Strong Secrecy in Compound Broadcast Channels with Confidential Messages

Rafael F. Wyrembelski and Holger Boche

Lehrstuhl für Theoretische Informationstechnik
Technische Universität München, Germany

***Abstract*—In this paper the *compound broadcast channel with confidential messages* is studied, where it is only known to the transmitter and receivers that the actual channel realization is fixed and from a pre-specified set of channels. An achievable rate region for the *strong secrecy* criterion is derived. Further, a multi-letter outer bound is given, which establishes, together with the achievable rate region, a multi-letter expression of the strong secrecy capacity region.**

I. Introduction

Operators of wireless networks are confronted with an inherent problem: a transmitted signal is received by its intended users but can also easily be eavesdropped by non-legitimate receivers due to the open nature of the wireless channel. To meet this challenge, current systems usually apply cryptographic techniques to keep information secret. These techniques are based on the assumption of insufficient computational capabilities of non-legitimate receivers, but due to increasing computational power, recent advances in number theory, and improved algorithms, these techniques are becoming more and more insecure.

Information theoretic, or physical layer, security solely uses the physical properties of the wireless channel to establish a higher level of security. Thus, whatever transformation is applied to the signals at the eavesdroppers, the original message cannot be reproduced with high probability. Information theoretic security was initiated by Wyner, who introduced the *wiretap channel* [1], and later generalized by Csiszár and Körner to the *broadcast channel with confidential messages* [2]. Recently, there is growing interest in information theoretic security; for instance see [3, 4] and references therein.

However, usually the criterion of *weak secrecy* is applied, which is heuristic in nature in that no operational meaning has been given to it yet. This means that even if this criterion holds, it is not clear what an eavesdropper can or cannot do to decode the confidential message. But recently, an operational meaning has been given to the *strong secrecy* criterion introduced by Maurer and Wolf [5]: it was established in [6, 7] for the wiretap channel that the strong secrecy criterion implies that the average decoding error at the eavesdropper tends to one for any decoder it may use.

This work was partly supported by the German Ministry of Education and Research (BMBF) under Grant 01BQ1050 and by the German Research Foundation (DFG) under Grant BO 1734/25-1.

Another challenge for operators of wireless networks is the provision of sufficient channel state information at transmitter and receivers. In practical systems there is always uncertainty in channel state information due to the nature of the wireless medium. A reasonable model is to assume that the exact channel realization is not known; rather, it is only known that it belongs to a pre-specified set of channels. If this channel remains fixed during the whole transmission of a codeword, this corresponds to the concept of *compound channels* [8, 9].

To date, there is only little work that incorporates both tasks: information theoretic security in interaction with channel uncertainty. The compound wiretap channel is analyzed in [6, 7, 10]. The MIMO compound wiretap channel is studied in [11] and the MIMO compound broadcast channel with confidential messages in [12].

In this paper we consider the *compound broadcast channel with confidential messages* where the sender transmits not only a confidential message to a legitimate receiver with strong secrecy, but also an additional common message to both, the legitimate and non-legitimate receiver. Thus, it is related to [2] and extends it in two ways: first, it takes channel uncertainty into account and, second, it employs the strong secrecy criterion.[1]

II. Compound Broadcast Channel with Confidential Messages

Let $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$ be finite input and output sets and $\mathcal{S} = \{1, ..., S\}$ be an index set. Then for fixed $s \in \mathcal{S}$ and input and output sequences $x^n \in \mathcal{X}^n$, $y^n \in \mathcal{Y}^n$, and $z^n \in \mathcal{Z}^n$, the discrete memoryless broadcast channel is given by $W_s^{\otimes n}(y^n, z^n|x^n) := \prod_{i=1}^n W_s(y_i, z_i|x_i)$. We denote its marginal channels by $W_{\mathcal{Y},s}^{\otimes n}(y^n|x^n)$ and $W_{\mathcal{Z},s}^{\otimes n}(z^n|x^n)$.

Definition 1: The discrete memoryless *compound broadcast channel* $\mathfrak{W}$ is given by $\mathfrak{W} := \{(W_{\mathcal{Y},s}, W_{\mathcal{Z},s}) : s \in \mathcal{S}\}$.

We consider the standard model with a block code of arbitrary but fixed length n. Let $\mathcal{M}_0 := \{1, ..., M_{0,n}\}$ and $\mathcal{M}_1 := \{1, ..., M_{1,n}\}$ be the sets of common and confidential messages. Further we use the abbreviation $\mathcal{M} := \mathcal{M}_0 \times \mathcal{M}_1$.

[1] *Notation:* Discrete random variables are denoted by non-italic capital letters and their realizations and ranges by lower case and script letters, respectively; $H(\cdot)$ and $I(\cdot;\cdot)$ are the traditional entropy and mutual information; $\mathrm{X} - \mathrm{Y} - \mathrm{Z}$ denotes a Markov chain of random variables X, Y, and Z in this order; $\mathcal{P}(\cdot)$ denotes the set of all probability distributions; $\mathbb{E}[\cdot]$ and $\mathbb{P}\{\cdot\}$ are the expectation and probability.

