to \infty$, if the following condition is satisfied:

$$\tilde{\tilde{R}}_{p0} + \Delta_0 \leq I(U; Z|Q). \quad (86)$$

Now, we set the rates $\tilde{\tilde{R}}_{p0}$, Δ_0, R_{p1}, Δ_1, L_1, R_{p2}, Δ_2, L_2 as follows:

$$\begin{aligned}
\tilde{\tilde{R}}_{p0} + \Delta_0 &= I(U; Z|Q) - \epsilon &(87)\\
L_1 + L_2 &= I(V_1; V_2|U) + \frac{\epsilon}{2} &(88)\\
R_{p1} + \Delta_1 + R_{p2} + \Delta_2 &= I(V_1, V_2; Z|U) - \epsilon &(89)\\
R_{p1} + \Delta_1 + L_1 &< I(V_1; Z, V_2|U) &(90)\\
R_{p2} + \Delta_2 + L_2 &< I(V_2; Z, V_1|U). &(91)
\end{aligned}$$

In view of Lemma 1 and Corollary 4, the selections of $\tilde{\tilde{R}}_{p0}$, Δ_0, R_{p1}, Δ_1, L_1, R_{p2}, Δ_2, L_2 in (87)–(91) imply that

$$H\left(\tilde{\tilde{W}}_{p0}, \{W_{pj}\}_{j=1}^{2}, \{D_j\}_{j=0}^{2}|Z^n, Q^n, \{W_{sj}\}_{j=0}^{2}\right) \leq n\gamma_{2n} \quad (92)$$

using which and (87)–(89) in (79), we get

$$\begin{aligned}
H(W_{s0}, W_{s1}, W_{s2}|Z^n) &\geq H(W_{s0}, W_{s1}, W_{s2})\\
&\quad + n\left(\tilde{\tilde{R}}_{p0} + R_{p0} + R_{p1} + R_{p2} + \Delta_0 + \Delta_1 + \Delta_2\right)\\
&\quad - n(I(U, V_1, V_2; Z|Q) + \gamma_{1n}) - n\gamma_{2n} &(93)\\
&= H(W_{s0}, W_{s1}, W_{s2}) - n\frac{3\epsilon}{2} - n(\gamma_{1n} + \gamma_{2n} + \gamma_{3n}) &(94)
\end{aligned}$$

which implies that the proposed coding scheme satisfies the perfect secrecy requirement on the confidential messages; completing the equivocation computation.

Hence, we show that rate tuples $(R_{p0}, R_{s0}, R_{p1}, R_{s1}, R_{p2}, R_{s2})$ satisfying

$$\begin{aligned} L_1 + L_2 &= I(V_1; V_2|U) && (95)\\ R_{p0} + R_{s0} + \Delta_0 &\le \min_{j=1,2} I(U; Y_j) && (96)\\ \tilde{\tilde{R}}_{p0} + R_{s0} + \Delta_0 &\le \min_{j=1,2} I(U; Y_j|Q) && (97)\\ R_{p1} + R_{s1} + \Delta_1 + L_1 &\le I(V_1; Y_1|U) && (98)\\ R_{p2} + R_{s2} + \Delta_2 + L_2 &\le I(V_2; Y_2|U) && (99)\\ \tilde{\tilde{R}}_{p0} + \Delta_0 &= I(U; Z|Q) && (100)\\ R_{p1} + \Delta_1 + R_{p2} + \Delta_2 &= I(V_1, V_2; Z|U) && (101)\\ R_{p1} + \Delta_1 + L_1 &\le I(V_1; Z, V_2|U) && (102)\\ R_{p2} + \Delta_2 + L_2 &\le I(V_2; Z, V_1|U) && (103) \end{aligned}$$

are achievable. Next, one can obtain the achievable rate region in Theorem 1 by using Fourier–Motzkin elimination in conjunction with the fact that since the common public and confidential messages W_{p0}, W_{s0} are decoded by both users, they can be converted into public and confidential messages $(W_{p1}, W_{s1}, W_{p2}, W_{s2})$ of the legitimate users.

APPENDIX B
PROOF OF LEMMA 1

Assume that, given $(W_{s0} = w_{s0}, W_{s1} = w_{s1}, W_{s2} = w_{s1}, W_{p0} = w_{p0})$, the eavesdropper tries to decode W_{p1}, D_1, L_1, W_{p2}, D_2, L_2 by looking for the unique (V_1^n, V_2^n) such that $(q^n, u^n, v_1^n, v_2^n, z^n)$ is jointly typical. There are four possible error events.

1) $\mathcal{E}_0^e = \{(q^n, u^n, v_1^n, v_2^n, z^n)$ is not jointly typical for the transmitted $(q^n, u^n, v_1^n, v_2^n)\}$.
2) $\mathcal{E}_i^e = \{(W_{p1}, D_1, L_1) = (1,1,1), (W_{p2}, D_2, L_2) \neq (1,1,1)$, and the corresponding tuple $(q^n, u^n, v_1^n, v_2^n, z^n)$ is jointly typical $\}$.
3) $\mathcal{E}_{ii}^e = \{(W_{p1}, D_1, L_1) \neq (1,1,1), (W_{p2}, D_2, L_2) = (1,1,1)$ and the corresponding tuple $(q^n, u^n, v_1^n, v_2^n, z^n)$ is jointly typical $\}$.
4) $\mathcal{E}_{iii}^e = \{(W_{p1}, D_1, L_1) \neq (1,1,1), (W_{p2}, D_2, L_2) \neq (1,1,1)$, and the corresponding tuple $(q^n, u^n, v_1^n, v_2^n, z^n)$ is jointly typical $\}$.

