# Physical Layer Integration of Private, Common, and Confidential Messages in Bidirectional Relay Networks

Rafael F. Wyrembelski, *Student Member, IEEE*, and Holger Boche, *Fellow, IEEE*

***Abstract*—In order to increase spectral efficiency, it is becoming more and more important that next generation wireless networks wisely integrate multiple services such as transmissions of private, common, and confidential messages at the physical layer. This is referred to as *physical layer service integration*, and in this paper is being studied for bidirectional relay networks. Here, a relay node establishes a bidirectional communication between two other nodes using a decode-and-forward protocol. This is also known as two-way relaying. In the broadcast phase, the relay efficiently integrates additional common and confidential services at the physical layer, which then requires the study of the *bidirectional broadcast channel (BBC) with common and confidential messages*. The entire secrecy capacity regions for discrete memoryless and MIMO Gaussian channels are established. These results further unify previous partial results such as the BBC with common messages or the classical broadcast channel with common and confidential messages, where the relay node provides only some of the services.**

***Index Terms*—Bidirectional Relaying, Bidirectional Broadcast Channel, Capacity Region, Physical Layer Security, Embedded Security, Multicast, MIMO, Wireless Network, Physical Layer Service Integration.**

## I. Introduction

Recently, significant progress has been made in improving the performance of next generation cellular networks. Proposed techniques such as multiuser MIMO, channel adaptive scheduling, cooperative multi-point transmission, or relaying can increase the spectral efficiency.

An additional research area that is gaining importance is the efficient physical layer implementation of multiple services such as the simultaneous transmission of private, common, or confidential messages. For example, in current cellular systems, operators not only offer traditional services such as (bidirectional) voice communication, but also further multicast services or confidential services that are subject to certain secrecy constraints. Nowadays, the integration of multiple services is realized by policies that allocate different services on different logical channels and further by applying secrecy techniques on higher levels. In general this is quite inefficient, and thus there is a trend to efficiently merge multiple coexisting services from an information theoretic point of view, so that they work on the same wireless resources. Such an integration of multiple transmission tasks at the physical layer is referred to as *physical layer service integration* and has the potential to significantly increase the spectral efficiency for next generation wireless networks and, especially, 5G cellular networks.

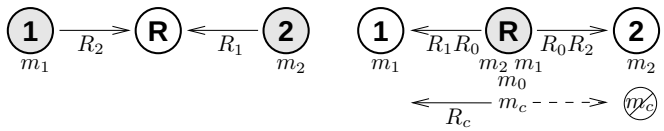
Multicast services can efficiently be realized by common messages; for example the Multimedia Broadcast Multicast Service (MBMS), as specified by the 3GPP organization [1], or the Multicast and Broadcast Service (MCBCS) in WiMAX [2] benefit from such studies. Broadcast channels with common messages and certain receiver side information are studied in [3, 4]. A general model for multi-user settings with correlated sources can be found in [5].

Since the aforementioned services do not require that they are kept secret from non-legitimate receivers, they are classified as *public services*. But there are services such as mobile banking or industrial applications which have security constraints. Accordingly, these are classified as *confidential services*. Currently, secrecy techniques usually rely on the assumption of unproven hardness of certain problems or insufficient computational capabilities of non-legitimate receivers. Thus, physical layer secrecy techniques are becoming more and more attractive since they do not rely on such assumptions and therefore provide so-called unconditional security. Not surprisingly, this is also identified by operators as a promising and important task for next generation mobile networks [6].

In the seminal work [7], Wyner introduced the *wiretap channel* which characterizes the secure communication problem for a point-to-point link with an additional eavesdropper. Csiszár and Körner generalized this to the *broadcast channel with confidential messages* in [8] and characterized the optimal integration of common and confidential services at the physical layer. Recently, there has been growing interest in physical-layer secrecy, cf. [9, 10] and references therein. Besides the point-to-point link [7, 11–13], there are extensions to multi-user settings such as the multiple access channel with confidential messages [14], the MIMO Gaussian broadcast channel with common and confidential messages [15, 16], or the two-way wiretap channel [17–19].

The concept of *bidirectional relaying*, or two-way relaying, is becoming more and more attractive since it has the potential to significantly improve the overall performance and coverage in wireless networks such as ad-hoc, sensor, and even cellular systems, especially in those that use relays for coverage extension. But it also significantly improves the inter-cell

The authors are with the Lehrstuhl für Theoretische Informationstechnik, Technische Universität München, Germany (e-mail: {wyrembelski, boche}@tum.de). This work was partly supported by the German Research Foundation (DFG) under Grants BO 1734/12-1 and BO 1734/25-1 and by the German Ministry of Education and Research (BMBF) under Grant 01BQ1050. This work was partly presented at IEEE-ITW, Paraty, Brazil, Oct. 2011 and IEEE-GLOBECOM, Houston, TX, USA, Dec. 2011.




(a) MAC phase (b) BBC phase

Fig. 1. Physical layer service integration in decode-and-forward bidirectional relaying. In the initial MAC phase, nodes 1 and 2 transmit their messages $m_1$ and $m_2$ with rates $R_2$ and $R_1$ to the relay node. Then, in the BBC phase, the relay forwards the messages $m_1$ and $m_2$ and adds a common message $m_0$ with rate $R_0$ to the communication and further a confidential message $m_c$ for node 1 with rate $R_c$ which should be kept secret from node 2.

performance of cellular systems if it is directly applied at the base station [20]. This is mainly based on the fact that it advantageously exploits the property of bidirectional communication to reduce the inherent loss in spectral efficiency induced by half-duplex relays [21–24].

Bidirectional relaying applies to three-node networks, where a half-duplex relay node establishes a bidirectional communication between two other nodes using a decode-and-forward protocol. There, in the initial multiple access (MAC) phase, two nodes transmit their messages to the relay node which decodes them. In the succeeding bidirectional broadcast (BBC) phase, the relay re-encodes and transmits both messages in such a way that both receiving nodes can decode their intended message using their own message from the previous phase as side information. It is shown in [4, 25, 26] that capacity is achieved by a single data stream that combines both messages based on the network coding idea.

In this work, we consider physical layer service integration in bidirectional relay networks. Here, the relay node integrates additional common and confidential services in the broadcast phase. More precisely, in addition to the transmission of both private messages, the relay node has the following tasks as shown in Figure 1: the transmission of a common message to both nodes, and further, the transmission of a confidential message to one node, which should be kept secret from the other non-legitimate node. Since the receiving nodes can use their own message from the previous phase for decoding, this channel differs from the classical broadcast scenario and is therefore called *bidirectional broadcast channel (BBC) with common and confidential messages*. For this scenario we completely characterize the optimal integration of private, common, and confidential services at the physical layer.

The rest of this paper is organized as follows. In Section II we introduce the BBC with common and confidential messages and derive the secrecy capacity region for discrete memoryless channels. In Section III we prove the corresponding result for MIMO Gaussian channels. It is shown that these results unify previous partial results, where the relay provides only some of the services. This is discussed in Section IV, while Section V concludes the paper.

*Notation*

In this paper we denote random variables by non-italic capital letters and their realizations and ranges by lower case italic letters and script letters, respectively; scalars, vectors, and matrices are denoted by lower case letters, bold lower case letters, and bold capital letters; $H(\cdot)$, $h(\cdot)$, and $I(\cdot;\cdot)$ are the traditional entropy, differential entropy, and mutual information; $\mathrm{X}-\mathrm{Y}-\mathrm{Z}$ denotes a Markov chain of the random variables X, Y, and Z in this order; $\mathbb{N}$ and $\mathbb{R}_+$ are the sets of non-negative integers and non-negative real numbers; $(\cdot)^{-1}$, $(\cdot)^T$, and $|\cdot|$ denote the inverse, transpose, and determinant respectively; $\mathrm{tr}(\cdot)$ is the trace of a matrix; $\boldsymbol{Q} \succeq \mathbf{0}$ means the matrix $\boldsymbol{Q}$ is positive semidefinite; $\mathbb{E}\{\cdot\}$ and $\mathbb{P}\{\cdot\}$ are the expectation and probability; $A_\epsilon^{(n)}(\cdot)$ is the set of (weakly) typical sequences, cf. for example [27].

## II. Bidirectional Broadcast Channel with Common and Confidential Messages

In this section we analyze physical layer service integration in bidirectional relay networks for discrete memoryless channels with finite input and output alphabets. This channel model is motivated by the fact that in practical systems, a transmitter usually uses a finite modulation scheme and a receiver usually quantizes the received signal before further base band processing.

Besides establishing the bidirectional communication, the relay integrates additional common and confidential messages in the broadcast phase, which necessitates the study of the *bidirectional broadcast channel (BBC) with common and confidential messages*. The aim of the relay node is to integrate all messages as efficiently as possible while keeping the confidential message secret from the non-legitimate node. We address this transmission problem from a general point of view and therefore derive the corresponding secrecy capacity region. This allows us to gain insights to the best possible approach for the integration of private, common, and confidential messages in bidirectional relay networks. It characterizes the maximal achievable rates for all messages, while at the same time keeping the non-legitimate node ignorant of the confidential message. We prove the secrecy capacity region using random coding arguments which mainly exploit ideas of the BBC with common messages [28], and of the classical broadcast channel with confidential messages [8, 29].

### A. Physical Layer Description and Capacity Result

Let $\mathcal{X}$ and $\mathcal{Y}_i$, $i = 1, 2$, be finite input and output sets. Then for input and output sequences $x^n \in \mathcal{X}^n$ and $y_i^n \in \mathcal{Y}_i^n$, $i = 1, 2$, of length $n$, the discrete memoryless broadcast channel is given by $W^{\otimes n}(y_1^n, y_2^n|x^n) \coloneqq \prod_{k=1}^n W(y_{1,k}, y_{2,k}|x_k)$. We do not allow any cooperation between the receiving nodes so that it is sufficient to consider the marginal transition probabilities $W_i^{\otimes n} \coloneqq \prod_{k=1}^n W_i(y_{i,k}|x_k)$, $i = 1, 2$ only.

