Cooperative Broadcast Channels with a Secret Message

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

Gerhard Kramer
Technische Universität München
gerhard.kramer@tum.de

Haim H. Permuter
Ben Gurion University of the Negev
haimp@bgu.ac.il

***Abstract*—The broadcast channel (BC) with one confidential message and where the decoders cooperate via a one-sided link is considered. A pair of messages is transmitted, one message for each user. The message to the cooperative user is confidential and is kept secret from the cooperation-aided user. The secrecy level is measured by the equivocation rate. An inner bound on the secrecy-capacity region of the BC is derived. The inner bound is achieved by *double-binning* the codebook of the secret message. The inner bound is tight for the semi-deterministic (SD) and physically degraded (PD) cases. The secrecy results are compared to those of the corresponding BCs without a secrecy constraint. A cooperative Blackwell channel example illustrates the impact of secrecy on the rate regions.**

I. Introduction

User cooperation and security are two essential aspects of modern communication systems. Cooperation between nodes potentially increases the transmission rates, whereas confidential transmissions might limit these rates. To shed light on the interaction between these two phenomena, we study broadcast channels (BCs) with one-sided decoder cooperation and one confidential message (Fig. 1). Cooperation is modeled as *conferencing*, i.e., information exchange via a rate-limited link that extends from one receiver (referred to as the *cooperative receiver*) to the other (the *cooperation-aided receiver*). The cooperative receiver possesses confidential information, which should be kept secret from the other user. Thus, the cooperative receiver helps the other user while keeping its own message secret. We derive an inner bound on the secrecy-capacity region of this BC, which we show is tight for semi-deterministic (SD) and physically degraded (PD) scenarios.

A. Brief History

Information theoretic secrecy was introduced by Shannon in his seminal work [1], where he studied communication between a source and a receiver in the presence of an eavesdropper. Later, Wyner modeled secret communication over noisy channels when he introduced the degraded wiretap channel and derived its secrecy-capacity region [2]. Csiszár and Köner [3] extended Wyner's result to a general BC in which the source also transmits a common message to both users. The development of wireless communication, whose inherent open nature makes it vulnerable to security attacks, has inspired a growing interest in understanding the fundamental limits of secure communication [4]–[12].

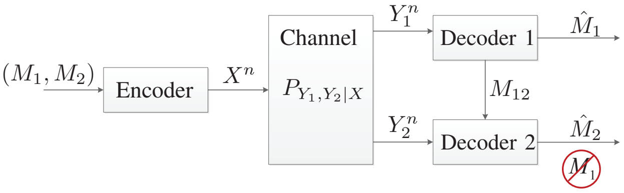


Fig. 1. SD-BC with cooperation and one confidential message.

BC settings combining secrecy and cooperation were considered in [13], where the authors derive inner and outer bounds on the rate-equivocation region of the relay-BC (RBC) with one or two confidential messages. The inner bound in [13] recovers past results without cooperation, e.g., [2] and [3], however it remains unclear whether it is tight for cooperative settings.

B. Contributions

We derive an inner bound on the secrecy-capacity region of the cooperative BC with one confidential message (Fig. 1), and show it is tight for SD and PD BCs. Our coding strategy relies on double-binning the codebook of the confidential message to allow joint encoding and preserve confidentiality. The cooperation link conveys information on a portion of the non-confidential message. The converses for the SD and PD cases are established by using telescoping identities [14].

Comparing our coding scheme to the one for the BC with conferencing but without secrecy [15] reveals two main differences. The first is a randomizer that introduces an additional layer of binning and, in turn, ensures secrecy. Second, our cooperation protocol is based on a public message that is assembled from the non-confidential message only. Without secrecy constraints, the public message comprises parts of both messages. This difference is fundamental since when coding for the BC with secrecy, a cooperation protocol that shares information about the confidential message violates the secrecy constraint. The effect of secrecy is further studied by considering the cooperative PD-BC and the SD-BC without cooperation. A Blackwell channel example illustrates the results. Comparing the regions to the ones without secrecy reveals that, although a confidential message shrinks the region, if the confidential message rate is below a certain threshold, there is no rate-loss.

978-1-4673-7704-1/15/$31.00 ©2015 IEEE

II. Problem Definition

We use the following notations. Given two numbers $a, b \in \mathbb{R}$, let $[a:b]$ be the set of integers $\{n \in \mathbb{N} \big| \lceil a \rceil \leq n \leq \lfloor b \rfloor\}$. We define $\mathbb{R}_+ = \{x \in \mathbb{R} | x \geq 0\}$. The other notations are standard and are as in [16], see also Section II of [15].

