MIMO Gaussian Broadcast Channels with Common, Private and Confidential Messages

Ziv Goldfeld
Ben Gurion University of the Negev
gziv@post.bgu.ac.il

***Abstract*—The two-user multiple-input multiple-output (MIMO) Gaussian broadcast channel (BC) with common, private and confidential messages is considered. The transmitter sends a common message to both users, a confidential message to User 1 and a private (non-confidential) message to User 2. The secrecy-capacity region is characterized by showing that certain inner and outer bounds coincide and that the boundary points are achieved by Gaussian inputs. The proof relies on factorization of upper concave envelopes and a variant of dirty-paper coding (DPC). The entire region is exhausted by using DPC to cancel out the signal of the non-confidential message at Receiver 1, making DPC against the signal of the confidential message unnecessary. The secrecy-capacity results are visualized using a numerical example.**

I. Introduction

Channels with an additive Gaussian noise are a common model for wireless communication, whose open nature makes it susceptible to eavesdropping. However, eavesdroppers are not always a malicious entity from which *all* transmissions are concealed. Rather, a legitimate receiver of a certain message may serve as an eavesdropper for other messages. We encapsulate this notion in a two-user multiple-input multiple-output (MIMO) Gaussian broadcast channel (BC) with common, private and confidential messages (Fig. 1). The common message M_0 is intended to both users, while M_1 and M_2 are private messages that are sent to users 1 and 2, respectively. Further, M_1 is confidential and is kept secret from user 2. Secrecy is insured in terms of weak-secrecy, i.e., a vanishing *information-rate leakage*.

In recent years, information-theoretic study of secret MIMO communication over Gaussian channels has been an active area of research (see [1] for a recent survey of progress in this area). The optimality of Gaussian inputs in typically established based on channel enhancement arguments, originally used in [2] to characterise the private message capacity region of the MIMO Gaussian BC (without secrecy constraints).

In this work we take a different approach and prove the optimality of Gaussian inputs via factorization of upper concave envelopes (UCE). This approach was proposed in [3], where the capacity region of the MIMO Gaussian BC with common and private messages was established. We first characterize the secrecy-capacity region under an input covariance constraint for the setting with private and confidential messages only (i.e., when no common message is present). The derivation

The work of Z. Goldfeld was supported by an ERC starting grant and the Cyber Security Research Center (CSRC) at Ben-Gurion University of the Negev.

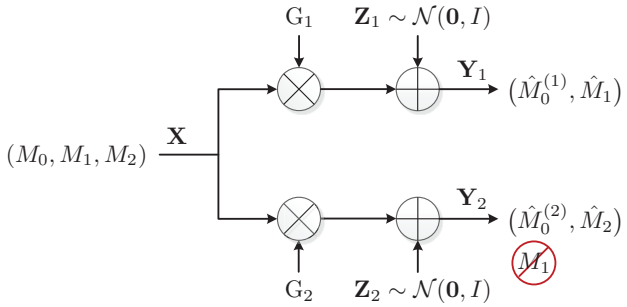

Fig. 1: MIMO Gaussian BC with common, private and confidential messages.

leverages UCEs to show that the boundary point of a certain outer bound are achieved by Gaussian inputs. Then, using an adaptation of dirty-paper coding (DPC) [4], we establish the equivalence of the outer bound to a particular inner bound, thus characterizing the secrecy-capacity region. Interestingly, optimality is achieved by using DPC to cancel out the signal of the non-confidential message M_2 at Receiver 1 only. The other variant, i.e., DPC against the signal of the confidential message M_1, turns out to be unnecessary.

We then focus on the MIMO Gaussian BC with common, private and confidential messages (Fig. 1). The result without a common message is used to show that Gaussian inputs are optimal for a certain portion of the region with a common message. The rest of the region is characterized by extending the tools from [3] and introducing the notion of a double-nested UCE. Gaussian inputs once again are shown to exhaust the entire region. Finally, we visualize our results by a numerical example which provides a comparison to the scenario where both private messages are confidential. The comparison shows that while in the MIMO Gaussian BC with confidential messages the transmission rate of each user cannot exceed the secrecy-capacity of the MIMO Gaussian WTC, removing the secrecy requirement from one of the messages allows the corresponding user to achieve strictly higher transmission. Since the regions derived in this work are described as non-convex matrix optimization problems, we simplify them into a computational from by relying on matrix decomposition properties from [5].

A. Problem Definition

We use notation from [6, Section II]. The outputs of a MIMO Gaussian BC at the i-th channel use is:

$$\mathbf{Y}_j(i) = \mathrm{G}_j \mathbf{X}(i) + \mathbf{Z}_j(i), \quad j = 1, 2, \quad i \in [1 : n], \qquad (1)$$

978-1-5090-1090-5/16/$31.00 ©2016 IEEE

where $\mathrm{G}_1, \mathrm{G}_2 \in \mathbb{R}^{t\times t}$ are channel gain matrices, $\{\mathbf{Z}_j(i)\}_{i\in[1:n]}$, for $j=1,2$, is an independent and identically distributed (i.i.d.) additive vector Gaussian noise process, and $\{\mathbf{X}(i)\}_{i\in[1:n]}$ is the channel input process that is subject to the covariance constraint

$$\frac{1}{n}\sum_{i=1}^{n}\mathbb{E}\left[\mathbf{X}(i)\mathbf{X}^{\top}(i)\right] \preceq \mathrm{K}, \tag{2}$$

where $\mathrm{K}\succeq 0$.

