Secrecy Capacity Region of Some Classes of Wiretap Broadcast Channels

Meryem Benammar and Pablo Piantanida

Abstract

This work investigates the secrecy capacity of the Wiretap Broadcast Channel (WBC) with an external eavesdropper where a source wishes to communicate two private messages over a Broadcast Channel (BC) while keeping them secret from the eavesdropper. We derive a non-trivial outer bound on the secrecy capacity region of this channel which, in absence of security constraints, reduces to the best known outer bound to the capacity of the standard BC. An inner bound is also derived which follows the behaviour of both the best known inner bound for the BC and the Wiretap Channel. These bounds are shown to be tight for the deterministic BC with a general eavesdropper, the semi-deterministic BC with a more-noisy eavesdropper and the Wiretap BC where users exhibit a less-noisiness order between them. Finally, by rewriting our outer bound to encompass the characteristics of parallel channels, we also derive the secrecy capacity region of the product of two inversely less-noisy BCs with a more-noisy eavesdropper. We illustrate our results by studying the impact of security constraints on the capacity of the WBC with binary erasure (BEC) and binary symmetric (BSC) components.

I. INTRODUCTION

Information theoretic secrecy was first introduced by Shannon in his seminal work [1]. He investigates a communication system between a source, a legitimate receiver and an eavesdropper where the source and the legitimate receiver share a secret key. It is shown that, to achieve perfect secrecy, one has to let the key rate be at least as large as the message rate. This result motivated the work [2] by Wyner who introduced the notion of Wiretap Channel. In such a setting, a source wishes to transmit a message to a legitimate receiver in the presence of an eavesdropper but without resorting to a shared key. Besides communicating reliably to the legitimate receiver

Meryem Benammar and Pablo Piantanida are with the Department of Telecommunications, SUPELEC, 91192 Gif-sur-Yvette, France (e-mail: meryem.benammar, pablo.piantanida@supelec.fr).
at a maximum rate, the source has to maximize the equivocation at the eavesdropper so that it cannot recover the message sent over the channel. In the case of perfect secrecy, the conditional probability of the message given the eavesdropper’s observation has to be approximately uniform over the set of messages, i.e., there is no leakage of information to the eavesdropper. The surprising result of Wyner’s work [2] is that the use of a secret key is no longer required to guarantee a positive equivocation rate or even perfect secrecy. Csiszár & Körner’s [3] generalized this result –first derived with the assumption of a degraded eavesdropper– to the general BC and where the source must also transmit a common message to both users. As a matter of fact, an analysis of the corresponding rate region regarding the necessity of two auxiliary random variables, namely, rate splitting and channel prefixing, was carried out by Ozel & Ulukus in [4]. It was shown that under specific channel ordering the rate region requires only one or even none of these variables.

Several multi-terminal Wiretap networks were studied, e.g., the MAC Wiretap Channel has been investigated by Liang & Poor in [5] while physical layer security in broadcast networks was studied by Liang et al. in [6] though, the capacity region is yet to be fully characterized.

**Related works**

The Wiretap Broadcast Channel (WBC) was first studied under two types of secrecy constraints. The Broadcast Channel (BC) with confidential messages where the encoder transmits two private messages, each to its respective user, while keeping both of them secret from the opposite user. In [7], inner and outer bounds on the secrecy capacity were derived. The secrecy capacity of the semi-deterministic BC with confidential messages is derived in [8] while in [9] it is assumed that only one message has to be kept secret from the other user and the capacity of the semi-deterministic eavesdropper setting was characterized. As for the Gaussian MIMO BCs with confidential messages, it was considered in the works of Liu et al. in [10], [11] while the Gaussian MIMO multi-receiver wiretap channel was addressed by Ekrem & Ulukus in [12] (see [13], [14] and references therein).

An alternate setting is the BC with an **external eavesdropper** where the secrecy requirement consists in that all messages be kept secret from the eavesdropper which is different from both users. Following this setting, the capacity of some classes of ordered and product BCs were first investigated by Ekrem & Ulukus in [15], where the legitimate users’ channels exhibit a
degradedness order and the eavesdropper is more-noisy than all legitimate users’ channels. In a concurrent work by Bagherikaram et al. in [16], the secrecy capacity was characterized for the case where the eavesdropper is degraded towards the weakest user and also for its corresponding additive white Gaussian noise (AWGN) channel model.

**Main contributions**

In this work, we consider the Wiretap BC where the encoder transmits two private messages to two users while it wishes to keep them secret from an external eavesdropper. We derive both an outer bound and an inner bound on the secrecy capacity region of this setting. The outer bound is obtained through a careful single-letter derivation that addresses the main difficulty of our setting which relies on upper bounding techniques for three terminals’ problems. It should be emphasized that both converse techniques for the standard BC and the Wiretap Channel require the use of Csiszár & Körner’s sum-identity [3] which does not apply to more than two output sequences. Besides this well-known difficulty, our outer bound clearly copies the mathematical form and behaviour of the best known outer bound for the BC without an eavesdropper [17]. As for the inner bound, our techniques simply follow the notion of double binning, superposition coding and bit recombination. Moreover, in the absence of secrecy requirement, the obtained inner bound naturally reduces to Marton’s inner bound for the BC with common message [18].

By developing an equivalent but non-straightforward representation of the outer bound, we show that it matches the inner bound for several novel classes of non-degraded Wiretap Broadcast Channels. More precisely, we are able to characterize the secrecy region of the following settings:

1) The deterministic BC with an arbitrary eavesdropper where both legitimate users observe a deterministic function of the input,

2) The semi-deterministic BC with a more-noisy eavesdropper where only one of the legitimate users is a deterministic channel while the other is less-noisy than the eavesdropper,

3) The less-noisy BC with an eavesdropper degraded respect to the best legitimate user,

4) The product of two inversely less-noisy BC with a more-noisy eavesdropper.

Besides of novel secrecy capacity results, the outer and the inner bound also recover some known results, e.g., the degraded BC with a more-noisy eavesdropper [15] which generalizes the degraded BC with a degraded eavesdropper [16].
We finally illustrate the results by investigating the impact of secrecy constraints on the capacity of the Wiretap Broadcast Channel with binary erasure (BEC) and binary symmetric (BSC) components. To this end, we derive the secrecy capacity region of a Less Noisy BEC/BSC BC with a degraded BSC eavesdropper and compare it to the standard capacity region, i.e. without secrecy constraints. In this setting, the central difficulty arises from the converse part for which we were able to show, through convexity arguments, a novel inequality on the conditional entropy of binary sequences. Indeed, this inequality appears to be crucial in the study of the WBC with BSC and BEC components, similar to Mrs. Gerber’s lemma [19] for the binary symmetric BC. The analysis of the secrecy capacity region proved that the degraded eavesdropper’s impediment can be very severe on the BSC user whilst, it would still allow, for the worst degraded case, for positive rates for the BEC user.

The remainder of this paper is organized as follows. In Section II, we give relevant definitions of the Wiretap BC setting and the main outer and inner bounds. We then show in Section III that the obtained bounds are tight for various classes of WBCs. In Section IV, we fully characterize the capacity region of the BEC/BSC Broadcast Channel with a BSC eavesdropper. Sections V, resp. VI are dedicated to the corresponding proofs of the outer, resp. inner bounds. Last, summary and concluding remarks are drawn in Section VIII.

Notations

For any sequence \((x_i)_{i \in \mathbb{N}_+}\), notation \(x_k^n\) stands for the collection \((x_k, x_{k+1}, \ldots, x_n)\). \(x_k^n\) is simply denoted by \(x^n\). Entropy is denoted by \(H(\cdot)\), and mutual information by \(I(\cdot; \cdot)\). \(E\) resp. \(P\) denote the expectation resp. the generic probability while the notation \(P\) is specific to the probability of a random variable (rv). \(\|\mathcal{X}\|\) stands for the cardinality of the set \(\mathcal{X}\). We denote typical and conditional typical sets by \(T^n_\delta(X)\) and \(T^n_\delta(Y|x^n)\), respectively (see Appendix A for details). Let \(X, Y\) and \(Z\) be three random variables on some alphabets with probability distribution \(p\). If \(p(x|yz) = p(x|y)\) for each \(x, y, z\), then they form a Markov chain, which is denoted by \(X \notightarrow Y \notightarrow Z\). The binary entropy function \(h_2\) is defined \(\forall x \in [0 : 1]\) by

\[
h_2(x) \triangleq -x \log_2(x) - (1 - x) \log_2(1 - x),
\]

and the binary convolution operator \((\ast)\) as: \(x \ast y \triangleq x(1 - y) + (1 - x)y\) for all \((x, y) \in [0 : 1]^2\).

We will use FME to designate Fourier-Motzkin elimination.
II. SYSTEM MODEL AND SECRECY CAPACITY BOUNDS

Hereafter, we introduce the Wiretap Broadcast Channel (WBC) as represented in Fig. 1, and then derive both an outer and an inner bound on its secrecy capacity region.

A. The Wiretap Broadcast Channel

- Consider an n-th extension of a three-user memoryless Broadcast Channel:

\[
W^n = \{ P_{Y_1^n Y_2^n Z^n | X^n} : X^n \mapsto Y_1^n \times Y_2^n \times Z^n \},
\]

defined by the conditional p.m.f:

\[
P_{Y_1^n Y_2^n Z^n | X^n} \triangleq \prod_{i=1}^{n} P_{Y_1,i Y_2,i Z,i | X,i}.
\]

- An \((M_{1n}, M_{2n}, n)\)-code for this channel consists of: two sets of messages \(M_1\) and \(M_2\), an encoding function that assigns an n-sequence \(x^n(w_1, w_2)\) to each message pair \((w_1, w_2) \in M_1 \otimes M_1\) and decoding functions, one at each receiver, that assign to the received signal an estimate message \((\hat{w}_j)\) in \(M_j, j \in \{1, 2\}\) or an error.

The probability of error is given by:

\[
P_e^{(n)} \triangleq P\left( \bigcup_{j \in \{1,2\}} \{ \hat{W}_j \neq W_j \} \right).
\]

- A rate pair \((R_1, R_2)\) is said to be achievable if there exists an \((M_{1n}, M_{2n}, n)\)-code satisfying:

\[
\liminf_{n \to \infty} \frac{1}{n} \log_2 M_{jn} \geq R_j \quad \forall j \in \{1, 2\},
\]

\[
\limsup_{n \to \infty} P_e^{(n)} = 0,
\]

\[
\liminf_{n \to \infty} \frac{1}{n} H(W_1 W_2 | Z^n) \geq R_1 + R_2.
\]
Note that the last constraint implies that for some sequence $\epsilon_n$ of positive values:

$$I(W_1W_2; Z^n) \leq n\epsilon_n,$$  \hspace{1cm} (7)

which implies individual secrecy constraints given by

$$I(W_j; Z^n) \leq n\epsilon_n, \; \forall \; j \in \{1, 2\}. \hspace{1cm} (8)$$

- The secrecy capacity region is the closure of the set of all achievable rate pairs $(R_1, R_2)$.

**B. Outer bound on the secrecy capacity region of the WBC**

We next present an outer bound on the secrecy capacity region of the WBC under study. This bound originates from a careful single-letter characterization and accounts for different channel configurations which provides the secrecy capacity region for some new classes of wiretap broadcast channels.