The BC with cooperation and one confidential message is illustrated in Fig. 1. The sender chooses a pair (m_1, m_2) of indices uniformly and independently from the set $[1:2^{nR_1}] \times [1:2^{nR_2}]$ and maps them to a sequence $\mathbf{x} \in \mathcal{X}^n$, which is the channel input. The sequence $\mathbf{x}$ is transmitted over a BC with transition probability $P_{Y_1,Y_2|X}$. If the channel transition matrix factors as $\mathbb{1}_{\{Y_1=f(X)\}} P_{Y_2|X}$ or $P_{Y_1|X} P_{Y_2|Y_1}$ we call the BC SD or PD, respectively. The output sequence $\mathbf{y}_j \in \mathcal{Y}_j^n$, where $j = 1, 2$, is received by decoder j. Decoder j produces an estimate of m_j, which is denoted by $\hat{m}_j$. Furthermore, the message m_1 is to be kept secret from Decoder 2. There is a one-sided noiseless cooperation link of rate R_{12} from Decoder 1 to Decoder 2. By conveying a message $m_{12} \in [1:2^{nR_{12}}]$ over this link, Decoder 1 can share with Decoder 2 information about $\mathbf{y}_1$, $\hat{m}_1$, or both.

Definition 1 (Code Description): A $(n, 2^{nR_{12}}, 2^{nR_1}, 2^{nR_2})$ code for the BC cooperation and one confidential message has:

1) Three message sets $\mathcal{M}_{12} = [1:2^{nR_{12}}]$, $\mathcal{M}_1 = [1:2^{nR_1}]$ and $\mathcal{M}_2 = [1:2^{nR_2}]$.
2) A stochastic encoder that is described by a matrix of conditional PMFs $P_{X^n|M_1,M_2}$.
3) A decoder cooperation function $\phi_{12} : \mathcal{Y}_1^n \to \mathcal{M}_{12}$.
4) Two decoding functions $\psi_1 : \mathcal{Y}_1^n \to \mathcal{M}_1$ and $\psi_2 : \mathcal{Y}_2^n \times \mathcal{M}_{12} \to \mathcal{M}_2$.

Definition 2 (Error Probability): The average error probability for a $(n, 2^{nR_{12}}, 2^{nR_1}, 2^{nR_2})$ code is $P_e = \mathbb{P}\big((\hat{M}_1, \hat{M}_2) \neq (M_1, M_2)\big)$, where $\hat{M}_1 = \psi_1(Y_1^n)$ and $\hat{M}_2 = \psi_2(Y_2^n, M_{12})$.

The secrecy level at receivers 2 is measured with respect to the equivocation rate $\frac{1}{n} H(M_1 | M_{12}, Y_2^n)$.

Definition 3 (Achievable Rates): A rate triple (R_{12}, R_1, R_2) is *achievable* if for any $\epsilon, \xi > 0$ there is a sufficiently large $n \in \mathbb{N}$ and a $(n, 2^{nR_{12}}, 2^{nR_1}, 2^{nR_2})$ code such that $P_e \leq \epsilon$ and $nR_1 - H(M_1|M_{12}, Y_2^n) \leq n\xi$.

The *secrecy-capacity region* $\mathcal{C}$ is the closure of the set of achievable rates.

A. Main Results

We state an inner bound on the secrecy-capacity region of a BC with cooperation and one confidential message (Fig. 1).

Theorem 1 (General Inner Bound): Let $\mathcal{R}_I$ be the union of rate triples $(R_{12}, R_1, R_2) \in \mathbb{R}_+^3$ satisfying:

$$R_1 \leq I(U_1; Y_1|V) - I(U_1; U_2|V) - I(U_1; Y_2|V, U_2) \tag{1a}$$

$$R_2 \leq I(V, U_2; Y_2) + R_{12} \tag{1b}$$

$$R_1 + R_2 \leq I(V, U_1; Y_1) - I(U_1; U_2|V) - I(U_1; Y_2|V, U_2) + I(U_2; Y_2|V) \tag{1c}$$

where the union is over all probability mass functions (PMFs) $P_{V,U_1,U_2,X} P_{Y_1,Y_2|X}$ where V, U_1 and U_2 are auxiliary random variables with bounded cardinalities. The following inclusion holds:

$$\mathcal{R}_I \subseteq \mathcal{C}. \tag{2}$$

The proof of Theorem 1 is relegated to Appendix A. The inner bound in Theorem 1 is tight for SD- and PD-BCs, as stated in the following theorems.