Thus, the probability of decoding error at the eavesdropper is given by

$$\begin{aligned} \Pr[\mathcal{E}^e] &\le \Pr[\mathcal{E}_0^e] + \Pr[\mathcal{E}_i^e] + \Pr[\mathcal{E}_{ii}^e] + \Pr[\mathcal{E}_{iii}^e] && (104)\\ &\le \epsilon_{1n} + \Pr[\mathcal{E}_i^e] + \Pr[\mathcal{E}_{ii}^e] + \Pr[\mathcal{E}_{iii}^e] && (105) \end{aligned}$$

where we first use the union bound, and next the fact that $\Pr[\mathcal{E}_0^e] \le \epsilon_{1n}$ for some ϵ_{1n} satisfying $\epsilon_{1n} \to 0$ as $n \to \infty$, which follows from the properties of the jointly typical sequences [8]. Next, we consider $\Pr[\mathcal{E}_i^e]$ as follows:

$$\begin{aligned} \Pr[\mathcal{E}_i^e] &\le \sum_{(w_{p2},d_2,l_2)\neq \mathbf{1}} \Pr[(q^n, u^n, v_1^n, V_2^n, Z^n) \in \mathcal{A}_\epsilon^n] && (106)\\ &\le \sum_{(w_{p2},d_2,l_2)\neq \mathbf{1}} \sum_{(v_2^n, z^n)\in\mathcal{A}_\epsilon^n} p(v_2^n|u^n) p(z^n|u^n, v_1^n) && (107)\\ &\le \sum_{(w_{p2},d_2,l_2)\neq \mathbf{1}} \sum_{(v_2^n, z^n)\in\mathcal{A}_\epsilon^n} 2^{-n(H(V_2|U)-\gamma_\epsilon)} 2^{-n(H(Z|U,V_1)-\gamma_\epsilon)} && (108)\\ &= \sum_{(w_{p2},d_2,l_2)\neq \mathbf{1}} |\mathcal{A}_\epsilon^n| 2^{-n(H(V_2|U)-\gamma_\epsilon)} 2^{-n(H(Z|U,V_1)-\gamma_\epsilon)} && (109)\\ &\le \sum_{(w_{p2},d_2,l_2)\neq \mathbf{1}} 2^{n(H(V_2,Z|U,V_1)+\gamma_\epsilon)} 2^{-n(H(V_2|U)-\gamma_\epsilon)} \\ &\qquad 2^{-n(H(Z|U,V_1)-\gamma_\epsilon)} && (110)\\ &\le 2^{n(R_{p2}+\Delta_2+L_2)} 2^{-n(I(V_2;Z,V_1|U)-3\gamma_\epsilon)} && (111) \end{aligned}$$

where $\mathbf{1}$ denotes the all 1s vector of appropriate size, $\mathcal{A}_\epsilon^n$ denotes the typical set, γ_ϵ is a constant that is a function of ϵ, and satisfies $\gamma_\epsilon \to 0$ as $\epsilon \to 0$, (107) is due to the joint distribution of (q^n, u^n, v_1^n, v_2^n), (108) is due to the properties of the typical sequences [8], and (110) comes from the bounds on the size of $\mathcal{A}_\epsilon^n$ [8]. Equation (111) implies that $\Pr[\mathcal{E}_i^e] \to 0$ as $n \to \infty$ if the following condition is satisfied:

$$R_{p2} + \Delta_2 + L_2 < I(V_2; Z, V_1|U) - 3\gamma_\epsilon. \qquad (112)$$

Similarly, we can show that $\Pr[\mathcal{E}_{ii}^e] \to 0$ as $n \to \infty$ if the following condition is satisfied:

$$R_{p1} + \Delta_1 + L_1 < I(V_1; Z, V_2|U) - 3\gamma_\epsilon. \qquad (113)$$

Next, we consider $\Pr[\mathcal{E}_{iii}^e]$ as follows:

$$\begin{aligned} \Pr[\mathcal{E}_{iii}^e] &\le \sum_{\substack{(w_{p1},d_1,l_1)\neq \mathbf{1}\\ (w_{p2},d_2,l_2)\neq \mathbf{1}}} \Pr[(q^n, u^n, V_1^n, V_2^n, Z^n) \in \mathcal{A}_\epsilon^n] && (114)\\ &\le \sum_{\substack{(w_{p1},d_1,l_1)\neq \mathbf{1}\\ (w_{p2},d_2,l_2)\neq \mathbf{1}}} \sum_{(v_1^n, v_2^n, z^n)\in\mathcal{A}_\epsilon^n} p(v_1^n|u^n) p(v_2^n|u^n) p(z^n|u^n) && (115)\\ &\le \sum_{\substack{(w_{p1},d_1,l_1)\neq \mathbf{1}\\ (w_{p2},d_2,l_2)\neq \mathbf{1}}} \sum_{(v_1^n, v_2^n, z^n)\in\mathcal{A}_\epsilon^n} 2^{-n(H(V_1|U)-\gamma_\epsilon)} 2^{-n(H(V_2|U)-\gamma_\epsilon)} \\ &\qquad 2^{-n(H(Z|U)-\gamma_\epsilon)} && (116)\\ &= \sum_{\substack{(w_{p1},d_1,l_1)\neq \mathbf{1}\\ (w_{p2},d_2,l_2)\neq \mathbf{1}}} |\mathcal{A}_\epsilon^n| 2^{-n(H(V_1|U)+H(V_2|U)+H(Z|U)-3\gamma_\epsilon)} && (117)\\ &\le \sum_{\substack{(w_{p1},d_1,l_1)\neq \mathbf{1}\\ (w_{p2},d_2,l_2)\neq \mathbf{1}}} 2^{n(H(V_1,V_2,Z|U)+\gamma_\epsilon)} \\ &\qquad 2^{-n(H(V_1|U)+H(V_2|U)+H(Z|U)-3\gamma_\epsilon)} && (118)\\ &\le 2^{n\left(\sum_{j=1}^{2} R_{pj}+\Delta_j+L_j\right)} 2^{-n(I(V_1,V_2;Z|U)+I(V_2;V_1|U)-4\gamma_\epsilon)} && (119) \end{aligned}$$

where (115) is due to the joint distribution of (q^n, u^n, v_1^n, v_2^n), (116) stems from the properties of the typical sequences [8], and (118) comes from the bounds on the size of $\mathcal{A}_\epsilon^n$ [8]. Equation (119) implies that $\Pr[\mathcal{E}_{iii}^e]$ vanishes as $n \to \infty$ if the following condition is satisfied:

$$\sum_{j=1}^{2} R_{pj} + \Delta_j + L_j < I(V_1, V_2; Z|U) + I(V_2; V_1|U) - 4\gamma_\epsilon. \tag{120}$$

Thus, we show that if the rates $(R_{p1}, \Delta_1, L_1, R_{p2}, \Delta_2, L_2)$ satisfy (112), (113), and (120), the eavesdropper can decode W_{p1}, D_1, L_1, W_{p2}, D_2, L_2 by using its knowledge of $(W_{s0}, W_{s1}, W_{s2}, W_{p0})$, i.e., $\Pr[\mathcal{E}^e]$ vanishes as $n \to \infty$. In view of this fact, using Fano's lemma, we get

$$H\left(\{W_{pj}, D_j, L_j\}_{j=1}^2 | Z^n, Q^n, \{W_{sj}\}_{j=0}^2, W_{p0}, D_0\right) \le n\gamma_{2n} \tag{121}$$

where $\gamma_{2n} \to 0$ as $n \to \infty$, completing the proof.

