# Capacity Region Continuity of the Compound Broadcast Channel with Confidential Messages

Andrea Grigorescu*, Holger Boche*, Rafael F. Schaefer† and H. Vincent Poor†

* Lehrstuhl für Theoretische Informationstechnik, Technische Universität München, 80333 München, Germany
† Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA

***Abstract*—The compound *broadcast channel with confidential messages* (BCC) generalizes the BCC by modeling the uncertainty of the channel. For the compound BCC, it is known only that the actual channel realization belongs to a pre-specified uncertainty set of channels and that it is constant during the entire transmission. For reliable and secure communication it is necessary to operate at a rate pair within the compound BCC *capacity region*. Therefore, the question of whether small variations of the uncertainty set lead to large losses of the compound BCC capacity region is of interest, and this problem is studied here. In particular, it is shown that the compound BCC model is robust, i.e., the capacity region depends *continuously* on the uncertainty set.**

## I. Introduction

Information theoretic security was initiated by Wyner in [1] introducing the wiretap channel, where the physical properties of the channel are used to guarantee security; see also [2] and [3]. Subsequently, Csiszár and Körner generalized the wiretap channel to the *broadcast channel with confidential messages* (BCC) [4] using the *weak secrecy* criterion.

For secure and reliable transmission over a wireless channel, channel state information (CSI) is needed; however, in practical systems it is not perfectly known. *Compound channels* model a simple and realistic CSI situation in which the legitimate users are not aware of the actual channel realization. Nevertheless, they know it belongs to a known uncertainty set of channels and that it remains constant during the entire transmission. This model applies, for example, to the downlink of a cellular system, in which the base station transmits information to a user. The base station obtains limited CSI, for example via the uplink from pilot signal estimation at the receiver. Compound channels model the channel uncertainty based on a finite number of estimates. *Arbitrarily varying channels* model an even more limited CSI assumption, in which it is assumed that the actual channel realization may additionally vary from channel use to channel use in an arbitrary fashion.

In this paper, the compound BCC is studied. The discrete memoryless compound BCC consists of one sender and two receivers. The sender wants to transmit two messages: a common message for both receivers and a confidential message for receiver 1. Receiver 2 must be kept ignorant of the confidential message. In [5], a multi-letter characterization of the compound BCC capacity region using the *strong secrecy* criterion was established.

In this work we investigate whether the capacity region of the compound BCC depends *continuously* on the uncertainty set or not. If small changes in the uncertainty set cause large changes in the corresponding capacity region, the compound BCC is fragile, which complicates the design of practical communication systems. Hence, a continuous behavior of the capacity region is desired.

In [6], the continuity of the compound wiretap channel and arbitrarily varying wiretap channel (AVWC) was studied. The authors show that the secrecy capacity is continuous for the compound wiretap channel and discontinuous for the AVWC.

Our main contribution is to show that the compound BCC capacity region depends continuously on the uncertainty set. For a channel example from [6], we show that the capacity region of the arbitrarily varying BCC (AVBCC) is discontinuous, which implies that continuity of the compound BCC capacity region cannot be generalized to the AVBCC.

In Section II we introduce the compound BCC and its capacity region. In Section III we introduce a distance between two compound BCC and a distance between two sets and we show that the capacity region of the compound BCC is a continuous function of the uncertainty set. Finally, we conclude our paper with a discussion in Section IV.[1]

## II. Compound Broadcast Channel with Confidential Messages

The transmitter and the receiver of a compound channel know an uncertainty set of channels to which the channel belongs; however, they do not know the actual channel realization. The channel remains constant during the entire

This work of H. Boche was supported by the German Ministry of Education and Research (BMBF) under Grant 01BQ1050. This work of R. F. Schaefer was supported by the German Research Foundation (DFG) under Grant WY 151/2-1. This work of H. V. Poor was supported by the U.S. National Science Foundation under Grant CMMI-1435778.

[1] *Notation*: $\mathbb{N}$ and $\mathbb{R}_+$ denote the sets of non-negative integers and non-negative real numbers, respectively; $\mathcal{I} = (\cdot,\cdot)$ and $\mathcal{J} = [\cdot,\cdot]$ denote open and closed intervals, respectively; $\overline{\text{conv}}(\mathcal{A})$ denotes the convex hull closure of the set $\mathcal{A}$; $H(\cdot)$, $H_2(\cdot)$, $I(\cdot;\cdot)$ are the entropy, binary entropy, and mutual information, respectively; all logarithms and information quantities are taken to the base 2; $\|\nu-\mu\| := \sum_{a\in\mathcal{A}} |\nu(a)-\mu(a)|$ is the total variation distance of measures $\mu$ and $\nu$ on a finite set $\mathcal{A}$; the space of probability distribution on the finite set $\mathcal{A}$ is denoted by $\mathcal{P}(\mathcal{A})$.

transmission. We consider a two receiver compound BCC. The transmitter sends simultaneously a common message to both receivers and a confidential message to receiver 1, which must be kept secret from receiver 2. Let $\mathcal{X}$ be the finite input alphabet, $\mathcal{Y}$ and $\mathcal{Z}$ the finite output alphabets of receivers 1 and 2, respectively, and let $\mathcal{S}$ be a finite set of channel states. For each channel state $s \in \mathcal{S}$, input sequence $x^n \in \mathcal{X}^n$ and output sequences $y^n \in \mathcal{Y}^n$ and $z^n \in \mathcal{Z}^n$, the discrete memoryless broadcast channel is given by $Q_s^n(y^n, z^n|x^n) := \prod_{i=1}^n Q_s(y_i, z_i|x_i)$ with marginal channels $W_s^n(y^n|x^n)$ and $V_s^n(z^n|x^n)$.

