Secure Broadcasting Using Multiple Antennas

Ersen Ekrem and Sennur Ulukus

(Invited Paper)

Abstract: **We consider three different secure broadcasting scenarios: i) Broadcast channels with common and confidential messages (BCC), ii) multi-receiver wiretap channels with public and confidential messages, and iii) compound wiretap channels. The BCC is a broadcast channel with two users, where in addition to the common message sent to both users, a private message, which needs to be kept hidden as much as possible from the other user, is sent to each user. In this model, each user treats the other user as an eavesdropper. The multi-receiver wiretap channel is a broadcast channel with two legitimate users and an external eavesdropper, where the transmitter sends a pair of public and confidential messages to each legitimate user. Although there is no secrecy concern about the public messages, the confidential messages need to be kept perfectly secret from the eavesdropper. The compound wiretap channel is a compound broadcast channel with a group of legitimate users and a group of eavesdroppers. In this model, the transmitter sends a common confidential message to the legitimate users, and this confidential message needs to be kept perfectly secret from all eavesdroppers. In this paper, we provide a survey of the existing information-theoretic results for these three forms of secure broadcasting problems, with a closer look at the Gaussian multiple-input multiple-output (MIMO) channel models. We also present the existing results for the more general discrete memoryless channel models, as they are often the first step in obtaining the capacity results for the corresponding Gaussian MIMO channel models.**

Index Terms: **Broadcast channels, information theoretic security, multiple antennas.**

I. INTRODUCTION

Information theoretic secrecy was initiated by Wyner in his landmark paper [1], where he introduced the wiretap channel which consists of a transmitter, a legitimate user and an eavesdropper. In the wiretap channel, the transmitter sends a message to the legitimate user, where this message needs to be kept hidden as much as possible from the eavesdropper. Wyner considers the degraded wiretap channel, where the eavesdropper's observation is degraded with respect to the legitimate user, and obtains the capacity-equivocation region of the degraded wiretap channel. Wyner's result is generalized by Csiszar-Korner [2] in two ways: i) Csiszar-Korner considers a general, *not necessarily degraded*, wiretap channel and ii) in their set-up, there is also a common message sent to both the legitimate user and the eavesdropper, in addition to the legitimate user's private message that needs to be kept hidden as much as possible from the eavesdropper. For this rather general scenario, Csiszar-Korner establishes the capacity-equivocation region.

Recently, information-theoretic secrecy has gathered a renewed interest, and the basic wiretap channel [1], [2] has been extended to various multi-user communication scenarios. The motivation of these works comes from wireless communications, where the inherent openness of the wireless medium lets each user have an overheard information on all ongoing communication sessions. This overheard information is the basis for both cooperation and loss of confidentiality. There have been many extensions of the basic wiretap channel to multi-user channels, such as multiple-access channels with confidential messages, interference channels with confidential messages, relay channels with confidential messages, etc. A tutorial on all these models can be found in [3]. Here, we focus on one of these multi-user scenarios: *Secure broadcasting*, and provide an in depth tutorial on its development, as well as the current state-of-the-art in this field.

In the secure broadcasting problem, generally speaking, there is a transmitter that broadcasts confidential information to many users while this communication is being eavesdropped. In this paper, we consider three different secure broadcasting problems. In other words, we consider three different channel models that capture different aspects of the secure broadcasting problem: i) Broadcast channel with common and confidential messages (BCC)[1], ii) multi-receiver wiretap channels, and iii) compound wiretap channels.

The BCC is a two-user broadcast channel where each user treats the other user as an eavesdropper. For this channel model, we consider the most general communication scenario where the transmitter sends a common message to both users as well as a private message to each user. In this scenario, the aim of the transmitter is to send the private message of each user while keeping the other user as ignorant of this message as possible. This scenario can be viewed as a symmetrized version of the wiretap channel [1], [2], where only one of the two users was modeled to receive a private message with a secrecy concern on it. We note that this scenario can be used to model the communication from a base station to the end-users in a cellular system, where each end-user treats the other end-users as potential eavesdroppers.

The multi-receiver wiretap channel is a broadcast channel with two legitimate users, and an external eavesdropper. For this channel model, we consider the most general communication scenario studied in the literature so far, where the transmitter sends a pair of public and confidential messages to each legiti-

Manuscript received September 21, 2010.

This work was supported by NSF grants CCF 04-47613, CCF 05-14846, CNS 07-16311, CCF 07-29127 and CCF 09-64645.

The authors are with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742, USA, email: {ersen, ulukus}@umd.edu.

[1] A survey for the BCC is also provided in [4]. After the publication of [4], many other results have appeared for the BCC, which are provided in this paper.

mate user. In this scenario, although there is no secrecy concern on the public messages, the confidential messages need to be kept perfectly secret from the eavesdropper. This scenario can be viewed as a generalization of the basic wiretap channel [1], [2] to a broadcast channel with multiple legitimate users. We also note that, similar to the previous channel model, this channel model can also be used to model the communication from a base station to the end-users in a cellular system, where now this communication needs to be kept secure from an external eavesdropper in the communication range.

The compound wiretap channel can be defined in two equivalent ways. In the first, classical, definition, there is a basic wiretap channel [1], [2] where the channel has a finite number of states determining the transition probability of the channel, and the transmitter does not know the realization of the channel state. The goal of the transmitter is to send a message to the legitimate user while keeping the eavesdropper totally ignorant of the message, irrespective of the channel state realization. Since each channel state yields a different wiretap channel, the compound wiretap channel can be viewed as a collection of many wiretap channels such that there is a group of legitimate users and a group of eavesdroppers in the channel, and the transmitter sends a common confidential message to all legitimate users while keeping all eavesdroppers ignorant of this message [5]. This interpretation corresponds to the second definition of the compound wiretap channel, and is the reason why we consider the compound wiretap channel as a form of secure broadcasting. This second definition reveals that the compound wiretap channel can be viewed as a generalization of the basic wiretap channel to the wiretap channel with many legitimate users and many eavesdroppers. We note that compound wiretap channel can be used to model the broadcast of a television station to the subscribed users aiming to keep the unsubscribed users ignorant of the content.

In this paper, we mainly consider the Gaussian multi-input multi-output (MIMO) models for these three scenarios. In each scenario, we start our discussion with the corresponding discrete memoryless channel model as it generally serves as an intermediate step in obtaining the result for the Gaussian MIMO channel model. In this paper, we give a special emphasis to the Gaussian MIMO channel model because of the enhanced secrecy that can be obtained by the use of multiple antennas. To provide an example to the fact that secrecy can be enhanced by the use of multiple antennas, let us consider the Gaussian broadcast channel with two users where each user treats the other one as an eavesdropper, i.e., as in the first secure broadcasting scenario discussed above. It is well-known that in this single-antenna system, both users cannot have secrecy simultaneously [6]. On the other hand, if the transmitter and the receivers are equipped with multiple antennas, both users can enjoy simultaneous secure communication [7]. Similar examples can be provided for the Gaussian multi-receiver wiretap channel [8], [9], and Gaussian compound wiretap channel [5].

II. CHANNEL MODELS

In this paper, we review the state-of-art for three secure broadcasting scenarios. In this section, we introduce the corresponding Gaussian MIMO channel models for these three problems. Since achievable schemes, outer bounds and capacity results for discrete memoryless channel models serve as intermediate steps to obtain achievable schemes, outer bounds and capacity results for Gaussian MIMO channel models, here we also introduce the corresponding discrete memoryless channel models for these three problems.

A. Broadcast Channels with Common and Confidential Messages

The BCC consists of a transmitter with an input $X \in \mathcal{X}$, and two receivers with observations $Y_1 \in \mathcal{Y}_1$ and $Y_2 \in \mathcal{Y}_2$. The channel is memoryless with a transition probability $p(y_1, y_2|x)$. The transmitter sends a common message to both users, and a private message to each user. In this channel, each user (receiver) treats the other one as an eavesdropper, and hence, wants its private message to be kept hidden as much as possible from the other user.

An $(n, 2^{nR_0}, 2^{nR_1}, 2^{nR_2})$ code for this channel consists of three message sets $\mathcal{W}_0 = \{1, \cdots, 2^{nR_0}\}, \mathcal{W}_1 = \{1, \cdots, 2^{nR_1}\}$, and $\mathcal{W}_2 = \{1, \cdots, 2^{nR_2}\}$, an encoder at the transmitter $f^n : \mathcal{W}_0 \times \mathcal{W}_1 \times \mathcal{W}_2 \to \mathcal{X}^n$, and two decoders $g_j^n : \mathcal{Y}_j^n \to \mathcal{W}_0 \times \mathcal{W}_j$, one at each receiver. The probability of error is defined as $P_e^n = \max\{P_{e1}^n, P_{e2}^n\}$, where $P_{ej}^n = \Pr[g_j^n(Y_j^n) \neq (W_0, W_j)]$, and W_0, W_1, and W_2 are uniformly distributed random variables in $\mathcal{W}_0, \mathcal{W}_1$, and $\mathcal{W}_2$, respectively. The secrecy of each user's private message is measured by its equivocation at the other user[2]

$$\frac{1}{n}H(W_1|W_0, W_2, Y_2^n) \quad \text{and} \quad \frac{1}{n}H(W_2|W_0, W_1, Y_1^n). \tag{1}$$

A rate tuple $(R_0, R_1, R_2, R_{e1}, R_{e2})$ is said to be achievable if there exists an $(n, 2^{nR_0}, 2^{nR_1}, 2^{nR_2})$ code which satisfies $\lim_{n\to\infty} P_e^n = 0$ and

$$R_{e1} \leq \lim_{n\to\infty} \frac{1}{n}H(W_1|W_0, W_2, Y_2^n), \tag{2}$$

$$R_{e2} \leq \lim_{n\to\infty} \frac{1}{n}H(W_2|W_0, W_1, Y_1^n). \tag{3}$$

The capacity-equivocation region of the BCC is defined as the closure of all achievable rate tuples $(R_0, R_1, R_2, R_{e1}, R_{e2})$. The capacity-equivocation region of the BCC is a five-dimensional region which contains many sub-regions. From a secrecy point of view, one important sub-region that the capacity-equivocation region of the BCC contains is the secrecy capacity region which contains all rate tuples of the form $(R_0, R_1, R_2, R_{e1} = R_1, R_{e2} = R_2)$ in the capacity-equivocation region of the BCC. Hence, the secrecy capacity region is a three dimensional region that contains rate triples (R_0, R_1, R_2) for which the private messages are transmitted in perfect secrecy, i.e., $R_{e1} = R_1$ and $R_{e2} = R_2$[3]. Moreover, we note that in view of (2)–(3),

[2]Equivalently, equivocation can be defined as

$$\frac{1}{n}H(W_1|Y_2^n) \quad \text{and} \quad \frac{1}{n}H(W_2|Y_1^n)$$

since the first user decodes W_0, W_1, and the second user decodes W_0, W_2.

[3]Whenever a private message is transmitted in perfect secrecy, i.e., $R_{ej} = R_j$, we call the private message *confidential* message.

the perfect secrecy requirement $R_{e1} = R_1$ and $R_{e2} = R_2$ can be expressed as

$$\lim_{n\to\infty} \frac{1}{n} I(W_1; W_0, W_2, Y_2^n) = 0, \tag{4}$$

$$\lim_{n\to\infty} \frac{1}{n} I(W_2; W_0, W_1, Y_1^n) = 0. \tag{5}$$

Another important point in the capacity-equivocation region of the BCC is the secrecy capacity of each user which is the maximum private message rate of a user such that the private message can be transmitted in perfect secrecy.

Now, we introduce a class of broadcast channels which satisfy the following Markov chain

$$X \to Y_1 \to Y_2. \tag{6}$$

A broadcast channel satisfying the Markov chain in (6) is called a *degraded* broadcast channel.

Next, we introduce the Gaussian MIMO BCC which is defined by

$$\mathbf{Y}_1 = \mathbf{H}_1\mathbf{X} + \mathbf{N}_1, \tag{7}$$

$$\mathbf{Y}_2 = \mathbf{H}_2\mathbf{X} + \mathbf{N}_2 \tag{8}$$

where the $t \times 1$ vector $\mathbf{X}$ denotes the channel input, the $r_j \times t$ matrix $\mathbf{H}_j$ is the channel gain matrix of the jth user, and $\mathbf{N}_j$ is the Gaussian noise with zero-mean and identity covariance matrix at the jth user's receiver. The channel input is subject to the following covariance constraint

$$E\left[\mathbf{X}\mathbf{X}^\top\right] \preceq \mathbf{S} \tag{9}$$

where $\mathbf{S}$ is a strictly positive definite matrix.

B. Multi-Receiver Wiretap Channels

The multi-receiver wiretap is a broadcast channel with $K+1$ receivers where there are K legitimate users receiving confidential messages, and an eavesdropper which is listening to the communication between the transmitter and the legitimate users. For the sake of simplicity, we set $K = 2$ here[4]. Thus, the multi-receiver channel under consideration consists of one transmitter with input alphabet $\mathcal{X}$, two legitimate users with output alphabets $\mathcal{Y}_1$ and $\mathcal{Y}_2$, and an eavesdropper with output alphabet $\mathcal{Z}$. 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 $Y_1 \in \mathcal{Y}_1, Y_2 \in \mathcal{Y}_2$, and $Z \in \mathcal{Z}$ denote the channel output 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[5]. While there are no secrecy constraints on the public messages, we require the confidential messages to be transmitted in perfect secrecy. We call the channel model arising from this scenario the multi-receiver wiretap channel 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 $\mathcal{W}_{p1} = \{1, \cdots, 2^{nR_{p1}}\}, \mathcal{W}_{s1} = \{1, \cdots, 2^{nR_{s1}}\}, \mathcal{W}_{p2} = \{1, \cdots, 2^{nR_{p2}}\}$, and $\mathcal{W}_{s2} = \{1, \cdots, 2^{nR_{s2}}\}$, one encoder at the transmitter $f^n : \mathcal{W}_{p1} \times \mathcal{W}_{s1} \times \mathcal{W}_{p2} \times \mathcal{W}_{s2} \to \mathcal{X}^n$, and one decoder at each legitimate user $g_j^n : \mathcal{Y}_j^n \to \mathcal{W}_{pj} \times \mathcal{W}_{sj}$. The probability of error is defined as $P_e^n = \max\{P_{e1}^n, P_{e2}^n\}$, where $P_{ej}^n = \Pr[g_j^n(Y_j^n) \neq (W_{pj}, W_{sj})]$ and W_{p1}, W_{s1}, W_{p2}, and W_{s2} are uniformly distributed random variables in $\mathcal{W}_{p1}, \mathcal{W}_{s1}, \mathcal{W}_{p2}$, and $\mathcal{W}_{s2}$, 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 $\lim_{n\to\infty} P_e^n = 0$ and

$$\lim_{n\to\infty} \frac{1}{n} I(W_{s1}, W_{s2}; Z^n) = 0. \tag{10}$$

We note that the perfect secrecy requirement in (10) implies the following two conditions

$$\lim_{n\to\infty} \frac{1}{n} I(W_{s1}; Z^n) = 0 \quad \text{and} \quad \lim_{n\to\infty} \frac{1}{n} I(W_{s2}; Z^n) = 0. \tag{11}$$

The capacity region of the multi-receiver wiretap channel with public and confidential messages is defined as the convex closure of all achievable rate tuples $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$. From a secrecy point of view, one important sub-region that the capacity region of the multi-receiver wiretap channel includes is the secrecy capacity region which contains all rate tuples of the form $(R_{p1} = 0, R_{s1}, R_{p2} = 0, R_{s2})$ in the capacity region of the multi-receiver wiretap channel. Thus, the secrecy capacity region of the multi-receiver wiretap channel corresponds to the scenario where there are only two confidential messages, one for each legitimate user, i.e., there are no public messages, and these confidential messages need to be kept perfectly secret from the eavesdropper.

Now, we introduce a class of multi-receiver wiretap channels which satisfy the following Markov chain

$$X \to Y_1 \to Y_2 \to Z. \tag{12}$$

A multi-receiver wiretap channel satisfying the Markov chain in (12) is called a *degraded* multi-receiver wiretap channel.

Next, we introduce the Gaussian MIMO multi-receiver wiretap channel which is defined by

$$\mathbf{Y}_1 = \mathbf{H}_1\mathbf{X} + \mathbf{N}_1, \tag{13}$$

$$\mathbf{Y}_2 = \mathbf{H}_2\mathbf{X} + \mathbf{N}_2, \tag{14}$$

$$\mathbf{Z} = \mathbf{H}_Z\mathbf{X} + \mathbf{N}_Z \tag{15}$$

where the $t \times 1$ vector $\mathbf{X}$ denotes the channel input, the $r_j \times t$ matrix $\mathbf{H}_j$ is the channel gain matrix of the jth user, the $r_Z \times t$ matrix $\mathbf{H}_Z$ is the channel gain matrix of the eavesdropper, and $\{\mathbf{N}_j\}_{j=1}^2$ and $\mathbf{N}_Z$ are the Gaussian noise vectors with zero-mean and identity covariance matrices at the legitimate users'

[4]When necessary, we will give references to papers where $K > 2$ was considered.

[5]We note that this scenario is not the most general one that can be studied for the multi-receiver wiretap channel. For example, in addition to the public and confidential messages involved in this scenario, there might be a common message sent to both the eavesdropper and the legitimate users. Inclusion of this common message would yield a more general scenario than the one considered here. However, the scenario considered here is the most general scenario studied so far.

and the eavesdropper's receivers, respectively. The channel input is subject to the following covariance constraint

$$E\left[\mathbf{X}\mathbf{X}^{\top}\right] \preceq \mathbf{S} \tag{16}$$

where $\mathbf{S}$ is a strictly positive definite matrix.