We consider the standard model with a block code of arbitrary but fixed length $n$. The set of private messages of node $i$, $i = 1, 2$, is denoted by $\mathcal{M}_i \coloneqq \{1, ..., M_{i,n}\}$, which is also known at the relay node. Further, the sets of common and confidential messages of the relay node are denoted by $\mathcal{M}_0 \coloneqq \{1, ..., M_{0,n}\}$ and $\mathcal{M}_c \coloneqq \{1, ..., M_{c,n}\}$, respectively. We use the abbreviation $\mathcal{M}_p \coloneqq \mathcal{M}_0 \times \mathcal{M}_1 \times \mathcal{M}_2$ for all public messages, and further $\mathcal{M} \coloneqq \mathcal{M}_c \times \mathcal{M}_p$.

In the bidirectional broadcast (BBC) phase, we assume that the relay has successfully decoded both private messages $m_1 \in \mathcal{M}_1$ and $m_2 \in \mathcal{M}_2$ which nodes 1 and 2 have transmitted in the previous multiple access (MAC) phase. Besides both private messages, the relay additionally integrates a common message $m_0 \in \mathcal{M}_0$ for both nodes and a confidential message $m_c \in \mathcal{M}_c$ for node 1, which should be kept secret from the non-legitimate node 2.

*Definition 1:* An $(n, M_{c,n}, M_{0,n}, M_{1,n}, M_{2,n})$*-code* for the BBC with common and confidential messages consists of one (stochastic) encoder at the relay node

$$f : \mathcal{M}_c \times \mathcal{M}_0 \times \mathcal{M}_1 \times \mathcal{M}_2 \to \mathcal{X}^n$$

and decoders at nodes 1 and 2

$$g_1 : \mathcal{Y}_1^n \times \mathcal{M}_1 \to \mathcal{M}_c \times \mathcal{M}_0 \times \mathcal{M}_2$$
$$g_2 : \mathcal{Y}_2^n \times \mathcal{M}_2 \to \mathcal{M}_0 \times \mathcal{M}_1.$$

When the relay has sent the message $m = (m_c, m_0, m_1, m_2)$, and nodes 1 and 2 have received $y_1^n$ and $y_2^n$, the decoder at node 1 is in error if $g_1(y_1^n, m_1) \neq (m_c, m_0, m_2)$. Accordingly, the decoder at node 2 is in error if $g_2(y_2^n, m_2) \neq (m_0, m_1)$. Then, the average probability of error at node $i$, $i = 1, 2$ is given by

$$\mu_{i,n} \coloneqq \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} \lambda_i(m)$$

with $\lambda_1(m) = \mathbb{P}\{g_1(y_1^n, m_1) \neq (m_c, m_0, m_2) | m \text{ sent}\}$ and $\lambda_2(m) = \mathbb{P}\{g_2(y_2^n, m_2) \neq (m_0, m_1) | m \text{ sent}\}$.

The secrecy level of the confidential message $m_c \in \mathcal{M}_c$ is characterized by the concept of equivocation rate as, for example, is done in [7, 8]. Here, the equivocation rate $\frac{1}{n} H(\mathrm{M}_c | \mathrm{Y}_2^n, \mathrm{M}_2)$ describes the uncertainty of node 2 about the confidential message $\mathrm{M}_c$, having the received sequence $\mathrm{Y}_2^n$ and its own message $\mathrm{M}_2$ as side information available under the assumption that the random variables $\mathrm{M}_c$ and $\mathrm{M}_2$ are uniformly distributed over $\mathcal{M}_c$ and $\mathcal{M}_2$. Consequently, the higher the equivocation rate, the higher the secrecy level of the confidential message.

*Definition 2:* A rate tuple $\boldsymbol{R} = (R_c, R_0, R_1, R_2) \in \mathbb{R}_+^4$ is said to be *achievable* for the BBC with common and confidential messages if for any $\delta > 0$ there is an $n(\delta) \in \mathbb{N}$ and a sequence of $(n, M_{c,n}, M_{0,n}, M_{1,n}, M_{2,n})$-codes such that for all $n \geq n(\delta)$ we have $\frac{1}{n} \log M_{c,n} \geq R_c - \delta$, $\frac{1}{n} \log M_{0,n} \geq R_0 - \delta$, $\frac{1}{n} \log M_{2,n} \geq R_1 - \delta$, $\frac{1}{n} \log M_{1,n} \geq R_2 - \delta$, and

$$\tfrac{1}{n} H(\mathrm{M}_c | \mathrm{Y}_2^n, \mathrm{M}_2) \geq R_c - \delta \tag{1}$$

while $\mu_{1,n}, \mu_{2,n} \to 0$ as $n \to \infty$. The set of all achievable rate tuples is the *secrecy capacity region* of the BBC with common and confidential messages, and is denoted by $\mathcal{C}_{\mathrm{BBC}}$.

*Remark 1:* The secrecy condition (1) requires that the equivocation rate is as high as the rate of the confidential message. Hence, it is often equivalently written as

$$\tfrac{1}{n} I(\mathrm{M}_c; \mathrm{Y}_2^n | \mathrm{M}_2) \leq \delta \tag{2}$$

and usually referred to as *perfect secrecy* condition.

Now we are in the position to state the secrecy capacity region of the BBC with common and confidential messages.

*Theorem 1:* The secrecy capacity region $\mathcal{C}_{\mathrm{BBC}}$ of the discrete memoryless BBC with common and confidential messages is the set of all rate tuples $\boldsymbol{R} \in \mathbb{R}_+^4$ that satisfy

$$R_c \leq I(\mathrm{V}; \mathrm{Y}_1 | \mathrm{U}) - I(\mathrm{V}; \mathrm{Y}_2 | \mathrm{U}) \tag{3a}$$
$$R_0 + R_i \leq I(\mathrm{U}; \mathrm{Y}_i), \quad i = 1, 2 \tag{3b}$$

with perfect secrecy, i.e., (1) is satisfied, for random variables $\mathrm{U} - \mathrm{V} - \mathrm{X} - (\mathrm{Y}_1, \mathrm{Y}_2)$. The cardinalities of the ranges of U and V can be bounded by $|\mathcal{U}| \leq |\mathcal{X}| + 3$ and $|\mathcal{V}| \leq |\mathcal{X}|^2 + 4|\mathcal{X}| + 3$.

*Remark 2:* The security criterion is always given in terms of equivocation rate, which means that the equivocation is normalized by the block length $n$, cf. (1) and (2). This criterion is also known as weak secrecy and is heuristically reasonable, but no operational meaning has been given to it yet. There is a stronger version where (2) is strengthened by dropping the division by $n$ and thereby considering the absolute amount of information leaked to the non-legitimate node [30]. For the classical wiretap setup, the *strong secrecy* criterion has been given an operational meaning: it was established in [31, 32] that under the strong secrecy criterion, the average decoding error at a non-legitimate receiver tends to one for any decoding strategy it may use.

The operational meaning of strong secrecy in [31, 32] can also be interpreted as security against an attack of the wiretapper to decode the confidential message. The extension to other forms of attacks, such as identification attacks based on [33], or active wiretappers, would be an interesting and worthwhile research direction for future wireless systems.

Theorem 1 is proved in the following two subsections.

### B. Proof of Achievability

Here, we present a coding strategy that achieves the desired rates with prefect secrecy and therewith prove the achievability of Theorem 1.

*Lemma 1:* Let $\mathrm{U} - \mathrm{X} - (\mathrm{Y}_1, \mathrm{Y}_2)$ and $I(\mathrm{X}; \mathrm{Y}_1 | \mathrm{U}) > I(\mathrm{X}; \mathrm{Y}_2 | \mathrm{U})$. Then all rate tuples $\boldsymbol{R} \in \mathbb{R}_+^4$ that satisfy

$$R_c \leq I(\mathrm{X}; \mathrm{Y}_1 | \mathrm{U}) - I(\mathrm{X}; \mathrm{Y}_2 | \mathrm{U}) \tag{4a}$$
$$R_0 + R_i \leq I(\mathrm{U}; \mathrm{Y}_i), \quad i = 1, 2 \tag{4b}$$

are achievable with perfect secrecy, i.e., condition (1) is satisfied.

*Proof:* The proof uses the same codebook idea as presented in [34, Lemma 1] for the BBC with confidential messages (and no common messages) which is actually based on ideas for the classical broadcast channel with common and confidential messages [8] and the BBC with common messages [28]. It consists of two superimposed layers of codewords; one for the public communication, i.e., the common and individual messages, and one for the confidential communication. The structure of the codebook is visualized in Figure 2. For further details we refer to [34]. ■

By introducing an auxiliary channel V that enables additional randomization, the desired region in Theorem 1 follows immediately from Lemma 1 by standard arguments, cf. [8, 34].

To complete the proof all that remains is to bound the cardinalities of $\mathcal{U}$ and $\mathcal{V}$. Since the cardinalities depend only on the structure of the random variables, the bounds follow

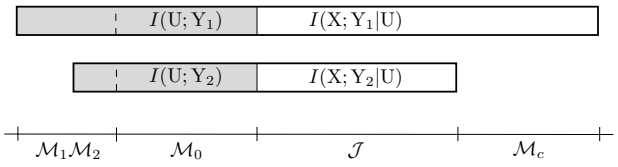



Fig. 2. Structure of the codebook for the BBC with common and confidential messages. It consists of two layers, one for the public communication (gray) and one for the confidential communication (white). The randomization set $\mathcal{J}$ is designed such that the non-legitimate node is forced to decode the corresponding index at the maximum rate its channel provide and therefore is not able to obtain any information about the confidential message.

immediately from [8, Appendix] or [34]. This completes the proof of achievability. ■

### C. Proof of Converse

To prove the weak converse we need a version of Fano's lemma that is suitable for the BBC with common and confidential messages.

*Lemma 2 (Fano's inequality):* For the BBC with common and confidential messages we have the following versions of Fano's inequality

$$\begin{aligned} &H(\mathrm{M}_c,\mathrm{M}_0,\mathrm{M}_2|\mathrm{Y}_1^n,\mathrm{M}_1) \\ &\qquad \le \mu_{1,n}\log(M_{c,n}M_{0,n}M_{2,n})+1 = n\epsilon_{1,n} \\ &H(\mathrm{M}_0,\mathrm{M}_1|\mathrm{Y}_2^n,\mathrm{M}_2) \\ &\qquad \le \mu_{2,n}\log(M_{0,n}M_{1,n})+1 = n\epsilon_{2,n} \end{aligned}$$

with $\epsilon_{1,n} = \frac{1}{n}\log(M_{c,n}M_{0,n}M_{2,n})\mu_{1,n}+\frac{1}{n} \to 0$ and $\epsilon_{2,n} = \frac{1}{n}\log(M_{0,n}M_{1,n})\mu_{2,n}+\frac{1}{n} \to 0$ for $n\to\infty$ as $\mu_{1,n},\mu_{2,n}\to 0$.