**Definition 1.** The discrete memoryless *compound broadcast channel* $\mathfrak{W}$ is given by the channel pair family with common input

$$\mathfrak{W} := \{(W_s, V_s) \colon s \in \mathcal{S}\}.$$

### A. Codes for Compound Broadcast Channels

We consider a block-code of arbitrary but fixed length $n$. Let $\mathcal{M}_0 := \{1, \dots, M_{0,n}\}$ be the common message set and $\mathcal{M}_1 := \{1, \dots, M_{1,n}\}$ the confidential message set. We use the abbreviation $\mathcal{M} := \mathcal{M}_0 \times \mathcal{M}_1$.

**Definition 2.** An $(n, M_{0,n}, M_{1,n})$-*code* for the compound BCC consists of a stochastic encoder

$$E \colon \mathcal{M}_0 \times \mathcal{M}_1 \to \mathcal{P}(\mathcal{X}^n)$$

i.e., a stochastic matrix, and decoders at receivers 1 and 2

$$\varphi_1 \colon \mathcal{Y}^n \to \mathcal{M}_0 \times \mathcal{M}_1$$
$$\varphi_2 \colon \mathcal{Z}^n \to \mathcal{M}_0.$$

The average error probability for receivers 1 and 2 and the channel realization $s \in \mathcal{S}$ are

$$\overline{e}_{1,n}(s) := \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} \sum_{x^n \in \mathcal{X}^n} \sum_{y^n : \varphi_1(y^n) \neq m} W_s^n(y^n|x^n) E(x^n|m)$$

$$\overline{e}_{2,n}(s) := \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} \sum_{x^n \in \mathcal{X}^n} \sum_{z^n : \varphi_2(z^n) \neq m_0} V_s^n(z^n|x^n) E(x^n|m).$$

Since reliable communication is required for all $s \in \mathcal{S}$, we consider the maximum average error probabilities, i.e. $\overline{e}_{1,n} = \max_{s \in \mathcal{S}} \overline{e}_{1,n}(s)$ and $\overline{e}_{2,n} = \max_{s \in \mathcal{S}} \overline{e}_{2,n}(s)$.

The confidential message has to be kept secret from the non-legitimate receiver for all channel realizations. Therefore, we require $\max_{s \in \mathcal{S}} I(M_1; Z_s^n) \leq \epsilon_n$ for some $\epsilon_n > 0$ with $M_1$ uniformly distributed over the set $\mathcal{M}_1$ and $Z_s^n$ the output at the non-legitimate receiver for the channel realization $s \in \mathcal{S}$. This criterion is known as *strong secrecy* [7], [8].

**Definition 3.** A rate pair $(R_0, R_1) \in \mathbb{R}_+^2$ is said to be achievable for the compound BCC if for any $\tau > 0$ there is an $n(\tau) \in \mathbb{N}$ and a sequence of $(n, M_{0,n}, M_{1,n})$-codes such that for all $n \geq n(\tau)$ we have $\frac{1}{n} \log M_{0,n} \geq R_0 - \tau, \frac{1}{n} \log M_{1,n} \geq R_1 - \tau$, and

$$\max_{s \in \mathcal{S}} I(M_1; Z_s^n) \leq \epsilon_n \tag{1}$$

with $\overline{e}_{1,n}, \overline{e}_{2,n}, \epsilon_n \to 0$ as $n \to \infty$.

**Definition 4.** The set closure of all achievable rate pairs is the *capacity region* $\mathcal{C}(\mathfrak{W})$ of the compound BCC $\mathfrak{W}$.

### B. Capacity Results

In this section we present an achievable rate region and a multi-letter characterization of the compound BCC capacity region [5].

**Lemma 1** ([5])**.** *An achievable secrecy rate region for the compound BCC is given by the set of all rate pairs* $(R_0, R_1) \in \mathbb{R}_+^2$ *satisfying*

$$R_0 \leq \min_{s \in \mathcal{S}} \min\{I(U; Y_s), I(U; Z_s)\}$$
$$R_1 \leq \min_{s \in \mathcal{S}} I(V; Y_s|U) - \max_{s \in \mathcal{S}} I(V; Z_s|U)$$

*for some random variables* $U, V, X$ *where* $U - V - X - (Y_s, Z_s)$ *forms a Markov chain. Furthermore, the strong secrecy criterion goes exponentially fast to zero and the decoding error at the non-legitimate receiver goes exponentially fast to one.*

We next present a multi-letter description of $\mathcal{C}(\mathfrak{W})$ of the compound BCC $\mathfrak{W}$. Let $n \in \mathbb{N}$ be arbitrary but fixed. We define the rate region $\mathcal{R}_n(\mathfrak{W}, U, V, X^n)$ as the set of all rate pairs $(R_0, R_1) \in \mathbb{R}_+^2$ satisfying

$$R_0 \leq \frac{1}{n} \inf_{s \in \mathcal{S}} \min\{I(U; Y_s^n), I(U; Z_s^n)\} \tag{2}$$

$$R_1 \leq \frac{1}{n} (\inf_{s \in \mathcal{S}} I(V; Y_s^n|U) - \sup_{s \in \mathcal{S}} I(V; Z_s^n|U)) \tag{3}$$

for the random variables satisfying the Markov chain relationship $U - V - X^n - (Y_s^n, Z_s^n)$. For a given $n \in \mathbb{N}$ we define the region

$$\mathcal{M}_n(\mathfrak{W}) = \bigcup_{U - V - X^n} \mathcal{R}_n(\mathfrak{W}, U, V, X^n)$$

that is, $\mathcal{M}_n(\mathfrak{W})$ is the union of the regions $\mathcal{R}_n(\mathfrak{W}, U, V, X^n)$ over all random variables satisfying the Markov chain relationship $U - V - X^n$.