Appendix C
Proof of Theorem 3

We define the following auxiliary random variables:

$$U_i = W_{s2} W_{p2} Y_1^{i-1} Z_{i+1}^n, \quad i = 1, \dots, n \tag{122}$$

which satisfy the Markov chains $U_i \to X_i \to Y_{1i} \to Y_{2i} \to Z_i, \forall i$, since the channel is degraded and memoryless. For any $(n, 2^{nR_{p1}}, 2^{nR_{s1}}, 2^{nR_{p2}}, 2^{nR_{s2}})$ code achieving the rate tuple $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$, we have

$$H(W_{sj}, W_{pj}|Y_j^n) \le n\epsilon_n, \; j = 1, 2 \tag{123}$$

$$I(W_{s1}, W_{s2}; Z^n) \le n\gamma_n \tag{124}$$

where $\epsilon_n \to 0$, $\gamma_n \to 0$ as $n \to \infty$. Equation (123) is due to Fano's lemma, and (124) is due to the perfect secrecy requirement in (1). We note that (124) implies the following:

$$H(W_{s1}, W_{s2}) \le H(W_{s1}, W_{s2}, W_{p1}, W_{p2}|Z^n) + n\gamma_n. \tag{125}$$

We introduce the following lemma which follows from Csiszar–Korner sum identity [2, Lemma 7].

Lemma 2:

$$\begin{aligned} &I(W; T_1^n|Q) - (W; T_2^n|Q) \\ &= \sum_{i=1}^{n} I(W; T_{1i}|Q, T_1^{i-1}, T_{2,i+1}^n) - I(W; T_{2i}|Q, T_1^{i-1}, T_{2,i+1}^n). \end{aligned} \tag{126}$$

First, we obtain an outer bound for R_{s2} as follows:

$$\begin{aligned} nR_{s2} &\le \sum_{i=1}^{n} I(W_{s2}; Y_{2i}|Y_2^{i-1}, Z_{i+1}^n) \\ &\qquad - I(W_{s2}; Z_i|Y_2^{i-1}, Z_{i+1}^n) + n(\epsilon_n + \gamma_n) \qquad (127) \\ &\le \sum_{i=1}^{n} I(W_{s2}, W_{p2}, Y_2^{i-1}, Z_{i+1}^n, Y_1^{i-1}; Y_{2i}) \\ &\qquad - I(W_{s2}, W_{p2}, Y_2^{i-1}, Z_{i+1}^n, Y_1^{i-1}; Z_i) + n(\epsilon_n + \gamma_n) \qquad (128) \\ &= \sum_{i=1}^{n} I(U_i; Y_{2i}) - I(U_i; Z_i) + n(\gamma_n + \epsilon_n) \qquad (129) \end{aligned}$$

where (127) comes from the converse proof for the secrecy capacity of wiretap channels in [2], and (128) and (129) come from the following Markov chains:

$$W_{s2}, W_{p2}, Y_2^{i-1}, Z_{i+1}^n, Y_1^{i-1} \to Y_{2i} \to Z_i \tag{130}$$

$$W_{s2}, W_{p2}, Z_i^n, Y_{2i} \to Y_1^{i-1} \to Y_2^{i-1} \tag{131}$$

respectively, which follow from the fact that the channel is degraded and memoryless.

Next, we obtain an outer bound for $R_{s1} + R_{s2}$ as follows:

$$\begin{aligned} &n(R_{s1} + R_{s2}) \le H(W_{s1}, W_{p1}, W_{s2}, W_{p2}|Z^n) + n\gamma_n \qquad (132) \\ &\le I(W_{s1}, W_{p1}; Y_1^n|W_{s2}, W_{p2}) - I(W_{s1}, W_{p1}; Z^n|W_{s2}, W_{p2}) \\ &\qquad + I(W_{s2}, W_{p2}; Y_2^n) - I(W_{s2}, W_{p2}; Z^n) + n(\gamma_n + 2\epsilon_n) \qquad (133) \\ &\le I(W_{s1}, W_{p1}; Y_1^n|W_{s2}, W_{p2}) - I(W_{s1}, W_{p1}; Z^n|W_{s2}, W_{p2}) \\ &\qquad + \sum_{i=1}^{n} I(U_i; Y_{2i}) - I(U_i; Z_i) + n(\gamma_n + 2\epsilon_n) \qquad (134) \\ &= \sum_{i=1}^{n} I(W_{s1}, W_{p1}; Y_{1i}|U_i) - I(W_{s1}, W_{p1}; Z_i|U_i) \\ &\qquad + I(U_i; Y_{2i}) - I(U_i; Z_i) + n(\gamma_n + 2\epsilon_n) \qquad (135) \\ &\le \sum_{i=1}^{n} I(X_i; Y_{1i}|U_i) + I(U_i; Y_{2i}) - I(X_i; Z_i) + n(\gamma_n + 2\epsilon_n) \qquad (136) \end{aligned}$$

where (132) comes from (125), (134) is due to (129), (135) comes from Lemma 2, (136) is a consequence of the fact that the channel is memoryless and degraded.

