STRONG SECRECY AND DECODING PERFORMANCE ANALYSIS FOR ROBUST BROADCASTING UNDER CHANNEL UNCERTAINTY

Rafael F. Schaefer and Holger Boche†*

*Department of Electrical Engineering
Princeton University
Princeton, NJ 08544, USA

†Lehrstuhl für Theoretische Informationstechnik
Technische Universität München
80290 München, Germany

ABSTRACT

The *compound broadcast channel with confidential messages* is studied, where the transmitter sends a common message to two receivers and, at the same time, a confidential message to one receiver which has to be kept secret from the other one. It is only known to the transmitter and receivers that the actual channel realization is fixed and from a pre-specified set of channels. The information theoretic criterion of *strong secrecy* is analyzed in detail and generalized in such a way that it completely captures the behavior and the abilities of the non-legitimate receiver. Its impact on the decoding performance of the non-legitimate receiver is characterized as well. In particular, it is shown that regardless of the computational capabilities and the applied decoding strategy of the non-legitimate receiver, his decoding error always tends to one. This gives a valuable signal processing implication of the generalized secrecy criterion and identifies desirable properties of an optimal code design.

Index Terms— Broadcast channel with confidential messages, strong secrecy, compound channel, decoding performance.

1. INTRODUCTION

Rapid developments in communication systems make information available almost everywhere. Along with this, the security of sensitive information from unauthorized access becomes an important task. Especially wireless communication systems are inherently vulnerable, since transmitted signals are received by intended users but are also easily eavesdropped by non-legitimate receivers.

Nowadays, the architecture of communication systems is separated into error correction and data encryption. The former is typically implemented on the physical layer turning the noisy channel into an ideal "*bit pipe*." Then on higher layers, the data encryption is realized by applying cryptographic techniques which are based on the assumption of insufficient computational capabilities of eavesdroppers. But due to increasing computational power and improved algorithms, such approaches are becoming more and more insecure.

Another approach for realizing security is the so-called concept of information theoretic secrecy, which takes the physical properties of the noisy channel into account. This 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]. This area of research has drawn attention in recent years as it provides a promising approach to embed secure communication in wireless networks; for instance see [3–6] and references therein. Concurrently, it has been demonstrated that the joint implementation of different public and secure communication tasks on the physical layer can lead to significant gains in spectral efficiency. Thus, it is not surprising that the efficient *physical layer service integration* [7] has also been identified by operators and national agencies as a promising task to increase spectral efficiency [8, 9].

Another challenge, especially for operators of wireless communication systems, is the provision of accurate channel state information at transmitter and receivers. Practical systems always suffer from channel uncertainty due to the nature of the wireless medium and estimation/feedback inaccuracy. Thus, it is reasonable to assume that the exact channel realization is not known; rather, it is only known that it is fixed and belongs to a pre-specified set of channels. This is the concept of *compound channels* [10, 11] and, accordingly, one is interested in robust strategies that allow for secure communication over compound channels.

In this paper we consider the discrete memoryless *compound broadcast channel with confidential messages (BCC)*. This models the communication scenario with one transmitter and two receivers, where the transmitter broadcasts a common message to both receivers and, at the same time, sends a confidential message to receiver 1 which has to be kept secret from receiver 2. Thus, receiver 2 is both a legitimate receiver for the common message and a non-legitimate receiver for the confidential message. This is in contrast to the classical wiretap channel [1], where the eavesdropper does not belong to the communication system.[1]

1.1. Relation to Prior Work

In [1–6], the criterion of *weak secrecy* is usually applied, which is heuristic in nature in that no operational meaning has been given to it yet. But recently, an operational meaning has been given to the *strong secrecy* criterion [12, 13]: it was established in [14] for the wiretap channel that the strong secrecy criterion implies that the average decoding error at the eavesdropper tends to one for any decoder he (or she) may use. This gives the strong secrecy criterion important signal processing consequences and therewith paves the way for providing secure communication with guaranteed, i.e., provable, secrecy. The broadcast channel with confidential messages is studied in [2] for discrete memoryless channels and in [15–17] for MIMO Gaussian channels. However, there is only little work on secure communication over compound channels. The compound wire-

The work of Rafael F. Schaefer was supported by the German Research Foundation (DFG) under Grant WY 151/2-1. The work of Holger Boche was supported in part by the German Research Foundation (DFG) under Grant BO 1734/25-1 and in part by the German Ministry of Education and Research (BMBF) under Grant 01BQ1050.