Theorem 2 (Secrecy-Capacity Region of the SD-BC): The secrecy-capacity region $\mathcal{C}_{SD}$ of the SD-BC with cooperation and one confidential message is the union of rate triples $(R_{12}, R_1, R_2) \in \mathbb{R}_+^3$ satisfying:

$$R_1 \leq H(Y_1|V, U, Y_2) \tag{3a}$$

$$R_2 \leq I(V, U; Y_2) + R_{12} \tag{3b}$$

$$R_1 + R_2 \leq H(Y_1|V, U, Y_2) + I(U; Y_2|V) + I(V; Y_1) \tag{3c}$$

where the union is over all PMFs $P_{V,U,Y_1,X} P_{Y_2|X} \mathbb{1}_{\{Y_1=f(X)\}}$. Moreover, V and U are auxiliary random variables with bounded cardinalities.

For the achievability of Theorem 2 we set $U_1 = Y_1$ and relabel $U_2 = U$ in Theorem 1. A converse follows by setting $V_i \triangleq (M_{12}, Y_1^{i-1}, Y_{2,i+1}^n)$ and $U_i \triangleq M_2$. The Markov relation $(V, U) - X - (Y_1, Y_2)$ is shown to hold by using functional dependence graphs (FDGs) and the notion of d-separation [17]. Details are omitted due to lack of space.

Theorem 3 (Secrecy-Capacity Region of the PD-BC): The secrecy-capacity region $\mathcal{C}_{PD}$ of the PD-BC with cooperation and one confidential message is the union of rate triples $(R_{12}, R_1, R_2) \in \mathbb{R}_+^3$ satisfying:

$$R_1 \leq I(U; Y_1|V) - I(U; Y_2|V) \tag{4a}$$

$$R_2 \leq I(V; Y_2) + R_{12} \tag{4b}$$

$$R_1 + R_2 \leq I(U; Y_1) - I(U; Y_2|V) \tag{4c}$$

where the union is over all PMFs $P_{V,U} P_{X|U} P_{Y_1|X} P_{Y_2|Y_1}$. Moreover, V and U are auxiliary random variables with bounded cardinalities.

The direct part of Theorem 3 follows by setting $U_1 = U$ and $U_2 = 0$ in Theorem 1 and reducing the domain over which the union is taken to encompass only PMFs where $V - U - X$ form a Markov chain. For the converse, which is omitted due to space limitations, we take $V_i \triangleq (M_2, Y_1^{i-1}, Y_{2,i+1}^n)$ and $U_i \triangleq (M_1, V_i)$. This choice results in the Markov relation $V_i - U_i - X_i - Y_{1,i} - Y_{2,i}$ that holds for every $i \in [1:n]$, and therefore it also holds in its single-letter form.

III. Effect of Secrecy Constraints on Coding Schemes and Rate Regions

What is the impact of a confidential message on the best coding scheme and, consequently, on the capacity region of different classes of BCs? To help answer this question, we compare the SD and PD versions of the BC to their corresponding models without secrecy.

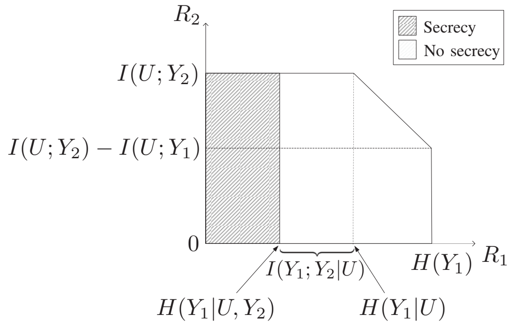


Fig. 2. SD-BC without cooperation: Capacity region without secrecy constraints vs. secrecy-capacity region where M_1 is confidential.

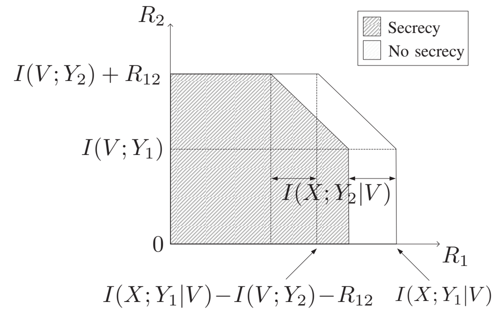


Fig. 3. PD-BC with cooperation: capacity region without secrecy constraints vs. secrecy-capacity region where M_1 is confidential.