Finally, we conclude this section by the definition of the degraded Gaussian MIMO multi-receiver wiretap channel. In view of the definition of the degraded discrete memoryless multi-receiver wiretap channel and the Markov chain in (12), a Gaussian MIMO multi-receiver wiretap channel is said to be degraded if it satisfies the following Markov chain

$$\mathbf{X} \to \mathbf{Y}_1 \to \mathbf{Y}_2 \to \mathbf{Z}. \tag{17}$$

Equivalently, the degradedness of a Gaussian MIMO multi-receiver wiretap channel can be defined as follows: A Gaussian MIMO multi-receiver wiretap channel is degraded if there exist two matrices $\mathbf{D}_{12}$ and $\mathbf{D}_{2Z}$ which satisfy the following conditions.

i) $\mathbf{H}_2 = \mathbf{D}_{12}\mathbf{H}_1$ and $\mathbf{H}_Z = \mathbf{D}_{2Z}\mathbf{H}_2$.

ii) $\mathbf{D}_{12}\mathbf{D}_{12}^{\top} \preceq \mathbf{I}$ and $\mathbf{D}_{2Z}\mathbf{D}_{2Z}^{\top} \preceq \mathbf{I}$.

C. Compound Wiretap Channels

The compound wiretap channel consists of a legitimate user and an eavesdropper. In compound wiretap channels, there are a finite number of channel states determining the channel transition probability. The channel takes a certain fixed state for the entire duration of the transmission, and the transmitter does not have any knowledge about the channel state realization, whereas both the legitimate user and the eavesdropper know the realization of the channel state. Thus, the aim of the transmitter is to ensure both the reliability and the secrecy of messages irrespective of the channel state realization. In addition to this definition, the compound wiretap channel admits another interpretation. Consider the multi-receiver wiretap channel with several legitimate users and many eavesdroppers, where the transmitter wants to transmit a common confidential message to legitimate users while keeping all of the eavesdroppers totally ignorant of the message. Since each eavesdropper and legitimate user pair can be regarded as a different channel state realization, this channel is equivalent to a compound wiretap channel. Therefore, one can interpret a compound wiretap channel as *multicasting* a common confidential message to several legitimate receivers in the presence of one or more eavesdroppers [5]. Due to this interpretation, we treat the compound wiretap channel as a form of secure broadcasting.

The discrete memoryless compound wiretap channel consists of a transmitter with input alphabet $\mathcal{X}$, K_Y legitimate users with output alphabets $\mathcal{Y}_j$, and K_Z eavesdroppers with output alphabets $\mathcal{Z}_k$. The channel is memoryless with a transition probability $p(y_1, \cdots, y_{K_Y}, z_1, \cdots, z_{K_Z}|x)$ where $x \in \mathcal{X}$ is the channel input, $y_j \in \mathcal{Y}_j$ is the jth legitimate user's output, and $z_k \in \mathcal{Z}_k$ is the kth eavesdropper's channel output. We consider the scenario where the transmitter sends a common confidential message to K_Y legitimate users, and this common confidential message needs to be kept perfectly secret from K_Z eavesdroppers.

An $(n, 2^{nR})$ code for the compound wiretap channel consists of a message set $\mathcal{W} = \{1, \cdots, 2^{nR}\}$, an encoder at the transmitter $f^n : \mathcal{W} \to \mathcal{X}^n$, and one decoder at each legitimate user $g_j^n : \mathcal{Y}_j^n \to \mathcal{W}$. The probability of error is defined as $P_e^n = \max_{j=1,\cdots,K_Y} P_{ej}^n$, where $P_{ej}^n = \Pr\left[g_j^n(Y_j^n) \neq W\right]$, and W is a uniformly distributed random variable in $\mathcal{W}$. A secrecy rate R is said to be achievable if there exists an $(n, 2^{nR})$ code which satisfies $\lim_{n\to\infty} P_e^n = 0$ and

$$\lim_{n\to\infty} \frac{1}{n} I(W; Z_k^n) = 0, \quad k = 1, \cdots, K_Z. \tag{18}$$

The maximum of all achievable secrecy rates for a compound wiretap channel is called the secrecy capacity.

Now, we define a class of compound wiretap channels called the *degraded* compound wiretap channel which satisfies the following Markov chain

$$X \to Y_j \to Z_k \tag{19}$$

for any (j, k) pair.

Next, we introduce the Gaussian MIMO compound wiretap channel which is defined by

$$\mathbf{Y}_j = \mathbf{H}_j^Y \mathbf{X} + \mathbf{N}_j^Y, \tag{20}$$

$$\mathbf{Z}_k = \mathbf{H}_k^Z \mathbf{X} + \mathbf{N}_k^Z \tag{21}$$

where the $t \times 1$ vector $\mathbf{X}$ denotes the channel input, the $r_j^Y \times t$ matrix $\mathbf{H}_j^Y$ is the channel gain matrix of the jth legitimate user, the $r_k^Z \times t$ matrix $\mathbf{H}_k^Z$ is the channel gain matrix of the kth eavesdropper, and $\mathbf{N}_j^Y$ and $\mathbf{N}_k^Z$ are the Gaussian noise vectors with zero-mean and identity covariance matrices at the jth legitimate user's and the kth eavesdropper's receivers, respectively. The channel input is subject to the following covariance constraint

$$E\left[\mathbf{X}\mathbf{X}^{\top}\right] \preceq \mathbf{S} \tag{22}$$

where $\mathbf{S}$ is a strictly positive definite matrix.

Now, we define the *degraded* Gaussian MIMO compound wiretap channel. In view of the definition of the degraded discrete memoryless compound wiretap channel and the Markov chain in (19), a Gaussian MIMO compound wiretap channel is said to be degraded if it satisfies the following Markov chain

$$\mathbf{X} \to \mathbf{Y}_j \to \mathbf{Z}_k \tag{23}$$

for any (j, k) pair. Equivalently, the degradedness of a Gaussian MIMO compound wiretap channel can be defined as follows: A Gaussian MIMO compound wiretap channel is degraded if, for any (j, k) pair, there exists a matrix $\mathbf{D}_{jk}$ satisfying $\mathbf{D}_{jk}\mathbf{H}_j^Y = \mathbf{H}_k^Z$ and $\mathbf{D}_{jk}\mathbf{D}_{jk}^{\top} \preceq \mathbf{I}$.

D. Comments on Gaussian MIMO Channels

We provide some comments about the way we define Gaussian MIMO channel models. The first one is about the fact that we use the covariance constraint $E\left[\mathbf{X}\mathbf{X}^{\top}\right] \preceq \mathbf{S}$ instead of the more common total power constraint $\mathrm{tr}\left(E\left[\mathbf{X}\mathbf{X}^{\top}\right]\right) \leq P$. We note that the covariance constraint is more general and it subsumes the total power constraint as a special case [10]. In particular, any result for the covariance constraint can be used to obtain the corresponding result for the total power constraint.

For example, if we denote a capacity region that arises from the use of a covariance constraint by $C(\mathbf{S})$, the capacity region arising from the use of a total power constraint $C^{\text{tot}-\text{pow}}(P)$ can be obtained as [10]

$$C^{\text{tot}-\text{pow}}(P) = \bigcup_{\mathbf{S}:\text{tr}(\mathbf{S})\leq P} C(\mathbf{S}). \tag{24}$$

If $C(\mathbf{S})$ is the capacity arising from the use of a covariance constraint, the capacity arising from the use of a total power constraint is given by

$$C^{\text{tot}-\text{pow}}(P) = \max_{\mathbf{S}:\text{tr}(\mathbf{S})\leq P} C(\mathbf{S}). \tag{25}$$

The conversion of any inner or outer bound obtained for a covariance constraint to the corresponding inner and outer bound for a total power constraint can be accomplished by using relations similar to the ones given in (24) and (25).

The second comment is about our assumption that $\mathbf{S}$ is strictly positive definite. This assumption does not lead to any loss of generality because for any Gaussian MIMO channel model with a positive semi-definite covariance constraint, i.e., $\mathbf{S} \succeq \mathbf{0}$ and $|\mathbf{S}| = 0$, we can always construct an equivalent channel with the constraint $E\left[\mathbf{X}\mathbf{X}^{\top}\right] \preceq \mathbf{S}'$ where $\mathbf{S}' \succ \mathbf{0}$ (see Lemma 2 of [10]).

III. BROADCAST CHANNELS WITH COMMON AND CONFIDENTIAL MESSAGES

First, we review the results for the capacity-equivocation region of the discrete memoryless BCC, and next present the results for the Gaussian MIMO BCC. We start with the best known inner bound for the capacity-equivocation region of the BCC, i.e., the largest achievable region. This achievable region is given by the following theorem.

Theorem 1 ([11], [12]) Rate tuples $(R_0, R_1, R_2, R_{e1}, R_{e2})$ satisfying

$$R_0 \leq \min\{I(U;Y_1), I(U;Y_2)\}, \tag{26}$$

$$R_0 + R_1 \leq \min\{I(U;Y_1), I(U;Y_2)\} + I(V_1;Y_1|U), \tag{27}$$

$$R_0 + R_2 \leq \min\{I(U;Y_1), I(U;Y_2)\} + I(V_2;Y_2|U), \tag{28}$$

$$\begin{aligned} R_0 + R_1 + R_2 \leq{}& \min\{I(U;Y_1), I(U;Y_2)\} + I(V_1;Y_1|U) \\ &+ I(V_2;Y_2|U) - I(V_1;V_2|U), \end{aligned} \tag{29}$$

$$R_{e1} \leq [I(V_1;Y_1|U) - I(V_1;Y_2,V_2|U)]^+, \tag{30}$$

$$R_{e2} \leq [I(V_2;Y_2|U) - I(V_2;Y_1,V_1|U)]^+, \tag{31}$$

$$R_{e1} \leq R_1, \tag{32}$$

$$R_{e2} \leq R_2 \tag{33}$$

for some $(U, V_1, V_2) \rightarrow X \rightarrow (Y_1, Y_2)$ are achievable.

This achievable rate region can viewed as a generalization of Marton's inner bound [13] for broadcast channels to the secrecy context. Similar to Marton's inner bound for broadcast channels, in Theorem 1, U denotes the common message intended to both receivers as well as the parts of the private messages through rate-splitting, i.e., each private message can be divided into two parts, and one of these two parts can be sent together with the common message by using U. Since U denotes the information that is decoded by both users, the parts of the private messages carried by U cannot have any confidentiality. In Theorem 1, V_1 and V_2 represent the private messages, or parts of the private messages if rate-splitting is used, of the first and second user, respectively. Besides rate-splitting, this achievable scheme uses superposition coding and random binning. U and (V_1, V_2) correspond to the two layers of the superposition coding. To encode the private messages into V_1 and V_2, random binning is used. The difference of the achievable scheme in Theorem 1 from Marton's inner bound comes from the equivocation computation which necessitates one more random binning on top of the already present random binning in Marton's achievable scheme. Thus, the achievable scheme in Theorem 1 uses double binning. In Marton's achievable scheme, random binning is used to ensure the joint typicality of the codewords generated through V_1 and V_2. On the other hand, the additional binning used for the achievable scheme in Theorem 1 provides the necessary randomness and protection to achieve equivocation.

In general, it is unknown whether the achievable rate region in Theorem 1 is equal to the capacity-equivocation region of the BCC. However, the partial tightness of this achievable region has been shown, i.e., if certain rates are set to zero, this inner bound matches the capacity-equivocation region of the BCC. Since our main emphasis is on secrecy in this paper, we review only the relevant secrecy literature. In the secrecy context, the partial tightness of the region in Theorem 1 has been shown by Wyner for the first time [1]. Wyner studied the *degraded* broadcast channel for the scenario where there is no common message, and no private message for the second user. Hence, the second user acts as a pure eavesdropper, i.e., no information is sent to the second user. Thus, in this scenario, there is only one private message sent to the first user and this message needs to be kept hidden as much as possible from the second user (eavesdropper), i.e., the scenario studied by Wyner can be obtained from the general scenario introduced for the BCC in subsection II-A by setting $R_0 = R_2 = R_{e2} = 0$. The capacity-equivocation region for this scenario is given by the following theorem.

Theorem 2 ([1]) The capacity-equivocation region of the degraded broadcast channel with only one private message is given by the union of rate pairs (R_1, R_{e1}) satisfying

$$R_1 \leq I(X;Y_1), \tag{34}$$

$$R_{e1} \leq I(X;Y_1) - I(X;Y_2), \tag{35}$$

$$R_{e1} \leq R_1 \tag{36}$$

where $X \rightarrow Y_1 \rightarrow Y_2$.

We note that the capacity-equivocation region in Theorem 2 can be obtained by setting $U = V_2 = \phi$ and $V_1 = X$ in the achievable region in Theorem 1, hence the achievable region in Theorem 1 is tight for this case. From Theorem 2, by setting $R_{e1} = R_1$, we can obtain the secrecy capacity of a degraded wiretap channel as follows.

Corollary 1 ([1]) The secrecy capacity of a degraded wiretap

channel is given by

$$\max_X I(X;Y_1) - I(X;Y_2) \tag{37}$$

where $X \to Y_1 \to Y_2$.

Wyner's result is generalized by Csiszar-Korner [2] in two ways: i) They consider a general, i.e., *not necessarily degraded*, broadcast channel and ii) their scenario includes a common message intended to both the first user and the second user (eavesdropper) in addition to the private message for the first user. Thus, their scenario can be obtained from the general scenario introduced for the BCC in subsection II-A by setting $R_2 = R_{e2} = 0$. The capacity-equivocation region for this scenario is given by the following theorem.

Theorem 3 ([2]) The capacity-equivocation region of the broadcast channel with common and only one private message is given by the union of rate tuples (R_0, R_1, R_{e1}) satisfying

$$R_0 \le \min\{I(U;Y_1), I(U;Y_2)\}, \tag{38}$$
$$R_0 + R_1 \le \min\{I(U;Y_1), I(U;Y_2)\} + I(V;Y_1|U), \tag{39}$$
$$R_{e1} \le [I(V;Y_1|U) - I(V;Y_2|U)]^+, \tag{40}$$
$$R_{e1} \le R_1 \tag{41}$$

where $U \to V \to X \to Y_1 \to Y_2$.

We note that the capacity-equivocation region in Theorem 3 can be obtained from the achievable region in Theorem 1 by setting $V_2 = \phi$ and $V_1 = V$. Hence, the achievable scheme in Theorem 1 is tight for this scenario as well.

Since the proof of Theorem 3 provides many new tools which proved to be very useful for many subsequent secrecy problems, now we provide some more detail about the proof of Theorem 3. The achievability proof of the capacity result in Theorem 3 brought the concept of channel pre-fixing. In particular, in the achievability proof of Theorem 3, [2] first shows the achievability of the region that consists of rate triples (R_0, R_1, R_{e1}) satisfying

$$R_0 \le \min\{I(U;Y_1), I(U;Y_2)\}, \tag{42}$$
$$R_0 + R_1 \le \min\{I(U;Y_1), I(U;Y_2)\} + I(X;Y_1|U), \tag{43}$$
$$R_{e1} \le [I(X;Y_1|U) - I(X;Y_2|U)]^+, \tag{44}$$
$$R_{e1} \le R_1 \tag{45}$$

where $U \to X \to Y_1, Y_2$. Next, they consider a new channel, i.e., stochastic mapping, with transition probability $p(x|v)$ which is used to pre-fix the original channel $p(y_1, y_2|x)$ yielding a new equivalent channel $p(y_1, y_2|v)$. We note that any coding scheme for the new equivalent channel can be transformed into a coding scheme for the original channel because the encoder for the new channel f' can be transformed into the encoder f for the original channel by multiplying f' with $p(x|v)$, and the stochastic connection between the messages and the received sequences would be the same in both cases, i.e., the decoder for the new channel works for the original channel as well. In light of these facts, the achievability of the region in (42)–(45) implies the achievability of the region in Theorem 3. We note that although one reduces the rate transmitted to the first user by replacing X with V, i.e., by using channel pre-fixing, because the rate goes down from $I(X;Y_1|U)$ to $I(V;Y_1|U)$, channel pre-fixing reduces the rate eavesdropped by the second user as well. Thus, if channel pre-fixing reduces the rate going to the eavesdropper more than the rate transmitted to the first user, the equivocation can be improved. Hence, the main idea of channel pre-fixing is to introduce more randomness to the channel which might improve the confidentiality of the private message by harming the eavesdropper more than harming the first user.

Similar to the achievability proof of Theorem 3, the converse proof in [2] also provides new tools. In particular, the construction of the auxiliary random variables U and V, and the bounding technique for the equivocation proved to be very useful for many subsequent secrecy problems. Indeed, both of these contributions are inspired by the Csiszar-Korner sum identity, which is introduced in [2] as well. The Csiszar-Korner sum identity is given as follows.

Lemma 1 ([2]) Let T be an arbitrary random variable, and Y_1^n, Y_2^n be two length-n random vectors. We have

$$\sum_{i=1}^n I(Y_{2(i+1)}^n; Y_{1i}|T, Y_1^{i-1}) = \sum_{i=1}^n I(Y_1^{i-1}; Y_{2i}|T, Y_{2(i+1)}^n). \tag{46}$$

In the converse proof of Theorem 3, by using Lemma 1, [2] has showed that

$$nR_{e1} \le \sum_{i=1}^n I(W_1; Y_{1i}|W_0, Y_1^{i-1}, Y_{2(i+1)}^n) - I(W_1; Y_{2i}|W_0, Y_1^{i-1}, Y_{2(i+1)}^n) + n\epsilon_n \tag{47}$$

where $\epsilon_n \to 0$ as $n \to \infty$. In view of (47), [2] has identified the auxiliary random variables U_i and V_i as $U_i = (W_0, Y_1^{i-1}, Y_{2(i+1)}^n)$ and $V_i = (W_1, U_i)$. Once the equivocation is bounded as in (47) and the auxiliary random variables are identified, the bounds on R_0 and R_1 can be obtained in a rather straightforward way. Thus, the Csiszar-Korner sum identity in Lemma 1 can be viewed as the most important instrument to obtain the converse proof for Theorem 3.

We note an interesting point about Theorem 3, by focusing on the scenario where the transmitter sends only a private message to the first user and this message needs to be kept hidden as much as possible from the second user (eavesdropper). Hence, this scenario can be obtained from the general scenario introduced for the BCC in subsection II-A by setting $R_0 = R_2 = R_{e2} = 0$. Moreover, this scenario can be viewed as the generalization of Wyner's scenario from the degraded broadcast channel to the general, not necessarily degraded, broadcast channel. The corresponding capacity-equivocation region is given as follows.

