Privacy in Bidirectional Relay Networks

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

***Abstract*—In this work, the *bidirectional broadcast channel (BBC) with confidential messages* is studied. The problem is motivated by the concept of bidirectional relaying in three-node network, where a half-duplex relay node establishes a bidirectional communication between two other nodes using a decode-and-forward protocol and thereby transmits additional confidential information to one of them in the broadcast phase. The corresponding confidential message is transmitted at a certain secrecy level which characterizes the amount of information that can be kept secret from the non-legitimate node. The capacity-equivocation and secrecy capacity regions of the BBC with confidential messages are established where the latter characterizes the communication scenario with perfect secrecy, which means that the confidential information is completely hidden from the non-legitimate node. Thereby, it is shown that the optimal processing exploits ideas and concepts of the BBC with common messages and of the classical broadcast channel with confidential messages.**

***Index Terms*—Bidirectional Broadcast Channel, Confidential Message, Secrecy Capacity Region, Bidirectional Relaying, Privacy in Wireless Networks.**

I. Introduction

It is becoming more and more important that next generation wireless networks wisely integrate multiple services at the physical layer in order to increase spectral efficiency. For example, in current cellular systems, operators offer not only traditional services such as (bidirectional) voice communication, but also further multicast or confidential services that are subject to certain secrecy constraints. Nowadays this is usually realized by allocating 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 merge multiple coexisting services efficiently on the physical layer to advantageously exploit the broadcast nature of the wireless medium.

Currently, secrecy techniques usually rely on the assumption of the 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. In the seminal work [1] Wyner introduced the wiretap channel which models 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 [2] and studied the optimal integration of common and confidential messages at the physical layer. Recently, there has been growing interest in physical layer secrecy; for current surveys we refer, for example, to [3–6]. Several multi-user settings are under investigation, e.g., secrecy in multiple access channels is analyzed in [7, 8], while [9] discusses the interference channel with confidential messages and [10, 11] the MIMO Gaussian broadcast channel with common and confidential messages. Secure communication with relays is addressed in [12, 13] and in two-way wiretap channels in [14, 15]. Improvement in secrecy via cooperation is addressed in [16] and via helping interference in [17].

In this work, we study the broadcast scenario with one sender and two receivers, where the sender transmits two individual messages and a confidential message designated for one receiver, which has to be kept secret from the other, non-legitimate receiver. Further, we assume that each receiver has one individual message a priori as side information available. Thus, this scenario differs from the classical broadcast channel with confidential messages and is therefore known as *bidirectional broadcast channel (BBC) with confidential messages* as shown in Figure 1.

The problem is motivated by the concept of bidirectional relaying which has the potential to significantly improve the overall performance and coverage in wireless networks. This is mainly based on the fact that it advantageously exploits the property of bidirectional communication to reduce the inherent loss in spectral efficiency which is induced by half-duplex relays [18–21].

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 phase both nodes transmit their messages to the relay node which decodes them. This is the classical multiple access channel. In the succeeding bidirectional broadcast 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 [22–25] that capacity is achieved by a single data stream that combines both messages based on the network coding idea.

Currently, the concept of bidirectional relaying and its extensions are subject of further research activities, e.g., confer [26] for a survey of different processing strategies. In [27] it is presented how bidirectional relaying can be efficiently embedded in a cellular downlink. Bidirectional relaying for multiple pairs of nodes is discussed in [28–30]. Optimal beamforming strategies for multi-antenna bidirectional relaying with analog network coding is analyzed in [31].

The bidirectional broadcast channel with confidential messages corresponds to the scenario where the relay transmits

This work was partly presented at IEEE-ISIT, Saint Petersburg, Russia, July/August 2011.

The work was supported by the German Research Foundation (DFG) under Grant BO 1734/25-1 and by the German Ministry of Education and Research (BMBF) under Grant 01BU920.

Rafael F. Wyrembelski and Holger Boche are with the Lehrstuhl für Theoretische Informationstechnik, Technische Universität München, Germany (e-mail: {wyrembelski, boche}@tum.de).

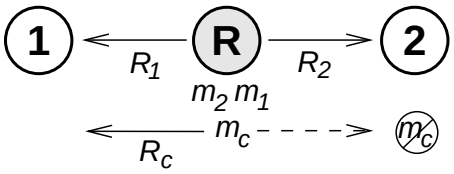

Fig. 1. Bidirectional broadcast channel with confidential messages: The relay transmits the messages m_1 and m_2 with rates R_2 and R_1 and adds a confidential message m_c for node 1 with rate R_c to the communication which should be kept as secret as possible from node 2.

both (bidirectional) individual messages and further an additional confidential message to one node, which should be kept secret from the other, non-legitimate node. Thus, we address the problem realizing additional confidential communication within a bidirectional relay network. We want to stress that this scenario differs from the wiretap scenario where the bidirectional communication itself should be secure from possible eavesdroppers outside the network as studied for example in [32, 33].

The rest of the paper is organized as follows. We introduce the system model for privacy in bidirectional relay networks in Section II. Therefore, we define the BBC with confidential messages and state the corresponding capacity-equivocation and secrecy capacity regions. Then, in Section III we present an optimal coding strategy that achieves the desired rates with the required secrecy level. The optimality of this strategy is proved in Section IV. Finally, we end up with a conclusion in Section V.

Notation

In this paper we denote discrete random variables by non-italic capital letters and their realizations and ranges by lower case letters and script letters, respectively; $\mathbb{N}$ and $\mathbb{R}_+$ are the sets of positive integers and non-negative real numbers; $H(\cdot)$ and $I(\cdot;\cdot)$ are the traditional 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; all logarithms, exponentials, and information quantities are taken to the basis 2; $\mathcal{P}(\cdot)$ is the set of all probability distributions and $A_\epsilon^{(n)}(\cdot)$ the set of (weakly) typical sequences, cf. for example [34]; $\mathbb{P}\{\cdot\}$ denotes the probability; lhs $:=$ rhs assigns the right hand side (rhs) to the left hand side (lhs), lhs $=:$ rhs accordingly.

II. Bidirectional Broadcast Channel with Confidential Messages

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 $W^{\otimes n}(y_1^n, y_2^n|x^n) := \prod_{k=1}^n W(y_{1,k}, y_{2,k}|x_k)$. Since we do not allow any cooperation between the receiving nodes, it is sufficient to consider the marginal transition probabilities $W_i^{\otimes n}(y_i^n|x^n) = \prod_{k=1}^n W_i(y_{i,k}|x_k)$, $i=1,2$, only.

In this work we consider the standard model with a block code of arbitrary but fixed length n. Let $\mathcal{M}_i := \{1,...,M_i^{(n)}\}$ be the set of individual messages of node i, $i=1,2$, which is also known at the relay node. Further, $\mathcal{M}_c := \{1,...,M_c^{(n)}\}$ is the set of confidential messages of the relay node. We use the abbreviation $\mathcal{M} := \mathcal{M}_c \times \mathcal{M}_1 \times \mathcal{M}_2$.

For the bidirectional broadcast (BBC) phase we assume that the relay has successfully decoded the individual messages $m_1 \in \mathcal{M}_1$ from node 1 and $m_2 \in \mathcal{M}_2$ from node 2 that it received in the previous multiple access (MAC) phase. Then the relay transmits both individual messages to the corresponding nodes and an additional confidential message $m_c \in \mathcal{M}_c$ at a certain secrecy level to node 1.

Definition 1: An $(n, M_c^{(n)}, M_1^{(n)}, M_2^{(n)})$*-code* for the BBC with confidential messages consists of one (stochastic) encoder at the relay node

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

and decoders at nodes 1 and 2

$$g_1 : \mathcal{Y}_1^n \times \mathcal{M}_1 \to \mathcal{M}_c \times \mathcal{M}_2 \cup \{0\}$$
$$g_2 : \mathcal{Y}_2^n \times \mathcal{M}_2 \to \mathcal{M}_1 \cup \{0\}$$

where the element 0 in the definition of the decoders plays the role of an erasure symbol and is included for convenience only.

Since randomization may increase the secrecy level [2, 3], we allow the encoder f to be stochastic. This means it is specified by conditional probabilities $f(x^n|m)$ with $\sum_{x^n \in \mathcal{X}^n} f(x^n|m) = 1$ for each $m = (m_c, m_1, m_2) \in \mathcal{M}$. Here, $f(x^n|m)$ is the probability that the message $m \in \mathcal{M}$ is encoded as $x^n \in \mathcal{X}^n$.

The quality of a code for the BBC with confidential messages is measured by two performance criteria. First, each receiver should successfully decode its intended messages, i.e., the average probabilities of decoding errors have to be small. In more detail, when the relay has sent the message $m = (m_c, m_1, m_2)$, and nodes 1 and 2 have received y_1^n and y_2^n, the decoder at node 1 is in error if $g_1(y_1^n, m_1) \neq (m_c, m_2)$. Accordingly, the decoder at node 2 is in error if $g_2(y_2^n, m_2) \neq m_1$. Then, with $\lambda_1(m) := \mathbb{P}\{g_1(y_1^n, m_1) \neq (m_c, m_2)|m \text{ has been sent}\}$ and $\lambda_2(m) := \mathbb{P}\{g_2(y_2^n, m_2) \neq m_1|m \text{ has been sent}\}$ the average probability of error at node i, $i=1,2$, is given by

$$\mu_i^{(n)} := \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} \lambda_i(m).$$

The second criterion is security. Similarly as in [1, 2] we characterize the secrecy level of the confidential message $m_c \in \mathcal{M}_c$ at node 2 by the concept of equivocation. The equivocation $H(\mathrm{M}_c|\mathrm{Y}_2^n, \mathrm{M}_2)$ describes the uncertainty of node 2 about the confidential message M_c having the received sequence Y_2^n and its own message M_2 from the previous MAC phase as side information available. Thus, the higher the equivocation is, the more ignorant node 2 is about the confidential message that is solely intended for node 1.