Next, we obtain an outer bound for $R_{p2} + R_{s2}$ as follows:

$$\begin{aligned} n(R_{p2} + R_{s2}) &\le I(W_{s2}, W_{p2}; Y_2^n) + n\epsilon_n \qquad (137) \\ &= \sum_{i=1}^{n} I(W_{s2}, W_{p2}; Y_{2i}|Y_2^{i-1}) + n\epsilon_n \qquad (138) \\ &= \sum_{i=1}^{n} I(W_{s2}, W_{p2}, Y_1^{i-1}, Z_{i+1}^n; Y_{2i}|Y_2^{i-1}) \\ &\qquad - I(Y_1^{i-1}, Z_{i+1}^n; Y_{2i}|W_{s2}, W_{p2}, Y_2^{i-1}) + n\epsilon_n \qquad (139) \\ &\le \sum_{i=1}^{n} I(W_{s2}, W_{p2}, Y_1^{i-1}, Y_2^{i-1}, Z_{i+1}^n; Y_{2i}) \\ &\qquad - I(Y_1^{i-1}, Z_{i+1}^n; Y_{2i}|W_{s2}, W_{p2}, Y_2^{i-1}) + n\epsilon_n \qquad (140) \\ &= \sum_{i=1}^{n} I(U_i; Y_{2i}) - I(Y_1^{i-1}, Z_{i+1}^n; Y_{2i}|W_{s2}, W_{p2}, Y_2^{i-1}) \\ &\qquad + n\epsilon_n \qquad (141) \\ &\le \sum_{i=1}^{n} I(U_i; Y_{2i}) + n\epsilon_n \qquad (142) \end{aligned}$$

where (141) comes from the Markov chain in (131).

Finally, we obtain an outer bound for the sum rate $R_{p1}+R_{s1}+R_{p2}+R_{s2}$. To this end, we consider the following:

$$n(R_{p1}+R_{s1}) \le I(W_{p1},W_{s1};Y_1^n|W_{p2},W_{s2}) + n\epsilon_n \tag{143}$$

$$= \sum_{i=1}^{n} I(W_{p1},W_{s1};Y_{1i}|W_{p2},W_{s2},Y_1^{i-1}) + n\epsilon_n \tag{144}$$

$$\le \sum_{i=1}^{n} I(W_{p1},W_{s1},Z_{i+1}^n;Y_{1i}|W_{p2},W_{s2},Y_1^{i-1}) + n\epsilon_n \tag{145}$$

$$\begin{aligned} &= \sum_{i=1}^{n} I(Z_{i+1}^n;Y_{1i}|W_{p2},W_{s2},Y_1^{i-1}) + I(W_{p1},W_{s1};Y_{1i}|U_i) \\ &\quad + n\epsilon_n \end{aligned} \tag{146}$$

$$\le \sum_{i=1}^{n} I(Z_{i+1}^n;Y_{1i}|W_{p2},W_{s2},Y_1^{i-1}) + I(X_i;Y_{1i}|U_i) + n\epsilon_n \tag{147}$$

using which and (141), we have

$$\begin{aligned} &n(R_{p1}+R_{s1}+R_{p2}+R_{s2}) \\ &\le \sum_{i=1}^{n} I(U_i;Y_{2i}) - I(Y_1^{i-1},Z_{i+1}^n;Y_{2i}|Y_2^{i-1},W_{s2},W_{p2}) \\ &\quad + I(Z_{i+1}^n;Y_{1i}|W_{p2},W_{s2},Y_1^{i-1}) + I(X_i;Y_{1i}|U_i) + 2n\epsilon_n \end{aligned} \tag{148}$$

$$\begin{aligned} &= \sum_{i=1}^{n} I(U_i;Y_{2i}) - I(Z_{i+1}^n;Y_{2i}|Y_2^{i-1},W_{s2},W_{p2}) \\ &\quad - I(Y_1^{i-1};Y_{2i}|Y_2^{i-1},W_{s2},W_{p2},Z_{i+1}^n) \\ &\quad + I(Z_{i+1}^n;Y_{1i}|W_{p2},W_{s2},Y_1^{i-1}) + I(X_i;Y_{1i}|U_i) + 2n\epsilon_n \end{aligned} \tag{149}$$

$$\begin{aligned} &= \sum_{i=1}^{n} I(U_i;Y_{2i}) - I(Y_2^{i-1};Z_i|W_{s2},W_{p2},Z_{i+1}^n) \\ &\quad - I(Y_1^{i-1};Y_{2i}|Y_2^{i-1},W_{s2},W_{p2},Z_{i+1}^n) \\ &\quad + I(Y_1^{i-1};Z_i|W_{p2},W_{s2},Z_{i+1}^n) + I(X_i;Y_{1i}|U_i) + 2n\epsilon_n \end{aligned} \tag{150}$$

$$\begin{aligned} &= \sum_{i=1}^{n} I(U_i;Y_{2i}) - I(Y_2^{i-1};Z_i|W_{s2},W_{p2},Z_{i+1}^n) \\ &\quad - I(Y_1^{i-1};Y_{2i}|Y_2^{i-1},W_{s2},W_{p2},Z_{i+1}^n) \\ &\quad + I(Y_2^{i-1},Y_1^{i-1};Z_i|W_{p2},W_{s2},Z_{i+1}^n) + I(X_i;Y_{1i}|U_i) \\ &\quad + 2n\epsilon_n \end{aligned} \tag{151}$$

$$\begin{aligned} &= \sum_{i=1}^{n} I(U_i;Y_{2i}) - I(Y_1^{i-1};Y_{2i}|Y_2^{i-1},W_{s2},W_{p2},Z_{i+1}^n) \\ &\quad + I(Y_1^{i-1};Z_i|W_{p2},W_{s2},Z_{i+1}^n,Y_2^{i-1}) + I(X_i;Y_{1i}|U_i) \\ &\quad + 2n\epsilon_n \end{aligned} \tag{152}$$

$$\begin{aligned} &= \sum_{i=1}^{n} I(U_i;Y_{2i}) - I(Y_1^{i-1};Y_{2i},Z_i|Y_2^{i-1},W_{s2},W_{p2},Z_{i+1}^n) \\ &\quad + I(Y_1^{i-1};Z_i|W_{p2},W_{s2},Z_{i+1}^n,Y_2^{i-1}) + I(X_i;Y_{1i}|U_i) \\ &\quad + 2n\epsilon_n \end{aligned} \tag{153}$$

$$\begin{aligned} &= \sum_{i=1}^{n} I(U_i;Y_{2i}) - I(Y_1^{i-1};Y_{2i}|Y_2^{i-1},W_{s2},W_{p2},Z_{i+1}^n,Z_i) \\ &\quad + I(X_i;Y_{1i}|U_i) + 2n\epsilon_n \end{aligned} \tag{154}$$

where (150) comes from Csiszar–Korner sum identity [2, Lemma 7], (151) is due to the Markov chain in (131), and (153) is a consequence of the Markov chain in (130). Equation (154) implies

$$\begin{aligned} n(R_{p1}+R_{s1}+R_{p2}+R_{s2}) &\le \sum_{i=1}^{n} I(U_i;Y_{2i}) + I(X_i;Y_{1i}|U_i) \\ &\quad + 2n\epsilon_n. \end{aligned} \tag{155}$$

Using (129), (136), (142), and (155), Theorem 3 can be concluded.

