Strong Secrecy in Bidirectional Broadcast Channels With Confidential Messages

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

***Abstract*—To increase the spectral efficiency of future wireless networks, it is important to wisely integrate multiple services at the physical layer. Here the efficient integration of confidential services in the three-node bidirectional relay channel is studied. A relay node establishes a bidirectional communication between two other nodes using a decode-and-forward protocol, which is also known as two-way relaying. In the broadcast phase, the relay transmits not only the two bidirectional messages it received in the previous multiple access phase, but also an additional confidential message to one node while keeping the other node completely ignorant of it. The concept of *strong information theoretic secrecy* is used to ensure that the nonlegitimate node cannot decode the confidential message no matter what its computational resources are. Moreover, this implies that the average decoding error at the nonlegitimate node goes exponentially fast to one for any decoding strategy it may use. This results in the study of the *bidirectional broadcast channel with confidential messages* for which the strong secrecy capacity region is established. Furthermore, it is shown that the efficient integration of confidential messages with strong secrecy extends to such scenarios, where the relay further transmits an additional common message to both nodes.**

***Index Terms*—Bidirectional broadcast channel, bidirectional relaying, capacity region, confidential message, physical layer security, strong secrecy, wireless network.**

I. Introduction

A research area that is gaining importance is the efficient integration of certain services at the physical layer. For example, already in current cellular systems, operators offer not only 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. In general this is quite inefficient and thus there is a trend to merge multiple coexisting services efficiently from an information theoretic point of view so that they work on the same wireless resources.

When integrating confidential services, operators of wireless networks are confronted with an inherent problem: due to the open nature of the wireless channel a transmitted signal is received by its intended users but can also easily be eavesdropped by nonlegitimate receivers. To keep information secret, current systems usually apply cryptographic techniques which are based on the assumption of insufficient computational capabilities of nonlegitimate receivers. It is clear that with increasing computational power, improved algorithms, or recent advances in number theory, these techniques become more and more insecure.

Information theoretic, or physical layer, security uses the physical properties of the wireless channel in order to establish a higher level of security. This security only depends on the channel; so whatever transformation is applied to the signals that are received by nonlegitimate receivers, the original message cannot be reproduced with high probability. Not surprisingly, information theoretic security is becoming more and more attractive and is identified by operators as a promising task for next generation mobile networks [1].

Information theoretic security was initiated by Wyner, who introduced the *wiretap channel* [2], and later generalized by Csiszár and Körner to the *broadcast channel with confidential messages* [3]. Recently, there is growing interest in information theoretic security, for example we refer to [4]–[7] and references therein. Besides the wiretap channel [2], [8]–[10], there is also work on multiuser settings such as the multiple access channel with confidential messages [11], the MIMO Gaussian broadcast channel with common and confidential messages [12], [13], the interference channel with confidential messages [14], or the two-way wiretap channel [15], [16]. Secure communication in wireless networks, where the source broadcasts several confidential messages is studied in [17]. Secret key agreement over wireless fading channels is analyzed in [18].

However, most of these works use the criterion of *weak secrecy* which is heuristic in nature, in that no operational meaning has been given to it yet. This means that even if this criterion holds, one still does not know what a nonlegitimate receiver can or cannot do to decode the confidential message. A criterion that can be given an operational meaning is the criterion of *strong secrecy* introduced by Maurer and Wolf in [19]: it was established in [20], [21] for the wiretap channel that under the strong secrecy criterion, the average decoding error at a nonlegitimate receiver tends to one for any decoding strategy it may use. This criterion is stronger than the one used so far and has further been investigated under several aspects in [20]–[26][1].

The observation in [20], [21] constitutes the main motivation to consider strong secrecy in *bidirectional relay channels*.

Manuscript received June 14, 2012; revised September 10, 2012; accepted December 04, 2012. Date of publication December 11, 2012; date of current version January 09, 2013. This work was supported by the German Ministry of Education and Research (BMBF) under Grant 01BU920. This work was presented in part at the Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA, November 2011. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Shantanu Rane.

The authors are with Lehrstuhl für Theoretische Informationstechnik, Technische Universität München, Munich 80290, Germany (e-mail: wyrembelski@tum.de; wiese@tum.de; boche@tum.de).

Digital Object Identifier 10.1109/TIFS.2012.2233473

[1] The authors thank the anonymous reviewer who brought their attention to reference [25].

1556-6013/$31.00 © 2012 IEEE

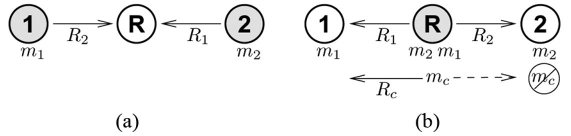

Fig. 1. Decode-and-forward bidirectional relaying. In the initial multiple access (MAC) phase, nodes 1 and 2 transmit their messages m_1 and m_2 with rates R_2 and R_1 to the relay node. In the succeeding bidirectional broadcast (BBC) phase, the relay forwards the messages m_1 and m_2 with rates R_2 and R_1 and adds a confidential message m_c for node 1 with rate R_c to the communication which has to be kept secret from node 2. (a) MAC phase. (b) BBC phase.

Here, a relay node establishes a bidirectional communication between two other nodes using a two-phase decode-and-forward protocol [27]–[31]. In the initial multiple access (MAC) phase both nodes transmit their messages to the relay node which decodes them. This is the classical multiple access channel which is well understood. In the succeeding broadcast phase the relay reencodes 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 [29]–[31] that capacity is achieved by a single data stream that combines both messages based on the network coding idea. The concept of bidirectional relaying and its extensions are widely studied. Besides the decode-and-forward protocol [29]–[32] there are other strategies such as amplify-and-forward [32], [33], compress-and-forward [34]–[36], compute-and-forward [37]–[41], or noisy network coding [42]–[44].

In this paper we consider the three-node bidirectional relay channel as depicted in Fig. 1, where the relay node establishes the bidirectional communication and at the same time transmits an additional confidential message to one node in the broadcast phase in such a way that the other nonlegitimate node is kept completely ignorant of it. Due to the side information at the receivers this differs from the classical broadcast scenario and is therefore known as *bidirectional broadcast channel (BBC) with confidential messages*.

The rest of the paper is organized as follows. We introduce the system model for strong secrecy in bidirectional relay channels in Section II. Therefore, we define the BBC with confidential messages and state the corresponding strong secrecy capacity region. In Section III we present the key idea to achieve strong secrecy in the BBC with confidential messages. This allows us to establish the corresponding strong secrecy capacity region in Section IV. Section V discusses the scenario where the relay additionally integrates a common message, and Section VI finally concludes the paper.

Notation

In this paper we denote discrete random variables by 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 nonnegative real numbers; $H(\cdot)$ and $I(\cdot;\cdot)$ are the traditional entropy and mutual information; $D(\cdot\|\cdot)$ is the Kullback-Leibler (information) divergence and $\|\mu-\nu\|$ is the total variation distance of measures μ, ν on $\mathcal{A}$ defined as $\|\mu-\nu\| := \sum_{a\in\mathcal{A}} |\mu(a)-\nu(a)|$ or equivalently as $\|\mu-\nu\| := 2\sup_{A\subseteq\mathcal{A}} |\mu(A)-\nu(A)|$, cf. for example [45, Lemma 4.1.1]; $X-Y-Z$ denotes a Markov chain of random variables X, Y, and Z in this order; all logarithms, exponentials, and information quantities are taken to the basis 2; $\mathcal{P}(\cdot)$ denotes the set of all probability distributions; the product distribution $P_A \otimes P_B$ is defined by the product of its marginal distributions P_A and P_B, i.e., $P_A \otimes P_B(a,b) = P_A(a)P_B(b)$ for all $a\in\mathcal{A}, b\in\mathcal{B}$; $\mathbb{1}(\cdot)$ is the indicator function; $\mathbb{E}[\cdot]$ and $\mathbb{P}\{\cdot\}$ are the expectation and the probability; $\mathrm{lhs} := \mathrm{rhs}$ means the value of the right hand side (rhs) is assigned to the left hand side (lhs).

II. Bidirectional Broadcast Channel With Confidential Messages

A. System Model and Strong Secrecy

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 channels $W_i^{\otimes n}(y_i^n|x^n) = \prod_{k=1}^n W_i(y_{i,k}|x_k),\ i=1,2$, only.

In this paper we consider the standard model with a block code of arbitrary but fixed length n. The set of individual (or bidirectional) messages of node i is denoted by $\mathcal{M}_i := \{1,\dots,M_{i,n}\}$, $i=1,2$, which is also known at the relay node. Further, the set of confidential messages of the relay node is denoted by $\mathcal{M}_c := \{1,\dots,M_{c,n}\}$. We will frequently abbreviate the set of all individual messages by $\mathcal{M}_{12} := \mathcal{M}_1 \times \mathcal{M}_2$ and the set of all messages by $\mathcal{M} := \mathcal{M}_c \times \mathcal{M}_{12} = \mathcal{M}_c \times \mathcal{M}_1 \times \mathcal{M}_2$. Note that the messages sets will have the size of the form $M_{1,n} = 2^{nR_2}$, $M_{2,n} = 2^{nR_1}$, and $M_{c,n} = 2^{nR_c}$, where R_i and R_c are the rates of the corresponding individual and confidential messages, $i=1,2$.

In the bidirectional broadcast (BBC) phase we assume that the relay has successfully decoded both individual messages $m_1 \in \mathcal{M}_1$ and $m_2 \in \mathcal{M}_2$ that nodes 1 and 2 have sent in the previous multiple access (MAC) phase. Besides both individual messages the relay additionally transmits a confidential message $m_c \in \mathcal{M}_c$ intended for node 1, which has to be kept secret from nonlegitimate node 2.