Definition 2: A rate-equivocation tuple $(R_c, R_e, R_1, R_2) \in \mathbb{R}_+^4$ is said to be *achievable* for the BBC with confidential messages if for any $\delta > 0$ there is an $n(\delta) \in \mathbb{N}$ and a sequence of $(n, M_c^{(n)}, M_1^{(n)}, M_2^{(n)})$-codes such that for all $n \geq n(\delta)$ we have $\frac{\log M_c^{(n)}}{n} \geq R_c - \delta$, $\frac{\log M_2^{(n)}}{n} \geq R_1 - \delta$, $\frac{\log M_1^{(n)}}{n} \geq R_2 - \delta$, and

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

while $\mu_1^{(n)}, \mu_2^{(n)} \to 0$ as $n \to \infty$. The set of all achievable rate-equivocation tuples is the *capacity-equivocation region* of the BBC with confidential messages and is denoted by $\mathcal{C}_{\text{BBC}}$.

If there is no additional confidential message for the relay to transmit, we have the classical BBC for which the capacity-achieving coding strategies are known [22–25].

Theorem 1 ([22–25]): The capacity region of the BBC is the set of all rate pairs $(R_1, R_2) \in \mathbb{R}_+^2$ that satisfy

$$R_i \leq I(\mathrm{X}; \mathrm{Y}_i|\mathrm{U}), \quad i = 1, 2 \tag{2}$$

for random variables $\mathrm{U} - \mathrm{X} - (\mathrm{Y}_1, \mathrm{Y}_2)$ with joint probability distribution $P_{\mathrm{U}}(u)P_{\mathrm{X}|\mathrm{U}}(x|u)W(y_1, y_2|x)$. Here, U is an auxiliary random variable that describes a possible time-sharing operation. The cardinality of the range of U can be bounded by $|\mathcal{U}| \leq 2$. ■

Remark 1: Following [25, Theorem 1] it is further possible to get rid of the time-sharing random variable U so that the region given in (2) simplifies to

$$R_i \leq I(\mathrm{X}; \mathrm{Y}_i), \quad i = 1, 2. \tag{3}$$

Now, we focus our attention on the broadcast scenario with an additional confidential message as shown in Figure 1 and present the main result of this work.

Theorem 2: The capacity-equivocation region $\mathcal{C}_{\text{BBC}}$ of the BBC with confidential messages is a closed convex set of those rate-equivocation tuples $(R_c, R_e, R_1, R_2) \in \mathbb{R}_+^4$ that satisfy

$$0 \leq R_e \leq R_c \tag{4a}$$
$$R_e \leq I(\mathrm{V}; \mathrm{Y}_1|\mathrm{U}) - I(\mathrm{V}; \mathrm{Y}_2|\mathrm{U}) \tag{4b}$$
$$R_c + R_i \leq I(\mathrm{V}; \mathrm{Y}_1|\mathrm{U}) + I(\mathrm{U}; \mathrm{Y}_i), \quad i = 1, 2 \tag{4c}$$
$$R_i \leq I(\mathrm{U}; \mathrm{Y}_i), \quad i = 1, 2 \tag{4d}$$

for random variables $\mathrm{U} - \mathrm{V} - \mathrm{X} - (\mathrm{Y}_1, \mathrm{Y}_2)$ with joint probability distribution $P_{\mathrm{U}}(u)P_{\mathrm{V}|\mathrm{U}}(v|u)P_{\mathrm{X}|\mathrm{V}}(x|v)W(y_1, y_2|x)$. Moreover, the cardinalities of the ranges of U and V can be bounded by

$$|\mathcal{U}| \leq |\mathcal{X}| + 3, \qquad |\mathcal{V}| \leq |\mathcal{X}|^2 + 4|\mathcal{X}| + 3.$$

Remark 2: While for the BBC without confidential messages the auxiliary random variable U only enables a time-sharing operation and carries no information, cf. Theorem 1, for the BBC with confidential messages we will see that U carries the bidirectional information and V realizes an additional randomization.

Remark 3: The capacity-equivocation region of the BBC with confidential messages, cf. Theorem 2, includes the capacity region of the BBC without confidential messages, cf. Theorem 1. In the case of no confidential messages we have $R_c = R_e = 0$ and observe that there is no need for the auxiliary random variables anymore, since there are no confidential messages to transmit. Therefore, with $\mathrm{U} = \mathrm{V} = \mathrm{X}$ in (4) we obtain the corresponding region given in (3).

From Theorem 2 follows immediately the *secrecy capacity region* $\mathcal{C}_{\text{BBC}}^S$of the BBC with confidential messages which is the set of rate triples $(R_c, R_1, R_2) \in \mathbb{R}_+^3$ such that $(R_c, R_c, R_1, R_2) \in \mathcal{C}_{\text{BBC}}$. Since we require $R_c = R_e$ in this case, the secrecy condition (1) is often equivalently written as

$$\tfrac{1}{n} I(\mathrm{M}_c; \mathrm{Y}_2^n|\mathrm{M}_2) \leq \delta \tag{5}$$

and usually referred to as *perfect secrecy* condition.

Corollary 1: The secrecy capacity region $\mathcal{C}_{\text{BBC}}^S$ of the BBC with confidential messages is the set of all rate triples $(R_c, R_1, R_2) \in \mathbb{R}_+^3$ satisfying

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

for random variables $\mathrm{U} - \mathrm{V} - \mathrm{X} - (\mathrm{Y}_1, \mathrm{Y}_2)$ with joint probability distribution $P_{\mathrm{U}}(u)P_{\mathrm{V}|\mathrm{U}}(v|u)P_{\mathrm{X}|\mathrm{V}}(x|v)W(y_1, y_2|x)$. ■

The capacity-equivocation region in Theorem 2 describes the scenario where the confidential message is transmitted with rate R_c at a certain secrecy level R_e. Thereby, the equivocation rate R_e can be interpreted as the amount of information of the confidential message that can be kept secret from the non-legitimate node. Therefore, Theorem 2 includes the case where the non-legitimate node has some partial knowledge about the confidential information, namely if $R_c > R_e$. The secrecy capacity region in Corollary 1 characterizes the scenario with perfect secrecy which is, from today's point of view, the practically more relevant case. Since $R_c = R_e$, the confidential message can be kept completely hidden from the non-legitimate node.

Remark 4: Here 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 (5). This criterion is also known as *weak secrecy*. There exists a stronger version where (5) is strengthened by dropping the division by n and therewith by considering the absolute amount of information leaked to the non-legitimate node. *Strong secrecy* in bidirectional relay networks is analyzed in [35].

Remark 5: In this paper we assume perfect channel state information at all nodes. But in practical systems there is always some uncertainty in channel state information due to the nature of the wireless medium or imperfect channel estimation. Thus, to obtain robust strategies which work also under channel uncertainty, it is important to also take such impairments into account for future work. Some results for the compound wiretap channel can be found in [36, 37], where the latter considers the strong secrecy criterion, cf. Remark 4. Strong secrecy for the arbitrarily varying wiretap channel is analyzed in [38] which provides a suitable model for secrecy in uncoordinated networks.

In the following two sections we prove Theorem 2 and therewith establish the capacity-equivocation region $\mathcal{C}_{\text{BBC}}$ of the BBC with confidential messages.

III. Secrecy-Achieving Coding Strategy

In this section we present a coding strategy that achieves the desired rates with the required secrecy level and therewith prove the achievability part of the corresponding Theorem 2.

A. Codebook Design

A crucial part is the construction of a suitable codebook with a specific structure consisting of two layers. This is done in the following Lemma 1.

The first layer corresponds to a codebook that is suitable for the relay to transmit (bidirectional) individual messages

$m_2' \in \mathcal{M}_2'$ and $m_1' \in \mathcal{M}_1'$ to nodes 1 and 2 as well as a common (multicast) message $m_0' \in \mathcal{M}_0'$ to both nodes. This corresponds to the coding problem for the BBC with common messages which is studied in detail in [39].

Then, for each codeword there is a sub-codebook with a product structure similarly as in [2] for the classical broadcast channel with confidential messages. The legitimate receiver for the confidential message, i.e., node 1, can decode each codeword regardless to which column and row index it corresponds. But the main idea behind such a codebook design is that the non-legitimate receiver, i.e., node 2, has to decode the column index of the transmitted codeword with the maximum rate its channel provides, and therefore is not able to decode the remaining row index [3].

