Chapter 5
Broadcast Channels with Confidential Messages: Channel Uncertainty, Robustness, and Continuity

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

Abstract The *broadcast channel with confidential messages (BCC)* models the communication scenario in which a transmitter sends simultaneously common and confidential information to two receivers. The common information must be received by both receivers while the confidential information is designated for one receiver only and must be secured against the other one. The performance of this system is usually characterized by its secrecy capacity region determining the maximum transmission rates. In this chapter, the issue of whether this secrecy capacity region depends *continuously* on the system parameters or not is examined. In particular, this is done for *compound channels*, in which the users know only that the true channel realization is constant for the whole duration of transmission and this comes from a pre-specified uncertainty set. The secrecy capacity region of the compound BCC is shown to be robust in the sense that it is a continuous function of the uncertainty set. This means that small variations in the uncertainty set result in small variations in secrecy capacity.

R.F. Schaefer (✉) · H.V. Poor
Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA
e-mail: rafaelfs@princeton.edu

H.V. Poor
e-mail: poor@princeton.edu

A. Grigorescu · H. Boche
Lehrstuhl für Theoretische Informationstechnik, Technische Universität München, 80333 Munchen, Germany
e-mail: andrea.grigorescu@tum.de

H. Boche
e-mail: boche@tum.de

M. Baldi and S. Tomasin (eds.), *Physical and Data-Link Security Techniques for Future Communication Systems*, Lecture Notes in Electrical Engineering 358, DOI 10.1007/978-3-319-23609-4_5

5.1 Introduction

Error correction and data encryption are usually strictly separated in current communication systems. While error correction is typically realized at the physical layer transforming the unreliable communication channel into a reliable bit-pipe, data encryption is done on top of that with the help of cryptographic principles. A drawback of this approach is its reliance on the assumption of insufficient computational capabilities of non-legitimate receivers.

Nowadays, *information theoretic approaches to security* are intensively discussed to complement such cryptographic techniques. By taking the properties of the noisy communication channel into account, information theoretic approaches establish reliable communication and data confidentiality jointly at the physical layer. Information theoretic security was initiated by Shannon [36] and continued by Wyner, who introduced the now-popular wiretap channel in [39]. Subsequently, this was generalized to the broadcast channel with confidential messages (BCC) by Csiszár and Körner [14]. This area of research provides a promising approach to achieve unconditional security and to embed secure communication into wireless networks. It is not surprising that it has drawn considerable attention recently; see for example [7, 22, 27, 28, 32, 40] and references therein. Accordingly, it has also been identified by operators and national agencies as a key technique for future secure communication systems [16, 18, 21].

Wireless communication systems are inherently vulnerable to eavesdropping due to the open nature of the wireless medium. Indeed, transmitted signals are received by intended users but are easily eavesdropped upon by non-legitimate receivers. These observations make the above discussed studies particularly crucial for wireless systems. However, many of the previous works lack in practical relevance as they usually assume perfect knowledge of all channels (including those to potential eavesdroppers). But practical systems will always be limited in channel state information (CSI) due to the nature of the wireless medium and estimation/feedback inaccuracy. Moreover, malevolent eavesdroppers will not share any channel information with the legitimate users making eavesdropping even harder. Accordingly, limited CSI must be assumed to ensure reliability and confidentiality.

In this chapter, the concept of *compound channels* [5, 38] is considered, which makes a first step in the direction of more realistic CSI assumptions. In this model, the actual channel realization is assumed to be unknown. The users know only that the true channel realization belongs to a known uncertainty set and that this realization remains constant for the entire duration of transmission. Secure communication over compound wiretap channels has been studied in [4, 17, 23, 26, 34, 35]. Despite all these efforts, a general single-letter characterization of the secrecy capacity remains unknown (if it exists at all). Such a description has been found only for certain special cases such as degraded channels or certain MIMO channels.

In this chapter, the *compound broadcast channel with confidential messages (BCC)* is considered. In this communication problem, a transmitter aims to send a common message to two receivers and, at the same time, a confidential message

to only one of them keeping the other receiver in the dark. This channel provides a useful model for studying wireless networks involving both multicast and unicast messages, such as subscription content-delivery systems. First studies can be found in [24, 33] and, similarly to the compound wiretap channel, a general single-letter characterization of the secrecy capacity region remains unknown. Only a multi-letter description has been established so far.

The following analysis is motivated by the observation that the performance of a communication system should depend *continuously* on its system parameters. In the context of compound BCCs, this means that small variations in the uncertainty set should only lead to small variations in the secrecy capacity; i.e., that the system will be *robust* to the uncertainty. Since otherwise, if small changes would lead to dramatic losses in performance, the approach at hand will most likely not be used. Surprisingly, the question of continuity of capacities is rarely discussed. Some work for the compound wiretap channel and arbitrarily varying wiretap channel can be found in [10, 11].

The aim of this work is to extend these concepts and ideas to the compound BCC. For this purpose, the compound BCC is introduced in Sect. 5.2 and a distance concept to measure how "close" two compound BCCs are in Sect. 5.3. The main contribution of this work is then that the secrecy capacity region of the compound BCC is continuous in the uncertainty set. This shows that small variations in the uncertainty set only lead to small variations in the secrecy capacity. Finally, a concluding discussion is given in Sect. 5.4. Parts of this work have been presented before in [20].

Notation

Discrete random variables are denoted by capital letters and their realizations and ranges by lower case and script letters, respectively; all information quantities and logarithms are taken to the base 2; $\mathbb{N}$ and $\mathbb{R}_+$ denote the sets of non-negative integers and non-negative real numbers; $(0, 1)$ and $[0, 1]$ denote open and closed intervals between 0 and 1; $H(\cdot)$, $H_2(\cdot)$, $I(\cdot;\cdot)$ are the entropy, binary entropy, and mutual information, respectively; $X - Y - Z$ denotes a Markov chain of random variables X, Y, and Z in this order; the set of all probability distributions is denoted by $\mathscr{P}(\cdot)$; $\overline{\text{conv}}(\cdot)$ denotes the convex hull closure; $\|\nu - \mu\| =: \sum_{a\in\mathscr{A}} |\nu(a) - \mu(a)|$ is the total variation distance of measures μ and ν on $\mathscr{A}$; lhs =: rhs means the value of the right hand side (rhs) is assigned to the left hand side (lhs); lhs := rhs is defined accordingly.

5.2 Compound Broadcast Channels with Confidential Messages

In this section we introduce the *compound broadcast channel with confidential messages (BCC)* in which the actual channel realization is unknown to the transmitter and both receivers. They know only that this realization remains constant during the entire duration of transmission and belongs to a known uncertainty set.

5.2.1 Compound Broadcast Channels

Let $\mathscr{X}$, $\mathscr{Y}$, and $\mathscr{Z}$ be finite input and output alphabets of the transmitter and both receivers respectively. Let $\mathscr{S}$ be a finite state set. For each channel state $s \in \mathscr{S}$, input and output sequences $x^n \in \mathscr{X}^n$, $y^n \in \mathscr{Y}^n$, and $z^n \in \mathscr{Z}^n$ of length n, the discrete memoryless broadcast channel is given by $P^n_{YZ|X,s}(y^n, z^n|x^n) =: \prod_{i=1}^n P_{YZ|X,s}(y_i, z_i|x_i)$. Since there is no cooperation allowed between receiver 1 and 2, it suffices to consider the marginal channels only which are denoted by $W^n_s(y^n|x^n) =: \prod_{i=1}^n W_s(y_i|x_i)$ and $V^n_s(z^n|x^n) =: \prod_{i=1}^n V_s(z_i|x_i)$ respectively.

This allows us to define the marginal compound channels to both receivers by the families of channels for all $s \in \mathscr{S}$ as

$$\mathscr{W} =: \{W_s : s \in \mathscr{S}\} \quad \text{and} \quad \mathscr{V} =: \{V_s : s \in \mathscr{S}\}.$$

Definition 5.1 The discrete memoryless *compound broadcast channel* $\mathfrak{W}$ is given by the families of pairs of compound channels with common input as

$$\mathfrak{W} =: \{\mathscr{W}, \mathscr{V}\} = \{(W_s, V_s) : W_s \in \mathscr{W}, V_s \in \mathscr{V}\}.$$

Remark 5.1 In what follows we will call $\mathfrak{W}$ also the uncertainty set of the compound BCC. In [10, Sect. II-B] it is discussed why it is reasonable to specify the uncertainty set by the set of channel matrices $(\mathscr{W}, \mathscr{V})$ and not by the state set $\mathscr{S}$ itself. Indeed, two compound channels can be "close" in their set of channel matrices although their state sets may differ considerably.