Appendix D
Proofs of Theorems 5 and 6

A) Background: Here, we introduce some properties of the Fisher information and the differential entropy.

Definition 1 ([6, Definition 3]): Let $(\mathbf{U},\mathbf{X})$ be an arbitrary length-n random vector pair with well-defined densities. The conditional Fisher information matrix of $\mathbf{X}$ given $\mathbf{U}$ is

$$\mathbf{J}(\mathbf{X}|\mathbf{U}) = E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})^\top\right] \tag{156}$$

where the expectation is over the joint density $f(\mathbf{u},\mathbf{x})$, and $\boldsymbol{\rho}(\mathbf{x}|\mathbf{u})$ is the conditional score function given by $\boldsymbol{\rho}(\mathbf{x}|\mathbf{u}) = \nabla_{\mathbf{x}} \log f(\mathbf{x}|\mathbf{u})$.

The following two lemmas, which were proved in [6], will be used in the upcoming proof.

Lemma 3 ([6, Lemma 6]): Let $\mathbf{T}$, $\mathbf{U}$, $\mathbf{V}_1$, $\mathbf{V}_2$ be random vectors such that $(\mathbf{T},\mathbf{U})$ and $(\mathbf{V}_1,\mathbf{V}_2)$ are independent. Moreover, let $\mathbf{V}_1$, $\mathbf{V}_2$ be Gaussian random vectors with covariance matrices $\boldsymbol{\Sigma}_1, \boldsymbol{\Sigma}_2$ such that $\mathbf{0} \prec \boldsymbol{\Sigma}_1 \preceq \boldsymbol{\Sigma}_2$. Then, we have

$$\mathbf{J}^{-1}(\mathbf{U}+\mathbf{V}_2|\mathbf{T}) - \boldsymbol{\Sigma}_2 \succeq \mathbf{J}^{-1}(\mathbf{U}+\mathbf{V}_1|\mathbf{T}) - \boldsymbol{\Sigma}_1. \tag{157}$$

Lemma 4 ([6, Lemma 8]): Let $\mathbf{K}_1$ and $\mathbf{K}_2$ be positive semidefinite matrices satisfying $\mathbf{0} \preceq \mathbf{K}_1 \preceq \mathbf{K}_2$, and $\mathbf{f}(\mathbf{K})$ be a matrix-valued function such that $\mathbf{f}(\mathbf{K}) \succeq \mathbf{0}$ for $\mathbf{K}_1 \preceq \mathbf{K} \preceq \mathbf{K}_2$. Moreover, $\mathbf{f}(\mathbf{K})$ is assumed to be gradient of some scalar field. Then, we have

$$\int_{\mathbf{K}_1}^{\mathbf{K}_2} \mathbf{f}(\mathbf{K})d\mathbf{K} \ge 0. \tag{158}$$

The following generalization of the de Bruijn identity is due to [9], where the unconditional form of this identity, i.e., $\mathbf{U} = \phi$, is proved. Its generalization to this conditional form for an arbitrary $\mathbf{U}$ is rather straightforward, and is given in Lemma 16 of [6].

Lemma 5 ([6, Lemma 16]): Let $(\mathbf{U},\mathbf{X})$ be an arbitrarily correlated random vector pair with finite second-order moments, and also be independent of the random vector $\mathbf{N}$ which is zero-mean Gaussian with covariance matrix $\boldsymbol{\Sigma}_N \succ \mathbf{0}$. Then, we have

$$\nabla_{\boldsymbol{\Sigma}_N} h(\mathbf{X}+\mathbf{N}|\mathbf{U}) = \frac{1}{2}\mathbf{J}(\mathbf{X}+\mathbf{N}|\mathbf{U}). \tag{159}$$

The following lemma is due to [13] and [14] which lower bounds the differential entropy in terms of the Fisher information matrix.

Lemma 6 ([13], [14]): Let $(\mathbf{U},\mathbf{X})$ be an arbitrary random vector, where the conditional Fisher information matrix of $\mathbf{X}$, conditioned on $\mathbf{U}$, exists. Then, we have

$$h(\mathbf{X}|\mathbf{U}) \geq \frac{1}{2}\log|(2\pi e)\mathbf{J}^{-1}(\mathbf{X}|\mathbf{U})|. \tag{160}$$

B) Proofs: First, we prove Theorem 5 by showing that for any $(\mathbf{U},\mathbf{X})$, there exists a Gaussian $(\mathbf{U}^G,\mathbf{X}^G)$ which provides a larger region. Essentially, this proof will also yield a proof for Theorem 6 because the outer bound in Theorem 3 is defined by the same inequalities that define the inner bound given in Theorem 2 except for the inequality in (21).

First Step: We consider the bound on R_{s2} given in (18) as follows:

$$\begin{aligned} R_{s2} &\leq I(\mathbf{U};\mathbf{Y}_2) - I(\mathbf{U};\mathbf{Z}) && (161)\\ &= [h(\mathbf{Y}_2) - h(\mathbf{Z})] + [h(\mathbf{Z}|\mathbf{U}) - h(\mathbf{Y}_2|\mathbf{U})] && (162)\\ &\leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{S}+\mathbf{\Sigma}_Z|} + [h(\mathbf{Z}|\mathbf{U}) - h(\mathbf{Y}_2|\mathbf{U})] && (163)\end{aligned}$$

where (163) follows from the worst additive noise lemma [15, Lemma II.2]. Next, we consider the remaining terms in (163) as follows:

$$h(\mathbf{Z}|\mathbf{U}) - h(\mathbf{Y}_2|\mathbf{U}) = \frac{1}{2}\int_{\mathbf{\Sigma}_2}^{\mathbf{\Sigma}_Z} \mathbf{J}(\mathbf{X}+\mathbf{N}|\mathbf{U})d\mathbf{\Sigma}_N \tag{164}$$

which follows from Lemma 5, and $\mathbf{N}$ is a Gaussian random vector with covariance matrix $\mathbf{\Sigma}_N$ satisfying $\mathbf{\Sigma}_2 \preceq \mathbf{\Sigma}_N \preceq \mathbf{\Sigma}_Z$. Using Lemma 3, we have