**Theorem 1.** *The strong secrecy capacity region* $\mathcal{C}(\mathfrak{W})$ *of the compound BCC* $\mathfrak{W}$ *is the convex hull closure of the union of the regions* $\mathcal{M}_n(\mathfrak{W})$ *over all* $n \in \mathbb{N}$*, i.e.*

$$\mathcal{C}(\mathfrak{W}) = \overline{\text{conv}}(\bigcup_{n \in \mathbb{N}} \mathcal{M}_n(\mathfrak{W})).$$

*Remark* 1. To the best of our knowledge, there is still no single-letter characterization of $\mathcal{C}(\mathfrak{W})$ known.

*Remark* 2. The union of the rate regions $\bigcup_{n \in \mathbb{N}} \mathcal{M}_n(\mathfrak{W})$ may itself not be convex. However, all rate pairs in the convex hull can be achieved by time sharing between the points in the rate regions $\mathcal{M}_n(\mathfrak{W})$.

## III. Continuity of the Compound BCC Capacity Region

In this section we first define the distance between two compound BCCs and the distance between rate regions. We then analyze the continuity of the compound BCC capacity region.

### A. Distance between Compound Broadcast Channels and Sets

Let $(W, V)$ and $(\widetilde{W}, \widetilde{V})$ be two broadcast channels. We define the distance between channels as

$$d(W, \widetilde{W}) \coloneqq \max_{x\in\mathcal{X}} \sum_{y\in\mathcal{Y}} |W(y|x) - \widetilde{W}(y|x)|$$
$$d(V, \widetilde{V}) \coloneqq \max_{x\in\mathcal{X}} \sum_{z\in\mathcal{Z}} |V(z|x) - \widetilde{V}(z|x)|$$

and the distance between two broadcast channels as

$$d((W, V), (\widetilde{W}, \widetilde{V})) \coloneqq \max(d(W, \widetilde{W}), d(V, \widetilde{V})).$$

Let $\mathfrak{W}_1 = \{(W_{s_1}, V_{s_1})\colon s_1 \in \mathcal{S}_1\}$ and $\mathfrak{W}_2 = \{(W_{s_2}, V_{s_2})\colon s_2 \in \mathcal{S}_2\}$ be two finite compound broadcast channels with marginal compound channels $\mathcal{W}_i = \{W_{s_i}\colon s_i \in \mathcal{S}_i\}$ and $\mathcal{V}_i = \{V_{s_i}\colon s_i \in \mathcal{S}_i\}$ for $i \in \{1, 2\}$. We define the distance between two marginal compound channels as

$$d_1(\mathcal{W}_1, \mathcal{W}_2) = \max_{s_2\in\mathcal{S}_2} \min_{s_1\in\mathcal{S}_1} d(W_{s_1}, W_{s_2})$$
$$d_2(\mathcal{W}_1, \mathcal{W}_2) = \max_{s_1\in\mathcal{S}_1} \min_{s_2\in\mathcal{S}_2} d(W_{s_1}, W_{s_2})$$

$$d_1(\mathcal{V}_1, \mathcal{V}_2) = \max_{s_2\in\mathcal{S}_2} \min_{s_1\in\mathcal{S}_1} d(V_{s_1}, V_{s_2})$$
$$d_2(\mathcal{V}_1, \mathcal{V}_2) = \max_{s_1\in\mathcal{S}_1} \min_{s_2\in\mathcal{S}_2} d(V_{s_1}, V_{s_2}).$$

**Definition 5.** Let $\mathfrak{W}_1$ and $\mathfrak{W}_2$ be two compound broadcast channels. The distance $D(\mathfrak{W}_1, \mathfrak{W}_2)$ between $\mathfrak{W}_1$ and $\mathfrak{W}_2$ is defined as

$$D(\mathfrak{W}_1, \mathfrak{W}_2) = \max\Big\{d_1(\mathcal{W}_1, \mathcal{W}_2), d_2(\mathcal{W}_1, \mathcal{W}_2), d_1(\mathcal{V}_1, \mathcal{V}_2), d_2(\mathcal{V}_1, \mathcal{V}_2)\Big\}.$$

To compare different rate regions, we define the following distance of sets.

**Definition 6.** Let $\mathcal{R}_1$ and $\mathcal{R}_2$ be two non-empty compact subsets of the metric space $(\mathbb{R}_+^2, d)$ with $d(x, y) = \sum_{i=1}^2 |x_i - y_i|$ for all $x, y \in \mathbb{R}_+^2$. We define the distance between two sets as

$$D_R(\mathcal{R}_1, \mathcal{R}_2) = \max\big\{ \max_{r_1\in\mathcal{R}_1} \min_{r_2\in\mathcal{R}_2} d(r_1, r_2), \max_{r_2\in\mathcal{R}_2} \min_{r_1\in\mathcal{R}_2} d(r_1, r_2)\big\}.$$

### B. Continuity of the Capacity Region of the Compound BCC

We use the following technical result, which is an extension of Lemma 2 in [6].