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

$$E : \mathcal{M}_c \times \mathcal{M}_1 \times \mathcal{M}_2 \rightarrow \mathcal{P}(\mathcal{X}^n)$$

and decoders at nodes 1 and 2

$$\varphi_1 : \mathcal{Y}_1^n \times \mathcal{M}_1 \rightarrow \mathcal{M}_c \times \mathcal{M}_2$$
$$\varphi_2 : \mathcal{Y}_2^n \times \mathcal{M}_2 \rightarrow \mathcal{M}_1.$$

The encoder is allowed to be stochastic which means that it is specified by conditional probabilities $E(x^n|m)$ with $\sum_{x^n\in\mathcal{X}^n} E(x^n|m) = 1$ for each $m \in \mathcal{M}$. Here, $E(x^n|m)$ denotes the probability that the message $m \in \mathcal{M}$ is encoded as $x^n \in \mathcal{X}^n$.

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 $\varphi_1(y_1^n,m_1)\neq(m_c,m_2)$. Accordingly, the decoder at node 2 is in error if $\varphi_2(y_2^n,m_2)\neq m_1$. Then, the average probabilities of error at nodes 1 and 2 are given by

$$\begin{aligned}\bar{e}_{1,n}:=&\frac{1}{|\mathcal{M}|}\sum_{m\in\mathcal{M}}\sum_{x^n\in\mathcal{X}^n}\\ &\times\sum_{\substack{y_1^n\in\mathcal{Y}_1^n:\\ \varphi_1(y_1^n,m_1)\neq(m_c,m_2)}}W_1^{\otimes n}(y_1^n|x^n)E(x^n|m)\\ \bar{e}_{2,n}:=&\frac{1}{|\mathcal{M}|}\sum_{m\in\mathcal{M}}\sum_{x^n\in\mathcal{X}^n}\\ &\times\sum_{\substack{y_2^n\in\mathcal{Y}_2^n:\\ \varphi_2(y_2^n,m_2)\neq m_1}}W_2^{\otimes n}(y_2^n|x^n)E(x^n|m).\end{aligned}$$

To ensure that the confidential message is kept secret from nonlegitimate node 2, we require $I(M_c;Y_2^n|M_2)\leq\epsilon_n$ for some (small) $\epsilon_n>0$ with M_c and M_2 the random variables uniformly distributed over the sets $\mathcal{M}_c$ and $\mathcal{M}_2$ and $Y_2^n=(Y_{2,1},Y_{2,2},\ldots,Y_{2,n})$ the corresponding output at node 2. This criterion is known as *strong secrecy* [19].

Remark 1: There exists a weaker notion of secrecy where the mutual information term is additionally normalized by the block length n, i.e., we require $I(M_c;Y_2^n|M_2)/n\leq\epsilon_n$ for some (small) $\epsilon_n>0$. This criterion is known as *weak secrecy*.

B. Strong Secrecy and Classes of Attacks

Based on the wiretapper's intentions and its available resources, one can classify the behavior of the wiretapper into different classes of attacks. For example, attacks with limited computational power as usually assumed in the cryptographic context or attacks with unlimited computational capabilities.

The weak secrecy criterion has the drawback that no operational meaning has been given to it yet. This means that even if this criterion is satisfied, it is not clear what a nonlegitimate receiver can or cannot do to obtain information about the confidential message. Thus, it is not clear against what kind of attacks the confidential message is protected. However, this secrecy criterion is widely adopted and was first analyzed by Wyner in his landmark paper [2].

In contrast, it is shown in [20], [21] for the wiretap channel that the strong secrecy criterion has the following operational meaning: no matter how the nonlegitimate node tries to decode the confidential message, the average probability of error tends to one. Since this holds for all possible decoding strategies, the confidential message is protected against attacks with unlimited computational capabilities (and therewith also against attacks with limited resources). Here, we want to establish a similar interpretation for the BBC with confidential messages.

Proposition 1: Assume that for any given code of Definition 1 the nonlegitimate node 2 has a decoder intended for the confidential message given as

$$\varphi_2':\mathcal{Y}_2^n\times\mathcal{M}_2\rightarrow\mathcal{M}_c.$$

If $I(M_c;Y_2^n|M_2)\leq\epsilon_n$, then

$$\mathbb{P}\{\varphi_2'(Y_2^n,M_2)\neq M_c\}\geq 1-\lambda_n(\epsilon_n)$$

with $\lambda_n(\epsilon_n)\rightarrow 0$ as $\epsilon_n\rightarrow 0$.

Proof: Suppose that the decoder φ_2' at nonlegitimate node 2 is specified by decoding sets $\{\mathcal{D}_{m_c|m_2}\subset\mathcal{Y}_2^n:(m_c,m_2)\in\mathcal{M}_c\times\mathcal{M}_2\}$ with $\bigcup_{m_c\in\mathcal{M}_c}\mathcal{D}_{m_c|m_2}=\mathcal{Y}_2^n$ for every $m_2\in\mathcal{M}_2$. Note that for given side information $m_2\in\mathcal{M}_2$, the decoding sets are disjoint, i.e., $\mathcal{D}_{\hat{m}_c|m_2}\cap\mathcal{D}_{m_c|m_2}=\emptyset$ for $\hat{m}_c\neq m_c$, but need not be disjoint for different $\hat{m}_2\neq m_2$. Since M_c and M_2 are assumed to be independent and uniformly distributed, we can write the average probability of error as

$$\begin{aligned}&\mathbb{P}\{\varphi_2'(Y_2^n,M_2)\neq M_c\}\\ &=\frac{1}{|\mathcal{M}_c||\mathcal{M}_2|}\sum_{(m_c,m_2)\in\mathcal{M}_c\times\mathcal{M}_2}\\ &\quad\times\mathbb{P}\{Y_2^n\notin\mathcal{D}_{m_c|m_2}|M_c=m_c,M_2=m_2\}\\ &=\frac{1}{|\mathcal{M}_2|}\sum_{(m_c,m_2)\in\mathcal{M}_c\times\mathcal{M}_2}\\ &\quad\times P_{Y_2^nM_c|M_2}(\mathcal{D}_{m_c|m_2}^c\times\{m_c\}|m_2).\end{aligned}\tag{1}$$

On the other hand we know from the strong secrecy criterion that

$$\begin{aligned}\epsilon_n&>I(M_c;Y_2^n|M_2)\\ &=\frac{1}{|\mathcal{M}_2|}\sum_{m_2\in\mathcal{M}_2}\\ &\quad\times D\big(P_{Y_2^nM_c|M_2=m_2}\big\|P_{Y_2^n|M_2=m_2}\otimes P_{M_c|M_2=m_2}\big)\\ &\geq\frac{1}{|\mathcal{M}_2|}\sum_{m_2\in\mathcal{M}_2}\\ &\quad\times\frac{1}{2\ln 2}\big\|P_{Y_2^n|M_2=m_2}\otimes P_{M_c|M_2=m_2}-P_{Y_2^nM_c|M_2=m_2}\big\|^2\\ &\geq\frac{1}{|\mathcal{M}_2|}\sum_{m_2\in\mathcal{M}_2}\\ &\quad\times\frac{1}{\ln 2}\bigg((P_{Y_2^n|M_2}\otimes P_{M_c|M_2})\Big(\bigcup_{m_c\in\mathcal{M}_c}\mathcal{D}_{m_c|m_2}^c\times\{m_c\}|m_2\Big)\\ &\qquad-P_{Y_2^nM_c|M_2}\Big(\bigcup_{m_c\in\mathcal{M}_c}\mathcal{D}_{m_c|m_2}^c\times\{m_c\}|m_2\Big)\bigg)^2\end{aligned}$$

where the second last step follows from Pinsker's inequality[2] and the last one from the definition of total variation distance. Using the Jensen's inequality, we obtain

$$\begin{aligned}\epsilon_n\geq\frac{1}{\ln 2}\bigg(&\frac{1}{|\mathcal{M}_2|}\sum_{(m_c,m_2)\in\mathcal{M}_c\times\mathcal{M}_2}\\ &\times P_{Y_2^n|M_2}(\mathcal{D}_{m_c|m_2}^c|m_2)P_{M_c|M_2}(m_c|m_2)\\ &-\frac{1}{|\mathcal{M}_2|}\sum_{(m_c,m_2)\in\mathcal{M}_c\times\mathcal{M}_2}\\ &\times P_{Y_2^nM_c|M_2}(\mathcal{D}_{m_c|m_2}^c\times\{m_c\}|m_2)\bigg)^2.\end{aligned}$$

[2] This bound with a worse constant was first given by Pinsker [46] and is therefore also known as Pinsker's inequality, cf. also [47, Problem 3.18].

Extracting the root and inserting this into (1), the average probability of error can be bounded from below as

$$\begin{aligned}
&\mathbb{P}\{\varphi_2'(Y_2^n, M_2) \neq M_c\} \\
&\geq \frac{1}{|\mathcal{M}_2|} \sum_{(m_c,m_2)\in\mathcal{M}_c\times\mathcal{M}_2} P_{Y_2^n|M_2}(\mathcal{D}^c_{m_c|m_2}|m_2) \\
&\quad \times P_{M_c|M_2}(m_c|m_2) - \sqrt{\epsilon_n \ln 2} \\
&= \frac{1}{|\mathcal{M}_c||\mathcal{M}_2|} \sum_{(m_c,m_2)\in\mathcal{M}_c\times\mathcal{M}_2} P_{Y_2^n|M_2}(\mathcal{D}^c_{m_c|m_2}|m_2) \\
&\quad - \sqrt{\epsilon_n \ln 2} \\
&= \frac{1}{|\mathcal{M}_c||\mathcal{M}_2|} \sum_{(m_c,m_2)\in\mathcal{M}_c\times\mathcal{M}_2} \\
&\quad \times \big(1 - P_{Y_2^n|M_2}(\mathcal{D}_{m_c|m_2}|m_2)\big) - \sqrt{\epsilon_n \ln 2} \\
&= 1 - \frac{1}{|\mathcal{M}_c|} - \sqrt{\epsilon_n \ln 2} = 1 - \lambda_n(\epsilon_n)
\end{aligned}$$

with $\lambda_n(\epsilon_n) = 1/|\mathcal{M}_c| - \sqrt{\epsilon_n \ln 2}$. The first equality follows from the fact that M_c and M_2 are independent of each other and uniformly distributed and the last equality follows from the observation that for any nonnegative numbers $a_1, \dots, a_N$ with $\sum_{i=1}^N a_i = 1$ we have $\sum_{i=1}^N (1 - a_i) = N - 1$. Later we will choose ϵ_n to have the form $\epsilon_n = 2^{-n\beta}$ with some $\beta > 0$, so that the average (and therewith also the maximum) probability of error at nonlegitimate node 2 tends to one exponentially fast as $n \longrightarrow \infty$. ■

Remark 2: Proposition 1 shows that if $I(M_c; Y_2^n|M_2)$ is small, the decoding error at nonlegitimate node 2 tends to one regardless of the decoding sets at the nonlegitimate node. Thus, the confidential message is protected against all possible decoding strategies the nonlegitimate node might choose.