[1] *Notation:* $X - Y - Z$ denotes a Markov chain of random variables X, Y, and Z; $D(\cdot\|\cdot)$ is the Kullback-Leibler (information) divergence; $\|\mu - \nu\|$ denotes the total variation distance of measures μ and ν.

978-1-4799-2893-4/14/$31.00 ©2014 IEEE

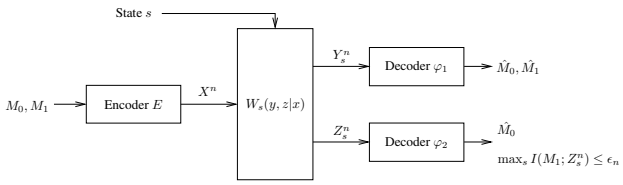

Fig. 1. The transmitter encodes (M_0, M_1) into the codeword $X^n = E(M_0, M_1)$ and sends it to the receivers, which have to decode $(\hat{M}_0, \hat{M}_1) = \varphi_1(Y_s^n)$ and $\hat{M}_0 = \varphi_1(Z_s^n)$ for all $s \in \mathcal{S}$. Receiver 2 has to be kept ignorant of M_1, i.e., $\max_{s\in\mathcal{S}} I(M_1; Z_s^n) \leq \epsilon_n$.

tap channel is analyzed for discrete memoryless channels in [14, 18] and for MIMO Gaussian channels in [19, 20]. First studies for the MIMO Gaussian compound BCC can be found in [21]. Finally, [22] presents first results for the discrete memoryless compound BCC but only for the classical strong secrecy criterion which does not capture the whole behavior of the non-legitimate receiver. They all have in common that they do not explore the signal processing implications.

2. COMPOUND BROADCAST CHANNEL WITH CONFIDENTIAL MESSAGES

Here we introduce the system model for the compound BCC which is depicted in Fig. 1 and formalized as follows. Let $\mathcal{X}$ and $\mathcal{Y}$, $\mathcal{Z}$ be finite input and output sets and $\mathcal{S}$ be a finite index set. Then for fixed channel realization $s \in \mathcal{S}$ and input and output sequences $x^n \in \mathcal{X}^n$ and $y^n \in \mathcal{Y}^n$, $z^n \in \mathcal{Z}^n$, the discrete memoryless broadcast channel is given by $W_s^n(y^n, z^n|x^n) := \prod_{i=1}^n W_s(y_i, z_i|x_i)$. We denote its marginal channels by $W_{\mathcal{Y},s}^n(y^n|x^n)$ and $W_{\mathcal{Z},s}^n(z^n|x^n)$.

Definition 1. *The discrete memoryless* compound broadcast channel $\mathfrak{W}$ *is given by the families of pairs of channels as*

$$\mathfrak{W} := \big\{(W_{\mathcal{Y},s}, W_{\mathcal{Z},s}) : s \in \mathcal{S}\big\}.$$

Let $\mathcal{M}_0 := \{1, ..., M_{0,n}\}$ and $\mathcal{M}_1 := \{1, ..., M_{1,n}\}$ be the sets of common and confidential messages. We write $\mathcal{M} := \mathcal{M}_0 \times \mathcal{M}_1$.

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

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

i.e., a stochastic matrix, and decoders φ_1 *and* φ_2 *at receivers 1 and 2 given by disjoint decoding sets*

$$\big\{\mathcal{D}_1(m_0, m_1) \subset \mathcal{Y}^n : (m_0, m_1) \in \mathcal{M}_0 \times \mathcal{M}_1\big\}$$
$$\big\{\mathcal{D}_2(m_0) \subset \mathcal{Z}^n : m_0 \in \mathcal{M}_0\big\}.$$

The encoder is allowed to be stochastic in the sense that it is specified by conditional probabilities $E(x^n|m_0, m_1)$ with $\sum_{x^n\in\mathcal{X}^n} E(x^n|m_0, m_1) = 1$ for each $m_0 \in \mathcal{M}_0$ and $m_1 \in \mathcal{M}_1$. Thus, $E(x^n|m_0, m_1)$ denotes the probability that the message pair $(m_0, m_1) \in \mathcal{M}_0 \times \mathcal{M}_1$ is encoded as the codeword $x^n \in \mathcal{X}^n$.

Encoder and decoders have to be designed in such a way that they realize reliable communication and secrecy at the same time. Moreover, since neither the transmitter nor the receivers know the actual channel realization, they must be universal such that they work for all channel realizations simultaneously.