**Lemma 2.** *Let $\mathcal{X}$ and $\mathcal{Y}$ be finite alphabets and $W, \widetilde{W}\colon \mathcal{X} \to \mathcal{P}(\mathcal{Y})$ be arbitrary channels with*

$$d(W, \widetilde{W}) \leq \epsilon$$

*for some $\epsilon > 0$. For an arbitrary $n \in \mathbb{N}$, let $\mathcal{U}$ and $\mathcal{V}$ be two finite sets, $P_U \in \mathcal{P}(\mathcal{U})$ be the uniform distribution on $\mathcal{U}$, $P_{V|U}(\cdot|u)$ be the conditional distribution of the random variable $V$ over $\mathcal{V}$ given $U = u$, and $E(x^n|v)$ with $x^n \in \mathcal{X}^n$ conditioned on $u \in \mathcal{U}$ be an arbitrary stochastic encoder. We consider the probability distributions*

$$P_{UVY^n}(u, v, y^n) = \sum_{x^n\in\mathcal{X}^n} W^n(y^n|x^n) E(x^n|v) P_{V|U}(v|u) P_U(u)$$
$$P_{UV\widetilde{Y}^n}(u, v, y^n) = \sum_{x^n\in\mathcal{X}^n} \widetilde{W}^n(y^n|x^n) E(x^n|v) P_{V|U}(v|u) P_U(u).$$

*Then it holds that*

$$|I(V; Y^n|U) - I(V; \widetilde{Y}^n|U)| \leq n\delta_2(\epsilon, |\mathcal{Y}|) \tag{4}$$

*with $\delta_2(\epsilon, |\mathcal{Y}|) \coloneqq 4\epsilon \log |\mathcal{Y}| + 4H_2(\epsilon)$.*

*Proof:* See the arXiv version of this work [9]. ∎

*Remark* 3. Note that the right-hand side of (4) depends only on the size of the output alphabet $\mathcal{Y}$, and is independent of the size of the auxiliary alphabets $\mathcal{U}$ and $\mathcal{V}$, the conditional distribution $P_{V|U}$ and the chosen stochastic encoder $E$.

**Lemma 3.** *Let $\epsilon \in (0, 1)$ and $n \in \mathbb{N}$. Let $\mathfrak{W}_1$ and $\mathfrak{W}_2$ be two compound BCCs and consider random variables satisfying the Markov chain relationship $U - V - X^n$. If*

$$D(\mathfrak{W}_1, \mathfrak{W}_2) \leq \epsilon$$

*then it holds that*

$$D_R(\mathcal{R}_n(\mathfrak{W}_1, U, V, X^n), \mathcal{R}_n(\mathfrak{W}_2, U, V, X^n)) \leq \delta(\epsilon, |\mathcal{Y}|, |\mathcal{Z}|)$$

*with $\delta(\epsilon, |\mathcal{Y}|, |\mathcal{Z}|) = \delta'(\epsilon, |\mathcal{Y}|, |\mathcal{Z}|) + \delta''(\epsilon, |\mathcal{Y}|, |\mathcal{Z}|)$, $\delta'(\epsilon, |\mathcal{Y}|, |\mathcal{Z}|) \coloneqq 4H_2(\epsilon) + 4\epsilon \max\{\log |\mathcal{Y}|, \log |\mathcal{Z}|\}$ and $\delta''(\epsilon, |\mathcal{Y}|, |\mathcal{Z}|) \coloneqq 4\epsilon \log |\mathcal{Y}||\mathcal{Z}| + 8H_2(\epsilon)$.*

*Proof:* The regions $\mathcal{R}_n(\mathfrak{W}_1, U, V, X^n) \in \mathbb{R}_+^2$ and $\mathcal{R}_n(\mathfrak{W}_2, U, V, X^n) \in \mathbb{R}_+^2$ are rectangles described by the rates $(R_{0,\mathcal{S}_1}, R_{1,\mathcal{S}_1})$ and $(R_{0,\mathcal{S}_2}, R_{1,\mathcal{S}_2})$ satisfying (2) and (3) respectively. For $i = 1, 2$, we define $A_{0_{\mathcal{S}_i}}$ and $A_{1_{\mathcal{S}_i}}$ as

$$A_{0_{\mathcal{S}_i}} = \max_{(R_{0,\mathcal{S}_i}, R_{1,\mathcal{S}_i})\in\mathcal{R}_n(\mathfrak{W}_i, U, V, X^n)} R_{0,\mathcal{S}_i}$$
$$A_{1_{\mathcal{S}_i}} = \max_{(R_{0,\mathcal{S}_i}, R_{1,\mathcal{S}_i})\in\mathcal{R}_n(\mathfrak{W}_i, U, V, X^n)} R_{1,\mathcal{S}_i}.$$

Note that both regions are rectangles sharing the corner point $(0, 0)$. Therefore, the longest distance between these two sets is given by the corner points $(A_{0_{\mathcal{S}_1}}, A_{1_{\mathcal{S}_1}})$ and $(A_{0_{\mathcal{S}_2}}, A_{1_{\mathcal{S}_2}})$, i.e.,

$$D_R(\mathcal{R}_n(\mathfrak{W}_1, U, V, X^n), \mathcal{R}_n(\mathfrak{W}_2, U, V, X^n)) = |A_{0_{\mathcal{S}_1}} - A_{0_{\mathcal{S}_2}}| + |A_{1_{\mathcal{S}_1}} - A_{1_{\mathcal{S}_2}}|.$$

We first analyze the difference between the maximum achievable common rates, i.e., $|A_{0_{\mathcal{S}_1}} - A_{0_{\mathcal{S}_2}}|$ and then the difference between the maximum achievable confidential rates, i.e., $|A_{1_{\mathcal{S}_1}} - A_{1_{\mathcal{S}_2}}|$.