$$\begin{aligned}\mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_2|\mathbf{U}) - \mathbf{\Sigma}_2 &\preceq \mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}|\mathbf{U}) - \mathbf{\Sigma}_N\\ &\preceq \mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_Z|\mathbf{U}) - \mathbf{\Sigma}_Z \quad (165)\end{aligned}$$

for any $\mathbf{\Sigma}_N$ satisfying $\mathbf{\Sigma}_2 \preceq \mathbf{\Sigma}_N \preceq \mathbf{\Sigma}_Z$, which imply

$$\begin{aligned}&\left[\mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_Z|\mathbf{U}) - \mathbf{\Sigma}_Z + \mathbf{\Sigma}_N\right]^{-1}\\ &\qquad \preceq \mathbf{J}(\mathbf{X}+\mathbf{N}|\mathbf{U})\\ &\qquad \preceq \left[\mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_2|\mathbf{U}) - \mathbf{\Sigma}_2 + \mathbf{\Sigma}_N\right]^{-1}. \end{aligned} \tag{166}$$

Using these inequalities in (164) in conjunction with Lemma 4, we get

$$\begin{aligned}&\frac{1}{2}\log\frac{|\mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_Z|\mathbf{U})|}{|\mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_Z) - \mathbf{\Sigma}_Z + \mathbf{\Sigma}_2|}\\ &\qquad \leq h(\mathbf{Z}|\mathbf{U}) - h(\mathbf{Y}_2|\mathbf{U})\\ &\qquad \leq \frac{1}{2}\log\frac{|\mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_2|\mathbf{U}) - \mathbf{\Sigma}_2 + \mathbf{\Sigma}_Z|}{|\mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_2)|} \quad (167)\end{aligned}$$

which can be expressed as

$$f(0) \leq h(\mathbf{Z}|\mathbf{U}) - h(\mathbf{Y}_2|\mathbf{U}) \leq f(1) \tag{168}$$

where $f(t)$ is defined as

$$f(t) = \frac{1}{2}\log\frac{|\mathbf{K}_1(t)+\mathbf{\Sigma}_Z|}{|\mathbf{K}_1(t)+\mathbf{\Sigma}_2|}, \quad 0 \leq t \leq 1 \tag{169}$$

and $\mathbf{K}_1(t)$ is given by

$$\begin{aligned}\mathbf{K}_1(t) = (1-t)&\left[\mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_Z|\mathbf{U}) - \mathbf{\Sigma}_Z\right]\\ &+ t\left[\mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_2|\mathbf{U}) - \mathbf{\Sigma}_2\right]. \end{aligned}\tag{170}$$

Since $f(t)$ is continuous in t, due to the intermediate value theorem, there exists a t_1^* such that $0 \leq t_1^* \leq 1$, and

$$f(t_1^*) = h(\mathbf{Z}|\mathbf{U}) - h(\mathbf{Y}_2|\mathbf{U}) = \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{\Sigma}_Z|}{|\mathbf{K}_1+\mathbf{\Sigma}_2|} \tag{171}$$

where $\mathbf{K}_1 = \mathbf{K}_1(t_1^*)$. Since $0 \leq t_1^* \leq 1$, $\mathbf{K}_1$ satisfies

$$\mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_2|\mathbf{U}) - \mathbf{\Sigma}_2 \preceq \mathbf{K}_1 \preceq \mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_Z|\mathbf{U}) - \mathbf{\Sigma}_Z \tag{172}$$

in view of (170). Moreover, we have

$$\begin{aligned}\mathbf{K}_1 &\preceq \mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_Z|\mathbf{U}) - \mathbf{\Sigma}_Z && (173)\\ &\preceq \mathrm{Cov}(\mathbf{X}+\mathbf{N}_Z|\mathbf{U}) - \mathbf{\Sigma}_Z && (174)\\ &\preceq \mathrm{Cov}(\mathbf{X}+\mathbf{N}_Z) - \mathbf{\Sigma}_Z && (175)\\ &\preceq \mathbf{S} && (176)\end{aligned}$$

where (174) comes from the conditional Cramer–Rao inequality [6, Lemma 13] and (175) is due to the fact that conditioning reduces the MMSE matrix in a positive semidefinite ordering sense. Thus, in view of (172) and (176), $\mathbf{K}_1$ satisfies

$$\mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_2|\mathbf{U}) - \mathbf{\Sigma}_2 \preceq \mathbf{K}_1 \preceq \mathbf{S}. \tag{177}$$

Now, using (171) in (163), we get the following bound on R_{s2}:

$$R_{s2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}_1+\mathbf{\Sigma}_2|} - \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{K}_1+\mathbf{\Sigma}_Z|} \tag{178}$$

which completes the first step of the proof.

Second Step: We consider the bound on $R_{s1}+R_{s2}$ given in (19) as follows:

$$\begin{aligned}R_{s1}+R_{s2} &\leq I(\mathbf{U};\mathbf{Y}_2) + I(\mathbf{X};\mathbf{Y}_1|\mathbf{U}) - I(\mathbf{X};\mathbf{Z}) && (179)\\ &= [h(\mathbf{Y}_2)-h(\mathbf{Z})] + [h(\mathbf{Y}_1|\mathbf{U}) - h(\mathbf{Y}_2|\mathbf{U})] - \frac{1}{2}\log\frac{|\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_Z|} && (180)\\ &\leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{S}+\mathbf{\Sigma}_Z|} + [h(\mathbf{Y}_1|\mathbf{U}) - h(\mathbf{Y}_2|\mathbf{U})] - \frac{1}{2}\log\frac{|\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_Z|} && (181)\end{aligned}$$

where (181) comes from the worst additive noise lemma [15, Lemma II.2]. Next, we consider the remaining term in (181) as follows:

$$h(\mathbf{Y}_2|\mathbf{U}) - h(\mathbf{Y}_1|\mathbf{U}) = \frac{1}{2}\int_{\mathbf{\Sigma}_1}^{\mathbf{\Sigma}_2} \mathbf{J}(\mathbf{X}+\mathbf{N}|\mathbf{U})d\mathbf{\Sigma}_N \tag{182}$$

which follows from Lemma 5, and $\mathbf{N}$ is a Gaussian random vector with covariance matrix $\mathbf{\Sigma}_N$ satisfying $\mathbf{\Sigma}_1 \preceq \mathbf{\Sigma}_N \preceq \mathbf{\Sigma}_2$. For any Gaussian random vector $\mathbf{N}$ with $\mathbf{\Sigma}_N \preceq \mathbf{\Sigma}_2$, we have

$$\begin{aligned}\mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}|\mathbf{U}) - \mathbf{\Sigma}_N &\preceq \mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_2|\mathbf{U}) - \mathbf{\Sigma}_2 \quad (183)\\ &\preceq \mathbf{K}_1 \quad (184)\end{aligned}$$

where (183) is due to Lemma 3, and (184) comes from (177). Equation (184) implies

$$\mathbf{J}(\mathbf{X}+\mathbf{N}|\mathbf{U}) \succeq (\mathbf{K}_1+\mathbf{\Sigma}_N)^{-1}, \quad \mathbf{\Sigma}_N \preceq \mathbf{\Sigma}_2. \quad (185)$$