A. SD-BCs

Consider the SD-BC without cooperation in which M_1 is secret. Although the non-cooperative channel is easier to compare, the impact of secrecy on the cooperative model is similar. Using Theorem 2, we establish the secrecy-capacity region of the SD-BC with one confidential message.

Corollary 4 (Secrecy-Capacity Region of the SD-BC without Cooperation): The secrecy-capacity region $\mathcal{C}_{SD}^{\star}$ of the SD-BC with one confidential message is the union of rate pairs $(R_1,R_2)\in\mathbb{R}_+^2$ satisfying:

$$R_1 \le H(Y_1|U,Y_2) \tag{5a}$$

$$R_2 \le I(U;Y_2) \tag{5b}$$

where the union is over all PMFs $P_{U,Y_1,X}P_{Y_2|X}\mathbb{1}_{\{Y_1=f(X)\}}$ and U is and auxiliary random variables with bounded cardinality.

Marton coding [18] achieves the capacity region of the classic SD-BC [19]. The capacity is the union of rate pairs $(R_1,R_2)\in\mathbb{R}_+^2$ satisfying:

$$R_1 \le H(Y_1) \tag{6a}$$

$$R_2 \le I(U;Y_2) \tag{6b}$$

$$R_1+R_2 \le H(Y_1|U)+I(U;Y_2) \tag{6c}$$

where the union is over the same domain as in Corollary 4.

The regions in (5) and (6) (for a fixed PMF) are depicted in Fig. 2. When M_1 is secret, one can no longer operate on both corner points of Marton's region. Rather, the optimal coding scheme is the one with the lower transmission rate to User 1. An additional rate-loss of $I(Y_1;Y_2|U)$ in R_1 is caused by the extra layer of binning used to conceal M_1 from the 2nd user. A coding scheme for the higher corner point of the region without secrecy, i.e., to $\big(H(Y_1)\ ,\ I(U;Y_2)-I(U;Y_1)\big)$, is not feasible for the case with secrecy since the larger value of R_1 violates the secrecy constraint. A similar relation holds for the corresponding regions with cooperation.

B. PD-BCs

Consider next the PD-BC and its secrecy-capacity region stated in Theorem 3. A consequence of Theorem 3 is that the region described by the union over all $P_{U,X}P_{Y_1|X}P_{Y_2|Y_1}$ of rate triples $(R_{12},R_1,R_2)\in\mathbb{R}_+^3$ satisfying:

$$R_1 \le I(X;Y_1|V)-I(X;Y_2|V) \tag{7a}$$

$$R_2 \le I(V;Y_2)+R_{12} \tag{7b}$$

$$R_1+R_2 \le I(X;Y_1)-I(X;Y_2|V) \tag{7c}$$

is achievable. Henceforth, we consider the region in (7), which we denote by $\mathcal{R}_{PD}^{I}$, to compare to the setting without secrecy. Note that by prefixing a channel $P_{X|U}$, the region $\mathcal{R}_{PD}^{I}$ is expanded to exhaust the secrecy-capacity region $\mathcal{C}_{PD}$. Keeping this in mind, $\mathcal{R}_{PD}^{I}$ suffices for the subsequent discussion.

The capacity region $\mathcal{C}_{PD}^{\star}$ of the corresponding channel without a secrecy constraint on M_1 (see [20] and [21]) is the union over the same domain as (7) of rate triples $(R_{12},R_1,R_2)\in\mathbb{R}_+^3$ satisfying:

$$R_1 \le I(X;Y_1|V) \tag{8a}$$

$$R_2 \le I(V;Y_2)+R_{12} \tag{8b}$$

$$R_1+R_2 \le I(X;Y_1). \tag{8c}$$

In contrast to the SD case, the only impact of a secrecy constraint on M_1 on the rate region is expressed in a rate-loss of $I(X;Y_2|V)$ in R_1. Thus, for a fixed $P_{U,X}P_{Y_1|X}P_{Y_2|Y_1}$, if $(R_{12},R_1,R_2)\in\mathcal{C}_{PD}^{\star}$ then $\Big(R_{12},\big(R_1-I(X;Y_2|V)\big)^+,R_2\Big)\in\mathcal{C}_{PD}$, and vice versa, where $(x)^+=\max(0,x)$. This relation is illustrated in Fig. 3 for some fixed value of R_{12} and under the assumption that $I(V;Y_2)+R_{12}>I(V;Y_1)$. The code construction for both problems is the same up to the use of a randomizer for secrecy. The reason for this similarity is that, whether M_1 is secret or not, its codebook is superposed on the codebook of M_2. The cooperation protocol in both cases conveys part of M_2 from Decoder 1 (which is able to decode M_2 without cost due the degraded property of the channel) to Decoder 2. Thus, introducing a secrecy constraint on M_1 results in an additional layer of binning of its codewords, while the codebook of M_2 and the cooperation protocol remain unaffected.