*1) Common Message Rate:* There are four cases that may occur:

**1)** $A_{0_{\mathcal{S}_1}} = \frac{1}{n}\inf_{s_1\in\mathcal{S}_1} I(U;Y_{s_1}^n)$
$A_{0_{\mathcal{S}_2}} = \frac{1}{n}\inf_{s_2\in\mathcal{S}_2} I(U;Y_{s_2}^n)$

**2)** $A_{0_{\mathcal{S}_1}} = \frac{1}{n}\inf_{s_1\in\mathcal{S}_1} I(U;Z_{s_1}^n)$
$A_{0_{\mathcal{S}_2}} = \frac{1}{n}\inf_{s_2\in\mathcal{S}_2} I(U;Z_{s_2}^n)$

**3)** $A_{0_{\mathcal{S}_1}} = \frac{1}{n}\inf_{s_1\in\mathcal{S}_1} I(U;Y_{s_1}^n)$
$A_{0_{\mathcal{S}_2}} = \frac{1}{n}\inf_{s_2\in\mathcal{S}_2} I(U;Z_{s_2}^n)$

**4)** $A_{0_{\mathcal{S}_1}} = \frac{1}{n}\inf_{s_1\in\mathcal{S}_1} I(U;Z_{s_1}^n)$
$A_{0_{\mathcal{S}_2}} = \frac{1}{n}\inf_{s_2\in\mathcal{S}_2} I(U;Y_{s_2}^n)$

For Case 1), we have

$$\begin{aligned}&\left|A_{0_{\mathcal{S}_1}} - A_{0_{\mathcal{S}_2}}\right| \\ &\quad= \left|\frac{1}{n}\inf_{s_1\in\mathcal{S}_1} I(U;Y_{s_1}^n) - \frac{1}{n}\inf_{s_2\in\mathcal{S}_2} I(U;Y_{s_2}^n)\right|. \quad (5)\end{aligned}$$

Let $\eta > 0$ be arbitrary. There exists an $\hat{s}_1 = \hat{s}_1(\eta)$ such that

$$\inf_{s_1\in\mathcal{S}_1} I(U;Y_{s_1}^n) \geq I(U;Y_{\hat{s}_1}^n) - \eta. \quad (6)$$

Since $D(\mathfrak{W}_1,\mathfrak{W}_2) < \epsilon$, there is an $\hat{s}_2 = \hat{s}_2(\hat{s}_1)$ such that

$$d(W_{\hat{s}_1}, W_{\hat{s}_2}) < \epsilon. \quad (7)$$

We can now apply Lemma 2. (We let $U$ in (4) be a constant and we let $U$ in (5) take the role of $V$ in (4).) By (7), we have

$$\left|I(U;Y_{\hat{s}_1}^n) - I(U;Y_{\hat{s}_2}^n)\right| \leq n\delta_2(\epsilon,|\mathcal{Y}|). \quad (8)$$

Combining (6) and (8) we obtain

$$\begin{aligned}\inf_{s_1\in\mathcal{S}_1} I(U;Y_{s_1}^n) &\geq I(U;Y_{\hat{s}_2}^n) - n\delta_2(\epsilon,|\mathcal{Y}|) - \eta \\ &\geq \inf_{s_2\in\mathcal{S}_2} I(U;Y_{s_2}^n) - n\delta_2(\epsilon,|\mathcal{Y}|) - \eta.\end{aligned}$$

Since this inequality holds for all $\eta > 0$, we then obtain

$$\inf_{s_1\in\mathcal{S}_1} I(U;Y_{s_1}^n) > \inf_{s_2\in\mathcal{S}_2} I(U;Y_{s_2}^n) - n\delta_2(\epsilon,|\mathcal{Y}|).$$

By changing the roles of $\mathcal{S}_1$ and $\mathcal{S}_2$ in the previous derivation, we get

$$\left|\inf_{s_1\in\mathcal{S}_1} I(U;Y_{s_1}^n) - \inf_{s_2\in\mathcal{S}_2} I(U;Y_{s_2}^n)\right| \leq n\delta_2(\epsilon,|\mathcal{Y}|).$$

Using the same line of argument as for Case 1), for Case 2), we have

$$\left|\inf_{s_1\in\mathcal{S}_1} I(U;Z_{s_1}^n) - \inf_{s_2\in\mathcal{S}_2} I(U;Z_{s_2}^n)\right| \leq n\delta_2(\epsilon,|\mathcal{Z}|).$$

In Case 3) and Case 4) we have that for one compound BCC the maximum achievable common rate depends on the random variable $Y$ and for the other, the maximum achievable common rate depends on the random variable $Z$. We first study Case 3). We have

$$\begin{aligned}B_{0_{\mathcal{S}_1}} &= \frac{1}{n}\inf_{s_1\in\mathcal{S}_1} I(U;Z_{s_1}^n) \geq \frac{1}{n}\inf_{s_1\in\mathcal{S}_1} I(U;Y_{s_1}^n) = A_{0_{\mathcal{S}_1}} \\ B_{0_{\mathcal{S}_2}} &= \frac{1}{n}\inf_{s_2\in\mathcal{S}_2} I(U;Y_{s_2}^n) \geq \frac{1}{n}\inf_{s_2\in\mathcal{S}_2} I(U;Z_{s_2}^n) = A_{0_{\mathcal{S}_2}}.\end{aligned}$$

We have six possibilities to relate the two previous inequalities:

**I)** $B_{0_{\mathcal{S}_1}} \geq A_{0_{\mathcal{S}_1}} \geq B_{0_{\mathcal{S}_2}} \geq A_{0_{\mathcal{S}_2}}$ and Lemma 2 implies
$\left|A_{0_{\mathcal{S}_1}} - A_{0_{\mathcal{S}_2}}\right| \leq \left|B_{0_{\mathcal{S}_1}} - A_{0_{\mathcal{S}_2}}\right| \leq \delta_2(\epsilon,|\mathcal{Z}|)$

**II)** $B_{0_{\mathcal{S}_1}} \geq B_{0_{\mathcal{S}_2}} \geq A_{0_{\mathcal{S}_1}} \geq A_{0_{\mathcal{S}_2}}$ implying
$|A_{0_{\mathcal{S}_1}} - A_{0_{\mathcal{S}_2}}| \leq |B_{0_{\mathcal{S}_1}} - A_{0_{\mathcal{S}_2}}| \leq \delta_2(\epsilon,|\mathcal{Z}|)$