5.2.2 Codes for Compound BCCs

In the communication problem at hand, the transmitter sends over the compound BCC simultaneously a common message M_0 to both receivers and a confidential message M_1 to receiver 1, which must be kept secret from receiver 2. The corresponding compound BCC is depicted in Fig. 5.1.

We consider a block code of arbitrary but fixed length n. Let $\mathscr{M}_0 =: \{1, \ldots, M_{0,n}\}$ be the set of common messages and $\mathscr{M}_1 =: \{1, \ldots, M_{1,n}\}$ the set of confidential messages. We frequently make use of the abbreviation $\mathscr{M} =: \mathscr{M}_0 \times \mathscr{M}_1$.

Definition 5.2 An $(n, M_{0,n}, M_{1,n})$-*code* for the compound BCC consists of a stochastic encoder at the transmitter

$$E : \mathscr{M}_0 \times \mathscr{M}_1 \to \mathscr{P}(\mathscr{X}^n), \tag{5.1}$$

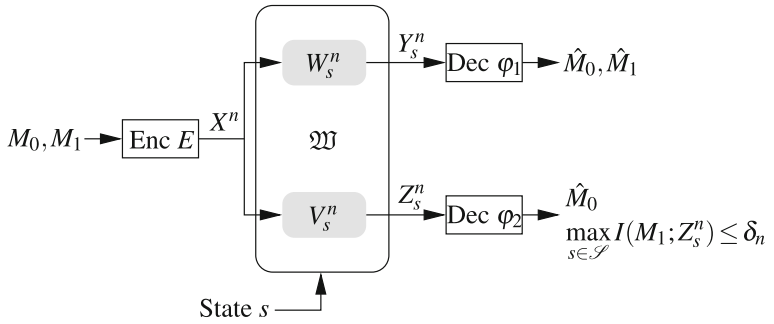

Fig. 5.1 Compound broadcast channel with confidential messages. The transmitter encodes messages M_0 and M_1 into a codeword $X^n = E(M_0, M_1)$ and transmits it over the compound BCC to the receivers, which have to decode their intended messages $(\hat{M}_0, \hat{M}_1) = \varphi_1(Y_s^n)$ and $\hat{M}_0 = \varphi_2(Z_s^n)$ for any channel realization $s \in \mathscr{S}$. At the same time, the second receiver has to be kept ignorant of M_1 in the sense that $\max_{s\in\mathscr{S}} I(M_1; Z_s^n) \le \delta_n$

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

$$\varphi_1 \colon \mathscr{Y}^n \to \mathscr{M}_0 \times \mathscr{M}_1 \tag{5.2a}$$

$$\varphi_2 \colon \mathscr{Z}^n \to \mathscr{M}_0. \tag{5.2b}$$

Remark 5.2 Note that since the actual channel realization is unknown to the transmitter and both receivers, the encoder (5.1) and decoders (5.2) must not depend on the state $s \in \mathscr{S}$ (and therewith not the particular (W_s, V_s)), i.e., they must be universal with respect to the state set $\mathscr{S}$ (and uncertainty set $\mathfrak{W}$).

When the transmitter has sent the message pair $m = (m_0, m_1) \in \mathscr{M}$ and the receivers have received $y^n \in \mathscr{Y}^n$ and $z^n \in \mathscr{Z}^n$, their decoders are in error if $\varphi_1(y^n) \neq (m_0, m_1)$ or $\varphi_2(z^n) \neq m_0$. Then for an $(n, M_{0,n}, M_{1,n})$-code of Definition 5.2, the average probabilities of decoding error for receivers 1 and 2 and channel realization $s \in \mathscr{S}$ are

$$\overline{e}_{1,n}(s) := \frac{1}{|\mathscr{M}|} \sum_{m\in\mathscr{M}} \sum_{x^n\in\mathscr{X}^n} \sum_{y^n:\varphi_1(y^n)\neq(m_0,m_1)} W_s^n(y^n|x^n) E(x^n|m_0, m_1)$$

$$\overline{e}_{2,n}(s) := \frac{1}{|\mathscr{M}|} \sum_{m\in\mathscr{M}} \sum_{x^n\in\mathscr{X}^n} \sum_{z^n:\varphi_2(z^n)\neq m_0} V_s^n(z^n|x^n) E(x^n|m_0, m_1).$$

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

The confidential message M_1 has to be kept secret from receiver 2 for all channel realizations $s \in \mathscr{S}$. Therefore, we require $\max_{s\in\mathscr{S}} I(M_1; Z_s^n) \le \delta_n$ for some $\delta_n > 0$ with M_1 the random variable uniformly distributed over the set $\mathscr{M}_1$ and $Z_s^n = (Z_{s,1}, Z_{s,2}, \ldots, Z_{s,n})$ the output at receiver 2 for the channel realization $s \in \mathscr{S}$.

This criterion is known as *strong secrecy* [13, 29] and the intuition is to control the total amount of information leaked to the non-legitimate receiver. This leads to the following definition.

Definition 5.3 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 $\frac{1}{n} \log M_{0,n} \geq R_0 - \tau, \frac{1}{n} \log M_{1,n} \geq R_1 - \tau$,

$$\max_{s \in \mathscr{S}} \left\{ \bar{e}_{1,n}(s), \bar{e}_{2,n}(s) \right\} \leq \lambda_n,$$

and

$$\max_{s \in \mathscr{S}} I(M_1; Z_s^n) \leq \delta_n \tag{5.3}$$

with $\lambda_n, \delta_n \to 0$ as $n \to \infty$.

The closure of the set of all achievable rate pairs (R_0, R_1) is the *secrecy capacity region* $\mathscr{C}_S(\mathfrak{W})$ of the compound BCC $\mathfrak{W}$.

Remark 5.3 One might argue that the secrecy criterion (5.3) should reflect the fact that the common message M_0 is available at receiver 2 as side information. In [33] it has been shown that incorporating this type of side information does not change the secrecy capacity. Accordingly, (5.3) can be generalized to $\max_{s \in \mathscr{S}} I(M_1; Z_s^n | M_0) \leq \delta_n$ (or equivalently to $\max_{s \in \mathscr{S}} I(M_1; M_0, Z_s^n) \leq \delta_n$ if M_0 and M_1 are independent) at no cost.

5.2.3 Capacity Results

The discrete memoryless compound BCC has been studied in [19, 33]. In [33] an achievable secrecy rate region and a multi-letter outer bound have been established. Based on this, [19] presents a precise multi-letter characterization of the corresponding secrecy capacity region.

Proposition 5.1 ([33, Theorem 2]) *An achievable secrecy rate region for the compound BCC $\mathfrak{W}$ is given by the set of all rate pairs $(R_0, R_1) \in \mathbb{R}_+^2$ that satisfy*

$$\begin{aligned} R_0 &\leq \min_{s \in \mathscr{S}} \min \left\{ I(U; Y_s), I(U; Z_s) \right\} \\ R_1 &\leq \min_{s \in \mathscr{S}} I(V; Y_s | U) - \max_{s \in \mathscr{S}} I(V; Z_s | U) \end{aligned}$$

for random variables $U - V - X - (Y_s, Z_s)$ forming a Markov chain with Y_s and Z_s the random variables associated with the outputs of the channels W_s and V_s.

Furthermore, the generalized secrecy criterion (cf. Remark 5.3) goes exponentially fast to zero and the decoding error of the confidential message M_1 at the non-legitimate receiver 2 goes exponentially fast to one.

A single-letter expression for the secrecy capacity region is still unknown (if it exists at all). However, a multi-letter outer bound has been established in [33, Theorem 3] which yields a multi-letter description of $\mathscr{C}_S(\mathfrak{W})$ of the compound BCC $\mathfrak{W}$ in [19]. For this purpose, let $n \in \mathbb{N}$ be arbitrary but fixed and we define the rate region $\mathscr{R}_n(\mathfrak{W}, U, V, X^n)$ as the set of all rate pairs $(R_0, R_1) \in \mathbb{R}_+^2$ that satisfy

$$R_0 \leq \frac{1}{n} \inf_{s\in\mathscr{S}} \min\left\{I(U; Y_s^n), I(U; Z_s^n)\right\} \tag{5.4a}$$

$$R_1 \leq \frac{1}{n}\Big(\inf_{s\in\mathscr{S}} I(V; Y_s^n|U) - \sup_{s\in\mathscr{S}} I(V; Z_s^n|U)\Big) \tag{5.4b}$$

for random variables satisfying the Markov chain relationship $U - V - X^n - (Y_s^n, Z_s^n)$. Then, we define the region

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

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

Theorem 5.1 ([19]) *The secrecy capacity region $\mathscr{C}_S(\mathfrak{W})$ of the compound BCC $\mathfrak{W}$ is the convex hull closure of the union of the regions $\overline{\mathscr{R}}_n(\mathfrak{W})$ over all $n \in \mathbb{N}$, i.e.,*

$$\mathscr{C}_S(\mathfrak{W}) = \overline{\text{conv}}\Big(\bigcup_{n\in\mathbb{N}} \overline{\mathscr{R}}_n(\mathfrak{W})\Big). \tag{5.5}$$

Remark 5.4 The union of the rate regions $\bigcup_{n\in\mathbb{N}} \overline{\mathscr{R}}_n(\mathfrak{W})$ may itself not be convex, which necessitates the convex hull in (5.5). Note that all rate pairs in the convex hull can be achieved by time sharing between rate pairs in $\overline{\mathscr{R}}_n(\mathfrak{W})$.