When the transmitter has sent the message $m = (m_0, m_1) \in \mathcal{M}$ and receivers 1 and 2 have received $y^n \in \mathcal{Y}^n$ and $z^n \in \mathcal{Z}^n$, the decoder at receiver 1 is in error if $y^n \notin \mathcal{D}_1(m_0, m_1)$. Accordingly, the decoder at receiver 2 is in error if $z^n \notin \mathcal{D}_2(m_0)$. Then for an $(n, M_{0,n}, M_{1,n})$-code, the average probability of errors at the receivers 1 and 2 for channel realization $s \in \mathcal{S}$ are then given by

$$\bar{e}_{1,n}(s) := \frac{1}{|\mathcal{M}|} \sum_{m\in\mathcal{M}} \sum_{x^n\in\mathcal{X}^n} W_{\mathcal{Y},s}^n(\mathcal{D}_1^c(m_0, m_1)|x^n) E(x^n|m)$$

$$\bar{e}_{2,n}(s) := \frac{1}{|\mathcal{M}|} \sum_{m\in\mathcal{M}} \sum_{x^n\in\mathcal{X}^n} W_{\mathcal{Z},s}^n(\mathcal{D}_2^c(m_0)|x^n) E(x^n|m).$$

As reliable communication has to be guaranteed for all $s \in \mathcal{S}$, we set $\bar{e}_{i,n} = \max_{s\in\mathcal{S}} \bar{e}_{i,n}(s)$, $i = 1, 2$.

To ensure the confidential message to be kept secret from non-legitimate receiver 2 for all channel realizations $s \in \mathcal{S}$, we require $\max_{s\in\mathcal{S}} I(M_1; Z_s^n) \leq \epsilon_n$ for some (small) $\epsilon_n > 0$ with M_1 the random variable uniformly distributed over the set $\mathcal{M}_1$ and $Z_s^n = (Z_{s,1}, Z_{s,2}, ..., Z_{s,n})$ the output at receiver 2 for channel realization $s \in \mathcal{S}$. This criterion is known as *strong secrecy* [12, 13].

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

$$\max_{s\in\mathcal{S}} I(M_1; Z_s^n) \leq \epsilon_n \tag{2}$$

while $\bar{e}_{1,n}, \bar{e}_{2,n}, \epsilon_n \to 0$ *as* $n \to \infty$. *The set of all achievable rate pairs is the* strong secrecy capacity region $\mathcal{C}_S(\mathfrak{W})$.

The secrecy is characterized by the mutual information between the message and the channel output at receiver 2. This is the classical approach as used in [2]. However, there were no implications discussed. It is not clear what receiver 2 can or cannot do to infer the confidential information, especially since he is part of the system.

3. STRONG SECRECY AND DECODING PERFORMANCE

3.1. Strong Secrecy and Vanishing Output Variation

The concept of *vanishing output variation* has been identified to be necessary for achieving the strong secrecy capacity of the wiretap channel with side information at the eavesdropper [23]. It suggests itself to study this concept also for the compound BCC. For this purpose we define for each $s \in \mathcal{S}$ the channel to the non-legitimate receiver $\overline{W}_{\mathcal{Z},s}^n(z^n|m_0, m_1) := \sum_{x^n\in\mathcal{X}^n} W_{\mathcal{Z},s}^n(z^n|x^n) E(x^n|m_0, m_1)$ which takes the stochastic encoder E into account, cf. (1).

Definition 4. *A code has exponentially fast* vanishing output variation *if there exists for each* $s \in \mathcal{S}$ *and* $m_0 \in \mathcal{M}_0$ *a non-negative measure* ϑ_{s,m_0} *on* $\mathcal{Z}^n$ *such that for all* $m_1 \in \mathcal{M}_1$ *it holds*

$$\sum_{z^n\in\mathcal{Z}^n} \big|\overline{W}_{\mathcal{Z},s}^n(z^n|m_0, m_1) - \vartheta_{s,m_0}(z^n)\big| \leq 2^{-n\beta} \tag{3}$$

for some $\beta > 0$. *Instead of* (3) *we also write* $\|\overline{W}_{\mathcal{Z},s}^n(\cdot|m_0, m_1) - \vartheta_{s,m_0}\| \leq 2^{-n\beta}$ *interchangeably.*

Next we show that vanishing output variation (3) implies strong secrecy (2), which establishes an desirable and important property.

Proposition 1. *If a code for the compound BCC has the vanishing output variation property, then the strong secrecy criterion satisfies*

$$\max_{s\in\mathcal{S}} I(M_1; Z_s^n) \leq \epsilon_n \tag{4}$$

with $\epsilon_n \to 0$ *exponentially fast as* $n \to \infty$.