*Proof:* The lemma can be shown analogously as in [25, 28], where similar versions of Fano's inequality for the BBC (without confidential messages) are presented. ■

Next, we have to show that for any given sequence of $(n, M_{c,n}, M_{0,n}, M_{1,n}, M_{2,n})$-codes with $\mu_{1,n},\mu_{2,n}\to 0$ there exist random variables $\mathrm{U}-\mathrm{V}-\mathrm{X}-(\mathrm{Y}_1,\mathrm{Y}_2)$ such that all rate tuples $\boldsymbol{R} = (R_c,R_0,R_1,R_2) \in \mathbb{R}_+^4$ are bounded by (3). For notational convenience we introduce the abbreviation $\mathrm{M}_p = (\mathrm{M}_0,\mathrm{M}_1,\mathrm{M}_2)$.

From the independence of $\mathrm{M}_c$, $\mathrm{M}_0$, $\mathrm{M}_1$, $\mathrm{M}_2$, the chain rule for entropy, the definition of mutual information, Fano's inequality, cf. Lemma 2, and the chain rule for mutual information, we get for the public rates

$$\begin{aligned} n(R_0+R_1) &\le H(\mathrm{M}_0)+H(\mathrm{M}_2) = H(\mathrm{M}_0,\mathrm{M}_2|\mathrm{M}_1) \\ &\le I(\mathrm{M}_0,\mathrm{M}_2;\mathrm{Y}_1^n|\mathrm{M}_1)+n\epsilon_{1,n} \\ &\le I(\mathrm{M}_p;\mathrm{Y}_1^n)+n\epsilon_{1,n} \end{aligned} \tag{5}$$

and similarly

$$n(R_0+R_2) \le I(\mathrm{M}_p;\mathrm{Y}_2^n)+n\epsilon_{2,n}. \tag{6}$$

Due to the perfect secrecy condition (1) the confidential rate is bounded by

$$\begin{aligned} nR_c &\le H(\mathrm{M}_c|\mathrm{Y}_2^n,\mathrm{M}_2) \\ &= H(\mathrm{M}_c|\mathrm{Y}_2^n,\mathrm{M}_p)+I(\mathrm{M}_c;\mathrm{M}_0,\mathrm{M}_1|\mathrm{Y}_2^n,\mathrm{M}_2) \\ &= H(\mathrm{M}_c|\mathrm{M}_p)-I(\mathrm{M}_c;\mathrm{Y}_2^n|\mathrm{M}_p) \\ &\qquad +I(\mathrm{M}_c;\mathrm{M}_0,\mathrm{M}_1|\mathrm{Y}_2^n,\mathrm{M}_2) \\ &= I(\mathrm{M}_c;\mathrm{Y}_1^n|\mathrm{M}_p)-I(\mathrm{M}_c;\mathrm{Y}_2^n|\mathrm{M}_p) \\ &\qquad +H(\mathrm{M}_c|\mathrm{Y}_1^n,\mathrm{M}_p)+I(\mathrm{M}_c;\mathrm{M}_0,\mathrm{M}_1|\mathrm{Y}_2^n,\mathrm{M}_2) \\ &\le I(\mathrm{M}_c;\mathrm{Y}_1^n|\mathrm{M}_p)-I(\mathrm{M}_c;\mathrm{Y}_2^n|\mathrm{M}_p)+n\epsilon_{1,n}+n\epsilon_{2,n} \end{aligned} \tag{7}$$

where the last inequality follows from $H(\mathrm{M}_c|\mathrm{Y}_1^n,\mathrm{M}_p) \le H(\mathrm{M}_c,\mathrm{M}_0,\mathrm{M}_2|\mathrm{Y}_1^n,\mathrm{M}_1) \le n\epsilon_{1,n}$, $I(\mathrm{M}_c;\mathrm{M}_0,\mathrm{M}_1|\mathrm{Y}_2^n,\mathrm{M}_2) = H(\mathrm{M}_0,\mathrm{M}_1|\mathrm{Y}_2^n,\mathrm{M}_2) - H(\mathrm{M}_0,\mathrm{M}_1|\mathrm{Y}_2^n,\mathrm{M}_c,\mathrm{M}_2) \le H(\mathrm{M}_0,\mathrm{M}_1|\mathrm{Y}_2^n,\mathrm{M}_2) \le n\epsilon_{2,n}$, and Fano's inequality, cf. Lemma 2.

Once we have established the bounds (5)-(7), the rest of the proof goes along with [34, Sec. IV]. Starting from [34, Eq. (17)] and introducing auxiliary random variables U and V that satisfy the Markov chain relation $\mathrm{U}-\mathrm{V}-\mathrm{X}-(\mathrm{Y}_1,\mathrm{Y}_2)$, it is straightforward to show that

$$\begin{aligned} &I(\mathrm{M}_p;\mathrm{Y}_i^n) \le nI(\mathrm{U};\mathrm{Y}_i), \quad i=1,2 \\ &I(\mathrm{M}_c;\mathrm{Y}_1^n|\mathrm{M}_p)-I(\mathrm{M}_c;\mathrm{Y}_2^n|\mathrm{M}_p) \\ &\qquad \le nI(\mathrm{V};\mathrm{Y}_1|\mathrm{U})-nI(\mathrm{V};\mathrm{Y}_2|\mathrm{U}). \end{aligned}$$

Substituting this into (5)-(7) and dividing by $n$, we end up with (3) which establishes the weak converse. ■

## III. MIMO Gaussian Channels

In this section we consider physical layer service integration multiantenna bidirectional relay networks and prove the corresponding secrecy capacity region of the MIMO Gaussian BBC with common and confidential messages. In principle, the secrecy capacity region is computable by evaluating the corresponding region of the discrete case for MIMO Gaussian channels. Unfortunately, a direct evaluation is almost intractable due to the presence of the auxiliary random variables U and V, cf. Theorem 1, so that we establish a precise matrix characterization in the following.

The main idea for proving the secrecy capacity is to construct an enhanced MIMO Gaussian BBC that reveals some degradedness similar to [29]. This results in a secrecy capacity region that needs only one auxiliary random variable, which again makes the evaluation tractable. Finally, an extremal entropy inequality from [35] establishes the desired result.

### A. Physical Layer Description and Capacity Result

Here we consider MIMO Gaussian channels. Therefore let $N_R$ be the number of antennas at the relay node and $N_i$ be the number of antennas at node $i$, $i=1,2$, as shown in Figure 3. The discrete-time real-valued input-output relation between the relay node and node $i$, $i=1,2$, can now be modeled as

$$\boldsymbol{y}_i = \boldsymbol{H}_i\boldsymbol{x}+\boldsymbol{n}_i, \tag{8}$$

where $\boldsymbol{y}_i \in \mathbb{R}^{N_i\times 1}$ denotes the output at node $i$, $\boldsymbol{H}_i \in \mathbb{R}^{N_i\times N_R}$ the multiplicative channel matrix, $\boldsymbol{x} \in \mathbb{R}^{N_R\times 1}$ the

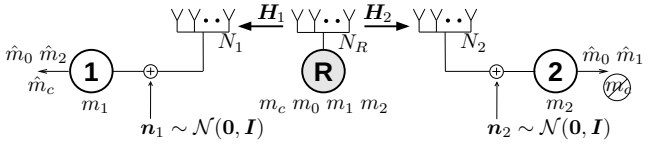



Fig. 3. General MIMO Gaussian BBC with common and confidential messages.

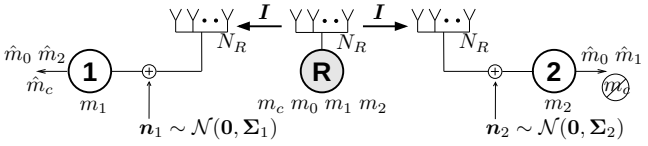



Fig. 4. Aligned MIMO Gaussian BBC with common and confidential messages.

input of the relay node, and $\boldsymbol{n}_i \in \mathbb{R}^{N_i \times 1}$ the independent additive noise according to a Gaussian distribution $\mathcal{N}(\boldsymbol{0}, \boldsymbol{I}_{N_i})$ with zero mean and identity covariance matrix. We assume perfect channel state information at all nodes.

As in [29, 36, 37], we consider two different kinds of power constraints: an average power constraint and a more general matrix power constraint. An input sequence $\boldsymbol{x}^n = (\boldsymbol{x}_1, \boldsymbol{x}_2, ..., \boldsymbol{x}_n)$ of length $n$ satisfies an average power constraint $P$ if

$$\frac{1}{n}\sum_{k=1}^{n} \boldsymbol{x}_k^T \boldsymbol{x}_k \leq P \tag{9}$$

holds. Similarly, a sequence $\boldsymbol{x}^n$ satisfies a matrix power constraint $\boldsymbol{S}$ if

$$\frac{1}{n}\sum_{k=1}^{n} \boldsymbol{x}_k \boldsymbol{x}_k^T \preceq \boldsymbol{S} \tag{10}$$

where $\boldsymbol{S} \succeq \boldsymbol{0}$ is a positive semidefinite matrix.[1]

*Theorem 2:* The secrecy capacity region $\mathcal{C}_{\text{BBC}}^{\text{MIMO}}$ of the MIMO Gaussian BBC with common and confidential messages under the matrix power constraint $\boldsymbol{S}$ is the set of all rate tuples $\boldsymbol{R} \in \mathbb{R}_+^4$ that satisfy

$$\begin{aligned} R_c &\leq \frac{1}{2}\log\left|\boldsymbol{I}_{N_1} + \boldsymbol{H}_1\boldsymbol{Q}^{(c)}\boldsymbol{H}_1^T\right| \\ &\quad - \frac{1}{2}\log\left|\boldsymbol{I}_{N_2} + \boldsymbol{H}_2\boldsymbol{Q}^{(c)}\boldsymbol{H}_2^T\right| \\ R_0 + R_i &\leq \frac{1}{2}\log\left|\frac{\boldsymbol{I}_{N_i} + \boldsymbol{H}_i\boldsymbol{S}\boldsymbol{H}_i^T}{\boldsymbol{I}_{N_i} + \boldsymbol{H}_i\boldsymbol{Q}^{(c)}\boldsymbol{H}_i^T}\right|, \quad i = 1, 2 \end{aligned}$$

for some $\boldsymbol{0} \preceq \boldsymbol{Q}^{(c)} \preceq \boldsymbol{S}$.