IV. Blackwell Channel Example

Consider the Blackwell channel [22], [23] illustrated in Fig 4. Using Theorem 2 we derive the secrecy-capacity region and

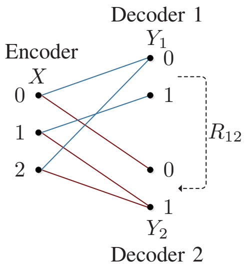
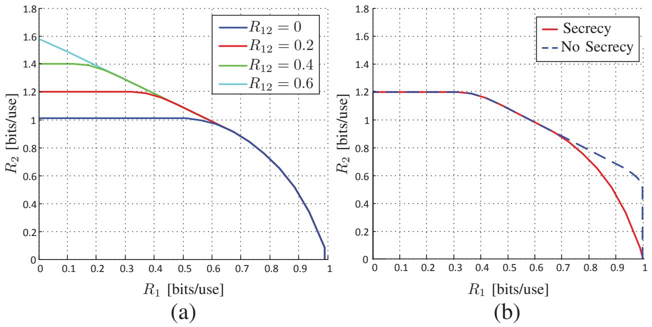


Fig. 4. Blackwell channel with cooperation and one confidential message.



(a) (b)

Fig. 5. (a) Projection of the secrecy-capacity region of the Blackwell channel onto the plane (R_1, R_2) for different R_{12} values; (b) For $R_{12} = 0.2$: secrecy-capacity region where M_1 is secret vs. capacity region without secrecy

parameterize the input PMF P_X as $P_X(0) = \alpha$, $P_X(1) = \beta$ and $P_X(2) = 1 - \alpha - \beta$ (where $\alpha, \beta \in \mathbb{R}_+$ and $\alpha + \beta \leq 1$) to obtain capacity region:

$$\mathcal{C}_{\text{BW}} = \bigcup_{\substack{\alpha,\beta\in\mathbb{R}_+,\\ \alpha+\beta\leq 1}} \left\{ \begin{array}{l} R_1 \leq (1-\alpha) H_b\left(\frac{\beta}{1-\alpha}\right) \\ R_2 \leq H_b(\alpha) + R_{12} \\ R_1 + R_2 \leq H_b(\alpha) + (1-\alpha) H_b(\frac{\beta}{1-\alpha}) \end{array} \right\}. \tag{9}$$

The projection of $\mathcal{C}_{\text{BW}}$ onto the plane (R_1, R_2) for different values of R_{12} is depicted in Fig. 5(a).

For every fixed value of $R_{12} \in \mathbb{R}_+$, the maximal R_1 in $\mathcal{C}_{\text{BW}}$ is 1 [bits/use]. This can be obtained from the rate bounds in (9) by setting $\alpha = 0$ and $\beta = \frac{1}{2}$, which implies that $(R_{12}, 1, 0)$ is achievable for every $R_{12} \in \mathbb{R}_+$. The corresponding coding strategy has the encoder choose each channel input symbol uniformly from the set $\{1, 2\} \subset \mathcal{X}$. Doing so lets Decoder 1 effectively see a clean binary channel (by mapping every received $Y_1 = 0$ to the input symbol $X = 2$) with capacity 1. Decoder 2, on the other hand, sees a zero-capacity channel since both $X = 1$ and $X = 2$ are mapped to $Y_2 = 1$. Thus, Decoder 2 has no information on the transmitted sequence (and secrecy is achieved) while one bit is conveyed securely to Decoder 1 in each channel use.