Proof. Let $P_{Z_s^n M_0 M_1}$ be the joint distribution and P_{M_0}, P_{M_1}, and $P_{Z_s^n}$ be the marginal distributions where the former are uniformly distributed over $\mathcal{M}_0$ and $\mathcal{M}_1$. With this and $P_{Z_s^n M_1}(z^n, m_1) = \sum_{m_0 \in \mathcal{M}_0} P_{Z_s^n M_0 M_1}(z^n, m_0, m_1)$ we can write

$$P_{Z_s^n M_1}(z^n, m_1) = \frac{1}{|\mathcal{M}|} \sum_{m_0 \in \mathcal{M}_0} \overline{W}_{\mathcal{Z},s}^n(z^n | m_0, m_1). \quad (5)$$

If the code has the vanishing output variation property, we then have for each $s \in \mathcal{S}$ and $m_0 \in \mathcal{M}_0$ a measure ϑ_{s,m_0} which satisfies (3). Averaging over all common messages we obtain the measure $\bar{\vartheta}_s(z^n) \coloneqq \frac{1}{|\mathcal{M}_0|} \sum_{m_0 \in \mathcal{M}_0} \vartheta_{s,m_0}(z^n)$ so that

$$\bar{\vartheta}_{s,M_1}(z^n, m_1) \coloneqq \frac{1}{|\mathcal{M}_1|} \bar{\vartheta}_s(z^n) = \frac{1}{|\mathcal{M}|} \sum_{m_0 \in \mathcal{M}_0} \vartheta_{s,m_0}(z^n) \quad (6)$$

defines a product measure on $\mathcal{Z}^n \times \mathcal{M}_1$. Now by the triangle inequality we can bound the total variation distance by

$$\begin{aligned} &\|P_{Z_s^n M_1} - P_{Z_s^n} P_{M_1}\| \\ &\quad \leq \|P_{Z_s^n M_1} - \bar{\vartheta}_{s,M_1}\| + \|\bar{\vartheta}_{s,M_1} - P_{Z_s^n} P_{M_1}\|. \end{aligned} \quad (7)$$

Next we bound both terms individually. With (5) and (6) we obtain

$$\begin{aligned} &\|P_{Z_s^n M_1} - \bar{\vartheta}_{s,M_1}\| \\ &= \sum_{m_1 \in \mathcal{M}_1} \sum_{z^n \in \mathcal{Z}^n} \left| P_{Z_s^n M_1}(z^n, m_1) - \bar{\vartheta}_{s,M_1}(z^n, m_1) \right| \\ &= \sum_{m_1 \in \mathcal{M}_1} \sum_{z^n \in \mathcal{Z}^n} \left| \frac{1}{|\mathcal{M}|} \sum_{m_0 \in \mathcal{M}_0} \left(\overline{W}_{\mathcal{Z},s}^n(z^n | m_0, m_1) - \vartheta_{s,m_0}(z^n) \right) \right| \\ &\leq \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} \sum_{z^n \in \mathcal{Z}^n} \left| \overline{W}_{\mathcal{Z},s}^n(z^n | m_0, m_1) - \vartheta_{s,m_0}(z^n) \right| \leq 2^{-n\beta} \end{aligned} \quad (8)$$

where the last step follows from the vanishing output variation property, cf. (3). Similarly, with (5) and (6) we get for the second term

$$\begin{aligned} &\|\bar{\vartheta}_{s,M_1} - P_{Z_s^n} P_{M_1}\| \\ &= \sum_{m_1 \in \mathcal{M}_1} \sum_{z^n \in \mathcal{Z}^n} \left| \bar{\vartheta}_{s,M_1}(z^n, m_1) - P_{Z_s^n}(z^n) P_{M_1}(m_1) \right| \\ &= \sum_{m_1 \in \mathcal{M}_1} \sum_{z^n \in \mathcal{Z}^n} \left| \frac{1}{|\mathcal{M}|} \sum_{i \in \mathcal{M}_0} \vartheta_{s,i}(z^n) - \frac{1}{|\mathcal{M}_1|} P_{Z_s^n}(z^n) \right| \\ &= \sum_{m_1 \in \mathcal{M}_1} \sum_{z^n \in \mathcal{Z}^n} \left| \frac{1}{|\mathcal{M}||\mathcal{M}_1|} \sum_{(i,j) \in \mathcal{M}} \left(\vartheta_{s,i}(z^n) - \overline{W}_{\mathcal{Z},s}^n(z^n | i, j) \right) \right| \\ &\leq \frac{1}{|\mathcal{M}|} \frac{1}{|\mathcal{M}_1|} \sum_{(i,j) \in \mathcal{M}} \sum_{m_1 \in \mathcal{M}_1} \sum_{z^n \in \mathcal{Z}^n} \left| \vartheta_{s,i}(z^n) - \overline{W}_{\mathcal{Z},s}^n(z^n | i, j) \right| \\ &\leq 2^{-n\beta} \end{aligned} \quad (9)$$