Having [36, Lemma 1] in mind, we immediately obtain from the secrecy capacity region under the matrix power constraint (10) the corresponding region under the average power constraint (9) which usually characterizes the practically more relevant case.

*Corollary 1:* The secrecy capacity region $\mathcal{C}_{\text{BBC}}^{\text{MIMO}}$ of the MIMO Gaussian BBC with common and confidential messages under the average power constraint $P$ is the set of all rate tuples $\boldsymbol{R} \in \mathbb{R}_+^4$ that satisfy

$$\begin{aligned} R_c &\leq \frac{1}{2}\log\left|\boldsymbol{I}_{N_1} + \boldsymbol{H}_1\boldsymbol{Q}^{(c)}\boldsymbol{H}_1^T\right| \\ &\quad - \frac{1}{2}\log\left|\boldsymbol{I}_{N_2} + \boldsymbol{H}_2\boldsymbol{Q}^{(c)}\boldsymbol{H}_2^T\right| \\ R_0 + R_i &\leq \frac{1}{2}\log\left|\frac{\boldsymbol{I}_{N_i} + \boldsymbol{H}_i(\boldsymbol{Q}^{(c)} + \boldsymbol{Q}^{(p)})\boldsymbol{H}_i^T}{\boldsymbol{I}_{N_i} + \boldsymbol{H}_i\boldsymbol{Q}^{(c)}\boldsymbol{H}_i^T}\right|, \quad i = 1, 2 \end{aligned}$$

for some $\boldsymbol{Q}^{(c)} \succeq \boldsymbol{0}$, $\boldsymbol{Q}^{(p)} \succeq \boldsymbol{0}$ with $\text{tr}(\boldsymbol{Q}^{(c)} + \boldsymbol{Q}^{(p)}) \leq P$. ■

[1]The notation $\boldsymbol{A} \succeq \boldsymbol{B}$ means the matrix $\boldsymbol{A} - \boldsymbol{B}$ is positive semidefinite.

Theorem 2 is proved in the following subsections. First, we consider the special case of square and invertible channel matrices and establish the secrecy capacity region for this case using channel-enhancement arguments. Then we outline how this result can be extended to arbitrary (possibly non-square and non-invertible) channel matrices using standard approximation arguments as in [29, 36, 37] to finally end up with the desired result.

### *B. Aligned MIMO Bidirectional Broadcast Channel*

In this section, we consider the case where the channel matrices $\boldsymbol{H}_1$ and $\boldsymbol{H}_2$ are square and invertible. Then, multiplying both sides (8) by $\boldsymbol{H}_i^{-1}$, an equivalent channel model is given by

$$\boldsymbol{y}_i = \boldsymbol{x} + \boldsymbol{n}_i \tag{11}$$

where $\boldsymbol{y}_i, \boldsymbol{x}, \boldsymbol{n}_i \in \mathbb{R}^{N_R \times 1}$ but the additive noise $\boldsymbol{n}_i$ is now Gaussian distributed with zero mean and covariance matrix

$$\boldsymbol{\Sigma}_i = \boldsymbol{H}_i^{-1}\boldsymbol{H}_i^{-T} \in \mathbb{R}^{N_R \times N_R}, \tag{12}$$

i.e., $\boldsymbol{n}_i \sim \mathcal{N}(\boldsymbol{0}, \boldsymbol{\Sigma}_i)$, $i = 1, 2$, as shown in Figure 4. We adopt the notation used in [29, 36] and call the channel model (11) the *aligned* MIMO Gaussian BBC and (8) the *general* MIMO Gaussian BBC. The main result for the aligned case is summarized in the following theorem.

*Theorem 3:* The secrecy capacity region $\mathcal{C}_{\text{BBC}}^{\text{aligned}}$ of the aligned MIMO Gaussian BBC with common and confidential messages under the matrix power constraint $\boldsymbol{S}$ is the set of all rate tuples $\boldsymbol{R} \in \mathbb{R}_+^4$ that satisfy

$$\begin{aligned} R_c &\leq \frac{1}{2}\log\left|\frac{\boldsymbol{Q}^{(c)} + \boldsymbol{\Sigma}_1}{\boldsymbol{\Sigma}_1}\right| - \frac{1}{2}\log\left|\frac{\boldsymbol{Q}^{(c)} + \boldsymbol{\Sigma}_2}{\boldsymbol{\Sigma}_2}\right| \\ R_0 + R_i &\leq \frac{1}{2}\log\left|\frac{\boldsymbol{S} + \boldsymbol{\Sigma}_i}{\boldsymbol{Q}^{(c)} + \boldsymbol{\Sigma}_i}\right|, \quad i = 1, 2 \end{aligned} \tag{13}$$

for some $\boldsymbol{0} \preceq \boldsymbol{Q}^{(c)} \preceq \boldsymbol{S}$.

The theorem is proved in the following two subsections.

### *C. Proof of Achievability*

Similarly, as for the classical aligned MIMO Gaussian broadcast channel [29], the proof of achievability is a straightforward extension of its discrete counterpart. To obtain the desired region (13) we follow the proof of the discrete case, cf. Section II, with a proper choice of auxiliary and input random variables. More precisely, with $\mathrm{G} \sim \mathcal{N}(\boldsymbol{0}, \boldsymbol{Q}^{(c)})$ for the confidential messages and $\mathrm{U} \sim \mathcal{N}(\boldsymbol{0}, \boldsymbol{S} - \boldsymbol{Q}^{(c)})$ for the public messages with G and U being independent, and further $\mathrm{V} = \mathbf{X} = \mathrm{U} + \mathrm{G}$, the region (13) follows immediately from Theorem 1. Therefore we omit the details for brevity.

### D. Proof of Converse

To establish the converse it remains to show that no other rate tuples than characterized by (13) are achievable for some $\mathbf{0} \preceq \boldsymbol{Q}^{(c)} \preceq \boldsymbol{S}$. At this point it suffices to consider only matrix power constraints that satisfy $\boldsymbol{S} \succ \mathbf{0}$.[2]

We prove the optimality by contradiction. Therefore, we construct a rate tuple $\boldsymbol{R}^o = (R_c^o, R_0^o, R_1^o, R_2^o) \in \mathbb{R}_+^4$ that lies outside the desired region (13) and assume that this rate tuple is achievable for the aligned MIMO Gaussian BBC with common and confidential messages.

First, we observe that achievable public rates $R_0^o$, $R_1^o$, and $R_2^o$ are bounded from above by

$$R_0^o + R_i^o \leq \frac{1}{2}\log\left|\frac{\boldsymbol{S}+\boldsymbol{\Sigma}_i}{\boldsymbol{\Sigma}_i}\right|, \quad i = 1, 2.$$

We note that for $R_c^o = 0$ and $\boldsymbol{Q}^{(c)} = \mathbf{0}$ in (13) there are public rates that actually achieve this upper bound. Further, for given achievable public rates $R_0^o$, $R_1^o$, and $R_2^o$ the achievable confidential rate $R_{c,\text{opt}}$ according to Theorem 3 is characterized by the following optimization problem:

$$\begin{aligned} \max_{\boldsymbol{Q}^{(c)}} \quad & \frac{1}{2}\log\left|\frac{\boldsymbol{Q}^{(c)}+\boldsymbol{\Sigma}_1}{\boldsymbol{\Sigma}_1}\right| - \frac{1}{2}\log\left|\frac{\boldsymbol{Q}^{(c)}+\boldsymbol{\Sigma}_2}{\boldsymbol{\Sigma}_2}\right| \\ \text{s.t.} \quad & \frac{1}{2}\log\left|\frac{\boldsymbol{S}+\boldsymbol{\Sigma}_i}{\boldsymbol{Q}^{(c)}+\boldsymbol{\Sigma}_i}\right| \geq R_0^o + R_i^o, \quad i = 1, 2 \\ & \mathbf{0} \preceq \boldsymbol{Q}^{(c)} \preceq \boldsymbol{S}. \end{aligned} \tag{14}$$

Finally, we set $R_c^o = R_{c,\text{opt}} + \delta$ for some $\delta > 0$ to ensure that this rate tuple lies outside the region (13) as required, i.e., $\boldsymbol{R}^o \notin \mathcal{C}_{\text{BBC}}^{\text{aligned}}$.