Lemma 1: For any $\delta > 0$ let $\mathrm{U} - \mathrm{X} - (\mathrm{Y}_1, \mathrm{Y}_2)$ be a Markov chain of random variables which further satisfy $I(\mathrm{X};\mathrm{Y}_1|\mathrm{U}) > I(\mathrm{X};\mathrm{Y}_2|\mathrm{U})$.

i) Let $\lambda_1(m_0', m_2'|m_1')$ be the probability that node 1 decodes $(m_0', m_2') \in \mathcal{M}_0' \times \mathcal{M}_2'$ incorrectly if $m_1' \in \mathcal{M}_1'$ is given. The probability of error $\lambda_2(m_0', m_1'|m_2')$ for node 2 is defined accordingly. There exists a set of codewords $u_{m'}^n \in \mathcal{U}^n$, $m' = (m_0', m_1', m_2') \in \mathcal{M}_0' \times \mathcal{M}_1' \times \mathcal{M}_2' =: \mathcal{M}'$, with

$$\tfrac{1}{n}\big(\log|\mathcal{M}_0'| + \log|\mathcal{M}_2'|\big) \geq I(\mathrm{U};\mathrm{Y}_1) - \delta \tag{6a}$$
$$\tfrac{1}{n}\big(\log|\mathcal{M}_0'| + \log|\mathcal{M}_1'|\big) \geq I(\mathrm{U};\mathrm{Y}_2) - \delta \tag{6b}$$

such that

$$\frac{1}{|\mathcal{M}'|}\sum_{m'\in\mathcal{M}'} \lambda_1(m_0', m_2'|m_1') \leq \epsilon^{(n)} \tag{7a}$$
$$\frac{1}{|\mathcal{M}'|}\sum_{m'\in\mathcal{M}'} \lambda_2(m_0', m_1'|m_2') \leq \epsilon^{(n)} \tag{7b}$$

and $\epsilon^{(n)} \to 0$ as $n \to \infty$.

ii) Let $\lambda_1(j, l|m')$ be the probability that node 1 decodes $j \in \mathcal{J}$ or $l \in \mathcal{L}$ incorrectly if $m' \in \mathcal{M}'$ is known. Similarly, $\lambda_2(j|l, m')$ is the probability that node 2 decodes $j \in \mathcal{J}$ incorrectly if $l \in \mathcal{L}$ and $m' \in \mathcal{M}'$ are given. For each $u_{m'}^n \in \mathcal{U}^n$ there exist codewords $x_{jlm'}^n \in \mathcal{X}^n$, $j \in \mathcal{J}$, $l \in \mathcal{L}$, $m' \in \mathcal{M}'$, with

$$\tfrac{1}{n}\log|\mathcal{J}| \geq I(\mathrm{X};\mathrm{Y}_2|\mathrm{U}) - \delta \tag{8a}$$
$$\tfrac{1}{n}\log|\mathcal{L}| \geq I(\mathrm{X};\mathrm{Y}_1|\mathrm{U}) - I(\mathrm{X};\mathrm{Y}_2|\mathrm{U}) - \delta \tag{8b}$$

such that

$$\frac{1}{|\mathcal{J}||\mathcal{L}||\mathcal{M}'|}\sum_{j\in\mathcal{J}}\sum_{l\in\mathcal{L}}\sum_{m'\in\mathcal{M}'} \lambda_1(j, l|m') \leq \epsilon^{(n)} \tag{9a}$$
$$\frac{1}{|\mathcal{J}||\mathcal{L}||\mathcal{M}'|}\sum_{j\in\mathcal{J}}\sum_{l\in\mathcal{L}}\sum_{m'\in\mathcal{M}'} \lambda_2(j|l, m') \leq \epsilon^{(n)} \tag{9b}$$

and $\epsilon^{(n)} \to 0$ as $n \to \infty$.

Proof: The proof exploits ideas from the BBC with common messages [39] for the first part and from the classical broadcast channel with confidential messages [2] for the second part. The details can be found in the appendix. ∎

Of course, the communication of confidential information and especially the codebook design above is only meaningful, if the channel from the relay node to the intended receiver provides higher rates than the one to the non-legitimate node.

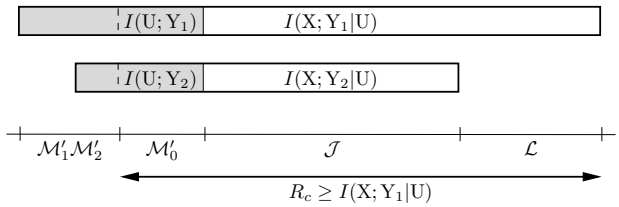

Fig. 2. The two bars visualize the available resources of both links. Each one is split up into two parts: one designated for the bidirectional communication (gray) and one for the confidential communication (white). Since $R_c \geq I(\mathrm{X};\mathrm{Y}_1|\mathrm{U})$, some resources of the bidirectional communication have to be spent for the confidential message as well (realized by a common message).

From Lemma 1 we see that $I(\mathrm{X};\mathrm{Y}_1|\mathrm{U}) > I(\mathrm{X};\mathrm{Y}_2|\mathrm{U})$ is the limiting criterion that decides if confidential communication is possible or not.

B. Achievable Equivocation-Rate Region

Next, we use the codebook from Lemma 1 to construct suitable encoder and decoders for the BBC with confidential messages.

Lemma 2: Using the codebook from Lemma 1 all rate-equivocation tuples $(R_c, R_e, R_1, R_2) \in \mathbb{R}_+^4$ that satisfy

$$0 \leq R_e = I(\mathrm{X};\mathrm{Y}_1|\mathrm{U}) - I(\mathrm{X};\mathrm{Y}_2|\mathrm{U}) \leq R_c \tag{10a}$$
$$R_c + R_i \leq I(\mathrm{X};\mathrm{Y}_1|\mathrm{U}) + I(\mathrm{U};\mathrm{Y}_i), \quad i = 1, 2 \tag{10b}$$
$$R_i \leq I(\mathrm{U};\mathrm{Y}_i), \quad i = 1, 2 \tag{10c}$$

for random variables $\mathrm{U} - \mathrm{X} - (\mathrm{Y}_1, \mathrm{Y}_2)$ with $I(\mathrm{X};\mathrm{Y}_1|\mathrm{U}) > I(\mathrm{X};\mathrm{Y}_2|\mathrm{U})$ are achievable for the BBC with confidential messages.

Proof: For any $\mathrm{U} - \mathrm{X} - (\mathrm{Y}_1, \mathrm{Y}_2)$ which satisfy $I(\mathrm{X};\mathrm{Y}_1|\mathrm{U}) > I(\mathrm{X};\mathrm{Y}_2|\mathrm{U})$, any $\delta > 0$, and given rate-equivocation tuple $(R_c, R_e, R_1, R_2) \in \mathbb{R}_+^4$ satisfying (10a)-(10c) we have to construct message sets, encoder, and decoders with

$$\tfrac{1}{n}\log|\mathcal{M}_c| \geq R_c - \delta \tag{11a}$$
$$\tfrac{1}{n}\log|\mathcal{M}_2| \geq R_1 - \delta \tag{11b}$$
$$\tfrac{1}{n}\log|\mathcal{M}_1| \geq R_2 - \delta \tag{11c}$$

and further, cf. also (1),

$$\tfrac{1}{n}H(\mathrm{M}_c|\mathrm{Y}_2^n, \mathrm{M}_2) \geq I(\mathrm{X};\mathrm{Y}_1|\mathrm{U}) - I(\mathrm{X};\mathrm{Y}_2|\mathrm{U}) - \delta. \tag{12}$$

The following construction is mainly based on the one for the classical broadcast channel with confidential messages [2]. Thereby, we have to distinguish between two cases as visualized in Figures 2 and 3.

If $R_c \geq I(\mathrm{X};\mathrm{Y}_1|\mathrm{U})$, cf. Figure 2, we construct the set of confidential messages as

$$\mathcal{M}_c := \mathcal{J} \times \mathcal{L} \times \mathcal{M}_0'$$

where the sets $\mathcal{J}$ and $\mathcal{L}$ are chosen as in Lemma 1 and $\mathcal{M}_0'$ is an arbitrary set of common messages such that (11a) is satisfied. The sets $\mathcal{M}_1 = \mathcal{M}_1'$ and $\mathcal{M}_2 = \mathcal{M}_2'$ are arbitrary such that (11b)-(11c) hold. Finally, we define the deterministic encoder f that maps the confidential message $(j, l, m_0') \in \mathcal{M}_c$

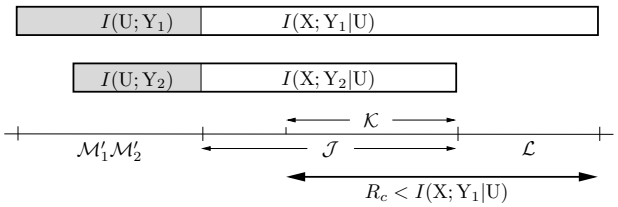

Fig. 3. Since $R_c < I(\mathrm{X};\mathrm{Y}_1|\mathrm{U})$, there are more resources for the confidential communication available than needed. This allows the relay to enable a stochastic coding strategy that exploits all the available resources by introducing a mapping from $\mathcal{J}$ to $\mathcal{K}$.

and the individual messages $m_i \in \mathcal{M}_i$, $i = 1, 2$, into the codeword $x^n_{jlm'} \in \mathcal{X}^n$ with $m' = (m'_0, m'_1, m'_2)$ and $m'_i = m_i$, $i = 1, 2$.

Remark 6: Since $R_c \geq I(\mathrm{X};\mathrm{Y}_1|\mathrm{U})$, a part of the confidential message must be transmitted as a common message decodable at both receivers, cf. Figure 2. Therefore, the confidential rate is not only constrained by the channel to the legitimate node, but also by the channel to the non-legitimate node, cf. (10b). Note that it is not possible to simply "add" the remaining part to the individual message for node 1, since this would require that this part of the confidential message is already available a priori as side information at node 2.