where the third step follows from the fact that $\vartheta_{s,i}$ does not depend on $j \in \mathcal{M}_1$ and the last step follows from (3). From (8) and (9) follows that the total variation distance in (7) is exponentially small, i.e., $\|P_{Z_s^n M_1} - P_{Z_s^n} P_{M_1}\| \leq 2 \cdot 2^{-n\beta}$ for all $s \in \mathcal{S}$. Then the continuity of the entropy function, cf. [24, Lemma 1.2.7], implies that the mutual information is exponentially small as well, i.e.,

$$\begin{aligned} I(M_1; Z_s^n) &= H(Z_s^n) + H(M_1) - H(Z_s^n, M_1) \\ &= H(P_{Z_s^n} P_{M_1}) - H(P_{Z_s^n M_1}) \\ &\leq -2 \cdot 2^{-n\beta} \log(2 \cdot 2^{-n\beta}) + 2n \cdot 2^{-n\beta} \log(|\mathcal{Z}||\mathcal{M}_1|) \\ &\leq 2^{-n\beta/2} =: \epsilon_n \end{aligned}$$

for all $s \in \mathcal{S}$ where the last inequality holds for n large enough. □

3.2. Decoding Performance of Non-Legitimate Receiver

In addition, to characterize the secrecy of the confidential message also from a signal processing point of view, we want to analyze the decoding performance of the non-legitimate receiver as well. To obtain guaranteed performance bounds, one has to prepare for the worst. This is a non-legitimate receiver who knows the actual channel realization $s \in \mathcal{S}$, but also the common message $m_0 \in \mathcal{M}_0$. However, such knowledge must not provide any information about the confidential information. In more detail, knowing $s \in \mathcal{S}$ and $m_0 \in \mathcal{M}_0$, receiver 2 is able to create decoding sets

$$\left\{ \widetilde{\mathcal{D}}_{s,m_0}(m_1) \subset \mathcal{Z}^n : m_1 \in \mathcal{M}_1 \right\} \quad (10)$$

with $\bigcup_{m_1 \in \mathcal{M}_1} \widetilde{\mathcal{D}}_{s,m_0}(m_1) = \mathcal{Z}^n$ and $\widetilde{\mathcal{D}}_{s,m_0}(m_1) \cap \widetilde{\mathcal{D}}_{s,m_0}(\hat{m}_1) = \emptyset$ for $\hat{m}_1 \neq m_1$. Thus, in contrast to the original communication problem, cf. Definition 2, we allow the decoding sets to depend on the particular channel realization and common message. For channel realization $s \in \mathcal{S}$ this defines the average decoding error as

$$\bar{e}'_{2,n}(s) \coloneqq \frac{1}{|\mathcal{M}|} \sum_{m_0 \in \mathcal{M}_0} \sum_{m_1 \in \mathcal{M}_1} \overline{W}_{\mathcal{Z},s}^n(\widetilde{\mathcal{D}}_{s,m_0}^c(m_1) | m_0, m_1).$$

With this, we define the best decoding performance of the non-legitimate receiver as $\bar{e}'_{2,n} = \min_{s \in \mathcal{S}} \bar{e}'_{2,n}(s)$.

Having in mind that the non-legitimate receiver is aware of the common message, it is also reasonable to question the validity of the expression $\max_{s \in \mathcal{S}} I(M_1; Z_s^n) \leq \epsilon_n$, cf. (2). Therefore we also want to analyze what happens if we replace this by

$$\max_{s \in \mathcal{S}} I(M_1; Z_s^n | M_0) \leq \epsilon_n. \quad (11)$$

Such a secrecy criterion also appears in [25] in the context of rate-distortion-based secrecy for optical communication.

Fortunately, it shows that a code with vanishing output variation (3) implies also strong secrecy in the sense of (11) and further yields the worst decoding performance at the non-legitimate receiver.