**III)** $B_{0_{\mathcal{S}_1}} \geq B_{0_{\mathcal{S}_2}} \geq A_{0_{\mathcal{S}_2}} \geq A_{0_{\mathcal{S}_1}}$ implying
$|A_{0_{\mathcal{S}_1}} - A_{0_{\mathcal{S}_2}}| \leq |A_{0_{\mathcal{S}_1}} - B_{0_{\mathcal{S}_2}}| \leq \delta_2(\epsilon,|\mathcal{Y}|)$

**IV)** $B_{0_{\mathcal{S}_2}} \geq A_{0_{\mathcal{S}_2}} \geq B_{0_{\mathcal{S}_1}} \geq A_{0_{\mathcal{S}_1}}$ implying
$|A_{0_{\mathcal{S}_1}} - A_{0_{\mathcal{S}_2}}| \leq |A_{0_{\mathcal{S}_1}} - B_{0_{\mathcal{S}_2}}| \leq \delta_2(\epsilon,|\mathcal{Y}|)$

**V)** $B_{0_{\mathcal{S}_2}} \geq B_{0_{\mathcal{S}_1}} \geq A_{0_{\mathcal{S}_2}} \geq A_{0_{\mathcal{S}_1}}$ implying
$|A_{0_{\mathcal{S}_1}} - A_{0_{\mathcal{S}_2}}| \leq |A_{0_{\mathcal{S}_1}} - B_{0_{\mathcal{S}_2}}| \leq \delta_2(\epsilon,|\mathcal{Y}|)$

**VI)** $B_{0_{\mathcal{S}_2}} \geq B_{0_{\mathcal{S}_1}} \geq A_{0_{\mathcal{S}_1}} \geq A_{0_{\mathcal{S}_2}}$ implying
$|A_{0_{\mathcal{S}_1}} - A_{0_{\mathcal{S}_2}}| \leq |A_{0_{\mathcal{S}_2}} - B_{0_{\mathcal{S}_1}}| \leq \delta_2(\epsilon,|\mathcal{Z}|)$

We use the same line of argument for Case 4) as for Case 3) to bound the distance between the two maximum achievable common rates. It then holds for all cases that

$$\begin{aligned}|A_{0_{\mathcal{S}_1}} - A_{0_{\mathcal{S}_2}}| &\leq \max\{\delta_2(\epsilon,|\mathcal{Y}|),\delta_2(\epsilon,|\mathcal{Y}|)\} \\ &= 4H_2(\epsilon) + 4\epsilon\max\{\log|\mathcal{Y}|,\log|\mathcal{Z}|\}.\end{aligned}$$

*2) Confidential Message Rate:* Using the same line of argument as in Case 1) for the common-message rate, we obtain

$$\begin{aligned}|A_{1_{\mathcal{S}_1}} - A_{1_{\mathcal{S}_2}}| &= \Big|\frac{1}{n}\inf_{s_1\in\mathcal{S}_1} I(V;Y_{s_1}^n|U) - \frac{1}{n}\sup_{s_1\in\mathcal{S}_1} I(V;Z_{s_1}^n|U) \\ &\quad - \frac{1}{n}\inf_{s_2\in\mathcal{S}_2} I(V;Y_{s_2}^n|U) + \frac{1}{n}\sup_{s_2\in\mathcal{S}_2} I(V;Z_{s_2}^n|U)\Big| \\ &\leq \frac{1}{n}\Big|\inf_{s_1\in\mathcal{S}_1} I(V;Y_{s_1}^n|U) - \inf_{s_2\in\mathcal{S}_2} I(V;Y_{s_2}^n|U)\Big| \\ &\quad + \frac{1}{n}\Big|\inf_{s_2\in\mathcal{S}_2} I(V;Z_{s_2}^n|U) - \inf_{s_1\in\mathcal{S}_1} I(V;Z_{s_1}^n|U)\Big| \\ &\leq \delta_2(\epsilon,|\mathcal{Y}|) + \delta_2(\epsilon,|\mathcal{Z}|) \\ &\leq 4\epsilon\log|\mathcal{Y}||\mathcal{Z}| + 8H_2(\epsilon).\end{aligned}$$

■

**Theorem 2.** *Let $\epsilon \in (0,1)$. Let $\mathfrak{W}_1$ and $\mathfrak{W}_2$ be two compound BCCs. If*

$$D(\mathfrak{W}_1,\mathfrak{W}_2) \leq \epsilon \quad (9)$$

*then it holds that*

$$D_R(\mathcal{C}(\mathfrak{W}_1),\mathcal{C}(\mathfrak{W}_2)) \leq \delta(\epsilon,|\mathcal{Y}|,|\mathcal{Z}|).$$

*Proof:* We define the sets $\mathcal{D}_1, \mathcal{B}_1 \subset \mathbb{R}_+^2$ and

$$\begin{aligned}\mathcal{D}_1 &= \bigcup_{n\in\mathbb{N}}\bigcup_{U-V-X^n} \mathcal{R}_n(\mathfrak{W}_1,U,V,X^n) \\ \mathcal{B}_1 &= \mathcal{C}(\mathfrak{W}_1)\setminus\bigcup_{n\in\mathbb{N}}\bigcup_{U-V-X^n} \mathcal{R}_n(\mathfrak{W}_1,U,V,X^n)\end{aligned}$$

with random variables $U - V - X^n$ forming a Markov chain. Let $(R_{0_{\mathcal{S}_1}}, R_{1_{\mathcal{S}_1}}) \in \mathcal{D}_1$. Then there exists an $n \in \mathbb{N}$ and random variables satisfying the Markov chain relationship $\hat{U} - \hat{V} - \hat{X^n}$ such that $(R_{0_{\mathcal{S}_1}}, R_{1_{\mathcal{S}_1}}) \in \mathcal{R}_n(\mathfrak{W}_1, \hat{U}, \hat{V}, \hat{X^n})$. From Lemma 3 and (9) we have that

$$D_R(\mathcal{R}_n(\mathfrak{W}_1, \hat{U}, \hat{V}, \hat{X^n}), \mathcal{R}_n(\mathfrak{W}_2, \hat{U}, \hat{V}, \hat{X^n})) \leq \delta(\epsilon, |\mathcal{Y}|, |\mathcal{Z}|).$$