**Theorem 1** (Outer bound). The secrecy capacity region of the Wiretap BC with an external eavesdropper is included in the set of rate pairs satisfying:

1. $R_1 \leq I(U_1; Y_1|TV_1) - I(U_1; Z|TV_1),$ \hspace{1cm} (9)
2. $R_1 \leq I(U_1; Y_1Y_2|TV_1V_2) - I(U_1; Z|TV_1V_2), \hspace{1cm} (10)$
3. $R_1 \leq I(U_1; Y_1|TV_1U_2) - I(U_1; Z|TV_1U_2),$ \hspace{1cm} (11)
4. $R_1 \leq I(U_1; Y_1Y_2|TV_1U_2V_2) - I(U_1; Z|TV_1U_2V_2), \hspace{1cm} (12)$
5. $R_2 \leq I(U_2; Y_2|TV_2) - I(U_2; Z|TV_2),$ \hspace{1cm} (13)
6. $R_2 \leq I(U_2; Y_2Y_1|TV_1V_2) - I(U_2; Z|TV_1V_2), \hspace{1cm} (14)$
7. $R_2 \leq I(U_2; Y_2|TV_2U_1) - I(U_2; Z|TV_2U_1),$ \hspace{1cm} (15)
8. $R_2 \leq I(U_2; Y_2|TU_1V_1V_2) - I(U_2; Z|TU_1V_1V_2),$ \hspace{1cm} (16)
9. $R_1 + R_2 \leq I(X; Y_2|TZV_1) + I(U_1S_1; Y_1|TV_1) - I(U_1S_1; ZY_2|TV_1),$ \hspace{1cm} (17)
10. $R_1 + R_2 \leq I(X; Y_2|TZV_1V_2) + I(U_1S_1; Y_1Y_2|TV_1V_2) - I(U_1S_1; ZY_2|TV_1V_2),$ \hspace{1cm} (18)
11. $R_1 + R_2 \leq I(X; Y_1|TZV_2) + I(U_2S_2; Y_2|TV_2) - I(U_2S_2; ZY_1|TV_2),$ \hspace{1cm} (19)
12. $R_1 + R_2 \leq I(X; Y_1|TZV_1V_2) + I(U_2S_2; Y_2|TV_2) - I(U_2S_2; ZY_1|TV_1V_2),$ \hspace{1cm} (20)
for some joint input p.m.f \( P_{TV_1V_2U_1U_2S_1S_2X} = P_{TV_1V_2U_1U_2S_1S_2}P_{X|U_1U_2S_1S_2} \).

**Proof:** The proof of this theorem is relegated to Section V. \[\Box\]

The next corollary proceeds to the reduction of some auxiliary rvs which can be removed without reducing the rate region. This simplifies the complexity of the optimization of the many variables present in the bound.

**Corollary 1** (Outer bound). The rate region stated in Theorem 9 implies the next outer bound:

\[ R_1 \leq I(U_1; Y_1|TV_1) - I(U_1; Z|TV_1), \quad (21) \]
\[ R_2 \leq I(U_2; Y_2|TV_2) - I(U_2; Z|TV_2), \quad (22) \]
\[ R_1 + R_2 \leq I(X; Y_2|TZV_1) + I(U_1; Y_1|TV_1) - I(U_1; ZY_2|TV_1), \quad (23) \]
\[ R_1 + R_2 \leq I(X; Y_1|TZV_2) + I(U_2; Y_2|TV_2) - I(U_2; ZY_1|TV_2), \quad (24) \]

for some joint input p.m.f \( P_{TV_1V_2U_1U_2X} \).

**Proof:** The proof is relegated to Section V-C. \[\Box\]

It is easy to check that by removing the secrecy constraint, i.e., if \( Z \) is dropped, the above rate region reduces to the best known outer bound to the capacity of the standard BC [17, Lemma 3.5]. Moreover, this outer bound will prove to be crucial to characterize the secrecy capacity of several classes of WBCs, as will be stated later on.

**C. Inner bound on the secrecy capacity region of the WBC**

In this section, we present an inner bound on the secrecy capacity region of the WBC. The coding argument combines both stochastic encoding to achieve secrecy and the standard coding techniques for the BC, i.e., superposition coding and random binning to let the sent codewords be arbitrarily dependent.

**Theorem 2** (Inner bound). The secrecy capacity region of the WBC includes all rate pairs \((R_1, R_2)\) satisfying:

\[ R_1 \leq I(QU_1; Y_1|T) - I(QU_1; Z|T), \quad (25) \]
\[ R_2 \leq I(QU_2; Y_2|T) - I(QU_2; Z|T), \quad (26) \]
Figure 2: Deterministic BC with an arbitrary eavesdropper.

\[ R_1 + R_2 \leq I(U_1; Y_1 | TQ) + I(QU_2; Y_2 | T) - I(U_1; U_2; Z | T) - I(U_1; U_2 | TQ), \]
\[ R_1 + R_2 \leq I(U_2; QU_1 | TQ) + I(U_1; Y_1) + I(U_1; QU_2; Y_2 | T) - I(U_1; U_2; Z | T) - I(U_1; U_2 | TQ), \]
\[ R_1 + R_2 \leq I(QU_1; Y_1 | T) + I(QU_2; Y_2 | T) - I(U_1; U_2; Z | T) - I(U_1; U_2 | TQ) - I(Q; Z | T), \]

for some joint p.m.f. \( P_{TQU_1 U_2 X} \) such that \((T, Q, U_1, U_2) \rightarrow X \rightarrow (Y_1, Y_2, Z)\).

**Proof:** The full proof of this inner bound is given in Section VI.

III. Secrecy Capacity of Some Wiretap Broadcast Channels

In this section, we derive the secrecy capacity of various Wiretap Broadcast Channel models.

A. Deterministic BC with an arbitrary eavesdropper

Let us assume that both legitimate users’ channel outputs are deterministic functions of the input \( X \), as shown in Fig. 2.

**Theorem 3** (Secrecy capacity of the deterministic BC with a general eavesdropper). The secrecy capacity of the deterministic BC with an arbitrary eavesdropper’s channel is given by the set of all rate pairs \((R_1, R_2)\) satisfying:

\[ R_1 \leq H(Y_1 | Z), \]
\[ R_2 \leq H(Y_2 | Z), \]
\[ R_1 + R_2 \leq H(Y_1Y_2 | Z), \]

for some input p.m.f. \( P_X \).
Figure 3: The Semi-deterministic Wiretap Broadcast Channel with a more-noisy eavesdropper.

Proof: We start with the achievability part for which we evaluate the inner bound in Theorem 2 by setting: $Q = \emptyset$, $U_1 = Y_1$ and $U_2 = Y_2$. The claim follows then in a straightforward manner. As for the outer bound, it follows from the reduced outer bound in Corollary 1, by writing the next set of inequalities for $j \in \{1, 2\}$:

$$I(U_j; Y_j|V_j) - I(U_j; Z|V_j) \leq I(U_j; Y_jZ|V_j) - I(U_j; Z|V_j)$$

$$= I(U_j; Y_j|Z, V_j)$$

$$\leq H(Y_j|Z)$$

with strict equality if $U_j = Y_j$ and $V_j = \emptyset$. Note also that:

$$I(X; Y_2|ZV_1) + I(U_1; Y_1|V_1) - I(U_1; ZY_2|V_1) \leq I(X; Y_2|ZV_1) + I(U_1; Y_1|ZV_2V_1)$$

$$\leq H(Y_2|ZV_1) + H(Y_1|ZY_2V_1)$$

$$\leq H(Y_1Y_2|Z)$$

with strict equality if $U_1 = Y_1$ and $V_1 = \emptyset$. The second sum-rate yields the same constraint. Thus, the outer bound is maximized with the choice $U_1 = Y_1$, $U_2 = Y_2$ and $V_1 = V_2 = \emptyset$.

Below, we generalize the equality between the regions in Corollary 1 and Theorem 2 to the case of the Semi-Deterministic BC with a more-noisy eavesdropper.

B. Semi-deterministic BC with a more-noisy eavesdropper

Let us assume that only $Y_1$ is a deterministic function of $X$ but we further assume that $Y_2$ is less-noisy respect to the eavesdropper’s output $Z$, as shown in Fig. 3.
Theorem 4 (Secrecy capacity region of the semi-deterministic BC with a more-noisy eavesdropper). The secrecy capacity of the semi-deterministic BC with a more-noisy eavesdropper is the set of all rate pairs \((R_1, R_2)\) satisfying:

\[
R_1 \leq H(Y_1|ZQ), \quad (39)
\]
\[
R_2 \leq I(U;Y_2|Q) - I(U;Z|Q), \quad (40)
\]
\[
R_1 + R_2 \leq H(Y_1|ZQU) + I(U;Y_2|Q) - I(U;Z|Q) \quad (41)
\]

for some joint p.m.f \(P_{QUX} = P_QP_{U|Q}P_{X|U}\) such that \((Q,U) \leftrightarrow X \leftrightarrow (Y_1,Y_2,Z)\).

Proof: Achievability follows from the rate region stated in Theorem 2 by letting: \(Q = T\) and \(U_1 = Y_1\). As for the converse, we will first evaluate the outer bound given in Corollary 1. Since \(Y_2\) is less-noisy than \(Z\), then one can easily notice that:

\[
I(U;Y_2|VQ) - I(U;Z|VQ) \leq I(UV;Y_2|Q) - I(UV;Z|Q) \quad (42)
\]

Considering the same chain of inequalities as in (34)-(35), one can write the outer bound as:

\[
R_1 \leq H(Y_1|ZQ), \quad (43)
\]
\[
R_2 \leq I(UV;Y_2|Q) - I(UV;Z|Q), \quad (44)
\]
\[
R_1 + R_2 \leq H(Y_1|ZQUV) + I(UV;Y_2|Q) - I(UV;Z|Q) \quad (45)
\]

and thus, defining \((UV) = U\), we can write that the outer bound is the union over all p.m.f \(P_{QUX} = P_QP_{U|Q}P_{X|U}\) of the rate region given in Theorem 4.

Remark 5. When \(Y_2\) is not less-noisy than \(Z\), it is not clear yet whether the two bounds can be tight due to the fact that the auxiliary rv \(V\) does not seem to be useless then.

C. Degraded BC with a more-noisy eavesdropper

In this section, we assume that the legitimate user \(Y_2\) is degraded respect to the legitimate user \(Y_1\). Moreover, assume that both users are less-noisy than the eavesdropper as shown in Fig. 4. The capacity region of this setting was first derived in [20], and here, we simply rely on the optimality of our outer bound for this setting.
Figure 4: Degraded BC with a more-noisy eavesdropper.

**Theorem 6** (Secrecy capacity region of the degraded WBC [20]). The secrecy capacity region of the degraded WBC is given by the set of rate pairs \((R_1, R_2)\) satisfying:

\[
R_1 \leq I(X; Y_1 | TU) - I(X; Z | TU) ,
\]

\[
R_2 \leq I(U; Y_2 | T) - I(U; Z | T) ,
\]

for some input p.m.f \(P_{TUX}\) where \((T, U) \rightarrow X \rightarrow (Y_1, Y_2, Z)\).

**Proof:** To show this, we first note that the outer bound given in Theorem 1 is included in the following outer bound obtained through keeping only the constraints:

\[
R_1 \leq I(U_1; Y_1 Y_2 | TV_1 U_2 V_2) - I(U_1; Z | TV_1 U_2 V_2) ,
\]

\[
R_2 \leq I(U_2; Y_2 | TV_2) - I(U_2; Z | TV_2) .
\]

Now, since \(Y_2\) is degraded respect to \(Y_1\), then

\[
I(U_1; Y_1 Y_2 | TV_1 U_2 V_2) = I(U_1; Y_1 | TV_1 U_2 V_2) ,
\]

and since \(Y_1\) is less-noisy than \(Z\) we can write

\[
I(U_1; Y_1 | TV_1 U_2 V_2) - I(U_1; Z | TV_1 U_2 V_2) \leq I(U_1 V_1; Y_1 | TV_1 U_2) - I(U_1 V_1; Z | TV_2 V_2) \leq I(X; Y_1 | TV_2 V_2) - I(X; Z | TV_2 V_2) .
\]

Thus, the outer bound reduces to the union over all joint p.m.fs \(P_{TUX}\) of the rate region given in Theorem 6.