Definition 2: An $(n, M_{0,n}, M_{1,n})$-*code* for the compound broadcast channel $\mathfrak{W}$ with confidential messages consists of a stochastic encoder

$$E : \mathcal{M}_0 \times \mathcal{M}_1 \to \mathcal{P}(\mathcal{X}^n) \tag{1}$$

specified by its transition probabilities, and decoders

$$\varphi_1 : \mathcal{Y}^n \to \mathcal{M}_0 \times \mathcal{M}_1 \quad \text{and} \quad \varphi_2 : \mathcal{Z}^n \to \mathcal{M}_0. \tag{2}$$

The average probability of errors at the receivers 1 and 2 are then given by

$$\bar{e}_{1,n} \coloneqq \max_{s\in\mathcal{S}} \frac{1}{|\mathcal{M}|} \sum_{m\in\mathcal{M}} \sum_{x^n\in\mathcal{X}^n} \sum_{\substack{y^n\in\mathcal{Y}^n:\\ \varphi_1(y^n)\neq(m_0,m_1)}} E(x^n|m) W_{\mathcal{Y},s}^{\otimes n}(y^n|x^n)$$

$$\bar{e}_{2,n} \coloneqq \max_{s\in\mathcal{S}} \frac{1}{|\mathcal{M}|} \sum_{m\in\mathcal{M}} \sum_{x^n\in\mathcal{X}^n} \sum_{\substack{z^n\in\mathcal{Z}^n:\\ \varphi_2(z^n)\neq m_0}} E(x^n|m) W_{\mathcal{Z},s}^{\otimes n}(z^n|x^n).$$

To ensure that the confidential message is kept secret from non-legitimate receiver 2 for all $s \in \mathcal{S}$, we require $\max_{s\in\mathcal{S}} I(\mathrm{M}_1; \mathrm{Z}_s^n) \leq \epsilon_n$ for some (small) $\epsilon_n > 0$ with M_1 the random variable uniformly distributed over the confidential message set $\mathcal{M}_1$ and $\mathrm{Z}^n = (\mathrm{Z}_1, \mathrm{Z}_2, ..., \mathrm{Z}_n)$ the output at receiver 2. This criterion is known as *strong secrecy* [5].

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

$$\max_{s\in\mathcal{S}} I(\mathrm{M}_1; \mathrm{Z}_s^n) \leq \epsilon_n$$

while $\bar{e}_{1,n}, \bar{e}_{2,n}, \epsilon_n \to 0$ as $n \to \infty$. The closure of the set of all achievable rate pairs is the *strong secrecy capacity region* of the compound broadcast channel with confidential messages.

Theorem 1: An achievable strong secrecy rate region for the compound broadcast channel with confidential messages is given by the set of all rate pairs $(R_0, R_1) \in \mathbb{R}_+^2$ that satisfy

$$R_0 \leq \min_{s\in\mathcal{S}} \min\left\{I(\mathrm{U}; \mathrm{Y}_s), I(\mathrm{U}; \mathrm{Z}_s)\right\} \tag{3a}$$

$$R_1 \leq \min_{s\in\mathcal{S}} I(\mathrm{V}; \mathrm{Y}_s|\mathrm{U}) - \max_{s\in\mathcal{S}} I(\mathrm{V}; \mathrm{Z}_s|\mathrm{U}) \tag{3b}$$

for random variables $\mathrm{U} - \mathrm{V} - \mathrm{X} - (\mathrm{Y}_s, \mathrm{Z}_s)$.

Remark 1: Since receiver 2 is a legitimate receiver for the common message and at the same time a non-legitimate receiver for the confidential message, we have made different assumptions on its channel. Accordingly, we have to assume the worst channel in (3a) for the common message and the best channel in (3b) for the confidential message.

III. Key Idea for Strong Secrecy

In this paper we extend Devetak's approach [13] introduced for the wiretap channel to the compound broadcast channel with confidential messages. This approach establishes strong secrecy using only the noisy channel. We start with a basic observation concerning the relationship of total variation distance and mutual information.

Lemma 1: Let $\mathcal{A}$ and $\mathcal{B}$ be finite sets and let A and B be corresponding random variables. If $\|P_\mathrm{A} \otimes P_\mathrm{B} - P_\mathrm{AB}\| \leq \epsilon \leq \frac{1}{2}$, then

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

with $P_\mathrm{A} \otimes P_\mathrm{B}(a, b) = P_\mathrm{A}(a) P_\mathrm{B}(b)$.

Proof: A proof can be found in [14, Lemma 1.2.7]. ∎

Thus, for $I(\mathrm{M}_1; \mathrm{Z}_s^n)$ to be small, it suffices to find for every $\epsilon > 0$ a code that satisfies

$$\left\|P_{\mathrm{Z}_s^n} \otimes P_{\mathrm{M}_1} - P_{\mathrm{Z}_s^n \mathrm{M}_1}\right\| \leq \epsilon.$$

From $P_{\mathrm{Z}_s^n} = \frac{1}{|\mathcal{M}_0||\mathcal{M}_1|} \sum_{m_0,m_1} P_{\mathrm{Z}_s^n|\mathrm{M}_0=m_0,\mathrm{M}_1=m_1}$, and the triangle inequality follows that it is sufficient to find for every $s \in \mathcal{S}$ and every $(m_0, m_1) \in \mathcal{M}_0 \times \mathcal{M}_1$ a measure ϑ_{s,m_0} on $\mathcal{Z}^n$ such that

$$\left\|P_{\mathrm{Z}_s^n|\mathrm{M}_0=m_0,\mathrm{M}_1=m_1} - \vartheta_{s,m_0}\right\| \leq \epsilon. \tag{4}$$

IV. Achievability

Here we prove Theorem 1, i.e., the achievability of (3) with strong secrecy. Therefore, we construct a codebook that enables reliable communication of all messages, while ensuring the secrecy of the confidential message. Additionally to the key observation in (4), we need two ingredients.

The first one ensures reliable communication of the common message m_0 to both receivers and of the confidential message m_1 to receiver 1. Let us drop the security requirement on m_1 for a moment, i.e., m_1 need not be be kept secret from non-legitimate receiver 2. Then this scenario corresponds to the broadcast channel with degraded message sets [15].

Lemma 2: An achievable rate region for the compound broadcast channel with degraded message sets is given by all rate pairs $(R_0, R_1) \in \mathbb{R}_+^2$ that satisfy

$$R_0 \leq \min_{s\in\mathcal{S}} \min\left\{I(\mathrm{U}; \mathrm{Y}_s), I(\mathrm{U}; \mathrm{Z}_s)\right\} \tag{5a}$$

$$R_1 \leq \min_{s\in\mathcal{S}} I(\mathrm{X}; \mathrm{Y}_s|\mathrm{U}) \tag{5b}$$

for random variables $\mathrm{U} - \mathrm{X} - (\mathrm{Y}_s, \mathrm{Z}_s)$ with average probability of errors $\bar{e}_{1,n}, \bar{e}_{2,n} \leq 2^{-n\gamma}$ for some $\gamma > 0$.