Remark 1 *By reasoning similar to this of [3, Remark 1] we assume that* G_1 *and* G_2 *are invertible and that the Gaussian noise processes,* $\{\mathbf{Z}_j(i)\}_{i\in[1:n]}$*, for* $j=1,2$*, are i.i.d. according to* $\mathcal{N}(0,\mathrm{I})$*, where* I *is the* $t\times t$*-identity matrix. The first assumption is essentially justified since invertible matrices are dense in the set of all* $t\times t$ *matrices, while the second assumption relies on standard noise whitening arguments.*

We study the scenario of a MIMO Gaussian BC with common, private and confidential messages (Fig. 1). The sender communicates three messages (M_0, M_1, M_2) over a MIMO Gaussian BC. M_0 is a common message intended for both users, while M_j, for $j=1,2$, is delivered to user j only. The receivers are to recover their intended messages with arbitrarily small error probability. Moreover, a weak-secrecy constraint is imposed on M_1 at the 2nd receiver, i.e., we require $\frac{1}{n}I(M_1;\mathbf{Y}_2^n)\xrightarrow[n\to\infty]{}0$, where $\mathbf{Y}_2^n=\big(\mathbf{Y}_2(1),\mathbf{Y}_2(2),\cdots,\mathbf{Y}_2(n)\big)$ and n is the number of channel uses. Achievability is defined in a standard manner and the *secrecy-capacity region* $\mathcal{C}_{\mathrm{K}}$ is the closure of all achievable rate triples $(R_0,R_1,R_2)\in\mathbb{R}_+^3$.

II. Secrecy-Capacity Results

To state our results we set the following shorthand notations:

$$r_0^{(j)}(\mathrm{A},\mathrm{B}) = \frac{1}{2}\log\left|\frac{\mathrm{I}+\mathrm{G}_j\mathrm{K}\mathrm{G}_j^{\top}}{\mathrm{I}+\mathrm{G}_j(\mathrm{A}+\mathrm{B})\mathrm{G}_j^{\top}}\right| \tag{3a}$$

$$r_1(\mathrm{B}) = \frac{1}{2}\log\left|\frac{\mathrm{I}+\mathrm{G}_1\mathrm{B}\mathrm{G}_1^{\top}}{\mathrm{I}+\mathrm{G}_2\mathrm{B}\mathrm{G}_2^{\top}}\right| \tag{3b}$$

$$r_2(\mathrm{A},\mathrm{B}) = \frac{1}{2}\log\left|\frac{\mathrm{I}+\mathrm{G}_2(\mathrm{A}+\mathrm{B})\mathrm{G}_2^{\top}}{\mathrm{I}+\mathrm{G}_2\mathrm{B}\mathrm{G}_2^{\top}}\right|, \tag{3c}$$

where $j=1,2$ and $\mathrm{A},\mathrm{B}\in\mathbb{R}^{t\times t}$. Furthermore, define

$$\mathcal{C}_{\mathrm{K}}(\mathrm{K}_1,\mathrm{K}_2)\triangleq\left\{(R_0,R_1,R_2)\in\mathbb{R}_+^3\left|\begin{array}{l}R_0\le r_0(\mathrm{K}_1,\mathrm{K}_2)\\ R_1\le r_1(\mathrm{K}_2)\\ R_2\le r_2(\mathrm{K}_1,\mathrm{K}_2)\end{array}\right.\right\} \tag{4}$$

where $r_0(\mathrm{K}_1,\mathrm{K}_2)=\min\left\{r_0^{(1)}(\mathrm{K}_1,\mathrm{K}_2), r_0^{(2)}(\mathrm{K}_1,\mathrm{K}_2)\right\}$.

Theorem 1 (Secrecy-Capacity with Common Message) *The secrecy-capacity region* $\mathcal{C}_{\mathrm{K}}$ *of the MIMO Gaussian BC with common, private and confidential messages under the covariance constraint* (2) *is*

$$\mathcal{C}_{\mathrm{K}} = \bigcup_{\substack{0\preceq\mathrm{K}_1,\mathrm{K}_2:\\ \mathrm{K}_1+\mathrm{K}_2\preceq\mathrm{K}}}\mathcal{C}_{\mathrm{K}}(\mathrm{K}_1,\mathrm{K}_2). \tag{5}$$

Due to space limitations, in Section IV we give the proof for the setting without a common message (i.e., when $R_0=0$), whose secrect-capacity region is state in Corollary 2. The proof of Theorem 1 follows similar lines but requires stronger technical tools, viz. the notion of double-nested UCEs. The reader is referred to [7] for details.

Remark 2 *We interpret the structure of* $\mathcal{C}_{\mathrm{K}}$ *as follows. First,* $r_1(\mathrm{K}_2)$ *indicates that User 1 achieves rates up to the secrecy-capacity of the MIMO Gaussian WTC with input covariance* K_2*. The 2nd user treats this signal as an additive Gaussian noise when decoding its private message* M_2*, which is transmitted using another (independent) Gaussian signal with covariance* K_1 *(see* $r_2(\mathrm{K}_1\mathrm{K}_2)$*). Finally, the structure of* $r_0^{(j)}(\mathrm{K}_1,\mathrm{K}_2)$ *implies that the remaining portion of the total covariance matrix, that is,* $\mathrm{K}-(\mathrm{K}_1+\mathrm{K}_2)$*, is employed to encode the common message* M_0*, which is decoded by each receiver while treating all other signals as noise. As in the case without a common message, a layered coding scheme, when optimized over the choices of* K_1 *and* K_2*, exhausts the entire secrecy-capacity region.*

Corollary 2 (Secrecy-Capacity without Common Message) *The secrecy-capacity region* $\hat{\mathcal{C}}_{\mathrm{K}}$ *of the MIMO Gaussian BC with private and confidential messages but without a common message (*$R_0=0$*) under the covariance constraint (2) is*

$$\hat{\mathcal{C}}_{\mathrm{K}} = \bigcup_{0\preceq\mathrm{K}^\star\preceq\mathrm{K}}\hat{\mathcal{C}}_{\mathrm{K}}(\mathrm{K}^\star), \tag{6}$$

where

$$\hat{\mathcal{C}}_{\mathrm{K}}(\mathrm{K}^\star)\triangleq\left\{(R_1,R_2)\in\mathbb{R}_+^2\left|\begin{array}{l}R_1\le r_1(\mathrm{K}^\star)\\ R_2\le r_2(\mathrm{K}-\mathrm{K}^\star,\mathrm{K}^\star)\end{array}\right.\right\}. \tag{7}$$

Corollary 2 follows from Theorem 1 by setting $\mathrm{K}_2=\mathrm{K}^\star$ and $\mathrm{K}_1=\mathrm{K}-\mathrm{K}^\star$. A self-contained proof of the corollary is found in Section IV.