If $R_c < I(\mathrm{X};\mathrm{Y}_1|\mathrm{U})$, cf. Figure 3, we set $\mathcal{M}_c := \mathcal{K} \times \mathcal{L}$ where $\mathcal{K}$ is an arbitrary set such that (11a) holds. Further, we define a mapping $h : \mathcal{J} \to \mathcal{K}$ that partitions $\mathcal{J}$ into subsets of "nearly equal size" [2], which means

$$|h^{-1}(k)| \leq 2|h^{-1}(k')|, \quad \text{for all } k, k' \in \mathcal{K}.$$

Moreover, since $R_c < I(\mathrm{X};\mathrm{Y}_1|\mathrm{U})$, there is no need for a set of common messages so that $\mathcal{M}'_0 = \emptyset$. The sets $\mathcal{M}_1 = \mathcal{M}'_1$ and $\mathcal{M}_2 = \mathcal{M}'_2$ are arbitrary such that (11b)-(11c) hold. Finally, we define the stochastic encoder f that maps the confidential message $(k, l) \in \mathcal{M}_c$ and the individual messages $m_i \in \mathcal{M}_i$, $i = 1, 2$, into the codeword $x^n_{jlm'} \in \mathcal{X}^n$ with $m' = (0, m'_1, m'_2)$, where j is uniformly drawn from the set $h^{-1}(k) \subset \mathcal{J}$ and $m'_i = m_i$, $i = 1, 2$.

Remark 7: This time, set $\mathcal{J}$ is not needed in total for the confidential communication. However, to force the non-legitimate receiver, i.e., node 2, to decode at its maximum rate, we define a stochastic encoder that spreads the confidential messages over the whole set $\mathcal{J}$. Moreover, if $R_c \leq I(\mathrm{X};\mathrm{Y}_1|\mathrm{U}) - I(\mathrm{X};\mathrm{Y}_2|\mathrm{U})$, the whole set $\mathcal{J}$ is used for additional randomization.

Up to now we defined message sets and the encoder. In both cases the decoders are immediately determined by the decoding sets of Lemma 1. Hence, the achievability of the rates as specified in (10a)-(10c) follows immediately from Lemma 1.

To complete the proof it remains to show that this coding strategy achieves the required secrecy level (12) at node 2. Proceeding as in [2] let X^n be the input random variable of the channel, whose realizations are the codewords $x^n_{jlm'} \in \mathcal{X}^n$ (as specified by the encoder above). Further, let $\mathrm{M}' = (\mathrm{M}'_0, \mathrm{M}'_1, \mathrm{M}'_2)$ be the random variable that corresponds to the third index of the realization of X^n. With $\mathrm{M}_i = \mathrm{M}'_i$, $i = 1, 2$, from the definition of the encoder above, we get for the equivocation

$$\begin{aligned}
&H(\mathrm{M}_c|\mathrm{Y}_2^n, \mathrm{M}_2) \\
&\quad \geq H(\mathrm{M}_c|\mathrm{Y}_2^n, \mathrm{M}') \\
&\quad = H(\mathrm{M}_c, \mathrm{Y}_2^n|\mathrm{M}') - H(\mathrm{Y}_2^n|\mathrm{M}') \\
&\quad = H(\mathrm{M}_c, \mathrm{Y}_2^n, \mathrm{X}^n|\mathrm{M}') - H(\mathrm{X}^n|\mathrm{M}_c, \mathrm{M}', \mathrm{Y}_2^n) - H(\mathrm{Y}_2^n|\mathrm{M}') \\
&\quad = H(\mathrm{M}_c, \mathrm{X}^n|\mathrm{M}') + H(\mathrm{Y}_2^n|\mathrm{M}_c, \mathrm{M}', \mathrm{X}^n) \\
&\qquad\quad - H(\mathrm{X}^n|\mathrm{M}_c, \mathrm{M}', \mathrm{Y}_2^n) - H(\mathrm{Y}_2^n|\mathrm{M}') \\
&\quad \geq H(\mathrm{X}^n|\mathrm{M}') + H(\mathrm{Y}_2^n|\mathrm{X}^n) \\
&\qquad\quad - H(\mathrm{X}^n|\mathrm{M}_c, \mathrm{M}', \mathrm{Y}_2^n) - H(\mathrm{Y}_2^n|\mathrm{M}').
\end{aligned} \tag{13}$$

In the following we bound all terms in (13) separately. We start with the first term and observe that for given $\mathrm{M}' = m'$ the random variable X^n has $|\mathcal{J}||\mathcal{L}|$ possible values. Since we assume X^n to be independently and uniformly distributed, we have $H(\mathrm{X}^n|\mathrm{M}') = \log|\mathcal{J}| + \log|\mathcal{L}|$. With the definition of the sets $\mathcal{J}$ and $\mathcal{L}$, cf. (8) of Lemma 1, we obtain

$$\tfrac{1}{n} H(\mathrm{X}^n|\mathrm{M}') \underset{n\to\infty}{\longrightarrow} I(\mathrm{X};\mathrm{Y}_1|\mathrm{U}). \tag{14}$$

For the second term in (13) we get from the weak law of large numbers

$$\tfrac{1}{n} H(\mathrm{Y}_2^n|\mathrm{X}^n) \underset{n\to\infty}{\longrightarrow} H(\mathrm{Y}_2|\mathrm{X}). \tag{15}$$

If $R_c \geq I(\mathrm{X};\mathrm{Y}_1|\mathrm{U})$, the third term in (13) vanishes, since given M_c and M' the deterministic encoder already determines X^n. If $R_c < I(\mathrm{X};\mathrm{Y}_1|\mathrm{U})$, we have a stochastic encoder and define

$$\varphi(k, l, m', y_2^n) = \begin{cases} x^n_{klm'} & \text{if } (u^n_{m'}, x^n_{jlm'}, y_2^n) \in A_\epsilon^{(n)}(\mathrm{UXY}_2) \\ & \quad \text{with } h(j) = k \\ \text{arbitrary} & \text{otherwise.} \end{cases}$$

Then we have $\mathbb{P}\{\mathrm{X}^n \neq \varphi(\mathrm{M}_c, \mathrm{M}', \mathrm{Y}_2^n)\} \leq \epsilon^{(n)}$ with $\epsilon^{(n)} \to 0$ as $n \to \infty$ and therefore, by Fano's lemma, cf. also [2, 3],

$$\tfrac{1}{n} H(\mathrm{X}^n|\mathrm{M}_c, \mathrm{M}', \mathrm{Y}_2^n) \underset{n\to\infty}{\longrightarrow} 0 \tag{16}$$

so that the third term vanishes also in this case. For the last term in (13) we define

$$\hat{y}_2^n = \begin{cases} y_2^n & \text{if } (u^n_{m'}, y_2^n) \in A_\epsilon^{(n)}(\mathrm{UY}_2) \\ \text{arbitrary} & \text{otherwise} \end{cases}$$

so that

$$H(\mathrm{Y}_2^n|\mathrm{M}') \leq H(\mathrm{Y}_2^n|\hat{\mathrm{Y}}_2^n) + H(\hat{\mathrm{Y}}_2^n|\mathrm{M}').$$

For the first term we have $\mathbb{P}\{\mathrm{Y}_2^n \neq \hat{\mathrm{Y}}_2^n\} \leq \epsilon^{(n)}$ with $\epsilon^{(n)} \to 0$ as $n \to \infty$ by Fano's lemma, cf. [2, 3], so that it is negligible. Moreover, following [2, 3] for given $\mathrm{M}' = m'$ we get for the conditional entropy

$$\begin{aligned}
H(\hat{\mathrm{Y}}_2^n|\mathrm{M}' = m') &\leq \log|A_\epsilon^{(n)}(\mathrm{Y}_2|u^n_{m'})| \\
&\leq \log(2^{n(H(\mathrm{Y}_2|\mathrm{U})+2\epsilon)}) = n(H(\mathrm{Y}_2|\mathrm{U}) + 2\epsilon)
\end{aligned}$$

where the second inequality follows from the definition of the decoding sets, cf. also [34, Theorem 15.2.2]. With this we obtain

$$\tfrac{1}{n} H(\hat{\mathrm{Y}}_2^n|\mathrm{M}') \underset{n\to\infty}{\longrightarrow} H(\mathrm{Y}_2|\mathrm{U}). \tag{17}$$

Finally, by substituting (14)-(17) into (13) we obtain (12) which establishes the desired secrecy level at node 2 and therewith proves the lemma. ■

C. Randomization and Convexity

Here, we complete the proof of achievability of Theorem 2 where the argumentation goes along with the one for the classical broadcast channel with confidential messages [2].

To obtain the whole region as given in Theorem 2, we follow [2] and introduce an auxiliary channel that enables an additional randomization. Therefore we define the following rate region. Let $\mathcal{R}$ be the set of all rate-equivocation tuples $(R_c, R_e, R_1, R_2) \in \mathbb{R}_+^4$ that satisfy

$$0 \leq R_e \leq I(\mathrm{V};\mathrm{Y}_1|\mathrm{U}) - I(\mathrm{V};\mathrm{Y}_2|\mathrm{U}) \leq R_c \tag{18a}$$

$$R_c + R_i \leq I(\mathrm{V};\mathrm{Y}_1|\mathrm{U}) + I(\mathrm{U};\mathrm{Y}_i), \quad i = 1,2 \tag{18b}$$

$$R_i \leq I(\mathrm{U};\mathrm{Y}_i), \quad i = 1,2 \tag{18c}$$

for random variables $\mathrm{U}-\mathrm{V}-\mathrm{X}-(\mathrm{Y}_1,\mathrm{Y}_2)$ with $I(\mathrm{V};\mathrm{Y}_1|\mathrm{U}) > I(\mathrm{V};\mathrm{Y}_2|\mathrm{U})$.