Theorem 4 ([2]) The capacity-equivocation region of the broadcast channel with only one private message is given by the union of rate pairs (R_1, R_{e1}) satisfying

$$R_1 \le I(V;Y_1), \tag{48}$$
$$R_{e1} \le I(V;Y_1|U) - I(V;Y_2|U) \tag{49}$$

where $U \to V \to X \to Y_1, Y_2$.

The interesting point revealed by Theorem 4 is that although there is only one message to be transmitted, we need

rate-splitting and superposition coding to achieve the capacity-equivocation region. In particular, this single message needs to be divided into two parts, where the first part is mapped to codewords generated by U and the second part is superimposed on the first one and mapped to the codewords generated by V. Moreover, as (49) suggests, the first part of the private message sent with U does not contribute to the equivocation. Indeed, it can be shown that this first part of the private message is decoded by the second user (eavesdropper) as well. We also note that, as Theorem 2 shows, if the broadcast channel is degraded, there is no need for rate-splitting or superposition coding to attain the capacity-equivocation region of the broadcast channel with only one private message.

Finally, we conclude our discussion about the discrete memoryless BCC by obtaining the secrecy capacity in a general, not necessarily degraded, broadcast channel. By setting $R_{e1} = R_1$ in Theorem 4, we can obtain the secrecy capacity as follows.

$$\max_{U,V\to X\to Y_j} I(V;Y_1|U) - I(V;Y_2|U)$$

$$= \max_{U,V\to X\to Y_j} \sum_{u\in\mathcal{U}} p(u)\Big[I(V;Y_1|U=u) - I(V;Y_2|U=u)\Big] \tag{50}$$

$$\leq \max_{U,V\to X\to Y_j} \sum_{u\in\mathcal{U}} p(u) \max_{u\in\mathcal{U}} \Big[I(V;Y_1|U=u) - I(V;Y_2|U=u)\Big] \tag{51}$$

$$= \max_{V\to X\to Y_j} \max_{u\in\mathcal{U}} \Big[I(V;Y_1|U=u) - I(V;Y_2|U=u)\Big] \tag{52}$$

$$= \max_{V\to X\to Y_j} I(V;Y_1) - I(V;Y_2). \tag{53}$$

This result is formally stated in the following corollary.

Corollary 2 ([2]) The secrecy capacity of a general, not necessarily degraded, wiretap channel is given by

$$\max_{V,X} I(V;Y_1) - I(V;Y_2) \tag{54}$$

where $V \to X \to Y_1, Y_2$.

This corollary states that as opposed to the degraded wiretap channel, to achieve the secrecy capacity of a general, *not necessarily degraded*, wiretap channel, channel pre-fixing might be necessary. In other words, although, in view of Corollary 1, $V = X$ achieves the secrecy capacity of a degraded wiretap channel, $V = X$ might be sub-optimal in a general, not necessarily degraded, wiretap channel.

A. Gaussian MIMO BCC

In this section, we review the results for the capacity-equivocation region of the Gaussian MIMO BCC. First, we present an achievable rate region which can be obtained by evaluating the region in Theorem 1 by using certain selections for the auxiliary random variables U, V_1, and V_2 in Theorem 1. In particular, the following achievable rate region corresponds to a jointly Gaussian selection of U, V_1, and V_2 with a certain correlation structure.

Theorem 5: An achievable region for the Gaussian MIMO BCC is given by

$$\text{conv}\left(\mathcal{R}_{12}\bigcup\mathcal{R}_{21}\right) \tag{55}$$

where $\mathcal{R}_{12}$ consists of the rate tuples satisfying

$$R_0 = \min_{j=1,2}\frac{1}{2}\log\frac{|\mathbf{H}_j\mathbf{S}\mathbf{H}_j^\top+\mathbf{I}|}{|\mathbf{H}_j(\mathbf{K}_1+\mathbf{K}_2)\mathbf{H}_j^\top+\mathbf{I}|}, \tag{56}$$

$$R_1 = \frac{1}{2}\log\frac{|\mathbf{H}_1(\mathbf{K}_1+\mathbf{K}_2)\mathbf{H}_1^\top+\mathbf{I}|}{|\mathbf{H}_1\mathbf{K}_2\mathbf{H}_1^\top+\mathbf{I})|}, \tag{57}$$

$$R_2 = \frac{1}{2}\log|\mathbf{H}_2\mathbf{K}_2\mathbf{H}_2^\top+\mathbf{I}|, \tag{58}$$

$$R_{e1} = \frac{1}{2}\log\frac{|\mathbf{H}_1(\mathbf{K}_1+\mathbf{K}_2)\mathbf{H}_1^\top+\mathbf{I}|}{|\mathbf{H}_1\mathbf{K}_2\mathbf{H}_1^\top+\mathbf{I}|} - \frac{1}{2}\log\frac{|\mathbf{H}_2(\mathbf{K}_1+\mathbf{K}_2)\mathbf{H}_2^\top+\mathbf{I}|}{|\mathbf{H}_2\mathbf{K}_2\mathbf{H}_2^\top+\mathbf{I}|}, \tag{59}$$

$$R_{e2} = \frac{1}{2}\log|\mathbf{H}_2\mathbf{K}_2\mathbf{H}_2^\top+\mathbf{I}| - \frac{1}{2}\log|\mathbf{H}_1\mathbf{K}_2\mathbf{H}_1^\top+\mathbf{I}| \tag{60}$$

for some positive semi-definite matrices $\mathbf{K}_1$ and $\mathbf{K}_2$ such that $\mathbf{K}_1+\mathbf{K}_2 \preceq \mathbf{S}$, and $\mathcal{R}_{21}$ can be obtained from $\mathcal{R}_{12}$ by swapping the indices 1 and 2.

Theorem 5 states that the common message, for which a covariance matrix $\mathbf{S}-\mathbf{K}_1-\mathbf{K}_2$ is allotted, should be encoded by using a standard Gaussian codebook generated by using U, and the private messages, for which covariance matrices $\mathbf{K}_1$ and $\mathbf{K}_2$ are allotted, need to be encoded by using dirty-paper coding (DPC) [14]. The codewords for the private messages need to be generated by using V_1 and V_2. The receivers first decode the common message by treating the private messages as noise, and then each receiver decodes the private message intended for itself. Depending on the encoding order used in DPC, one of the users gets a clean link for the transmission of its private message, where there is no interference originating from the other user's private message.

Next, we note that the inner bound in Theorem 6 can potentially be improved by using the following observation: If $(R_0, R_1, R_2, R_{e1}, R_{e2})$ is an achievable rate tuple, the rate tuple $(R_0-\alpha-\beta, R_1+\alpha, R_2+\beta, R_{e1}, R_{e2})$ is also achievable for any α,β satisfying $0\leq\alpha, 0\leq\beta, \alpha+\beta\leq R_0$. In other words, since the common message is decoded by both users, its rate can be given up in the favor of the rates of the private messages without changing the equivocations. Using this observation and Theorem 6, the achievability of the following region can be shown.

Theorem 6: An achievable region for the Gaussian MIMO BCC is given by

$$\text{conv}\left(\mathcal{R}_{12}\bigcup\mathcal{R}_{21}\right) \tag{61}$$

where $\mathcal{R}_{12}$ consists of the rate tuples satisfying

$$R_0 \leq \min_{j=1,2}\frac{1}{2}\log\frac{|\mathbf{H}_j\mathbf{S}\mathbf{H}_j^\top+\mathbf{I}|}{|\mathbf{H}_j(\mathbf{K}_1+\mathbf{K}_2)\mathbf{H}_j^\top+\mathbf{I}|}, \tag{62}$$

$$R_0+R_1 \leq \min_{j=1,2}\frac{1}{2}\log\frac{|\mathbf{H}_j\mathbf{S}\mathbf{H}_j^\top+\mathbf{I}|}{|\mathbf{H}_j(\mathbf{K}_1+\mathbf{K}_2)\mathbf{H}_j^\top+\mathbf{I}|}$$

$$+\frac{1}{2}\log\frac{|\mathbf{H}_1(\mathbf{K}_1+\mathbf{K}_2)\mathbf{H}_1^\top+\mathbf{I}|}{|\mathbf{H}_1\mathbf{K}_2\mathbf{H}_1^\top+\mathbf{I})|}, \tag{63}$$

$$R_0+R_2\le\min_{j=1,2}\frac{1}{2}\log\frac{|\mathbf{H}_j\mathbf{S}\mathbf{H}_j^\top+\mathbf{I}|}{|\mathbf{H}_j(\mathbf{K}_1+\mathbf{K}_2)\mathbf{H}_j^\top+\mathbf{I}|}+\frac{1}{2}\log|\mathbf{H}_2\mathbf{K}_2\mathbf{H}_2^\top+\mathbf{I}|, \tag{64}$$

$$R_0+R_1+R_2\le\min_{j=1,2}\frac{1}{2}\log\frac{|\mathbf{H}_j\mathbf{S}\mathbf{H}_j^\top+\mathbf{I}|}{|\mathbf{H}_j(\mathbf{K}_1+\mathbf{K}_2)\mathbf{H}_j^\top+\mathbf{I}|}+\frac{1}{2}\log\frac{|\mathbf{H}_1(\mathbf{K}_1+\mathbf{K}_2)\mathbf{H}_1^\top+\mathbf{I}|}{|\mathbf{H}_1\mathbf{K}_2\mathbf{H}_1^\top+\mathbf{I})|}+\frac{1}{2}\log|\mathbf{H}_2\mathbf{K}_2\mathbf{H}_2^\top+\mathbf{I}|, \tag{65}$$

$$R_{e1}\le\frac{1}{2}\log\frac{|\mathbf{H}_1(\mathbf{K}_1+\mathbf{K}_2)\mathbf{H}_1^\top+\mathbf{I}|}{|\mathbf{H}_1\mathbf{K}_2\mathbf{H}_1^\top+\mathbf{I}|}-\frac{1}{2}\log\frac{|\mathbf{H}_2(\mathbf{K}_1+\mathbf{K}_2)\mathbf{H}_2^\top+\mathbf{I}|}{|\mathbf{H}_2\mathbf{K}_2\mathbf{H}_2^\top+\mathbf{I}|}, \tag{66}$$

$$R_{e2}\le\frac{1}{2}\log|\mathbf{H}_2\mathbf{K}_2\mathbf{H}_2^\top+\mathbf{I}|-\frac{1}{2}\log|\mathbf{H}_1\mathbf{K}_2\mathbf{H}_1^\top+\mathbf{I}|, \tag{67}$$

$$R_{e1}\le R_1, \tag{68}$$

$$R_{e2}\le R_2 \tag{69}$$

for some positive semi-definite matrices $\mathbf{K}_1$ and $\mathbf{K}_2$ such that $\mathbf{K}_1+\mathbf{K}_2\preceq\mathbf{S}$, and $\mathcal{R}_{21}$ can be obtained from $\mathcal{R}_{12}$ by swapping the indices 1 and 2.

Similar to the inner bound for the discrete memoryless BCC in Theorem 1, the achievable region for the Gaussian MIMO channel in Theorem 6 is also known to be partially tight although, in general, it is unknown whether it is exactly equal to the capacity-equivocation region of the Gaussian MIMO BCC. Next, we present the cases where the inner bound in Theorem 6 is partially tight. To this end, we note that the capacity-equivocation region of the Gaussian MIMO BCC is a five-dimensional region $(R_0,R_1,R_2,R_{e1},R_{e2})$. As of now, two three-dimensional sub-regions of the capacity-equivocation region have been obtained, where these two sub-regions are the dimension-wise largest known sub-regions of the capacity-equivocation region [15]–[19]. These two dimension-wise largest known sub-regions correspond to the following scenarios.

- In the first scenario, there is a common message sent to both users, and a private message intended to the first user where this private message needs to be kept hidden as much as possible from the second user. Hence, this scenario can be obtained by setting $R_2=R_{e2}=0$ in the most general scenario for the Gaussian MIMO BCC. Thus, this scenario is identical to the one that was studied by [2], and can be viewed as an application of their scenario to the Gaussian MIMO BCC. Moreover, since the capacity-equivocation region of this scenario has been obtained by [2] for discrete memoryless BCC, the single-letter description for the capacity-equivocation region of the Gaussian MIMO BCC exists. To obtain capacity-equivocation of the Gaussian MIMO BCC in an explicit form, one needs to find to the optimal $(U,V,\mathbf{X})$ to evaluate the single-letter description in Theorem 3. This is accomplished in [15] and [16], and it is shown that this explicit form of the capacity-equivocation region is the same as the achievable region that can be obtained from Theorem 6, that is jointly Gaussian $(U,V,\mathbf{X})$ is optimal.
- In the second scenario, there is a common message sent to both users, and a private message for each user where the private messages need to be transmitted in perfect secrecy. Hence, this scenario can be obtained by setting $R_{e1}=R_1$ and $R_{e2}=R_2$ in the most general scenario for the Gaussian MIMO BCC. Thus, the second scenario addresses the description of the secrecy capacity region of the Gaussian MIMO BCC. Unlike to the first scenario, the single-letter description for the capacity-equivocation region of this scenario does not exist since the secrecy capacity region of the discrete memoryless BCC is unknown in general. Despite the absence of a single-letter description, the secrecy capacity region of the Gaussian MIMO BCC has been obtained in [17]–[19], and is the same as the achievable region that can be obtained from Theorem 6.

In the upcoming two sub-sections, we present the capacity results for these two scenarios and some specializations of these capacity results.

A.1 First Scenario

We start with the capacity result for the first scenario, i.e., the capacity-equivocation region of the Gaussian MIMO BCC with common and only one private messages, which is stated in the following theorem.

Theorem 7 ([15], [16]) The capacity-equivocation region of the Gaussian MIMO BCC with common and only one private message is given by the union of rate triples (R_0,R_1,R_{e1}) satisfying

$$R_0\le\min_{j=1,2}\frac{1}{2}\log\frac{|\mathbf{H}_j\mathbf{S}\mathbf{H}_j^\top+\mathbf{I}|}{|\mathbf{H}_j\mathbf{K}\mathbf{H}_j^\top+\mathbf{I}|}, \tag{70}$$

$$R_0+R_1\le\min_{j=1,2}\frac{1}{2}\log\frac{|\mathbf{H}_j\mathbf{S}\mathbf{H}_j^\top+\mathbf{I}|}{|\mathbf{H}_j\mathbf{K}\mathbf{H}_j^\top+\mathbf{I}|}+\frac{1}{2}\log|\mathbf{H}_1\mathbf{K}\mathbf{H}_1^\top+\mathbf{I}|, \tag{71}$$

$$R_{e1}\le\frac{1}{2}\log|\mathbf{H}_1\mathbf{K}\mathbf{H}_1^\top+\mathbf{I}|-\frac{1}{2}\log|\mathbf{H}_2\mathbf{K}\mathbf{H}_2^\top+\mathbf{I}| \tag{72}$$

where $\mathbf{K}$ is a positive semi-definite matrix such that $\mathbf{K}\preceq\mathbf{S}$.

We note that the capacity-equivocation region in Theorem 7 can be attained by the inner bound in Theorem 6 by setting $R_2=R_{e2}=0,\mathbf{K}_2=\mathbf{0}$, and $\mathbf{K}_1=\mathbf{K}$. Thus, Theorem 6 is tight for this case. Besides Theorem 6, the achievability of the capacity-equivocation region in Theorem 7 can be shown by evaluating the single-letter description for the capacity-equivocation region given in Theorem 3 for the following selections of U,V, and $\mathbf{X}$: i) U is selected as a Gaussian random vector with zero-mean and covariance matrix $\mathbf{S}-\mathbf{K}$ and ii) we set $V=\mathbf{X}=U+U'$ where U' is a Gaussian random vector with zero-mean and covariance matrix $\mathbf{K}$, and is independent of U. The converse proof of Theorem 7 is more involved than the achievability proof. In particular, to provide a converse proof, one needs to show that this

selection of $(U, V, \mathbf{X})$ is sufficient to exhaust the single-letter description given in Theorem 3. This is accomplished in [15] and [16] by using the channel enhancement technique [10] and some extremal inequalities.

Next, we investigate Theorem 7 for special cases. The first special case is the secrecy capacity region of the Gaussian MIMO BCC with common and only one private message, which can be obtained from Theorem 7 by setting $R_{e1} = R_1$.

Corollary 3 ([20]) The secrecy capacity region of the Gaussian MIMO BCC with common and only one private message is given by the union of rate pairs (R_0, R_1) satisfying

$$R_0 \leq \min_{j=1,2} \frac{1}{2} \log \frac{|\mathbf{H}_j \mathbf{S} \mathbf{H}_j^\top + \mathbf{I}|}{|\mathbf{H}_j \mathbf{K} \mathbf{H}_j^\top + \mathbf{I}|}, \tag{73}$$

$$R_1 \leq \frac{1}{2} \log |\mathbf{H}_1 \mathbf{K} \mathbf{H}_1^\top + \mathbf{I}| - \frac{1}{2} \log |\mathbf{H}_2 \mathbf{K} \mathbf{H}_2^\top + \mathbf{I}| \tag{74}$$

where $\mathbf{K}$ is a positive semi-definite matrix such that $\mathbf{K} \preceq \mathbf{S}$.

The second special scenario is the capacity-equivocation region of the Gaussian MIMO BCC with only one private message and no common message, which can be obtained from Theorem 7 by setting $R_0 = 0$.

Corollary 4 ([21]) The capacity-equivocation region of the Gaussian MIMO BCC with only one private message is given by the union of rate pairs (R_1, R_{e1}) satisfying

$$R_1 \leq \frac{1}{2} \log |\mathbf{H}_1 \mathbf{S} \mathbf{H}_1^\top + \mathbf{I}|, \tag{75}$$

$$R_{e1} \leq \frac{1}{2} \log |\mathbf{H}_1 \mathbf{K} \mathbf{H}_1^\top + \mathbf{I}| - \frac{1}{2} \log |\mathbf{H}_2 \mathbf{K} \mathbf{H}_2^\top + \mathbf{I}| \tag{76}$$

where $\mathbf{K}$ is a positive semi-definite matrix such that $\mathbf{K} \preceq \mathbf{S}$.