Sketch of Proof: The region can be proved using random coding arguments. More precisely, a superposition of codewords for the common message and for the private message according to the chosen input distributions (6) and (7) will allow to prove the result in a similar way as for example in [16] for the compound bidirectional broadcast channel. The details are omitted due to lack of space. ∎

Remark 2: For $|\mathcal{S}| = 1$ the region (5) reduces to a subregion of [15]. More precisely, the sum constraint on receiver 1 of the form $R_0 + R_1 \leq I(\mathrm{X}; \mathrm{Y}_s)$ in [15] is replaced by individual constraints on $R_0 \leq I(\mathrm{U}; \mathrm{Y}_s)$ and $R_1 \leq I(\mathrm{X}; \mathrm{Y}_s|\mathrm{U})$ which makes the region smaller. However, (5) will be sufficient to establish the desired result in (3).

The second ingredient will be used to incorporate the strong secrecy requirement on m_1. In more detail, we will exploit the concentration of sums of i.i.d. random variables around their expectation as given in the following lemma which is due to Chernoff and Hoeffding [17].

Lemma 3: Let $b > 0$ and $\mathrm{Z}_1, \mathrm{Z}_2, ..., \mathrm{Z}_L$ be i.i.d. random variables with values in $[0, b]$. Further, let $\mu = \mathbb{E}[\mathrm{Z}_1]$ be the expectation of Z_1. Then

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

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

After these preliminary considerations we come to the coding part. For probability distribution $P_{\mathrm{U}} \in \mathcal{P}(\mathcal{U})$ and $\delta > 0$, let $\mathcal{T}^n_{\mathrm{U},\delta}$ be the set of δ-typical sequences on $\mathcal{U}^n$, cf. for example [14]. We define

$$P'_{\mathrm{U}^n}(u^n) \coloneqq \frac{P^{\otimes n}_{\mathrm{U}}(u^n)}{P^{\otimes n}_{\mathrm{U}}(\mathcal{T}^n_{\mathrm{U},\delta})} \tag{6}$$

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

$$P'_{\mathrm{X}^n|\mathrm{U}^n}(x^n|u^n) \coloneqq \frac{P^{\otimes n}_{\mathrm{X}|\mathrm{U}}(x^n|u^n)}{P^{\otimes n}_{\mathrm{X}|\mathrm{U}}(\mathcal{T}^n_{\mathrm{X}|\mathrm{U},\delta}(u^n)|u^n)} \tag{7}$$

if $x^n \in \mathcal{T}^n_{\mathrm{X}|\mathrm{U},\delta}(u^n)$ and $P'_{\mathrm{X}^n|\mathrm{U}^n}(x^n|u^n) = 0$ else.

This allows us to define the random coding scheme as follows. Let $\mathcal{M}_0$ be the set of common messages where its size $M_{0,n}$ is determined by (5a), cf. Lemma 2. Let $\mathcal{M}_1$ be the set of confidential messages and further $\mathcal{L} \coloneqq \{1, ..., L_n\}$ with $M_{1,n}$ and L_n to be determined later. Let $\{\mathrm{U}^n_{m_0} : m_0 \in \mathcal{M}_0\}$ be i.i.d. random variables with values in $\mathcal{U}^n$ according to P'_{U^n}, cf. (6). Then for each $m_0 \in \mathcal{M}_0$ we define random variables $\{\mathrm{X}^n_{lm_1m_0} : (l, m_1) \in \mathcal{L}\times\mathcal{M}_1\}$ with values in $\mathcal{X}^n$, which are i.i.d. conditional on $\mathrm{U}^n_{m_0}$ according to $P'_{\mathrm{X}^n|\mathrm{U}^n}$, cf. (7).

Now we come to the application of Lemma 3. We note that the channel $W_{\mathcal{Z},s}$ can also be regarded as a channel with inputs in $\mathcal{U}\times\mathcal{X}$ where the $\mathcal{U}$-inputs do not make any difference. Moreover, it will be sufficient to concentrate only on those outputs that are typical; the probability of all other outputs will be of no consequence as we will see later. Therefore, we define for every channel $s \in \mathcal{S}$, message triple (l, m_1, m_0), and $z^n \in \mathcal{Z}^n$ the random variable

$$\begin{aligned}&\mathrm{Q}^n_s(z^n|\mathrm{X}^n_{lm_1m_0}, \mathrm{U}^n_{m_0})\\ &\quad\coloneqq W^{\otimes n}_{\mathcal{Z},s}(z^n|\mathrm{X}^n_{lm_1m_0})\mathbb{1}_{\mathcal{T}^n_{\mathrm{Z}_s|\mathrm{XU},\delta}(\mathrm{X}^n_{lm_1m_0},\mathrm{U}^n_{m_0})}(z^n),\end{aligned} \tag{8}$$

where for any set $\mathcal{A} \subset \mathcal{Z}^n$, we let $\mathbb{1}_{\mathcal{A}}(z^n) = 1$ if $z^n \in \mathcal{A}$ and $\mathbb{1}_{\mathcal{A}}(z^n) = 0$ else. Conditional on $\mathrm{U}^n_{m_0}$, these random variables are i.i.d. Moreover, as the input $(\mathrm{X}^n_{lm_1m_0}, \mathrm{U}^n_{m_0})$ is jointly δ-typical with respect to the joint distribution P_{XU}, and the outputs of Q^n_s are δ-typical conditional on the inputs, it is well known that (8) is bounded from above by