Then the Lagrangian for the corresponding minimization problem of (14) is given by

$$\begin{aligned} \mathcal{L}(\boldsymbol{Q}^{(c)}, \boldsymbol{\mu}, \boldsymbol{\Psi}_1, \boldsymbol{\Psi}_2) &= \frac{1}{2}\log\left|\frac{\boldsymbol{Q}^{(c)}+\boldsymbol{\Sigma}_2}{\boldsymbol{\Sigma}_2}\right| - \frac{1}{2}\log\left|\frac{\boldsymbol{Q}^{(c)}+\boldsymbol{\Sigma}_1}{\boldsymbol{\Sigma}_1}\right| \\ &\quad + \sum_{i=1}^{2}\mu_i\Big(R_0^o + R_i^o - \frac{1}{2}\log\left|\frac{\boldsymbol{S}+\boldsymbol{\Sigma}_i}{\boldsymbol{Q}^{(c)}+\boldsymbol{\Sigma}_i}\right|\Big) \\ &\quad - \operatorname{tr}(\boldsymbol{Q}^{(c)}\boldsymbol{\Psi}_1) + \operatorname{tr}\big((\boldsymbol{Q}^{(c)} - \boldsymbol{S})\boldsymbol{\Psi}_2\big) \end{aligned}$$

with Lagrange multipliers $\boldsymbol{\mu} = (\mu_1, \mu_2)$, $\mu_i \geq 0$, and $\boldsymbol{\Psi}_i \succeq \mathbf{0}$, $i = 1, 2$. Then we know from the Karush-Kuhn-Tucker (KKT) conditions, cf. for example [38], that the derivative of the Lagrangian must vanish at an optimal $\boldsymbol{Q}_{\text{opt}}^{(c)}$ which yields[3]

$$\begin{aligned} &\frac{\mu_1}{2}\big(\boldsymbol{Q}_{\text{opt}}^{(c)} + \boldsymbol{\Sigma}_1\big)^{-1} + \frac{\mu_2+1}{2}\big(\boldsymbol{Q}_{\text{opt}}^{(c)} + \boldsymbol{\Sigma}_2\big)^{-1} + \boldsymbol{\Psi}_2 \\ &\qquad = \frac{1}{2}\big(\boldsymbol{Q}_{\text{opt}}^{(c)} + \boldsymbol{\Sigma}_1\big)^{-1} + \boldsymbol{\Psi}_1 \end{aligned} \tag{15}$$

while the optimal $\boldsymbol{Q}_{\text{opt}}^{(c)}$ further has to satisfy the complementary slackness conditions

$$\mu_i\left(R_0^o + R_i^o - \frac{1}{2}\log\left|\frac{\boldsymbol{S}+\boldsymbol{\Sigma}_i}{\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_i}\right|\right) = 0, \quad i = 1, 2 \tag{16}$$

$$\boldsymbol{Q}_{\text{opt}}^{(c)}\boldsymbol{\Psi}_1 = \mathbf{0}, \qquad (\boldsymbol{S} - \boldsymbol{Q}_{\text{opt}}^{(c)})\boldsymbol{\Psi}_2 = \mathbf{0}. \tag{17}$$

By combining (14) and (16) we get for the weighted secrecy sum-capacity of the constructed rate tuple $\boldsymbol{R}^o$ the following

$$\begin{aligned} &R_c^o + \mu_1(R_0^o + R_1^o) + \mu_2(R_0^o + R_2^o) \\ &\quad = R_{c,\text{opt}} + \delta + \mu_1(R_0^o + R_1^o) + \mu_2(R_0^o + R_2^o) \\ &\quad = \frac{1}{2}\log\left|\frac{\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_1}{\boldsymbol{\Sigma}_1}\right| - \frac{1}{2}\log\left|\frac{\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_2}{\boldsymbol{\Sigma}_2}\right| \\ &\qquad + \sum_{i=1}^{2}\frac{\mu_i}{2}\log\left|\frac{\boldsymbol{S}+\boldsymbol{\Sigma}_i}{\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_i}\right| + \delta. \end{aligned} \tag{18}$$

But we will show in the following that for any achievable rate tuple $\boldsymbol{R} \in \mathbb{R}_+^4$, the weighted secrecy sum-capacity is bounded from above by

$$\begin{aligned} &R_c + \mu_1(R_0 + R_1) + \mu_2(R_0 + R_2) \\ &\quad \leq \frac{1}{2}\log\left|\frac{\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_1}{\boldsymbol{\Sigma}_1}\right| - \frac{1}{2}\log\left|\frac{\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_2}{\boldsymbol{\Sigma}_2}\right| \\ &\qquad + \sum_{i=1}^{2}\frac{\mu_i}{2}\log\left|\frac{\boldsymbol{S}+\boldsymbol{\Sigma}_i}{\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_i}\right| \end{aligned}$$

which will then establish the desired contradiction to (18).

*1) Reinterpretation of Legitimate Receiver:* For the following analysis it will be beneficial to reinterpret this scenario by splitting the legitimate node 1 into two virtual receivers: one designated for the public and one for the confidential communication. Then, an equivalent aligned MIMO Gaussian BBC can be represented by

$$\boldsymbol{y}_{1\text{a}} = \boldsymbol{x} + \boldsymbol{n}_{1\text{a}} \tag{19a}$$

$$\boldsymbol{y}_{1\text{b}} = \boldsymbol{x} + \boldsymbol{n}_{1\text{b}} \tag{19b}$$

$$\boldsymbol{y}_2 = \boldsymbol{x} + \boldsymbol{n}_2 \tag{19c}$$

with $\boldsymbol{n}_{1\text{a}} \sim \mathcal{N}(\mathbf{0}, \boldsymbol{\Sigma}_1)$, $\boldsymbol{n}_{1\text{b}} \sim \mathcal{N}(\mathbf{0}, \boldsymbol{\Sigma}_1)$, and $\boldsymbol{n}_2 \sim \mathcal{N}(\mathbf{0}, \boldsymbol{\Sigma}_2)$. Here, each (virtual) receiver is only interested in either the public or the confidential messages. Receiver 1a wants to know the confidential message $m_c$, receiver 1b the public messages $m_0$ and $m_2$, and receiver 2 the public messages $m_0$ and $m_1$. Here the confidential message has to be kept secret only from receiver 2, but, of course, need not be kept secret from (virtual) receiver 1b.

Note that (virtual) receivers 1a and 1b in (19a) are affected by noise that has the same covariance matrix $\boldsymbol{\Sigma}_1$, cf. (12), which is the same as of the noise at the legitimate receiver 1 in the original aligned BBC (11). Similarly, the noise at receiver 2 in (19c) is according to the same covariance matrix $\boldsymbol{\Sigma}_2$, cf. (12), corresponding to the noise at the non-legitimate receiver 2 in (11). Therefore, any strategy that achieves a certain rate tuple for (11) will do likewise for (19) and vice versa, so that both scenarios share the same secrecy capacity region.

[2] For the validity of this restriction we refer to [36, Lemma 2].

[3] As in [36, Appendix IV] or [29] one can easily show that a set of constraint qualifications hold for the optimization problem (14). This implies that the KKT conditions hold and are necessary for characterizing the optimal transmit covariance matrix.

*2) Channel Enhancement:* Next, with the reinterpretation (19) of the communication scenario as a starting point, we enhance the channel designated for the confidential message, i.e., (virtual) receiver 1a. For this purpose let $\widetilde{\boldsymbol{\Sigma}}_1$ be a real symmetric matrix that satisfies

$$\frac{1}{2}(\boldsymbol{Q}_{\text{opt}}^{(c)}+\widetilde{\boldsymbol{\Sigma}}_1)^{-1}=\frac{1}{2}(\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_1)^{-1}+\boldsymbol{\Psi}_1. \tag{20}$$

Then we know from [36, Lemma 11] that

$$\mathbf{0}\prec\widetilde{\boldsymbol{\Sigma}}_1\preceq\boldsymbol{\Sigma}_1 \tag{21}$$

and

$$\left|\frac{\boldsymbol{Q}_{\text{opt}}^{(c)}+\widetilde{\boldsymbol{\Sigma}}_1}{\widetilde{\boldsymbol{\Sigma}}_1}\right|=\left|\frac{\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_1}{\boldsymbol{\Sigma}_1}\right| \tag{22}$$

hold. With (20), Equation (15) becomes

$$\begin{aligned}\frac{\mu_1}{2}(\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_1)^{-1}+\frac{\mu_2+1}{2}(\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_2)^{-1}+\boldsymbol{\Psi}_2\\ =\frac{1}{2}(\boldsymbol{Q}_{\text{opt}}^{(c)}+\widetilde{\boldsymbol{\Sigma}}_1)^{-1}.\end{aligned} \tag{23}$$

Since the matrices $(\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_1)^{-1}$, $(\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_2)^{-1}$, and $\boldsymbol{\Psi}_2$ on the right hand side of (23) are all positive semidefinite, it follows immediately that $\frac{1}{2}(\boldsymbol{Q}_{\text{opt}}^{(c)}+\widetilde{\boldsymbol{\Sigma}}_1)^{-1}\succeq\frac{1}{2}(\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_2)^{-1}$ and consequently

$$\widetilde{\boldsymbol{\Sigma}}_1\preceq\boldsymbol{\Sigma}_2. \tag{24}$$

This allows us to construct an enhanced MIMO Gaussian BBC by replacing the noise covariance matrix $\boldsymbol{\Sigma}_1$ at the (virtual) receiver 1a with its enhanced version $\widetilde{\boldsymbol{\Sigma}}_1$, cf. (21). Then, (19a) becomes

$$\tilde{\boldsymbol{y}}_{1\text{a}}=\boldsymbol{x}+\tilde{\boldsymbol{n}}_{1\text{a}} \tag{25}$$

with $\tilde{\boldsymbol{n}}_{1\text{a}}\sim\mathcal{N}(\mathbf{0},\widetilde{\boldsymbol{\Sigma}}_1)$, while the channels for receiver 1b and 2 remain the same. Figure 5 shows the communication scenario of the enhanced MIMO Gaussian BBC. Since $\widetilde{\boldsymbol{\Sigma}}_1\preceq\boldsymbol{\Sigma}_1$, cf. also (21), the covariance matrix of the noise for receiving the confidential message for the enhanced BBC (25) is "*smaller*" than for the original BBC (19). Hence, its secrecy capacity region is at least as large as that of the aligned MIMO Gaussian BBC. Moreover, from (21) and (24) we get

$$\mathbf{0}\preceq\widetilde{\boldsymbol{\Sigma}}_1\preceq\boldsymbol{\Sigma}_i,\quad i=1,2 \tag{26}$$

which means that both received signals $\boldsymbol{y}_{1\text{b}}$ and $\boldsymbol{y}_2$ at the public receivers are (stochastically) degraded with respect to the received signal $\tilde{\boldsymbol{y}}_{1\text{a}}$ at the confidential receiver. For the discrete memoryless counterpart of the enhanced BBC, the following proposition characterizes the corresponding secrecy capacity region.