To compare $\mathcal{C}_{BW}$ to the region without secrecy, we once again parameterize the input distribution P_X as before and plug it into the result from [15, Corollary 13], which states the capacity region of the DBC with one-sided decoder cooperation. The capacity region of the Blackwell channel without secrecy is (see also [24, Eq. (26) and Fig. 6]):

$$\mathcal{C}^{\star}_{\text{BW}} = \bigcup_{\substack{\alpha,\beta\in\mathbb{R}_+,\\ \alpha+\beta\leq 1}} \left\{ \begin{array}{l} R_1 \leq H_b(\beta) \\ R_2 \leq H_b(\alpha) + R_{12} \\ R_1 + R_2 \leq H_b(\alpha) + (1-\alpha) H_b(\frac{\beta}{1-\alpha}) \end{array} \right\}. \tag{10}$$

Fig. 5(b) shows the projection of the regions in (9) and (10) onto the plane (R_1, R_2) for $R_{12} = 0.2$. The dashed blue line represents the capacity region without secrecy while the red line depicts the region with secrecy.

The secrecy-capacity region where a confidential message is present is strictly smaller than the corresponding region without secrecy. However, as long as $R_1 \leq R_1^{(\text{Th})}$, where $R_1^{(\text{Th})} \approx 0.6597$, the secrecy of M_1 is achieved without rate loss in R_2. When $R_1 > R_1^{(\text{Th})}$, an increased rate of the confidential message is accompanied by a decreased value of R_2 as compared to when no secrecy is required. Considering the extreme point where $R_1 = 1$, we note that if M_1 is *not* confidential, then one can transmit M_1 at rate $R_1 = 1$ and still have a positive value of R_2 (up to approximately $R_2 \approx 0.5148$). When M_1 is confidential, however, $R_1 = 1$ is achievable only if $R_2 = 0$.

Acknowledgments

The work of Z. Goldfeld and H. H. Permuter was supported by the European Research Council (ERC) starting grant, ISF grant no. 684/11. The work of G. Kramer was supported by an Alexander von Humboldt Professorship endowed by the German Federal Ministry of Education and Research.

Appendix A
Proof of Theorem 1

Codebook Generation: Split M_2 into two independent parts (M_{20}, M_{22}) with rates R_{20} and R_{22}, that satisfy

$$R_2 = R_{20} + R_{22}, \tag{11}$$

and alphabets $\mathcal{M}_{20}$ and $\mathcal{M}_{22}$, respectively. M_{20} is referred to as a *public message* while M_{22} denotes *private message number 2*. Let W be a random variable uniformly distributed over $\mathcal{W} = [1 : 2^{n\tilde{R}}]$ and independent of (M_1, M_2).

Generate a public message codebook $\mathcal{C}_V$ that comprises $2^{R_{20}}$ v-codewords $\mathbf{v}(m_{20})$, $m_{20} \in \mathcal{M}_{20}$, drawn according to P_V^n. Randomly and uniformly partition $\mathcal{C}_V$ into $2^{nR_{12}}$ bins $\mathcal{B}(m_{12})$, where $m_{12} \in \mathcal{M}_{12}$.

For each $\mathbf{v}(m_{20}) \in \mathcal{C}_V$, generate a codebook $C_{U_1}(m_{20})$ that comprises $2^{n(R_1+R_1'+\tilde{R})}$ codewords $\mathbf{u}_1$, each drawn according to $P^n_{U_1|V}\big(\cdot\,\big|v_i(m_{20})\big)$ independent of all the other u_1-codewords. Label these codewords $\mathbf{u}_1(m_{20}, m_1, i, w)$, where $(m_1, i, w) \in \mathcal{M}_1 \times [1 : 2^{nR_1'}] \times \mathcal{W}$.

For each $\mathbf{v}(m_{20}) \in \mathcal{C}_V$ also generate a codebook $C_{U_2}(m_{20})$ that comprises $2^{nR_{22}}$ u_2-codewords, each associated with a private message $m_{22} \in \mathcal{M}_{22}$. Each u_2-codeword in $C_{U_2}(m_{20})$

is drawn according to $P^n_{U_2|V}\big(\cdot\,\big|v_i(m_{20})\big)$ independent of the other u_2-codewords.

Encoding: To transmit the message pair $(m_1, m_2) = \big(m_1,(m_{20},m_{22})\big)$, the encoder chooses w uniformly from $\mathcal{W}$ and searches for an index $i \in [1 : 2^{nR'_1}]$ such that $\Big(\mathbf{v}(m_{20}), \mathbf{u}_1(m_{20}, m_1, i, w), \mathbf{u}_2(m_{20}, m_{22})\Big)$ are jointly typical with respect to P_{V,U_1,U_2}. The channel input sequence $\mathbf{x}$ is then randomly generated symbol-by-symbol according to $P_{X|V,U_1,U_2}$ and is transmitted over the channel.