$$\mathrm{Q}^n_s(z^n|\mathrm{X}^n_{lm_1m_0}, \mathrm{U}^n_{m_0}) \leq 2^{-n(H(\mathrm{Z}_s|\mathrm{X},\mathrm{U})-\delta_1)} \tag{9}$$

for some $\delta_1 = \delta_1(\delta)$, see e.g. [14]. Now let

$$\vartheta'_{s,\mathrm{U}^n_{m_0}}(z^n) = \mathbb{E}\big[\mathrm{Q}^n_s(z^n|\mathrm{X}^n_{lm_1m_0}, \mathrm{U}^n_{m_0})|\mathrm{U}^n_{m_0}\big]$$

be the expectation of (8) conditional on $\mathrm{U}^n_{m_0}$. For any $\epsilon_n > 0$ we define

$$\begin{aligned}\mathcal{F}_{s,\mathrm{U}^n_{m_0}} \coloneqq \big\{&z^n \in \mathcal{T}^n_{\mathrm{Z}_s|\mathrm{U},2|\mathcal{X}|\delta}(\mathrm{U}^n_{m_0}) :\\ &\vartheta'_{s,\mathrm{U}^n_{m_0}}(z^n) \geq \epsilon_n|\mathcal{T}^n_{\mathrm{Z}_s|\mathrm{U},2|\mathcal{X}|\delta}(\mathrm{U}^n_{m_0})|^{-1}\big\}.\end{aligned} \tag{10}$$

Finally, we set $\vartheta_{s,\mathrm{U}^n_{m_0}}(z^n) \coloneqq \vartheta'_{s,\mathrm{U}^n_{m_0}}(z^n)\mathbb{1}_{\mathcal{F}_{s,\mathrm{U}^n_{m_0}}}(z^n)$ and similarly $\widetilde{\mathrm{Q}}^n_{s,\mathrm{U}^n_{m_0}}(z^n|\mathrm{X}^n_{lm_1m_0}, \mathrm{U}^n_{m_0}) = \mathrm{Q}^n_{s,\mathrm{U}^n_{m_0}}(z^n|\mathrm{X}^n_{lm_1m_0}, \mathrm{U}^n_{m_0})\mathbb{1}_{\mathcal{F}_{s,\mathrm{U}^n_{m_0}}}(z^n)$. Then we define the event $\mathcal{Q}(z^n)$ as

$$\frac{1}{L_n}\sum_{l=1}^{L_n}\widetilde{\mathrm{Q}}^n_{s,\mathrm{U}^n_{m_0}}(z^n|\mathrm{X}^n_{lm_1m_0}, \mathrm{U}^n_{m_0}) \in \big[(1\pm\epsilon_n)\vartheta_{s,\mathrm{U}^n_{m_0}}(z^n)\big]. \tag{11}$$

Now let $z^n \in \mathcal{Z}^n$. Then for the complement of $\mathcal{Q}(z^n)$ we get

$$\begin{aligned}\mathbb{P}\big\{(\mathcal{Q}(z^n))^c\big\} &= \sum_{u^n\in\mathcal{U}^n}\mathbb{P}\{\mathrm{U}^n_{m_0} = u^n\}\mathbb{P}\big\{(\mathcal{Q}(z^n))^c|u^n_{m_0}\big\}\\ &\leq 2\exp\left(-L_n\cdot\frac{\epsilon_n^2 2^{n(H(\mathrm{Z}_s|\mathrm{X},\mathrm{U})-\delta_1)}\vartheta_{s,\mathrm{U}^n_{m_0}}(z^n)}{2\ln 2}\right)\\ &\leq 2\exp\left(-L_n\cdot\frac{\epsilon_n^3 2^{-n(I(\mathrm{X};\mathrm{Z}_s|\mathrm{U})+\delta_1+\delta_2)}}{2\ln 2}\right)\end{aligned} \tag{12}$$

where the steps follow from the law of total probability, from Lemma 3 and (9), and from (10) and

$$\big|\mathcal{T}^n_{\mathrm{Z}_s|\mathrm{U},2|\mathcal{X}|\delta}(\mathrm{U}^n_{m_0})\big| \leq 2^{n(H(\mathrm{Z}_s|\mathrm{U})+\delta_2)}$$

for some $\delta_2 = \delta_2(\delta)$, see e.g. [14], since $\mathrm{U}^n_{m_0}$ is δ-typical. Note that if we choose $\epsilon_n = 2^{-n\beta}$ for some $\beta \leq \frac{1}{4}\min\{\gamma, \delta_1+\delta_2\}$, then (12) tends to zero doubly-exponentially for

$$L_n \geq 2^{n(\max_{s\in\mathcal{S}} I(\mathrm{X};\mathrm{Z}_s|\mathrm{U})+2(\delta_1+\delta_2))}. \tag{13}$$

This provides the basis for the proof of (4). Note that we have to choose the maximum in (13) to ensure that (12) tends to zero doubly-exponentially for all channel realizations $s \in \mathcal{S}$.

Next, we determine the sizes of the remaining sets for the confidential message. For $\max_{s'\in\mathcal{S}} I(\mathrm{X};\mathrm{Z}_{s'}|\mathrm{U}) < I(\mathrm{X};\mathrm{Y}_s|\mathrm{U})$ for all $s \in \mathcal{S}$, we choose δ (and therewith also δ_1 and δ_2) small enough such that (13) is satisfied and at the same time

$$L_n \leq 2^{n(\max_{s\in\mathcal{S}} I(\mathrm{X};\mathrm{Z}_s|\mathrm{U})+3(\delta_1+\delta_2))} \leq 2^{nI(\mathrm{X};\mathrm{Y}_s|\mathrm{U})}.$$

Further, for the confidential messages we set

$$M_{1,n} \leq 2^{n(\min_{s\in\mathcal{S}} I(\mathrm{X};\mathrm{Y}_s|\mathrm{U})-\max_{s\in\mathcal{S}} I(\mathrm{X};\mathrm{Z}_s|\mathrm{U})-3(\delta_1+\delta_2))}.$$

From (12)-(13) we know that (11) is satisfied for every $s \in \mathcal{S}$, (m_0, m_1), and $z^n \in \mathcal{Z}^n$ with probability close to one. Further, with $M_{0,n}, M_{1,n}, L_n$ as defined above it follows from Lemma 2 that the random codewords we have chosen are the codewords of a deterministic code achieving $\bar{e}_{1,n}, \bar{e}_{2,n} \leq 2^{-n\gamma}$ for some $\gamma > 0$ with probability close to one. Thus, there must be realizations of $(\mathrm{U}^n_{m_0}, \mathrm{X}^n_{lm_1m_0})$ and $\vartheta_{s,\mathrm{U}^n_{m_0}}$ with both these properties, which we denote by $(u^n_{m_0}, x^n_{lm_1m_0})$ and ϑ_{s,m_0}.