In the sequel, it turns out that the outer bound we derived yields also the capacity region of another class of ordered BC, which does not include the class of degraded BC with a more-noisy eavesdropper as will be clarified shortly.
D. Less-Noisy BC with a partly degraded eavesdropper

Let us assume that \( Y_1 \) is a less-noisy channel than \( Y_2 \) and that \( Z \) is a degraded version of \( Y_1 \). As shown in Fig. 5, this model is more general than the one first considered in [16], while it does not really generalize the model in Fig. 4, first considered in [20]. Notice that in this setting the eavesdropper is not compulsorily degraded. However, the present class is wider in that users are no longer compulsorily degraded between them and the eavesdropper is no longer more noisy than the weaker legitimate user.

**Theorem 7** (Secrecy capacity region of the less-noisy WBC). The secrecy capacity region of the ordered WBC under study is the set of all rate pairs \((R_1, R_2)\) satisfying:

\[
R_2 \leq I(U; Y_2 | T) - I(U; Z | T) ,
\]

\[
R_1 + R_2 \leq I(X; Y_1 | Z U T) + I(U; Y_2 | T) - I(U; Z | T) ,
\]

for some joint p.m.f \( P_{TUX} = P_T P_{U|T} P_{X|U} \) such that \((T, U) \rightarrow X \leftarrow (Y_1, Y_2, Z)\).

**Proof:** The converse follows from the outer bound in Corollary [1] by keeping only the terms:

\[
R_2 \leq I(U_2; Y_2 | T V_2) - I(U_2; Z | T V_2) ,
\]

\[
R_1 + R_2 \leq I(X; Y_1 | T Z U_2 V_2) + I(U_2; Y_2 | T V_2) - I(U_2; Z Y_1 | T V_2) ,
\]

and defining the common auxiliary rv \( T \equiv (T, V_2) \). As for the achievability, let \( U_1 = X \) and \( Q = U_2 \) in the inner bound given by Theorem [2]. This bound reduces to:

\[
R_1 \leq I(X; Y_1 | T) - I(X; Z | T) = I(X; Y_1 | Z T) ,
\]
Figure 6: The Parallel Broadcast Channel (PBC) with an eavesdropper.

\[
R_2 \leq I(U; Y_2 | T) - I(U; Z | T) , \tag{58}
\]

\[
R_1 + R_2 \leq I(X; Y_1 | ZUT) + I(U; Y_2 | T) - I(U; Z | T) , \tag{59}
\]

\[
R_1 + R_2 \leq I(X; Y_1 | T) - I(X; Z | T) = I(X; Y_1 | ZT) . \tag{60}
\]

The first bound is redundant with respect to the last one. Moreover, since \( Y_1 \) is less-noisy than \( Y_2 \), then the bound (60) becomes redundant with respect to (59). The inner bound reduces henceforth to the one given in Theorem 7.

In the sequel, we study a non-straightforward extension of this WBC for which the secrecy capacity region remained open since the previous results in literature apply only to the degraded BC case.

**E. Product of two inversely less-noisy wiretap broadcast channels**

The product of inversely less-noisy broadcast channels is defined as the product of two less-noisy WBCs. The BC \((Y_1, T_1)\) has a component \( Y_1 \) which is less-noisy than \( T_1 \) and an eavesdropper \( Z_1 \) is degraded towards the best user \( Y_1 \) and more-noisy than the worst user \( T_1 \). The BC \((Y_2, T_2)\) is less-noisy in the inverse order and the eavesdropper \( Z_2 \) is degraded towards \( T_2 \) and more-noisy than \( Y_2 \).

**Theorem 8** (Product of two inversely less-noisy BCs with a more-noisy eavesdropper). The secrecy capacity region of such a setting is given by the set of rates pairs \((R_1, R_2)\) satisfying:

\[
R_1 \leq I(X_1; Y_1 | Z_1) + I(U_2; Y_2) - I(U_2; Z_2) , \tag{61}
\]

\[
R_2 \leq I(X_2; T_2 | Z_2) + I(U_1; T_1) - I(U_1; Z_1) , \tag{62}
\]
\[ R_1 + R_2 \leq I(X_1; Y_1 | Z_1) + I(U_2; Y_2) - I(U_2; Z_2) + I(X_2; T_2 | Z_2 U_2) , \]  
\[ R_1 + R_2 \leq I(X_2; T_2 | Z_2) + I(U_1; T_1) - I(U_1; Z_1) + I(X_1; Y_1 | Z_1 U_1) , \]  

for some input p.m.f \( P_{U_1 X_1 U_2 X_2} = P_{U_1 X_1} P_{U_2 X_2} \) that satisfies \((U_1, U_2) \rightarrow (X_1, X_2) \rightarrow \rightarrow (Y_1, Y_2, T_1, T_2, Z_1, Z_2)\).

**Proof:** The proof is quite evolved in that it requires a new outer bound formulation, and is thus relegated to Appendix G. \(\blacksquare\)

Note here that, in the absence of the eavesdropper, this theorem yields the capacity region of the product of two reversely less-noisy BCs which, though not proved in [21], can be deducted from the result of [22] for the product of reversely more-capable BCs.

**IV. THE BEC/BSC BROADCAST CHANNEL WITH A BSC EAVESDROPPER**

In this section, we characterize the capacity region of the BEC/BSC broadcast channel with an external BSC eavesdropper. This model falls into the class of ordered BCs and is extremely rich since the BC (BEC and BSC) provides for a variety of orderings following the respective values of the erasure probability “e” and the crossover probability “p”, as it is summarized in the table I and shown in [23]. Let us consider the channel model where:

\[
\mathcal{W} : \left\{ \begin{array}{ll}
\mathcal{X} & \leftrightarrow \mathcal{Y}_1 \equiv \text{BEC}(e), \\
\mathcal{X} & \leftrightarrow \mathcal{Y}_2 \equiv \text{BSC}(p_2), \\
\mathcal{X} & \leftrightarrow \mathcal{Z} \equiv \text{BSC}(p).
\end{array} \right.
\]  

| \(0 \leq e \leq 2p\) | \(2p < e \leq 4p(1-p)\) | \(4p(1-p) < e \leq h(p)\) | \(h(p) < e \leq 1\) |
|-----------------|-----------------|-----------------|-----------------|
| BSC degraded than BEC | BEC less-noisy than BSC | BEC more-capable than BSC | BSC Ess. less-noisy than BEC |

Table I: Different orderings allowed by BEC(e) and BSC(p) models.

We will consider the case where \(Y_1\) is less-noisy that \(Y_2\) and where \(Z\) is degraded towards \(Y_2\). Besides, we make sure that \(Z\) is degraded towards \(Y_1\).\(^1\) Summarizing these constraints, we

---

\(^1\)It is worth emphasizing here that our choice of \(Z\) degraded respect to \(Y_2\) follows from that both channels are naturally degraded since these are BSC channels. Otherwise, if \(Y_2\) were to be degraded respect to \(Z\), no positive rate could be transmitted to user 2.
end up with the inequalities:
\[ 2p^2 \leq e \leq \min\{2p, 4p^2(1 - p^2)\}. \] (66)

**Theorem 9** (Secrecy capacity region of the BEC(e) / BSC(p) BC with BSC(p) eavesdropper).

The capacity region of the BC with BEC(e) / BSC(p) components and a BSC(p) eavesdropper, defined by the constraint (66) where \(1 - 4p(1 - p) \geq 4p^2(1 - p^2)\), is given by the set of rate pairs satisfying:

\[
\mathcal{C} : \begin{cases} 
R_1 & \leq (1 - e)h_2(x) + h_2(p) - h_2(p \ast x), \\
R_2 & \leq h_2(p \ast x) - h_2(p_2 \ast x),
\end{cases}
\] (67)

for some \(x \in [0 : 0.5]\).

**Proof:** The proof consists in evaluating the capacity region of such an ordered channel given by the set of rate pairs \((R_1, R_2)\) satisfying:

\[
\mathcal{R} : \begin{cases} 
R_1 & \leq I(X; Y_1|TU) - I(X; Z|TU) = I(X; Y_1|ZTU), \\
R_2 & \leq I(U; Y_2|T) - I(U; Z|T) = I(U; Y_2|ZT),
\end{cases}
\] (68)

and is two fold. The challenging part is obviously the converse part since it requires the use of an inequality, similar in a way to Mrs. Gerber’s lemma [19] applied to the secrecy capacity region, which we have been able to prove only under the assumption \(1 - 4p(1 - p) \geq 4p^2(1 - p^2)\), although there is strong evidence that the converse can be proved besides this case.

Note that \(T = \emptyset\) maximizes the region since it can easily be shown to be convex and thus, will not need the time-sharing variable \(T\). Moreover, we can state a cardinality bound on the auxiliary rv \(U\) used in evaluating the previous region following the usual Fenchel-Eggleston-Carathéodory theorem that is it suffices to evaluate the region using an auxiliary rv with a quaternary alphabet.

First, note that the choice \(X = U \oplus V\) where \(U \sim \text{Bern}(0.5), V \sim \text{Bern}(x)\) yields that \(X \sim \text{Bern}(0.5)\) and that \(X|U \sim \text{Bern}(x)\). Thus, we can write:

\[
I(X; Y_1|U) = (1 - e)H(X|U) = (1 - e)h_2(x), \quad (69)
\]

\[
I(X; Z|U) = h_2(p \ast x) - h_2(p), \quad (70)
\]

\[
I(U; Y_2) = 1 - h_2(p_2 \ast x), \quad (71)
\]

\[
I(U; Z) = 1 - h_2(p \ast x), \quad (72)
\]

which proves the inclusion of the region \(\mathcal{R}\) in the rate region \(\mathcal{C}\), i.e., the achievability.
As for the inclusion in the appositive way, i.e., the converse, we will use the following lemma.