5.3 Continuity of the Compound Secrecy Capacity Region

In this section we analyze the secrecy capacity region $\mathscr{C}_S(\mathfrak{W})$ of the compound BCC $\mathfrak{W}$. The main result will be that $\mathscr{C}_S(\mathfrak{W})$ depends in a *continuous* way on the uncertainty set $\mathfrak{W}$. To do so, we need a suitable concept to measure the distance between two compound BCCs. This is introduced first.

5.3.1 Distance Between Compound BCCs

Let (W, V) and $(\widetilde{W}, \widetilde{V})$ be two broadcast channels with finite input and output alphabets $\mathscr{X}$, $\mathscr{Y}$, and $\mathscr{Z}$. We define the distance between the two marginal channels (to receivers 1 and 2 respectively) based on the total variation distance[1] as

$$d(W, \widetilde{W}) =: \max_{x \in \mathscr{X}} \sum_{y \in \mathscr{Y}} \left| W(y|x) - \widetilde{W}(y|x) \right|$$
$$d(V, \widetilde{V}) =: \max_{x \in \mathscr{X}} \sum_{z \in \mathscr{Z}} \left| V(z|x) - \widetilde{V}(z|x) \right|$$

and the distance between two BCs as

$$d\big((W, V), (\widetilde{W}, \widetilde{V})\big) =: \max\big\{d(W, \widetilde{W}), d(V, \widetilde{V})\big\}.$$

To extend this concept to compound BCs, let $\mathfrak{W}_1 = \{(W_{s_1}, V_{s_1}) \colon s_1 \in \mathscr{S}_1\}$ and $\mathfrak{W}_2 = \{(W_{s_2}, V_{s_2}) \colon s_2 \in \mathscr{S}_2\}$ be two finite compound BCs with marginal compound channels $\mathscr{W}_i = \{W_{s_i} \colon s_i \in \mathscr{S}_i\}$ and $\mathscr{V}_i = \{V_{s_i} \colon s_i \in \mathscr{S}_i\}$ for $i \in \{1, 2\}$. We define the distance between two marginal compound channels to receiver 1 as

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

and to receiver 2 as

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

Definition 5.4 Let $\mathfrak{W}_1$ and $\mathfrak{W}_2$ be two compound BCs. The distance $D(\mathfrak{W}_1, \mathfrak{W}_2)$ between $\mathfrak{W}_1$ and $\mathfrak{W}_2$ is then defined as

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

This concept is suitable to characterize how "close" two compound BCs are. In addition, it can also be used to quantify how well one compound BC approximates another one.

Finally, to compare different rate regions, we define a distance between two sets as follows.

[1] Note that the distance can also be defined based on another norm. This follows from the fact that the output alphabets $\mathscr{Y}$ and $\mathscr{Z}$ are finite. A norm other than the total variation distance would only result in slightly different constants.

Definition 5.5 Let $\mathscr{R}_1$, and $\mathscr{R}_2$ be two non-empty compact subsets of the metric space $(\mathbb{R}_+^2, d)$ with $d(x^2, y^2) = \sum_{i=1}^2 |x_i - y_i|$ for all $x^2 = (x_1, x_2)$ and $y^2 = (y_1, y_2)$. We define the distance between two sets as

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

5.3.2 Continuity of the Secrecy Capacity Region

Now we are in the position to study the behavior of the secrecy capacity of the compound BCC. In particular, we are interested in the question of what happens if there are variations in the uncertainty set. Obviously, one is interested in a *continuous* behavior of the secrecy capacity. Since small changes in the uncertainty set should only lead to small changes in the corresponding secrecy capacity region.

For the following analysis, we need some technical results stated in the following. Similar results appeared first in the area of quantum information theory [2, 25] and have recently been extended to the compound wiretap channel in [10, 11].

The following lemma is also stated in [10, 11].

Lemma 5.1 *Let $\mathscr{X}$ and $\mathscr{Y}$ be finite alphabets and $\varepsilon \in (0, 1)$ be arbitrary. Further, let (X, Y) and $(\tilde{X}, \tilde{Y})$ be random variables according to joint probability distributions $P_{XY}, P_{\tilde{X}\tilde{Y}} \in \mathscr{P}(\mathscr{X} \times \mathscr{Y})$ with $\|P_{XY} - P_{\tilde{X}\tilde{Y}}\| \leq \varepsilon$. It holds that*

$$\big|H(Y|X) - H(\tilde{Y}|\tilde{X})\big| \leq \delta_1(\varepsilon, |\mathscr{Y}|) \tag{5.6}$$

with $\delta_1(\varepsilon, |\mathscr{Y}|) =: 2\varepsilon \log |\mathscr{Y}| + 2H_2(\varepsilon)$.

Proof The proof follows the idea of [2] for quantum sources. We obtain sharper constants by considering classical probability distributions only in this work. For completeness, the details can be found in the appendix. □

Lemma 5.2 *Let $\mathscr{X}$ and $\mathscr{Y}$ be finite alphabets and $W, \widetilde{W} \colon \mathscr{X} \to \mathscr{P}(\mathscr{Y})$ be arbitrary channels with*

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

for some $\varepsilon > 0$. For an arbitrary $n \in \mathbb{N}$, let $\mathscr{U}$ and $\mathscr{V}$ be two finite sets, $P_U \in \mathscr{P}(\mathscr{U})$ the uniform distribution of U, $P_{V|U} : \mathscr{U} \to \mathscr{P}(\mathscr{V})$ the conditional distribution of V given U and $E(x^n|v)$, $x^n \in \mathscr{X}^n$ conditioned on $v \in \mathscr{V}$, an arbitrary stochastic encoder. We consider the probability distributions

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

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

Then it holds that

$$\left|I(V;Y^n|U) - I(V;\tilde{Y}^n|U)\right| \leq n\delta_2(\varepsilon, |\mathscr{Y}|) \tag{5.7}$$

with $\delta_2(\varepsilon, |\mathscr{Y}|) =: 4\varepsilon \log |\mathscr{Y}| + 4H_2(\varepsilon)$.

Proof The proof is an adaptation of the proof in [10, 11] for the compound wiretap channel (which itself goes back to a proof idea in [25] for quantum capacities). The details can be found in the appendix. □

Remark 5.5 Note that the right-hand side of (5.6) and (5.7) depend only on the size of the output alphabet $\mathscr{Y}$, but they are independent of the size of the auxiliary alphabets $\mathscr{U}$ and $\mathscr{V}$, the conditional distribution $P_{V|U}$, and the chosen stochastic encoder E.

The previous lemma shows that whenever two channels are close, certain conditional mutual information terms are close as well. We use this observation to prove the following result which states that two similar compound BCCs have similar corresponding secrecy rate regions, cf. (5.4).

Lemma 5.3 *Let* $\varepsilon \in (0,1)$ *and* $n \in \mathbb{N}$ *be fixed. Further, let* $\mathfrak{W}_1$ *and* $\mathfrak{W}_2$ *be two compound BCCs and* U, V, *and* X^n *be random variables satisfying the Markov chain relationship* $U - V - X^n$. *If*

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

then it holds that

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

with $\delta(\varepsilon, |\mathscr{Y}|, |\mathscr{Z}|) = \delta'(\varepsilon, |\mathscr{Y}|, |\mathscr{Z}|) + \delta''(\varepsilon, |\mathscr{Y}|, |\mathscr{Z}|)$, $\delta'(\varepsilon, |\mathscr{Y}|, |\mathscr{Z}|) =: 4H_2(\varepsilon) + 4\varepsilon \max\{\log |\mathscr{Y}|, \log |\mathscr{Z}|\}$, *and* $\delta''(\varepsilon, |\mathscr{Y}|, |\mathscr{Z}|) =: 4\varepsilon \log |\mathscr{Y}||\mathscr{Z}| + 8H_2(\varepsilon)$.