Definition 2: A rate triple $(R_c, R_1, R_2) \in \mathbb{R}_+^3$ is said to be *achievable* for the BBC with confidential messages if for every $\tau > 0$ there is an $n(\tau) \in \mathbb{N}$ and a sequence of $(n, M_{c,n}, M_{1,n}, M_{2,n})$-codes such that for all $n \geq n(\tau)$ we have $1/n \log M_{c,n} \geq R_c - \tau$, $1/n \log M_{2,n} \geq R_1 - \tau$, $1/n \log M_{1,n} \geq R_2 - \tau$, and

$$I(M_c; Y_2^n|M_2) \leq \epsilon_n \tag{2}$$

while $\bar{e}_{1,n}, \bar{e}_{2,n}, \epsilon_n \longrightarrow 0$ as $n \longrightarrow \infty$. The set of all achievable rate triples is the *strong secrecy capacity region* of the BBC with confidential messages and is denoted by $\mathcal{C}_{\mathrm{BBC}}^S$.

Now we are in the position to state the main result of this paper which is given the following theorem.

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

$$R_c \leq I(V; Y_1|U) - I(V; Y_2|U) \tag{3a}$$

$$R_i \leq I(U; Y_i), \quad i = 1, 2 \tag{3b}$$

for random variables $U - V - X - (Y_1, Y_2)$ with joint probability distribution $P_U(u)P_{V|U}(v|u)P_{X|V}(x|v)W(y_1, y_2|x)$.

Proof: The converse follows immediately from the following observation. In [48] we established the *weak secrecy capacity region* of the BBC with confidential messages where (2) is replaced by the weaker condition $I(M_c; Y_2^n|M_2)/n$, cf. also Remark 1. Thus, it is clear that the strong secrecy capacity region $\mathcal{C}_{\mathrm{BBC}}^S$ must be contained in the weak secrecy capacity region $\mathcal{C}_{\mathrm{BBC}}^W$, i.e., $\mathcal{C}_{\mathrm{BBC}}^S \subseteq \mathcal{C}_{\mathrm{BBC}}^W$. Since interestingly, $\mathcal{C}_{\mathrm{BBC}}^W$ is given by exactly the same expression (3), the weak secrecy capacity region $\mathcal{C}_{\mathrm{BBC}}^W$ establishes immediately the desired converse for $\mathcal{C}_{\mathrm{BBC}}^S$. Therefore, it remains to show the achievability of (3) for the strong secrecy criterion.

III. Key Idea for Strong Secrecy

There were several methods proposed to establish strong secrecy based on different techniques such as coloring hypergraphs [22], privacy-amplification [19], or resolvability [25], [26]. In this paper we use Devetak's approach introduced in [24] for the wiretap channel and extend it to the BBC with confidential messages. This approach establishes strong secrecy using only the noisy broadcast channel. Therefore we start with a basic observation concerning the relationship of total variation distance and (conditional) mutual information.

Lemma 1: Let $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ be finite sets and A, B, and C be corresponding random variables. If

$$\|P_{A|C=c} \otimes P_{B|C=c} - P_{AB|C=c}\| \leq \epsilon \leq \frac{1}{2}$$

is satisfied for every $c \in \mathcal{C}$, then

$$I(A; B|C) \leq -\epsilon \log \frac{\epsilon}{|\mathcal{A}||\mathcal{B}|}.$$

Proof: Basically, the proof follows from the continuity of the entropy function, cf. [47, Lemma 1.2.7]. Accordingly, we observe that we can rewrite the (conditional) mutual information as

$$\begin{aligned}
&I(A; B|C) \\
&\quad = H(A|C) + H(B|C) - H(A, B|C) \\
&\quad = \sum_{c\in\mathcal{C}} \mathbb{P}\{C = c\} \\
&\qquad \times \big(H(P_{A|C=c} \otimes P_{B|C=c}) - H(P_{AB|C=c})\big)
\end{aligned}$$

using the definition of mutual information. Since $\|P_{A|C=c} \otimes P_{B|C=c} - P_{AB|C=c}\| \leq \epsilon \leq 1/2$ for all $c \in \mathcal{C}$, we immediately obtain from [47, Lemma 1.2.7] that $|H(P_{A|C=c} \otimes P_{B|C=c}) - H(P_{AB|C=c})| \leq -\epsilon \log \epsilon/(|\mathcal{A}||\mathcal{B}|)$ for all $c \in \mathcal{C}$ which proves the lemma. ■

Thus, for $I(M_c; Y_2^n|M_2)$ to be small, it suffices to find for every $\epsilon > 0$ a code that satisfies $\|P_{Y_2^n|M_2=m_2} \otimes P_{M_c|M_2=m_2} - P_{Y_2^n M_c|M_2=m_2}\| \leq \epsilon$ for all $m_2 \in \mathcal{M}_2$. Moreover, the following lemma shows that it suffices to find for every $m = (m_c, m_{12}) \in \mathcal{M}$ a measure $\vartheta_{m_{12}}$ on $\mathcal{Y}_2^n$ such that $\|P_{Y_2^n|M=m} - \vartheta_{m_{12}}\| \leq \epsilon$.

Lemma 2: If there exists for every $m_{12} \in \mathcal{M}_1 \times \mathcal{M}_2$ a measure $\vartheta_{m_{12}}$ on $\mathcal{Y}_2^n$ with

$$\|P_{Y_2^n|M=m} - \vartheta_{m_{12}}\| \leq 2^{-n\beta} \tag{4}$$

for some $\beta > 0$, then

$$I(M_c; Y_2^n|M_2) \leq 2^{-n\beta/2} \tag{5}$$

for n large enough.

Proof: Since we can write

$$P_{Y_2^n|M_2=m_2} = \frac{1}{|\mathcal{M}_c||\mathcal{M}_1|} \sum_{m_c,m_1} P_{Y_2^n|M_c=m_c,M_1=m_1,M_2=m_2}$$

and M_c, M_1, and M_2 are independent and uniformly distributed, we get for all $m_2 \in \mathcal{M}_2$

$$\begin{aligned}
&\|P_{Y_2^n M_c|M_2=m_2} - P_{Y_2^n|M_2=m_2} \otimes P_{M_c|M_2=m_2}\| \\
&\quad\le \frac{1}{|\mathcal{M}_c||\mathcal{M}_1|} \sum_{(m_c,m_1)\in\mathcal{M}_c\times\mathcal{M}_1} \|P_{Y_2^n|M=m} - P_{Y_2^n|M_{12}=m_{12}}\| \\
&\quad\le \frac{1}{|\mathcal{M}_c||\mathcal{M}_1|} \sum_{(m_c,m_1)\in\mathcal{M}_c\times\mathcal{M}_1} \Big(\|P_{Y_2^n|M=m} - \vartheta_{m_{12}}\| \\
&\qquad\qquad + \|\vartheta_{m_{12}} - P_{Y_2^n|M_{12}=m_{12}}\|\Big) \\
&\quad\le \frac{1}{|\mathcal{M}_c||\mathcal{M}_1|} \sum_{(m_c,m_1)\in\mathcal{M}_c\times\mathcal{M}_1} \Big(\|P_{Y_2^n|M=m} - \vartheta_{m_{12}}\| \\
&\qquad\qquad + \frac{1}{|\mathcal{M}_c|} \sum_{m_c\in\mathcal{M}_c} \|\vartheta_{m_{12}} - P_{Y_2^n|M=m}\|\Big) \\
&\quad\le 2\cdot 2^{-n\beta}.
\end{aligned}$$

where the second inequality follows from the triangle inequality and the last inequality from assumption (4). Thus, we have $\|P_{Y_2^n M_c|M_2=m_2} - P_{Y_2^n|M_2=m_2} \otimes P_{M_c|M_2=m_2}\| \le 2\cdot 2^{-n\beta} \le 1/2$ for n large enough, so that Lemma 1 immediately yields

$$I(M_c;Y_2^n|M_2) \le -2\cdot 2^{-n\beta} \log \frac{2\cdot 2^{-n\beta}}{|\mathcal{M}_c||\mathcal{Y}_2^n|} \le 2^{-n\beta/2}$$

where the last inequality holds for n large enough proving the lemma. ■

Remark 3: The measure $\vartheta_{m_{12}}$ in Lemma 2 is constructed in such a way that the mutual information term $I(M_c;Y_2^n|M_2)$ decreases exponentially fast for increasing block length. With Proposition 1 this immediately implies that the decoding error at nonlegitimate node 2 goes exponentially fast to one regardless of the decoding strategy the nonlegitimate receiver may use, cf. also Section II-B.

IV. Codebook Design for Strong Secrecy

In this section we present the proof of achievability of Theorem 1. First, we only consider random variables $U - X - (Y_1,Y_2)$ and prove the achievability of all rate triples $(R_c,R_1,R_2) \in \mathbb{R}_+^3$ that satisfy

$$R_c \le I(X;Y_1|U) - I(X;Y_2|U) \tag{6a}$$

$$R_i \le I(U;Y_i), \quad i=1,2 \tag{6b}$$

with strong secrecy. After that we are able to extend this to the desired region (3).