Decoding and Cooperation Process: *Decoder 1:* Searches for a unique triple $(\hat{m}_{20}, \hat{m}_1, \hat{w}) \in \mathcal{M}_{20} \times \mathcal{M}_1 \times \mathcal{W}$ for which there is an index $\hat{i} \in [1 : 2^{nR'_1}]$ such that $\Big(\mathbf{v}(\hat{m}_{20}), \mathbf{u}_1(\hat{m}_{20}, \hat{m}_1, \hat{i}, \hat{w}), \mathbf{y}_1\Big)$ are in $\mathcal{T}_\epsilon^{(n)}(P_{V,U_1,Y_1})$. Upon finding such unique triple, $\hat{m}_1$ is declared as the decoded message; otherwise, an error is declared.
Cooperation: Having $(\hat{m}_{20}, \hat{m}_1, \hat{i}, \hat{w})$, Decoder 1 conveys the bin number of $\mathbf{v}(\hat{m}_{20})$ to Decoder 2 via the cooperation link.
Decoder 2: Upon receiving $(\hat{m}_{12}, \mathbf{y}_2)$, Decoder 2 searches for a unique pair $(\hat{\hat{m}}_{20}, \hat{\hat{m}}_{22}) \in \mathcal{M}_{20} \times \mathcal{M}_{22}$ such that $\Big(\mathbf{v}(\hat{\hat{m}}_{20}), \mathbf{u}_2(\hat{\hat{m}}_{20}, \hat{\hat{m}}_{22}), \mathbf{y}_2\Big)$ are in $\mathcal{T}_\epsilon^{(n)}(P_{V,U_2,Y_2})$, where $\mathbf{v}(\hat{\hat{m}}_{20}) \in \mathcal{B}(\widehat{m_{12}})$. If such a unique pair is found, then $\hat{\hat{m}}_2 \triangleq (\hat{\hat{m}}_{20}, \hat{\hat{m}}_{22})$ is declared as the decoded message; otherwise an error is declared.

By standard analysis, which we omit due to space limitations, reliability is achieved provided that

$$R'_1 > I(U_1; U_2|V) \tag{12a}$$

$$R_1 + R'_1 + \tilde{R} < I(U_1; Y_1|V) \tag{12b}$$

$$R_{20} + R_1 + R'_1 + \tilde{R} < I(V, U_1; Y_1) \tag{12c}$$

$$R_{22} < I(U_2; Y_2|V) \tag{12d}$$

$$R_2 - R_{12} < I(V, U_2; Y_2). \tag{12e}$$

Equivocation Analysis: We take $\tilde{R} = I(U_1; Y_2|V, U_2) - \epsilon'$, where $\epsilon' > 0$ is small for sufficiently large n, and show that the secrecy constraint is satisfied. Consider:

$$\begin{aligned}
&H(M_1|M_{12}, \mathbf{Y}_2) \overset{(a)}{\geq} H(M_1|\mathbf{V}, \mathbf{U}_2, \mathbf{Y}_2)\\
&= H(M_1, \mathbf{Y}_2|\mathbf{V}, \mathbf{U}_2) - H(\mathbf{Y}_2|\mathbf{V}, \mathbf{U}_2)\\
&\overset{(b)}{\geq} H(\mathbf{U}_1|\mathbf{V},\mathbf{U}_2) - H(\mathbf{U}_1|M_1,\mathbf{V},\mathbf{U}_2,\mathbf{Y}_2) - I(\mathbf{U}_1;\mathbf{Y}_2|\mathbf{V},\mathbf{U}_2)
\end{aligned} \tag{13}$$

where (a) follows because conditioning cannot increase entropy and because M_{12} is defined by $\mathbf{V}$, while (b) follows since $\mathbf{Y}_2 - (\mathbf{V}, \mathbf{U}_1, \mathbf{U}_2) - M_1$ forms a Markov chain (this can be shown using functional dependence graphs [17]). Following the approach devised in Lemmas 2 and 3 of [4], and by using the fact that for every $\mathbf{V} = \mathbf{v}$, $\mathbf{U}_1$ attains $2^{n(R_1+R'_1+\tilde{R})}$ possible realizations with equal probability, we find that $H(M_1|M_{12}, \mathbf{Y}_2) \geq nR_1 - n\epsilon'_\xi$, where ξ' can be made arbitrarily small with n. The proof is concluded by applying Fourier-Motzkin elimination on (12) while substituting $\tilde{R} = I(U_1; Y_2|V, U_2) - \epsilon'$ and using (11).