Proof For any particular choice of U, V, and X^n, the rate regions $\mathscr{R}_n(\mathfrak{W}_1, U, V, X^n)$ and $\mathscr{R}_n(\mathfrak{W}_2, U, V, X^n)$ are

$$\mathscr{R}_n(\mathfrak{W}_1, U, V, X^n) = \left\{ \begin{array}{l} R_{0,\mathscr{S}_1} \leq \frac{1}{n} \inf_{s_1 \in \mathscr{S}_1} \min\{I(U;Y^n_{s_1}), I(U;Z^n_{s_1})\} \\ R_{1,\mathscr{S}_1} \leq \frac{1}{n} \inf_{s_1 \in \mathscr{S}_1} I(V;Y^n_{s_1}|U) - \frac{1}{n} \sup_{s_1 \in \mathscr{S}_1} I(V;Z^n_{s_1}|U) \end{array} \right\}$$

and

$$\mathscr{R}_n(\mathfrak{W}_2, U, V, X^n) = \left\{ \begin{array}{l} R_{0,\mathscr{S}_2} \leq \frac{1}{n} \inf_{s_2 \in \mathscr{S}_2} \min\{I(U;Y^n_{s_2}), I(U;Z^n_{s_2})\} \\ R_{1,\mathscr{S}_2} \leq \frac{1}{n} \inf_{s_2 \in \mathscr{S}_2} I(V;Y^n_{s_2}|U) - \frac{1}{n} \sup_{s_2 \in \mathscr{S}_2} I(V;Z^n_{s_2}|U) \end{array} \right\},$$

i.e., they are rectangles described by the rates $(R_{0,\mathscr{S}_1}, R_{1,\mathscr{S}_1})$ and $(R_{0,\mathscr{S}_2}, R_{1,\mathscr{S}_2})$ satisfying (5.4a) and (5.4b) respectively.

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

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

denotes the maximum common rate and

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

the maximum confidential rate of region $\mathscr{R}_n(\mathfrak{W}_i, U, V, X^n)$, $i = 1, 2$. With this observation, the distance $D_R(\mathscr{R}_n(\mathfrak{W}_1, U, V, X^n), \mathscr{R}_n(\mathfrak{W}_2, U, V, X^n))$, cf. Definition 5.5, is

$$D_R(\mathscr{R}_n(\mathfrak{W}_1, U, V, X^n), \mathscr{R}_n(\mathfrak{W}_2, U, V, X^n)) = |A_{0,\mathscr{S}_1} - A_{0,\mathscr{S}_2}| + |A_{1,\mathscr{S}_1} - A_{1,\mathscr{S}_2}|. \tag{5.8}$$

Thus, it remains to evaluate both terms on the right hand side of (5.8), i.e., the difference between the maximum common rates $|A_{0,\mathscr{S}_1} - A_{0,\mathscr{S}_2}|$ and the difference between the maximum confidential rates $|A_{1,\mathscr{S}_1} - A_{1,\mathscr{S}_2}|$.

Common Message Rate

From (5.4a) we see that there are four cases that may occur:

1. $A_{0,\mathscr{S}_1} = \frac{1}{n} \inf_{s_1 \in \mathscr{S}_1} I(U; Y_{s_1}^n)$ and $A_{0,\mathscr{S}_2} = \frac{1}{n} \inf_{s_2 \in \mathscr{S}_2} I(U; Y_{s_2}^n)$
2. $A_{0,\mathscr{S}_1} = \frac{1}{n} \inf_{s_1 \in \mathscr{S}_1} I(U; Z_{s_1}^n)$ and $A_{0,\mathscr{S}_2} = \frac{1}{n} \inf_{s_2 \in \mathscr{S}_2} I(U; Z_{s_2}^n)$
3. $A_{0,\mathscr{S}_1} = \frac{1}{n} \inf_{s_1 \in \mathscr{S}_1} I(U; Y_{s_1}^n)$ and $A_{0,\mathscr{S}_2} = \frac{1}{n} \inf_{s_2 \in \mathscr{S}_2} I(U; Z_{s_2}^n)$
4. $A_{0,\mathscr{S}_1} = \frac{1}{n} \inf_{s_1 \in \mathscr{S}_1} I(U; Z_{s_1}^n)$ and $A_{0,\mathscr{S}_2} = \frac{1}{n} \inf_{s_2 \in \mathscr{S}_2} I(U; Y_{s_2}^n)$.

In the following we treat these cases individually. For the first case, we have

$$\left| A_{0,\mathscr{S}_1} - A_{0,\mathscr{S}_2} \right| = \left| \frac{1}{n} \inf_{s_1 \in \mathscr{S}_1} I(U; Y_{s_1}^n) - \frac{1}{n} \inf_{s_2 \in \mathscr{S}_2} I(U; Y_{s_2}^n) \right|. \tag{5.9}$$

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

$$\inf_{s_1 \in \mathscr{S}_1} I(U; Y_{s_1}^n) \geq I(U; Y_{\hat{s}_1}^n) - \eta. \tag{5.10}$$

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

$$d(W_{\hat{s}_1}, W_{\hat{s}_2}) < \varepsilon. \tag{5.11}$$

We can now apply Lemma 5.2 (with U in (5.7) of Lemma 5.2 being constant and U in (5.9) taking the role of V in (5.7) of Lemma 5.2). By (5.11), we then have

$$\left| I(U; Y_{\hat{s}_1}^n) - I(U; Y_{\hat{s}_2}^n) \right| \leq n\delta_2(\varepsilon, |\mathscr{Y}|). \tag{5.12}$$

Combining (5.10) and (5.12) we obtain

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

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

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

By changing the roles of $\mathscr{S}_1$ and $\mathscr{S}_2$ in the previous derivation, we also get $\inf_{s_2 \in \mathscr{S}_2} I(U; Y_{s_2}^n) > \inf_{s_1 \in \mathscr{S}_1} I(U; Y_{s_1}^n) - n\delta_2(\varepsilon, |\mathscr{Y}|)$ so that

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

Using the same line of argument as for the first case above, we accordingly have for the second case

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

In the third and fourth case, one maximum common rate depends on Y and the other on Z. For the third case, we have

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

This necessitates further case studies and we have six possibilities to relate the two previous inequalities:

1. $B_{0_{\mathscr{S}_1}} \geq A_{0_{\mathscr{S}_1}} \geq B_{0_{\mathscr{S}_2}} \geq A_{0_{\mathscr{S}_2}}$ and Lemma 5.2 implies

$$|A_{0_{\mathscr{S}_1}} - A_{0_{\mathscr{S}_2}}| \leq |B_{0_{\mathscr{S}_1}} - A_{0_{\mathscr{S}_2}}| \leq \delta_2(\varepsilon, |\mathscr{Z}|)$$

2. $B_{0_{\mathscr{S}_1}} \geq B_{0_{\mathscr{S}_2}} \geq A_{0_{\mathscr{S}_1}} \geq A_{0_{\mathscr{S}_2}}$ implying

$$|A_{0_{\mathscr{S}_1}} - A_{0_{\mathscr{S}_2}}| \leq |B_{0_{\mathscr{S}_1}} - A_{0_{\mathscr{S}_2}}| \leq \delta_2(\varepsilon, |\mathscr{Z}|)$$

3. $B_{0_{\mathscr{S}_1}} \geq B_{0_{\mathscr{S}_2}} \geq A_{0_{\mathscr{S}_2}} \geq A_{0_{\mathscr{S}_1}}$ implying

$$|A_{0_{\mathscr{S}_1}} - A_{0_{\mathscr{S}_2}}| \leq |A_{0_{\mathscr{S}_1}} - B_{0_{\mathscr{S}_2}}| \leq \delta_2(\varepsilon, |\mathscr{Y}|)$$

4. $B_{0_{\mathscr{S}_2}} \geq A_{0_{\mathscr{S}_2}} \geq B_{0_{\mathscr{S}_1}} \geq A_{0_{\mathscr{S}_1}}$ implying

$$|A_{0_{\mathscr{S}_1}} - A_{0_{\mathscr{S}_2}}| \leq |A_{0_{\mathscr{S}_1}} - B_{0_{\mathscr{S}_2}}| \leq \delta_2(\varepsilon, |\mathscr{Y}|)$$

5. $B_{0_{\mathscr{S}_2}} \geq B_{0_{\mathscr{S}_1}} \geq A_{0_{\mathscr{S}_2}} \geq A_{0_{\mathscr{S}_1}}$ implying

$$|A_{0_{\mathscr{S}_1}} - A_{0_{\mathscr{S}_2}}| \leq |A_{0_{\mathscr{S}_1}} - B_{0_{\mathscr{S}_2}}| \leq \delta_2(\varepsilon, |\mathscr{Y}|)$$

6. $B_{0_{\mathscr{S}_2}} \geq B_{0_{\mathscr{S}_1}} \geq A_{0_{\mathscr{S}_1}} \geq A_{0_{\mathscr{S}_2}}$ implying

$$|A_{0_{\mathscr{S}_1}} - A_{0_{\mathscr{S}_2}}| \leq |A_{0_{\mathscr{S}_2}} - B_{0_{\mathscr{S}_1}}| \leq \delta_2(\varepsilon, |\mathscr{Z}|).$$