**Lemma 1.** If $1 - 4p(1 - p) \leq 4p_2(1 - p_2)$, then $\mathcal{R}$ defines a convex set.

**Proof:** The proof is given in Appendix E. □

Now, since $\mathcal{R}$ and $\mathcal{C}$ define convex bounded sets, then both are uniquely defined by their supporting hyperplanes. And finally, since $\mathcal{R}$ is included in $\mathcal{C}$, it thus suffices to show that all their supporting hyperplanes intersect, so let then $\lambda \in [0 : \infty[$. We want to show that:

$$\max_{(R_1,R_2) \in \mathcal{C}} R_1 + \lambda R_2 \leq \max_{(R_1,R_2) \in \mathcal{R}} R_1 + \lambda R_2.$$  \hspace{1cm} (73)

Let us choose the following notation: $U$ is an auxiliary rv that takes its values in $\mathcal{U} = \{1, \ldots, \|U\|\}$ following the law: $\mathbb{P}(U = u) = P_U(u) \triangleq p_u$. Let us assume that $X$ is a Bern$(\alpha)$ distributed Binary rv and that $\mathbb{P}(X = 0|U = u) = P_{X|U}(0|u) \triangleq x_u$. Define the set $\mathcal{P}$ of admissible transition probabilities as:

$$\mathcal{P} \triangleq \left\{(\alpha, \mathbf{x}_{\|\ell\|}, \mathbf{p}_{\|\ell\|}) = (\alpha, x_1, \ldots, x_{\|\ell\|}, p_1, \ldots, p_{\|\ell\|}) \in [0 : 0.5]^{\|\ell\|+1} \times [0 : 1]^{\|\ell\|} \bigg| \sum_{u=1}^{\|\ell\|} p_u = 1, \sum_{u=1}^{\|\ell\|} p_u x_u = \alpha \right\}.$$  \hspace{1cm} (74)

With this, note that:

$$\max_{(R_1,R_2) \in \mathcal{C}} R_1 + \lambda R_2 = \max_{U \in \mathcal{X}} \max_{X \in \{(Y_1,Y_2,Z)\}} I(X; Y_1|U) - I(X; Z|U) + \lambda \left[I(U; Y_2) - I(U; Z)\right]$$  \hspace{1cm} (75)

$$= \max_{(\alpha, \mathbf{x}_{\|\ell\|}, \mathbf{p}_{\|\ell\|}) \in \mathcal{P}} h_2(p) + \lambda \left[h_2(p_2 \ast \alpha) - h_2(p \ast \alpha)\right]$$

$$+ \sum_{u \in \mathcal{U}} P_u \left\{(1 - e) h_2(x_u) - h_2(p \ast x_u) + \lambda \left[h_2(p \ast x_u) - h_2(p_2 \ast x_u)\right]\right\}$$  \hspace{1cm} (76)

$$\leq \max_{(\alpha, \mathbf{x}_{\|\ell\|}, \mathbf{p}_{\|\ell\|}) \in \mathcal{P}} h_2(p)$$

$$+ \sum_{u \in \mathcal{U}} P_u \left\{(1 - e) h_2(x_u) - h_2(p \ast x_u) + \lambda \left[h_2(p \ast x_u) - h_2(p_2 \ast x_u)\right]\right\}$$  \hspace{1cm} (77)

$$\leq h_2(p) + (1 - e) h_2(x_u^\lambda) - h_2(p \ast x_u^\lambda) + \lambda \left[h_2(p \ast x_u^\lambda) - h_2(p_2 \ast x_u^\lambda)\right]$$  \hspace{1cm} (78)

Note that the maxima are well defined for both regions due to the cardinality bound (for $C$) and for the closed and bounded interval for $\mathcal{R}$ which results in compact supports for both optimizations.

$\mathcal{U}$ is the support of the law $P_U$, as such, $P_{X|U}(0|u)$ is well defined.
\[\max_{(R_1,R_2) \in \mathcal{R}} R_1 + \lambda R_2, \quad (79)\]

where:

\[x_u^\lambda = \arg \max \left\{ (1 - e) h_2(x) - h_2(p \ast x) + \lambda \left[ h_2(p \ast x) - h_2((p_2 \ast x)) \right] \right\}. \quad (80)\]

Now, (a) follows from the fact that since \(x, p_1, p_2 \in [0 : 1/2]\) and \(p \geq p_2\), then:

\[\forall \alpha \in [0 : 1/2], \quad p_2 \ast \alpha \leq p \ast \alpha \leq 1/2 \quad (81)\]

and

\[\max_{\alpha \in [0, 1/2]} [h_2(p_2 \ast \alpha) - h_2(p \ast \alpha)] = 0 \quad (82)\]

with equality for \(\alpha = 1/2\). As for (b), it is a direct result of the existence of a value of \(x_u^\lambda\) that maximizes the expression, and from that letting \(\mathcal{U} = \{0, 1\}\) and \(P_0 = P_1 = \frac{1}{2}\) and \(U \mapsto X \equiv BSC(x_u^\lambda)\), leads to this maximum value equality in (b) in addition to being admissible: \(P_0 x_u^\lambda + P_1 (1 - x_u^\lambda) = \alpha = \frac{1}{2}\). This ends the proof of equality of the two rate regions.

In the sequel, we evaluate the effect of eavesdropping on such a BEC(e)/BSC(p_2) BC with a BSC(p) eavesdropper.

First note \(C_{std}\) the standard capacity region of the BC without an eavesdropper, \(C\) being its secrecy capacity region. We have that [23]:

\[C_{std} : \begin{cases} R_1 \leq (1 - e) h_2(x), \\ R_2 \leq 1 - h_2(p_2 \ast x), \end{cases} \quad (83)\]

for some \(x \in [0 : 0.5]\).

The presence of eavesdropper engenders an impediment on the sum rate given by \(1 - h_2(p)\), that does not depend on the choice of the channel parameters \((e, p_2)\). As such, it turns out that the channel to user 2, i.e. BSC(p_2) is very sensitive to such the BSC(p) eavesdropper in that it could have zero admissible rate \(R_2\) if the eavesdropper were to have a channel as good as to allow for \(p = p_2\). However, and that’s peculiar to the BEC(e) channel, user 1 always has strictly positive rates whatever the value of \(p\), since \(e \leq 2p \leq h_2(p)\) and thus, a rate of \(h_2(p) - 2p > 0\) is always achievable.

To illustrate this, we consider the following transmission scheme where \(e = 2p\), i.e. the worst eavesdropper is considered for user 1, and where we vary \(p\) in the interval \([p_2 : 0.5]\). Fig[7] plots the obtained curves. As expected, the eavesdropper has no impediment on the available rates for
both users when $p$ is close to 0.5, however, as $p$ decreases, the gap between the standard capacity region and the secrecy capacity region increases, and the rate available at user 2 decreases to zero whilst that of user 1, stays above a given threshold.

V. PROOF OF THEOREM 1: OUTER BOUND

In this section, we prove the outer bound in Theorem 1 since this rate region is symmetric in the rates $R_j$, $j \in \{1, 2\}$, the constraints will be shown only for the following two single rates and two sum-rates:

\[ R_1 \leq I(U_1; Y_1|TV_1) - I(U_1; Z|TV_1) , \tag{84} \]

\[ R_1 \leq I(U_1; Y_1Y_2|TV_1V_2) - I(U_1; Z|TV_1V_2) , \tag{85} \]
\[ R_1 + R_2 \leq I(X; Y_2 T Z V_1) + I(U_1 S_1; Y_1 | T V_1) - I(U_1 S_1; Z Y_2 | T V_1) , \tag{86} \]
\[ R_1 + R_2 \leq I(X; Y_2 T Z V_1 V_2) + I(U_1 S_1; Y_1 Y_2 | T V_1 V_2) - I(U_1 S_1; Z Y_2 | T V_1 V_2) . \tag{87} \]

A. Single rates’ constraints

By Fano’s inequality we have that:
\[ nR_1 \leq I(W_1; Y_1^n) + n \epsilon_n . \tag{88} \]
Moreover, from the secrecy constraint: \( I(W_1; Z^n) \leq n \epsilon_n \). Thus, one can write that:
\[ n R_1 \leq I(W_1; Y_1^n) - I(W_1; Z^n) + 2 n \epsilon_n \tag{89} \]
\[ = \sum_{i=1}^{n} [I(W_1; Y_{1,i} | Y_{1,i}^{-1}) - I(W_1; Z_i | Z_{i+1}^n)] + 2 n \epsilon_n \tag{90} \]
\[ \overset{(a)}{=} \sum_{i=1}^{n} [I(W_1 Z_{i+1}^n; Y_{1,i} | Y_{1,i}^{-1}) - I(W_1 Y_{1,i}^{-1}; Z_i | Z_{i+1}^n)] + 2 n \epsilon_n \tag{91} \]
\[ \overset{(b)}{=} \sum_{i=1}^{n} [I(W_1; Y_{1,i} | Y_{1,i}^{-1} Z_{i+1}^n) - I(W_1; Z_i | Y_{1,i}^{-1} Z_{i+1}^n)] + 2 n \epsilon_n , \tag{92} \]
where (a) and (b) follow both from the Csiszár & Körner’s sum-identity (163):
\[ \sum_{i=1}^{n} [I(Z_{i+1}^n; Y_{1,i} | W_1 Y_{1,i}^{-1}) - I(Y_{1,i}^{-1}; Z_i | W_1 Z_{i+1}^n)] = 0 , \tag{93} \]
\[ \sum_{i=1}^{n} [I(Z_{i+1}^n; Y_{1,i} | Y_{1,i}^{-1}) - I(Y_{1,i}^{-1}; Z_i | Z_{i+1}^n)] = 0 . \tag{94} \]

We then define: \( U_{1,i} = W_1, V_{1,i} = Y_{1,i}^{-1} \) and \( T_i = Z_{i+1}^n \), which yields the first single rate constraint.

In the same fashion, we can write the other single rates by treating the two outputs \( Y_1 \) and \( Y_2 \) together, i.e \( Y_1 \sim (Y_1, Y_2) \) letting \( V_{2,i} = Y_{2,i}^{-1} \). We end up with the couple of constraints:
\[
\begin{cases}
R_1 \leq I(U_1; Y_1 T V_1) - I(U_1; Z T V_1) , \\
R_1 \leq I(U_1; Y_1 Y_2 T V_1 V_2) - I(U_1; Z T V_1 V_2).
\end{cases} \tag{95} \]
Furthermore, similar all manipulations can be performed by starting from the Fano’s inequality and secrecy requirement:
\[ nR_1 \leq I(W_1; Y_1^n | W_2) - I(W_1; Z^n | W_2) + n \epsilon_n . \tag{96} \]
Thus, we could condition over $U_{2,i} = W_2$ the two previous rate constraints to obtain:

$$
\begin{align*}
R_1 &\leq I(U_1; Y_1 | TV_1 U_2) - I(U_1; Z | TV_1 U_2) , \\
R_1 &\leq I(U_1; Y_1 Y_2 | TV_1 U_2 V_2) - I(U_1; Z | TV_1 U_2 V_2) .
\end{align*}
$$

(97)

B. Sum-rate constraints

Let us start by Fano’s inequality writing:

$$
n R_1 \leq I(W_1; Y_1^n) - I(W_1; Y_2^n Z^n) + I(W_1; Y_2^n Z^n) + n \epsilon_n .
$$

(98)

Then, combining with the following constraint obtained from Fano’s inequality:

$$
n R_2 \leq I(W_2; Y_2^n Z^n | W_1) + n \epsilon_n ,
$$

(99)

we can write:

$$
n (R_1 + R_2) \leq I(W_1; Y_1^n) - I(W_1; Y_2^n Z^n) + I(W_1 W_2; Y_2^n Z^n) + 2n \epsilon_n .
$$

(100)

Now, let us elaborate on that:

$$
I(W_1; Y_1^n) - I(W_1; Y_2^n Z^n)

= \sum_{i=1}^{n} [I(W_1; Y_1, i | Y_1^{i-1}) - I(W_1; Y_2, i | Y_1^{i-1}, Z_2^{i+1} Z_{i+1}^n)]

= \sum_{i=1}^{n} [I(W_1 Y_2^{n+1}, Z_2^{n+1}, Y_1, i | Y_1^{i-1}) - I(W_1 Y_1^{i-1}, Y_2, i | Y_1^{i-1}, Z_2^{n+1}, Z_{i+1}^n, Y_1, i)]

= \sum_{i=1}^{n} [I(W_1 Y_1^{i-1}, Y_2^{n+1}, Z_2^{n+1}, Y_1, i) - I(W_1 Y_1^{i-1}, Y_2^{n+1}, Z_2^{n+1}, Y_2, i) + I(Y_2^{n+1}, Z_2^{n+1}, Y_2, i) - I(Y_1^{i-1}, Y_1, i)],
$$