From this we construct an appropriate code with a stochastic encoder. Therefore, each message pair $(m_0, m_1) \in \mathcal{M}_0\times\mathcal{M}_1$ is mapped into the codeword $x^n_{lm_1m_0} \in \mathcal{X}^n$ with probability $1/L_n$ which defines a stochastic encoder. The decoder at legitimate receiver 1 decodes all indices, i.e., (l, m_1, m_0), while the decoder at non-legitimate receiver 2 only decodes the common message m_0. From Lemma 2 we know that this code is suitable for reliable transmission of all messages to their respective receivers. It remains to prove that (4) is satisfied.

From the triangle inequality we obtain for every $s \in \mathcal{S}$ and $(m_0, m_1) \in \mathcal{M}_0 \times \mathcal{M}_1$

$$\begin{aligned}
&\left\| P_{\mathrm{Z}_s^n|\mathrm{M}_0=m_0,\mathrm{M}_1=m_1} - \vartheta_{s,m_0} \right\| \\
&\quad \leq \left\| P_{\mathrm{Z}_s^n|\mathrm{M}_0=m_0,\mathrm{M}_1=m_1} - \frac{1}{L_n} \sum_{l=1}^{L_n} \mathrm{Q}_s^n(\cdot|x_{lm_1m_0}^n, u_{m_0}^n) \right\| \\
&\qquad + \left\| \frac{1}{L_n} \sum_{l=1}^{L_n} \mathrm{Q}_s^n(\cdot|x_{lm_1m_0}^n, u_{m_0}^n)(1 - \mathbb{1}_{\mathcal{F}_{s,m_0}}) \right\| \\
&\qquad + \left\| \frac{1}{L_n} \sum_{l=1}^{L_n} \mathrm{Q}_s^n(\cdot|x_{lm_1m_0}^n, u_{m_0}^n) \mathbb{1}_{\mathcal{F}_{s,m_0}} - \vartheta_{s,m_0} \right\|.
\end{aligned}$$

In the following we bound all three parts individually which we denote by I, II, and III. Since all codewords satisfy (11), we have for the third term $III \leq \epsilon$.

For the first term I we have

$$\frac{1}{L_n} \sum_{l=1}^{L_n} W_{\mathcal{Z},s}^{\otimes n}(\mathcal{Z}^n \setminus \mathcal{T}_{\mathrm{Z}_s|\mathrm{XU},\delta}^n(x_{lm_1m_0}^n, u_{m_0}^n)|x_{lm_1m_0}^n) \leq 2^{-nc\delta^2}$$

for some constant $c > 0$, where we again interpret $W_{\mathcal{Z},s}$ as a channel from $\mathcal{U} \times \mathcal{X}$ to $\mathcal{Z}$ and use the fact that the probability that the output of a channel is not δ-typical conditional on the inputs is exponentially small, cf. for example [14].

Finally, the second term II can be rewritten as

$$1 - \frac{1}{L_n} \sum_{l=1}^{L_n} \mathrm{Q}_s^n(\mathcal{F}_{s,m_0}|x_{lm_1m_0}^n, u_{m_0}^n)$$

which is at most $1 - (1-\epsilon)\vartheta'_{s,m_0}(\mathcal{F}_{s,m_0})$ by (11). Note that if z^n is δ-typical conditional on $(x_{lm_1m_0}^n, u_{m_0}^n)$, then it is $2|\mathcal{X}|\delta$-typical conditional on $u_{m_0}^n$, so that $\vartheta'_{s,m_0}(z^n) \neq 0$ only for $z^n \in \mathcal{T}_{\mathrm{Z}_s|\mathrm{U},2|\mathcal{X}|\delta}^n(u_{m_0}^n)$. With the definition of $\mathcal{F}_{s,m_0}$, this implies

$$\begin{aligned}
\vartheta'_{s,m_0}(\mathcal{F}_{s,m_0}) &\geq \vartheta'_{s,m_0}(\mathcal{Z}^n) - \epsilon_n \\
&= \mathbb{E}\big[W_{\mathcal{Z},s}^{\otimes n}(\mathcal{T}_{\mathrm{Z}_s|\mathrm{XU},\delta}^n(\mathrm{X}_{11m_0}^n, \mathrm{U}_{m_0}^n)|\mathrm{X}_{11m_0}^n)|\mathrm{U}_{m_0}^n\big] - \epsilon_n \\
&\geq 1 - 2^{-nc\delta^2} - \epsilon_n
\end{aligned}$$

by the same argument as for term I. Thus, in total we can bound the second term from above as

$$II \leq 2\epsilon_n + 2^{-nc\delta^2}.$$

Putting all three terms together, we can bound the total variation distance as

$$\left\| P_{\mathrm{Z}_s^n|\mathrm{M}_0=m_0,\mathrm{M}_1=m_1} - \vartheta_{s,m_0} \right\| \leq 3\epsilon_n + 2 \cdot 2^{-nc\delta^2} \tag{14}$$

which proves (4). Note that (14) becomes exponentially small since we chose $\epsilon_n = 2^{-n\beta}$. Thus, the mutual information between the confidential message M_1 and the corresponding output Z_s^n at the non-legitimate receiver is exponentially small for every $s \in \mathcal{S}$, cf. Section III.