This corollary can be viewed as Gaussian MIMO version of the capacity result in Theorem 4, where although there is a single message to be transmitted, rate-splitting and superposition coding was necessary to attain the capacity-equivocation region. The capacity result in this corollary provides a concrete example to show this necessity. In particular, this corollary states that the private message of the first user needs to be decomposed into two parts, and these two parts need to be encoded by using superposition coding [22]. The transmitter allots the covariance matrix $\mathbf{S} - \mathbf{K}$ to the first part, and the covariance matrix $\mathbf{K}$ to the second part, where the the first part does not contribute to the equivocation, and the entire equivocation comes from the second part.

We conclude this section by presenting the secrecy capacity of the Gaussian MIMO BCC, which can be obtained from Theorem 7 by setting $R_0 = 0$ and $R_1 = R_{e1}$.

Corollary 5 ([23]–[26]) The secrecy capacity of the Gaussian MIMO BCC is given by

$$\max_{\mathbf{0} \preceq \mathbf{K} \preceq \mathbf{S}} \frac{1}{2} \log |\mathbf{H}_1 \mathbf{K} \mathbf{H}_1^\top + \mathbf{I}| - \frac{1}{2} \log |\mathbf{H}_2 \mathbf{K} \mathbf{H}_2^\top + \mathbf{I}|. \tag{77}$$

This corollary states that the secrecy capacity of the Gaussian MIMO BCC can be achieved by selecting $V = \mathbf{X}$ as a zero-mean Gaussian vector with covariance matrix $\mathbf{K}$ in Corollary 2. There are various proofs of Corollary 5 [23]–[26]. Most of these proofs [23]–[25] rely on a Sato-type outer bound [27]. In this outer bound, first a new channel is constructed by providing the second user's (eavesdropper's) observation to the first user. Hence, the secrecy capacity of this new channel serves as an outer bound for the secrecy capacity of the original channel. Moreover, the new channel is degraded and its secrecy capacity is known in a single-letter form due to Wyner [1], see Corollary 1. We note that since this new channel is degraded, there is no auxiliary random variable in its secrecy capacity, and its secrecy capacity can be obtained in an explicit form by showing the optimality of Gaussian $\mathbf{X}$. Second, this outer bound is tightened by noting the fact that the secrecy capacity in a broadcast channel does not depend on the entire distribution $p(y_1, y_2|x)$ but the marginal distributions $p(y_1|x)$ and $p(y_2|x)$. Thus, this Sato-type outer bound can be tightened by minimizing it over all possible joint distributions $q(y_1, y_2|x)$ such that the corresponding marginal distributions $q(y_1|x)$ and $q(y_2|x)$ are equal to the ones in the original channel, i.e., $q(y_1|x) = p(y_1|x)$ and $q(y_2|x) = p(y_2|x)$. After this tightening, it is shown that this outer bound is equal to the achievable secrecy rate.

The proofs in [23]–[25] involve rather complicated optimization problems, however, indeed, a simpler proof can be provided as was done in [26] by using channel enhancement [10]. The proofs in [23]–[25] which rely on a Sato-type outer bound reveal that for any Gaussian MIMO BCC, there exists a degraded Gaussian MIMO BCC whose secrecy capacity is potentially larger than the secrecy capacity of the original channel, and thus the secrecy capacity of the degraded channel is an outer bound for the secrecy capacity of the original channel. In fact, due to the insensitivity of the secrecy capacity on the joint distribution, there exist many degraded Gaussian MIMO BCCs, which provide potentially loose outer bounds. The development in [23]–[25] shows that, at least one of these degraded Gaussian MIMO BCCs have secrecy capacity which equals to the secrecy capacity of the original channel. Indeed, this outline of the proofs [23]–[25] relying on Sato-type outer bound is a manifestation of the channel enhancement technique [10], where exactly the same steps are taken to prove a capacity result. This similarity is noticed in [26] where an alternative proof for the secrecy capacity of the Gaussian MIMO BCC is provided by using channel enhancement.

We note that the optimal covariance matrix $\mathbf{K}^*$ that attains the maximum in (77) can be obtained in an explicit form by using the generalized eigenvalue decomposition [28] as it is done in [7] and [29]. The last point we discuss about Corollary 5 is that to achieve the secrecy capacity of the Gaussian MIMO BCC, channel pre-fixing is not necessary, i.e., $V = \mathbf{X}$ is an optimal selection. Interestingly, [7] shows that this secrecy capacity can also be achieved by using channel pre-fixing. In particular, [7] shows that the secrecy capacity of the Gaussian MIMO BCC also admits the following form.

Theorem 8 ([7]) The secrecy capacity of the Gaussian MIMO BCC is given by

$$\max_{\mathbf{0} \preceq \mathbf{K} \preceq \mathbf{S}} \frac{1}{2} \log \frac{|\mathbf{H}_1 \mathbf{S} \mathbf{H}_1^\top + \mathbf{I}|}{|\mathbf{H}_1 \mathbf{K} \mathbf{H}_1^\top + \mathbf{I}|} - \frac{1}{2} \log \frac{|\mathbf{H}_2 \mathbf{S} \mathbf{H}_2^\top + \mathbf{I}|}{|\mathbf{H}_2 \mathbf{K} \mathbf{H}_2^\top + \mathbf{I}|}. \tag{78}$$

This alternative form of the secrecy capacity of the Gaussian

MIMO BCC can be achieved by selecting V as a zero-mean Gaussian random vector with covariance matrix $\mathbf{S}-\mathbf{K}$, and $\mathbf{X} = V + V'$, where V' is also a zero-mean Gaussian random vector with covariance matrix $\mathbf{K}$, and is independent of V. We note that in this alternative form of the secrecy capacity, one does not set $V = \mathbf{X}$, i.e., channel pre-fixing is used.

A.2 Second Scenario

The second dimension-wise largest known sub-region, for which the inner bound in Theorem 6 is tight, is the secrecy capacity region of the Gaussian MIMO BCC [17]–[19]. In other words, in the second scenario, there is a common message sent to both users and a private message for each user, where the private messages need to be transmitted in perfect secrecy, i.e., $R_{e1} = R_1$ and $R_{e2} = R_2$. We note that as opposed to the first scenario, where the capacity-equivocation region is known for the discrete memoryless BCC as it is given in Theorem 3, for the second scenario, the capacity-equivocation region is not known for the discrete memoryless channel in general. However, as the following theorem states, the capacity-equivocation region corresponding to the second scenario can be obtained for the Gaussian MIMO BCC.

Theorem 9 ([17]–[19]) The secrecy capacity region of the Gaussian MIMO BCC is given by

$$\mathcal{R}_{12}^{\text{S-DPC}} = \mathcal{R}_{21}^{\text{S-DPC}} \tag{79}$$

where $\mathcal{R}_{12}^{\text{S-DPC}}$ is given by the union of rate triples (R_0, R_1, R_2) satisfying

$$R_0 \leq \min_{j=1,2} \frac{1}{2} \log \frac{|\mathbf{H}_j \mathbf{S} \mathbf{H}_j^\top + \mathbf{I}|}{|\mathbf{H}_j (\mathbf{K}_1 + \mathbf{K}_2) \mathbf{H}_j^\top + \mathbf{I}|}, \tag{80}$$

$$R_1 \leq \frac{1}{2} \log \frac{|\mathbf{H}_1 (\mathbf{K}_1 + \mathbf{K}_2) \mathbf{H}_1^\top + \mathbf{I}|}{|\mathbf{H}_1 \mathbf{K}_2 \mathbf{H}_1^\top + \mathbf{I}|} - \frac{1}{2} \log \frac{|\mathbf{H}_2 (\mathbf{K}_1 + \mathbf{K}_2) \mathbf{H}_2^\top + \mathbf{I}|}{|\mathbf{H}_2 \mathbf{K}_2 \mathbf{H}_2^\top + \mathbf{I}|}, \tag{81}$$

$$R_2 \leq \frac{1}{2} \log |\mathbf{H}_2 \mathbf{K}_2 \mathbf{H}_2^\top + \mathbf{I}| - \frac{1}{2} \log |\mathbf{H}_1 \mathbf{K}_2 \mathbf{H}_1^\top + \mathbf{I}| \tag{82}$$

for some positive semi-definite matrices $\mathbf{K}_1$ and $\mathbf{K}_2$ such that $\mathbf{K}_1 + \mathbf{K}_2 \preceq \mathbf{S}$. $\mathcal{R}_{21}^{\text{S-DPC}}$ can be obtained from $\mathcal{R}_{12}^{\text{S-DPC}}$ by swapping the indices 1 and 2.

This theorem implies that the secrecy capacity region of the Gaussian MIMO BCC can be obtained from the inner bound given in Theorem 6 by setting $R_{e1} = R_1$ and $R_{e2} = R_2$. We remind that DPC [14] is used to encode the private messages in Theorem 6, where depending on the encoding order used, one of the two users gets a clean link because it does not see any interference originating from the existence of the other user. As mentioned earlier, the difference of this DPC from the one used when there is no secrecy concern is the additional random binning introduced on top of the already present binning. This additional binning is necessitated by the secrecy concern. Consequently, this double binning provides codewords for the private messages, by using V_1 and V_2, with three indices. One of these three indices is a dummy fixed index to ensure the joint typicality of the codewords generated by V_1 and V_2, and the other two indices carry the parts of the private messages, i.e., each private message is divided into two parts. One of these two indices provides the necessary protection for the confidentiality of the other index. Thus, one of these two indices is transmitted in perfect secrecy, and the other index, the one providing the necessary protection, does not contribute to the equivocation. Consequently, if we specialize the DPC scheme to the perfect secrecy case here, the information content of the index providing protection for the other one is replaced by some dummy content. This specialization of DPC to the perfect secrecy case is called secret DPC (S-DPC) [7], [17]–[19]. This is why we have superscript S-DPC in (79).

Since S-DPC corresponds to a specialization of DPC, in S-DPC, depending on the encoding order used, a user gets a clean link, where there is no interference from the other user's confidential message. Thus, one expects that the two achievable rate regions, i.e., $\mathcal{R}_{12}^{\text{S-DPC}}$ and $\mathcal{R}_{21}^{\text{S-DPC}}$, arising from two possible encoding orders, should not be equal, and taking a convex closure of these two regions, i.e., the region $\text{conv}(\mathcal{R}_{12}^{\text{S-DPC}} \cup \mathcal{R}_{21}^{\text{S-DPC}})$, should yield a larger achievable rate region. However, Theorem 9 reveals that both achievable rate regions are identical, and are equal to the secrecy capacity region of the Gaussian MIMO BCC. Thus, to achieve the secrecy capacity region of the Gaussian MIMO BCC, anyone of the two possible encoding orders used in S-DPC, which lead to the achievable regions $\mathcal{R}_{12}^{\text{S-DPC}}$ and $\mathcal{R}_{21}^{\text{S-DPC}}$, is sufficient. This invariance property of the S-DPC has connections with the capacity region of the Gaussian MIMO broadcast channel with common and private messages [30]–[32], where there is no secrecy concern on the private messages. A more detailed discussion about the invariance of S-DPC with respect to the encoding order can be found in [17] and [18].

Next, we consider the specializations of the capacity result in Theorem 9. First, we note that if we disable one of the two confidential messages by setting its rate to zero, we recover the secrecy capacity region of the Gaussian MIMO BCC with common and only one confidential message given in Corollary 3. In addition to one of the two confidential messages, if we also disable the common message by setting its rate to zero, we recover the secrecy capacity of the Gaussian MIMO BCC stated in Corollary 5. The final specialization of the capacity result in Theorem 9 can be obtained by disabling only the common message by setting its rate to zero. The corresponding result is stated in the following corollary.

Corollary 6 ([7]) The secrecy capacity region of the Gaussian MIMO BCC without a common message is given by the union of rate pairs (R_1, R_2) satisfying

$$R_1 \leq \frac{1}{2} \log \frac{|\mathbf{H}_1 \mathbf{S} \mathbf{H}_1^\top + \mathbf{I}|}{|\mathbf{H}_1 \mathbf{K} \mathbf{H}_1^\top + \mathbf{I}|} - \frac{1}{2} \log \frac{|\mathbf{H}_2 \mathbf{S} \mathbf{H}_2^\top + \mathbf{I}|}{|\mathbf{H}_2 \mathbf{K} \mathbf{H}_2^\top + \mathbf{I}|}, \tag{83}$$

$$R_2 \leq \frac{1}{2} \log |\mathbf{H}_2 \mathbf{K} \mathbf{H}_2^\top + \mathbf{I}| - \frac{1}{2} \log |\mathbf{H}_1 \mathbf{K} \mathbf{H}_1^\top + \mathbf{I}| \tag{84}$$

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

As pointed out in [7], the secrecy capacity region in Corollary 6 is rectangular which is implied by the fact that both (83) and (84) have the same maximizer. Thus, the secrecy capacity region in Corollary 6 can be restated as follows.

Corollary 7 ([7]) The secrecy capacity region of the Gaussian MIMO BCC without common message is given by the

union of rate pairs (R_1, R_2) satisfying

$$R_1 \leq \max_{\mathbf{0} \preceq \mathbf{K} \preceq \mathbf{S}} \frac{1}{2} \log \frac{|\mathbf{H}_1 \mathbf{S} \mathbf{H}_1^\top + \mathbf{I}|}{|\mathbf{H}_1 \mathbf{K} \mathbf{H}_1^\top + \mathbf{I}|} - \frac{1}{2} \log \frac{|\mathbf{H}_2 \mathbf{S} \mathbf{H}_2^\top + \mathbf{I}|}{|\mathbf{H}_2 \mathbf{K} \mathbf{H}_2^\top + \mathbf{I}|}, \tag{85}$$

$$R_2 \leq \max_{\mathbf{0} \preceq \mathbf{K} \preceq \mathbf{S}} \frac{1}{2} \log |\mathbf{H}_2 \mathbf{K} \mathbf{H}_2^\top + \mathbf{I}| - \frac{1}{2} \log |\mathbf{H}_1 \mathbf{K} \mathbf{H}_1^\top + \mathbf{I}|. \tag{86}$$

Finally, we note that in a Gaussian MIMO BCC without a common message, both users can achieve their secrecy capacity because in view of Theorem 8, (85) is the secrecy capacity of the first user, and in view of Corollary 5, (86) is the secrecy capacity of the second user.

IV. MULTI-RECEIVER WIRETAP CHANNELS

Similar to our presentation for the BCC, here also, we first present the results for the discrete memoryless multi-receiver wiretap channel, and next present the results for the Gaussian MIMO channel. We start with the best known inner bound for the capacity region of the discrete memoryless multi-receiver wiretap channel.

Theorem 10 ([33]) The rate tuples $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ satisfying

$$R_{s1} \leq \min_{j=1,2} I(U;Y_j) + I(V_1;Y_1|U) - I(U,V_1;Z), \tag{87}$$

$$R_{s2} \leq \min_{j=1,2} I(U;Y_j) + I(V_2;Y_2|U) - I(U,V_2;Z), \tag{88}$$

$$R_{s1} + R_{s2} \leq \min_{j=1,2} I(U;Y_j) + I(V_1;Y_1|U) + I(V_2;Y_2|U) - I(V_1;V_2|U) - I(U,V_1,V_2;Z), \tag{89}$$

$$R_{s1} + R_{p1} \leq \min_{j=1,2} I(U;Y_j) + I(V_1;Y_1|U), \tag{90}$$

$$R_{s2} + R_{p2} \leq \min_{j=1,2} I(U;Y_j) + I(V_2;Y_2|U), \tag{91}$$

$$\sum_{j=1}^{2} R_{sj} + R_{p1} \leq \min_{j=1,2} I(U;Y_j) + I(V_1;Y_1|U) + I(V_2;Y_2|U) - I(V_2;Z|U), \tag{92}$$

$$\sum_{j=1}^{2} R_{sj} + R_{p2} \leq \min_{j=1,2} I(U;Y_j) + I(V_1;Y_1|U) + I(V_2;Y_2|U) - I(V_1;Z|U), \tag{93}$$

$$\sum_{j=1}^{2} R_{sj} + R_{pj} \leq \min_{j=1,2} I(U;Y_j) + I(V_1;Y_1|U) + I(V_2;Y_2|U) - I(V_1;V_2|U) \tag{94}$$

for some U, V_1, and V_2 such that $(U, V_1, V_2) \rightarrow X \rightarrow (Y_1, Y_2, Z)$ are achievable.

This inner bound is obtained by using rate-splitting, superposition coding [22] and Marton coding [13]. In particular, each public and confidential message pair (W_{sj}, W_{pj}) is divided into two parts as (W_{sj}^1, W_{pj}^1) and (W_{sj}^2, W_{pj}^2). After rate-splitting, the first parts of public and confidential message pairs, i.e., (W_{s1}^1, W_{p1}^1) and (W_{s2}^1, W_{p2}^1), are encoded by using the codewords generated through U. These codewords constitute the first layer of the superposition coding. In the second layer of the superposition coding, the second parts of the public and confidential message pairs are encoded. In particular, the second part of each public and confidential message pair (W_{sj}^2, W_{pj}^2) is encoded to the codewords generated by using V_j, where encoding is performed by using Marton's coding. Similar to the use of Marton's coding for the inner bound in Theorem 1, here also Marton's coding is slightly modified due to the presence of the secrecy requirement. In particular, similar to Theorem 1, here also, an additional level of binning is required to meet the secrecy constraints, on top of the already existing binning in Marton's coding. Indeed, here additional binning is necessitated by not only the presence of the secrecy requirement but also the presence of the public messages. In other words, the public messages have a dual role of both carrying information and also providing protection for the confidential messages.

Next, we consider the specializations of Theorem 10 to the degraded multi-receiver wiretap channel. For the degraded multi-receiver wiretap channel, first, we provide the following achievable rate region which can be obtained from the one in Theorem 10 by setting $U = V_2$ and $V_1 = X$ which satisfy the Markov chain $U \rightarrow X \rightarrow Y_1, Y_2, Z$, and eliminating the redundant bounds.