*Proposition 1:* For a discrete memoryless BBC with common and confidential messages and transition probability $\widetilde{W}(\tilde{y}_{1a},y_{1b},y_2|x)$ that satisfies the Markov chain conditions $\mathrm{X}-\widetilde{\mathrm{Y}}_{1\text{a}}-\mathrm{Y}_{1\text{b}}$ and $\mathrm{X}-\widetilde{\mathrm{Y}}_{1\text{a}}-\mathrm{Y}_2$, the secrecy capacity region is given by the set of all rate tuples $\boldsymbol{R}\in\mathbb{R}_+^4$ that satisfy

$$\begin{aligned}R_c&\le I(\mathrm{X};\widetilde{\mathrm{Y}}_{1\text{a}}|\mathrm{U})-I(\mathrm{X};\mathrm{Y}_2|\mathrm{U})\\ R_0+R_1&\le I(\mathrm{U};\mathrm{Y}_{1\text{b}})\\ R_0+R_2&\le I(\mathrm{U};\mathrm{Y}_2)\end{aligned}$$

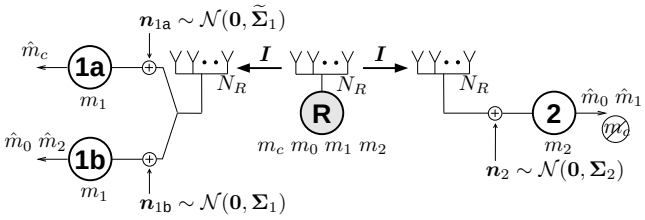



Fig. 5. Enhanced MIMO Gaussian BBC with common and confidential messages. Node 1 is split up into two virtual receivers, one enhanced for the confidential message and one for the public messages. For receiver 1a the noise covariance matrix $\boldsymbol{\Sigma}_1$ is replaced by $\widetilde{\boldsymbol{\Sigma}}_1$ to enhance the channel for the confidential message.

for random variables $\mathrm{U}-\mathrm{X}-\widetilde{\mathrm{Y}}_{1a}-(\mathrm{Y}_{1b},\mathrm{Y}_2)$.

*Proof:* Using the same ideas and techniques as for the non-degraded case, cf. Section II-B, the achievability follows immediately. Similarly, the converse follows the one in Section II-C while exploiting the degradedness as in [29, Proposition 1]. We omit the details for brevity. ■

*Remark 3:* In contrast to the non-degraded case, cf. Theorem 1, we only need one auxiliary random variable U instead of both U and V. This makes the evaluation of the secrecy capacity region for MIMO Gaussian channels tractable as is done in the following.

*3) Equivalence of Weighted Secrecy Sum-Capacity:* To establish the desired contradiction we must bound the weighted secrecy sum-capacity of the enhanced MIMO Gaussian BBC. As is done in [29] for the classical MIMO Gaussian broadcast channel with common and confidential messages, we use an extremal entropy inequality that is a special case of [35, Corollary 4].

*Proposition 2 ([35]):* Let $\tilde{\boldsymbol{n}}_{1\text{a}}\sim\mathcal{N}(\mathbf{0},\widetilde{\boldsymbol{\Sigma}}_1)$, $\boldsymbol{n}_{1\text{b}}\sim\mathcal{N}(\mathbf{0},\boldsymbol{\Sigma}_1)$, and $\boldsymbol{n}_2\sim\mathcal{N}(\mathbf{0},\boldsymbol{\Sigma}_2)$ be given, which satisfy $\mathbf{0}\preceq\widetilde{\boldsymbol{\Sigma}}_1\preceq\boldsymbol{\Sigma}_i$, $i=1,2$, cf. (26). Further, let $\boldsymbol{S}\succ\mathbf{0}$ be given. If there exists a $N_R\times N_R$ real symmetric matrix $\boldsymbol{Q}_{\text{opt}}^{(c)}$ such that $\mathbf{0}\preceq\boldsymbol{Q}_{\text{opt}}^{(c)}\preceq\boldsymbol{S}$ and satisfying

$$\begin{aligned}&\frac{1}{2}(\boldsymbol{Q}_{\text{opt}}^{(c)}+\widetilde{\boldsymbol{\Sigma}}_1)^{-1}\\ &\quad=\frac{\mu\lambda}{2}(\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_1)^{-1}+\frac{\mu(1-\lambda)}{2}(\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_2)^{-1}+\boldsymbol{\Psi}_2,\\ &(\boldsymbol{S}-\boldsymbol{Q}_{\text{opt}}^{(c)})\boldsymbol{\Psi}_2=\mathbf{0}\end{aligned}$$

for some $\boldsymbol{\Psi}_2\succeq\mathbf{0}$ and real scalars $\mu\ge0$ and $0\le\lambda\le1$, then

$$\begin{aligned}&h(\mathbf{X}+\widetilde{\mathbf{N}}_{1\text{a}}|\mathrm{U})-\mu\lambda h(\mathbf{X}+\mathbf{N}_{1\text{b}}|\mathrm{U})-\mu(1-\lambda)h(\mathbf{X}+\mathbf{N}_2|\mathrm{U})\\ &\quad\le\frac{1}{2}\log\left|2\pi e(\boldsymbol{Q}_{\text{opt}}^{(c)}+\widetilde{\mathbf{N}}_1)\right|-\frac{\mu\lambda}{2}\log\left|2\pi e(\boldsymbol{Q}_{\text{opt}}^{(c)}+\mathbf{N}_1)\right|\\ &\qquad-\frac{\mu(1-\lambda)}{2}\log\left|2\pi e(\boldsymbol{Q}_{\text{opt}}^{(c)}+\mathbf{N}_2)\right|\end{aligned}$$

for any $(\mathrm{U},\mathbf{X})$ independent of $(\widetilde{\mathbf{N}}_{1\text{a}},\mathbf{N}_{1\text{b}},\mathbf{N}_2)$ such that $\mathbb{E}\{\mathbf{X}\mathbf{X}^T\}\preceq\boldsymbol{S}$. ■

By Proposition 1 we get for the weighted secrecy sum-capacity of any rate tuple $\boldsymbol{R}\in\mathbb{R}_+^4$ for the enhanced BBC (25)

$$\begin{aligned}&R_c+\mu_1(R_0+R_1)+\mu_2(R_0+R_2)\\ &\quad\le I(\mathbf{X};\widetilde{\mathbf{Y}}_{1\text{a}}|\mathrm{U})-I(\mathbf{X};\mathbf{Y}_2|\mathrm{U})\\ &\qquad+\mu_1 I(\mathrm{U};\mathbf{Y}_{1\text{b}})+\mu_2 I(\mathrm{U};\mathbf{Y}_2)\end{aligned}$$

$$
\begin{aligned}
&= h(\mathbf{N}_2) - h(\widetilde{\mathbf{N}}_{1a}) + \mu_1 h(\mathbf{X}+\mathbf{N}_{1b}) + \mu_2 h(\mathbf{X}+\mathbf{N}_2) \\
&\qquad + \Big[ h(\mathbf{X}+\widetilde{\mathbf{N}}_{1a}|\mathrm{U}) - \mu_1 h(\mathbf{X}+\mathbf{N}_{1b}|\mathrm{U}) \\
&\qquad\qquad - (\mu_2+1) h(\mathbf{X}+\mathbf{N}_2|\mathrm{U}) \Big] \\
&\le \frac{1}{2}\log|2\pi e\boldsymbol{\Sigma}_2| - \frac{1}{2}\log\left|2\pi e\widetilde{\boldsymbol{\Sigma}}_1\right| \\
&\qquad + \sum_{i=1}^{2} \frac{\mu_i}{2}\log|2\pi e(\boldsymbol{S}+\boldsymbol{\Sigma}_i)| \\
&\qquad + \Big[ h(\mathbf{X}+\widetilde{\mathbf{N}}_{1a}|\mathrm{U}) - \mu_1 h(\mathbf{X}+\mathbf{N}_{1b}|\mathrm{U}) \\
&\qquad\qquad - (\mu_2+1) h(\mathbf{X}+\mathbf{N}_2|\mathrm{U}) \Big] \qquad (27)
\end{aligned}
$$

where the last inequality follows from $h(\widetilde{\mathbf{N}}_{1a}) = \frac{1}{2}\log\left|2\pi e\widetilde{\boldsymbol{\Sigma}}_1\right|$, $h(\mathbf{N}_2) = \frac{1}{2}\log|2\pi e\boldsymbol{\Sigma}_2|$ and $h(\mathbf{X}+\mathbf{N}_{1b}) \le \frac{1}{2}\log|2\pi e(\boldsymbol{S}+\boldsymbol{\Sigma}_1)|$, $h(\mathbf{X}+\mathbf{N}_2) \le \frac{1}{2}\log|2\pi e(\boldsymbol{S}+\boldsymbol{\Sigma}_2)|$.

Now with $\mu = \mu_1+\mu_2+1$ and $\lambda = \frac{\mu_1}{\mu_1+\mu_2+1}$ we get from (23) together with Proposition 2

$$
\begin{aligned}
&h(\mathbf{X}+\widetilde{\mathbf{N}}_{1a}|\mathrm{U}) - \mu_1 h(\mathbf{X}+\mathbf{N}_{1b}|\mathrm{U}) - (\mu_2+1) h(\mathbf{X}+\mathbf{N}_2|\mathrm{U}) \\
&\quad \le \frac{1}{2}\log\left|2\pi e(\boldsymbol{Q}_{\text{opt}}^{(c)} + \widetilde{\boldsymbol{\Sigma}}_1)\right| - \frac{\mu_1}{2}\log\left|2\pi e(\boldsymbol{Q}_{\text{opt}}^{(c)} + \boldsymbol{\Sigma}_1)\right| \\
&\qquad - \frac{\mu_2+1}{2}\log\left|2\pi e(\boldsymbol{Q}_{\text{opt}}^{(c)} + \boldsymbol{\Sigma}_2)\right|.
\end{aligned}
$$