Remark 3 *As evident in the proof of Corollary 2 (Proposition 8 in Section IV), the entire secrecy-capacity region* $\hat{\mathcal{C}}_{\mathrm{K}}$ *is achieved by using DPC to cancel out the signal of the non-confidential message* M_2 *at Receiver 1 only. The other variant, i.e., DPC against the signal of the confidential message* M_1 *at Receiver 2, is unnecessary. This is in contrast to when there in no secrecy requirement on* M_1 *(namely, the private message BC), where the capacity region is exhausted by taking the convex hull of both variants (DPC against* M_1 *and DPC against* M_2*).*

We also characterize the secrecy-capacity regions under the average total power constraint. This is a simple consequence of [2, Lemma 1].

Corollary 3 *The secrecy-capacity region of the MIMO Gaussian BC with common, private and confidential messages under the average total power constraint* $\frac{1}{n}\sum_{i=1}^{n}\left|\left|\mathbf{X}(i)\right|\right|^2\le P$ *is*

$$\mathcal{C}_P = \bigcup_{0\preceq\mathrm{K}:\ \mathrm{tr}(\mathrm{K})\le P}\mathcal{C}_{\mathrm{K}}. \tag{8}$$

Similarly, for the setting without a common message, we have

$$\hat{\mathcal{C}}_P = \bigcup_{0 \preceq \mathrm{K}:\ \mathrm{tr}(\mathrm{K}) \le P} \hat{\mathcal{C}}_{\mathrm{K}}. \tag{9}$$

A. Numerical Example

We visualize the secrecy-capacity region $\hat{\mathcal{C}}_P$ of the MIMO Gaussian BC with private and confidential messages (without a common message) under an average total power constraint P given in (9). The region is described as a union of all secrecy-capacity regions under a covariance constraint $\hat{\mathcal{C}}_{\mathrm{K}}$, with K that satisfies $\mathrm{tr}(\mathrm{K}) \le P$. However, $\hat{\mathcal{C}}_{\mathrm{K}}$ itself is described by matrix optimization problems that is not convex in general.

To compute the region under a covariance constraint $\hat{\mathcal{C}}_{\mathrm{K}}$, we use the decomposition proposed in [5, Equation (10)]: Every positive semidefinite matrix $\mathrm{K}^\star \in \mathbb{R}^{t\times t}$ with $\mathrm{K}^\star \preceq \mathrm{K}$ can be expressed as $\mathrm{K}^\star = \mathrm{K}^{\frac{1}{2}}\mathrm{V}\mathrm{D}\mathrm{V}^\top \mathrm{K}^{\frac{1}{2}^\top}$, where $\mathrm{V} \in \mathbb{R}^{t\times t}$ is a unitary matrix and $\mathrm{D} \in \mathbb{R}^{t\times t}$ is a diagonal matrix whose diagonal values are between 0 and 1. The region $\hat{\mathcal{C}}_P$ is computed according to (9), while noting that one may restrict the optimization domain to positive semidefinite matrices K with $\mathrm{tr}(\mathrm{K}) = P$. This follows because for every K' with $\mathrm{tr}(\mathrm{K}') = \pi < P$, there is a K with $\mathrm{tr}(\mathrm{K}) = P$, such that

$$\hat{\mathcal{C}}'_{\mathrm{K}} \subseteq \hat{\mathcal{C}}_{\mathrm{K}}. \tag{10}$$

The matrix K is constructed by increasing the $(1,1)$-th entry of K' by $P-\pi$, while keeping all other entries unchanged. The construction satisfied $\mathrm{K}' \preceq \mathrm{K}$ and the inclusion in (10) follows because fixing $\mathrm{K}^\star \preceq \mathrm{K}' \preceq \mathrm{K}$ and replacing K' with K in (7) does not alter $r_1(\mathrm{K}^\star)$ while strictly increasing $r_2(\mathrm{K}-\mathrm{K}^\star, \mathrm{K}^\star)$.

Let the channel matrices and the average total power be

$$\mathrm{G}_1 = \begin{bmatrix} 0.3 & 2.5 \\ 2.2 & 1.8 \end{bmatrix}, \quad \mathrm{G}_2 = \begin{bmatrix} 1.3 & 1.2 \\ 1.5 & 3.9 \end{bmatrix} \tag{11}$$

and $P = 12$, respectively. The secrecy-capacity region $\hat{\mathcal{C}}_P$ is given by the solid blue curve in Fig. 2. For comparison, the secrecy-capacity region of the MIMO Gaussian BC with confidential messages [8] (i.e., when each user serves as an eavesdropped to the message of the other user) is depicted by the dashed red curve. Fig. 2 shows that imposing a secrecy constraint on M_2 at the 1st receiver strictly shrinks the secrecy-capacity region. Although in *both* regions the maximal value of R_1 is the secrecy-capacity of the corresponding MIMO Gaussian WTC (see (3b) and [8, Equation (4)]), the achievable values of R_2 drop due to the additional secrecy requirement.

III. Mathematical Background and UCEs

This section provides a brief mathematical background for characterizing the secrecy-capacity region of the considered MIMO Gaussian BC without a common message (Corollary 2). More specifically, we define some generic functions and claim that they are maximized by Gaussian distributions. The proofs of all the properties stated in this section are omitted due to space limitations (see [7, Sections IV and VI]).

The UCE of and arbitrary function is defined as follow.

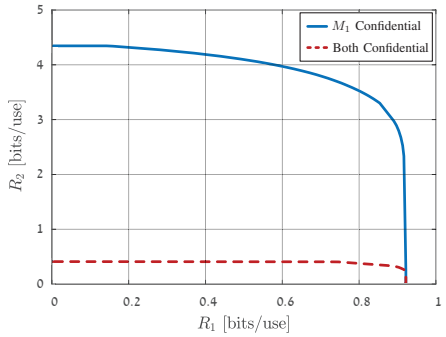

Fig. 2: Secrecy-capacity region under average total power constraint of the MIMO Gaussian BC with: private and confidential messages (solid blue) vs. confidential messages (dashed red).