To prove (6) we construct a codebook that enables reliable communication of all messages with the desired rates, while ensuring the secrecy of the confidential message. Additionally to the key observation in Lemma 2, we need the following two ingredients.

The first one ensures reliable communication of the two bidirectional messages m_1 and m_2 to nodes 2 and 1, respectively, and of the confidential message m_c to node 1. Let us drop the security requirement on m_c for a moment, i.e., it need not be kept secret from nonlegitimate node 2. For better differentiation we call this a *private* message and obtain the following achievable rate region.

Lemma 3: An achievable rate region for the BBC with an additional private message for node 1 is given by set of all rate triples $(R_p,R_1,R_2) \in \mathbb{R}_+^3$ that satisfy

$$R_p \le I(X;Y_1|U) \tag{7a}$$

$$R_i \le I(U;Y_i), \quad i=1,2 \tag{7b}$$

for random variables $U - X - (Y_1,Y_2)$ with joint probability distribution $P_U(u)P_{X|U}(x|u)W(y_1,y_2|x)$ and average probability of errors smaller than $2^{-n\gamma}$ with some $\gamma > 0$ for block length n large enough.

Proof: The proof can be found in the appendix. ■

The second ingredient will be used to incorporate the strong secrecy requirement on m_c and to ensure the validity of (4). In more detail, we will exploit the concentration of sums of i.i.d. random variables around their expectation as given in the following lemma which is due to Chernoff and Hoeffding.

Lemma 4: Let $b > 0$ and let $Z_1,\dots,Z_L$ be i.i.d. random variables with values in $[0,b]$. Let $\mu = \mathbb{E}[Z_1]$ be the expectation of Z_1. Then

$$\mathbb{P}\left\{\frac{1}{L}\sum_{l=1}^{L} Z_l \notin [(1\pm\epsilon)\mu]\right\} \le 2\exp\left(-L\cdot\frac{\epsilon^2\mu}{2b\ln 2}\right)$$

where $[(1\pm\epsilon)\mu]$ denotes the interval $[(1-\epsilon)\mu,(1+\epsilon)\mu]$. ■

After these preliminary considerations we come to the coding part. Here we extensively make use of the concept of δ-*typical* sequences from Csiszár and Körner [47] which is briefly recalled.

For any distribution $P_U \in \mathcal{P}(\mathcal{U})$ a sequence $u^n \in \mathcal{U}^n$ is said to be δ-*typical* if $|N(u|u^n)/n - P_U(u)| \le \delta$ for every $u \in \mathcal{U}$ and, in addition, $N(u|u^n) = 0$ if $P_U(u) = 0$. Here, $N(u|u^n)$ denotes the number of indices i such that $u_i = u$, $i = 1,\dots,n$. The set of all such typical sequences is denoted by $\mathcal{T}_{U,\delta}^n$. Further, for any stochastic matrix $P_{X|U} : \mathcal{U} \to \mathcal{P}(\mathcal{X})$ a sequence $x^n \in \mathcal{X}^n$ is called δ-*typical* for given $u^n \in \mathcal{U}^n$ if $|N(u,x|u^n,x^n)/n - P_{X|U}(x|u)N(u|u^n)/n| \le \delta$ for every $x \in \mathcal{X}$ and, in addition, $N(u,x|u^n,x^n) = 0$ if $P_{X|U}(x|u) = 0$. The set of all such sequences is denoted by $\mathcal{T}_{X|U,\delta}^n(u^n)$.

For any probability distribution $P_U \in \mathcal{P}(\mathcal{U})$ we define the probability measure $P'_{U^n} \in \mathcal{P}(\mathcal{U}^n)$ as

$$P'_{U^n}(u^n) := \frac{P_U^{\otimes n}(u^n)}{P_U^{\otimes n}(\mathcal{T}_{U,\delta}^n)} \tag{8}$$

if $u^n \in \mathcal{T}_{U,\delta}^n$ and $P'_{U^n}(u^n) = 0$ else, where $P_U^{\otimes n}(u^n) := \prod_{k=1}^n P_U(u_k)$. Similarly, for any $P_{X|U} : \mathcal{U} \to \mathcal{P}(\mathcal{X})$ we define $P'_{X^n|U^n}$ as

$$P'_{X^n|U^n}(x^n|u^n) := \frac{P_{X|U}^{\otimes n}(x^n|u^n)}{P_{X|U}^{\otimes n}(\mathcal{T}_{X|U,\delta}^n(u^n)|u^n)} \tag{9}$$

if $x^n \in \mathcal{T}_{X|U,\delta}^n(u^n)$ and $P'_{X^n|U^n}(x^n|u^n) = 0$ else, where $P_{X|U}^{\otimes n}(x^n|u^n) := \prod_{k=1}^n P_{X|U}(x_k|u_k)$.

This allows us to define the random coding scheme with block length n as follows. Let $\mathcal{M}_1$ and $\mathcal{M}_2$ be the sets of individual messages where their sizes $M_{1,n}$ and $M_{2,n}$ are determined by (7b), cf. Lemma 3. Let $\mathcal{M}_c$ be the set of confidential messages and further $\mathcal{L} := \{1, \dots, L_n\}$ with $M_{c,n}$ and L_n to be fixed later. Let $\{U^n_{m_{12}} : m_{12} \in \mathcal{M}_1 \times \mathcal{M}_2\}$ be i.i.d. random variables with values in $\mathcal{U}^n$ according to P'_{U^n}, cf. (8). Then for each pair of bidirectional messages $m_{12} = (m_1, m_2) \in \mathcal{M}_{12}$ we define random variables $\{X^n_{lm_cm_{12}} : (l, m_c) \in \mathcal{L} \times \mathcal{M}_c\}$ with values in $\mathcal{X}^n$, which are i.i.d. conditional on $U^n_{m_{12}}$ according to $P'_{X^n|U^n}$, cf. (9).

Now we come to the application of Lemma 4. Note that the channel $W_2 : \mathcal{X} \to \mathcal{P}(\mathcal{Y}_2)$ to the nonlegitimate node 2 can also be regarded as a channel $W_2 : \mathcal{U} \times \mathcal{X} \to \mathcal{P}(\mathcal{Y}_2)$ where the $\mathcal{U}$-inputs do not make any difference. Moreover, it will be sufficient to concentrate only on those outputs that are typical; the probability of all other outputs will be of no consequence as we will see later, cf. (18). Therefore, for every $(l, m_c, m_{12}) \in \mathcal{L} \times \mathcal{M}_c \times \mathcal{M}_{12}$ and $y^n_2 \in \mathcal{Y}^n_2$, let

$$\begin{aligned}\vartheta'_{U^n_{m_{12}}}(y^n_2) = \mathbb{E}\big[&W_2^{\otimes n}(y^n_2|X^n_{lm_cm_{12}})\\ &\times \mathbb{1}_{\mathcal{T}^n_{Y_2|XU,\delta}(X^n_{lm_cm_{12}}, U^n_{m_{12}})}(y^n_2)|U^n_{m_{12}}\big],\end{aligned} \tag{10}$$

where for any set $\mathcal{A} \subset \mathcal{Y}^n_2$, we let $\mathbb{1}_{\mathcal{A}}(y^n_2) = 1$ if $y^n_2 \in \mathcal{A}$ and $\mathbb{1}_{\mathcal{A}}(y^n_2) = 0$ else. Then for any $\epsilon_n > 0$ we define

$$\begin{aligned}\mathcal{F}_{U^n_{m_{12}}} := \big\{&y^n_2 \in \mathcal{T}^n_{Y_2|U,2|\mathcal{X}|\delta}(U^n_{m_{12}}) :\\ &\vartheta'_{U^n_{m_{12}}}(y^n_2) \geq \epsilon_n |\mathcal{T}^n_{Y_2|U,2|\mathcal{X}|\delta}(U^n_{m_{12}})|^{-1}\big\}\end{aligned} \tag{11}$$

and finally set

$$\vartheta_{U^n_{m_{12}}}(y^n_2) := \vartheta'_{U^n_{m_{12}}}(y^n_2)\mathbb{1}_{\mathcal{F}_{U^n_{m_{12}}}}(y^n_2). \tag{12}$$

Next, we consider for every $(l, m_c, m_{12}) \in \mathcal{L} \times \mathcal{M}_c \times \mathcal{M}_{12}$ and $y^n_2 \in \mathcal{Y}^n_2$, the random variable

$$\begin{aligned}\tilde{W}^n_2(y^n_2|X^n_{lm_cm_{12}}, U^n_{m_{12}}) := &W_2^{\otimes n}(y^n_2|X^n_{lm_cm_{12}})\\ &\times \mathbb{1}_{\mathcal{T}^n_{Y_2|XU,\delta}(X^n_{lm_cm_{12}}, U^n_{m_{12}})}(y^n_2)\mathbb{1}_{\mathcal{F}_{U^n_{m_{12}}}}(y^n_2).\end{aligned} \tag{13}$$

Note that from (10)–(13) follows that $\vartheta_{U^n_{m_{12}}}(y^n_2) = \mathbb{E}[\tilde{W}^n_2(y^n_2|X^n_{lm_cm_{12}}, U^n_{m_{12}})|U^n_{m_{12}}]$ is satisfied. Conditional on $U^n_{m_{12}}$, these random variables are i.i.d. Moreover, as the input pair $(X^n_{lm_cm_{12}}, U^n_{m_{12}})$ is jointly 2δ-typical with respect to the joint distribution P_{XU}, and the outputs of $\tilde{W}^n_2$ are δ-typical conditional on the inputs, it is well-known that (13) is upper-bounded by

$$\tilde{W}^n_2(y^n_2|X^n_{lm_cm_{12}}, U^n_{m_{12}}) \leq 2^{-n(H(Y_2|X,U)-\delta_1)} \tag{14}$$

for some $\delta_1 = \delta_1(\delta)$, see e.g., [47]. Then we define $\mathcal{W}_{U^n_{m_{12}}}(y^n_2)$ to be the event that

$$\frac{1}{L_n}\sum_{l=1}^{L_n} \tilde{W}^n_2(y^n_2|X^n_{lm_cm_{12}}, U^n_{m_{12}}) \in \big[(1 \pm \epsilon_n)\vartheta_{U^n_{m_{12}}}(y^n_2)\big]. \tag{15}$$