This means that there exists a rate pair $(R_{0_{\mathcal{S}_2}}(R_{0_{\mathcal{S}_1}}), R_{1_{\mathcal{S}_2}}(R_{1_{\mathcal{S}_1}})) \in \mathcal{R}_n(\mathfrak{W}_2, \hat{U}, \hat{V}, \hat{X^n})$ such that

$$|R_{0_{\mathcal{S}_1}} - R_{0_{\mathcal{S}_2}}| + |R_{1_{\mathcal{S}_1}} - R_{1_{\mathcal{S}_2}}| \leq \delta(\epsilon, |\mathcal{Y}|, |\mathcal{Z}|).$$

Let $(\hat{R}_{0_{\mathcal{S}_1}}, \hat{R}_{1_{\mathcal{S}_1}}) \in \mathcal{B}_1$. Then there exist two rate pairs $(\dot{R}_{0_{\mathcal{S}_1}}, \dot{R}_{1_{\mathcal{S}_1}}), (\tilde{R}_{0_{\mathcal{S}_1}}, \tilde{R}_{1_{\mathcal{S}_1}}) \in \mathcal{D}_1$ such that

$$\begin{aligned}\hat{R}_{0_{\mathcal{S}_1}} &= \lambda \dot{R}_{0_{\mathcal{S}_1}} + (1-\lambda)\tilde{R}_{0_{\mathcal{S}_1}} \\ \hat{R}_{1_{\mathcal{S}_1}} &= \lambda \dot{R}_{1_{\mathcal{S}_1}} + (1-\lambda)\tilde{R}_{1_{\mathcal{S}_1}}\end{aligned}$$

for some $\lambda \in (0,1)$. For each $(\dot{R}_{0_{\mathcal{S}_1}}, \dot{R}_{1_{\mathcal{S}_1}})$ and $(\tilde{R}_{0_{\mathcal{S}_1}}, \tilde{R}_{1_{\mathcal{S}_1}})$ there exist random variables satisfying the Markov chain relation $\dot{U} - \dot{V} - \dot{X}^n$ and $\tilde{U} - \tilde{V} - \tilde{X}^n$ such that $(\dot{R}_{0_{\mathcal{S}_1}}, \dot{R}_{1_{\mathcal{S}_1}}) \in \mathcal{R}_n(\mathfrak{W}_1, \dot{U}, \dot{V}, \dot{X}^n)$ and $(\tilde{R}_{0_{\mathcal{S}_1}}, \tilde{R}_{1_{\mathcal{S}_1}}) \in \mathcal{R}_n(\mathfrak{W}_1, \tilde{U}, \tilde{V}, \tilde{X}^n)$. Then from Lemma 3 and (9) we have that there exist rate pairs $(\dot{R}_{0_{\mathcal{S}_2}}(\dot{R}_{0_{\mathcal{S}_1}}), \dot{R}_{1_{\mathcal{S}_2}}(\dot{R}_{1_{\mathcal{S}_1}})) \in \mathcal{R}_n(\mathfrak{W}_2, \dot{U}, \dot{V}, \dot{X}^n)$ and $(\tilde{R}_{0_{\mathcal{S}_2}}(\tilde{R}_{0_{\mathcal{S}_1}}), \tilde{R}_{1_{\mathcal{S}_2}}(\tilde{R}_{1_{\mathcal{S}_1}})) \in \mathcal{R}_n(\mathfrak{W}_2, \tilde{U}, \tilde{V}, \tilde{X}^n)$ such that

$$\begin{aligned}|\dot{R}_{0_{\mathcal{S}_1}} - \dot{R}_{0_{\mathcal{S}_2}}| + |\dot{R}_{1_{\mathcal{S}_1}} - \dot{R}_{1_{\mathcal{S}_2}}| &\leq \delta(\epsilon, |\mathcal{Y}|, |\mathcal{Z}|) \\ |\tilde{R}_{0_{\mathcal{S}_1}} - \tilde{R}_{0_{\mathcal{S}_2}}| + |\tilde{R}_{1_{\mathcal{S}_1}} - \tilde{R}_{1_{\mathcal{S}_2}}| &\leq \delta(\epsilon, |\mathcal{Y}|, |\mathcal{Z}|).\end{aligned}$$

Then there is a rate pair $(\hat{R}_{0_{\mathcal{S}_2}}, \hat{R}_{1_{\mathcal{S}_2}}) \in \mathcal{C}(\mathfrak{W}_2)$ with

$$\begin{aligned}\hat{R}_{0_{\mathcal{S}_2}} &= \lambda \dot{R}_{0_{\mathcal{S}_2}} + (1-\lambda)\tilde{R}_{0_{\mathcal{S}_2}} \\ \hat{R}_{1_{\mathcal{S}_2}} &= \lambda \dot{R}_{1_{\mathcal{S}_2}} + (1-\lambda)\tilde{R}_{1_{\mathcal{S}_2}}.\end{aligned}$$