Definition 1 (Upper Concave Envelope) *Let $f : \mathcal{D} \to \mathbb{R}$ be a function defined on a convex set $\mathcal{D}$. The UCE $\mathfrak{C}(f) : \mathcal{D} \to \mathbb{R}$ of f is the pointwise smallest concave function F such that $F(x) \ge f(x),\ \forall x \in \mathcal{D}$.*

A representation of the UCE $F = \mathfrak{C}(f)$ using the supporting hyperplanes of f is

$$F(x) = \sup_{V:\ \mathbb{E}[V]=x} \mathbb{E} f(V). \tag{12}$$

A. Difference of Mutual Information Terms

Consider a broadcast channel $Q_{\mathbf{Y}_1,\mathbf{Y}_2|\mathbf{X}}$. For any $\eta > 1$, let s_η^Q be a function of $P_{\mathbf{X}}$ defined by

$$s_\eta^Q(\mathbf{X}) \triangleq I(\mathbf{X};\mathbf{Y}_2) - \eta I(\mathbf{X};\mathbf{Y}_1). \tag{13}$$

For a pair of random variables $(V,\mathbf{X})$ such that $V - \mathbf{X} - (\mathbf{Y}_1,\mathbf{Y}_2)$ forms a Markov chain, set

$$s_\eta^Q(\mathbf{X}|V) \triangleq I(\mathbf{X};\mathbf{Y}_2|V) - \eta I(\mathbf{X};\mathbf{Y}_1|V), \tag{14}$$

and note the UCE of s_η^Q (cf. (12)) is given by

$$S_\eta^Q(\mathbf{X}) \triangleq \mathfrak{C}\big(s_\eta^Q\big)(\mathbf{X}) = \sup_{\substack{P_{V|\mathbf{X}}:\\ V-\mathbf{X}-(\mathbf{Y}_1,\mathbf{Y}_2)}} s_\eta^Q(\mathbf{X}|V). \tag{15}$$

We also set $S_\eta^Q(\mathbf{X}|V) \triangleq \sum_v P(v) S_\eta^Q(\mathbf{X}|V=v)$, for a discrete random variable V and its natural extension for an arbitrary V.

Proposition 4 (Continuity) *$S_\eta^Q(\mathbf{X})$ is convex in η inside $(0,2)$, and therefore, it is contentious in η at $\eta = 1$.*

Definition 2 (Maximized Concave Envelope) *For a MIMO Gaussian BC $Q_{\mathbf{Y}_1,\mathbf{Y}_2|\mathbf{X}}$ and $\mathrm{K} \succeq 0$, define*

$$V_\eta^Q(\mathrm{K}) \triangleq \sup_{\mathbf{X}:\ \mathbb{E}[\mathbf{X}\mathbf{X}^\top] \preceq \mathrm{K}} S_\eta^Q(\mathbf{X}) = \sup_{\substack{(V,\mathbf{X}):\ \mathbb{E}[\mathbf{X}\mathbf{X}^\top] \preceq \mathrm{K},\\ V-\mathbf{X}-(\mathbf{Y}_1,\mathbf{Y}_2)}} s_\eta^Q(\mathbf{X}|V).$$

B. Nested Upper Concave Envelopes

For a BC $Q_{\mathbf{Y}_1,\mathbf{Y}_2|\mathbf{X}}$, $\eta > 1$ and $\boldsymbol{\lambda} = (\lambda_1,\lambda_2)$, where $\lambda_j > 0$, $j = 1,2$, define

$$t_{\boldsymbol{\lambda},\eta}^Q(\mathbf{X}) \triangleq \lambda_1 I(\mathbf{X};\mathbf{Y}_1) - (\lambda_1+\lambda_2) I(\mathbf{X};\mathbf{Y}_2) + \lambda_1 S_\eta^Q(\mathbf{X}), \tag{16}$$

where $S_\eta^Q(\mathbf{X})$ is given by (15). As before, for a pair of random variables $(V,\mathbf{X})$ for which $V-\mathbf{X}-(\mathbf{Y}_1,\mathbf{Y}_2)$ forms a Markov chain, let

$$t^Q_{\boldsymbol{\lambda},\eta}(\mathbf{X}|V) \triangleq \lambda_1 I(\mathbf{X};\mathbf{Y}_1|V) - (\lambda_1+\lambda_2) I(\mathbf{X};\mathbf{Y}_2|V) + \lambda_1 S^Q_\eta(\mathbf{X}|V). \quad (17)$$

Thus $T^Q_{\boldsymbol{\lambda},\eta}(\mathbf{X}) \triangleq \mathfrak{C}\big(t^Q_{\boldsymbol{\lambda},\eta}\big)(\mathbf{X}) = \sup_{\substack{P_{V|\mathbf{X}}:\\ V-\mathbf{X}-(\mathbf{Y}_1,\mathbf{Y}_2)}} t^Q_{\boldsymbol{\lambda},\eta}(\mathbf{X}|V)$. Define $T^Q_{\boldsymbol{\lambda},\eta}(\mathbf{X}|V)$ analogously to the definition of $S^Q_\eta(\mathbf{X}|V)$.

Remark 4 (Nested UCE Properties) *Since $T^Q_{\boldsymbol{\lambda},\eta}(\mathbf{X})$ is concave in $P_{\mathbf{X}}$, Jensen's inequality implies that $T^Q_{\boldsymbol{\lambda},\eta}(\mathbf{X}|V) \le T^Q_{\boldsymbol{\lambda},\eta}(\mathbf{X})$. Moreover, if $W-V-\mathbf{X}$ forms a Markov chain, then $T^Q_{\boldsymbol{\lambda},\eta}(\mathbf{X}|W,V) = T^Q_{\boldsymbol{\lambda},\eta}(\mathbf{X}|V)$, because $P_{\mathbf{X}|W,V} = P_{\mathbf{X}|V}$. Finally, $T^Q_{\boldsymbol{\lambda},\eta}(\mathbf{X})$ is convex in η inside $(0,2)$, and therefore, it is contentious in η at $\eta=1$.*

Definition 3 (Maximized Nested UCE) *For a MIMO Gaussian BC $Q_{\mathbf{Y}_1,\mathbf{Y}_2|\mathbf{X}}$ and $\mathrm{K}\succeq 0$, define*

$$\hat{V}^Q_{\boldsymbol{\lambda},\eta}(\mathrm{K}) \triangleq \sup_{\mathbf{X}:\ \mathbb{E}[\mathbf{X}\mathbf{X}^\top]\preceq \mathrm{K}} T^Q_{\boldsymbol{\lambda},\eta}(\mathbf{X}) = \sup_{\substack{(V,\mathbf{X}):\ \mathbb{E}[\mathbf{X}\mathbf{X}^\top]\preceq \mathrm{K},\\ V-\mathbf{X}-(\mathbf{Y}_1,\mathbf{Y}_2)}} t^Q_{\boldsymbol{\lambda},\eta}(\mathbf{X}|V).$$