(101)

(102)

(103)

where $(a)$ is again a consequence of Csiszár & Körner’s sum-identity $[163]$:

$$
\sum_{i=1}^{n} [I(Z_{i+1}^{n}, Y_1, i | W_1 Y_1^{i-1}) - I(Y_1^{i-1}, Y_2, i | Z_1^{n}, Z_{i+1}^{n}, Y_1, i)] = 0 .
$$

(104)

As for the other term, note that:

$$
I(W_1 W_2; Y_2^n Z^n) = \sum_{i=1}^{n} [I(W_1 W_2 Y_2^{n}, Z_2^{n}, Y_2, i) - I(Y_2^{n}, Z_2^{n}, Y_2, i)] .
$$

(105)
Looking at the first term of the last equality:

\[
\sum_{i=1}^{n} I(W_1 W_2 Y_{2,i+1}^{n} Z_{i+1}^{n}; Y_{2,i} Z_i)
\]

\[
= \sum_{i=1}^{n} \left[ I(W_1 W_2 Y_{2,i+1}^{n} Z_{i+1}^{n}; Y_{2,i} Z_i) - I(Z_{i}^{i-1}; Y_{2,i} Z_i|W_1 W_2 Y_{2,i+1}^{n} Z_{i+1}^{n}) \right]
\]

\[
= \sum_{i=1}^{n} \left[ I(W_1 W_2 Y_{2,i+1}^{n} Z_{i+1}^{n}; Y_{2,i} Z_i) - I(Y_{2,i+1}^{n} Z_{i+1}^{n}; Z_i|W_1 W_2 Z_{i}^{i-1}) \right]
\]

\[
= \sum_{i=1}^{n} \left[ I(W_1 W_2 Z_{i}^{i-1}; Z_i) + I(W_1 W_2 Y_{2,i+1}^{n} Z_{i+1}^{n} Z_{i}^{i-1}; Y_{2,i} Z_i) \right]
\]

\[
= \sum_{i=1}^{n} \left[ I(W_1 W_2; Z_i) Z_{i}^{i-1} + I(Z_{i}^{i-1}; Z_i) + I(W_1 W_2 Y_{2,i+1}^{n} Z_{i+1}^{n} Z_{i}^{i-1}; Y_{2,i} Z_i) \right].
\]

Here, \((a)\) is a consequence of Csiszár & Körner’s sum-identity \((163)\) but between the outputs \(Z\) and \((Y_{2}, Z)\):

\[
\sum_{i=1}^{n} \left[ I(Z_{i}^{i-1}; Y_{2,i} Z_i|W_1 W_2 Y_{2,i+1}^{n} Z_{i+1}^{n}) - I(Y_{2,i+1}^{n} Z_{i+1}^{n}; Z_i|W_1 W_2 Z_{i}^{i-1}) \right] = 0.
\]

Using the secrecy constraint, one can then notice that:

\[
\sum_{i=1}^{n} I(W_1 W_2; Z_i) Z_{i}^{i-1} = I(W_1 W_2; Z^n) \leq n \epsilon_n.
\]

Moreover, observe that:

\[
\sum_{i=1}^{n} I(Z_{i}^{i-1}; Z_i) = \sum_{i=1}^{n} I(Z_{i+1}^{n}; Z_i),
\]

and

\[
I(W_1 W_2 Y_{2,i+1}^{n} Z_{i+1}^{n} Z_{i}^{i-1}; Y_{2,i} Z_i) \leq I(W_1 W_2 Y_{2,i+1}^{n} Z_{i+1}^{n} Y_{1}^{i-1} Z_{i}^{i-1}; Y_{2,i} Z_i).
\]

The sum-rate can be then bounded as follows:

\[
n(R_1 + R_2) \leq I(W_1; Y_1^n) - I(W_1; Y_2^n Z^n) + I(W_1 W_2; Y_2^n Z^n) + 2n \epsilon_n
\]

\[
\leq \sum_{i=1}^{n} \left[ I(W_1 Y_1^{i-1} Y_{2,i+1}^{n} Z_{i+1}^{n}; Y_{1,i}) - I(W_1 Y_1^{i-1} Y_{2,i+1}^{n} Z_{i+1}^{n}; Y_{2,i} Z_i) \right]
\]

\[
+ I(W_1 W_2 Y_{2,i+1}^{n} Z_{i+1}^{n} Y_{1}^{i-1} Z_{i}^{i-1}; Y_{2,i} Z_i)
\]

\[
+ I(Z_{i+1}^{n}; Z_i) - I(Y_{1}^{i-1}; Y_{1,i})] + 2n \epsilon_n.
\]
And to end, we use the following remarks:

\[
\sum_{i=1}^{n} \left[ I(Z_{i+1}^n; Z_i) - I(Y_1^{i-1}; Y_{1,i}) \right] = \sum_{i=1}^{n} \left[ I(Y_{i-1}^{i-1}Z_{i+1}^n; Z_i) - I(Y_{i-1}^{i-1}Z_{i+1}^n; Y_{1,i}) \right] 
\]

\[
= \sum_{i=1}^{n} \left[ I(Y_{i-1}^{i-1}Z_{i+1}^n; Y_{2,i}Z_i) - I(Y_{i-1}^{i-1}Z_{i+1}^n; Y_{1,i}) \right] - I(Y_{i-1}^{i-1}Z_{i+1}^n; Y_{2,i}Z_i) \] .

(117)

Thus, combining with the previous equality, we end up with:

\[
n(R_1 + R_2) \leq I(W_1; Y_1^n) - I(W_1; Y_2^n Z^n) + I(W_1 W_2; Y_2^n Z^n) + 2n \epsilon_n
\]

\[
\leq \sum_{i=1}^{n} \left[ I(W_1 Y_1^{i-1}Y_{2,i+1}^nZ_{i+1}^n; Y_{1,i}) - I(Y_{i-1}^{i-1}Z_{i+1}^n; Y_{1,i}) \right] - I(W_1 Y_1^{i-1}Y_{2,i+1}^nZ_{i+1}^n; Y_{2,i}Z_i) + I(Y_{i-1}^{i-1}Z_{i+1}^n; Y_{2,i}Z_i)
\]

\[
+ I(W_1 W_2 Y_{2,i+1}^nY_1^{i-1}Z_{i+1}^n Z_{i+1}^n; Y_{2,i}Z_i) - I(Y_{i-1}^{i-1}Z_{i+1}^n; Y_{2,i}Z_i)] + 2n \epsilon_n
\]

\[
\leq \sum_{i=1}^{n} \left[ I(W_1 Y_1^{n}Y_{2,i+1}^n; Y_{1,i}) - I(W_1 Y_2^n Z_{i+1}^n; Y_{1,i}) \right] + I(X_i; Y_{2,i}Z_{i+1}^n) + 2n \epsilon_n .
\]

(119)

(120)

Letting: \(S_{1,i} = Y_{2,i+1}^n, U_{1,i} = W_1, V_{1,i} = Y_1^{i-1}, \) and \(T_i = Z_{i+1}^n, \) by resorting to a standard time-sharing argument we end up with the following single-letter constraint:

\[
R_1 + R_2 \leq I(U_1 S_1; Y_1 V_1 T) - I(U_1 S_1; Y_2 Z | V_1 T) + I(X_i; Y_2 Z V_1 T) .
\]

(121)

Similarly, we can show the same sum-rate constraint, by replacing the output \(Y_1\) with the two outputs \((Y_1 Y_2), \) which results in:

\[
R_1 + R_2 \leq I(X; Y_2 T Z V_1 V_2) + I(U_1 S_1; Y_1 Y_2 T V_1 V_2) - I(U_1 S_1; Y_2 T V_1 V_2) .
\]

(122)

C. Proof of Corollary [7]

In the previous section, we found that an outer bound on the secrecy region for the Wiretap BC can be obtained by considering only the constraints:

\[
R_1 \leq I(U_1; Y_1 | T V_1) - I(U_1; Z | T V_1) ,
\]

(123)

\[
R_2 \leq I(U_2; Y_2 | T V_2) - I(U_2; Z | T V_2) ,
\]

(124)

\[
R_1 + R_2 \leq I(X; Y_2 | T Z V_1) + I(U_1 S_1; Y_1 | T V_1) - I(U_1 S_1; Y_2 | T V_1) ,
\]

(125)

\[
R_1 + R_2 \leq I(X; Y_1 | T Z V_2) + I(U_2 S_2; Y_2 | T V_2) - I(U_2 S_2; Y_1 | T V_2) .
\]

(126)
An important claim is then that the auxiliary rvs $S_1$ and $S_2$ can be eliminated with no impediment to the rate region. Since the region is symmetric in $R_1$ and $R_2$, we only show the claim for $S_1$. We are looking for a random variable $U_1^*$ such that we can write:

$$R_1 \leq I(U_1^*; Y_1 | TV_1) - I(U_1^*; Z | TV_1), \quad (127)$$

$$R_1 + R_2 \leq I(X; Y_2 | TZV_1) + I(U_1^*; Y_1 | TV_1) - I(U_1^*; ZY_2 | TV_1). \quad (128)$$

To see this, define the two following functions:

$$f_1(Q) \triangleq I(U_1; Y_1 | TV_1) - I(U_1; Z | TV_1) - I(Q; Y_1 | TV_1) + I(Q; Z | TV_1),$$

$$f_2(Q) \triangleq I(U_1 S_1; Y_1 | TV_1) - I(U_1 S_1; Y_2 Z | TV_1) - I(Q; Y_1 | TV_1) + I(Q; Y_2 Z | TV_1).$$

We note first that:

$$f_1(U_1) = 0 \quad , \quad f_2(U_1 S_1) = 0. \quad (129)$$

Moreover,

$$f_1(U_1 S_1) + f_2(U_1) = -I(U_1 S_1; Y_2 | TZV_1) + I(U_1; Y_2 | TZV_1)$$

$$= -I(S_1; Y_2 | TZU_1 V_1) \quad (130)$$

$$\leq 0. \quad (131)$$

Therefore, either $f_1(U_1 S_1) \leq 0$ and thus, letting $U_1^* = (U_1 S_1)$ will not reduce the region, or $f_1(U_1) \leq 0$ and in this case $U_1^* = U$ allows us to prove our claim. The same holds for the other couple of constraints on $R_2$ and $R_1 + R_2$.

VI. PROOF OF THEOREM 2: INNER BOUND

In this section, we prove the achievability of the inner bound stated in Theorem 2. Let $R_1$ and $R_2$ denote the information rates. Let $T$ be any the time sharing random variable. The coding argument is as follows.

A. Code generation, encoding and decoding procedures

1) Rate splitting: We split the message intended to each user of rate $R_j$ into two sub-messages: one of rate $\tilde{R}_j = R_j - R_{0j}$ that will be decoded only by the user, and one of rate $R_{0j}$ that will be
carried through the common message. Thus in stead of transmitting the message pair \((w_1, w_2)\), we transmit the triple \((\bar{w}_0, \bar{w}_1, \bar{w}_2)\).

\[
\begin{aligned}
\bar{R}_0 &\triangleq R_{01} + R_{02}, \\
\bar{R}_j &\triangleq R_j - R_{0j} \geq 0.
\end{aligned}
\] (133)

2) Codebook generation: Generate \(2^{nT_0}\) sequences \(q^n(s_0)\) following

\[
P_Q^n(q^n(s_0)) = \prod_{i=1}^{n} P_Q(q^n_i(s_0)),
\] (134)

where \(T_0 \geq \bar{R}_0\) and map these in \(2^{n\bar{R}_0}\) bins indexed by \(\bar{w}_0: B^n_0(\bar{w}_0)\).