Corollary 8 ([33], [34]) In a degraded multi-receiver wiretap channel, the rate tuples $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ satisfying

$$R_{s2} \leq I(U;Y_2) - I(U;Z), \tag{95}$$

$$R_{s1} + R_{s2} \leq I(U;Y_2) + I(X;Y_1|U) - I(X;Z), \tag{96}$$

$$R_{s2} + R_{p2} \leq I(U;Y_2), \tag{97}$$

$$R_{s1} + R_{s2} + R_{p2} \leq I(U;Y_2) + I(X;Y_1|U) - I(X;Z|U), \tag{98}$$

$$R_{s1} + R_{s2} + R_{p1} + R_{p2} \leq I(U;Y_2) + I(X;Y_1|U) \tag{99}$$

are achievable, where U and X satisfy the following Markov chain

$$U \rightarrow X \rightarrow Y_1 \rightarrow Y_2 \rightarrow Z. \tag{100}$$

As mentioned earlier, this inner bound for the degraded multi-receiver wiretap channel can be obtained by a proper selection of the auxiliary random variables U, V_1, and V_2 in Theorem 10. However, Corollary 8 can also be obtained without invoking Theorem 10. In this alternative derivation, only superposition coding is used, i.e., as opposed to Theorem 10, there is no need to use Marton's coding. The alternative derivation of Corollary 8 consists of two steps. As a first step, using superposition coding, one can show that the rate tuples $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ satisfying

$$R_{p2} \leq I(U;Z), \tag{101}$$

$$R_{s2} \leq I(U;Y_2) - I(U;Z), \tag{102}$$

$$R_{p1} \leq I(X;Z|U), \tag{103}$$

$$R_{s1} \leq I(X;Y_1|U) - I(X;Z|U) \tag{104}$$

are achievable, where (U, X) satisfy (100). As the second step for the alternative derivation of Corollary 8, one can use the following facts.

- Since confidential messages can be considered as public messages as well, each legitimate user's confidential message rate R_{sj} can be given up in the favor of its public message rate R_{pj}, i.e., if $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ is achievable, $(R_{p1}+\alpha_1, R_{s1}-\alpha_1, R_{p2}+\alpha_2, R_{s2}-\alpha_2)$ is also achievable for non-negative (α_1, α_2) pairs satisfying $\alpha_j \leq R_{sj}$.
- Since the channel is degraded, the second legitimate user's confidential message rate R_{s2} can be given up in the favor of the first legitimate user's public and confidential message rates R_{p1} and R_{s1}, i.e., if $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ is achievable, $(R_{p1}+\alpha, R_{s1}+\beta, R_{p2}, R_{s2}-\alpha-\beta)$ is also achievable for non-negative (α, β) pairs satisfying $\alpha+\beta \leq R_{s2}$.
- Since the channel is degraded, the second legitimate user's public message rate R_{p2} can be given up in the favor of the first legitimate user's public message rate R_{p1}, i.e., if $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ is achievable, $(R_{p1}+\alpha, R_{s1}, R_{p2}-\alpha, R_{s2})$ is also achievable for any non-negative α satisfying $\alpha \leq R_{p2}$,

in conjunction with Fourier-Motzkin elimination, and show that the region given in (101)–(104) is equivalent to the one given in Corollary 8.

We next present an outer bound for the capacity region of the degraded multi-receiver wiretap channel which demonstrates the partial tightness of the inner bound in Corollary 8.

Theorem 11 ([33], [34]) The capacity region of the degraded multi-receiver wiretap channel with public and confidential messages is contained in the union of rate tuples $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ satisfying

$$R_{s2} \leq I(U;Y_2) - I(U;Z), \tag{105}$$

$$R_{s1}+R_{s2} \leq I(U;Y_2) + I(X;Y_1|U) - I(X;Z), \tag{106}$$

$$R_{p2}+R_{s2} \leq I(U;Y_2), \tag{107}$$

$$R_{p1}+R_{s1}+R_{p2}+R_{s2} \leq I(U;Y_2) + I(X;Y_1|U) \tag{108}$$

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

$$U \to X \to Y_1 \to Y_2 \to Z. \tag{109}$$

This outer bound provides a partial converse for the capacity region of the degraded multi-receiver wiretap channel because the only difference between the inner bound in Corollary 8 and the outer bound in Theorem 11 is the bound on $R_{s1}+R_{p2}+R_{s2}$ given by (98). In particular, in addition to the bounds defining the outer bound for the capacity region, the inner bound includes the following constraint

$$R_{s1}+R_{p2}+R_{s2} \leq I(U;Y_2) + I(X;Y_1|U) - I(X;Z|U). \tag{110}$$

Besides that, the inner and outer bounds are identical. However, still there are cases where the capacity region can be obtained. The first case where the inner bound in Corollary 8 and the outer bound in Theorem 11 match can be obtained by setting the confidential message rate of the first legitimate user to zero, i.e., $R_{s1}=0$.

Corollary 9 ([33], [34]) The capacity region of the degraded multi-receiver wiretap channel without the first legitimate user's confidential message is given by the union of rate triples (R_{p1}, R_{s1}, R_{s2}) satisfying

$$R_{s2} \leq I(U;Y_2) - I(U;Z), \tag{111}$$

$$R_{s2}+R_{p2} \leq I(U;Y_2), \tag{112}$$

$$R_{p1}+R_{p2}+R_{s2} \leq I(U;Y_2) + I(X;Y_1|U) \tag{113}$$

where U and X exhibit the following Markov chain

$$U \to X \to Y_1 \to Y_2 \to Z. \tag{114}$$

The second case where the inner bound in Corollary 8 and the outer bound in Theorem 11 match can be obtained by setting the public message rate of the second legitimate user to zero, i.e., $R_{p2}=0$.

Corollary 10 ([33], [34]) The capacity region of the degraded multi-receiver wiretap channel without the second legitimate user's public message is given by the union of rate triples (R_{p1}, R_{s1}, R_{s2}) satisfying

$$R_{s2} \leq I(U;Y_2) - I(U;Z), \tag{115}$$

$$R_{s1}+R_{s2} \leq I(U;Y_2) + I(X;Y_1|U) - I(X;Z), \tag{116}$$

$$R_{p1}+R_{s1}+R_{s2} \leq I(U;Y_2) + I(X;Y_1|U) \tag{117}$$

where U, X exhibit the following Markov chain

$$U \to X \to Y_1 \to Y_2 \to Z. \tag{118}$$

Corollary 10 also implies that the inner bound in Corollary 8 and the outer bound in Theorem 11 match on the secrecy capacity region of the degraded multi-receiver wiretap channel. In particular, Corollary 8 and the outer bound in Theorem 11 match if the rates of both public messages are set to zero, i.e., $R_{p1}=R_{p2}=0$. The secrecy capacity region of the degraded multi-receiver wiretap channel is given by the following corollary.

Corollary 11 ([35]–[37]) The secrecy capacity region of the degraded multi-receiver wiretap channel is given by the union of rate pairs (R_{s1}, R_{s2}) satisfying[6]

$$R_{s2} \leq I(U;Y_2) - I(U;Z), \tag{119}$$

$$R_{s1} \leq I(X;Y_1|U) - I(X;Z|U) \tag{120}$$

where U, X exhibit the following Markov chain

$$U \to X \to Y_1 \to Y_2 \to Z. \tag{121}$$

We note that in addition to its representation in Corollary 11, the secrecy capacity region of the degraded multi-receiver wiretap channel can be stated in an alternative form as the union of rate pairs (R_{s1}, R_{s2}) satisfying

$$R_{s2} \leq I(U;Y_2) - I(U;Z), \tag{122}$$

$$R_{s1}+R_{s2} \leq I(U;Y_2) + I(X;Y_1|U) - I(X;Z) \tag{123}$$

where U, X exhibit the Markov chain in (121).

[6]The secrecy capacity region of the degraded multi-receiver wiretap channel for an arbitrary number of legitimate users, i.e., for more than two legitimate users, can be found in [36] and [37].

A. Gaussian MIMO Multi-Receiver Wiretap Channels

In this section, we present the existing results for the capacity region of the Gaussian MIMO multi-receiver wiretap channel. We start with an inner bound for the capacity region of the Gaussian MIMO channel, where this inner bound can be obtained by using a specific selection of (U, V_1, V_2) in Theorem 10.

Theorem 12 ([33]) An achievable rate region for the Gaussian MIMO multi-receiver wiretap channel is given by

$$\text{conv}\left(\mathcal{R}_{12}\bigcup\mathcal{R}_{21}\right) \tag{124}$$

where $\mathcal{R}_{12}$ is given by the union of rate tuples $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ satisfying

$$R_{s1} \leq \frac{1}{2}\log\frac{|\mathbf{H}_1(\mathbf{K}_1+\mathbf{K}_2)\mathbf{H}_1^\top+\mathbf{I}|}{|\mathbf{H}_1\mathbf{K}_2\mathbf{H}_1^\top+\mathbf{I}|} - \frac{1}{2}\log\frac{|\mathbf{H}_Z(\mathbf{K}_1+\mathbf{K}_2)\mathbf{H}_Z^\top+\mathbf{I}|}{|\mathbf{H}_Z\mathbf{K}_2\mathbf{H}_Z^\top+\mathbf{I}|}, \tag{125}$$

$$R_{s1}+R_{p1} \leq \frac{1}{2}\log\frac{|\mathbf{H}_1(\mathbf{K}_1+\mathbf{K}_2)\mathbf{H}_1^\top+\mathbf{I}|}{|\mathbf{H}_1\mathbf{K}_2\mathbf{H}_1^\top+\mathbf{I}|}, \tag{126}$$

$$R_{s2} \leq \frac{1}{2}\log|\mathbf{H}_2\mathbf{K}_2\mathbf{H}_2^\top+\mathbf{I}| - \frac{1}{2}\log|\mathbf{H}_Z\mathbf{K}_2\mathbf{H}_Z^\top+\mathbf{I}|, \tag{127}$$

$$R_{s2}+R_{p2} \leq \frac{1}{2}\log|\mathbf{H}_2\mathbf{K}_2\mathbf{H}_2^\top+\mathbf{I}| \tag{128}$$

where $\mathbf{K}_1$ and $\mathbf{K}_2$ are positive semi-definite matrices satisfying $\mathbf{K}_1+\mathbf{K}_2 \preceq \mathbf{S}$. $\mathcal{R}_{21}$ can be obtained from $\mathcal{R}_{12}$ by swapping the indices 1 and 2.

This inner bound can be obtained from the achievable rate region in Theorem 10 by selecting $U=\phi$ and V_1, V_2 as jointly Gaussian random vectors. In particular, the pairs of confidential and public messages are encoded by using DPC [14], where a covariance matrix $\mathbf{K}_2$ is allotted for the second legitimate user's confidential and public message pair, and the covariance matrix $\mathbf{K}_1$ is allotted for the first legitimate user's confidential and public message pair. To obtain the achievable rate region $\mathcal{R}_{12}$, the first legitimate user's confidential and public message pair is encoded by a standard Gaussian codebook generated by using the Gaussian random vector V_1 with covariance matrix $\mathbf{K}_1$. Next, the second legitimate user's confidential and public message pair is encoded by using DPC such that the second legitimate user observes an interference-free link between itself and the transmitter. The second achievable rate region $\mathcal{R}_{21}$ is obtained by changing the encoding order, i.e., to obtain $\mathcal{R}_{21}$, the second legitimate user's messages are encoded first, and next, the first legitimate user's messages are encoded.

Similar to the inner bound in Theorem 10, under certain scenarios, the inner bound in Theorem 12 is tight for the degraded Gaussian MIMO channel. However, there is also a case where the inner bound in Theorem 12 is shown to be tight for the non-degraded Gaussian MIMO channel. This case can be obtained by setting the rates of both public messages to zero, i.e., $R_{p1}=R_{p2}=0$. In other words, the inner bound in Theorem 12 matches the secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel. This result is stated in the following theorem.

Theorem 13 ([8], [9]) The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel is given by[7]

$$\text{conv}\left(\mathcal{R}_{12}\bigcup\mathcal{R}_{21}\right) \tag{129}$$

where $\mathcal{R}_{12}$ is given by the union of rate pairs (R_{s1}, R_{s2}) satisfying

$$R_{s1} \leq \frac{1}{2}\log\frac{|\mathbf{H}_1(\mathbf{K}_1+\mathbf{K}_2)\mathbf{H}_1^\top+\mathbf{I}|}{|\mathbf{H}_1\mathbf{K}_2\mathbf{H}_1^\top+\mathbf{I}|} - \frac{1}{2}\log\frac{|\mathbf{H}_Z(\mathbf{K}_1+\mathbf{K}_2)\mathbf{H}_Z^\top+\mathbf{I}|}{|\mathbf{H}_Z\mathbf{K}_2\mathbf{H}_Z^\top+\mathbf{I}|}, \tag{130}$$

$$R_{s2} \leq \frac{1}{2}\log|\mathbf{H}_2\mathbf{K}_2\mathbf{H}_2^\top+\mathbf{I}| - \frac{1}{2}\log|\mathbf{H}_Z\mathbf{K}_2\mathbf{H}_Z^\top+\mathbf{I}| \tag{131}$$

where $\mathbf{K}_1$ and $\mathbf{K}_2$ are positive semi-definite matrices satisfying $\mathbf{K}_1+\mathbf{K}_2 \preceq \mathbf{S}$. $\mathcal{R}_{21}$ can be obtained from $\mathcal{R}_{12}$ by swapping the indices 1 and 2.

This theorem states that the inner bound in Theorem 12 can attain the the secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel if one sets $R_{p1}=R_{p2}=0$ in Theorem 12. Thus, using DPC, one can achieve the secrecy capacity region of the Gaussian multi-receiver wiretap channel. There is a slight difference between the use of DPC for Theorem 12 and the use of DPC for Theorem 13. In Theorem 12, DPC was used to generate codewords that carry both the confidential message and the public message. In other words, codewords generated through V_j carries the pair of confidential and public messages, where besides their information content, public messages provide the necessary protection for the confidential messages. However, in Theorem 13, the public messages are replaced with dummy messages with no information content, where the sole purpose of these dummy messages is to protect the confidential messages from the eavesdropper. We note that the difference between the DPC used to achieve Theorem 12 and the DPC used to achieve Theorem 13 is similar to the difference between the DPC used to achieve Theorem 6 and the DPC, which was called S-DPC, used to achieve Theorem 9.

Next, we provide an outline of the converse proof of Theorem 13. One of the main challenges to provide a converse proof for Theorem 13 is that Theorem 13 gives the secrecy capacity region of a *non-degraded* multi-receiver wiretap channel and although there is a single-letter expression for the secrecy capacity region of the degraded multi-receiver wiretap channel, there is no such description for the general, not necessarily degraded, multi-receiver wiretap channel. However, despite the lack of a single-letter description for the secrecy capacity region of the non-degraded multi-receiver wiretap channel, a converse proof is provided in [8] and [9]. This converse proof consists of two main steps. In the first step, [8] and [9] obtains the secrecy capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel[8]. Contrary to the non-degraded multi-receiver wiretap channel, the secrecy capacity region of the degraded

[7]The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel for an arbitrary number of legitimate users, i.e., for more than two legitimate users, can be found in [8] and [9].

[8]The secrecy capacity region of the *degraded* Gaussian MIMO multi-receiver wiretap channel for $K=2$ was independently and concurrently obtained in [38].

channel is known due to Corollary 11. Thus, to obtain the secrecy capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel, one needs to find the optimal random vector $(U, \mathbf{X})$ that exhausts the region given in Corollary 11. References [8] and [9] achieve this task by showing that jointly Gaussian $(U, \mathbf{X})$ is sufficient to evaluate the region in Corollary 11. This task is accomplished by using the de Bruijn identity [39], [40], a connection between the Fisher information matrix and the differential entropy, and the properties of the Fisher information matrix. In particular, using these tools, [8] and [9] show that for any non-Gaussian $(U, \mathbf{X})$, there exists a jointly Gaussian $(U^G, \mathbf{X}^G)$ which provides higher secrecy rates than the ones that any non-Gaussian $(U, \mathbf{X})$ can provide.

The second step of the converse proof consists of lifting the capacity result for the degraded Gaussian MIMO channel to the general, i.e., non-degraded, Gaussian MIMO channel by using channel enhancement [10]. In this step, [8] and [9] consider a non-degraded Gaussian MIMO multi-receiver wiretap channel and examines the boundary of the achievable region given in Theorem 13 for this non-degraded channel. Next, [8] and [9] pick an arbitrary point on the boundary of the achievable region in Theorem 13. For this arbitrary point, a new degraded Gaussian MIMO multi-receiver wiretap channel is constructed by using channel enhancement [10], such that the secrecy capacity region of the new degraded channel includes the secrecy capacity of the original non-degraded channel. Thus, the secrecy capacity region of the new degraded channel, which is known due to the first step of the converse proof, serves as an outer bound for the secrecy capacity region of the original non-degraded channel. Finally, [8] and [9] show that the point picked on the boundary of the achievable region in Theorem 13, from which the new degraded channel was constructed, is also on the boundary of the secrecy capacity region of the new degraded channel. Since the secrecy capacity region of the new degraded channel is an outer bound for the secrecy capacity region of the original non-degraded channel, the point picked on the boundary of the achievable region in Theorem 13 should be on the boundary of the secrecy capacity region of the original non-degraded channel. This argument finalizes the converse proof in [8] and [9].

Next, as we previously show the partial tightness of the inner bound in Theorem 10 for the degraded discrete memoryless multi-receiver wiretap channel, we consider the degraded Gaussian MIMO multi-receiver wiretap channel, and state the partial tightness of the inner bound in Theorem 12 for the degraded Gaussian MIMO multi-receiver wiretap channel. To this end, first we specialize the inner bound in Theorem 12 to the degraded Gaussian MIMO multi-receiver wiretap channel[9].