Proposition 2. *For any given code of Definition 2, assume that the non-legitimate receiver knows the channel realization $s \in \mathcal{S}$ and the common message $m_0 \in \mathcal{M}_0$ and chooses arbitrary decoding sets as in* (10)*. If the code has vanishing output variation according to Definition 4, cf.* (3)*, then the following holds:*

i) The strong secrecy criterion satisfies

$$\max_{s \in \mathcal{S}} I(M_1; Z_s^n | M_0) \leq \epsilon_n \quad (12)$$

with $\epsilon_n \to 0$ exponentially fast as $n \to \infty$.

ii) The average probability of decoding error satisfies

$$\min_{s \in \mathcal{S}} \bar{e}'_{2,n}(s) \geq 1 - \frac{1}{|\mathcal{M}_1|} - \lambda_n \quad (13)$$

with $\frac{1}{|\mathcal{M}_1|} \to 0$ and $\lambda_n \to 0$ exponentially fast as $n \to \infty$.

Proof. The proof of the first assertion is similar to the one of Proposition 1 and the one given in [25]. With this it easy to show that for any $s \in \mathcal{S}$ and $m_0 \in \mathcal{M}_0$ we have

$$\|P_{Z_s^n M_1 | M_0 = m_0} - P_{Z_s^n | M_0 = m_0} P_{M_1| M_0 = m_0}\| \leq \lambda_n \quad (14)$$

with $\lambda_n = 2 \cdot 2^{-n\beta}$ for all $s \in \mathcal{S}$ and $m_0 \in \mathcal{M}_0$. Similarly as in Proposition 1, the continuity of the entropy function and $I(M_1; Z_s^n | M_0) = \frac{1}{|\mathcal{M}_0|} \sum_{m_0 \in \mathcal{M}_0} I(M_1; Z_s^n | M_0 = m_0)$ imply

$$I(M_1; Z_s^n | M_0) \leq 2^{-n\beta/2} =: \epsilon_n$$

for n large enough proving the strong secrecy criterion (12).

To prove the second assertion (13), we write the average probability of decoding error at the non-legitimate receiver as

$$\begin{aligned}\bar{e}'_{2,n}(s) &= \frac{1}{|\mathcal{M}|}\sum_{m_0\in\mathcal{M}_0}\sum_{m_1\in\mathcal{M}_1}\overline{W}^n_{\mathcal{Z},s}(\widetilde{\mathcal{D}}^c_{s,m_0}(m_1)|m_0,m_1)\\ &= \frac{1}{|\mathcal{M}_0|}\sum_{m_0\in\mathcal{M}_0}\sum_{m_1\in\mathcal{M}_1}P_{Z_s^nM_1|M_0}\big(\widetilde{\mathcal{D}}^c_{s,m_0}(m_1),m_1|m_0\big)\\ &= \frac{1}{|\mathcal{M}_0|}\sum_{m_0\in\mathcal{M}_0}P_{Z_s^nM_1|M_0}\Big(\bigcup_{m_1\in\mathcal{M}_1}\big\{\widetilde{\mathcal{D}}^c_{s,m_0}(m_1),m_1\big\}|m_0\Big). \quad (15)\end{aligned}$$

From (14) we know that for all $s\in\mathcal{S}$ and $m_0\in\mathcal{M}_0$ we have $\|P_{Z_s^nM_1|M_0=m_0}\|\geq\|P_{Z_s^n|M_0=m_0}P_{M_1|M_0=m_0}\|-\lambda_n$ with $\lambda_n\to 0$ as $n\to\infty$. With this we can bound $\bar{e}'_{2,n}(s)$ in (15) from below by

$$\begin{aligned}\bar{e}'_{2,n}(s) &\geq \frac{1}{|\mathcal{M}_0|}\sum_{m_0\in\mathcal{M}_0}\\ &\quad\times P_{Z_s^n|M_0}P_{M_1|M_0}\Big(\bigcup_{m_1\in\mathcal{M}_1}\big\{\widetilde{\mathcal{D}}^c_{s,m_0}(m_1),m_1\big\}|m_0\Big)-\lambda_n\\ &= \frac{1}{|\mathcal{M}_0|}\sum_{m_0\in\mathcal{M}_0}\sum_{m_1\in\mathcal{M}_1}P_{Z_s^n|M_0}P_{M_1|M_0}\big(\widetilde{\mathcal{D}}^c_{s,m_0}(m_1),m_1|m_0\big)-\lambda_n\\ &= \frac{1}{|\mathcal{M}|}\sum_{m_0\in\mathcal{M}_0}\sum_{m_1\in\mathcal{M}_1}P_{Z_s^n|M_0}(\widetilde{\mathcal{D}}^c_{s,m_0}(m_1)|m_0)-\lambda_n\\ &= \frac{1}{|\mathcal{M}|}\sum_{m_0\in\mathcal{M}_0}\sum_{m_1\in\mathcal{M}_1}\big(1-P_{Z_s^n|M_0}(\widetilde{\mathcal{D}}_{s,m_0}(m_1)|m_0)\big)-\lambda_n\\ &= \frac{1}{|\mathcal{M}_0||\mathcal{M}_1|}\sum_{m_0\in\mathcal{M}_0}\big(|\mathcal{M}_1|-1\big)-\lambda_n = 1-\frac{1}{|\mathcal{M}_1|}-\lambda_n\end{aligned}$$