For each \(s_0 \in [1 : 2^{nT_0}]\) and for each \(j \in \{1, 2\}\), generate \(2^{nT_j}\) sequences \(u^n_j(s_0, s_j)\) following

\[
P^n_{U_j|Q}(u^n_j(s_0, s_j) | q^n(s_0)) = \prod_{i=1}^{n} P_{U_j|Q}(u^n_{j,i}(s_0, s_j) | q^n_i(s_0)).
\] (135)

Map these sequences in \(2^{n\bar{R}_j}\) bins indexed by \(\bar{w}_j: B^n_j(s_0, \bar{w}_j)\) and consisting in \(2^{n(T_j - \bar{R}_j)}\) \(n\)-sequences. Each of these bins are divided into \(2^{n\bar{R}_j}\) sub-bins indexed by \(l_j: B^n_{j,l}(s_0, \bar{w}_j, l_j)\), thus each bin contains \(2^{n(T_j - \bar{R}_j - \bar{R}_j)}\) sequences where \(0 \leq \bar{R}_j \leq T_j - \bar{R}_j\).

The codebook consisting of all the bins is known to all terminals, including the eavesdropper.

3) Encoding: Fig. 8 plots the encoding operation. To send \((\bar{W}_0, \bar{W}_1, \bar{W}_2)\), the encoder selects at random an index \(s_0\) such that \(q^n(s_0) \in B^n_0(\bar{w}_0)\). Then, in the product bin \(B^n_1(s_0, \bar{w}_1) \times B^n_2(s_0, \bar{w}_2)\), it chooses at random a pair of sub-bins \(B^n_{j,l}(s_0, \bar{w}_1, l_1)\) and \(B^n_{j,l}(s_0, \bar{w}_2, l_2)\) indexed by \(l_1\) and \(l_2\).
In the corresponding product sub-bin, it looks for a pair of sequences indexed with \( s_1 \) and \( s_2 \) satisfying:

\[
(q^n(s_0), u_1^n(s_0, s_1), u_2^n(s_0, s_2)) \in T^n_\delta(QU_1U_2).
\]  

(136)

Based on the Mutual Covering Lemma [24], the encoding will succeed if the following inequalities hold:

\[
\begin{aligned}
T_1 - (\bar{R}_1 + \tilde{R}_1) + T_2 - (\bar{R}_2 + \tilde{R}_2) &> I(U_1; U_2|Q), \\
0 &\leq \bar{R}_1 \leq T_1 - R_1, \\
0 &\leq \tilde{R}_2 \leq T_2 - \bar{R}_2.
\end{aligned}
\]

(137)

4) Decoding: Upon receiving \( y_j^n \), decoder \( j \) looks jointly for a pair of indices \( (s_0, s_j) \) such that:

\[
(q^n(s_0), u_j^n(s_0, s_j), y_j^n) \in T^n_\delta(QU_jY_j).
\]

(138)

From the decoded indices \( s_0 \) and \( s_j \), it can infer the initial values of both \( \bar{W}_0 \) and \( \bar{W}_j \).

Based on Lemma [5] the error probability can be made arbitrarily small provided that:

\[
\begin{aligned}
T_j &\leq I(U_j; Y_j|Q), \\
T_j + T_0 &\leq I(U_j; Y_j).
\end{aligned}
\]

(139)

B. Equivocation analysis

We find conditions on the rates \( T_0, T_1, T_2 \) and \( \bar{R}_1, \bar{R}_2 \) to achieve perfect secrecy for all message triples \((\bar{W}_0, \bar{W}_1, \bar{W}_2)\).

To this end, we first note that it suffices to find conditions for which \( \frac{1}{n} I(\bar{W}_0\bar{W}_1\bar{W}_2; Z^n|C) \) can be made arbitrarily small where \( C \) denotes the codebook used in the transmission, the latter constraint leading to the individual secrecy requirements being fulfilled.

Note that:

\[
I(\bar{W}_0\bar{W}_1\bar{W}_2; Z^n|C) = n(\bar{R}_0 + \bar{R}_1 + \bar{R}_2) - H(\bar{W}_0\bar{W}_1\bar{W}_2|Z^n, C)
\]

\[
\stackrel{(a)}{=} n(\bar{R}_0 + \bar{R}_1 + \bar{R}_2) - H(S_0S_1S_2|Z^n, C)
\]

\[
+ H(S_0S_1S_2|Z^n\bar{W}_0\bar{W}_1\bar{W}_2, C),
\]

(140)

(141)

where (a) follows from that, knowing the codebook, the sent messages are deterministic functions of the binning indices chosen.
We first start by giving a lower bound to \( H(S_0 S_1 S_2 | Z^n, C) \). Let us write:

\[
H(S_0 S_1 S_2 | Z^n, C) = H(S_0 | Z^n, C) + H(S_1 S_2 | S_0, C) - I(S_0; Z^n | S_0, C) = n T_0 - I(S_0; Z^n | C) + H(S_1 S_2 | S_0, C) - I(S_1; S_2 | S_0, C) = n (T_0 + T_1 + T_2) - I(Q^n; Z^n | C) - I(U_1^n; U_2^n | Q^n, C) - I(U_1^n U_2^n; Z^n | Q^n, C),
\]

(142)

where (a) follows similarly from the fact that, knowing the codebook, the sent sequences are functions of the chosen binning indices.

The next lemma provides the main result for carrying on with the analysis.

**Lemma 2.** Assuming the codebook generation presented before, the next inequalities hold true:

\[
I(Q^n; Z^n | C) \leq n I(Q; Z) + n \epsilon_n,
\]

(143)

\[
I(U_1^n; U_2^n | Q^n, C) \leq n I(U_1; U_2 | Q) + n \epsilon_n,
\]

(144)

\[
I(U_1^n U_2^n; Z^n | Q^n, C) \leq n I(U_1 U_2; Z | Q) + n \epsilon_n.
\]

(145)

**Proof:** The proof of this lemma is presented in Appendix B.

Lemma 2 allows us thus to write:

\[
\frac{1}{n} H(S_0 S_1 S_2 | Z^n, C) \geq T_0 + T_1 + T_2 - I(U_1 U_2 | Q) - I(Q U_1 U_2; Z).
\]

(150)

Now, let us upper bound the remainder term to be studied: \( H(S_0 S_1 S_2 | Z^n W_0 W_1 W_2, C) \).

The following Lemma is useful to carry on with the proof.

**Lemma 3.** Assuming the same coding scheme presented before, then

\[
\limsup_{n \to \infty} \frac{1}{n} H(S_0 S_1 S_2 | Z^n W_0 W_1 W_2, C) \leq \max \{0, I_1, I_2, I_3, I_4\}.
\]

(151)
where

\[ I_1 = T_1 - \bar{R}_1 - I(U_1; ZU_2 | Q), \]  
\[ I_2 = T_2 - \bar{R}_2 - I(U_2; ZU_1 | Q), \]  
\[ I_3 = T_1 - \bar{R}_1 + T_2 - \bar{R}_2 - I(U_1U_2; Z | Q) - I(U_1; U_2 | Q), \]  
\[ I_4 = T_0 - \bar{R}_0 + T_1 - \bar{R}_1 + T_2 - \bar{R}_2 - I(QU_1U_2; Z) - I(U_1; U_2 | Q). \]  

Proof: This Lemma is proved in Appendix \[C\].

As a conclusion of this lemma, and combining (141) and (150) we can conclude that:

\[
\frac{1}{n} I(W_0W_1 W_2; Z^n | C) - \epsilon_n \leq \bar{R}_0 + \bar{R}_1 + \bar{R}_2 - (T_0 + T_1 + T_2) \\
+ I(QU_1U_2; Z) + I(U_1; U_2 | Q) + \max \{0, I_1, I_2, I_3, I_4\} \\
= \max \{ \bar{R}_0 + \bar{R}_1 + \bar{R}_2 - (T_0 + T_1 + T_2) + I(QU_1U_2; Z) + I(U_1; U_2 | Q), \bar{R}_0 - T_0 + \bar{R}_2 - T_2 + I(QU_2; Z), \bar{R}_0 - T_0 + \bar{R}_1 - T_1 + I(QU_1; Z), \bar{R}_0 - T_0 + I(Q; Z), 0 \}. \tag{157}
\]

Hence, full secrecy is guaranteed by forcing all operands in the max term to be less than zero.

By collecting all inequalities and applying FME on the rates \(R_{01}\) and \(R_{02}\) (see details in Appendix \[D\]), we obtain the desired rate region:

\[ R_1 \leq I(QU_1; Y_1) - I(QU_1; Z), \]  
\[ R_2 \leq I(QU_2; Y_2) - I(QU_2; Z), \]  
\[ R_1 + R_2 \leq I(U_1; Y_1 | Q) + I(QU_2; Y_2) - I(QU_1U_2; Z) - I(U_1; U_2 | Q), \]  
\[ R_1 + R_2 \leq I(U_2; Y_2 | Q) + I(QU_1; Y_1) - I(QU_1U_2; Z) - I(U_1; U_2 | Q), \]  
\[ R_1 + R_2 \leq I(QU_1; Y_1) + I(QU_2; Y_2) - I(QU_1U_2; Z) - I(U_1; U_2 | Q) - I(Q; Z). \]  

Obviously, the time sharing variable \(T\) can be added and thus, the achievability of the region (25) is proved.

\[\Box\]

VII. Summary and Discussion

In this work, we investigated the secrecy capacity region of the general memoryless two-user Wiretap Broadcast Channel (WBC). We derived a novel outer bound which implies, to
the best of our knowledge, all known capacity results in the corresponding setting while by removing secrecy constraints it performs as well as the best-known outer bound for the general Broadcast Channel (BC). An inner bound on the secrecy capacity region of the WBC was also derived by simply using existent encoding techniques based on random binning and stochastic encoders. These bounds allowed us to characterize the secrecy capacity region of several classes of channels, including the deterministic BC with a general eavesdropper, the semi-deterministic BC with a more-noisy eavesdropper and the less-noisy BC with a degraded eavesdropper, as well as some classes of ordered BCs previously studied. Furthermore, the secrecy capacities of the BC with BEC/BSC components and a BSC eavesdropper, as well as the product of two inversely ordered BC with a degraded eavesdropper were also characterized.

In the same spirit of Corollary 1, a more general study of the role of the auxiliary variables of the outer bound in Theorem 1 may lead to the characterization of capacity for other classes of Wiretap BCs and this will be object of future work.
APPENDIX A

USEFUL NOTIONS AND RESULTS

The appendix below provides basic notions on some concepts used in this paper.

Following [25], we use in this paper strongly typical sets and the so-called Delta-Convention. Some useful facts are recalled here. Let $X$ and $Y$ be random variables on some finite sets $\mathcal{X}$ and $\mathcal{Y}$, respectively. We denote by $P_{XY}$ (resp. $P_{Y|X}$, and $P_X$) the joint probability distribution of $(X,Y)$ (resp. conditional distribution of $Y$ given $X$, and marginal distribution of $X$).

**Definition 10.** For any sequence $x^n \in \mathcal{X}^n$ and any symbol $a \in \mathcal{X}$, notation $N(a|x^n)$ stands for the number of occurrences of $a$ in $x^n$.