Lemma 3: The rate region $\mathcal{R}$ is achievable for the BBC with confidential messages.

Sketch of Proof: For any $\mathrm{U}-\mathrm{V}-\mathrm{X}-(\mathrm{Y}_1,\mathrm{Y}_2)$ with $I(\mathrm{V};\mathrm{Y}_1|\mathrm{U}) > I(\mathrm{V};\mathrm{Y}_2|\mathrm{U})$ the prefixing realized by the random variable V is exactly the same as in [2, Lemma 4]. Then the achievability of all rate-equivocation tuples $(R_c, R_e, R_1, R_2) \in \mathbb{R}_+^4$ that satisfy (18) follows immediately from Lemma 2.

We want to note that Lemma 2 provides only the achievability with an equality in the condition on the equivocation rate, cf. (10a), instead of the proposed inequality in (18a). But it is obvious that if the rate-equivocation tuple (R_c, R_e, R_1, R_2) is achievable, than each rate-equivocation tuple (R_c, R_e', R_1, R_2) with $0 \leq R_e' \leq R_e$ is also achievable. Consequently, we can further replace the equality by an inequality. ■

Lemma 4: The rate region $\mathcal{R}$ is convex.

Sketch of Proof: Exactly as in [2, Lemma 5] it is easy to show that any linear combination of two rate-equivocation tuples in $\mathcal{R}$ is contained in $\mathcal{R}$ which proves the convexity. ■

It remains to show that $\mathcal{R}$ describes the same rate region as the one specified by Theorem 2.

Lemma 5: The rate region $\mathcal{R}$ equals the region $\mathcal{C}_{\mathrm{BBC}}$ given in Theorem 2.

Proof: From the definitions of the regions $\mathcal{C}_{\mathrm{BBC}}$ and $\mathcal{R}$ it is obvious that $\mathcal{R} \subseteq \mathcal{C}_{\mathrm{BBC}}$ holds. To show the reversed inclusion, i.e., $\mathcal{C}_{\mathrm{BBC}} \subseteq \mathcal{R}$, we take any rate-equivocation tuple (R_c, R_e, R_1, R_2) which is in $\mathcal{C}_{\mathrm{BBC}}$ for some $\mathrm{U}-\mathrm{V}-\mathrm{X}-(\mathrm{Y}_1,\mathrm{Y}_2)$, and show that this tuple is also in $\mathcal{R}$. To show this, we construct similarly as in [2] the maximal achievable confidential and equivocation rates that are possible for these individual rates R_1, R_2 and random variables $\mathrm{U}-\mathrm{V}-\mathrm{X}-(\mathrm{Y}_1,\mathrm{Y}_2)$ as

$$R_c^* \coloneqq I(\mathrm{V};\mathrm{Y}_1|\mathrm{U}) + \min\big\{I(\mathrm{U};\mathrm{Y}_1) - R_1, I(\mathrm{U};\mathrm{Y}_2) - R_2\big\}$$

$$R_e^* \coloneqq I(\mathrm{V};\mathrm{Y}_1|\mathrm{U}) - I(\mathrm{V};\mathrm{Y}_2|\mathrm{U}).$$

Based on this construction we observe that for given R_1 and R_2 the extremal points (R_c^*, R_e^*, R_1, R_2), (R_e^*, R_e^*, R_1, R_2), $(R_c^*, 0, R_1, R_2)$, and $(0, 0, R_1, R_2)$ belong all to the desired region $\mathcal{R}$. But since $0 \leq R_e \leq R_e^*$ and $R_e \leq R_c \leq R_c^*$, it follows from the convexity of $\mathcal{R}$, cf. Lemma 4, that the original rate-equivocation tuple (R_c, R_e, R_1, R_2) is also in $\mathcal{R}$ which proves the lemma. ■

To complete the proof of achievability it remains to bound the cardinalities of the ranges of U and V. Since the bounds of the cardinalities depend only on the structure of the random variables, the result follows immediately from [2, Appendix] or [40, Section 17] where the same bounds are established for the classical broadcast channel with confidential messages. ■

IV. Optimality

Already the presented coding strategy indicates that, basically, the BBC with confidential messages exploits ideas of the BBC (with common messages) [22, 39] and of the classical broadcast channel with confidential messages [2]. Based on this observation it is easy to establish the weak converse by extending the converse of the classical broadcast channel with confidential messages [2] using standard arguments for the BBC [22, 39].

We have to show that for any given sequence of $(n, M_c^{(n)}, M_1^{(n)}, M_2^{(n)})$-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

$$\tfrac{1}{n}H(\mathrm{M}_c|\mathrm{Y}_2^n,\mathrm{M}_2) \leq I(\mathrm{V};\mathrm{Y}_1|\mathrm{U}) - I(\mathrm{V};\mathrm{Y}_2|\mathrm{U}) + o(n^0) \tag{19a}$$

$$\tfrac{1}{n}H(\mathrm{M}_2) \leq I(\mathrm{U};\mathrm{Y}_1) + o(n^0) \tag{19b}$$

$$\tfrac{1}{n}H(\mathrm{M}_1) \leq I(\mathrm{U};\mathrm{Y}_2) + o(n^0) \tag{19c}$$

$$\tfrac{1}{n}\big(H(\mathrm{M}_c) + H(\mathrm{M}_2)\big) \leq I(\mathrm{V};\mathrm{Y}_1|\mathrm{U}) + I(\mathrm{U};\mathrm{Y}_1) + o(n^0) \tag{19d}$$

$$\tfrac{1}{n}\big(H(\mathrm{M}_c) + H(\mathrm{M}_1)\big) \leq I(\mathrm{V};\mathrm{Y}_1|\mathrm{U}) + I(\mathrm{U};\mathrm{Y}_2) + o(n^0) \tag{19e}$$

are satisfied. For this purpose we need a version of Fano's lemma suitable for the BBC with confidential messages.

Lemma 6 (Fano's inequality): For the BBC with confidential messages we have the following versions of Fano's inequality

$$H(\mathrm{M}_c,\mathrm{M}_2|\mathrm{Y}_1^n,\mathrm{M}_1) \leq \mu_1^{(n)}\log(M_c^{(n)}M_2^{(n)}) + 1 = n\epsilon_1^{(n)}$$

$$H(\mathrm{M}_1|\mathrm{Y}_2^n,\mathrm{M}_2) \leq \mu_2^{(n)}\log M_1^{(n)} + 1 = n\epsilon_2^{(n)}$$

with $\epsilon_1^{(n)} = \frac{\log(M_c^{(n)}M_2^{(n)})}{n}\mu_1^{(n)} + \frac{1}{n} \to 0$ and $\epsilon_2^{(n)} = \frac{\log M_1^{(n)}}{n}\mu_2^{(n)} + \frac{1}{n} \to 0$ for $n \to \infty$ as $\mu_1^{(n)}, \mu_2^{(n)} \to 0$.

Proof: The lemma can be shown analogously as in [22, 39], where similar versions of Fano's inequality for the BBC with and without common messages are presented. Therefore, we omit the details for brevity. ■

We start with some upper bounds on the entropy terms. Using the fact that M_c, M_1, M_2 are independent, the definition of mutual information, the chain rule for entropy, and Fano's inequality, cf. Lemma 6, we obtain for the entropy of the confidential message similarly as in [2, Equation (35)]

$$H(\mathrm{M}_c) \leq I(\mathrm{M}_c;\mathrm{Y}_1^n|\mathrm{M}_1,\mathrm{M}_2) + n\epsilon_1^{(n)} \tag{20}$$

and for the entropy terms of the individual messages similarly as in [22]

$$H(\mathrm{M}_2) \leq I(\mathrm{M}_1,\mathrm{M}_2;\mathrm{Y}_1^n) + n\epsilon_1^{(n)} \tag{21a}$$

$$H(\mathrm{M}_1) \leq I(\mathrm{M}_1,\mathrm{M}_2;\mathrm{Y}_2^n) + n\epsilon_2^{(n)}. \tag{21b}$$