for all $s\in\mathcal{S}$. Note that in the third step we used the fact that M_0 and M_1 are independent. This proves the second assertion (13). □

Finally, we collect all the properties and implications. As the vanishing output variation property guarantees strong secrecy in the sense of (4) and (12) we can generalize and extend the criterion.

Theorem 1. *If a code for the compound BCC has the vanishing output variation property, then secrecy is guaranteed in the information theoretic sense of*

$$\max_{s\in\mathcal{S}}\max\big\{I(M_1;Z_s^n),I(M_1;Z_s^n|M_0)\big\}\leq\epsilon_n \quad (16)$$

but also in the signal processing sense of

$$\min_{s\in\mathcal{S}}\bar{e}'_{2,n}(s)\geq 1-\frac{1}{|\mathcal{M}_1|}-\lambda_n \quad (17)$$

with $\frac{1}{|\mathcal{M}_1|}\to 0$, $\epsilon_n\to 0$, *and* $\lambda_n\to 0$ *exponentially fast as* $n\to\infty$.

Remark 1. *As Theorem 1 holds for any decoding strategy, there are no restrictions on the complexity or computational resources. It leads to universal results which holds for any applied post-processing strategy of the non-legitimate receiver.*

3.3. Operational Meaning

Now, we directly connect the information theoretic criterion with the signal processing inspired concept. The following shows that strong secrecy $\max_{s\in\mathcal{S}}I(M_1;Z_s^n|M_0)\to 0$ exponentially fast implies worst behavior of decoding performance, i.e., $\min_{s\in\mathcal{S}}\bar{e}'_{2,n}(s)\to 1$ exponentially fast. This gives the strong secrecy criterion an important signal processing meaning. This is particularly important as this result shows that any code (not necessarily having the vanishing output variation property) that realizes strong secrecy guarantees that the average decoding error at the non-legitimate receiver goes to 1.

Corollary 1. *The validity of the strong secrecy criterion* $\max_{s\in\mathcal{S}}I(M_1;Z_s^n|M_0)\leq\epsilon_n$ *immediately implies worst decoding performance, i.e.,* $\min_{s\in\mathcal{S}}\bar{e}'_{2,n}(s)\geq 1-\frac{1}{|\mathcal{M}_1|}-\lambda_n$.

Proof. The result follows immediately from Pinsker's inequality, cf. [24, Problem 3.18], and from previous Proposition 2. □

4. IMPLICATIONS ON SECRECY CAPACITY

The previous discussion showed that a code having the vanishing output variation property is desirable for the secrecy task. Next, we discuss that such codes can simultaneously be good for transmitting the common message to both receivers. In [22] an achievable secrecy rate region was established for the classical secrecy criterion of strong secrecy (2) using codes having vanishing output variation. Since codes with vanishing output variation are used, Theorem 1 allows to generalize this region to hold also for the generalized information theoretic criterion (16) and the signal processing inspired criterion of worst decoding performance (17).

Theorem 2. *An achievable secrecy rate region for the compound BCC is the set of all rate pairs* $(R_0,R_1)\in\mathbb{R}_+^2$ *that satisfy*

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

for random variables $U-V-X-(Y_s,Z_s)$. *Furthermore, the generalized criterion of strong secrecy* (16) *goes exponentially fast to 0 and the decoding error* (17) *exponentially fast to 1.*

Moreover, based on [22] and Theorem 2, a multi-letter description of the secrecy capacity region can be established as well.

Remark 2. *A multi-letter description of the strong secrecy capacity region* $\mathcal{C}_S(\mathfrak{W})$ *of the compound BCC* $\mathfrak{W}$ *is given by the set of all rate pairs* $(R_0,R_1)\in\mathbb{R}_+^2$ *that satisfy*

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

for random variables $U-V-X^n-(Y_s^n,Z_s^n)$.