**Definition 11.** A sequence $x^n \in \mathcal{X}^n$ is called (strongly) $\delta$-typical w.r.t. $X$ (or simply typical if the context is clear) if

$$\frac{1}{n} N(a|x^n) - P_X(a) \leq \delta \text{ for each } a \in \mathcal{X},$$

and $N(a|x^n) = 0$ for each $a \in \mathcal{X}$ such that $P_X(a) = 0$. The set of all such sequences is denoted by $T^n_\delta(X)$.

**Definition 12.** Let $x^n \in \mathcal{X}^n$. A sequence $y^n \in \mathcal{Y}^n$ is called (strongly) $\delta$-typical (w.r.t. $Y$) given $x^n$ if

$$\frac{1}{n} N(a,b|x^n,y^n) - \frac{1}{n} N(a|x^n) P_{Y|X}(b|a) \leq \delta \text{ for each } a \in \mathcal{X}, b \in \mathcal{Y},$$

and, $N(a,b|x^n,y^n) = 0$ for each $a \in \mathcal{X}, b \in \mathcal{Y}$ such that $P_{Y|X}(b|a) = 0$. The set of all such sequences is denoted by $T^n_\delta(Y|x^n)$.

**Delta-Convention [25]:** For any sets $\mathcal{X}, \mathcal{Y}$, there exists a sequence $\{\delta_n\}_{n \in \mathbb{N}}$ such that lemmas below hold. From now on, typical sequences are understood with $\delta = \delta_n$. Typical sets are still denoted by $T^n_\delta(\cdot)$.

**Lemma 4 ([25] Lemma 1.2.12).** There exists a sequence $\eta_n \xrightarrow{n \to \infty} 0$ such that

$$P_X^n(T^n_\delta(X)) \geq 1 - \eta_n$$

As a matter of fact, $\delta_n \to 0$ and $\sqrt{n} \delta_n \to \infty$ as $n \to \infty$. 

July 22, 2014 DRAFT
Lemma 5 (Joint typicality lemma [24]). There exists a sequence $\eta_n \to 0$ such that
\[
\left| -\frac{1}{n} \log P_Y^n(T^n_\delta(Y|x^n)) - I(X;Y) \right| \leq \eta_n \quad \text{for each } x^n \in T^n_\delta(X).
\]

Lemma 6 (Csiszár & Körner’s sum-identity [3, Lemma 7]). Consider two i.i.d. sequences $X^n$ and $Y^n$, and a constant $C$. The following identity holds:
\[
\sum_{i=1}^{n} I(Y_{i+1}^n; X_i | C X^{i-1}) = \sum_{j=1}^{n} I(X_{j-1}^n; Y_j | C Y_{j+1}^n).
\]

Proof: From the chain rule for conditional mutual information, we can write:
\[
\sum_{i=1}^{n} I(Y_{i+1}^n; X_i | C X^{i-1}) = \sum_{i=1}^{n} \sum_{j=i+1}^{n} I(Y_j; X_i | C X^{i-1} Y_{j+1}^n) = \sum_{i,j: i<j}^{n} I(Y_j; X_i | C X^{i-1} Y_{j+1}^n) = \sum_{j=1}^{n} \sum_{i=1}^{j-1} I(X_i; Y_j | C X^{i-1} Y_{j+1}^n) = \sum_{j=1}^{n} I(X_{j-1}^n; Y_j | C Y_{j+1}^n).
\]

APPENDIX B
PROOF OF LEMMA 2

We want to show the following set of inequalities:
\[
I(Q^n; Z^n) \leq n I(Q; Z) + n \epsilon_n,
\]
\[
I(U_1^n; U_2^n | Q^n) \leq n I(U_1; U_2 | Q) + n \epsilon_n,
\]
\[
I(U_1^n U_2^n; Z^n | Q^n) \leq n I(U_1 U_2; Z | Q) + n \epsilon_n.
\]

All inequalities can be proved using the same approach, so we only prove inequality (165).

Let $\mathcal{E}$ be the indicator function defined by
\[
\mathcal{E} \equaldef \begin{cases} 1 & \text{if } (q^n, u_1^n, u_2^n) \in T^n_\delta(QU_1 U_2) \\ 0 & \text{otherwise} \end{cases}
\]
with probability \( \mathbb{P}(\mathcal{E} = 1) \). We have that:

\[
I(U_1^n; U_2^n | Q^n) \leq I(U_1^n, \mathcal{E}; U_2^n | Q^n) \quad (168)
\]

\[
= I(U_1^n; U_2^n | Q^n, \mathcal{E}) + I(\mathcal{E}; U_2^n | Q^n) \quad (169)
\]

\[
\leq I(U_1^n; U_2^n | Q^n, \mathcal{E}) + 1 \quad (170)
\]

\[
= \mathbb{P}(\mathcal{E} = 1) I(U_1^n; U_2^n | Q^n, \mathcal{E} = 1) + \mathbb{P}(\mathcal{E} = 0) I(U_1^n; U_2^n | Q^n, \mathcal{E} = 0) + 1 \quad (171)
\]

\[
\leq I(U_1^n; U_2^n | Q^n, \mathcal{E} = 1) + n \mathbb{P}(\mathcal{E} = 0) \log_2(\|U_2^n\|) + 1, \quad (172)
\]

where \((a)\) is due to upper bounding \( h_2(\mathcal{E}) \leq 1 \). By the codebook generation, as \( n \) grows large, \( \mathbb{P}(\mathcal{E} = 0) \) can be made arbitrarily small. Note that if encoding is succeeds, only jointly typical sequences \( U_1^n \) and \( U_2^n \) are sent. Then, if \( \mathcal{E} = 1 \), as a result of Lemma \([5]\), we can have

\[
I(U_1^n; U_2^n | Q^n, \mathcal{E} = 1) \leq n I(U_1; U_2 | Q) + n \epsilon_n \quad (173)
\]

and thus,

\[
\frac{1}{n} I(U_1^n; U_2^n | Q^n) \leq I(U_1; U_2 | Q) + 2 \epsilon_n. \quad (174)
\]

The remaining inequalities follow in a similar manner and thus details are omitted here.

**APPENDIX C**

**PROOF OF LEMMA**

In this section, we want to prove the following:

\[
\limsup_{n \to \infty} \frac{1}{n} H(S_0 S_1 S_2 | Z^n W_0 W_1 W_2, C) \leq \max \{0, I_1, I_2, I_3, I_4\}. \quad (175)
\]

To do this, given the output \( z^n \) and the messages \( (\bar{W}_0, \bar{W}_1, \bar{W}_2) \), let us define \( \mathcal{S} \) as the set of indices \( (s_0, s_1, s_2) \) falling in the respective messages’ bins, such that:

\[
(q^n(s_0), u_1^n(s_0, s_1), u_2^n(s_0, s_2), z^n) \in T_\delta^n(Q U_1 U_2 Z). \quad (175)
\]

Then, we can show that the expected size of this list, over all codebooks, is upper bound by

\[
\mathbb{E}(\|\mathcal{S}\|) \leq 1 + 2^{nI_1} + 2^{nI_2} + 2^{nI_3} + 2^{nI_4}, \quad (176)
\]
where:

\[ I_1 = T_1 - R_1 - I(U_1; ZU_2|Q), \]  
\[ I_2 = T_2 - R_2 - I(U_2; ZU_1|Q), \]  
\[ I_3 = T_1 - R_1 + T_2 - R_2 - I(U_1U_2; Z|Q) - I(U_1; U_2|Q), \]  
\[ I_4 = T_0 - R_0 + T_1 - R_1 + T_2 - R_2 - I(QU_1U_2; Z) - I(U_1; U_2|Q). \]

To see this, one can note that:

\[ E\|S\| = P\{ (S_0, S_1, S_2) \in S \} + \sum_{(s_0, s_1, s_2) \neq (S_0, S_1, S_2)} P\{ (s_0, s_1, s_2) \in S \}, \]

where \((S_0, S_1, S_2)\) are the true indices chosen by the source.

Due to the LLN and the codebook construction, and Lemma 4, we can show that:

\[ P\{ (S_0, S_1, S_2) \in S \} \geq 1 - \eta \]

As for the probability of undetected errors, we can distinguish many cases following the values of \((s_0, s_1, s_2)\). Hereafter, we give only representative classes of errors.

- If \(s_1 \neq S_1\) and \((s_0, s_2) = (S_0, S_2)\), then by similar tools to Lemma 5, we can show that:
  \[ P\{ (S_0, s_1, S_2) \in S \} \leq 2^{-nI(U_1; ZU_2|Q) + n\epsilon_n} \]

- If \(s_1 \neq S_1\), \(s_2 \neq S_2\) and \(s_0 = S_0\), then:
  \[ P\{ (S_0, s_1, s_2) \in S \} \leq 2^{-nI(U_1U_2; Z|Q) - nI(U_1; U_2|Q) + n\epsilon_n} \]

- Last, if \(s_0 \neq S_0\), then for all \((s_1, s_2)\),
  \[ P\{ (s_0, s_1, s_2) \in S \} \leq 2^{-nI(QU_1U_2; Z) - nI(U_1; U_2|Q) + n\epsilon_n} \]

Now, once the list size has been bounded, by defining

\[ \mathcal{E} \triangleq \begin{cases} 
1 & \text{if } (S_0, S_1, S_2) \in S \\
0 & \text{if otherwise}
\end{cases} \]
we have that

\[
H(S_0S_1S_2|Z^n\bar{W}_0\bar{W}_1\bar{W}_2, C) = I(\mathcal{E}; S_0S_1S_2|Z^n\bar{W}_0\bar{W}_1\bar{W}_2, C) + H(S_0S_1S_2|Z^n\bar{W}_0\bar{W}_1\bar{W}_2, \mathcal{E}, \mathcal{C})
\]  

(187)

\[
\overset{(a)}{\leq} 1 + H(S_0S_1S_2|Z^n\bar{W}_0\bar{W}_1\bar{W}_2, \mathcal{E}, \mathcal{C})
\]  

(188)

\[
\overset{(b)}{\leq} 1 + H(S_0S_1S_2|Z^n\bar{W}_0\bar{W}_1\bar{W}_2, \mathcal{E} = 1, \mathcal{C})
\]

\[+ \mathbb{P}(\mathcal{E} = 0)H(S_0S_1S_2|\bar{W}_0\bar{W}_1\bar{W}_2) , \]  

(189)

where (a) comes from that the entropy of the binary variable $\mathcal{E}$ is upper-bounded by 1 while (b) follows by upper bounding: $\mathbb{P}(\mathcal{E} = 1) \leq 1$ and

\[
H(S_0S_1S_2|Z^n\bar{W}_0\bar{W}_1\bar{W}_2, \mathcal{E} = 0, \mathcal{C}) \leq H(S_0S_1S_2|\bar{W}_0\bar{W}_1\bar{W}_2) . \]  

(190)

By our codebook construction and Lemma 4, again $\mathbb{P}(\mathcal{E} = 0)$ can be made arbitrarily small. Next, note that:

\[
H(S_0S_1S_2|Z^n\bar{W}_0\bar{W}_1\bar{W}_2, \mathcal{E} = 1, \mathcal{C}) \overset{(a)}{=} H(S_0S_1S_2|Z^n\bar{W}_0\bar{W}_1\bar{W}_2, \mathcal{E} = 1, \mathcal{C}, \mathcal{S}, \|\mathcal{S}\|) \leq H(S_0S_1S_2|\mathcal{E} = 1, \mathcal{S}, \|\mathcal{S}\|) \]  

(191)

\[
= \sum_{s \in \text{supp}(\|\mathcal{S}\|)} P(\|\mathcal{S}\| = s)H(S_0S_1S_2|\mathcal{E} = 1, \mathcal{S}, \|\mathcal{S}\| = s) \]  