This proves the achievability of the desired rate region but only for random variables $\mathrm{U} - \mathrm{X} - (\mathrm{Y}_s, \mathrm{Z}_s)$. To obtain the whole region given in (3), note that the transmitter can prefix an artificial channel $P_{\mathrm{X}|\mathrm{V}} : \mathcal{V} \to \mathcal{P}(\mathcal{X})$ with finite $\mathcal{V}$ to $W_s = (W_{\mathcal{Y},s}, W_{\mathcal{Z},s})$. Then the whole construction above can similarly be done for the channel

$$(P_{\mathrm{X}|\mathrm{V}} W_s)(y, z|v) \coloneqq \sum_{x \in \mathcal{X}} W_s(y, z|x) P_{\mathrm{X}|\mathrm{V}}(x|v)$$

which completes the proof of Theorem 1. ∎

Remark 3: Note that the effect of the prefix channel can be integrated in the stochastic encoder, cf. Definition 2.

V. Converse

Here we consider the converse of Theorem 1, where we establish a multi-letter characterization of an outer bound on the strong secrecy capacity region. For this we need the following lemma.

Lemma 4: Let $\mathfrak{W} \coloneqq \{(W_{\mathcal{Y},s}, W_{\mathcal{Z},s}) : s \in \mathcal{S}\}$ be an arbitrary compound broadcast channel. Then

$$\lim_{n\to\infty} \tfrac{1}{n} \big(\inf_{s\in\mathcal{S}} I(\mathrm{V}; \mathrm{Y}_s^n|\mathrm{U}) - \sup_{s\in\mathcal{S}} I(\mathrm{V}; \mathrm{Z}_s^n|\mathrm{U}) \big)$$

exists and equals $\sup_{n\in\mathbb{N}} \frac{1}{n}(\inf_{s\in\mathcal{S}} I(\mathrm{V}; \mathrm{Y}_s^n|\mathrm{U}) - \sup_{s\in\mathcal{S}} I(\mathrm{V}; \mathrm{Z}_s^n|\mathrm{U}))$ for random variables $\mathrm{U} - \mathrm{V} - \mathrm{X}^n - (\mathrm{Y}_s^n, \mathrm{Z}_s^n)$.

Proof: We follow [7] and use Fekete's lemma [18] to prove the desired result. We have to show that the sequence $(a_n)_{n\in\mathbb{N}}$ with

$$a_n \coloneqq \inf_{s\in\mathcal{S}} I(\mathrm{V}; \mathrm{Y}_s^n|\mathrm{U}) - \sup_{s\in\mathcal{S}} I(\mathrm{V}; \mathrm{Z}_s^n|\mathrm{U})$$

satisfies

$$a_{n+m} \geq a_n + a_m$$

for all $n, m \in \mathbb{N}$. Therefore, we define Markov chains $\mathrm{U}_1 - \mathrm{V}_1 - \mathrm{X}^n - (\mathrm{Y}_s^n, \mathrm{Z}_s^n)$ and $\mathrm{U}_2 - \mathrm{V}_2 - \widetilde{\mathrm{X}}^m - (\widetilde{\mathrm{Y}}_s^m, \widetilde{\mathrm{Z}}_s^m)$ and set $\mathrm{U} \coloneqq (\mathrm{U}_1, \mathrm{U}_2)$, $\mathrm{V} \coloneqq (\mathrm{V}_1, \mathrm{V}_2)$, $\mathrm{X}^{n+m} \coloneqq (\mathrm{X}^n, \widetilde{\mathrm{X}}^m)$, and $(\mathrm{Y}_s^{n+m}, \mathrm{Z}_s^{n+m}) \coloneqq ((\mathrm{Y}_s^n, \widetilde{\mathrm{Y}}_s^m), (\mathrm{Z}_s^n, \widetilde{\mathrm{Z}}_s^m))$. By the definition of a_n we have

$$\begin{aligned}
a_{n+m} &= \inf_{s\in\mathcal{S}} I(\mathrm{V}; \mathrm{Y}_s^{n+m}|\mathrm{U}) - \sup_{s\in\mathcal{S}} I(\mathrm{V}; \mathrm{Z}_s^{n+m}|\mathrm{U}) \\
&\geq \inf_{s\in\mathcal{S}} I(\mathrm{V}_1; \mathrm{Y}_s^n|\mathrm{U}_1) + \inf_{s\in\mathcal{S}} I(\mathrm{V}_2; \widetilde{\mathrm{Y}}_s^m|\mathrm{U}_2) \\
&\qquad - \sup_{s\in\mathcal{S}} I(\mathrm{V}_1; \mathrm{Z}_s^n|\mathrm{U}_1) - \sup_{s\in\mathcal{S}} I(\mathrm{V}_2; \widetilde{\mathrm{Z}}_s^m|\mathrm{U}_2)
\end{aligned}$$

which follows from the independence of the two Markov chains. Since these Markov chains can be arbitrary, we conclude $a_{n+m} \geq a_n + a_m$ for all $n, m \in \mathbb{N}$. ∎

Theorem 2: An outer bound on the strong secrecy capacity region of the compound broadcast channel with confidential messages is given by all rate pairs $(R_0, R_1) \in \mathbb{R}_+^2$ that satisfy

$$R_0 \leq \lim_{n\to\infty} \tfrac{1}{n} \inf_{s\in\mathcal{S}} \min\big\{ I(\mathrm{U}; \mathrm{Y}_s^n), I(\mathrm{U}; \mathrm{Z}_s^n) \big\} \tag{15a}$$

$$R_1 \leq \lim_{n\to\infty} \tfrac{1}{n} \big(\inf_{s\in\mathcal{S}} I(\mathrm{V}; \mathrm{Y}_s^n|\mathrm{U}) - \sup_{s\in\mathcal{S}} I(\mathrm{V}; \mathrm{Z}_s^n|\mathrm{U}) \big) \tag{15b}$$

for random variables $\mathrm{U} - \mathrm{V} - \mathrm{X}^n - (\mathrm{Y}_s^n, \mathrm{Z}_s^n)$.