Proposition 5 (Continuity of Maximum) *$\hat{V}_{\boldsymbol{\lambda},\eta}(\mathrm{K})$ is contentious in η at $\eta=1$.*

Theorem 6 (Existence of Gaussian Maximizer) *Let $\mathbf{X}\sim\mathcal{N}(\mathbf{0},\mathrm{K})$. There exists a unique decomposition $\mathbf{X}=\mathbf{X}_1^\star+\mathbf{X}_2^\star+\mathbf{X}'$ into independent random variables $(\mathbf{X}_1^\star,\mathbf{X}_2^\star,\mathbf{X}')$, where $\mathbf{X}_j^\star\sim\mathcal{N}(\mathbf{0},\mathrm{K}_j)$, $j=1,2$, and $\mathbf{X}'\sim\mathcal{N}(\mathbf{0},\mathrm{K}-(\mathrm{K}_1+\mathrm{K}_2))$, $\mathrm{K}_1+\mathrm{K}_2\preceq\mathrm{K}$, such that*

$$T^Q_{\boldsymbol{\lambda},\eta}(\mathbf{X}) = t^Q_{\boldsymbol{\lambda},\eta}(\mathbf{X}_1^\star+\mathbf{X}_2^\star) = \hat{V}^Q_{\boldsymbol{\lambda},\eta}(\mathrm{K}) \quad (18a)$$

$$S^Q_\eta(\mathbf{X}_1^\star+\mathbf{X}_2^\star) = s^Q_\eta(\mathbf{X}_1^\star) = V^Q_\eta(\mathrm{K}_1+\mathrm{K}_2). \quad (18b)$$

IV. Proof of Theorem 2

We show that certain outer bound and inner bounds on the secrecy-capacity region (see Theorems 1 and 2 of [9]) match. To state the bounds, let $\hat{\mathcal{C}}$ denote the secrecy-capacity region of the corresponding discrete-memoryless (DM) BC.

Bound 1 (Outer Bound) *Let $\hat{\mathcal{O}}$ be the closure of the union of rate pairs $(R_1,R_2)\in\mathbb{R}_+^2$ satisfying:*

$$R_1 \le I(U;Y_1|V) - I(U;Y_2|V) \quad (19a)$$

$$R_2 \le I(V;Y_2) \quad (19b)$$

over all $(V,U)-X-(Y_1,Y_2)$. Then $\hat{\mathcal{C}}\subseteq\hat{\mathcal{O}}$.

Bound 2 (Inner Bound) *Let $\hat{\mathcal{I}}$ be the closure of the union of rate pairs $(R_1,R_2)\in\mathbb{R}_+^2$ satisfying:*

$$R_1 \le I(U;Y_1) - I(U;V) - I(U;Y_2|V) \quad (20a)$$

$$R_2 \le I(V;Y_2) \quad (20b)$$

over all $(V,U)-X-(Y_1,Y_2)$. Then $\hat{\mathcal{I}}\subseteq\hat{\mathcal{C}}$.

Let $\hat{\mathcal{C}}_\mathrm{K}$, $\hat{\mathcal{O}}_K$ and $\hat{\mathcal{I}}_K$ denote secrecy-capacity region, the outer bound and the inner bound for a MIMO Gaussian BC computed under a covariance input constraint $\mathbb{E}\big[\mathbf{X}\mathbf{X}^\top\big]\preceq\mathrm{K}$. By definition, we thus have $\hat{\mathcal{I}}_K\subseteq\hat{\mathcal{C}}_\mathrm{K}\subseteq\hat{\mathcal{O}}_K$.

The opposite inclusion, i.e., $\hat{\mathcal{O}}_K\subseteq\hat{\mathcal{I}}_K$, is shown next. The regions $\hat{\mathcal{I}}_K$ and $\hat{\mathcal{O}}_K$ are closed, convex and bounded subsets of the first quadrant, and therefore, are characterised by the intersection of their supporting hyperplanes.

Lemma 7 (Supporting Hyperplanes) *The following are supporting hyperplanes of $\hat{\mathcal{O}}_K$ and $\hat{\mathcal{I}}_K$:*

$$R_1\ge 0\ ,\ R_1\le\mathcal{H}_1^K\ ,\ R_2\ge 0\ ,\ R_2\le\mathcal{H}_2^K, \quad (21)$$

where $\mathcal{H}_1^K \triangleq \max_{\substack{(V,U)-\mathbf{X}-(\mathbf{Y}_1,\mathbf{Y}_2):\\ \mathbb{E}[\mathbf{X}\mathbf{X}^\top]\preceq\mathrm{K}}} I(U;\mathbf{Y}_1|V) - I(U;\mathbf{Y}_2|V)$ and $\mathcal{H}_2^K \triangleq \max_{\mathbf{X}:\ \mathbb{E}[\mathbf{X}\mathbf{X}^\top]\preceq\mathrm{K}} I(\mathbf{X};\mathbf{Y}_2)$. Furthermore, $(\mathcal{H}_1^K,0)$ and $(0,\mathcal{H}_2^K)$ are boundary points of $\hat{\mathcal{O}}_K$ and $\hat{\mathcal{I}}_K$.