References

[1] C. E. Shannon. Communication theory of secrecy systems. *Bell Sys. Techn.*, 28(4):656715, Oct. 1949.

[2] A. D. Wyner. The wire-tap channel. *Bell Sys. Techn.*, 54(8):1355–1387, Oct. 1975.

[3] I. Csiszár and J. Körner. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 24(3):339–348, May 1978.

[4] R. Liu, I. Maric, P. Spasojević, and R. D. Yates. Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions. *IEEE Trans. Inf. Theory*, 54(6):2493–2507, Jun. 2008.

[5] Y. Zhao, P. Xu, Y. Zhao, W. Wei, and Y. Tang. Secret communications over semi-deterministic broadcast channels. In *Fourth Int. Conf. Commun. and Netw. in China (CHINACOM)*, Xi'an, China, Aug. 2009.

[6] W. Kang and N. Liu. The secrecy capacity of the semi-deterministic broadcast channel. In *Proc. Int. Symp. Inf. Theory*, Seoul, Korea, Jun.-Jul. 2009.

[7] R. Liu and H. Poor. Secrecy capacity region of a multiple-antenna Gaussian broadcast channel with confidential messages. *IEEE Trans. Inf. Theory*, 55(3):1235–1249, Mar. 2009.

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

[9] E. Ekrem and S. Ulukus. The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel. *IEEE Trans. Inf. Theory*, 57(4):2083–2114, Apr. 2011.

[10] E. Ekrem and S. Ulukus. Secrecy capacity of a class of broadcast channels with an eavesdropper. *EURASIP Journal on Wireless Commun. and Netw.*, 2009(1):1–29, Mar. 2009.

[11] G. Bagherikaram, A. Motahari, and A. Khandani. Secrecy capacity region of Gaussian broadcast channel. In *43rd Annual Conf. on Inf. Sci. and Sys. (CISS) 2009*, pages 152–157, Baltimore, MD, US, Mar. 2009.

[12] M. Benammar and P. Piantanida. Secrecy capacity region of some classes of wiretap broadcast channels. *Available on ArXiv*, Jul. 2014. http://arxiv.org/abs/1407.5572.

[13] E. Ekrem and S. Ulukus. Secrecy in cooperative relay broadcast channels. *IEEE Trans. Inf. Theory*, 57(1):137–155, Jan. 2011.

[14] G. Kramer. Teaching IT: An identity for the Gelfand-Pinsker converse. *IEEE Inf. Theory Society Newsletter*, 61(4):4–6, Dec. 2011.

[15] Z. Goldfeld, H. H. Permuter, and G. Kramer. Duality of a source coding problem and the semi-deterministic broadcast channel with rate-limited cooperation. *Submitted for publication to IEEE Trans. Inf. Theory*, 2014. Available on ArXiv at http://arxiv.org/abs/1405.7812.

[16] A. El Gamal and Y.-H. Kim. *Network Information Theory*. Cambridge University Press, 2011.

[17] G. Kramer. Capacity results for the discrete memoryless networks. *IEEE. Trans. Inf. Theory*, 49(1):4–21, Jan. 2003.

[18] K. Marton. A coding theorem for the discrete memoryless broadcast channel. *IEEE Trans. Inf. Theory*, 25(3):306–311, May 1979.

[19] S. I. Gelfand and M. S. Pinsker. Capacity of a broadcast channel with one deterministic component. *Prob. Pered. Inf. (Problems of Inf. Transm.)*, 16(1):17–25, Jan-Mar 1980.

[20] R. Dabora and S. D. Servetto. Broadcast channels with cooperating decoders. *IEEE Trans. Inf. Theory*, 52:5438–5454, 2006.

[21] L. Dikstein, H. H. Permuter, and Y. Steinberg. On state dependent broadcast channels with cooperation. *Submitted for publication to IEEE Trans. Inf. Theory*, 2014.

[22] E. C. van der Meulen. Random coding theorems for the general discrete memoryless broadcast channel. *IEEE Trans. Inf. Theory*, IT-21(2):180–190, May 1975.

[23] S. I. Gelfand. Capacity of one broadcast channel. *Probl. Peredachi Inf.*, 13(3):106108, Jul./Sep. 1977.

[24] Y. Liang and G. Kramer. Rate regions for relay broadcast channels. *IEEE Trans. Inf. Theory*, 53(10):3517–3535, Oct 2007.