Now let $y^n_2 \in \mathcal{Y}^n_2$. Then the probability of the complement of $\mathcal{W}_{U^n_{m_{12}}}(y^n_2)$ is

$$\begin{aligned}&\mathbb{P}\{(\mathcal{W}_{U^n_{m_{12}}}(y^n_2))^c\}\\ &\quad= \sum_{u^n \in \mathcal{U}^n} \mathbb{P}\{U^n_{m_{12}} = u^n\}\\ &\qquad\times \mathbb{P}\left\{\big(\mathcal{W}_{U^n_{m_{12}}}(y^n_2)\big)^c\big|U^n_{m_{12}} = u^n\right\}\\ &\quad\leq \sum_{u^n \in \mathcal{U}^n} \mathbb{P}\{U^n_{m_{12}} = u^n\}\\ &\qquad\times 2\exp\left(-L_n \cdot \frac{\epsilon^2_n 2^{n(H(Y_2|X,U)-\delta_1)}\vartheta_{u^n}(y^n_2)}{2\ln 2}\right)\\ &\quad\leq 2\exp\left(-L_n \cdot \frac{\epsilon^3_n 2^{-n(I(X;Y_2|U)+\delta_1+\delta_2)}}{2\ln 2}\right)\end{aligned} \tag{16}$$

where the equality follows from the law of total probability, the first inequality is due to Lemma 3 (with $\vartheta_{U^n_{m_{12}}}(y^n_2)$ in the role μ) and (14), and the second inequality follows from (11) and

$$|\mathcal{T}^n_{Y_2|U,2|\mathcal{X}|\delta}(U^n_{m_{12}})| \leq 2^{n(H(Y_2|U)+\delta_2)}$$

for some $\delta_2 = \delta_2(\delta)$, see e.g., [47], which applies here because $U^n_{m_{12}}$ is δ-typical. Note that if we choose $\epsilon_n = 2^{-n\beta}$ with $\beta \leq \min\{\gamma, \delta_1 + \delta_2\}/4$, cf. also Lemma 3, then (16) tends to zero doubly-exponentially for

$$L_n \geq 2^{n(I(X;Y_2|U)+2(\delta_1+\delta_2))}. \tag{17}$$

This provides the basis for the proof of (4), which is the existence of a measure $\vartheta_{m_{12}}$ for given individual messages $m_{12} \in \mathcal{M}_{12}$ such that then all outputs at the nonlegitimate node are close to it regardless of the transmitted message m_c. Once (4) is established, Lemma 2 guarantees the strong secrecy of the confidential message.

Next, we determine the sizes of the remaining sets for the confidential messages. Without loss of generality we can assume that $I(X;Y_2|U) < I(X;Y_1|U)$ holds. We choose δ (and therewith also δ_1 and δ_2) small enough such that (17) is satisfied and at the same time

$$L_n \leq 2^{n(I(X;Y_2|U)+3(\delta_1+\delta_2))} < 2^{nI(X;Y_1|U)-\tau/2}$$

for some $\tau > 0$ small enough. Further, for the set of confidential messages $\mathcal{M}_c$ we set

$$M_{c,n} \leq 2^{n(I(X;Y_1|U)-\tau/2-I(X;Y_2|U)-3(\delta_1+\delta_2))}.$$

From (16)–(17) we know that (15) is satisfied for every $(m_c, m_{12}) \in \mathcal{M}_c \times \mathcal{M}_{12}$ and every $y^n_2 \in \mathcal{Y}^n_2$ with probability close to one. Further, with $\mathcal{M}_p = \mathcal{L} \times \mathcal{M}_c$ we know from the random coding proof of Lemma 3, cf. also the appendix, that the random codewords we have chosen are the codewords of a deterministic code achieving average errors $\bar{e}_{1,n}, \bar{e}_{2,n} \leq 2^{-n\gamma}$ with probability close to one. Thus, there must be realizations of $(U^n_{m_{12}}, X^n_{lm_cm_{12}})$ and $\vartheta_{U^n_{m_{12}}}$ which also have both these properties. We denote these realizations by $(u^n_{m_{12}}, x^n_{lm_cm_{12}})$ and $\vartheta_{m_{12}}$ respectively.

Now we construct an appropriate code with a stochastic encoder. Therefore, each message triple $(m_c, m_1, m_2) \in \mathcal{M}$ is mapped into the codeword $x^n_{lm_cm_{12}} \in \mathcal{X}^n$ with probability $1/L_n$. This already defines a stochastic encoder. Legitimate node 1 decodes the complete triple (l, m_c, m_2) having its side information m_1 available, while nonlegitimate node 2 only decodes its intended individual message m_1 with its own m_2. Interpreting (l, m_c) as a private message m_p for node 1 we know from Lemma 3 that this code is suitable for reliable transmission of all messages to their respective receivers. It remains to prove that (4) is satisfied.

Using the triangle inequality we obtain for every $m = (m_c, m_{12}) \in \mathcal{M}_c \times \mathcal{M}_{12}$

$$\begin{aligned}
&\left\|P_{Y_2^n|M=m} - \vartheta_{m_{12}}\right\| \\
&\quad\le \Bigg\|P_{Y_2^n|M}(\cdot|m) \\
&\qquad\quad - \frac{1}{L_n}\sum_{l=1}^{L_n} W_2^{\otimes n}(\cdot|x^n_{lm_cm_{12}}, u^n_{m_{12}}) \\
&\qquad\quad \times \mathbb{1}_{\mathcal{T}^n_{Y_2|XU,\delta}(x^n_{lm_cm_{12}}, u^n_{m_{12}})}\Bigg\| \\
&\qquad + \Bigg\|\frac{1}{L_n}\sum_{l=1}^{L_n} W_2^{\otimes n}(\cdot|x^n_{lm_cm_{12}}, u^n_{m_{12}}) \\
&\qquad\quad \times \mathbb{1}_{\mathcal{T}^n_{Y_2|XU,\delta}(x^n_{lm_cm_{12}}, u^n_{m_{12}})}(1 - \mathbb{1}_{\mathcal{F}_{m_{12}}})\Bigg\| \\
&\qquad + \Bigg\|\frac{1}{L_n}\sum_{l=1}^{L_n} \tilde{W}_2^n(\cdot|x^n_{lm_cm_{12}}, u^n_{m_{12}}) - \vartheta_{m_{12}}\Bigg\|.
\end{aligned}$$

We denote the three parts of the sum above by I, II, III in that order and bound each of them separately in the following. As the codewords satisfy (15), we immediately have $III \le \epsilon_n$.

We can write the first term I as

$$\begin{aligned}
I &= \Bigg\|P_{Y_2^n|M}(\cdot|m) \\
&\qquad - \frac{1}{L_n}\sum_{l=1}^{L_n} W_2^{\otimes n}(\cdot|x^n_{lm_cm_{12}}, u^n_{m_{12}}) \\
&\qquad \times \mathbb{1}_{\mathcal{T}^n_{Y_2|XU,\delta}(x^n_{lm_cm_{12}}, u^n_{m_{12}})}\Bigg\| \\
&\le \frac{1}{L_n}\sum_{l=1}^{L_n} \Bigg\|W_2^{\otimes n}(\cdot|x^n_{lm_cm_{12}}, u^n_{m_{12}}) \\
&\qquad \times (1 - \mathbb{1}_{\mathcal{T}^n_{Y_2|XU,\delta}(x^n_{lm_cm_{12}}, u^n_{m_{12}})})\Bigg\| \\
&= \frac{1}{L_n}\sum_{l=1}^{L_n} \\
&\qquad \times W_2^{\otimes n}\big((\mathcal{T}^n_{Y_2|XU,\delta}(x^n_{lm_cm_{12}}, u^n_{m_{12}}))^c|x^n_{lm_cm_{12}}, u^n_{m_{12}}\big) \\
&\le (n+1)^{|\mathcal{U}||\mathcal{X}||\mathcal{Y}_2|}2^{-nc\delta^2}
\end{aligned} \tag{18}$$

for some constant $c > 0$, where we again interpret $W_2 : \mathcal{U} \times \mathcal{X} \to \mathcal{P}(\mathcal{Y}_2)$ with additional $\mathcal{U}$-inputs which do not make a difference and use the fact that the probability that the output of a channel is not δ-typical conditional on the inputs is exponentially small, cf. for example [49, Lemma 2] or [50, Lemma III.1.3].