We can use the same line of argument for the fourth case to bound the distance between the two maximum achievable common rates. As a conclusion, it then holds for all cases that

$$\begin{aligned} |A_{0_{\mathscr{S}_1}} - A_{0_{\mathscr{S}_2}}| &\leq \max\{\delta_2(\varepsilon, |\mathscr{Y}|), \delta_2(\varepsilon, |\mathscr{Y}|)\} \\ &= 4H_2(\varepsilon) + 4\varepsilon \max\{\log|\mathscr{Y}|, \log|\mathscr{Z}|\}. \end{aligned} \tag{5.13}$$

Confidential Message Rate

It remains to evaluate the confidential message rate. Using the same line of argument as in the first case for the common message rate, we get

$$\begin{aligned} |A_{1_{\mathscr{S}_1}} - A_{1_{\mathscr{S}_2}}| &= \Big|\frac{1}{n}\inf_{s_1\in\mathscr{S}_1} I(V; Y_{s_1}^n|U) - \frac{1}{n}\sup_{s_1\in\mathscr{S}_1} I(V; Z_{s_1}^n|U) \\ &\qquad - \frac{1}{n}\inf_{s_2\in\mathscr{S}_2} I(V; Y_{s_2}^n|U) + \frac{1}{n}\sup_{s_2\in\mathscr{S}_2} I(V; Z_{s_2}^n|U)\Big| \\ &\leq \frac{1}{n}\Big|\inf_{s_1\in\mathscr{S}_1} I(V; Y_{s_1}^n|U) - \inf_{s_2\in\mathscr{S}_2} I(V; Y_{s_2}^n|U)\Big| \\ &\qquad + \frac{1}{n}\Big|\inf_{s_2\in\mathscr{S}_2} I(V; Z_{s_2}^n|U) - \inf_{s_1\in\mathscr{S}_1} I(V; Z_{s_1}^n|U)\Big| \\ &\leq \delta_2(\varepsilon, |\mathscr{Y}|) + \delta_2(\varepsilon, |\mathscr{Z}|) \\ &\leq 4\varepsilon \log|\mathscr{Y}||\mathscr{Z}| + 8H_2(\varepsilon). \end{aligned} \tag{5.14}$$

Putting (5.13) and (5.14) together yields the desired result proving the lemma. □

Now we are in a position to state and prove the main result of this work. The following theorem shows that whenever two compound BCCs are close, their corresponding secrecy capacity regions are close as well.

Theorem 5.2 *Let $\varepsilon \in (0, 1)$. Let $\mathfrak{W}_1$ and $\mathfrak{W}_2$ be two compound BCCs. If*

$$D(\mathfrak{W}_1, \mathfrak{W}_2) \leq \varepsilon, \tag{5.15}$$

then it holds that

$$D_R(\mathscr{C}_S(\mathfrak{W}_1), \mathscr{C}_S(\mathfrak{W}_2)) \leq \delta(\varepsilon, |\mathscr{Y}|, |\mathscr{Z}|).$$

Proof For any choice of random variables U, V, and X^n satisfying the Markov chain relationship $U - V - X^n$, we define the sets $\mathscr{D}_1, \mathscr{B}_1 \subset \mathbb{R}_+^2$ as

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

so that $\mathscr{D}_1 \cup \mathscr{B}_1 = \mathscr{C}_S(\mathfrak{W}_1)$. Now, let $(R_{0_{\mathscr{S}_1}}, R_{1_{\mathscr{S}_1}}) \in \mathscr{D}_1$. Then there exists an $n \in \mathbb{N}$ and random variables $\hat{U}$, $\hat{V}$, and $\hat{X}^n$ satisfying the Markov chain relationship $\hat{U} - \hat{V} - \hat{X}^n$ such that $(R_{0_{\mathscr{S}_1}}, R_{1_{\mathscr{S}_1}}) \in \mathscr{R}_n(\mathfrak{W}_1, \hat{U}, \hat{V}, \hat{X}^n)$. From Lemma 5.3 and (5.15) it then follows that

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

This means that there exists a rate pair

$$(R_{0_{\mathscr{S}_2}}(R_{0_{\mathscr{S}_1}}), R_{1_{\mathscr{S}_2}}(R_{1_{\mathscr{S}_1}})) \in \mathscr{R}_n(\mathfrak{W}_2, \hat{U}, \hat{V}, \hat{X}^n)$$

such that

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

Now, for any rate pair $(\hat{R}_{0_{\mathscr{S}_1}}, \hat{R}_{1_{\mathscr{S}_1}}) \in \mathscr{B}_1$, there exist two rate pairs

$$(\dot{R}_{0_{\mathscr{S}_1}}, \dot{R}_{1_{\mathscr{S}_1}}), (\tilde{R}_{0_{\mathscr{S}_1}}, \tilde{R}_{1_{\mathscr{S}_1}}) \in \mathscr{D}_1$$

such that

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

for some $\lambda \in (0,1)$. Now, for each $(\dot{R}_{0_{\mathscr{S}_1}}, \dot{R}_{1_{\mathscr{S}_1}})$ and $(\tilde{R}_{0_{\mathscr{S}_1}}, \tilde{R}_{1_{\mathscr{S}_1}})$ there exist random variables $\dot{U}$, $\dot{V}$, $\dot{X}^n$ $\tilde{U}$, $\tilde{V}$, and $\tilde{X}^n$ satisfying the Markov chain relations $\dot{U} - \dot{V} - \dot{X}^n$ and $\tilde{U} - \tilde{V} - \tilde{X}^n$ such that $(\dot{R}_{0_{\mathscr{S}_1}}, \dot{R}_{1_{\mathscr{S}_1}}) \in \mathscr{R}_n(\mathfrak{W}_1, \dot{U}, \dot{V}, \dot{X}^n)$ and $(\tilde{R}_{0_{\mathscr{S}_1}}, \tilde{R}_{1_{\mathscr{S}_1}}) \in \mathscr{R}_n(\mathfrak{W}_1, \tilde{U}, \tilde{V}, \tilde{X}^n)$. Then from Lemma 5.3 and (5.15) we have that there exist rate pairs $(\dot{R}_{0_{\mathscr{S}_2}}(\dot{R}_{0_{\mathscr{S}_1}}), \dot{R}_{1_{\mathscr{S}_2}}(\dot{R}_{1_{\mathscr{S}_1}})) \in \mathscr{R}_n(\mathfrak{W}_2, \dot{U}, \dot{V}, \dot{X}^n)$ and $(\tilde{R}_{0_{\mathscr{S}_2}}(\tilde{R}_{0_{\mathscr{S}_1}}), \tilde{R}_{1_{\mathscr{S}_2}}(\tilde{R}_{1_{\mathscr{S}_1}})) \in \mathscr{R}_n(\mathfrak{W}_2, \tilde{U}, \tilde{V}, \tilde{X}^n)$ such that

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

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

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

In addition, we have

$$
\begin{aligned}
|\hat{R}_{0_{\mathscr{S}_1}} - \hat{R}_{0_{\mathscr{S}_2}}| &= |\lambda \dot{R}_{0_{\mathscr{S}_2}} + (1-\lambda)\tilde{R}_{0_{\mathscr{S}_2}} - \lambda \dot{R}_{0_{\mathscr{S}_1}} + (1-\lambda)\tilde{R}_{0_{\mathscr{S}_1}}| \\
&\leq \lambda |\dot{R}_{0_{\mathscr{S}_1}} - \dot{R}_{0_{\mathscr{S}_2}}| + (1-\lambda)|\tilde{R}_{0_{\mathscr{S}_1}} - \tilde{R}_{0_{\mathscr{S}_2}}| \\
&\leq \delta'(\varepsilon, |\mathscr{Y}|, |\mathscr{Z}|) \qquad (5.16)
\end{aligned}
$$

and similarly

$$
|\hat{R}_{1_{\mathscr{S}_1}} - \hat{R}_{1_{\mathscr{S}_2}}| \leq \delta''(\varepsilon, |\mathscr{Y}|, |\mathscr{Z}|). \qquad (5.17)
$$

Now (5.16) and (5.17) results in

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

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

$$
|R_{0_{\mathscr{S}_1}} - R_{0_{\mathscr{S}_2}}| + |R_{1_{\mathscr{S}_1}} - R_{1_{\mathscr{S}_2}}| \leq \delta(\varepsilon, |\mathscr{Y}|, |\mathscr{Z}|). \qquad (5.18)
$$

Similarly, we can use the same line of argument to show the other direction: for every rate pair $(R_{0_{\mathscr{S}_2}}, R_{1_{\mathscr{S}_2}}) \in \mathscr{C}_S(\mathfrak{W}_2)$ there is a rate pair $(R_{0_{\mathscr{S}_1}}(R_{0_{\mathscr{S}_2}}), R_{1_{\mathscr{S}_1}}(R_{1_{\mathscr{S}_2}})) \in \mathscr{C}_S(\mathfrak{W}_1)$ such that (5.18) holds. This completes the proof. □

5.4 Discussion

This work was motivated by the question as to whether the secrecy capacity region of the compound BCC 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 only to small changes in the secrecy capacity region. The continuous behavior of the secrecy capacity is a necessary condition for the existence of codes that are robust against small variations in the uncertainty set, since otherwise, a discontinuous behavior of the secrecy capacity would immediately rule out the existence of robust codes. For future work, a detailed analysis of such robust codes is the next step for making this concept interesting for practical applications.