The proof of Lemma 7 is omitted due to space limitations (see [7] for details). Based on the lemma, to show that the regions coincide, it suffices to show that

$$\max_{(R_1,R_2)\in\hat{\mathcal{O}}_K} \lambda_1R_1+\lambda_2R_2 \le \max_{(R_1,R_2)\in\hat{\mathcal{I}}_K} \lambda_1R_1+\lambda_2R_2, \quad (22)$$

for $\lambda_1,\lambda_2>0$. Observe that

$$\begin{aligned}
&\max_{(R_1,R_2)\in\hat{\mathcal{O}}_K} \lambda_1R_1+\lambda_2R_2\\
&\overset{(a)}{\le} \sup_{\substack{(V,U)-\mathbf{X}-(\mathbf{Y}_1,\mathbf{Y}_2):\\ \mathbb{E}[\mathbf{X}\mathbf{X}^\top]\preceq\mathrm{K}}} \left\{\begin{array}{r}\lambda_1\Big[I(U;\mathbf{Y}_1|V)-I(U;\mathbf{Y}_2|V)\Big]\\ +\lambda_2 I(V;\mathbf{Y}_2)\end{array}\right\}\\
&\overset{(b)}{=} \sup_{\substack{(V,U)-\mathbf{X}-(\mathbf{Y}_1,\mathbf{Y}_2):\\ \mathbb{E}[\mathbf{X}\mathbf{X}^\top]\preceq\mathrm{K}}} \left\{\begin{array}{r}\lambda_1 I(\mathbf{X};\mathbf{Y}_1|V)-(\lambda_1+\lambda_2)I(\mathbf{X};\mathbf{Y}_2|V)\\ +\lambda_1\Big[I(\mathbf{X};\mathbf{Y}_2|V,U)-I(\mathbf{X};\mathbf{Y}_1|V,U)\Big]\\ +\lambda_2 I(\mathbf{X};\mathbf{Y}_2)\end{array}\right\}\\
&\overset{(c)}{\le} \sup_{\substack{V-\mathbf{X}-(\mathbf{Y}_1,\mathbf{Y}_2):\\ \mathbb{E}[\mathbf{X}\mathbf{X}^\top]\preceq\mathrm{K}}} \left\{\begin{array}{c}\lambda_1 I(\mathbf{X};\mathbf{Y}_1|V)-(\lambda_1+\lambda_2)I(\mathbf{X};\mathbf{Y}_2|V)\\ +\lim_{\eta\downarrow 1}\lambda_1 S^Q_\eta(\mathbf{X}|V)+\lambda_2 I(\mathbf{X};\mathbf{Y}_2)\end{array}\right\}\\
&\le \sup_{\mathbb{E}[\mathbf{X}\mathbf{X}^\top]\preceq\mathrm{K}} \lambda_2 I(\mathbf{X};\mathbf{Y}_2) + \sup_{\substack{V-\mathbf{X}-(\mathbf{Y}_1,\mathbf{Y}_2):\\ \mathbb{E}[\mathbf{X}\mathbf{X}^\top]\preceq\mathrm{K}}} \lim_{\eta\downarrow1} t_{\boldsymbol{\lambda},\eta}(\mathbf{X}|V)\\
&\overset{(d)}{=} \sup_{\mathbb{E}[\mathbf{X}\mathbf{X}^\top]\preceq\mathrm{K}} \lambda_2 I(\mathbf{X};\mathbf{Y}_2) + \sup_{\mathbb{E}[\mathbf{X}\mathbf{X}^\top]\preceq\mathrm{K}} \lim_{\eta\downarrow1} T_{\boldsymbol{\lambda},\eta}(\mathbf{X})\\
&\overset{(e)}{=} \sup_{\mathbb{E}[\mathbf{X}\mathbf{X}^\top]\preceq\mathrm{K}} \lambda_2 I(\mathbf{X};\mathbf{Y}_2) + \lim_{\eta\downarrow1} \hat{V}_{\boldsymbol{\lambda},\eta}(\mathrm{K}), \qquad (23)
\end{aligned}$$

where (a) is from (19); (b) uses the Markov relation $(V,U)-\mathbf{X}-(\mathbf{Y}_1,\mathbf{Y}_2)$; (c) follows by the definition of $S^Q_\eta(\cdot|\cdot)$ and since conditioned on V, $U-\mathbf{X}-(\mathbf{Y}_1,\mathbf{Y}_2)$ forms a Markov chain. Furthermore, (c) uses the continuity of $S^Q_\eta(\mathbf{X}|V)$ in η at $\eta=1$ (see Proposition 4), which implies that $S^Q_1(\mathbf{X}|V)\triangleq S^Q_{\lim_{\eta\downarrow1}\eta}(\mathbf{X}|V)=\lim_{\eta\downarrow1}S^Q_\eta(\mathbf{X}|V)$; (d) is by the definition of $T^Q_{\boldsymbol{\lambda},\eta}(\cdot|\cdot)$, the Markov relation $V-\mathbf{X}-(\mathbf{Y}_1,\mathbf{Y}_2)$, and because $T^Q_{\boldsymbol{\lambda},\eta}(\mathbf{X}|V)$ is continuous in η at $\eta=1$ (see Remark 4);
(e) follows by Proposition 5.

By Theorem 6, for every $\eta>1$, there exist independent random variables $\mathbf{X}_1^\star\sim\mathcal{N}(\mathbf{0},\mathrm{K}_1)$, $\mathbf{X}_2^\star\sim\mathcal{N}(\mathbf{0},\mathrm{K}_2)$ and

$\mathbf{X}' \sim \mathcal{N}\big(\mathbf{0}, \mathrm{K} - (\mathrm{K}_1 + \mathrm{K}_2)\big)$, $\mathrm{K}_1 + \mathrm{K}_2 \preceq \mathrm{K}$, such that $\hat{V}_\eta^Q(\mathrm{K}) = t^Q_{\boldsymbol{\lambda},\eta}(\mathbf{X}_1^\star + \mathbf{X}_2^\star)$ and $S_\eta^Q(\mathbf{X}_1^\star + \mathbf{X}_2^\star) = s_\eta^Q(\mathbf{X}_1^\star)$. Moreover, setting $\mathbf{X} = \mathbf{X}_1^\star + \mathbf{X}_2^\star + \mathbf{X}'$ maximizes $\lambda_2 I(\mathbf{X};\mathbf{Y}_2)$ and attains $\hat{V}_\eta^Q(\mathrm{K})$ simultaneously. To conform to notation in the bounds, let $V^\star = \mathbf{X}'$. Taking the limit as $\eta \downarrow 1$, we have

$$\begin{aligned}
&\max_{(R_1,R_2)\in\hat{\mathcal{O}}_K} \lambda_1 R_1 + \lambda_2 R_2 \\
&\le \lambda_1 I(\mathbf{X};\mathbf{Y}_1|V^\star) - (\lambda_1+\lambda_2) I(\mathbf{X};\mathbf{Y}_2|V^\star) + \lambda_2 I(\mathbf{X};\mathbf{Y}_2) \\
&\qquad + \lambda_1 \Big[I(\mathbf{X};\mathbf{Y}_2|V^\star,\mathbf{X}_2^\star) - I(\mathbf{X};\mathbf{Y}_2|V^\star,\mathbf{X}_2^\star) \Big] \\
&\le \lambda_1 \Big[I(\mathbf{X}_2^\star;\mathbf{Y}_1|V^\star) - I(\mathbf{X}_2^\star;\mathbf{Y}_2|V^\star) \Big] + \lambda_2 I(V^\star;\mathbf{Y}_2). \quad (24)
\end{aligned}$$