The second term II can be written as

$$\begin{aligned}
II &\le 1 - \frac{1}{L_n}\sum_{l=1}^{L_n} \\
&\qquad \times W_2^{\otimes n}(\mathcal{F}_{m_{12}} \\
&\qquad\qquad \cap \mathcal{T}^n_{Y_2|XU,\delta}(x^n_{lm_cm_{12}}, u^n_{m_{12}})|x^n_{lm_cm_{12}}, u^n_{m_{12}}) \\
&\le 1 - (1-\epsilon_n)\vartheta_{m_{12}}(\mathcal{F}_{m_{12}}) \\
&= 1 - (1-\epsilon_n)\vartheta'_{m_{12}}(\mathcal{F}_{m_{12}}) \\
&= 1 - (1-\epsilon_n) \\
&\qquad \times \big(\vartheta'_{m_{12}}(\mathcal{T}^n_{Y_2|U,2|\mathcal{X}|\delta}(u^n_{m_{12}})) \\
&\qquad\qquad - \vartheta'_{m_{12}}(\mathcal{T}^n_{Y_2|U,2|\mathcal{X}|\delta}(u^n_{m_{12}}) \setminus \mathcal{F}_{m_{12}})\big)
\end{aligned} \tag{19}$$

where the inequality follows from the validity of (15), the second equality from the fact that $\vartheta_{m_{12}}(\mathcal{F}_{m_{12}}) = \vartheta'_{m_{12}}(\mathcal{F}_{m_{12}})$, cf. (12), and the last equality from the definition of $\mathcal{F}_{m_{12}}$, cf. (11). Now we have

$$\begin{aligned}
&\vartheta'_{m_{12}}(\mathcal{T}^n_{Y_2|U,2|\mathcal{X}|\delta}(u^n_{m_{12}})) \\
&= \mathbb{E}\big[\tilde{W}_2^n\big(\mathcal{T}^n_{Y_2|U,2|\mathcal{X}|\delta}(U^n_{m_{12}})|X^n_{lm_cm_{12}}, U^n_{m_{12}}\big)|u^n_{m_{12}}\big] \\
&\ge \mathbb{E}\big[W_2^{\otimes n}\big(\mathcal{T}^n_{Y_2|XU,\delta}(X^n_{lm_cm_{12}}, U^n_{m_{12}})|X^n_{lm_cm_{12}}, U^n_{m_{12}}\big)|u^n_{m_{12}}\big] \\
&\ge 1 - (n+1)^{|\mathcal{U}||\mathcal{X}||\mathcal{Y}_2|}2^{-nc\delta^2}
\end{aligned} \tag{20}$$

and further

$$\vartheta'_{m_{12}}(\mathcal{T}^n_{Y_2|U,2|\mathcal{X}|\delta}(u^n_{m_{12}}) \setminus \mathcal{F}_{m_{12}}) \le \epsilon_n. \tag{21}$$

Inserting (20) and (21) into (19) the second term can be bounded from above as

$$\begin{aligned}
II &\le 1 - (1-\epsilon_n)(1 - (n+1)^{|\mathcal{U}||\mathcal{X}||\mathcal{Y}_2|}2^{-nc\delta^2} - \epsilon_n) \\
&\le 2\epsilon_n + (n+1)^{|\mathcal{U}||\mathcal{X}||\mathcal{Y}_2|}2^{-nc\delta^2}.
\end{aligned}$$

Altogether, we can bound the total variation distance as

$$\begin{aligned}
&\left\|P_{Y_2^n|M=m} - \vartheta_{m_{12}}\right\| \\
&\quad \le (n+1)^{|\mathcal{U}||\mathcal{X}||\mathcal{Y}_2|}2^{-nc\delta^2} \\
&\qquad + 2\epsilon_n + (n+1)^{|\mathcal{U}||\mathcal{X}||\mathcal{Y}_2|}2^{-nc\delta^2} + \epsilon_n \\
&\quad = 3\epsilon_n + 2(n+1)^{|\mathcal{U}||\mathcal{X}||\mathcal{Y}_2|}2^{-nc\delta^2}.
\end{aligned}$$

Note that this distance is exponentially small, as we chose ϵ_n to have the form $\epsilon_n = 2^{-n\beta}$. This establishes (4) so that by Lemma 2, the mutual information term $I(M_c; Y_2^n|M_2)$ can be made exponentially small as well.

This proves the achievability of the desired rate region, but only for random variables $U - X - (Y_1, Y_2)$ as given in (6). To obtain the whole region as given in (3), note that the relay can prefix an artificial channel $P_{X|V} : \mathcal{V} \to \mathcal{P}(\mathcal{X})$ with a finite alphabet $\mathcal{V}$ as initially proposed in [3] for the classical broadcast channel with confidential messages. Then the above construction can also be performed for the channel

$$(P_{X|V}W)(y_1, y_2|v) := \sum_{x \in \mathcal{X}} W(y_1, y_2|x)P_{X|V}(x|v)$$

which completes the proof of Theorem 1. ■

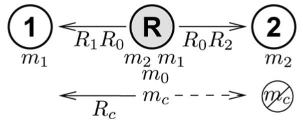

Fig. 2. Physical-layer service integration in bidirectional relay channels. In the BBC phase, the relay forwards the individual messages m_1 and m_2 and adds a common message m_0 with rate R_0 to the communication and further a confidential message m_c for node 1 with rate R_c which has to be kept secret from node 2.

Remark 4: Note that the effect of the prefix channel can be integrated in the stochastic encoder, cf. Definition 1.

V. Physical Layer Service Integration

The efficient integration of different services at the physical layer has been identified as a promising and important technique to further improve the spectral efficiency in next generation mobile networks. So far we studied the efficient integration of confidential services with strong secrecy in the three-node bidirectional relay channel at the physical layer. But besides such confidential services, operators of current wireless systems usually offer also multicast services where a common message has to be transmitted to a whole group of receivers; for example the Multimedia Broadcast Multicast Service (MBMS), as specified by the 3GPP organization, or the Multicast and Broadcast Service (MCBCS) in WiMAX.

Assuming the weak secrecy criterion, the efficient integration of common and confidential services in bidirectional relay channels is studied in [51], [52]. Therewith and with the results and techniques obtained so far, it is straightforward to extend the previous results to the case where common and confidential services are integrated in the three-node bidirectional relay channel at the physical layer where strong secrecy (instead of weak secrecy) is required for the confidential service, cf. Fig. 2. We immediately obtain the following result.

Corollary 1: The strong secrecy capacity region of the BBC with common and confidential messages is the set of all rate tuples $(R_c, R_0, R_1, R_2) \in \mathbb{R}_+^4$ that satisfy

$$\begin{aligned} R_c &\leq I(V;Y_1|U) - I(V;Y_2|U) \\ R_0 + R_i &\leq I(U;Y_i), \quad i = 1,2 \end{aligned}$$

for random variables $U - V - X - (Y_1, Y_2)$. ■

VI. Conclusion

In this work we studied the efficient integration of confidential services in the three-node bidirectional relay channel at the physical layer with strong secrecy. This required the analysis of the BBC with confidential messages for which we derived the strong secrecy capacity region. Interestingly, it is shown that the strong secrecy capacity region coincides with the corresponding weak secrecy capacity region. Thus, a requirement of strong security for confidential services in bidirectional relay channels does not lead to a loss in transmission rates compared to weaker security requirements.

Appendix

Here we present the proof of Lemma 3. We show the existence of a codebook that achieves the desired rates (7) by random coding arguments. Basically, we combine techniques of the classical bidirectional broadcast channel for the individual messages, cf. for example [29], and superposition coding techniques for the additional private message.

Remark 5: Note that for proving the achievability we will use the same input distributions (8)–(9) as considered later in the strong secrecy analysis, cf. Section IV. This will be indispensable to ensure that the random codebook will possess both properties-establishing reliable communication and realizing strong secrecy-simultaneously with high probability.

1) Random Codebook Generation and Encoding: We define individual message sets $\mathcal{M}_1$ and $\mathcal{M}_2$ with $M_{1,n} = \lfloor 2^{n(I(U;Y_2)-\tau/2)} \rfloor$ and $M_{2,n} = \lfloor 2^{n(I(U;Y_1)-\tau/2)} \rfloor$, respectively, and a private message set $\mathcal{M}_p$ with $M_{p,n} = \lfloor 2^{n(I(X;Y_1|U)-\tau/2)} \rfloor$ for some (small) $\tau > 0$.

In a first step, we generate $M_{12,n} = M_{1,n}M_{2,n}$ independent random codewords $U_{m_{12}}^n \in \mathcal{U}^n$ with $m_{12} = (m_1, m_2)$ according to P'_{U^n}, cf. (8). Then, for each $U_{m_{12}}^n \in \mathcal{U}^n$ we generate $M_{p,n}$ independent random random codewords $X_{m_p m_{12}}^n \in \mathcal{X}^n$ according to $P'_{X^n|U^n}$, cf. (9).

2) Decoding: The receiving nodes use typical set decoding where each node uses the received sequence and its side information to create the decoding sets. In more detail, if the message triple (m_p, m_1, m_2) has been sent, we define for the individual messages the sets

$$\mathcal{D}'_{m_2|m_1}(U_{m_{12}}^n) := \left\{ y_1^n \in \mathcal{Y}_1^n : (U_{m_{12}}^n, y_1^n) \in \mathcal{T}_{UY_1,\delta}^n \right\}$$

and therewith the decoding sets at receiving node 1 as

$$\begin{aligned} &\mathcal{D}_{m_2|m_1}(U^n) \\ &\qquad := \mathcal{D}'_{m_2|m_1}(U_{m_{12}}^n) \cap \Bigg(\bigcup_{\hat{m}_2 \neq m_2} \mathcal{D}'_{\hat{m}_2|m_1}(U_{m_1\hat{m}_2}^n) \Bigg)^c \end{aligned}$$

with $U^n := \{U_{m_{12}}^n\}_{m_{12} \in \mathcal{M}_{12}}$. Then in a second step we define for the additional private message the sets

$$\begin{aligned} &\mathcal{D}'_{m_p|m_{12}}(X_{m_p m_{12}}^n, U_{m_{12}}^n) \\ &\qquad := \left\{ y_1^n \in \mathcal{Y}_1^n : (U_{m_{12}}^n, X_{m_p m_{12}}^n, y_1^n) \in \mathcal{T}_{UXY_1,\delta}^n \right\} \end{aligned}$$

and therewith the decoding sets as

$$\begin{aligned} \mathcal{D}_{m_p|m_{12}}(X^n, U^n) &:= \mathcal{D}'_{m_p|m_{12}}(X_{m_p m_{12}}^n, U_{m_{12}}^n) \\ &\quad \cap \Bigg(\bigcup_{\hat{m}_p \neq m_p} \mathcal{D}'_{\hat{m}_p|m_{12}}(X_{\hat{m}_p m_{12}}^n, U_{m_{12}}^n) \Bigg)^c \end{aligned}$$

with $X^n := \{X_{m_p m_{12}}^n\}_{(m_p, m_{12}) \in \mathcal{M}_p \times \mathcal{M}_{12}}$. The sets $\mathcal{D}'_{m_1|m_2}(U_{m_{12}}^n)$ and $\mathcal{D}_{m_1|m_2}(U^n)$ for all individual messages $m_{12} \in \mathcal{M}_{12}$ at receiving node 2 are defined accordingly.