Proof: For any given sequence of $(n, M_{0,n}, M_{1,n})$-codes of Definition 2 with $\bar{e}_{1,n}, \bar{e}_{2,n} \to 0$ and

$$\sup_{s\in\mathcal{S}} I(\mathrm{M}_1; \mathrm{Z}_s^n) = H(\mathrm{M}_1) - \inf_{s\in\mathcal{S}} H(\mathrm{M}_1|\mathrm{Z}_s^n) =: \epsilon_{c,n} \tag{16}$$

with $\epsilon_{c,n} \to 0$, there exist $\mathrm{U} - \mathrm{V} - \mathrm{X}^n - (\mathrm{Y}_s^n, \mathrm{Z}_s^n)$ such that all rate tuples $(R_0, R_1) \in \mathbb{R}_+^2$ are bounded by (15).

Let M_0 and M_1 be random variables uniformly distributed over the message sets $\mathcal{M}_0$ and $\mathcal{M}_1$. We have the Markov chains $(\mathrm{M}_0, \mathrm{M}_1) - \mathrm{X}^n - \mathrm{Y}_s^n - (\hat{\mathrm{M}}_{0,1}, \hat{\mathrm{M}}_1)$ and $(\mathrm{M}_0, \mathrm{M}_1) - \mathrm{X}^n - \mathrm{Z}_s^n - \hat{\mathrm{M}}_{0,2}$ where the first transition is governed by the stochastic encoder E, cf. (1), the second by the channels $W_{\mathcal{Y},s}^{\otimes n}, W_{\mathcal{Z},s}^{\otimes n}$, and last one by the corresponding decoder, cf. (2). Then we have for all $s \in \mathcal{S}$ at receiver 1 for the common rate

$$\begin{aligned} nR_0 = H(\mathrm{M}_0) &= I(\mathrm{M}_0; \mathrm{Y}_s^n) + H(\mathrm{M}_0|\mathrm{Y}_s^n) \\ &\leq I(\mathrm{M}_0; \mathrm{Y}_s^n) + n\epsilon_{1,n} \end{aligned} \tag{17}$$

where the last inequality follows from Fano's inequality, i.e., $H(\mathrm{M}_0|\mathrm{Y}_s^n) \leq H(\mathrm{M}_0, \mathrm{M}_1|\mathrm{Y}_s^n) \leq n\epsilon_{1,n}$, and similarly for all $s \in \mathcal{S}$ at receiver 2

$$nR_0 = H(\mathrm{M}_0) \leq I(\mathrm{M}_0; \mathrm{Z}_s^n) + n\epsilon_{2,n} \tag{18}$$

by using Fano's inequality $H(\mathrm{M}_0|\mathrm{Z}_s^n) \leq n\epsilon_{2,n}$.

Next, we follow [2] and make use of the definition of mutual information. Rewriting (16) we get for the confidential rate

$$\begin{aligned} nR_1 = H(\mathrm{M}_1) &= \inf_{s\in\mathcal{S}} H(\mathrm{M}_1|\mathrm{Z}_s^n) + \epsilon_{c,n} \\ &= \inf_{s\in\mathcal{S}} \big(H(\mathrm{M}_1|\mathrm{Z}_s^n, \mathrm{M}_0) + I(\mathrm{M}_1; \mathrm{M}_0|\mathrm{Z}_s^n)\big) + \epsilon_{c,n} \\ &\leq H(\mathrm{M}_1|\mathrm{M}_0) - \sup_{s\in\mathcal{S}} I(\mathrm{M}_1; \mathrm{Z}_s^n|\mathrm{M}_0) + n\epsilon_{2,n} + \epsilon_{c,n} \\ &\leq I(\mathrm{M}_1; \mathrm{Y}_s^n|\mathrm{M}_0) - \sup_{s'\in\mathcal{S}} I(\mathrm{M}_1; \mathrm{Z}_{s'}^n|\mathrm{M}_0) + n\epsilon_{12,n} + \epsilon_{c,n} \end{aligned} \tag{19}$$

with $\epsilon_{12,n} = \epsilon_{1,n} + \epsilon_{2,n}$ where the first inequality follows from $I(\mathrm{M}_1; \mathrm{M}_0|\mathrm{Z}_s^n) = H(\mathrm{M}_0|\mathrm{Z}_s^n) - H(\mathrm{M}_0|\mathrm{Z}_s^n, \mathrm{M}_1) \leq H(\mathrm{M}_0|\mathrm{Z}_s^n) \leq \epsilon_{2,n}$ and the second inequality from $H(\mathrm{M}_1|\mathrm{Y}_s^n, \mathrm{M}_0) \leq H(\mathrm{M}_1, \mathrm{M}_0|\mathrm{Y}_s^n) \leq \epsilon_{1,n}$.