Note that each entropy term is bounded from above by a mutual information term that involves both individual messages and not only its own message. Thus, this already indicates that the optimal processing will combine both individual messages into one data stream based on the network coding idea. Further for the equivocation we get

$$\begin{aligned} &H(\mathrm{M}_c|\mathrm{Y}_2^n,\mathrm{M}_2) \\ &\quad= H(\mathrm{M}_c|\mathrm{Y}_2^n,\mathrm{M}_1,\mathrm{M}_2) + I(\mathrm{M}_c;\mathrm{M}_1|\mathrm{Y}_2^n,\mathrm{M}_2) \\ &\quad= H(\mathrm{M}_c|\mathrm{M}_1,\mathrm{M}_2) - I(\mathrm{M}_c;\mathrm{Y}_2^n|\mathrm{M}_1,\mathrm{M}_2) \\ &\qquad + I(\mathrm{M}_c;\mathrm{M}_1|\mathrm{Y}_2^n,\mathrm{M}_2) \\ &\quad= I(\mathrm{M}_c;\mathrm{Y}_1^n|\mathrm{M}_1,\mathrm{M}_2) - I(\mathrm{M}_c;\mathrm{Y}_2^n|\mathrm{M}_1,\mathrm{M}_2) \\ &\qquad + H(\mathrm{M}_c|\mathrm{Y}_1^n,\mathrm{M}_1,\mathrm{M}_2) + I(\mathrm{M}_c;\mathrm{M}_1|\mathrm{Y}_2^n,\mathrm{M}_2) \\ &\quad\le I(\mathrm{M}_c;\mathrm{Y}_1^n|\mathrm{M}_1,\mathrm{M}_2) - I(\mathrm{M}_c;\mathrm{Y}_2^n|\mathrm{M}_1,\mathrm{M}_2) \\ &\qquad + n\epsilon_1^{(n)} + n\epsilon_2^{(n)} \end{aligned} \tag{22}$$

where the last inequality follows from Fano's inequality, cf. Lemma 6, and $H(\mathrm{M}_c|\mathrm{Y}_1^n,\mathrm{M}_1,\mathrm{M}_2) \le H(\mathrm{M}_c,\mathrm{M}_2|\mathrm{Y}_1^n,\mathrm{M}_1) \le n\epsilon_1^{(n)}$ and $I(\mathrm{M}_c;\mathrm{M}_1|\mathrm{Y}_2^n,\mathrm{M}_2) = H(\mathrm{M}_1|\mathrm{Y}_2^n,\mathrm{M}_2) - H(\mathrm{M}_1|\mathrm{Y}_2^n,\mathrm{M}_c,\mathrm{M}_2) \le H(\mathrm{M}_1|\mathrm{Y}_2^n,\mathrm{M}_2) \le n\epsilon_2^{(n)}$.

The next step is to expand the mutual information terms in (20)-(22) by making extensively use of the chain rule for mutual information. For notational convenience we set $\mathrm{Y}_1^k = \mathrm{Y}_{1,1},...,\mathrm{Y}_{1,k}$ and $\tilde{\mathrm{Y}}_2^k = \mathrm{Y}_{2,k},...,\mathrm{Y}_{2,n}$ as suggested in [2, Sec. V] for the classical broadcast channel with confidential messages. We define

$$\Sigma_1 = \sum_{k=1}^{n} I(\tilde{\mathrm{Y}}_2^{k+1};\mathrm{Y}_{1,k}|\mathrm{Y}_1^{k-1},\mathrm{M}_1,\mathrm{M}_2)$$

$$\Sigma_1^* = \sum_{k=1}^{n} I(\mathrm{Y}_1^{k-1};\mathrm{Y}_{2,k}|\tilde{\mathrm{Y}}_2^{k+1},\mathrm{M}_1,\mathrm{M}_2)$$

and the analogous terms Σ_2 and Σ_2^* with $\mathrm{M}_1,\mathrm{M}_2$ replaced by $\mathrm{M}_c,\mathrm{M}_1,\mathrm{M}_2$. Then by replacing the common message in [2, Sec. V] with our (bidirectional) individual messages, it is straightforward to show that, similarly as in [2, Eqs. (38)-(41)], the mutual information terms in (20)-(22) can be expressed as

$$I(\mathrm{M}_c;\mathrm{Y}_1^n|\mathrm{M}_1,\mathrm{M}_2) = \sum_{k=1}^{n} I(\mathrm{M}_c;\mathrm{Y}_{1,k}|\mathrm{Y}_1^{k-1},\tilde{\mathrm{Y}}_2^{k+1},\mathrm{M}_1,\mathrm{M}_2) + \Sigma_1 - \Sigma_2 \tag{23a}$$

$$I(\mathrm{M}_c;\mathrm{Y}_2^n|\mathrm{M}_1,\mathrm{M}_2) = \sum_{k=1}^{n} I(\mathrm{M}_c;\mathrm{Y}_{2,k}|\mathrm{Y}_1^{k-1},\tilde{\mathrm{Y}}_2^{k+1},\mathrm{M}_1,\mathrm{M}_2) + \Sigma_1^* - \Sigma_2^* \tag{23b}$$

and

$$I(\mathrm{M}_1,\mathrm{M}_2;\mathrm{Y}_1^n) \le \sum_{k=1}^{n} I(\mathrm{Y}_1^{k-1},\tilde{\mathrm{Y}}_2^{k+1},\mathrm{M}_1,\mathrm{M}_2;\mathrm{Y}_{1,k}) - \Sigma_1 \tag{24a}$$

$$I(\mathrm{M}_1,\mathrm{M}_2;\mathrm{Y}_2^n) \le \sum_{k=1}^{n} I(\mathrm{Y}_1^{k-1},\tilde{\mathrm{Y}}_2^{k+1},\mathrm{M}_1,\mathrm{M}_2;\mathrm{Y}_{2,k}) - \Sigma_1^*. \tag{24b}$$

Note that it suffices to drop the non-negative terms Σ_1 and Σ_1^* in (24a) and (24b) and to define the auxiliary random variables as in (25) to obtain the upper bounds (19b) and (19c) on the individual messages. But for the other bounds (19a), (19d), and (19e) we have to keep Σ_1 and Σ_1^* and to apply the following lemma.

Lemma 7: We have the following identities: $\Sigma_1 = \Sigma_1^*$ and $\Sigma_2 = \Sigma_2^*$.

Proof: In [2, Lemma 7] a similar result for the classical broadcast channel with confidential messages is given. Our result follows immediately by simply replacing the common message in [2, Lemma 7] by our two (bidirectional) individual messages M_1 and M_2. ■

As in [2, Sec. V] we introduce an auxiliary random variable J that is independent of M_c, M_1, M_2, X^n, Y_1^n, and Y_2^n and uniformly distributed over $\{1,...,n\}$. Further, let

$$\mathrm{U} \coloneqq (\mathrm{Y}_1^{\mathrm{J}-1},\tilde{\mathrm{Y}}_2^{\mathrm{J}+1},\mathrm{M}_1,\mathrm{M}_2,\mathrm{J}) \tag{25a}$$

$$\mathrm{V} \coloneqq (\mathrm{U},\mathrm{M}_c) \tag{25b}$$

$$\mathrm{X} \coloneqq \mathrm{X}_{\mathrm{J}} \tag{25c}$$

$$\mathrm{Y}_i \coloneqq \mathrm{Y}_{i1,\mathrm{J}}, \quad i=1,2 \tag{25d}$$

so that

$$\frac{1}{n}\sum_{k=1}^{n} I(\mathrm{M}_c;\mathrm{Y}_{1,k}|\mathrm{Y}_1^{k-1},\tilde{\mathrm{Y}}_2^{k+1},\mathrm{M}_1,\mathrm{M}_2) = I(\mathrm{M}_c;\mathrm{Y}_1|\mathrm{U}) = I(\mathrm{V};\mathrm{Y}_1|\mathrm{U})$$

$$\frac{1}{n}\sum_{k=1}^{n} I(\mathrm{M}_c;\mathrm{Y}_{2,k}|\mathrm{Y}_1^{k-1},\tilde{\mathrm{Y}}_2^{k+1},\mathrm{M}_1,\mathrm{M}_2) = I(\mathrm{M}_c;\mathrm{Y}_2|\mathrm{U}) = I(\mathrm{V};\mathrm{Y}_2|\mathrm{U})$$

and

$$\frac{1}{n}\sum_{k=1}^{n} I(\mathrm{Y}_1^{k-1},\tilde{\mathrm{Y}}_2^{k+1},\mathrm{M}_1,\mathrm{M}_2;\mathrm{Y}_{1,k}) = I(\mathrm{U};\mathrm{Y}_1|\mathrm{J}) \le I(\mathrm{U};\mathrm{Y}_1)$$

$$\frac{1}{n}\sum_{k=1}^{n} I(\mathrm{Y}_1^{k-1},\tilde{\mathrm{Y}}_2^{k+1},\mathrm{M}_1,\mathrm{M}_2;\mathrm{Y}_{2,k}) = I(\mathrm{U};\mathrm{Y}_2|\mathrm{J}) \le I(\mathrm{U};\mathrm{Y}_2).$$

Now, to complete the proof it remains to put all ingredients together. Therefore, we substitute this into (23)-(24), apply Lemma 7, so that with (20)-(22) the weak converse is established. ■

V. Conclusion

In this work, we analyzed the bidirectional broadcast channel with confidential messages and therewith studied privacy in a bidirectional relay network that exploits principles from network coding which makes the optimal processing by no means self-evident. We characterized the corresponding capacity-equivocation and secrecy capacity regions in detail. This further describes the efficient integration of bidirectional and confidential services at the physical layer in bidirectional relay networks. The integration of an additional multicast service is then discussed in [41]. Such studies are initiated by operators of wireless networks to further increase the spectral efficiency. This concept is known as *physical layer service*

integration (PLSI) and becomes more and more important for future wireless networks and, especially, 5G cellular networks.

We note that the bidirectional broadcast channel with confidential messages is completely different to the bidirectional broadcast wiretap channel, where the relay should enable a secure bidirectional communication such that the bidirectional messages itself are kept as secret as possible from possible eavesdroppers outside of the bidirectional relay network. This is an interesting and important topic for itself and is studied for example in [32, 33].

APPENDIX

Here we present the proof of Lemma 1. As in [3] we prove the existence of a codebook with the desired properties by random coding arguments.