For compound channels the true channel realization is unknown. However, a crucial assumption is that it remains constant for the entire duration of transmission. Weakening this assumption leads to the concept of *arbitrarily varying channels (AVCs)* [1, 6, 15], in which the channel realization is allowed to vary in an unknown and arbitrary manner from channel use to channel use. The corresponding *arbitrarily varying wiretap channel (AVWC)* has been studied in [3, 8–12, 30, 31, 37] and interesting phenomena appear. In contrast to the compound wiretap channel, it now matters whether traditional deterministic/unassisted codes with pre-specified encoder and decoder are used, or more sophisticated codes, where the choice of encoder and decoder is coordinated based on coordination resources such as common randomness available to all users. There are situations in which the traditional approach leads to zero capacity, while the coordinated approach yields a positive capacity. Moreover, the unassisted secrecy capacity of the AVWC turns out to be discontinuous in the uncertainty set [10, 11], while common randomness allows recovering of the continuous dependence of the secrecy capacity on the uncertainty set [31, 37]. As a first step, in [19, 20] it has been demonstrated that the unassisted secrecy capacity region of the arbitrarily varying BCC depends on the uncertainty set in a discontinuous way. But it is an interesting and open question to find a complete characterization of this behavior (as in [31, 37] for the AVWC).

Acknowledgments This work of R. F. Schaefer was supported by the German Research Foundation (DFG) under Grant WY 151/2-1. This work of A. Grigorescu was supported by the German Research Foundation (DF) under Grant BO 1734/20-1. This work of H. Boche was supported by the German Ministry of Education and Research (BMBF) under Grants 01BQ1050 and 16KIS0118. This work of H. V. Poor was supported by the U.S. National Science Foundation under Grant CMMI-1435778.

Appendix

The following proofs of Lemmas 5.1 and 5.2 are adaptations of [2] and [25] where similar results were proved in the context of quantum information theory. However, we obtain bounds with better constants by restricting the analysis to classical probability distributions only.

Proof of Lemma 5.1

The proof of this lemma can also be found in [10, 11] and is given here for completeness. It follows [2] where a similar result is presented in the context of quantum information. However, we are able to get a better constant by using the fact that $H(Y|X) \geq 0$ for all $P_{XY} \in \mathscr{P}(\mathscr{X} \times \mathscr{Y})$. This is in contrast to the quantum version in [2].

Let $P_{XY}, P_{\tilde{X}\tilde{Y}} \in \mathscr{P}(\mathscr{X} \times \mathscr{Y})$ be joint probability distributions with $\|P_{XY} - P_{\tilde{X}\tilde{Y}}\| \leq \varepsilon$. We assume that

$$\sum_{x\in\mathscr{X}} \sum_{y\in\mathscr{Y}} \left|P_{XY}(x,y) - P_{\tilde{X}\tilde{Y}}(x,y)\right| = \varepsilon \tag{5.19}$$

is satisfied with equality since otherwise ε in (5.19) could be replaced with a smaller $\tilde{\varepsilon} < \varepsilon$ accordingly.

We define the function

$$f(x,y) =: \left|P_{XY}(x,y) - P_{\tilde{X}\tilde{Y}}(x,y)\right| \tag{5.20}$$

and set

$$p^*(x,y) = (1-\varepsilon)P_{XY}(x,y) + f(x,y)$$

for all $(x,y) \in \mathscr{X} \times \mathscr{Y}$ so that $p^* \in \mathscr{P}(\mathscr{X}, \mathscr{Y})$ is a joint probability distribution on $\mathscr{X} \times \mathscr{Y}$.

Further, we set

$$\hat{p}(x,y) = \frac{1}{\varepsilon} f(x,y), \tag{5.21a}$$

and

$$\hat{q}(x,y) = \frac{1}{\varepsilon}\big((1-\varepsilon)\big[P_{XY}(x,y) - P_{\tilde{X}\tilde{Y}}(x,y)\big] + f(x,y)\big). \tag{5.21b}$$

Next we check that $\hat{p}$ and $\hat{q}$ are well defined such that they are indeed probability distributions. $\hat{p}(x,y) \geq 0$ for all $(x,y) \in \mathscr{X} \times \mathscr{Y}$ is obviously true. It remains to verify that $\hat{q}(x,y) \geq 0$ for all $(x,y) \in \mathscr{X} \times \mathscr{Y}$ is also satisfied.

If $P_{XY}(x,y) \leq P_{\tilde{X}\tilde{Y}}(x,y)$, then

$$\begin{aligned} -f(x,y) &\leq P_{XY}(x,y) - P_{\tilde{X}\tilde{Y}}(x,y) \\ &\leq (1-\varepsilon)\big(P_{XY}(x,y) - P_{\tilde{X}\tilde{Y}}(x,y)\big) \\ &\leq 0 \end{aligned}$$

so that $\hat{q}(x, y) \geq 0$. On the other hand, if $P_{XY}(x, y) > P_{\tilde{X}\tilde{Y}}(x, y)$, then

$$\begin{aligned} 0 &< (1-\varepsilon)\big(P_{XY}(x, y) - P_{\tilde{X}\tilde{Y}}(x, y)\big) \\ &\leq P_{XY}(x, y) - P_{\tilde{X}\tilde{Y}}(x, y) \\ &\leq f(x, y) \end{aligned}$$

so that $\hat{q}(x, y) \geq 0$ also in this case. From the definition of $\hat{p}$ and $\hat{q}$ in (5.21) and (5.19)–(5.20) it can further easily be verified that

$$\sum_{x\in\mathscr{X}}\sum_{y\in\mathscr{Y}} \hat{p}(x, y) = \sum_{x\in\mathscr{X}}\sum_{y\in\mathscr{Y}} \hat{q}(x, y) = 1$$

which shows that $\hat{p} \in \mathscr{P}(\mathscr{X} \times \mathscr{Y})$ and $\hat{q} \in \mathscr{P}(\mathscr{X} \times \mathscr{Y})$ are joint probability distributions.

With this we can rewrite p^* as

$$p^*(x, y) = (1-\varepsilon)P_{XY}(x, y) + \varepsilon\hat{p}(x, y) \tag{5.22a}$$
$$= (1-\varepsilon)P_{\tilde{X}\tilde{Y}}(x, y) + \varepsilon\hat{q}(x, y) \tag{5.22b}$$

for all $(x, y) \in \mathscr{X} \times \mathscr{Y}$. Next, we show that (5.22a) implies

$$\big|H(Y|X) - H(Y^*|X^*)\big| \leq \varepsilon \log|\mathscr{Y}| + H_2(\varepsilon). \tag{5.23}$$

To do so, we use the fact that the conditional entropy is concave, i.e.,

$$H(Y^*|X^*) \geq (1-\varepsilon)H(Y|X) + \varepsilon H(\hat{Y}|\hat{X}).$$

With this, we have

$$\begin{aligned} H(Y|X) - H(Y^*|X^*) &\leq H(Y|X) - (1-\varepsilon)H(Y|X) - \varepsilon H(\hat{Y}|\hat{X}) \\ &= \varepsilon\big(H(Y|X) - H(\hat{Y}|\hat{X})\big) \\ &\leq \varepsilon H(Y|X) \\ &\leq \varepsilon \log|\mathscr{Y}|. \end{aligned} \tag{5.24}$$

Using the concavity of the entropy

$$H(X^*) \geq (1-\varepsilon)H(X) + \varepsilon H(\hat{X})$$

and the upper bound on the joint entropy

$$H(X^*, Y^*) \leq (1-\varepsilon)H(X, Y) + \varepsilon H(\hat{X}, \hat{Y}) + H_2(\varepsilon),$$

we get

$$\begin{aligned} H(Y^*|X^*) &= H(X^*, Y^*) - H(X^*) \\ &\le (1-\varepsilon)H(Y|X) + \varepsilon H(Y^*|X^*) + H_2(\varepsilon) \end{aligned}$$

and further

$$\begin{aligned} H(Y|X) - H(Y^*|X^*) &\ge -\varepsilon\big(H(Y^*|X^*) - H(Y|X)\big) - H_2(\varepsilon) \\ &\ge -\varepsilon H(Y^*|X^*) - H_2(\varepsilon) \\ &\ge -\varepsilon \log|\mathscr{Y}| - H_2(\varepsilon). \end{aligned} \tag{5.25}$$

Now, (5.24) and (5.25) yield

$$\big|H(Y|X) - H(Y^*|X^*)\big| \le \varepsilon \log|\mathscr{Y}| + H_2(\varepsilon)$$

which shows (5.23). (By the same arguments, one can show that (5.22b) implies $|H(\tilde{Y}|\tilde{X}) - H(Y^*|X^*)| \le \varepsilon \log|\mathscr{Y}| + H_2(\varepsilon)$.)