Proposition 8 (Partial DPC) *Let* $\mathbf{X}$, $\mathbf{X}_1^\star$, $\mathbf{X}_2^\star$ *and* V *be as described above. Let* $\mathbf{Y}_1 = \mathrm{G}_1\mathbf{X} + \mathbf{Z}_1$, *where* $\mathbf{Z}_1 \sim \mathcal{N}(\mathbf{0},\mathrm{I})$ *is independent of* $(\mathbf{X}_1^\star, \mathbf{X}_2^\star, V^\star)$. *If* $U = \mathbf{X}_2^\star + \mathrm{A}V^\star$, *where* $\mathrm{A} = \mathrm{K}_2\tilde{\mathrm{G}}_1^\top \big[\mathrm{I} + \tilde{\mathrm{G}}_1\mathrm{K}_2\tilde{\mathrm{G}}_1^\top\big]^{-1}$ *and* $\tilde{\mathrm{G}}_1 = (\mathrm{I} + \mathrm{G}_1\mathrm{K}_1\mathrm{G}_1^\top)^{-\frac{1}{2}}\mathrm{G}_1$, *then*

$$\begin{aligned}
&I(\mathbf{X}_2^\star;\mathbf{Y}_1|V^\star) - I(\mathbf{X}_2^\star;\mathbf{Y}_2|V^\star) \\
&\qquad = I(U^\star;\mathbf{Y}_1) - I(U^\star;V^\star) - I(\mathbf{X}_2^\star;\mathbf{Y}_2|V^\star). \quad (25)
\end{aligned}$$

Proof Outline: Setting $\tilde{\mathbf{X}} \triangleq \mathbf{X}_2^\star + V^\star$ and $\mathbf{Z}_1' \triangleq \mathrm{G}_1\mathbf{X}_1^\star + \mathbf{Z}_1$, we have $\mathbf{Y}_1 = \mathrm{G}_1\tilde{\mathbf{X}} + \mathbf{Z}_1'$. By the independence of $\mathbf{X}_1^\star$, $\mathbf{X}_2^\star$, $V^\star$ and $\mathbf{Z}_1$, we have that $\tilde{\mathbf{X}}$ and $\mathbf{Z}_1'$ are also independent. Moreover, $\mathbf{Z}_1' \sim \mathcal{N}(\mathbf{0}, \mathrm{I} + \mathrm{G}_1\mathrm{K}_1\mathrm{G}_1^\top)$, where the covariance matrix $\mathrm{I} + \mathrm{G}_1\mathrm{K}_1\mathrm{G}_1^\top$ is diagonalizable (due to its symmetry) and invertible (because it is positive-definite). Denoting $\Sigma \triangleq \mathrm{I} + \mathrm{G}_1\mathrm{K}_1\mathrm{G}_1^\top$, we decompose $\Sigma = \mathrm{Q}\Lambda\mathrm{Q}^\top$, where Q is a unitary matrix and Λ is diagonal, and further $\Sigma^{-\frac{1}{2}} = \mathrm{Q}\Lambda^{-\frac{1}{2}}\mathrm{Q}^\top$. Defining $\tilde{\mathbf{Y}}_1 = \Sigma^{-\frac{1}{2}}\mathbf{Y}_1$ gives

$$\tilde{\mathbf{Y}}_1 = \tilde{\mathrm{G}}_1\tilde{\mathbf{X}} + \tilde{\mathbf{Z}}_1, \quad (26)$$

where $\tilde{\mathrm{G}}_1 = \Sigma^{-\frac{1}{2}}\mathrm{G}_1$, $\tilde{\mathbf{Z}}_1 = \Sigma^{-\frac{1}{2}}\mathbf{Z}_1'$ and $\tilde{\mathbf{Z}}_1 \sim \mathcal{N}(\mathbf{0},\mathrm{I})$. Setting $U^\star$ as above and invoking the classic DPC Theorem (as formulated in [3, Proposition 12]), we obtain

$$I(\tilde{\mathbf{X}};\tilde{\mathbf{Y}}_1|V^\star) = I(U^\star;\tilde{\mathbf{Y}}_1) - I(U^\star;V^\star). \quad (27)$$

Since $U^\star = \mathbf{X}_2^\star + \mathrm{A}V^\star$ we also have

$$I(\mathbf{X}_2^\star;\mathbf{Y}_2|V^\star) = I(U^\star;\mathbf{Y}_2|V^\star). \quad (28)$$

Note that $\mathbf{Y}_1 \mapsto \Sigma^{-\frac{1}{2}}\mathbf{Y}_1$ is an invertible mapping, and as such, preserves mutual information. Concluding, we have

$$\begin{aligned}
&I(\mathbf{X}_2^\star;\mathbf{Y}_1|V^\star) - I(\mathbf{X}_2^\star;\mathbf{Y}_2|V^\star) \\
&\quad \overset{(a)}{=} I(\tilde{\mathbf{X}};\mathbf{Y}_1|V^\star) - I(U^\star;\mathbf{Y}_2|V^\star) \\
&\quad \overset{(b)}{=} I(\tilde{\mathbf{X}};\tilde{\mathbf{Y}}_1|V^\star) - I(U^\star;\mathbf{Y}_2|V^\star) \\
&\quad \overset{(c)}{=} I(U^\star;\tilde{\mathbf{Y}}_1) - I(U^\star;V^\star) - I(U^\star;\mathbf{Y}_2|V^\star) \\
&\quad \overset{(d)}{=} I(U^\star;\mathbf{Y}_1) - I(U^\star;V^\star) - I(U^\star;\mathbf{Y}_2|V^\star), \quad (29)
\end{aligned}$$

where (a) is because $\tilde{\mathbf{X}} = \mathbf{X}_2^\star + V^\star$ and by (28), (b) and (d) are since $\mathbf{Y}_1 \mapsto \Sigma^{-\frac{1}{2}}\mathbf{Y}_1$ is invertible, while (c) uses (27). ■