1) Random codebook generation and encoding: We define (bidirectional) message sets $\mathcal{M}_i'$, $i = 0, 1, 2$, such that $|\mathcal{M}_0'||\mathcal{M}_2'| = \lfloor 2^{n(I(\mathrm{U};\mathrm{Y}_1)-\delta/2)} \rfloor$ and $|\mathcal{M}_0'||\mathcal{M}_1'| = \lfloor 2^{n(I(\mathrm{U};\mathrm{Y}_2)-\delta/2)} \rfloor$ are fulfilled. Further, we choose (confidential) message sets $\mathcal{J}$ and $\mathcal{L}$ with $|\mathcal{J}| = \lfloor 2^{n(I(\mathrm{X};\mathrm{Y}_2|\mathrm{U})-\delta/2)} \rfloor$ and $|\mathcal{L}| = \lfloor 2^{n(I(\mathrm{X};\mathrm{Y}_1|\mathrm{U})-I(\mathrm{X};\mathrm{Y}_2|\mathrm{U})-\delta/2)} \rfloor$. Obviously, these sets satisfy conditions (6) and (8). In the following, we consider only the case where these sets are non-empty[1] and set $\epsilon := \delta/8$.

In a first step, we generate $|\mathcal{M}'| = |\mathcal{M}_0'||\mathcal{M}_1'||\mathcal{M}_2'|$ independent codewords $u_{m'}^n \in \mathcal{U}^n$ with $m' = (m_0', m_1', m_2')$ according to $P_{\mathrm{U}^n}(u^n) = \prod_{k=1}^n P_{\mathrm{U}}(u_k)$. Then, for each $u_{m'}^n \in \mathcal{U}^n$ we generate $|\mathcal{J}||\mathcal{L}|$ independent codewords $x_{jlm'}^n \in \mathcal{X}^n$ according to $P_{\mathrm{X}^n|\mathrm{U}^n}(x^n|u_{m'}^n) = \prod_{k=1}^n P_{\mathrm{X}|\mathrm{U}}(x_k|u_{m',k})$.

2) Decoding: The receiving nodes use typical set decoding where each node uses its received sequence and its side information to create the decoding sets. In more detail, if $x_{jlm'}^n \in \mathcal{X}^n$ has been sent, node 1 uses the received sequence $y_1^n \in \mathcal{Y}_1^n$ and its own message $m_1' \in \mathcal{M}_1'$ to create

$$\mathcal{D}_{11}(m_1', y_1^n) := \big\{(m_0', m_2') \in \mathcal{M}_0' \times \mathcal{M}_2' : (u_{m'}^n, y_1^n) \in A_\epsilon^{(n)}(\mathrm{UY}_1)\big\}.$$

If $\mathcal{D}_{11}(m_1', y_1^n)$ is empty or contains more than one element, node 1 maps to the symbol 0, cf. also Definition 1, and declares an error. Otherwise, in a second step it uses the unique $(m_0', m_2') \in \mathcal{D}_{11}(m_1', y_1^n)$ and its own $m_1' \in \mathcal{M}_1'$ to create

$$\mathcal{D}_{12}(m', y_1^n) := \big\{(j, l) \in \mathcal{J} \times \mathcal{L} : (u_{m'}^n, x_{jlm'}^n, y_1^n) \in A_\epsilon^{(n)}(\mathrm{UXY}_1)\big\}.$$

Again, if $\mathcal{D}_{12}(m', y_1^n)$ is empty or contains more than one element, node 1 maps to 0 and declares an error. Otherwise, if there is a unique $(j, l) \in \mathcal{D}_{12}(m', y_1^n)$, it declares that $(j, l, m') \in \mathcal{J} \times \mathcal{L} \times \mathcal{M}'$ has been sent.

Similarly, node 2 uses $y_2^n \in \mathcal{Y}_2^n$ and $m_2' \in \mathcal{M}_2'$ to define

$$\mathcal{D}_{21}(m_2', y_2^n) := \big\{(m_0', m_1') \in \mathcal{M}_0' \times \mathcal{M}_1' : (u_{m'}^n, y_2^n) \in A_\epsilon^{(n)}(\mathrm{UY}_2)\big\}.$$

[1]We need not consider the trivial cases of zero rates since they are always achievable.

If there is a unique $(m_0', m_1') \in \mathcal{D}_{21}(m_2', y_2^n)$, with its own $m_2' \in \mathcal{M}_2'$ and given $l \in \mathcal{L}$ it creates

$$\mathcal{D}_{22}(l, m', y_2^n) := \big\{j \in \mathcal{J} : (u_{m'}^n, x_{jlm'}^n, y_2^n) \in A_\epsilon^{(n)}(\mathrm{UXY}_2)\big\}.$$

It declares that $(j, l, m') \in \mathcal{J} \times \mathcal{L} \times \mathcal{M}'$ has been sent if there is a unique $j \in \mathcal{D}_{22}(l, m', y_2^n)$. The events of an error are defined accordingly as for node 1.

3) Analysis of probability of error: For the following analysis we introduce for any $(j, l, m') \in \mathcal{J} \times \mathcal{L} \times \mathcal{M}'$ the random error events for node 1:

$$\begin{aligned}
E_{11}(m_0', m_2'|m_1') &:= \big\{(u_{m'}^n, y_1^n) \notin A_\epsilon^{(n)}(\mathrm{UY}_1)\big\} \\
E_{12}(m_0', m_2'|m_1') &:= \big\{\exists\, (\hat{m}_0, \hat{m}_2) \neq (m_0', m_2') : (u_{\hat{m}_0 m_1' \hat{m}_2}^n, y_1^n) \in A_\epsilon^{(n)}(\mathrm{UY}_1)\big\} \\
E_{13}(j, l|m') &:= \big\{(u_{m'}^n, x_{jlm'}^n, y_1^n) \notin A_\epsilon^{(n)}(\mathrm{UXY}_1)\big\} \\
E_{14}(j, l|m') &:= \big\{\exists\, (\hat{j}, \hat{l}) \neq (j, l) : (u_{m'}^n, x_{\hat{j}\hat{l}m'}^n, y_1^n) \in A_\epsilon^{(n)}(\mathrm{UXY}_1)\big\}.
\end{aligned}$$

From the union bound we get for the probabilities of error

$$\lambda_1(m_0', m_2'|m_1') \leq \mathbb{P}\big\{E_{11}(m_0', m_2'|m_1')\big\} + \mathbb{P}\big\{E_{12}(m_0', m_2'|m_1')\big\} \tag{26a}$$

$$\lambda_1(j, l|m') \leq \mathbb{P}\big\{E_{13}(j, l|m')\big\} + \mathbb{P}\big\{E_{14}(j, l|m')\big\} \tag{26b}$$

where each one is bounded separately using standard arguments, cf. for example [34].

For $\mathbb{P}\{E_{11}(m_0', m_2'|m_1')\}$ we know from the definition of the decoding sets, cf. also [34], that for increasing n we have

$$\mathbb{P}\big\{(u_{m'}^n, y_1^n) \notin A_\epsilon^{(n)}(\mathrm{UY}_1)\big\} \underset{n\to\infty}{\longrightarrow} 0. \tag{27}$$

With $\hat{m} = (\hat{m}_0, m_1', \hat{m}_2)$ we get for the second event

$$\begin{aligned}
&\mathbb{P}\big\{E_{12}(m_0', m_2'|m_1')\big\} \\
&\quad\leq |\mathcal{M}_0'||\mathcal{M}_2'|\, \mathbb{P}\big\{(u_{\hat{m}_0 m_1' \hat{m}_2}^n, y_1^n) \in A_\epsilon^{(n)}(\mathrm{UY}_1)\big\} \\
&\quad= |\mathcal{M}_0'||\mathcal{M}_2'| \sum_{(u_{\hat{m}}^n, y_1^n) \in A_\epsilon^{(n)}(\mathrm{UY}_1)} P_{\mathrm{Y}_1^n}(y_1^n) P_{\mathrm{U}^n}(u_{\hat{m}}^n) \\
&\quad\leq 2^{n(I(\mathrm{U};\mathrm{Y}_1)-\delta/2)} 2^{n(H(\mathrm{U},\mathrm{Y}_1)+\epsilon)} 2^{-n(H(\mathrm{Y}_1)-\epsilon)} 2^{-n(H(\mathrm{U})-\epsilon)} \\
&\quad= 2^{-n\epsilon} \underset{n\to\infty}{\longrightarrow} 0
\end{aligned} \tag{28}$$

where the first inequality follows from the union bound, the second one from the definition of the sets $\mathcal{M}_0'$, $\mathcal{M}_2'$ and $|A_\epsilon^{(n)}(\mathrm{UY}_1)| \leq 2^{n(H(\mathrm{U},\mathrm{Y}_1)+\epsilon)}$, cf. [34], and the last equality from $\delta = 8\epsilon$. Substituting (27)-(28) into (26a) we conclude that $\lambda_1(m_0', m_2'|m_1') \to 0$ as $n \to \infty$.