Corollary 12 ([33], [34]) An inner bound for the capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel is given by the union of rate tuples $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ satisfying

$$R_{s2} \le \frac{1}{2}\log\frac{|\mathbf{H}_2\mathbf{S}\mathbf{H}_2^\top+\mathbf{I}|}{|\mathbf{H}_2\mathbf{K}\mathbf{H}_2^\top+\mathbf{I}|} - \frac{1}{2}\log\frac{|\mathbf{H}_Z\mathbf{S}\mathbf{H}_Z^\top+\mathbf{I}|}{|\mathbf{H}_Z\mathbf{K}\mathbf{H}_Z^\top+\mathbf{I}|}, \tag{132}$$

$$R_{s1}+R_{s2} \le \frac{1}{2}\log\frac{|\mathbf{H}_2\mathbf{S}\mathbf{H}_2^\top+\mathbf{I}|}{|\mathbf{H}_2\mathbf{K}\mathbf{H}_2^\top+\mathbf{I}|} + \frac{1}{2}\log|\mathbf{H}_1\mathbf{K}\mathbf{H}_1^\top+\mathbf{I}| - \frac{1}{2}\log|\mathbf{H}_Z\mathbf{S}\mathbf{H}_Z^\top+\mathbf{I}|, \tag{133}$$

$$R_{s2}+R_{p2} \le \frac{1}{2}\log\frac{|\mathbf{H}_2\mathbf{S}\mathbf{H}_2^\top+\mathbf{I}|}{|\mathbf{H}_2\mathbf{K}\mathbf{H}_2^\top+\mathbf{I}|}, \tag{134}$$

$$\sum_{j=1}^{2} R_{sj}+R_{p2} \le \frac{1}{2}\log\frac{|\mathbf{H}_2\mathbf{S}\mathbf{H}_2^\top+\mathbf{I}|}{|\mathbf{H}_2\mathbf{K}\mathbf{H}_2^\top+\mathbf{I}|} + \frac{1}{2}\log|\mathbf{H}_1\mathbf{K}\mathbf{H}_1^\top+\mathbf{I}| - \frac{1}{2}\log|\mathbf{H}_Z\mathbf{K}\mathbf{H}_Z^\top+\mathbf{I}|, \tag{135}$$

$$\sum_{j=1}^{2} R_{sj}+R_{pj} \le \frac{1}{2}\log\frac{|\mathbf{H}_2\mathbf{S}\mathbf{H}_2^\top+\mathbf{I}|}{|\mathbf{H}_2\mathbf{K}\mathbf{H}_2^\top+\mathbf{I}|} + \frac{1}{2}\log|\mathbf{H}_1\mathbf{K}\mathbf{H}_1^\top+\mathbf{I}| \tag{136}$$

where $\mathbf{K}$ is a positive semi-definite matrix satisfying $\mathbf{K} \preceq \mathbf{S}$.

This inner bound can be obtained from Theorem 12 in two steps. In the first step, only one of the two regions $\mathcal{R}_{12}$ and $\mathcal{R}_{21}$ needs to be considered, namely $\mathcal{R}_{21}$, which is given by the union of rate tuples $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ satisfying

$$R_{s2} \le \frac{1}{2}\log\frac{|\mathbf{H}_2\mathbf{S}\mathbf{H}_2^\top+\mathbf{I}|}{|\mathbf{H}_2\mathbf{K}\mathbf{H}_2^\top+\mathbf{I}|} - \frac{1}{2}\log\frac{|\mathbf{H}_Z\mathbf{S}\mathbf{H}_Z^\top+\mathbf{I}|}{|\mathbf{H}_Z\mathbf{K}\mathbf{H}_Z^\top+\mathbf{I}|}, \tag{137}$$

$$R_{s2}+R_{p2} \le \frac{1}{2}\log\frac{|\mathbf{H}_2\mathbf{S}\mathbf{H}_2^\top+\mathbf{I}|}{|\mathbf{H}_2\mathbf{K}\mathbf{H}_2^\top+\mathbf{I}|}, \tag{138}$$

$$R_{s1} \le \frac{1}{2}\log|\mathbf{H}_1\mathbf{K}\mathbf{H}_1^\top+\mathbf{I}| - \frac{1}{2}\log|\mathbf{H}_Z\mathbf{K}\mathbf{H}_Z^\top+\mathbf{I}|, \tag{139}$$

$$R_{s1}+R_{p1} \le \frac{1}{2}\log|\mathbf{H}_1\mathbf{K}\mathbf{H}_1^\top+\mathbf{I}| \tag{140}$$

where $\mathbf{K}$ is a positive semi-definite matrix satisfying $\mathbf{K} \preceq \mathbf{S}$. We set $\mathbf{K}_1+\mathbf{K}_2=\mathbf{S}$ and $\mathbf{K}_1=\mathbf{K}$ in the original $\mathcal{R}_{21}$ to obtain the region given by (137)–(140). The second step involves showing the equivalence between the two regions given in (133)–(136) and (137)–(140), respectively. This step can be done by using Fourier-Moztkin elimination for the region in (137)–(140) in conjunction with the following facts.

- Since confidential messages can be considered as public messages as well, each legitimate user's confidential message rate R_{sj} can be given up in the favor of its public message rate R_{pj}, i.e., if $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ is achievable, $(R_{p1}+\alpha_1, R_{s1}-\alpha_1, R_{p2}+\alpha_2, R_{s2}-\alpha_2)$ is also achievable for all non-negative (α_1, α_2) pairs satisfying $\alpha_j \le R_{sj}$.
- Since the channel is degraded, the second legitimate user's confidential message rate R_{s2} can be given up in the favor of the first legitimate user's public and confidential message rates R_{p1} and R_{s1}, i.e., if $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ is achievable, $(R_{p1}+\alpha, R_{s1}+\beta, R_{p2}, R_{s2}-\alpha-\beta)$ is also achievable for all non-negative (α, β) pairs satisfying $\alpha+\beta \le R_{s2}$.

[9]Indeed, one case, where the specialization of the inner bound in Theorem 12 to the degraded Gaussian MIMO multi-receiver wiretap channel is tight, is already stated in Theorem 13. In particular, since degraded Gaussian MIMO multi-receiver channels constitute a sub-class of Gaussian MIMO multi-receiver channels, Theorem 13 gives the secrecy capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel as well. Hence, the specialization of the inner bound in Theorem 12 to the degraded Gaussian MIMO channel is tight for the secrecy capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel.

- Since the channel is degraded, the second legitimate user's public message rate R_{p2} can be given up in the favor of the first legitimate user's public message rate R_{p1}, i.e., if $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ is achievable, $(R_{p1}+\alpha, R_{s1}, R_{p2}-\alpha, R_{s2})$ is also achievable for any non-negative α satisfying $\alpha \leq R_{p2}$.

Besides obtaining the achievable rate region in Corollary 12 from Theorem 12, an alternative derivation can be provided by using Corollary 8, where an achievable rate region is given for the degraded multi-receiver wiretap channel. This alternative derivation corresponds to the evaluation of the achievable rate region in Corollary 8 for the degraded Gaussian MIMO multi-receiver wiretap channel by using the following selection of U and $\mathbf{X}$: i) U is a zero-mean Gaussian random vector with covariance matrix $\mathbf{S}-\mathbf{K}$ and ii) $\mathbf{X}=U+U'$ where U' is a zero-mean Gaussian random vector with covariance matrix $\mathbf{K}$, and is independent of U. We note that besides this jointly Gaussian $(U,\mathbf{X})$ selection, there might be other possible $(U,\mathbf{X})$ selections which may yield a larger region than the one obtained by using jointly Gaussian $(U,\mathbf{X})$. However, it is shown in [33] and [34] that jointly Gaussian $(U,\mathbf{X})$ selection is sufficient to evaluate the achievable rate region in Corollary 8 for the degraded Gaussian MIMO wiretap channel. In other words, jointly Gaussian $(U,\mathbf{X})$ selection exhausts the achievable rate region in Corollary 8 for the degraded Gaussian MIMO multi-receiver wiretap channel. This sufficiency result is stated in the following theorem.

Theorem 14 ([33], [34]) For the degraded Gaussian multi-receiver wiretap channel, the achievable rate region in Corollary 8 is exhausted by jointly Gaussian $(U,\mathbf{X})$. In particular, for any non-Gaussian $(U,\mathbf{X})$, there exists a Gaussian $(U^G,\mathbf{X}^G)$ which yields a larger region than the one obtained by using the non-Gaussian $(U,\mathbf{X})$.

Next, we provide an outer bound for the capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel. This outer bound can be obtained by evaluating the outer bound given in Theorem 11 for the degraded Gaussian MIMO multi-receiver wiretap channel. This evaluation is tantamount to find the optimal $(U,\mathbf{X})$ which exhausts the outer bound in Theorem 11 for the degraded Gaussian MIMO multi-receiver wiretap channel. In [33] and [34], it is shown that jointly Gaussian $(U,\mathbf{X})$ is sufficient to exhaust the outer bound in Theorem 11. The corresponding outer bound is stated in the following theorem.

Theorem 15 ([33], [34]) The capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel is contained in the union of rate tuples $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ satisfying

$$R_{s2} \leq \frac{1}{2}\log\frac{|\mathbf{H}_2\mathbf{S}\mathbf{H}_2^\top+\mathbf{I}|}{|\mathbf{H}_2\mathbf{K}\mathbf{H}_2^\top+\mathbf{I}|}-\frac{1}{2}\log\frac{|\mathbf{H}_Z\mathbf{S}\mathbf{H}_Z^\top+\mathbf{I}|}{|\mathbf{H}_Z\mathbf{K}\mathbf{H}_Z^\top+\mathbf{I}|}, \tag{141}$$

$$R_{s1}+R_{s2} \leq \frac{1}{2}\log\frac{|\mathbf{H}_2\mathbf{S}\mathbf{H}_2^\top+\mathbf{I}|}{|\mathbf{H}_2\mathbf{K}\mathbf{H}_2^\top+\mathbf{I}|}+\frac{1}{2}\log|\mathbf{H}_1\mathbf{K}\mathbf{H}_1^\top+\mathbf{I}| - \frac{1}{2}\log|\mathbf{H}_Z\mathbf{S}\mathbf{H}_Z^\top+\mathbf{I}|, \tag{142}$$

$$R_{s2}+R_{p2} \leq \frac{1}{2}\log\frac{|\mathbf{H}_2\mathbf{S}\mathbf{H}_2^\top+\mathbf{I}|}{|\mathbf{H}_2\mathbf{K}\mathbf{H}_2^\top+\mathbf{I}|}, \tag{143}$$

$$\sum_{j=1}^{2} R_{sj}+R_{pj} \leq \frac{1}{2}\log\frac{|\mathbf{H}_2\mathbf{S}\mathbf{H}_2^\top+\mathbf{I}|}{|\mathbf{H}_2\mathbf{K}\mathbf{H}_2^\top+\mathbf{I}|} + \frac{1}{2}\log|\mathbf{H}_1\mathbf{K}\mathbf{H}_1^\top+\mathbf{I}| \tag{144}$$

where $\mathbf{K}$ is a positive semi-definite matrix satisfying $\mathbf{K}\preceq\mathbf{S}$.

We note that the only difference between the inner and the outer bounds for the degraded Gaussian MIMO multi-receiver wiretap given in Corollary 12 and Theorem 15, respectively, comes from the bound in (135). In other words, there is one more constraint in the inner bound given by Corollary 12 than the outer bound given by Theorem 15. This additional constraint is

$$R_{s1}+R_{s2}+R_{p2} \leq \frac{1}{2}\log\frac{|\mathbf{H}_2\mathbf{S}\mathbf{H}_2^\top+\mathbf{I}|}{|\mathbf{H}_2\mathbf{K}\mathbf{H}_2^\top+\mathbf{I}|} + \frac{1}{2}\log|\mathbf{H}_1\mathbf{K}\mathbf{H}_1^\top+\mathbf{I}| - \frac{1}{2}\log|\mathbf{H}_Z\mathbf{K}\mathbf{H}_Z^\top+\mathbf{I}|. \tag{145}$$

Besides this constraint on $R_{s1}+R_{s2}+R_{p2}$, both the inner bound in Corollary 12 and the outer bound in Theorem 15 are the same.

We conclude this section by providing the cases where the inner bound in Corollary 12 and the outer bound in Theorem 15 match. Indeed, one such case is already presented in Theorem 13, which provides the secrecy capacity region of the general, not necessarily degraded, Gaussian MIMO multi-receiver wiretap channel. Thus, the inner bound in Corollary 12 and the outer bound in Theorem 15 match on the secrecy capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel. Next, we present two other cases where these inner and outer bounds match. The first scenario where the inner bound in Corollary 12 and the outer bound in Theorem 15 match can be obtained by setting the confidential message rate of the first legitimate user to zero, i.e., $R_{s1}=0$. The corresponding capacity region is given by the following corollary.

Corollary 13 ([33], [34]) The capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel without the first legitimate user's confidential message rate is given by the union of rate tuples (R_{p1}, R_{p2}, R_{s2}) satisfying

$$R_{s2} \leq \frac{1}{2}\log\frac{|\mathbf{H}_2\mathbf{S}\mathbf{H}_2^\top+\mathbf{I}|}{|\mathbf{H}_2\mathbf{K}\mathbf{H}_2^\top+\mathbf{I}|} - \frac{1}{2}\log\frac{|\mathbf{H}_Z\mathbf{S}\mathbf{H}_Z^\top+\mathbf{I}|}{|\mathbf{H}_Z\mathbf{K}\mathbf{H}_Z^\top+\mathbf{I}|}, \tag{146}$$

$$R_{s2}+R_{p2} \leq \frac{1}{2}\log\frac{|\mathbf{H}_2\mathbf{S}\mathbf{H}_2^\top+\mathbf{I}|}{|\mathbf{H}_2\mathbf{K}\mathbf{H}_2^\top+\mathbf{I}|}, \tag{147}$$

$$R_{s2}+\sum_{j=1}^{2} R_{pj} \leq \frac{1}{2}\log\frac{|\mathbf{H}_2\mathbf{S}\mathbf{H}_2^\top+\mathbf{I}|}{|\mathbf{H}_2\mathbf{K}\mathbf{H}_2^\top+\mathbf{I}|} + \frac{1}{2}\log|\mathbf{H}_1\mathbf{K}\mathbf{H}_1^\top+\mathbf{I}| \tag{148}$$

where $\mathbf{K}$ is a positive semi-definite matrix satisfying $\mathbf{K}\preceq\mathbf{S}$.

We note that Corollary 13 is the Gaussian MIMO version of Corollary 9 which obtains the capacity region of the degraded discrete memoryless multi-receiver wiretap channel without the first legitimate user's confidential message. Corollary 13 can be

proved by setting $R_{s1} = 0$ in both Corollary 12 and Theorem 15 and eliminating the redundant bounds.

The last scenario where the inner bound in Corollary 12 and the outer bound in Theorem 15 match can be obtained by setting the public message rate of the second legitimate user to zero, i.e., $R_{p2} = 0$. The corresponding capacity region is stated in the following corollary.

Corollary 14 ([33], [34]) The capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel without the second legitimate user's public message is given by the union of rate tuples (R_{p1}, R_{s1}, R_{s2}) satisfying

$$R_{s2} \leq \frac{1}{2}\log\frac{|\mathbf{H}_2\mathbf{S}\mathbf{H}_2^\top + \mathbf{I}|}{|\mathbf{H}_2\mathbf{K}\mathbf{H}_2^\top + \mathbf{I}|} - \frac{1}{2}\log\frac{|\mathbf{H}_Z\mathbf{S}\mathbf{H}_Z^\top + \mathbf{I}|}{|\mathbf{H}_Z\mathbf{K}\mathbf{H}_Z^\top + \mathbf{I}|}, \tag{149}$$

$$R_{s1} + R_{s2} \leq \frac{1}{2}\log\frac{|\mathbf{H}_2\mathbf{S}\mathbf{H}_2^\top + \mathbf{I}|}{|\mathbf{H}_2\mathbf{K}\mathbf{H}_2^\top + \mathbf{I}|} + \frac{1}{2}\log|\mathbf{H}_1\mathbf{K}\mathbf{H}_1^\top + \mathbf{I}| - \frac{1}{2}\log|\mathbf{H}_Z\mathbf{S}\mathbf{H}_Z^\top + \mathbf{I}|, \tag{150}$$

$$\sum_{j=1}^{2} R_{sj} + R_{p1} \leq \frac{1}{2}\log\frac{|\mathbf{H}_2\mathbf{S}\mathbf{H}_2^\top + \mathbf{I}|}{|\mathbf{H}_2\mathbf{K}\mathbf{H}_2^\top + \mathbf{I}|} + \frac{1}{2}\log|\mathbf{H}_1\mathbf{K}\mathbf{H}_1^\top + \mathbf{I}| \tag{151}$$

where $\mathbf{K}$ is a positive semi-definite matrix satisfying $\mathbf{K} \preceq \mathbf{S}$.

We note that Corollary 14 is the Gaussian MIMO version of Corollary 10 which obtains the capacity region of the degraded discrete memoryless multi-receiver wiretap channel without the second legitimate user's public message. Corollary 14 can be proved by setting $R_{p2} = 0$ in both Corollary 12 and Theorem 15 and eliminating the redundant bounds.

V. COMPOUND WIRETAP CHANNELS

Similar to the previous sections, here also we first consider the discrete memoryless compound wiretap channel. We start with the following achievable secrecy rate for the discrete memoryless compound wiretap channel.

Theorem 16 ([5]) For the discrete memoryless compound wiretap channel, the following secrecy rate is achievable

$$\max \min_{j,k} I(V;Y_j) - I(V;Z_k) \tag{152}$$

where the maximization is over all (V, X) which satisfy the following Markov chain

$$V \to X \to Y_j, Z_k \tag{153}$$

for any (j, k) pair.