3) Analysis of Probability of Error: In the following we show that the expectations of the average probabilities of error at nodes 1 and 2 are exponentially small. For the corresponding analysis at receiving node 1, we identify from the decoding sets defined above for any message triple (m_p, m_1, m_2) the random error events:

$$\begin{aligned}\mathcal{E}^{(1)}_{m_2|m_1} &:= \big\{(U^n_{m_{12}}, Y^n_1) \notin \mathcal{T}^n_{UY_1,\delta}\big\} && \text{(22a)}\\ \mathcal{E}^{(2)}_{m_2|m_1} &:= \big\{\exists\, \hat{m}_2 \neq m_2 : (U^n_{m_1\hat{m}_2}, Y^n_1)\\ &\qquad \in \mathcal{T}^n_{UY_1,\delta}\big\} && \text{(22b)}\\ \mathcal{E}^{(3)}_{m_p|m_{12}} &:= \big\{(U^n_{m_{12}}, X^n_{m_p m_{12}}, Y^n_1) \notin \mathcal{T}^n_{UXY_1,\delta}\big\} && \text{(22c)}\\ \mathcal{E}^{(4)}_{m_p|m_{12}} &:= \big\{\exists\, \hat{m}_p \neq m_p : (U^n_{m_{12}}, X^n_{\hat{m}_p m_{12}}, Y^n_1)\\ &\qquad \in \mathcal{T}^n_{UXY_1,\delta}\big\}. && \text{(22d)}\end{aligned}$$

Here Y^n_2 is a random variable whose law is determined by the channel $P_{Y^n_1|X^n_{\hat{m}_p m_{12}} U^n_{m_{12}}} = W_1^{\otimes n}$. From the union bound follows that the average probability of decoding error is small if the probabilities of all these error events are small.

In more detail, the first two events regard the decoding of the individual message m_2 at node 1 given its own message m_1 as side information. For the probability of the first error event (22a) we have

$$\begin{aligned}&\mathbb{P}\{\mathcal{E}^{(1)}_{m_2|m_1}\}\\ &\quad = \mathbb{E}\big[W_1^{\otimes n}\big((\mathcal{D}'_{m_2|m_1}(U^n_{m_{12}}))^c | X^n_{m_p m_{12}}\big)\big]\\ &\quad \leq \sum_{u^n \in \mathcal{T}^n_{U,\delta}} \sum_{x^n \in \mathcal{T}^n_{X|U,\delta}(u^n)} W_1^{\otimes n}\big((\mathcal{D}'_{m_2|m_1}(u^n))^c | x^n\big)\\ &\qquad \times P'_{X^n|U^n}(x^n|u^n) P'_{U^n}(u^n)\\ &\quad \leq \sum_{u^n \in \mathcal{T}^n_{U,\delta}} \sum_{x^n \in \mathcal{X}^n} W_1^{\otimes n}\big((\mathcal{D}'_{m_2|m_1}(u^n))^c | x^n\big)\\ &\qquad \times \frac{P^{\otimes n}_{X|U}(x^n|u^n)}{P^{\otimes n}_{X|U}(\mathcal{T}^n_{X|U,\delta}(u^n)|u^n)} P'_{U^n}(u^n)\\ &\quad \leq \frac{1}{1-(n+1)^{|\mathcal{U}||\mathcal{X}|}2^{-nc\delta^2}}\\ &\qquad \times \sum_{u^n \in \mathcal{U}^n} P^{\otimes n}_{Y_1|U}\big((\mathcal{D}'_{m_2|m_1}(u^n))^c | u^n\big) P'_{U^n}(u^n)\\ &\quad \leq \frac{1}{1-(n+1)^{|\mathcal{U}||\mathcal{X}|}2^{-nc\delta^2}}\\ &\qquad \times \mathbb{E}\big[P^{\otimes n}_{Y_1|U}\big((\mathcal{D}'_{m_2|m_1}(U^n_{m_{12}}))^c | U^n_{m_{12}}\big)\big]\\ &\quad \leq \frac{(n+1)^{|\mathcal{U}||\mathcal{Y}_1|}2^{-nc\delta^2}}{1-(n+1)^{|\mathcal{U}||\mathcal{X}|}2^{-nc\delta^2}}\\ &\quad \leq 2^{-n\gamma} && \text{(23)}\end{aligned}$$

for some constant $c > 0$, where the third step follows from (9) and the fourth and sixth step from $P^{\otimes n}_{X|U}(\mathcal{T}^n_{X|U,\delta}(u^n)|u^n) \geq 1-(n+1)^{|\mathcal{U}||\mathcal{X}|}2^{-nc\delta^2}$, cf. for example [49, Lemma 2] or [50, Lemma III.1.3]. The last inequality holds for some $\gamma > 0$ for sufficiently large n.

Similarly, we get for the probability of the second event (22b)

$$\begin{aligned}&\mathbb{P}\{\mathcal{E}^{(2)}_{m_2|m_1}\}\\ &\quad \leq M_{2,n}\, \mathbb{P}\big\{(U^n_{m_1\hat{m}_2}, Y^n_1) \in \mathcal{T}^n_{UY_1,\delta}\big\}\\ &\quad = M_{2,n}\, \mathbb{E}\big[W_1^{\otimes n}\big(\mathcal{D}_{\hat{m}_2|m_1}(U^n_{m_1\hat{m}_2}) | X^n_{m_p m_{12}}\big)\big]\\ &\quad \leq M_{2,n} \sum_{x^n \in \mathcal{X}^n} \sum_{u^n, \hat{u}^n \in \mathcal{U}^n} W_1^{\otimes n}\big(\mathcal{D}_{\hat{m}_2|m_1}(\hat{u}^n) | x^n\big)\\ &\qquad \times \frac{P^{\otimes n}_{X|U}(x^n|u^n)}{P^{\otimes n}_{X|U}(\mathcal{T}^n_{X|U,\delta}(u^n)|u^n)} \frac{P^{\otimes n}_{U}(u^n)}{P^{\otimes n}_{U}(\mathcal{T}^n_{U,\delta})} P'_{U^n}(\hat{u}^n)\\ &\quad \leq M_{2,n} \frac{1}{(1-(n+1)^{|\mathcal{U}||\mathcal{X}|}2^{-nc\delta^2})^2}\\ &\qquad \times \mathbb{E}\big[P^{\otimes n}_{Y_1}\big(\mathcal{D}_{\hat{m}_2|m_1}(U^n_{m_1\hat{m}_2})\big)\big]\\ &\quad \leq \frac{1}{(1-(n+1)^{|\mathcal{U}||\mathcal{X}|}2^{-nc\delta^2})^2}\\ &\qquad \times 2^{n(I(U;Y_1)-\tau/2)} 2^{-n(I(U;Y_1)-f(\delta))}\\ &\quad = \frac{1}{(1-(n+1)^{|\mathcal{U}||\mathcal{X}|}2^{-nc\delta^2})^2} 2^{-n(\tau/2-f(\delta))}\\ &\quad \leq 2^{-n\gamma} && \text{(24)}\end{aligned}$$

where the first step comes from the union bound, the third step from (8) and (9), the fourth step from [49, Lemma 2] or [50, Lemma III.1.3], and the fifth step from the size of $\mathcal{M}_2$ and [49, Lemma 3] with $f(\delta) \to 0$ as $\delta \to 0$. Again, the last inequality holds for n large enough and δ small enough such that $\tau/2 > f(\delta)$.

The third and fourth events deal with the decoding of the additional private message m_p at receiving node 1. The key idea in the following is to interpret the channel $W_1 : \mathcal{X} \to \mathcal{P}(\mathcal{Y}_1)$ as a channel $W_1 : \mathcal{U} \times \mathcal{X} \to \mathcal{P}(\mathcal{Y}_1)$ with inputs in $\mathcal{X} \times \mathcal{U}$ where the $\mathcal{U}$-inputs do not matter. Then we get for error event (22c)

$$\begin{aligned}&\mathbb{P}\{\mathcal{E}^{(3)}_{m_p|m_{12}}\}\\ &\quad = \mathbb{E}\big[W_1^{\otimes n}\big((\mathcal{D}'_{m_p|m_{12}}(X^n_{m_p m_{12}}, U^n_{m_{12}}))^c | X^n_{m_p m_{12}}, U^n_{m_{12}}\big)\big]\\ &\quad \leq (n+1)^{|\mathcal{U}||\mathcal{X}||\mathcal{Y}_1|}2^{-nc\delta^2}\\ &\quad \leq 2^{-n\gamma} && \text{(25)}\end{aligned}$$

using the same argumentation as for the first error event (22a).