5. CONCLUSION

In this paper, we questioned the validity of the classical definition of strong secrecy for the compound BCC, since the non-legitimate receiver 2 is part of the communication system. As he is intended to decode the common message, this is available as side information for inferring the confidential message. Accordingly we generalized the secrecy criterion taking such side information into account. Along with this, we investigated codes with vanishing output variation and showed that these guarantee both notions of strong secrecy. Moreover, such codes yield the worst decoding performance at the non-legitimate receiver regardless of his computational capabilities. This makes this concept desirable, since it realizes secrecy from the information theoretic and from the signal processing point of view.

6. REFERENCES

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

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

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

[4] Ruoheng Liu and Wade Trappe, Eds., *Securing Wireless Communications at the Physical Layer*, Springer, 2010.

[5] Eduard A. Jorswieck, Anne Wolf, and Sabrina Gerbracht, "Secrecy on the Physical Layer in Wireless Networks," *Trends in Telecommunications Technologies*, pp. 413–435, Mar. 2010.

[6] Matthieu Bloch and João Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, Cambridge University Press, 2011.

[7] Rafael F. Schaefer and Holger Boche, "Physical Layer Service Integration in Wireless Networks – Signal Processing Challenges," *IEEE Signal Process. Mag.*, 2013, will appear.

[8] Deutsche Telekom AG Laboratories, "Next Generation Mobile Networks: (R)evolution in Mobile Communications," *Technology Radar Edition III/2010, Feature Paper*, 2010, available at http://www.lti.ei.tum.de/index.php?id=boche.

[9] Udo Helmbrecht and Rainer Plaga, "New Challenges for IT-Security Research in ICT," in *World Federation of Scientists International Seminars on Planetary Emergencies*, Erice, Italy, Aug. 2008, pp. 1–6.

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

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

[12] Imre Csiszár, "Almost Independence and Secrecy Capacity," *Probl. Pered. Inform.*, vol. 32, no. 1, pp. 48–57, 1996.

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

[14] Igor Bjelaković, Holger Boche, and Jochen Sommerfeld, "Secrecy Results for Compound Wiretap Channels," *Probl. Inf. Transmission*, vol. 49, no. 1, pp. 73–98, Mar. 2013.

[15] Hung D. Ly, Tie Liu, and Yingbin Liang, "Multiple-Input Multiple-Output Gaussian Broadcast Channels With Common and Confidential Messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5477–5487, Nov. 2010.

[16] Ersen Ekrem and Sennur Ulukus, "Capacity Region of Gaussian MIMO Broadcast Channels With Common and Confidential Messages," *IEEE Trans. Inf. Theory*, vol. 58, no. 9, pp. 5669–5680, Sept. 2012.

[17] Ruoheng Liu, Tie Liu, H. Vincent Poor, and Shlomo Shamai (Shitz), "New Results on Multiple-Input Multiple-Output Broadcast Channels With Confidential Messages," *IEEE Trans. Inf. Theory*, vol. 59, no. 3, pp. 1346–1359, Mar. 2013.

[18] Yingbin Liang, Gerhard Kramer, H. Vincent Poor, and Shlomo Shamai (Shitz), "Compound Wiretap Channels," *EURASIP J. Wireless Commun. Netw.*, vol. Article ID 142374, pp. 1–13, 2009.

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

[20] Ashish Khisti, "Interference Alignment for the Multiantenna Compound Wiretap Channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 2976–2993, May 2011.

[21] Mari Kobayashi, Yingbin Liang, Shlomo Shamai (Shitz), and Mérouane Debbah, "On the Compound MIMO Broadcast Channels with Confidential Messages," in *Proc. IEEE Int. Symp. Inf. Theory*, Seoul, Korea, June 2009, pp. 1283–1287.

[22] Rafael F. Wyrembelski and Holger Boche, "Strong Secrecy in Compound Broadcast Channels with Confidential Messages," in *Proc. IEEE Int. Symp. Inf. Theory*, Cambridge, MA, USA, July 2012, pp. 76–80.

[23] Holger Boche and Rafael F. Schaefer, "Wiretap Channels with Side Information – Strong Secrecy Capacity and Optimal Transceiver Design," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 8, pp. 1397–1408, Aug. 2013.

[24] Imre Csiszár and János Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, Cambridge University Press, 2 edition, 2011.

[25] Eva C. Song, Emina Soljanin, Paul Cuff, and H. Vincent Poor, "Rate-Distortion-Based Physical Layer Secrecy in Multimode Fiber," 2013, submitted, available at http://arxiv.org/abs/1304.4181.