For $\mathbb{P}\{E_{13}(j, l|m')\}$ follows, similarly as in the first event, from the definition of the decoding sets that for increasing n

$$\mathbb{P}\big\{(u_{m'}^n, x_{jlm'}^n, y_1^n) \notin A_\epsilon^{(n)}(\mathrm{UXY}_1)\big\} \underset{n\to\infty}{\longrightarrow} 0. \tag{29}$$

It remains to bound $\mathbb{P}\{E_{14}(j, l|m')\}$. Therefore, we proceed

as in the second event and obtain

$$\begin{aligned}
&\mathbb{P}\{E_{13}(j,l|m')\} \\
&\quad\leq |\mathcal{J}||\mathcal{L}| \sum_{(u^n_{m'},x^n_{\hat{j}\hat{l}m'},y^n_1)\in A^{(n)}_\epsilon(\mathrm{UXY}_1)} P_{\mathrm{Y}^n_1|\mathrm{U}^n}(y^n_1|u^n_{m'}) \\
&\qquad\qquad \times P_{\mathrm{X}^n|\mathrm{U}^n}(x^n_{\hat{j}\hat{l}m'}|u^n_{m'})P_{\mathrm{U}^n}(u^n_{m'}) \\
&\quad\leq |\mathcal{J}||\mathcal{L}|2^{n(H(\mathrm{U,X,Y}_1)+\epsilon)}2^{-n(H(\mathrm{Y}_1|\mathrm{U})-\epsilon)} \\
&\qquad\qquad \times 2^{-n(H(\mathrm{X}|\mathrm{U})-\epsilon)}2^{-n(H(\mathrm{U})-\epsilon)} \\
&\quad\leq 2^{-n4\epsilon} \underset{n\to\infty}{\longrightarrow} 0 \qquad (30)
\end{aligned}$$

where the second inequality follows from $|A^{(n)}_\epsilon(\mathrm{UXY}_1)| \leq 2^{n(H(\mathrm{U,X,Y}_1)+\epsilon)}$ and the third from $|\mathcal{J}||\mathcal{L}| \leq 2^{n(I(\mathrm{X;Y}_1|\mathrm{U})-\delta)}$ and $\delta = 8\epsilon$. Substituting (29)-(30) into (26b) we end up with $\lambda_1(j,l|m') \to 0$ as $n \to \infty$.

The analysis for the probability of error at node 2 follows accordingly with the random error events $E_{21}(m'_0,m'_1|m'_2) = \{(u^n_{m'},y^n_2) \notin A^{(n)}_\epsilon(\mathrm{UY}_2)\}$, $E_{22}(m'_0,m'_1|m'_2) = \{\exists(\hat{m}_0,\hat{m}_1) \neq (m'_0,m'_1) : (u^n_{\hat{m}_0\hat{m}_1m'_2},y^n_2) \in A^{(n)}_\epsilon(\mathrm{UY}_2)\}$, $E_{23}(j|l,m') = \{(u^n_{m'},x^n_{jlm'},y^n_2) \notin A^{(n)}_\epsilon(\mathrm{UXY}_2)\}$, and $E_{24}(j|l,m') = \{\exists\hat{j} \neq j : (u^n_{m'},x^n_{\hat{j}lm'},y^n_2) \in A^{(n)}_\epsilon(\mathrm{UXY}_2)\}$. Using the same arguments, it is straightforward to show that the probabilities of error fulfill

$$\begin{aligned}
\lambda_2(m'_0,m'_1|m'_2) &\leq \mathbb{P}\big\{E_{21}(m'_0,m'_1|m'_2)\big\} \\
&\quad + \mathbb{P}\big\{E_{22}(m'_0,m'_1|m'_2)\big\} \underset{n\to\infty}{\longrightarrow} 0 \qquad (31)\\
\lambda_2(j|l,m') &\leq \mathbb{P}\big\{E_{23}(j|l,m')\big\} \\
&\quad + \mathbb{P}\big\{E_{24}(j|l,m')\big\} \underset{n\to\infty}{\longrightarrow} 0. \qquad (32)
\end{aligned}$$

From (27)-(32) we conclude that the probabilities of error, averaged over all codewords and codebooks, get arbitrarily small. Finally, from the random coding argument it follows that for n large enough there exists a codebook with the desired rates (6) and (8) that satisfies the conditions on the probabilities of error (7) and (9) proving the lemma. ■

REFERENCES

[1] A. D. Wyner, "The Wire-Tap Channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.

[2] I. Csiszár and J. Körner, "Broadcast Channels with Confidential Messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[3] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information Theoretic Security," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4-5, pp. 355–580, 2009.

[4] R. Liu and W. Trappe, Eds., *Securing Wireless Communications at the Physical Layer*. Springer, 2010.

[5] E. A. Jorswieck, A. Wolf, and S. Gerbracht, "Secrecy on the Physical Layer in Wireless Networks," *Trends in Telecommunications Technologies*, pp. 413–435, Mar. 2010.

[6] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[7] 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.

[8] E. Ekrem and S. Ulukus, "On the Secrecy of Multiple Access Wiretap Channel," in *Proc. Allerton Conf. Commun., Control, Computing*, Urbana-Champaign, IL, USA, Sep. 2008, pp. 1014–1021.

[9] R. Liu, I. Marić, P. Spasojević, and R. D. Yates, "Discrete Memoryless Interference and Broadcast Channels With Confidential Messages: Secrecy Rate Regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.

[10] 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.

[11] 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.

[12] ——, "Secrecy in Cooperative Relay Broadcast Channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, Canada, Jul. 2008, pp. 2217–2221.

[13] X. He and A. Yener, "Cooperation with an Untrusted Relay: A Secrecy Perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.

[14] ——, "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.

[15] 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.

[16] N. Marina, H. Yagi, and H. V. Poor, "Improved Rate-Equivocation Regions for Secure Cooperative Communication," in *Proc. IEEE Int. Symp. Inf. Theory*, Saint Petersburg, Russia, Aug. 2011, pp. 2832–2836.

[17] X. Tang, R. Liu, P. Spasojević, and H. V. Poor, "Interference Assisted Secret Communication," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3153–3167, 2011.

[18] 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.

[19] 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.

[20] 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.

[21] R. Knopp, "Two-Way Radio Networks With a Star Topology ," in *Proc. Int. Zurich Seminar on Commun.*, Zurich, Switzerland, Feb. 2006, pp. 154–157.

[22] 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.

[23] 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.

[24] L.-L. Xie, "Network Coding and Random Binning for Multi-User Channels," in *Proc. Canadian Workshop on Inf. Theory*, Jun. 2007, pp. 85–88.

[25] 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.

[26] P. Popovski and T. Koike-Akino, *Coded Bidirectional Relaying in Wireless Networks*, ser. New Directions in Wireless Communications Research. Springer US, 2009, ch. 11, pp. 291–316.

[27] T. J. Oechtering, H. T. Do, and M. Skoglund, "Achievable Rates for Embedded Bidirectional Relaying in a Cellular Downlink," in *Proc. IEEE Int. Conf. Commun.*, Cape Town, South Africa, May 2010, pp. 1–5.

[28] M. Chen and A. Yener, "Multiuser Two-Way Relaying: Detection and Interference Management Strategies," *IEEE Trans. Wireless Commun.*, vol. 8, no. 8, pp. 4296–4305, Aug. 2009.

[29] A. S. Avestimehr, M. A. Khajehnejad, A. Sezgin, and B. Hassibi, "Capacity Region of the Deterministic Multi-Pair Bi-Directional Relay Network," in *Proc. IEEE Inf. Theory Workshop*, Volos, Greece, Jun. 2009, pp. 57–61.

[30] E. Yilmaz, R. Zakhour, D. Gesbert, and R. Knopp, "Multi-pair Two-way Relay Channel with Multiple Antenna Relay Station," in *Proc. IEEE Int. Conf. Commun.*, Cape Town, South Africa, May 2010, pp. 1–5.

[31] R. Zhang, Y.-C. Liang, C. C. Chai, and S. Cui, "Optimal Beamforming for Two-Way Multi-Antenna Relay Channel with Analogue Network Coding," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 5, pp. 699–712, Jun. 2009.

[32] A. Mukherjee and A. L. Swindlehurst, "Securing Multi-Antenna Two-Way Relay Channels With Analog Network Coding Against Eavesdroppers," in *Proc. IEEE Signal Process. Adv. Wireless Commun.*, Marrakech, Morocco, Jun. 2010, pp. 1–5.

[33] 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.
[34] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Wiley & Sons, 2006.
[35] R. F. Wyrembelski, M. Wiese, and H. Boche, "Strong Secrecy in Bidirectional Relay Networks," in *Proc. Asilomar Conf. Signals, Systems, Computers*, Pacific Grove, CA, USA, Nov. 2011, invited.
[36] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz), "Compound Wiretap Channels," *EURASIP J. Wireless Commun. Netw.*, vol. Article ID 142374, pp. 1–13, 2009.
[37] 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.
[38] ——, "Capacity Results for Arbitrarily Varying Wiretap Channels," submitted 2012.
[39] 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.
[40] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, 2nd ed. Cambridge University Press, 2011.
[41] R. F. Wyrembelski and H. Boche, "Service Integration in Multiantenna Bidirectional Relay Networks: Public and Confidential Services," in *Proc. IEEE Global Commun. Conf.*, Houston, TX, USA, Dec. 2011, pp. 914–918.

Rafael F. Wyrembelski (S'08) received the Dipl.-Ing. degree in Electrical Engineering and Computer Science from the Technische Universität Berlin, Germany, in 2007. Between 2007 and 2010 he worked as a research and teaching assistant at the Heinrich-Hertz-Lehrstuhl für Informationstheorie und theoretische Informationstechnik 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 towards a Ph.D. degree.

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.