Further we have

$$\begin{aligned}|\hat{R}_{0_{\mathcal{S}_1}} - \hat{R}_{0_{\mathcal{S}_2}}| &= |\lambda \dot{R}_{0_{\mathcal{S}_2}} + (1-\lambda)\tilde{R}_{0_{\mathcal{S}_2}} \\ &\quad - \lambda \dot{R}_{0_{\mathcal{S}_1}} + (1-\lambda)\tilde{R}_{0_{\mathcal{S}_1}}| \\ &\leq \lambda |\dot{R}_{0_{\mathcal{S}_1}} - \dot{R}_{0_{\mathcal{S}_2}}| + (1-\lambda)|\tilde{R}_{0_{\mathcal{S}_1}} - \tilde{R}_{0_{\mathcal{S}_2}}| \\ &\leq \delta'(\epsilon, |\mathcal{Y}|, |\mathcal{Z}|)\end{aligned}$$

and using the same line of argument

$$|\hat{R}_{1_{\mathcal{S}_1}} - \hat{R}_{1_{\mathcal{S}_2}}| \leq \delta''(\epsilon, |\mathcal{Y}|, |\mathcal{Z}|).$$

This leads us to the following result:

$$|\hat{R}_{0_{\mathcal{S}_1}} - \hat{R}_{0_{\mathcal{S}_2}}| + |\hat{R}_{1_{\mathcal{S}_1}} - \hat{R}_{1_{\mathcal{S}_2}}| \leq \delta(\epsilon, |\mathcal{Y}|, |\mathcal{Z}|).$$

We can conclude that for every rate pair $(R_{0_{\mathcal{S}_1}}, R_{1_{\mathcal{S}_1}}) \in \mathcal{C}(\mathfrak{W}_1)$ we can find a rate pair $(R_{0_{\mathcal{S}_2}}(R_{0_{\mathcal{S}_1}}), R_{1_{\mathcal{S}_2}}(R_{1_{\mathcal{S}_1}})) \in \mathcal{C}(\mathfrak{W}_2)$ such that

$$|R_{0_{\mathcal{S}_1}} - R_{0_{\mathcal{S}_2}}| + |R_{1_{\mathcal{S}_1}} - R_{1_{\mathcal{S}_2}}| \leq \delta(\epsilon, |\mathcal{Y}|, |\mathcal{Z}|). \tag{10}$$

We use the same line of argument to show that for every rate pair $(R_{0_{\mathcal{S}_2}}, R_{1_{\mathcal{S}_2}}) \in \mathcal{C}(\mathfrak{W}_2)$ there is a rate pair $(R_{0_{\mathcal{S}_1}}(R_{0_{\mathcal{S}_2}}), R_{1_{\mathcal{S}_1}}(R_{1_{\mathcal{S}_2}})) \in \mathcal{C}(\mathfrak{W}_1)$ such that (10) holds. This completes the proof. ∎

## IV. Discussion

This work was motivated by the question of whether the compound BCC capacity region depends continuously on the uncertainty set or not. We have shown that the compound BCC model is robust, i.e., small changes in the uncertainty set lead to small changes in the capacity region, which is desirable.

Let us see what happens when the user's CSI is reduced further. For example, the AVBCC is described by the same uncertainty set as the compound BCC, but in addition, the actual channel realization varies from channel use to channel use in an arbitrary fashion. The AVBCC can be used for example to model the presence of jamming; see [6]. This may lead the channel to "emulate" a valid input, impeding the legitimate receiver to decide on the correct codeword. This property is known as symmetrizability; see [6, Sec. III, Def. 5].

We adapt the AVC example from [6, Sec. V] to the channel of receiver 1 of the AVBCC, where the input and the output alphabets are of size $|\mathcal{X}| = 2$ and $|\mathcal{Y}| = 3$, respectively, and the uncertainty set consists of only two elements, i.e., $|\mathcal{S}| = 2$. The AVC to receiver 1 is given by $\mathcal{W}(\lambda) = \{W_1(\lambda), W_2(\lambda)\}$ with

$$W_1(\lambda) = \begin{pmatrix} 1 & 0 & 0 \\ 1 & \lambda & 1-\lambda \end{pmatrix} \text{ and } W_2(\lambda) = \begin{pmatrix} \lambda & 0 & 1-\lambda \\ 0 & 1 & 0 \end{pmatrix}$$

where $\lambda \in [0,1]$. The AVC $\mathcal{V}$ to receiver 2 has an output alphabet of size $|\mathcal{Z}| = 2$ and is defined as $\mathcal{V} = \{V, V\}$ with

$$V = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}.$$

In [6, Sec. V], it is shown that the AVC $\mathcal{W}(\lambda)$ is non-symmetrizable for all $\lambda \in (0,1]$, and symmetrizable for $\lambda = 0$, in which case the capacity region collapses to the point $(0,0) \in \mathbb{R}_+^2$. Following the argumentation in [6, Sec. V], it can be shown that capacity region is indeed discontinuous at $\lambda = 0$.

## References


[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Foundations and Trends in Comm. and Inf. Theory*, vol. 5, no. 4–5, pp. 355–580, 2008.

[3] M. Bloch and J. Barros, *Physical-layer Security*. Cambridge University Press, 2011.

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

[5] R. F. Schaefer and H. Boche, "Robust broadcasting of common and confidential messages over compound channels: Strong secrecy and decoding performance," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 10, pp. 1720–1732, 2014.

[6] H. Boche, R. F. Schaefer, and H. V. Poor, "On the continuity of the secrecy capacity of compound and arbitrarily varying wiretap channels," in *Proc. IEEE Int. Conf. Commun. (ICC)*, London, UK, Jun. 2015.

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

[8] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Adv. in Crypt. EUROCRYPT*, 2000, pp. 351–368.

[9] A. Grigorescu, H. Boche, R. F. Schaefer, and H. V. Poor, "Capacity region continuity of the compound broadcast channel with confidential messages," 2014, available online at http://arxiv.org/abs/1411.0294.