This achievable secrecy rate can be seen as the generalization of Csiszar-Korner's achievable secrecy rate for the broadcast channel with only one confidential message [2] to the compound setting. If we fix a (j, k) pair, due to [2], the following

$$I(V;Y_j) - I(V;Z_k) \tag{154}$$

is an achievable secrecy rate. Thus, following their footsteps, one expects to achieve the secrecy rate given in Theorem 16 because, intuitively, the secrecy rate in Theorem 16 considers the worst (j, k) pair by taking a minimization of (154) over all (j, k) pairs. Although this explanation seems to be intuitively correct, there is a subtlety which arises from the fact that there needs to exist a single codebook which needs to achieve a certain fixed secrecy rate in all of the underlying wiretap channels associated with the compound wiretap channel. In other words, if there is a codebook which provides the secrecy rate in (154) in the wiretap channel indexed by (j, k), this codebook might not achieve the following secrecy rate

$$I(V;Y_{j'}) - I(V;Z_{k'}) \tag{155}$$

in the wiretap channel indexed by (j', k'). Thus, this intuitive argument is not technically correct. To show the existence of a codebook which provides the secrecy rate in (152) in all of the underlying wiretap channels associated with the compound wiretap channel is the key part of the proof of Theorem 16. To show the existence of such a codebook, random binning and channel pre-fixing are used. First, the achievability of the following secrecy rate

$$\max_{X} \min_{j,k} I(X;Y_j) - I(X;Z_k) \tag{156}$$

is shown. To this end, a codebook of size $2^{n(R+\tilde{R})}$ is generated by using X. The codewords in this codebook have double indices, where one index, with rate R, carries the confidential message, and the other index, with rate $\tilde{R}$, has no information content, and has the sole purpose of providing the necessary protection for the confidential part. Until now, the codebook generation is identical to the one in Csisar-Korner [2]. The difference of the codebook in [5] from the one in [2] comes from the adjustment of the rates R and $\tilde{R}$. Since $\tilde{R}$ is the dummy index sent to protect the confidential message, it needs to be set according the best eavesdropper, namely its rate should be $\max_k I(X;Z_k)$. Since all legitimate users needs to decode the codewors, the total rate $R + \tilde{R}$ needs to be adjusted according to the worst legitimate user, namely the total rate $R + \tilde{R}$ needs to be $\min_j I(X;Y_j)$. These selections ensure both the reliability and the security of the confidential messages yielding (156) as an achievable secrecy rate. Finally, the achievability of the secrecy rate in Theorem 16 is concluded by the use of channel pre-fixing [2].

The lower bound in Theorem 16 is not tight in general, as it was shown in [41]. In [41], the compound wiretap channel with two legitimate users and one eavesdropper, i.e., $K_Y = 2$ and $K_Z = 1$, is considered, and the following achievable secrecy rate is provided.

Theorem 17 ([41]) The secrecy capacity of the two-user one-eavesdropper discrete memoryless compound wiretap channel is lower bounded by the maximum of R satisfying

$$R \leq I(V_0, V_1; Y_1) - I(V_0, V_1; Z), \tag{157}$$

$$R \leq I(V_0, V_2; Y_2) - I(V_0, V_2; Z) \tag{158}$$

for some (V_0, V_1, V_2) such that $(V_0, V_1, V_2) \to X \to$

(Y_1, Y_2, Z), and

$$I(V_1, V_2; Z|V_0) + I(V_1; V_2|V_0) \leq I(V_1; Z|V_0) + I(V_2; Z|V_0). \tag{159}$$

This achievable secrecy rate is obtained by using indirect decoding [42] and Marton's coding [13]. First, a codebook of size $2^{n(R+\tilde{R})}$ is generated by using V_0, and next for each V_0^n, a codebook of size $2^{n\tilde{R}_j}$ is generated by using V_j, $j = 1, 2$, where V_1^n and V_2^n are encoded by Marton's coding. Here, R denotes the rate of the confidential messages, and $\tilde{R}$, $\tilde{R}_1$, and $\tilde{R}_2$ denote the rates of the dummy messages whose sole purpose is to protect the confidential messages. The jth legitimate user estimates the transmitted confidential message by jointly decoding V_0^n, and V_j^n. Thus, here the same confidential message is transmitted to each legitimate user by different codewords, as opposed to the transmission by a single codeword in Theorem 16. This approach turns out to be more useful in the sense that it provides higher secrecy rates than Theorem 16 can provide because of the more randomness injected to the channel. In particular, in [41], an example is provided to show that the achievable secrecy rate given in Theorem 17 is strictly larger than the achievable secrecy rate given in Theorem 16. Thus, the lower bound in Theorem 16 is not the secrecy capacity of the compound wiretap channel.

In [43], a new achievable secrecy rate for the two-user one-eavesdropper compound wiretap channel is provided, and it is shown that this achievable secrecy rate is potentially better than the achievable secrecy rate in Theorem 17. This potentially better achievable scheme in [43] is similar to the achievable scheme given in Theorem 17 in terms of the techniques used. In particular, the achievable scheme in [43] also uses indirect decoding [42] and Marton's coding [13]. The only new ingredient in this potentially better achievable scheme, as compared to the achievable scheme in Theorem 17, is the computation of the equivocation rate, i.e., the method [43] uses to show that the perfect secrecy requirement on the confidential message given by (18) is satisfied. In particular, while computing the equivocation rate in the proof of Theorem 17, one needs to show the following

$$\lim_{n\to\infty} \frac{1}{n} H(V_1^n, V_2^n|W, V_0^n, Z^n) = 0. \tag{160}$$

Reference [41] shows that (160) is satisfied by using the following bound

$$\frac{1}{n} H(V_1^n, V_2^n|W, V_0^n, Z^n) \leq \frac{1}{n} H(V_1^n|W, V_0^n, Z^n) + \frac{1}{n} H(V_2^n|W, V_0^n, Z^n) \tag{161}$$

which might result in potential suboptimality in the achievable secrecy rate given in Theorem 17 as compared to the achievable secrecy rate that can be obtained by directly showing (160) without any recourse to the bound in (161). The corresponding new achievable secrecy rate, obtained by showing (160) without using the bound in (161), is given in the following theorem.

Theorem 18 ([43]) The secrecy capacity of the two-user one-eavesdropper discrete memoryless compound wiretap channel is lower bounded by the maximum of R satisfying

$$R \leq I(V_0, V_1; Y_1) - I(V_0, V_1; Z), \tag{162}$$

$$R \leq I(V_0, V_2; Y_2) - I(V_0, V_2; Z), \tag{163}$$

$$2R \leq I(V_0, V_1; Y_1) + I(V_0, V_2; Y_2) - 2I(V_0; Z) - I(V_1, V_2; Z|V_0) - I(V_1; V_2|V_0) \tag{164}$$

for some (V_0, V_1, V_2) such that $(V_0, V_1, V_2) \rightarrow X \rightarrow (Y_1, Y_2, Z)$.

We note that the achievable secrecy rate given in Theorem 18 has one more rate constraint than the achievable secrecy rate given in Theorem 17, while both achievable secrecy rates have two rate constraints (162)–(163) in common. On the other hand, the new achievable secrecy rate in Theorem 18 does not have the constraint in (159) that Theorem 17 has. In [43], it is shown that any secrecy rate achievable by Theorem 17 is also achievable by Theorem 18, and there might be achievable secrecy rates which can be achieved by Theorem 18 and cannot be achieved by Theorem 17, because of the constraint in (159).

Next, we provide the existing outer bounds for the compound wiretap channel. The first outer bound can be obtained by noting the facts that there are $K_Y \times K_Z$ wiretap channels associated with a compound wiretap channel with K_Y legitimate users and K_Z eavesdroppers, and the secrecy capacity of the compound wiretap channel cannot be larger than the minimum of the secrecy capacities of these $K_Y \times K_Z$ wiretap channels. This argument leads to the following outer bound.

Theorem 19 ([5]) The secrecy capacity of the compound wiretap channel is upper bounded by

$$\min_{j,k} \max I(V; Y_j) - I(V; Z_k) \tag{165}$$

where the maximization is over all (V, X) satisfying $V \rightarrow X \rightarrow Y_j, Z_k$, $\forall(j, k)$. In other words, the secrecy capacity of the compound wiretap channel is upper bounded by the minimum of the secrecy capacities of all underlying wiretap channels associated with the compound wiretap channel.

In general, it is not expected that the outer bound in Theorem 19 is equal to the secrecy capacity of the compound wiretap channel because of the fact that if a certain (V, X) achieves the secrecy capacity of the (j, k)th wiretap channel in the compound channel, it might not achieve the secrecy capacities of all other wiretap channels associated with the compound wiretap channel. In other words, if a codebook attains the secrecy capacity of the (j, k)th wiretap channel in the compound channel, the same codebook might not perform in the other wiretap channels associated with the compound wiretap channel as well as it performs in the (j, k)th wiretap channel, i.e., it might not simultaneously achieve the secrecy capacities of all of the underlying wiretap channels in the compound wiretap channel.

Next, we present another outer bound for the secrecy capacity of the compound wiretap channel.

Theorem 20 ([44]) The secrecy capacity of the compound wiretap channel is upper bounded by

$$\max \min_{j,k} I(X; Y_j|Z_k) \tag{166}$$

where the maximization is over all X.

This outer bound considers the (j, k)th wiretap channel in the compound channel, and enhances this wiretap channel by providing the eavesdropper's observation to the legitimate user. For

a fixed input distribution on X, the achievable secrecy rate is shown to be upper bounded by $I(X;Y_j|Z_k)$ for this (j,k)th wiretap channel. Finally, taking the minimum of $I(X;Y_j|Z_k)$ over all possible (j,k) pairs leads to an upper bound for the secrecy capacity of the compound wiretap channel, as stated in Theorem 20.

Although the secrecy capacity of the compound wiretap channel is unknown in general, there are special instances of the compound wiretap channel, for which the secrecy capacity is known. The first instance is the degraded compound wiretap channel. The secrecy capacity of the degraded compound wiretap channel is stated in the following theorem.

Theorem 21 ([5]) The secrecy capacity of the degraded compound wiretap channel is given by

$$\max \min_{j,k} I(X;Y_j) - I(X;Z_k) \tag{167}$$

where the maximization is over all X.

The achievability of the secrecy rate in Theorem 21 can be shown by setting $V = X$ in Theorem 16. The converse proof for Theorem 21 follows from Theorem 20 by noting the Markov chain $X \to Y_j \to Z_k$, $\forall(j,k)$. The second instance of the compound wiretap channel, for which the secrecy capacity is known, is a special class of parallel compound wiretap channels with $K_Z = 1$. In this special compound wiretap channel, there is only one eavesdropper, and an arbitrary number of legitimate users, where the channel between the transmitter and the receivers constitute L independent parallel channels. In other words, the channel transition probability is given by

$$p\left(\{y_{1\ell},\cdots,y_{K_Y\ell},z_\ell\}_{\ell=1}^L|\{x_\ell\}_{\ell=1}^L\right) = \prod_{\ell=1}^L p\left(y_{1\ell},\cdots,y_{K_Y\ell},z_\ell|x_\ell\right) \tag{168}$$

where x_ℓ is the channel input of the ℓth parallel channel, $y_{j\ell}$ is the channel output of the ℓth parallel channel at the jth legitimate user, and z_ℓ is the channel output of the ℓth parallel channel at the eavesdropper. This special class of parallel compound wiretap channels exhibits a certain degradation order in each parallel channel as follows

$$X \to Y_{j_1\ell}\cdots \to Z_\ell \to \cdots \to Y_{j_{K_y}\ell}, \quad \ell = 1,\cdots,L \tag{169}$$

where $j_1, j_2, \cdots, j_{K_Y}$ is a permutation of $1,\cdots,K_Y$, and can be different in each parallel channel. This special class of parallel compound wiretap channels is called the reversely degraded parallel compound wiretap channel [45], for which the secrecy capacity is stated in the following theorem.

Theorem 22 ([45]) The secrecy capacity of the reversely degraded parallel compound wiretap channel is given by

$$\max \min_j \sum_{\ell=1}^L I(X_\ell;Y_{j\ell}|Z_\ell) \tag{170}$$

where the maximization is over all input distributions of the form $p(x_1,\cdots,x_L) = \prod_{\ell=1}^L p(x_\ell)$.

The achievability of this secrecy rate can be shown by using the codebook in [45], where this codebook consists of L independent sub-codebooks, each of which is used for a parallel channel. The size of the ℓth codebook is $2^{n(R+I(X_\ell;Z_\ell))}$, where the rate $I(X_\ell;Z_\ell)$ is the rate of the dummy messages sent to protect the confidential message, and R is the rate of the confidential message. Thus, the rate of the confidential messages is not split into L sub-rates, instead, the entire confidential message is sent over each parallel channel. The converse proof of Theorem 22 can be obtained by specializing the outer bound in Theorem 20 to the reversely degraded parallel compound wiretap channel.

A. Gaussian Compound Wiretap Channels

Here, we investigate the Gaussian compound wiretap channel. First we start with the Gaussian parallel compound wiretap channel which can be defined as[10]

$$Y_{j\ell} = h_{j\ell}^Y X_\ell + N_{j\ell}, \quad j = 1,\cdots,K_Y \tag{171}$$

$$Z_{k\ell} = h_{k\ell}^Z X_\ell + N_{k\ell}, \quad k = 1,\cdots,K_Z \tag{172}$$

where $\ell = 1,\cdots,L$ denotes the index of the parallel channel, and $N_{j\ell}$ and $N_{k\ell}$ are the zero-mean unit-variance Gaussian random variables, and are independent across the parallel channels. The channel input is subject to a power constraint as follows

$$\sum_{\ell=1}^L E\left[X_\ell^2\right] \le P. \tag{173}$$

The secrecy capacity of the Gaussian parallel compound wiretap channel is unknown in general. However, the secrecy capacity is known when i) $K_Y = 1$ and K_Z is arbitrary and ii) K_Y is arbitrary and $K_Z = 1$. The secrecy capacity of the case $K_Y = 1$ and K_Z is arbitrary is stated in the following theorem.

Theorem 23 ([44]) The secrecy capacity of the Gaussian parallel compound wiretap channel with $K_Y = 1$ and arbitrary K_Z is given by

$$\max \min_k \frac{1}{2}\sum_{\ell=1}^L \left[\log\left(1+\left(h_\ell^Y\right)^2 P_\ell\right) - \log\left(1+\left(h_{k\ell}^Z\right)^2 P_\ell\right)\right]^+ \tag{174}$$

where the maximization is over all non-negative $P_1,\cdots,P_L$ satisfying $\sum_{\ell=1}^L P_\ell = P$.

The achievability of this theorem is shown by adapting the achievable scheme proposed in [46] for the wiretap II channel to the Gaussian parallel compound wiretap channel with $K_Y = 1$ and arbitrary K_Z. The converse proof can be shown by using the outer bound in Theorem 20.

Next, we consider the Gaussian parallel compound wiretap channel with $K_Z = 1$ and arbitrary K_Y. Indeed, this Gaussian parallel compound wiretap channel is an instance of the reversely degraded compound wiretap channel for which the secrecy capacity is known in a single-letter form as stated in Theorem 22. Evaluation of this single-letter expression provides us

[10]The Gaussian parallel compound wiretap channel corresponds to a special case of the Gaussian MIMO compound wiretap channel. The parallel channel can be obtained from the Gaussian MIMO channel by taking all channel gain matrices $\mathbf{H}_j^Y$ and $\mathbf{H}_k^Z$ as $L \times L$ diagonal matrices.

the secrecy capacity of the Gaussian parallel compound wiretap channel with $K_Z = 1$ and arbitrary K_Y as follows.

Theorem 24 ([45]) The secrecy capacity of the Gaussian parallel compound wiretap channel with $K_Z = 1$ and arbitrary K_Y is given by

$$\max \min_j \frac{1}{2} \sum_{\ell=1}^{L} \left[\log\left(1 + \left(h_{j\ell}^Y\right)^2 P_\ell\right) - \log\left(1 + \left(h_\ell^Z\right)^2 P_\ell\right) \right]^+ \tag{175}$$

where the maximization is over all non-negative $P_1, \cdots, P_L$ satisfying $\sum_{\ell=1}^{L} P_\ell = P$.

Next, we consider the Gaussian MIMO compound wiretap channel. We note that the secrecy capacity of the general, not necessarily degraded, Gaussian MIMO compound wiretap channel is unknown. However, the secrecy capacity of the degraded Gaussian MIMO compound wiretap channel is known as stated in the following theorem.

Theorem 25 ([5]) The secrecy capacity of the degraded Gaussian MIMO compound wiretap channel is given by

$$\min_{j,k} \frac{1}{2} \log |\mathbf{H}_j^Y \mathbf{S} (\mathbf{H}_j^Y)^\top + \mathbf{I}| - \frac{1}{2} \log |\mathbf{H}_k^Z \mathbf{S} (\mathbf{H}_k^Z)^\top + \mathbf{I}|. \tag{176}$$

We note that due to Theorem 21, the single-letter form of the secrecy capacity of the degraded compound wiretap channel is known. To obtain the secrecy capacity of the degraded Gaussian MIMO compound wiretap channel, one needs to find the optimal input distribution for $\mathbf{X}$ that attains the maximum for the single-letter formula given in Theorem 21. This is accomplished in [5] by showing that Gaussian $\mathbf{X}$ with covariance matrix $\mathbf{S}$ is the maximizer for this single-letter formula.

As we noted before, the secrecy capacity of the general, non-degraded, Gaussian MIMO compound wiretap channel is unknown in general. However, using either Theorem 16 or Theorem 18, lower bounds for the secrecy capacity of the general Gaussian MIMO compound wiretap channel can be provided. In particular, using Theorem 16, the following lower bound is provided in [5].

Theorem 26 ([5]) A lower bound for the secrecy capacity of the general Gaussian MIMO compound wiretap channel is given by

$$\max \min_{j,k} \frac{1}{2} \log |\mathbf{H}_j^Y \mathbf{K} (\mathbf{H}_j^Y)^\top + \mathbf{I}| - \frac{1}{2} \log |\mathbf{H}_k^Z \mathbf{K} (\mathbf{H}_k^Z)^\top + \mathbf{I}| \tag{177}$$

where the maximization is over all positive semi-definite matrices $\mathbf{K}$ satisfying $\mathbf{K} \preceq \mathbf{S}$.

This lower bound can be obtained from Theorem 16 by setting $V = \mathbf{X}$, and selecting $\mathbf{X}$ as a zero-mean Gaussian random vector with covariance matrix $\mathbf{K}$. The lower bound in Theorem 26 is further investigated in [5] to obtain some achievable secure degrees of freedom[11]. In particular, [5] proposes a linear beamforming scheme which corresponds to a special selection of the covariance matrix $\mathbf{K}$ in Theorem 26, and obtains the corresponding secure degrees of freedom. A similar approach is also taken in [47], where the general Gaussian multi-input single output (MISO) compound wiretap channel, i.e., the transmitter has multiple antennas whereas the legitimate users and the eavesdroppers have single antenna each, is studied. Reference [47] considers the lower bound in Theorem 16 and evaluates it by using interference alignment, i.e., V and $\mathbf{X}$ are selected according to an interference alignment scheme [48], [49]. Similar to [5], [47] also focuses on the achievable secure degrees of freedom. In particular, [47] obtains an achievable secure degrees of freedom corresponding to the evaluation of the inner bound in Theorem 16 by using an interference alignment scheme [48], [49]. Moreover, [47] proposes outer bounds for the general Gaussian MISO compound wiretap channel, and obtains the maximum achievable secure degrees of freedom under certain cases which are determined by the number of transmitter antennas, the number of legitimate users, and the number of eavesdroppers.