It remains to bound error event (22d) as follows

$$\begin{aligned}&\mathbb{P}\{\mathcal{E}^{(4)}_{m_p|m_{12}}\}\\ &\quad \leq M_{p,n}\, \mathbb{P}\big\{(U^n_{m_{12}}, X^n_{\hat{m}_p m_{12}}, Y^n_1) \in \mathcal{T}^n_{UXY_1,\delta}\big\}\\ &\quad = M_{p,n}\, \mathbb{E}\big[W_1^{\otimes n}\big(\mathcal{D}_{\hat{m}_p|m_{12}}(X^n_{\hat{m}_p m_{12}}, U^n_{m_{12}}) | X^n_{m_p m_{12}}, U^n_{m_{12}}\big)\big]\\ &\quad \leq M_{p,n} \frac{1}{1-(n+1)^{|\mathcal{U}||\mathcal{X}|}2^{-nc\delta^2}}\\ &\qquad \times \mathbb{E}\big[P^{\otimes n}_{Y_1|U}\big(\mathcal{D}_{\hat{m}_p|m_{12}}(X^n_{\hat{m}_p m_{12}}, U^n_{m_{12}}) | U^n_{m_{12}}\big)\big]\\ &\quad \leq \frac{1}{1-(n+1)^{|\mathcal{U}||\mathcal{X}|}2^{-nc\delta^2}}\\ &\qquad \times 2^{n(I(X;Y_1|U)-\tau/2)} 2^{-n(I(X;Y_1|U)-f'(\delta))}\\ &\quad = \frac{1}{1-(n+1)^{|\mathcal{U}||\mathcal{X}|}2^{-nc\delta^2}} 2^{-n(\tau/2-f'(\delta))}\\ &\quad \leq 2^{-n\gamma} && \text{(26)}\end{aligned}$$

where the first step comes from the union bound, the third step from (9) and $P^{\otimes n}_{X|U}(\mathcal{T}^n_{X|U,\delta}(u^n)|u^n) \geq 1-(n+1)^{|\mathcal{U}||\mathcal{X}|}2^{-nc\delta^2}$, and the fourth step from the size of $\mathcal{M}_p$ and similarly as in [49, Lemma 3] with $f'(\delta) \to 0$ as $\delta \to 0$. Again, the last inequality holds fro n large enough and δ small enough such that $\tau/2 > f'(\delta)$.

The analysis of probability of error at receiving node 2 follows accordingly with the error events $\mathcal{E}^{(1)}_{m_1|m_2} := \{(U^n_{m_{12}}, Y^n_2) \notin \mathcal{T}^n_{UY_2,\delta}\}$ and $\mathcal{E}^{(2)}_{m_1|m_2} := \{\exists\, \hat{m}_1 \neq m_1 :$

$(U^n_{m_1m_2}, Y_2^n) \in \mathcal{T}^n_{UY_2,\delta}\}$. Note that receiving node 2 only has to decode its intended individual message m_1 and is not interested in the additional private message m_p from the relay node. Thus, there is no need for further error events as given in (22c) –(22d).

From (23)–(26) and the corresponding expressions for receiving node 2, we conclude that the probabilities of decoding error, averaged over all codewords and codebooks, decreases exponentially fast for increasing block length n. Finally, from the random coding argument it follows that for n large enough there exists a codebook with desired rates (7) and required average probability of decoding errors proving the lemma. ■

Acknowledgment

The authors would like to thank Prof. H. Vincent Poor for bringing the problem of strong secrecy in bidirectional relay channels to their attention.

References

[1] Next Generation Mobile Networks: (R)evolution in Mobile Communications, Deutsche Telekom AG Laboratories, Technology Radar Edition III/2010, Feature Paper, 2010.

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.

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

[4] Y. Liang, H. V. Poor, and S. Shamai, "Information theoretic security," *Found. and Trends in Commun. and Inform. Theory*, vol. 5, no. 4–5, pp. 355–580, 2009.

[5] E. A. Jorswieck, A. Wolf, and S. Gerbracht, "Secrecy on the physical layer in wireless networks," *Trends Telecommun. Technol.*, pp. 413–435, Mar. 2010.

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

[7] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[8] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, "Compound wiretap channels," *EURASIP J. Wireless Commun. Netw.*, pp. 1–13, 2009, Article 142374.

[9] 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.

[10] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas-Part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[11] 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.

[12] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "MIMO Gaussian broadcast channels with confidential and common messages," in *Proc. IEEE Int. Symp. Inf. Theory*, Austin, TX, Jun. 2010, pp. 2578–2582.

[13] E. Ekrem and S. Ulukus, "Gaussian MIMO broadcast channels with common and confidential messages," in *Proc. IEEE Int. Symp. Inf. Theory*, Austin, TX, Jun. 2010, pp. 2583–2587.

[14] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.

[15] 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.

[16] 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.

[17] Y. Liang, H. V. Poor, and L. Ying, "Secure communications over wireless broadcast networks: Stability and utility maximization," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 682–692, Sep. 2011.

[18] L. Lai, Y. Liang, and H. V. Poor, "A unified framework for key agreement over wireless fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 480–490, Apr. 2012.

[19] U. M. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Proc. EUROCRYPT 2000, Lecture Notes in Computer Science*, May 2000, vol. 1807, pp. 351–368, Springer-Verlag.

[20] I. Bjelakovic, H. Boche, and J. Sommerfeld, "Capacity results for compound wiretap channels," in *Proc. IEEE Inf. Theory Workshop*, Paraty, Brazil, Oct. 2011, pp. 60–64.

[21] I. Bjelakovic, H. Boche, and J. Sommerfeld, "Secrecy results for compound wiretap channels," in *Proc. Probl. Inf. Transmission*, 2012 [Online]. Available: http://arxiv.org/abs/1106.2013

[22] I. Csiszár, "Almost independence and secrecy capacity," *Probl. Pered. Inform.*, vol. 32, no. 1, pp. 48–57, 1996.

[23] J. Barros and M. Bloch, "Strong secrecy for wireless channels," in *Proc. Int. Conf. Inform.-Theoretic Security*, Calgary, Canada, Aug. 2008, pp. 40–53.

[24] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 44–55, Jan. 2005.

[25] A. J. Pierrot and M. R. Bloch, "Strongly secure communications over the two-way wiretap channel," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 595–605, Sep. 2011.

[26] M. R. Bloch and J. N. Laneman, "Secrecy from resolvability," in *Proc. IEEE Trans. Inf. Theory* [Online]. Available: http://arxiv.org/abs/1105.5419

[27] 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.

[28] 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.

[29] T. J. Oechtering, C. Schnurr, I. Bjelakovic, and H. Boche, "Broadcast capacity region of two-phase bidirectional relaying," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 454–458, Jan. 2008.

[30] 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.

[31] G. Kramer and S. Shamai, "Capacity for classes of broadcast channels with receiver side information," in *Proc. IEEE Inf. Theory Workshop*, Tahoe City, CA, Sep. 2007, pp. 313–318.

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

[33] 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.

[34] C. Schnurr, T. J. Oechtering, and S. Stanczak, "Achievable rates for the restricted half-duplex two-way relay channel," in *Proc. Asilomar Conf. Signals, Systems, Comput.*, Pacific Grove, CA, Nov. 2007, pp. 1468–1472.

[35] D. Gündüz, E. Tuncel, and J. Nayak, "Rate regions for the separated two-way relay channel," in *Proc. Allerton Conf. Commun., Control, Computing*, Urbana-Champaign, IL, Sep. 2008, pp. 1333–1340.

[36] P. Zhong and M. Vu, "Compress-forward without Wyner-Ziv binning for the one-way and two-way relay channels," in *Proc. Allerton Conf. Commun., Control, Computing*, Urbana-Champaign, IL, Sep. 2011, pp. 426–433.

[37] L. Ong, C. M. Kellett, and S. J. Johnson, "Functional-decode-forward for the general discrete memoryless two-way relay channel," in *Proc. IEEE Int. Conf. Commun. Systems*, Singapore, Nov. 2010, pp. 351–355.

[38] M. P. Wilson, K. Narayanan, H. D. Pfister, and A. Sprintson, "Joint physical layer coding and network coding for bidirectional relaying," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5641–5654, Nov. 2010.

[39] W. Nam, S.-Y. Chung, and Y. H. Lee, "Capacity of the Gaussian two-way relay channel to within $1/2$ bit," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5488–5494, Nov. 2010.

[40] B. Nazer and M. Gastpar, "Compute-and-Forward: Harnessing interference through structured codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6463–6486, Oct. 2011.

[41] Y. Song and N. Devroye, "A lattice compress-and-Forward scheme," in *Proc. IEEE Inf. Theory Workshop*, Paraty, Brasil, Oct. 2011, pp. 110–114.

[42] S. H. Lim, Y.-H. Kim, A. El Gamal, and S.-Y. Chung, "Layered noisy network coding," in *Proc. IEEE Wireless Network Coding Conf.*, Boston, MA, Jun. 2010, pp. 1–6.

[43] S. H. Lim, Y.-H. Kim, A. El Gamal, and S.-Y. Chung, "Noisy network coding," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3132–3152, May 2011.

[44] G. Kramer and J. Hou, "On message lengths for noisy network coding," in *Proc. IEEE Inf. Theory Workshop*, Paraty, Brasil, Oct. 2011, pp. 430–431.

[45] P. Brémoud, *Markov Chains: Gibbs Fields, Monte Carlo Simulation, and Queues*. New York: Springer, 1999.

[46] M. S. Pinsker, *Information and Information Stability of Random Variables and Processes*. San Francisco, CA: Holden-Day, 1964.

[47] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[48] R. F. Wyrembelski and H. Boche, "How to achieve privacy in bidirectional relay networks," in *Proc. IEEE Int. Symp. Inf. Theory*, Saint Petersburg, Russia, Jul. 2011, pp. 1891–1895.

[49] R. F. Wyrembelski, I. Bjelakovic, 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.

[50] P. C. Shields, *The Ergodic Theory of Discrete Sample Paths*. Rhode Island: Amer. Math. Soc., 1996.

[51] 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.

[52] R. F. Wyrembelski and H. Boche, "Bidirectional broadcast channels with common and confidential messages," in *Proc. IEEE Inf. Theory Workshop*, Paraty, Brazil, Oct. 2011, pp. 713–717.

Rafael F. Wyrembelski (S'08–M'12) 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 Postdoctoral researcher.

Moritz Wiese (S'09) received the Dipl.-Math. degree in mathematics from the University of Bonn, Germany, in 2007. He has been working toward the Ph.D. degree since then.

From 2007 to 2010, he was a research assistant at the Heinrich-Hertz-Lehrstuhl für Mobilkommunikation, Technische Universität Berlin, Germany. Since 2010, he is a research and teaching assistant at the Lehrstuhl für Theoretische Informationstechnik, Technische Universität München, Munich, Germany.

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 Laboratory 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 corecipient of the 2006 IEEE Signal Processing Society Best Paper Award and recipient of the 2007 IEEE Signal Processing Society Best Paper Award.