Substituting this into (27) we end up with

$$
\begin{aligned}
&R_c + \mu_1(R_0+R_1) + \mu_2(R_0+R_2) \\
&\quad \le \frac{1}{2}\log\left|2\pi e\boldsymbol{\Sigma}_2\right| - \frac{1}{2}\log\left|2\pi e\widetilde{\boldsymbol{\Sigma}}_1\right| \\
&\qquad + \sum_{i=1}^{2}\frac{\mu_i}{2}\log\left|2\pi e(\boldsymbol{S}+\boldsymbol{\Sigma}_i)\right| + \frac{1}{2}\log\left|2\pi e(\boldsymbol{Q}_{\text{opt}}^{(c)} + \widetilde{\boldsymbol{\Sigma}}_1)\right| \\
&\qquad - \frac{\mu_1}{2}\log\left|2\pi e(\boldsymbol{Q}_{\text{opt}}^{(c)} + \boldsymbol{\Sigma}_1)\right| \\
&\qquad - \frac{\mu_2+1}{2}\log\left|2\pi e(\boldsymbol{Q}_{\text{opt}}^{(c)} + \boldsymbol{\Sigma}_2)\right| \\
&\quad = \frac{1}{2}\log\left|\frac{\boldsymbol{Q}_{\text{opt}}^{(c)} + \widetilde{\boldsymbol{\Sigma}}_1}{\widetilde{\boldsymbol{\Sigma}}_1}\right| - \frac{1}{2}\log\left|\frac{\boldsymbol{Q}_{\text{opt}}^{(c)} + \boldsymbol{\Sigma}_2}{\boldsymbol{\Sigma}_2}\right| \\
&\qquad + \sum_{i=1}^{2}\frac{\mu_i}{2}\log\left|\frac{\boldsymbol{S}+\boldsymbol{\Sigma}_i}{\boldsymbol{Q}_{\text{opt}}^{(c)} + \boldsymbol{\Sigma}_i}\right| \\
&\quad = \frac{1}{2}\log\left|\frac{\boldsymbol{Q}_{\text{opt}}^{(c)} + \boldsymbol{\Sigma}_1}{\boldsymbol{\Sigma}_1}\right| - \frac{1}{2}\log\left|\frac{\boldsymbol{Q}_{\text{opt}}^{(c)} + \boldsymbol{\Sigma}_2}{\boldsymbol{\Sigma}_2}\right| \\
&\qquad + \sum_{i=1}^{2}\frac{\mu_i}{2}\log\left|\frac{\boldsymbol{S}+\boldsymbol{\Sigma}_i}{\boldsymbol{Q}_{\text{opt}}^{(c)} + \boldsymbol{\Sigma}_i}\right| \qquad (28)
\end{aligned}
$$

where the last equality follows from (22), cf. [36, Lemma 11].

Since the secrecy capacity region of the aligned MIMO Gaussian BBC (8) is contained in the corresponding region of the enhanced MIMO Gaussian BBC (25), cf. also Section III-D2, it is clear that for any rate tuple $\boldsymbol{R} \in \mathbb{R}_+^4$ the upper bound on the weighted secrecy sum-capacity (28) – established above for the enhanced BBC – must hold, of course, for the non-enhanced aligned BBC as well. But since $\delta > 0$, this contradicts (18). This completes the proof of converse and therewith establishes the secrecy capacity region $\mathcal{C}_{\text{BBC}}^{\text{aligned}}$. ■

### E. General MIMO Bidirectional Broadcast Channel

Here we briefly outline how the results for the aligned MIMO Gaussian BBC (11) can be extended to the general case (8) to complete the proof of Theorem 2. Since the argumentation is the same as in [29, 36, 37], we only sketch the main ideas in the following.

Similarly as for the aligned case, cf. Theorem 3, the achievability follows from the discrete result in Theorem 1 with the same choice of auxiliary and input random variables. Therefore, the more intricate part is again the converse.

The case of square and invertible channel matrices can easily be transformed into an aligned MIMO Gaussian BBC, whose secrecy capacity region is known from Theorem 3. Thus, the goal is to approximate any general MIMO Gaussian BBC (with possibly non-square and non-invertible channel matrices) by an appropriate aligned MIMO Gaussian BBC. This can be done as in [29, 36, 37] where similar approximations are presented. This concludes the proof of the secrecy capacity of the general MIMO Gaussian BBC with common and confidential messages. ■

*Remark 4:* Interestingly, the derivation shows that a simple superposition strategy that superimposes two signals, one for the public messages and one for the confidential message, suffices to achieve capacity. Moreover, an additional randomization as in the discrete case, realized by the auxiliary random variable V in Theorem 1, is no longer needed for MIMO Gaussian channels.

## IV. Discussion

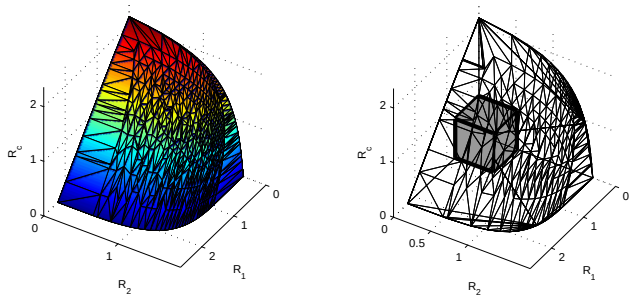
In this work we established the secrecy capacity region of the BBC with common and confidential messages where the relay transmits public private and common messages as well as a confidential message. This is a very general setup which includes some special cases where the relay provides only some these services. The corresponding capacity regions can be deduced from our result so that it unifies these previous partial results that were individually studied in [8, 28, 29, 34]. In more detail, if there are no confidential services for the relay to integrate, it solely transmits public services and the scenario reduces to the BBC with common messages [28]. For the case of no bidirectional messages we end up with the classical broadcast channel with common and confidential messages [29]. If the relay transmits only private and confidential messages, the scenario reduces to the BBC with confidential messages.

*Corollary 2:* The secrecy capacity region of the MIMO Gaussian BBC with confidential messages under the average power constraint $P$ is the set of all rate triples $(R_c, R_1, R_2) \in \mathbb{R}_+^3$ that satisfy

$$
\begin{aligned}
R_c &\le \frac{1}{2}\log\left|\boldsymbol{I}_{N_1} + \boldsymbol{H}_1\boldsymbol{Q}^{(c)}\boldsymbol{H}_1^T\right| - \frac{1}{2}\log\left|\boldsymbol{I}_{N_2} + \boldsymbol{H}_2\boldsymbol{Q}^{(c)}\boldsymbol{H}_2^T\right| \\
R_i &\le \frac{1}{2}\log\left|\frac{\boldsymbol{I}_{N_i} + \boldsymbol{H}_i(\boldsymbol{Q}^{(c)}+\boldsymbol{Q}^{(p)})\boldsymbol{H}_i^T}{\boldsymbol{I}_{N_i} + \boldsymbol{H}_i\boldsymbol{Q}^{(c)}\boldsymbol{H}_i^T}\right|, \quad i = 1,2
\end{aligned}
$$

for some $\boldsymbol{Q}^{(c)} \succeq \mathbf{0}$, $\boldsymbol{Q}^{(p)} \succeq \mathbf{0}$ with $\mathrm{tr}(\boldsymbol{Q}^{(c)}+\boldsymbol{Q}^{(p)}) \le P$. ■

Unfortunately, the optimal transmit covariance matrices are determined by non-convex optimization problems and so for




(a) Secrecy capacity region (b) Comparable TDMA approach

Fig. 6. Secrecy capacity region of the MISO Gaussian BBC with confidential messages with $N_R = 2$ and $N_1 = N_2 = 1$ for $\boldsymbol{h}_1 = [2\ 0.4]^T$, $\boldsymbol{h}_2 = [0.2\ 1.2]^T$, and $P = 5$. Fig. 6(b) compares the secrecy capacity region with the achievable rate region of a comparable TDMA approach (gray) which realizes the same routing task in three orthogonal time slots.

the weighted rate sum optimal rate tuples as well. Hence, obtaining the boundary of the secrecy capacity region is non-trivial. Following [39] or [29, Sec. V] one can reformulate the optimization problem for the single receive antenna case in such a way that the optimization problem becomes convex and therewith tractable.

Figure 6 depicts the secrecy capacity region of the MISO Gaussian BBC with confidential messages which characterizes the optimal processing at the relay node, cf. Corollary 2. This is compared with a comparable TDMA approach which realizes the same communication task in three orthogonal time slots. It shows that the optimal processing as given in Corollary 2 significantly outperforms the simple TDMA approach. For corresponding plots of capacity regions of the BBC with common messages and the classical broadcast channel with common and confidential messages, we refer to [28] and [29] respectively. Such an analysis is the indispensable basis for further studies such as fading channels or the impact of the geometric constellation or position of the relay and the other two nodes.

*Remark 5:* We presented the discussion for the average power constraint (9), but it is clear that this also holds for the general matrix power constraint (10). Further, the same discussion can be done for discrete memoryless channels.

## V. Conclusion

Physical layer service integration deals with the efficient implementation of different services at the physical layer. In this paper we studied physical layer service integration in bidirectional relay networks which basically required the study of the bidirectional broadcast channel with common and confidential messages. We established the entire secrecy capacity regions which characterize the fundamental limits up to which rates private, common, and confidential messages can be transmitted in bidirectional relay networks. Interestingly, it is shown that for MIMO Gaussian channels, a superposition of two streams–one for the public and one for the confidential communication–is optimal.

Accordingly, based on general observations regarding the optimal coding strategy, the next logical step for future work is to develop practical coding schemes that achieve these limits and to further characterize the optimal transmit strategies for MIMO processing. So far, perfect channel state information was assumed in the whole network. However, due to the nature of the wireless medium, channel uncertainty is a ubiquitous phenomenon in practical systems. Hence, it is essential to study robust physical layer service integration under channel uncertainty as a next step. For example, in [40] and [41] the classical broadcast channel with common and confidential messages and bidirectional relaying (without additional common and confidential services) are studied under channel uncertainty. In both, it is shown that reliable communication is still possible, but at reduced rates compared to the case with perfect channel state information. Therefore, robust physical layer service integration in bidirectional relay networks under channel uncertainty should be possible, but we similarly expect a degradation in performance. Another future research direction would be integration of further services in bidirectional relay networks. At the moment the relay integrates only one confidential message for one node. Similar to [15, 16], the relay could further integrate a second confidential message intended for the other node.