Using (185) in (182) in conjunction with Lemma 4, we have

$$\begin{aligned}h(\mathbf{Y}_2|\mathbf{U}) - h(\mathbf{Y}_1|\mathbf{U}) &\geq \frac{1}{2}\int_{\mathbf{\Sigma}_1}^{\mathbf{\Sigma}_2} (\mathbf{K}_1+\mathbf{\Sigma}_N)^{-1} d\mathbf{\Sigma}_N \quad (186)\\ &= \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{\Sigma}_2|}{|\mathbf{K}_1+\mathbf{\Sigma}_1|}. \quad (187)\end{aligned}$$

Using (187) in (181), we get

$$\begin{aligned}R_{s1}+R_{s2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}_1+\mathbf{\Sigma}_2|} + \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|}\\ - \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \quad (188)\end{aligned}$$

which completes the second step of the proof.

Third Step: We consider the bound on $R_{s2}+R_{p2}$ given in (20) as follows:

$$\begin{aligned}R_{p2}+R_{s2} &\leq I(\mathbf{U};\mathbf{Y}_2) \quad (189)\\ &\leq \frac{1}{2}\log|(2\pi e)(\mathbf{S}+\mathbf{\Sigma}_2)| - h(\mathbf{Y}_2|\mathbf{U}) \quad (190)\end{aligned}$$

where (190) comes from the maximum entropy theorem [8]. Next, we consider the remaining term in (190). Using (171), we have

$$\begin{aligned}h(\mathbf{Y}_2|\mathbf{U}) &= h(\mathbf{Z}|\mathbf{U}) - \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{\Sigma}_Z|}{|\mathbf{K}_1+\mathbf{\Sigma}_2|} \quad (191)\\ &\geq \frac{1}{2}\log|(2\pi e)\mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_Z|\mathbf{U})| - \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{\Sigma}_Z|}{|\mathbf{K}_1+\mathbf{\Sigma}_2|} \quad (192)\\ &\geq \frac{1}{2}\log|(2\pi e)(\mathbf{K}_1+\mathbf{\Sigma}_Z)| - \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{\Sigma}_Z|}{|\mathbf{K}_1+\mathbf{\Sigma}_2|} \quad (193)\\ &= \frac{1}{2}\log|(2\pi e)(\mathbf{K}_1+\mathbf{\Sigma}_2)| \quad (194)\end{aligned}$$

where (192) is due to Lemma 6, and (193) comes from (173) and monotonicity of $|\cdot|$ in positive semidefinite matrices. Using (194) in (190), we get

$$R_{p2}+R_{s2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}_1+\mathbf{\Sigma}_2|} \quad (195)$$

which completes the third step of the proof.

Fourth Step: We consider the bound in (21) as follows:

$$\begin{aligned}&R_{s1}+R_{p2}+R_{s2}\\ &\leq I(\mathbf{U};\mathbf{Y}_2) + I(\mathbf{X};\mathbf{Y}_1|\mathbf{U}) - I(\mathbf{X};\mathbf{Z}|\mathbf{U}) \quad (196)\\ &= h(\mathbf{Y}_2) - h(\mathbf{Y}_2|\mathbf{U}) + [h(\mathbf{Y}_1|\mathbf{U}) - h(\mathbf{Z}|\mathbf{U})] - \frac{1}{2}\log\frac{|\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_Z|} \quad (197)\\ &\leq \frac{1}{2}\log|(2\pi e)(\mathbf{S}+\mathbf{\Sigma}_2)| - h(\mathbf{Y}_2|\mathbf{U})\\ &\quad + [h(\mathbf{Y}_1|\mathbf{U}) - h(\mathbf{Z}|\mathbf{U})] - \frac{1}{2}\log\frac{|\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_Z|} \quad (198)\\ &\leq \frac{1}{2}\log|(2\pi e)(\mathbf{S}+\mathbf{\Sigma}_2)| - \frac{1}{2}\log|(2\pi e)(\mathbf{K}_1+\mathbf{\Sigma}_2)|\\ &\quad + [h(\mathbf{Y}_1|\mathbf{U}) - h(\mathbf{Z}|\mathbf{U})] - \frac{1}{2}\log\frac{|\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_Z|} \quad (199)\\ &= \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}_1+\mathbf{\Sigma}_2|} + [h(\mathbf{Y}_1|\mathbf{U}) - h(\mathbf{Y}_2|\mathbf{U})]\\ &\quad + [h(\mathbf{Y}_2|\mathbf{U}) - h(\mathbf{Z}|\mathbf{U})] - \frac{1}{2}\log\frac{|\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_Z|} \quad (200)\\ &= \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}_1+\mathbf{\Sigma}_2|} + [h(\mathbf{Y}_1|\mathbf{U}) - h(\mathbf{Y}_2|\mathbf{U})]\\ &\quad + \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{\Sigma}_2|}{|\mathbf{K}_1+\mathbf{\Sigma}_Z|} - \frac{1}{2}\log\frac{|\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_Z|} \quad (201)\\ &\leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}_1+\mathbf{\Sigma}_2|} + \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{\Sigma}_1|}{|\mathbf{K}_1+\mathbf{\Sigma}_2|}\\ &\quad + \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{\Sigma}_2|}{|\mathbf{K}_1+\mathbf{\Sigma}_Z|} - \frac{1}{2}\log\frac{|\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_Z|} \quad (202)\\ &= \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}_1+\mathbf{\Sigma}_2|} + \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|} - \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \quad (203)\end{aligned}$$

where (198) comes from the maximum entropy theorem [8], (199) comes from (194), (201) is due to (171), and (202) comes from (187).