Finally, this yields

$$\begin{aligned} &\big|H(Y|X) - H(\tilde{Y}|\tilde{X})\big| \\ &\quad = \big|H(Y|X) - H(Y^*|X^*) + \big(H(Y^*|X^*) - H(\tilde{Y}|\tilde{X})\big)\big| \\ &\quad \le \big|H(Y|X) - H(Y^*|X^*)\big| + \big|H(\tilde{Y}|\tilde{X}) - H(Y^*|X^*)\big| \\ &\quad \le 2\varepsilon \log|\mathscr{Y}| + 2H_2(\varepsilon) \end{aligned}$$

which is (5.6), proving the lemma. □

Proof of Lemma 5.2

The proof presented in the following is based on [10, Lemma 2]. Let $0 \le k \le n$ be arbitrary. We define

$$P_{UVY_1^k\tilde{Y}_{k+1}^n}(u, v, y_1^k, y_{k+1}^n) =: \sum_{x^n \in \mathscr{X}^n} \prod_{l=1}^{k} W(y_l|x_l) \prod_{l=k+1}^{n} \widetilde{W}(y_l|x_l) E(x^n|v) P_{V|U}(v|u) P_U(u).$$

So we have

$$I(V; Y^n|U) - I(V; \tilde{Y}^n|U) = \sum_{k=0}^{n-1} \Big(I(V; Y_1^{k+1}\tilde{Y}_{k+2}^n|U) - I(V; Y_1^k \tilde{Y}_{k+1}^n|U) \Big).$$

For all $0 \leq k \leq n-1$ it holds that

$$
\begin{aligned}
&I(V; Y_1^{k+1}\tilde{Y}_{k+2}^n|U) - I(V; Y_1^k\tilde{Y}_{k+1}^n|U) \\
&\quad = I(V; Y_1^k|U) + I(V; Y_{k+1}\tilde{Y}_{k+2}^n|Y_1^kU) - I(V; Y_1^k|U) - I(V; \tilde{Y}_{k+1}^n|Y_1^kU) \\
&\quad = I(V; Y_{k+1}\tilde{Y}_{k+2}^n|Y_1^kU) - I(V; \tilde{Y}_{k+1}^n|Y_1^kU) \\
&\quad = I(V; \tilde{Y}_{k+2}^n|Y_1^kU) + I(V; Y_{k+1}|\tilde{Y}_{k+2}^nY_1^kU) \\
&\qquad\quad - I(V; \tilde{Y}_{k+2}^n|Y_1^kU) - I(V; \tilde{Y}_{k+1}|\tilde{Y}_{k+2}^nY_1^kU) \\
&\quad = I(V; Y_{k+1}|\tilde{Y}_{k+2}^nY_1^kU) - I(V; \tilde{Y}_{k+1}|\tilde{Y}_{k+2}^nY_1^kU) \\
&\quad = H(Y_{k+1}|\tilde{Y}_{k+2}^nY_1^kU) - H(\tilde{Y}_{k+1}|\tilde{Y}_{k+2}^nY_1^kU) \\
&\qquad\quad - H(VY_{k+1}|\tilde{Y}_{k+2}^nY_1^kU) + H(V\tilde{Y}_{k+1}|\tilde{Y}_{k+2}^nY_1^kU). \qquad (5.26)
\end{aligned}
$$

We want to analyze the right-hand side of (5.26). For $0 \leq k \leq n-1$, it holds that

$$
\begin{aligned}
&\| P_{UVY_1^{k+1}\tilde{Y}_{k+2}^n} - P_{UVY_1^k\tilde{Y}_{k+1}^n} \| \\
&\quad = \sum_{v\in\mathscr{V}}\sum_{u\in\mathscr{U}}\sum_{y^n\in\mathscr{Y}^n} \left| P_{UVY_1^{k+1}\tilde{Y}_{k+2}^n}(u, v, y_1^{k+1}y_{k+2}^n) - P_{UVY_1^k\tilde{Y}_{k+1}^n}(u, v, y_1^k y_{k+1}^n) \right| \\
&\quad = \sum_{v\in\mathscr{V}}\sum_{u\in\mathscr{U}}\sum_{y^n\in\mathscr{Y}^n} \Bigg| \sum_{x^n\in\mathscr{X}^n} \Bigg(\prod_{l=1}^{k+1} W(y_l|x_l) \prod_{l=k+2}^{n} \widetilde{W}(y_l|x_l) \\
&\qquad\quad - \prod_{l=1}^{k+1} W(y_l|x_l) \prod_{l=k+2}^{n} \widetilde{W}(y_l|x_l) \Bigg) E(x^n|v) P_{V|U}(v|u) P_U(u) \Bigg| \\
&\quad = \sum_{v\in\mathscr{V}}\sum_{u\in\mathscr{U}}\sum_{y^n\in\mathscr{Y}^n} \Bigg| \sum_{x^n\in\mathscr{X}^n} \prod_{l=1}^{k} W(y_l|x_l) \prod_{l=k+2}^{n} \widetilde{W}(y_l|x_l) \Big(W(y_{k+1}|x_{k+1}) \\
&\qquad\quad - \widetilde{W}(y_{k+1}|x_{k+1}) \Big) E(x^n|v) P_{V|U}(v|u) P_U(u) \Bigg| \\
&\quad \leq \sum_{v\in\mathscr{V}}\sum_{u\in\mathscr{U}}\sum_{y^n\in\mathscr{Y}^n}\sum_{x^n\in\mathscr{X}^n} \prod_{l=1}^{k} W(y_l|x_l) \prod_{l=k+2}^{n} \widetilde{W}(y_l|x_l) \Big| W(y_{k+1}|x_{k+1}) \\
&\qquad\quad - \widetilde{W}(y_{k+1}|x_{k+1}) \Big| E(x^n|v) P_{V|U}(v|u) P_U(u) \\
&\quad = \sum_{v\in\mathscr{V}}\sum_{u\in\mathscr{U}}\sum_{x^n\in\mathscr{X}^n} \Bigg(\sum_{y^n\in\mathscr{Y}^n} \prod_{l=1}^{k} W(y_l|x_l) \prod_{l=k+2}^{n} \widetilde{W}(y_l|x_l) \Big| W(y_{k+1}|x_{k+1}) \\
&\qquad\quad - \widetilde{W}(y_{k+1}|x_{k+1}) \Big| \Bigg) E(x^n|v) P_{V|U}(v|u) P_U(u)
\end{aligned}
$$

$$
\begin{aligned}
&= \sum_{u\in\mathscr{U}} \sum_{x^n\in\mathscr{X}^n} \sum_{y_{k+1}\in\mathscr{Y}} \Big| W(y_{k+1}|x_{k+1}) \\
&\qquad - \widetilde{W}(y_{k+1}|x_{k+1}) \Big| E(x^n|v) P_{V|U}(v|u) P_U(u) \\
&< \varepsilon \sum_{v\in\mathscr{V}} \sum_{u\in\mathscr{U}} \sum_{x^n\in\mathscr{X}^n} E(x^n|v) P_{V|U}(v|u) P_U(u) = \varepsilon.
\end{aligned}
$$