## References

[1] 3GPP TS 23.246 V9.1.0 Rel. 9, "Multimedia Broadcat/Multicast Service (MBMS); Architecture and Functional Description."
[2] K. Etemad and L. Wang, "Multicast and Broadcast Multimedia Services in Mobile WiMAX Networks," *IEEE Commun. Mag.*, vol. 47, no. 10, pp. 84–91, Oct. 2009.
[3] Y. Wu, "Broadcasting when Receivers Know Some Messages A Priori," in *Proc. IEEE Int. Symp. Inf. Theory*, Nice, France, Jun. 2007, pp. 1141–1145.
[4] G. Kramer and S. Shamai (Shitz), "Capacity for Classes of Broadcast Channels with Receiver Side Information," in *Proc. IEEE Inf. Theory Workshop*, Tahoe City, CA, USA, Sep. 2007, pp. 313–318.
[5] D. Gündüz, E. Erkip, A. Goldsmith, and H. V. Poor, "Source and Channel Coding for Correlated Sources Over Multiuser Channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 3927–3944, Sep. 2009.
[6] Deutsche Telekom AG Laboratories, "Next Generation Mobile Networks: (R)evolution in Mobile Communications," *Technology Radar Edition III/2010, Feature Paper*, 2010.
[7] A. D. Wyner, "The Wire-Tap Channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.
[8] I. Csiszár and J. Körner, "Broadcast Channels with Confidential Messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
[9] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information Theoretic Security," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4-5, pp. 355–580, 2009.
[10] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering.* Cambridge University Press, 2011.
[11] J. Barros and M. Bloch, "Strong Secrecy for Wireless Channels," in *Int. Conf. on Information-Theoretic Security*, Calgary, Canada, Aug. 2008, pp. 40–53, invited.
[12] A. Khisti and G. W. Wornell, "Secure Transmission With Multiple Antennas I: The MISOME Wiretap Channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.
[13] ——, "Secure Transmission With Multiple Antennas–Part II: The MIMOME Wiretap Channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.
[14] Y. Liang and H. V. Poor, "Multiple-Access Channels With Confidential Messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.
[15] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz), "MIMO Gaussian Broadcast Channels with Confidential and Common Messages," in *Proc. IEEE Int. Symp. Inf. Theory*, Austin, TX, USA, Jun. 2010, pp. 2578–2582.
[16] E. Ekrem and S. Ulukus, "Gaussian MIMO Broadcast Channels with Common and Confidential Messages," in *Proc. IEEE Int. Symp. Inf. Theory*, Austin, TX, USA, Jun. 2010, pp. 2583–2587.

[17] X. He and A. Yener, "A New Outer Bound for the Secrecy Capacity Region of the Gaussian Two-Way Wiretap Channel," in *Proc. IEEE Int. Conf. Commun.*, Cape Town, South Africa, May 2010, pp. 1–5.
[18] A. El Gamal, O. O. Koyluoglu, M. Youssef, and H. El Gamal, "New Achievable Secrecy Rate Regions for the Two Way Wiretap Channel," in *Proc. IEEE Inf. Theory Workshop*, Cairo, Egypt, Jan. 2010, pp. 1–5.
[19] R. F. Wyrembelski, A. Sezgin, and H. Boche, "Secrecy in Broadcast Channels with Receiver Side Information," in *Proc. Asilomar Conf. Signals, Systems, Computers*, Pacific Grove, CA, USA, Nov. 2011, pp. 290–294.
[20] T. J. Oechtering, H. T. Do, and M. Skoglund, "Capacity-achieving Coding for Cellular Downlink with Bidirectional Communication," in *Proc. Int. ITG Conf. Source and Channel Coding*, Siegen, Germany, Jan. 2010, pp. 1–6.
[21] B. Rankov and A. Wittneben, "Spectral Efficient Protocols for Half-Duplex Fading Relay Channels," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 2, pp. 379–389, Feb. 2007.
[22] P. Larsson, N. Johansson, and K.-E. Sunell, "Coded Bi-directional Relaying," in *Proc. 5th Scandinavian Workshop on Ad Hoc Networks*, Stockholm, Sweden, May 2005, pp. 851–855.
[23] Y. Wu, P. Chou, and S.-Y. Kung, "Information Exchange in Wireless Networks with Network Coding and Physical-Layer Broadcast," in *Proc. Conf. Inf. Sciences and Systems*, Baltimore, MD, USA, Mar. 2005, pp. 1–6.
[24] R. Knopp, "Two-Way Radio Networks With a Star Topology ," in *Proc. Int. Zurich Seminar on Commun.*, Zurich, Switzerland, Feb. 2006, pp. 154–157.
[25] T. J. Oechtering, C. Schnurr, I. Bjelaković, and H. Boche, "Broadcast Capacity Region of Two-Phase Bidirectional Relaying," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 454–458, Jan. 2008.
[26] S. J. Kim, P. Mitran, and V. Tarokh, "Performance Bounds for Bidirectional Coded Cooperation Protocols," *IEEE Trans. Inf. Theory*, vol. 54, no. 11, pp. 5235–5241, Nov. 2008.
[27] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Wiley & Sons, 2006.
[28] R. F. Wyrembelski, T. J. Oechtering, and H. Boche, "MIMO Gaussian Bidirectional Broadcast Channels with Common Messages," *IEEE Trans. Wireless Commun.*, vol. 10, no. 9, pp. 2950–2959, Sep. 2011.
[29] H. D. Ly, T. Liu, and Y. Liang, "Multiple-Input Multiple-Output Gaussian Broadcast Channels With Common and Confidential Messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5477–5487, Nov. 2010.
[30] U. M. Maurer and S. Wolf, "Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free," in *EUROCRYPT 2000, Lecture Notes in Computer Science*. Springer-Verlag, May 2000, vol. 1807, pp. 351–368.
[31] I. Bjelaković, H. Boche, and J. Sommerfeld, "Capacity Results for Compound Wiretap Channels," in *Proc. IEEE Inf. Theory Workshop*, Paraty, Brazil, Oct. 2011, pp. 60–64.
[32] ——, "Secrecy Results for Compound Wiretap Channels," submitted 2011, available at http://arxiv.org/abs/1106.2013.
[33] R. Ahlswede and G. Dueck, "Identification via Channels," *IEEE Trans. Inf. Theory*, vol. 35, no. 1, pp. 15–29, Jan. 1989.
[34] R. F. Wyrembelski and H. Boche, "Privacy in Bidirectional Relay Networks," *IEEE Trans. Commun.*, 2012, accepted.
[35] H. Weingarten, T. Liu, S. Shamai (Shitz), Y. Steinberg, and P. Viswanath, "The Capacity Region of the Degraded Multiple-Input Multiple-Output Compound Broadcast Channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 11, pp. 5011–5023, Nov. 2009.
[36] H. Weingarten, Y. Steinberg, and S. Shamai (Shitz), "The Capacity Region of the Gaussian Multiple-Input Multiple-Output Broadcast Channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3936–3964, Sep. 2006.
[37] T. Liu and S. Shamai (Shitz), "A Note on the Secrecy Capacity of the Multiple-Antenna Wiretap Channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.
[38] S. P. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.
[39] H. Weingarten, Y. Steinberg, and S. Shamai (Shitz), "On the Capacity Region of the Multi-Antenna Broadcast Channel with Common Messages," in *Proc. IEEE Int. Symp. Inf. Theory*, Seattle, WA, USA, Jul. 2006, pp. 2195–2199.
[40] R. F. Wyrembelski and H. Boche, "Strong Secrecy in Compound Broadcast Channels with Confidential Messages," in *Proc. IEEE Int. Symp. Inf. Theory*, Cambridge, MA, USA, Jul. 2012.
[41] R. F. Wyrembelski, I. Bjelaković, T. J. Oechtering, and H. Boche, "Optimal Coding Strategies for Bidirectional Broadcast Channels under Channel Uncertainty," *IEEE Trans. Commun.*, vol. 58, no. 10, pp. 2984–2994, Oct. 2010.

**Rafael F. Wyrembelski** (S'08) received the Dipl.-Ing. degree in Electrical Engineering and Computer Science in 2007 from the Technische Universität Berlin, Germany, and the Dr.-Ing. degree in Electrical Engineering in 2012 from the Technische Universität München. Between 2007 and 2010 he worked as a research and teaching assistant at the Heinrich-Hertz-Lehrstuhl für Mobilkommunikation at the Technische Universität Berlin, Germany. Since November 2010 he has been with the Lehrstuhl für Theoretische Informationstechnik at the Technische Universität München, Germany, where he is currently working as a Post-Doctoral researcher.

**Holger Boche** (M'04-SM'07-F'11) received the Dipl.-Ing. and Dr.-Ing. degrees in electrical engineering from the Technische Universität Dresden, Dresden, Germany, in 1990 and 1994, respectively. He graduated in mathematics from the Technische Universität Dresden in 1992. From 1994 to 1997, he did postgraduate studies in mathematics at the Friedrich-Schiller Universität Jena, Jena, Germany. He received his Dr. rer. nat. degree in pure mathematics from the Technische Universität Berlin, Berlin, Germany, in 1998. In 1997, he joined the Heinrich-Hertz-Institut (HHI) für Nachrichtentechnik Berlin, Berlin, Germany. Starting in 2002, he was a Full Professor for mobile communication networks with the Institute for Communications Systems, Technische Universität Berlin. In 2003, he became Director of the Fraunhofer German-Sino Lab for Mobile Communications, Berlin, Germany, and in 2004 he became the Director of the Fraunhofer Institute for Telecommunications (HHI), Berlin, Germany. Since October 2010 he has been with the Institute of Theoretical Information Technology and Full Professor at the Technische Universität München, Munich, Germany. He was a Visiting Professor with the ETH Zurich, Zurich, Switzerland, during the 2004 and 2006 Winter terms, and with KTH Stockholm, Stockholm, Sweden, during the 2005 Summer term. Prof. Boche is a Member of IEEE Signal Processing Society SPCOM and SPTM Technical Committee. He was elected a Member of the German Academy of Sciences (Leopoldina) in 2008 and of the Berlin Brandenburg Academy of Sciences and Humanities in 2009. He received the Research Award "Technische Kommunikation" from the Alcatel SEL Foundation in October 2003, the "Innovation Award" from the Vodafone Foundation in June 2006, and the Gottfried Wilhelm Leibniz Prize from the Deutsche Forschungsgemeinschaft (German Research Foundation) in 2008. He was co-recipient of the 2006 IEEE Signal Processing Society Best Paper Award and recipient of the 2007 IEEE Signal Processing Society Best Paper Award.