Fifth Step: We consider the bound in (22) as follows:

$$\begin{aligned}R_{p1}+R_{s1}+R_{p2}+R_{s2} &\leq I(\mathbf{U};\mathbf{Y}_2) + I(\mathbf{X};\mathbf{Y}_1|\mathbf{U}) \quad (204)\\ &= h(\mathbf{Y}_2) + [h(\mathbf{Y}_1|\mathbf{U}) - h(\mathbf{Y}_2|\mathbf{U})] - \frac{1}{2}\log|(2\pi e)\mathbf{\Sigma}_1| \quad (205)\\ &\leq \frac{1}{2}\log|(2\pi e)(\mathbf{S}+\mathbf{\Sigma}_2)| + [h(\mathbf{Y}_1|\mathbf{U}) - h(\mathbf{Y}_2|\mathbf{U})]\\ &\quad - \frac{1}{2}\log|(2\pi e)\mathbf{\Sigma}_1| \quad (206)\\ &\leq \frac{1}{2}\log|(2\pi e)(\mathbf{S}+\mathbf{\Sigma}_2)| + \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{\Sigma}_1|}{|\mathbf{K}_1+\mathbf{\Sigma}_2|}\\ &\quad - \frac{1}{2}\log|(2\pi e)\mathbf{\Sigma}_1| \quad (207)\\ &= \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}_1+\mathbf{\Sigma}_2|} + \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|} \quad (208)\end{aligned}$$

where (206) comes from the maximum entropy theorem [8], and (207) comes from (187).

Hence, we have shown that for any feasible $(\mathbf{U},\mathbf{X})$, there exists a Gaussian $(\mathbf{U}^G,\mathbf{X}^G)$ which yields a larger rate region. This completes the proof.

REFERENCES

[1] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[3] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "The secrecy rate region of the broadcast channel," presented at the 46th Annu. Allerton Conf. Commun., Control Comput., Monticello, IL, USA, Sep. 2008, Also available at [arXiv:0806.4200].

[4] E. Ekrem and S. Ulukus, "On secure broadcasting," presented at the 42th Asilomar Conf. Signals, Syst. Comput., Pacific Grove, CA, USA, Oct. 2008.

[5] E. Ekrem and S. Ulukus, "Secrecy capacity of a class of broadcast channels with an eavesdropper," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, pp. 824235-1–824235-30, 2009.

[6] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2083–2114, Apr. 2011.

[7] K. Marton, "A coding theorem for the discrete memoryless channels," *IEEE Trans. Inf. Theory*, vol. 25, no. 1, pp. 306–311, May 1979.

[8] T. Cover and J. Thomas, *Elements of Information Theory*, 2nd ed. New York, NY, USA: Wiley, 2006.

[9] D. P. Palomar and S. Verdu, "Gradient of mutual information in linear vector Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 52, no. 1, pp. 141–154, Jan. 2006.

[10] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz), "A vector generalization of Costa's entropy-power inequality with applications," *IEEE Trans. Inf. Theory*, vol. 56, no. 4, pp. 1865–1879, Apr. 2010.

[11] A. E. Gamal and E. van der Meulen, "A proof of Marton's coding theorem for the discrete memoryless channels," *IEEE Trans. Inf. Theory*, vol. 27, no. 1, pp. 120–122, Jul. 1980.

[12] 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, Jun. 2008.

[13] A. Dembo, Information inequalities and uncertainty principles. Stanford, CA, USA, Stanford Univ., Dept. Statist., 1990, 75.

[14] A. Dembo, T. M. Cover, and J. A. Thomas, "Information theoretic inequalities," *IEEE Trans. Inf. Theory*, vol. 37, no. 6, pp. 1501–1518, Nov. 1991.

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

Ersen Ekrem (S'08) received his Ph.D. degree from the department of electrical and computer engineering at the University of Maryland, College Park in August 2012. Prior to that, he received the B.S. and M.S. degrees in electrical and electronics engineering from Boğaziçi University,İstanbul, Turkey, in 2006 and 2007, respectively. Currently, he is with Qualcomm, Santa Clara.

He received the Distinguished Dissertation Fellowship from the ECE Department at the University of Maryland, College Park, in 2012. His research interests include information theory and wireless communications.

Sennur Ulukus (S'90–M'98) is a Professor of Electrical and Computer Engineering at the University of Maryland at College Park, where she also holds a joint appointment with the Institute for Systems Research (ISR). Prior to joining UMD, she was a Senior Technical Staff Member at AT&T Labs-Research. She received her Ph.D. degree in Electrical and Computer Engineering from Wireless Information Network Laboratory (WINLAB), Rutgers University, and B.S. and M.S. degrees in Electrical and Electronics Engineering from Bilkent University. Her research interests are in wireless communication theory and networking, network information theory for wireless communications, signal processing for wireless communications, information-theoretic physical-layer security, and energy-harvesting communications.

Dr. Ulukus received the 2003 IEEE Marconi Prize Paper Award in Wireless Communications, an 2005 NSF CAREER Award, the 2010–2011 ISR Outstanding Systems Engineering Faculty Award, and the 2012 George Corcoran Education Award. She served as an Associate Editor for the IEEE TRANSACTIONS ON INFORMATION THEORY (2007–2010) and IEEE TRANSACTIONS ON COMMUNICATIONS (2003–2007). She served as a Guest Editor for the *Journal of Communications and Networks* for the special issue on energy harvesting in wireless networks (2012), IEEE TRANSACTIONS ON INFORMATION THEORY for the special issue on interference networks (2011), IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS for the special issue on multiuser detection for advanced communication systems and networks (2008). She served as the TPC co-chair of the Communication Theory Symposium at 2013 IEEE ICC, Physical-Layer Security Workshop at 2011 IEEE Globecom, Physical-Layer Security Workshop at 2011 IEEE ICC, 2011 Communication Theory Workshop (IEEE CTW), Wireless Communications Symposium at 2010 IEEE ICC, Medium Access Control Track at 2008 IEEE WCNC, and Communication Theory Symposium at 2007 IEEE Globecom. She was the Secretary of the IEEE Communication Theory Technical Committee (CTTC) in 2007–2009.