This shows that the total variation between the joint probability distribution $P_{UVY^k\tilde{Y}_{k+1}^n}$ and $P_{UVY^{k+1}\tilde{Y}_{k+2}^n}$ is smaller than ε. Then by Lemma 5.1 it holds that

$$
\Big| H(Y_{k+1}|\tilde{Y}_{k+2}^n Y_1^k U) - H(\tilde{Y}_{k+1}|\tilde{Y}_{k+2}^n Y_1^k U) \Big| < 2\varepsilon \log|\mathscr{Y}| + 2H_2(\varepsilon) \tag{5.27}
$$

and

$$
\begin{aligned}
&\Big| H(VY_{k+1}|\tilde{Y}_{k+2}^n Y_1^k U) - H(V\tilde{Y}_{k+1}|\tilde{Y}_{k+2}^n Y_1^k U) \Big| \\
&\quad = \Big| H(V|\tilde{Y}_{k+2}^n Y_1^k U) + H(Y_{k+1}|V\tilde{Y}_{k+2}^n Y_1^k U) \\
&\qquad\qquad - H(V|\tilde{Y}_{k+2}^n Y_1^k U) - H(\tilde{Y}_{k+1}|V\tilde{Y}_{k+2}^n Y_1^k U) \Big| \\
&\quad = \Big| H(Y_{k+1}|V\tilde{Y}_{k+2}^n Y_1^k U) - H(\tilde{Y}_{k+1}|V\tilde{Y}_{k+2}^n Y_1^k U) \Big| \\
&\quad < 2\varepsilon \log|\mathscr{Y}| + 2H_2(\varepsilon).
\end{aligned} \tag{5.28}
$$

Inserting (5.27) and (5.28) into (5.26) we obtain

$$
\Big| I(V; Y_1^{k+1}\tilde{Y}_{k+2}^n|U) - I(V; Y_1^k\tilde{Y}_{k+1}^n|U) \Big| \le 4\varepsilon \log|\mathscr{Y}| + 4H_2(\varepsilon) := \delta_2(\varepsilon, |\mathscr{Y}|). \tag{5.29}
$$

This gives in particular the following upper bound for the difference between $I(V; Y^n|U)$ and $I(V; \tilde{Y}^n|U)$:

$$
\begin{aligned}
\Big| I(V; Y^n|U) - I(V; \tilde{Y}^n|U) \Big| &\le \sum_{k=0}^{n-1} \Big| I(V; Y_1^{k+1}\tilde{Y}_{k+2}^n|U) - I(V; Y_1^k\tilde{Y}_{k+1}^n|U) \Big| \\
&\le n\delta_2(\varepsilon, |\mathscr{Y}|)
\end{aligned}
$$

proving the lemma. □

References

1. Ahlswede R (1978) Elimination of correlation in random codes for arbitrarily varying channels. Z Wahrscheinlichkeitstheorie verw Gebiete 44:159–175
2. Alicki R, Fannes M (2004) Continuity of quantum conditional information. J Phys A: Math Gen 37(5):L55–L57
3. Bjelaković I, Boche H, Sommerfeld J (2013) Capacity results for arbitrarily varying wiretap channels. Information theory, combinatorics, and search theory. Springer, Berlin, pp 123–144
4. Bjelaković I, Boche H, Sommerfeld J (2013) Secrecy results for compound wiretap channels. Prob Inf Trans 49(1):73–98
5. Blackwell D, Breiman L, Thomasian AJ (1959) The capacity of a class of channels. Ann Math Stat 30(4):1229–1241
6. Blackwell D, Breiman L, Thomasian AJ (1960) The capacities of certain channel classes under random coding. Ann Math Stat 31(3):558–567
7. Bloch M, Barros J (2011) Physical-layer security: from information theory to security engineering. Cambridge University Press, Cambridge
8. Boche H, Schaefer RF (2013) Capacity results and super-activation for wiretap channels with active wiretappers. IEEE Trans Inf Forensics Secur 8(9):1482–1496
9. Boche H, Schaefer RF (2014) Arbitrarily varying wiretap channels with finite coordination resources. In Proceedings of IEEE international conference on communication workshops, Sydney, Australia, pp 746–751
10. Boche H, Schaefer RF, Poor HV (2014) On the continuity of the secrecy capacity of compound and arbitrarily varying wiretap channels. IEEE Trans Inf Forensics Secur. http://arxiv.org/abs/1409.4752
11. Boche H, Schaefer RF, Poor HV (2015) On the continuity of the secrecy capacity of wiretap channels under channel uncertainty. In: Proceedings of IEEE international conference on communication, London, UK, June 2015
12. Boche H, Schaefer RF, Poor HV (2014) On arbitrarily varying wiretap channels for different classes of secrecy measures. In: Proceedings of IEEE international symposium on information theory, Honolulu, pp 2376–2380
13. Csiszár I (1996) Almost independence and secrecy capacity. Probl Pered Inf 32(1):48–57
14. Csiszár I, Körner J (1978) Broadcast channels with confidential messages. IEEE Trans inf theory 24(3):339–348
15. Csiszár I, Narayan P (1988) The capacity of the arbitrarily varying channel revisited: positivity, constraints. IEEE Trans Inf Theory 34(2):181–193
16. Deutsche Telekom AG Laboratories (2010) Next generation mobile networks: (r)evolution in mobile communications. Technology Radar Edition III/2010, Feature Paper
17. Ekrem E, Ulukus S (2010) On Gaussian MIMO compound wiretap channels. In: Proceedings of the conference on information sciences and systems, Baltimore, pp 1–6
18. Fettweis G, Boche H, Wiegand T et al (2014) The tactile internet. Technical report, ITU-T Technology Watch reports. http://www.itu.int/oth/T2301000023/en
19. Grigorescu A (2015) Robust biometric authentication and secure message transmission. Master's thesis, Technische Universität München, Munich, Germany
20. Grigorescu A, Boche H, Schaefer RF, Poor HV (2015) Capacity region continuity of the compound broadcast channel with confidential messages. In: Proceedings of IEEE conference on information theory workshop, Jerusalem, Israel
21. Helmbrecht U, Plaga R (2008) New challenges for IT-security research in ICT. In: World federation of scientists international seminars on planetary emergencies, Erice, Italy, pp 1–6
22. Jorswieck EA, Wolf A, Gerbracht S (2010) Secrecy on the physical layer in wireless networks. Trends in Telecommunications Technologies, pp 413–435
23. Khisti A (2011) Interference alignment for the multiantenna compound wiretap channel. IEEE Trans Inf Theory 57(5):2976–2993

24. Kobayashi M, Liang Y, Shamai (Shitz) S, Debbah M (2009) On the compound MIMO broadcast channels with confidential messages. In: Proceedings of IEEE international symposium on information theory, Seoul, Korea, pp 1283–1287
25. Leung D, Smith G (2009) Continuity of quantum channel capacities. Commun Math Phys 292(1):201–215
26. Liang Y, Kramer G, Poor HV, Shamai (Shitz) S (2009) Compound wiretap channels. EURASIP J Wireless Commun 142374:1–13
27. Liang Y, Poor HV, Shamai (Shitz) S (2009) Information theoretic security. Found Trends Commun Inf Theory 5(4–5):355–580
28. Liu R, Trappe W (eds) (2010) Securing wireless communications at the physical layer. Springer, Berlin
29. Maurer UM, Wolf S (2000) Information-theoretic key agreement: from weak to strong secrecy for free. In: EUROCRYPT 2000. Lecture Notes in Computer Science, vol 1807, Springer, Berlin, pp 351–368
30. MolavianJazi E, Bloch M, Laneman JN (2009) Arbitrary jamming can preclude secure communication. In: Proceedings of the 47th annual Allerton conference on communication, control, computing, Monticello, IL, pp 1069–1075
31. Nötzel J, Wiese M, Boche H (2015) The arbitrarily varying wiretapchannel—secret randomness, stability and super-activation. IEEE Trans Inf Theory. http://arxiv.org/abs/1501.07439
32. Schaefer RF, Boche H (2014a) Physical layer service integration in wireless networks—signal processing challenges. IEEE Signal Process Mag 31(3):147–156
33. Schaefer RF, Boche H (2014b) Robust broadcasting of common and confidential messages over compound channels: strong secrecy and decoding performance. IEEE Trans Inf Forensics Secur 9(10):1720–1732
34. Schaefer RF, Loyka S (2013) The secrecy capacity of a compound MIMO gaussian channel. In: Proceedings of IEEE conference information theory workshop, Seville, Spain, pp 104–108
35. Schaefer RF, Loyka S (2014) The compound secrecy capacity of a class of non-degraded MIMO gaussian channels. In: Proceedings of the 52nd annual allerton conference on communication, control, and computing, Monticello, pp. 1004–1010
36. Shannon CE (1949) Communication theory of secrecy systems. Bell Syst Tech J 28(4):656–715
37. Wiese M, Nötzel J, Boche H (2014) The arbitrarily varying wiretap channel-deterministic and correlated random coding capacities under the strong secrecy criterion. IEEE Trans Inf Theory. http://arxiv.org/abs/1410.8078
38. Wolfowitz J (1960) Simultaneous channels. Arch Rational Mech Anal 4(4):371–386
39. Wyner AD (1975) The wire-tap channel. Bell Syst Tech J 54:1355–1387
40. Zhou X, Song L, Zhang Y (eds) (2013) Physical layer security in wireless communications. CRC Press, Boca Raton