Another lower bound for the secrecy capacity of the general Gaussian MIMO compound wiretap channel with two legitimate users and one eavesdropper can be obtained by using Theorem 18 as follows.

Theorem 27 ([43]) The secrecy capacity of the two-user one-eavesdropper Gaussian MIMO compound wiretap channel is lower bounded by the maximum of R satisfying

$$R = \max\left\{R_S^{12}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2), R_S^{21}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2)\right\} \tag{178}$$

for some positive semi-definite matrices $\mathbf{K}_0, \mathbf{K}_1$, and $\mathbf{K}_2$ such that $\mathbf{K}_0 + \mathbf{K}_1 + \mathbf{K}_2 \preceq \mathbf{S}$, and $R_S^{12}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2)$ is given by

$$R_S^{12}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2) = \min_{j=1,2} R_{Sj}^{12}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2) \tag{179}$$

where $R_{S1}^{12}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2)$ and $R_{S2}^{12}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2)$ are

$$\begin{aligned} R_{S1}^{12}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2) = &\frac{1}{2} \log \frac{|\mathbf{K}_0 + \mathbf{K}_1 + \mathbf{K}_2 + \mathbf{\Sigma}_1|}{|\mathbf{K}_2 + \mathbf{\Sigma}_1|} \\ &- \frac{1}{2} \log \frac{|\mathbf{K}_0 + \mathbf{K}_1 + \mathbf{K}_2 + \mathbf{\Sigma}_Z|}{|\mathbf{K}_2 + \mathbf{\Sigma}_Z|}, \end{aligned} \tag{180}$$

$$\begin{aligned} R_{S2}^{12}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2) = &\frac{1}{2} \log \frac{|\mathbf{K}_0 + \mathbf{K}_1 + \mathbf{K}_2 + \mathbf{\Sigma}_1|}{|\mathbf{K}_1 + \mathbf{K}_2 + \mathbf{\Sigma}_2|} \\ &- \frac{1}{2} \log \frac{|\mathbf{K}_0 + \mathbf{K}_1 + \mathbf{K}_2 + \mathbf{\Sigma}_Z|}{|\mathbf{K}_1 + \mathbf{K}_2 + \mathbf{\Sigma}_Z|} \\ &+ \frac{1}{2} \log \frac{|\mathbf{K}_2 + \mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_2|} - \frac{1}{2} \log \frac{|\mathbf{K}_2 + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|}. \end{aligned} \tag{181}$$

We note that $R_S^{21}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2)$ can be obtained from $R_S^{12}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2)$ by swapping the indices 1 and 2.

This lower bound can be obtained from Theorem 18 in two steps. In the first step, Theorem 18 is used to show the achievability of the following rate

$$R = \max\left\{R_S^{12}, R_S^{21}\right\} \tag{182}$$

for some (V_0, V_1, V_2) such that $(V_0, V_1, V_2) \rightarrow X \rightarrow (Y_1, Y_2, Z)$, and R_S^{12} and R_S^{21} are given by

$$R_S^{12} = \min\{I(V_0, V_1; Y_1) - I(V_0, V_1; Z),$$

[11] A secure degrees of freedom d is said to be achievable if there is an achievable secrecy rate R such that $d = \lim_{P\to\infty} \frac{R}{\frac{1}{2}\log P}$. Thus, the secure degrees of freedom represents the scaling of the secrecy rate with $\frac{1}{2}\log P$ as $P \rightarrow \infty$.

$$I(V_0, V_2; Y_2) - I(V_0; Z) - I(V_2; Z, V_1|V_0)\}, \quad (183)$$

$$R_S^{21} = \min\{I(V_0, V_1; Y_1) - I(V_0; Z) - I(V_1; Z, V_2|V_0),$$
$$I(V_0, V_2; Y_2) - I(V_0, V_2; Z)\}. \quad (184)$$

In the second step, the achievable secrecy rate given by (182)–(184) is evaluated for the Gaussian MIMO compound wiretap channel by using a jointly Gaussian selection of V_0, V_1, and V_2 with a specific correlation structure. In particular, V_0 is selected as a zero-mean Gaussian random vector with covariance matrix $\mathbf{K}_0$, and V_1 and V_2 are encoded by using DPC. Reference [43] further studies the lower bound in Theorem 27 and shows that it achieves at least half of the minimum of secrecy capacities of the underlying two Gaussian MIMO wiretap channels in the two-user one-eavesdropper Gaussian MIMO compound wiretap channel. Moreover, [43] obtains the secrecy capacity of a class of two-user one-eavesdropper Gaussian MIMO compound wiretap channels, where for the channels in this class, the eavesdropper is degraded with respect to one of the two legitimate users, and there is no degradedness relationship between the eavesdropper and the other legitimate user.

B. Compound Wiretap Channels with Multiple Confidential Messages

Until now, we considered compound wiretap channels for the scenario where there is only one confidential message that needs to be transmitted both reliably and securely. In this section, we consider a more general scenario where there are more than one group of legitimate users, and the transmitter multicasts a different confidential message to each group of legitimate users. In the literature, there are two models which consider the multicast of more than one confidential message: i) The compound broadcast channel with confidential messages [47], [50] and ii) the compound multi-receiver wiretap channel [51], [52].

In the compound broadcast channel with confidential messages, there is a transmitter and two groups of users, where each group treats the other group as a collection of eavesdroppers. In this model, the transmitter sends a confidential message to each group of users, and this message needs to be kept perfectly secret from the other group of users. This channel model is investigated in [47] and [50]. Reference [50] first considers the discrete memoryless compound broadcast channels and proposes an achievable secrecy rate region by extending the achievable secrecy rate region given in Theorem 1 to the compound setting. Next, [50] studies the Gaussian MIMO compound broadcast channel and obtains an achievable secure degrees of freedom region by evaluating their achievable secrecy rate region, the one proposed for the discrete memoryless channel, for the Gaussian MIMO channel with a linear beamforming scheme. Reference [47] considers the Gaussian MISO compound channel with confidential messages, i.e., the transmitter has multiple antennas whereas all receivers are equipped with a single antenna each, for the sum secrecy rate. Reference [47] evaluates the achievable sum secrecy, that can be obtained from the achievable scheme proposed in [50] for the discrete memoryless channel, using an interference alignment scheme [48], [49], and obtains the achievable secure degrees of freedom for the sum secrecy rate. Moreover, [47] proposes outer bounds for the secure degrees of freedom of the sum secrecy rate.

In the compound multi-receiver wiretap channel, there are a transmitter, two groups of legitimate users and a group of eavesdroppers. References [51] and [52] consider the *degraded* compound multi-receiver wiretap channel, where the legitimate users in the second (weaker) group are degraded with respect to the legitimate users in the first (stronger) group, and eavesdroppers are degraded with respect to the legitimate users in the second group. References [51] and [52] study this degraded channel under two scenarios. In the first scenario, the transmitter sends a confidential message to each group of legitimate users where these messages need to be kept perfectly hidden from all eavesdroppers. In the second scenario, the transmitter again sends a confidential message to each group of legitimate users, where the message of the stronger group needs to be kept perfectly hidden from the weaker group in addition to all eavesdroppers, and the message of the weaker group needs to be kept perfectly secret from all eavesdroppers. References [51] and [52] obtain the secrecy capacity regions corresponding to both scenarios for both the discrete memoryless and the Gaussian MIMO channel under certain conditions on the number of users in each group and on the number of eavesdroppers.

VI. CONCLUSIONS

In this paper, we provided a survey of the literature for three forms of secure broadcasting problems, namely the broadcast channels with common and confidential messages, multi-receiver wiretap channels, and compound wiretap channels, by focusing on the Gaussian MIMO channel models more closely. We also considered the discrete memoryless channel models for these three secure broadcasting problems, as the discrete memoryless models often serve as intermediate steps to obtain information-theoretic results for the Gaussian MIMO channel models. We provided and explained the current capacity results, existing inner and outer bounds for these three forms of secure broadcasting problems. We described the main information-theoretic tools and approaches used to obtain these results with pointers to the works where these tools and approaches were originally devised.

REFERENCES

[1] A. Wyner, "The wire-tap channel," *Bell Syst. Technical 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. 24, no. 3, pp. 339–348, May 1978.

[3] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Foundations and Trends in Commun. Inf. Theory*, vol. 5, no. 4-5, pp. 355–380, 2008.

[4] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Physical layer security in broadcast networks," *Security and Commun. Netw.*, vol. 2, no. 3, pp. 227–238, May/June 2009.

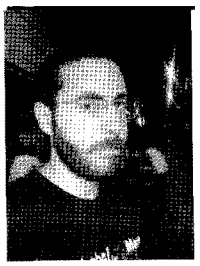
[5] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz), "Compound wire-tap channels," *EURASIP J. Wireless Commun. Netw. (Special Issue on Wireless Physical Layer Security)*, 2009.

[6] S. K. L.-Y. Cheong, and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, July 1978.

[7] 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, Sept. 2010.

[8] E. Ekrem and S. Ulukus. The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel. Submitted to *IEEE Trans. Inf. Theory.* [Online]. Available: http://arXiv.org/abs/0903.3096

[9] E. Ekrem and S. Ulukus, "Gaussian MIMO multi-receiver wiretap channel," in *Proc. IEEE GLOBECOM*, Nov. 2009.
[10] 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, Sept. 2006.
[11] 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.
[12] 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.
[13] K. Marton, "A coding theorem for the discrete memoryless channels," *IEEE Trans. Inf. Theory*, vol. 25, no. 1, pp. 306–311, May 1979.
[14] W. Yu and J. Cioffi, "Sum capacity of Gaussian vector broadcast channels," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 1875–1892, Sept. 2004.
[15] E. Ekrem and S. Ulukus. (2010, Apr.). Capacity-equivocation region of the Gaussian MIMO wiretap channel. Submitted to *IEEE Trans. Inf. Theory*. [Online]. Available: http://arXiv.org/abs/1005.0419
[16] E. Ekrem and S. Ulukus, "Transmission of common, public and confidential messages in broadcast channels with multiple antennas," in *Proc. IEEE PIMRC*, Sept. 2010.
[17] E. Ekrem and S. Ulukus. (2010, Feb.). Capacity region of the Gaussian MIMO broadcast channels with common and confidential messages. Submitted to *IEEE Trans. Inf. Theory*. [Online]. Available: http://arXiv.org/abs/1002.5026
[18] E. Ekrem and S. Ulukus, "Gaussian MIMO broadcast channels with common and confidential messages," in *Proc. IEEE ISIT*, June 2010.
[19] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz), "MIMO Gaussian broadcast channels with confidential and common messages," in *Proc. IEEE ISIT*, June. 2010.
[20] H. D. Ly, T. Liu, and Y. Liang. Multiple-input multiple-output Gaussian broadcast channels with common and confidential messages. Submitted to *IEEE Trans. Inf. Theory*. [Online]. Available: http://arXiv.org/abs/0907.2599
[21] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz), "The capacity-equivocation region of the MIMO Gaussian wiretap channel," in *Proc. IEEE ISIT*, June 2010.
[22] T. Cover and J. Thomas, *Elements of Information Theory*. 2nd ed., Wiley & Sons, 2006.
[23] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4033–4039, Sept. 2009.
[24] A. Khisti and G. Wornell. Secure transmission with multiple antennas I: The MIMO channel. Submitted to *IEEE Trans. Inf. Theory*. [Online]. Available: http://arXiv.org/abs/1006.5879
[25] F. Oggier and B. Hassibi. (2007, Oct.). The secrecy capacity of the MIMO wiretap channel. Submitted to *IEEE Trans. Inf. Theory*. [Online]. Available: http://arXiv.org/abs/0710.1920
[26] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multi-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, June 2009.
[27] H. Sato, "An outer bound to the capacity region of broadcast channels," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 374–377, May 1978.
[28] C. Paige and M. A. Saunders, "Towards a generalized singular value decomposition," *SIAM. J. Numer. Anal.*, June 1981.
[29] 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 J. Wireless Commun. Netw. (Special Isssue on Wireless Physical Layer Security)*, Dec. 2009.
[30] H. Weingarten, Y. Steinberg, and S. Shamai (Shitz), "On the capacity region of the multi-antenna broadcast channel with common messages," in *Proc. IEEE ISIT*, July 2006.
[31] H. Weingarten, *Multiple-input multiple-output broadcast systems*. Ph. D. thesis, Technion, Haifa, Israel, 2007.
[32] N. Jindal and A. Goldsmith, "Optimal power allocation for parallel broadcast channels with independent and common information," in *Proc. IEEE ISIT*, June 2004.
[33] E. Ekrem and S. Ulukus, "Gaussian MIMO multi-receiver wiretap channel with public and confidential messages," In preparation.
[34] E. Ekrem and S. Ulukus, "Degraded Gaussian MIMO multi-receiver wiretap channel with public and confidential messages," in *Proc. Allerton Conf. Commun., Control, and Comput.*, Sept.–Oct. 2010.
[35] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "The secrecy rate region of the broadcast channel," in *Proc. Allerton Conf. Commun., Control, and Comput.*, Sept. 2008.
[36] E. Ekrem and S. Ulukus, "Secrecy capacity of a class of broadcast channels with an eavesdropper," *EURASIP J. Wireless Commun. Netw. (Special Isssue on Wireless Physical Layer Security)*, Dec. 2009.
[37] E. Ekrem and S. Ulukus, "On secure broadcasting," in *Proc. Asilomar Conf. Signals, Syst. Comp.*, Oct. 2008.
[38] 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.
[39] N. M. Blachman, "The convolution inequality for entropy powers," *IEEE Trans. Inf. Theory*, vol. 11, no. 2, pp. 267–271, Apr. 1965.
[40] 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.
[41] Y-K. Chia and A. El Gamal. (2010, Oct.). 3-receiver broadcast channels with common and confidential messages. Submitted to *IEEE Trans. Inf. Theory*, [Online]. Available: http://arXiv.org/abs/0910.1407
[42] C. Nair and A. El Gamal, "The capacity region of a class of 3-receiver broadcast channels with degraded message sets," *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 4479–4493, Oct. 2009.
[43] E. Ekrem and S. Ulukus, "On Gaussian MIMO compound wiretap channels," in *Proc. CISS*, Mar. 2010.
[44] T. Liu, V. Prabhakaran, and S. Vishwanath, "The secrecy capacity of a class of non-degraded parallel Gaussian compound wiretap channels," in *Proc. IEEE ISIT*, July 2008.
[45] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453–2469, June 2008.
[46] L. H. Ozarow and A. Wyner, "Wire-tap channel II," in *Proc. EUROCRYPT 84-A Workshop on the Theory and Application of Cryptographic Techniques: Advances in Cryptology*, 1985.
[47] A. Khisti. (2010, Feb.). Interference alignment for the multi-antenna compound wiretap channel. Submitted to *IEEE Trans. Inf. Theory*. [Online]. Available: http://arXiv.org/abs/1002.4548
[48] A. S. Motahari, S. O. Gharan, and A. K. Khandani. (2009, Aug.). Real interference alignment with real numbers. Submitted to *IEEE Trans. Inf. Theory*. [Online]. Available: http://arXiv.org/abs/0908.1208
[49] A. S. Motahari, S. O. Gharan, M. Maddah-Ali, and A. K. Khandani. (2009, Aug.). Real interference alignment: Exploiting the potential of single antenna systems. Submitted to *IEEE Trans. Inf. Theory*. [Online]. Available: http://arXiv.org/abs/0908.2282
[50] M. Kobayashi, Y. Liang, S. Shamai (Shitz), and M. Debbah, "On the compound MIMO broadcast channels with confidential messages," in *Proc. IEEE ISIT*, June–July 2009.
[51] E. Ekrem and S. Ulukus. (2009, Oct.). Degraded compound multi-receiver wiretap channels. Submitted to *IEEE Trans. Inf. Theory*. [Online]. Available: http://arXiv.org/abs/0910.3033
[52] E. Ekrem and S. Ulukus, "Secrecy capacity region of the degraded compound multi-receiver wiretap channel," in *Proc. Allerton Conf. Commun., Control, and Comput.*, Sept. 2009.



Ersen Ekrem 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 working toward the Ph.D. degree in the Department of Electrical and Computer Engineering at the University of Maryland, College Park. His research interests include information theory and wireless communications.

Sennur Ulukus received the B.S. and M.S. degrees in Electrical and Electronics Engineering from Bilkent University, Ankara, Turkey, in 1991 and 1993, respectively, and the Ph.D. degree in Electrical and Computer Engineering from Rutgers University, NJ, in 1998. During her Ph.D. studies, she was with the Wireless Information Network Laboratory (WINLAB), Rutgers University. From 1998 to 2001, she was a Senior Technical Staff Member at AT&T Labs-Research in NJ. In 2001, she joined the University of Maryland at College Park, where she is currently an Associate Professor in the Department of Electrical and Computer Engineering, with a joint appointment at the Institute for Systems Research (ISR). Her research interests are in wireless communication theory and networking, network

information theory for wireless networks, signal processing for wireless communications, and security for multi-user wireless communications. She is a recipient of the 2005 NSF CAREER Award, and a co-recipient of the 2003 IEEE Marconi Prize Paper Award in Wireless Communications. She serves/served as an Associate Editor for the IEEE Transactions on Information Theory since 2007, as an Associate Editor for the IEEE Transactions on Communications between 2003–2007, as a Guest Editor for the IEEE Transactions on Information Theory for the special issue on interference networks, as a Guest Editor for the IEEE Journal on Selected Areas in Communications for the special issue on multiuser detection for advanced communication systems and networks, as the Co-Chair of the Communication Theory Symposium at the 2007 IEEE Global Telecommunications Conference, as the Co-Chair of the Medium Access Control (MAC) Track at the 2008 IEEE Wireless Communications and Networking Conference, as the Co-Chair of the Wireless Communications Symposium at the 2010 IEEE International Conference on Communications, as the Co-Chair of the 2011 Communication Theory Workshop, and as the Secretary of the IEEE Communication Theory Technical Committee (CTTC) in 2007-2009.