Inserting $U^\star$ into the RHS of (24) while (25) gives

$$\begin{aligned}
&\max_{(R_1,R_2)\in\hat{\mathcal{O}}_K} \lambda_1 R_1 + \lambda_2 R_2 \\
&= \lambda_1 \Big[I(U^\star;\mathbf{Y}_1) - I(U^\star;V^\star) - I(U^\star;\mathbf{Y}_2|V^\star) \Big] + \lambda_2 I(V^\star;\mathbf{Y}_2) \\
&\overset{(a)}{\le} \max_{(R_1,R_2)\in\hat{\mathcal{I}}_K} \lambda_1 R_1 + \lambda_2 R_2, \quad (30)
\end{aligned}$$

where (a) follows since $(U^\star, V^\star) - \mathbf{X} - (\mathbf{Y}_1, \mathbf{Y}_2)$ forms a Markov chain and $\mathbb{E}\big[\mathbf{X}\mathbf{X}^\top\big] \preceq \mathrm{K}$ is satisfied, which implies that the rate pair $R_1 = I(U^\star;\mathbf{Y}_1) - I(U^\star;V^\star) - I(U^\star;\mathbf{Y}_2|V^\star)$ and $R_2 = I(V^\star;\mathbf{Y}_2)$ belongs to $\hat{\mathcal{I}}_K$, which implies that $\hat{\mathcal{I}}_K = \hat{\mathcal{C}}_\mathrm{K} = \hat{\mathcal{O}}_K$. The equality (and hence the extreme points of $\hat{\mathcal{C}}_\mathrm{K}$) is attained by Gaussian inputs as stated in Proposition 8, thus making the region computable.

By evaluating $\hat{\mathcal{I}}_K$ with respect to this input distribution, the secrecy-capacity region $\hat{\mathcal{C}}_\mathrm{K}$ is the union of rate pairs $(R_1, R_2) \in \mathbb{R}_+^2$ satisfying:

$$R_1 \le \frac{1}{2}\log\left| \frac{\mathrm{I} + \mathrm{G}_1(\mathrm{K}_1+\mathrm{K}_2)\mathrm{G}_1^\top}{\mathrm{I} + \mathrm{G}_1\mathrm{K}_1\mathrm{G}_1^\top} \cdot \frac{\mathrm{I} + \mathrm{G}_2\mathrm{K}_1\mathrm{G}_2^\top}{\mathrm{I} + \mathrm{G}_2(\mathrm{K}_1+\mathrm{K}_2)\mathrm{G}_2^\top} \right| \quad (31a)$$

$$R_2 \le \frac{1}{2}\log\left| \frac{\mathrm{I} + \mathrm{G}_2\mathrm{K}\mathrm{G}_2^\top}{\mathrm{I} + \mathrm{G}_2(\mathrm{K}_1+\mathrm{K}_2)\mathrm{G}_2^\top} \right|, \quad (31b)$$

where the union is over all positive semi-definite matrices $\mathrm{K}_1, \mathrm{K}_2$, with $\mathrm{K}_1 + \mathrm{K}_2 \preceq \mathrm{K}$. To further simplify (31) note that the RHS of (31a) is the secrecy-capacity of the MIMO Gaussian WTC as derived in [3, Appendix III], which is maximized by setting $\mathrm{K}_1 = 0$ (see [10]–[12]). Further note that $\mathrm{K}_1 = 0$ cannot decrease the RHS of (31b) and relabel $\mathrm{K}_2 \triangleq \mathrm{K}^\star$ to obtain (6).

REFERENCES

[1] Y. Liang, H. V. Poor, and S. Shamai (Shitz). *Foundations and Trends in Communications and Information Theory*, volume 5, chapter Information Theoretic Security, pages 355–580. Now Publishers, MA, USA, 2008.

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

[3] Y. Geng and C. Nair. The capacity region of the two-receiver vector Gaussian broadcast channel with private and common messages. *Submitted for publication to IEEE Trans. Inf. Theory*, 2014.

[4] W. Yu and J. Cioffi. Sum capacity of Gaussian vector broadcast channels. *IEEE Trans. Inf. Theory*, 50(9):1875–1892, Sep. 2004.

[5] A. Khina, Y. Kochman, and A. Khisti. The confidential MIMO broadcast capacity: A simple derivation. In *Proc. Int. Symp. Inf. Theory (ISIT-2015)*, pages 1981–1985, Hong Kong, Jun. 2015.

[6] Z. Goldfeld, P. Cuff, and H. H. Permuter. Semantic-security capacity for wiretap channels of type II. *Submitted to IEEE Trans. Inf. Theory*, 2015. Available on ArXiv at http://arxiv.org/abs/1509.03619.

[7] Z. Goldfeld. MIMO Gaussian broadcast channels with common, private and confidential messages. *To be submitted to IEEE Trans. Inf. Theory*, 2016. Available on ArXiv at http://arxiv.org/abs/.

[8] R. Liu, T. Liu, H. V. Poor, and S. Shamai. Multiple-input multiple-output Gaussian broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 56(9):4215–4227, Sep. 2010.

[9] Z. Goldfeld, G. Kramer, and H. H. Permuter. Broadcast channels with privacy leakage constraints. *Submitted for publication to IEEE Trans. Inf. Theory*, 2015.

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

[11] A. Khisti and G. W. Wornell. Secure transmission with multiple antennas - part II: The MIMOME channel. *IEEE Trans. Inf. Theory*, 56(11):5515–5532, Nov. 2010.

[12] F. Oggier and B. Hassibi. The secrecy capacity of the MIMO wiretap channel. *IEEE Trans. Inf. Theory*, 57(8):4961–4972, Aug. 2011.