With $I(\mathrm{M}_1; \mathrm{Y}_s^n|\mathrm{M}_0) = I(\mathrm{M}_0, \mathrm{M}_1; \mathrm{Y}_s^n|\mathrm{M}_0)$ and $I(\mathrm{M}_1; \mathrm{Z}_s^n|\mathrm{M}_0) = I(\mathrm{M}_0, \mathrm{M}_1; \mathrm{Z}_s^n|\mathrm{M}_0)$, (17)-(19) imply that the rates are bounded by

$$\begin{aligned} nR_0 &\leq \inf_{s\in\mathcal{S}} \min\big\{I(\mathrm{M}_0; \mathrm{Y}_s^n), I(\mathrm{M}_0; \mathrm{Z}_s^n)\big\} \\ nR_1 &\leq \inf_{s\in\mathcal{S}} I(\mathrm{M}_0, \mathrm{M}_1; \mathrm{Y}_s^n|\mathrm{M}_0) - \sup_{s\in\mathcal{S}} I(\mathrm{M}_0, \mathrm{M}_1; \mathrm{Z}_s^n|\mathrm{M}_0). \end{aligned}$$

Recall that the transition between the messages $(\mathrm{M}_0, \mathrm{M}_1)$ and the input X^n is governed by a stochastic encoder, which allows us to introduce arbitrary auxiliary random variables U and V which satisfy the Markov chain $\mathrm{U} - \mathrm{V} - \mathrm{X}^n - (\mathrm{Y}_s^n, \mathrm{Z}_s^n)$, cf. also Remark 3. Dividing by n and taking the limit yields

$$\begin{aligned} R_0 &\leq \lim_{n\to\infty} \tfrac{1}{n} \inf_{s\in\mathcal{S}} \min\big\{I(\mathrm{U}; \mathrm{Y}_s^n), I(\mathrm{U}; \mathrm{Z}_s^n)\big\} \\ R_1 &\leq \lim_{n\to\infty} \tfrac{1}{n} \big(\inf_{s\in\mathcal{S}} I(\mathrm{V}; \mathrm{Y}_s^n|\mathrm{U}) - \sup_{s\in\mathcal{S}} I(\mathrm{V}; \mathrm{Z}_s^n|\mathrm{U})\big) \end{aligned}$$

where Lemma 4 guarantees that the quantities exist and are well defined. This concludes the proof. ∎

Remark 4: Applying the achievability result given in Theorem 1 to the channels $W_{\mathcal{Y},s}^{\otimes n}$ and $W_{\mathcal{Z},s}^{\otimes n}$ yields the achievability result for the corresponding multi-letter case. Together with the converse result given in Theorem 2 we conclude on the following.

Corollary 1: A multi-letter description of the strong secrecy capacity region of the compound broadcast channel with confidential messages is given by all rate pairs $(R_0, R_1) \in \mathbb{R}_+^2$ that satisfy

$$\begin{aligned} R_0 &\leq \lim_{n\to\infty} \tfrac{1}{n} \inf_{s\in\mathcal{S}} \min\big\{I(\mathrm{U}; \mathrm{Y}_s^n), I(\mathrm{U}; \mathrm{Z}_s^n)\big\} \\ R_1 &\leq \lim_{n\to\infty} \tfrac{1}{n} \big(\inf_{s\in\mathcal{S}} I(\mathrm{V}; \mathrm{Y}_s^n|\mathrm{U}) - \sup_{s\in\mathcal{S}} I(\mathrm{V}; \mathrm{Z}_s^n|\mathrm{U})\big) \end{aligned}$$

for random variables $\mathrm{U} - \mathrm{V} - \mathrm{X}^n - (\mathrm{Y}_s^n, \mathrm{Z}_s^n)$. ∎

VI. Conclusion

In this paper we derived an achievable strong secrecy rate region for the compound broadcast channel with confidential messages. We further presented a multi-letter outer bound which establishes a multi-letter expression of the corresponding strong secrecy capacity region.

References

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

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

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

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

[5] U. M. Maurer and S. Wolf, "Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free," in *EUROCRYPT 2000, Lecture Notes in Computer Science*. Springer-Verlag, May 2000, vol. 1807, pp. 351–368.

[6] I. Bjelaković, H. Boche, and J. Sommerfeld, "Capacity Results for Compound Wiretap Channels," in *Proc. IEEE Inf. Theory Workshop*, Paraty, Brazil, Oct. 2011, pp. 60–64.

[7] ——, "Secrecy Results for Compound Wiretap Channels," submitted 2011, available at http://arxiv.org/abs/1106.2013.

[8] D. Blackwell, L. Breiman, and A. J. Thomasian, "The Capacity of a Class of Channels," *Ann. Math. Stat.*, vol. 30, no. 4, pp. 1229–1241, Dec. 1959.

[9] J. Wolfowitz, "Simultaneous Channels," *Arch. Rational Mech. Analysis*, vol. 4, no. 4, pp. 371–386, 1960.

[10] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz), "Compound Wiretap Channels," *EURASIP J. Wireless Commun. Netw.*, vol. Article ID 142374, pp. 1–13, 2009.

[11] E. Ekrem and S. Ulukus, "On Gaussian MIMO Compound Wiretap Channels," in *Proc. Conf. Inf. Sciences and Systems*, Baltimore, MD, USA, Mar. 2010, pp. 1–6.

[12] M. Kobayashi, Y. Liang, S. Shamai (Shitz), and M. Debbah, "On the Compound MIMO Broadcast Channels with Confidential Messages," in *Proc. IEEE Int. Symp. Inf. Theory*, Seoul, Korea, Jun. 2009, pp. 1283–1287.

[13] I. Devetak, "The Private Classical Capacity and Quantum Capacity of a Quantum Channel," *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 44–55, Jan. 2005.

[14] I. Csiszár and J. Körner, *Information Theory - Coding Theorems for Discrete Memoryless Systems*, 1st ed. Academic Press, 1981.

[15] J. Körner and K. Marton, "General Broadcast Channels with Degraded Message Sets," *IEEE Trans. Inf. Theory*, vol. 23, no. 1, pp. 60–64, Jan. 1977.

[16] R. F. Wyrembelski, I. Bjelaković, T. J. Oechtering, and H. Boche, "Optimal Coding Strategies for Bidirectional Broadcast Channels under Channel Uncertainty," *IEEE Trans. Commun.*, vol. 58, no. 10, pp. 2984–2994, Oct. 2010.

[17] W. Hoeffding, "Probability Inequalities for Sums of Bounded Random Variables," *Jour. Amer. Math. Stat. Association*, vol. 58, pp. 13–30, 1963.

[18] M. Fekete, "Über die Verteilung von Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten," *Mathematische Zeitschrift*, vol. 17, no. 1, pp. 228–249, 1923.