(192)

\[
\overset{(b)}{\leq} \sum_{s \in \text{supp}(\|\mathcal{S}\|)} P(\|\mathcal{S}\| = s) \log_2(s) \]  

(193)

\[
= \mathbb{E} [\log_2(\|\mathcal{S}\|)] \]  

(194)

\[
\overset{(c)}{\leq} \log_2 (\mathbb{E} \|\mathcal{S}\|) \]  

(195)

\[
\overset{(d)}{\leq} n \max \{0, I_1, I_2, I_3, I_4\} + \log_2 (5) , \]  

(196)

where (a) follows from the fact that $\mathcal{S}$ and $\|\mathcal{S}\|$ are functions of the output $Z^n$, the codebook and the chosen messages to be sent; (b) is a result of that knowing $\mathcal{E} = 1$, the sent indices $(S_0, S_1, S_2)$ belong to the set $\mathcal{S}$ and thus their uncertainty can not exceed the log cardinality of that set; and finally, (c) is a consequence of Jensen’s inequality while (d) comes from \cite{176} along with an application of the log-sum-exp inequality:

\[
\log_2 \left( \sum_{x \in \mathcal{X}} 2^x \right) \leq \max_{x \in \mathcal{X}} x + \log_2(\|\mathcal{X}\|) . \]  

(197)
This, along with the previous remarks yields the following inequality:

\[
\limsup_{n \to \infty} \frac{1}{n} H(S_0S_1S_2|Z^n\tilde{W}_0\tilde{W}_1\tilde{W}_2, C) \leq \max \{0, I_1, I_2, I_3, I_4\} .
\]  

(199)

**APPENDIX D**

**FOURIER-MOTZKIN ELIMINATION**

We resort to FME, recalling all the constraints:

\[
T_1 \leq I(U_1; Y_1|Q) ,
\]

(200)

\[
T_1 + T_0 \leq I(QU_1; Y_1) ,
\]

(201)

\[
T_2 \leq I(U_2; Y_2|Q) ,
\]

(202)

\[
T_2 + T_0 \leq I(QU_2; Y_2) ,
\]

(203)

\[
T_0 - \tilde{R}_0 \geq I(Q; Z) ,
\]

(204)

\[
T_0 - \tilde{R}_0 + T_1 - \tilde{R}_1 \geq I(QU_1; Z) ,
\]

(205)

\[
T_0 - \tilde{R}_0 + T_2 - \tilde{R}_2 \geq I(QU_2; Z) ,
\]

(206)

\[
T_0 + T_1 + T_2 - (\tilde{R}_0 + \tilde{R}_1 + \tilde{R}_2) \geq I(QU_1U_2; Z) + I(U_1; U_2|Q) ,
\]

(207)

\[
T_1 - \tilde{R}_1 - \tilde{R}_2 + T_2 - \tilde{R}_2 \geq I(U_1; U_2|Q) ,
\]

(208)

\[
0 \leq \tilde{R}_1 \leq T_1 - \tilde{R}_1 , \quad 0 \leq \tilde{R}_2 \leq T_2 - \tilde{R}_2 .
\]

(209)

The resulting rate region after FME is as follows:

\[
\tilde{R}_1 \leq I(U_1; Y_1|Q) ,
\]

(210)

\[
\tilde{R}_1 + \tilde{R}_0 \leq I(QU_1; Y_1) ,
\]

(211)

\[
\tilde{R}_2 \leq I(U_2; Y_2|Q) ,
\]

(212)

\[
\tilde{R}_2 + \tilde{R}_0 \leq I(QU_2; Y_2) ,
\]

(213)

\[
\tilde{R}_1 + \tilde{R}_2 \leq I(U_1; Y_1|Q) + I(U_2; Y_2|Q) - I(U_1; U_2|Q) ,
\]

(214)

\[
\tilde{R}_0 + \tilde{R}_1 + \tilde{R}_2 \leq I(QU_1; Y_1) + I(U_2; Y_2|Q) - I(QU_1U_2; Z) - I(U_1; U_2|Q) ,
\]

(215)

\[
\tilde{R}_0 + \tilde{R}_1 + \tilde{R}_2 \leq I(QU_2; Y_2) + I(U_1; Y_1|Q) - I(QU_1U_2; Z) - I(U_1; U_2|Q) ,
\]

(216)

\[
2\tilde{R}_0 + \tilde{R}_1 + \tilde{R}_2 \leq I(QU_2; Y_2) + I(QU_1; Y_1)
\]

\[
- I(QU_1U_2; Z) - I(U_1; U_2|Q) - I(Q; Z) .
\]

(217)
Eliminating rate splitting parameters:

The achievable rate region writes then as:

\[ R_1 - R_{01} \leq I(U_1; Y_1 | Q) , \]  
\[ R_1 + R_{02} \leq I(QU_1; Y_1) , \]  
\[ R_2 - R_{02} \leq I(U_2; Y_2 | Q) , \]  
\[ R_2 + R_{01} \leq I(QU_2; Y_2) , \]  
\[ R_1 - R_{01} + R_2 - R_{02} \leq I(U_1; Y_1 | Q) + I(U_2; Y_2 | Q) - I(U_1; U_2 | Q) , \]  
\[ R_1 + R_2 \leq I(QU_1; Y_1) + I(U_2; Y_2 | Q) - I(QU_1 U_2; Z) - I(U_1; U_2 | Q) , \]  
\[ R_1 + R_2 \leq I(QU_2; Y_2) + I(U_1; Y_1 | Q) - I(QU_1 U_2; Z) - I(U_1; U_2 | Q) , \]  
\[ R_1 + R_2 + R_{01} + R_{02} \leq I(QU_2; Y_2) + I(QU_1; Y_1) - I(QU_1 U_2; Z) - I(U_1; U_2 | Q) - I(Q; Z) . \]  

Eliminating the rates splitting parameters \( R_{01} \) and \( R_{02} \) with the positivity constrains: \( R_{0,j} > 0 \) and \( R_j - R_{0j} > 0 \) for \( j \in \{1, 2\} \), yields the desired inner bound.

**APPENDIX E**

**PROOF OF LEMMA**

In this section, we show the convexity of the rate region given by:

\[ \mathcal{R} : \begin{cases} R_1 \leq (1 - e) h_2(x) + h_2(p) - h_2(p * x) , \\ R_2 \leq h_2(p * x) - h_2(p_2 * x) . \end{cases} \]  

where the union is over \( x \in [0 : 0.5] \).

Obtaining this result comes to writing an equivalent of Mrs. Gerber’s Lemma in the presence of an eavesdropper in the same fashion as in [19]. Our aim will be to show that, for the corner point of this region, the rate \( R_2 \) is a concave function of the rate \( R_1 \).

Let us define the function \( f_1 \) as follows:

\[ R_1 = f_1(x) \triangleq (1 - e) h_2(x) + h_2(p) - h_2(p * x) . \]  

We have that:

\[ f'_1(x) = (1 - e) h'_2(x) + (1 - 2p) h'_2(p * x) , \]
and,
\[ f''_1(x) = (1 - e)h''_2(x) + (1 - 2p)^2h''_2(p * x) , \]  
(229)

where:
\[ h'_2(x) = \log_2 \left( \frac{1 - x}{x} \right) \quad \text{and} \quad h''_2(x) = -\frac{1}{x(1 - x)} . \]  
(230)

Let us also define the function \( f_2 \) as:
\[ R_2 = f_2(x) \triangleq h_2(p_2 * x) - h_2(p * x) . \]  
(231)

In the same fashion, we can write:
\[ f'_2(x) = (1 - 2p_2)h'_2(p_2 * x) - (1 - 2p)h'_2(p * x) , \]  
(232)

and
\[ f''_2(x) = (1 - 2p_2)^2h''_2(p_2 * x) - (1 - 2p)^2h''_2(p * x) . \]  
(233)

To show that:
\[ \frac{d^2 R_2}{dR_1^2} = \frac{d^2 f_2}{df_1^2} \leq 0 , \]  
(234)

we observe that:
\[ \frac{df_2}{df_1} = \frac{df_2}{dx} \frac{dx}{df_1} = \frac{df_2}{dy} \frac{dy}{df_1} = \frac{1}{f'_1(y)} \frac{df_2}{dx} = \frac{1}{f'_1(x)} \frac{df_2}{dx} . \]  
(235)

As such, one can write in the same manner that:
\[ \frac{d^2 f_2}{df_1^2} = \frac{f''_2(x)f'_1(x) - f''_1(x)f'_2(x)}{(f'_1(x))^3} . \]  
(236)

Since \( 0 \leq x \leq \frac{1}{2} \), then \( 0 \leq p * x \leq \frac{1}{2} \), and thus, one can easily check that:
\[ f'_1(x) \geq 0 . \]  
(237)

Thus, it suffices to show that for all \( x \in [0 : 0.5] \),
\[ f''_2(x)f'_1(x) - f''_1(x)f'_2(x) \leq 0 . \]  
(238)

For notation convenience, we let:
\[ a \triangleq 1 - 2p \quad \text{and} \quad a_2 \triangleq 1 - 2p_2 . \]  
(239)
Now, one can write that:

$$f''_2(x) f'_1(x) - f''_1(x) f'_2(x) = a^2 h''_2(p * x) \left[ (1 - e) h'_2(x) - a_2 h'_2(p_2 * x) \right] - a^2 h''_2(p_2 * x) \left[ (1 - e) h'_2(x) - a h'_2(p * x) \right]$$

$$- (1 - e) h''_2(x) \left[ a h'_2(p * x) - a_2 h'_2(p_2 * x) \right],$$

and thus

$$\frac{f''_2(x) f'_1(x) - f''_1(x) f'_2(x)}{h''_2(p_2 * x) h''_2(p_2 * x) h''_2(x)} = a^2 (1 - e) h'_2(x) - a_2 h'_2(p_2 * x) - a^2 (1 - e) h'_2(x) - a h'_2(p * x)$$

$$- \frac{1}{h''_2(p_2 * x) h''_2(p_2 * x)} \left[ a h'_2(p * x) - a_2 h'_2(p_2 * x) \right].$$

Let us now define a variable $\alpha$ such that: $\alpha \triangleq 1 - 2x$. We have that:

$$a \cdot \alpha = 1 - 2(p * x) \quad \text{and} \quad a_2 \cdot \alpha = 1 - 2(p_2 * x).$$

Moreover:

$$h'_2(x) = \log_2 \left( \frac{1 - x}{x} \right) = \log_2 \left( \frac{1 + \alpha}{1 - \alpha} \right),$$

$$h''_2(x) = - \frac{1}{x(1 - x)} = - \frac{4}{1 - \alpha^2}.$$ (44)

Then, to show the desired inequality (238), since:

$$h''_2(p * x) h''_2(p_2 * x) h''_2(x) \leq 0,$$ (45)

one only has to show, after some simplifications, that:

$$(1 - e) \left( a^2 - a_2^2 \right) \log_2 \left( \frac{1 + \alpha}{1 - \alpha} \right) + a \left( 1 - (a \alpha)^2 \right) \left[ a_2^2 - 1 + e \left( 1 - (a_2 \alpha)^2 \right) \right] \log_2 \left( \frac{1 + a_2 \alpha}{1 - a_2 \alpha} \right)$$

$$- a_2 \left( 1 - (a_2 \alpha)^2 \right) \left[ a_2^2 - 1 + e \left( 1 - (a_2 \alpha)^2 \right) \right] \log_2 \left( \frac{1 + a_2 \alpha}{1 - a_2 \alpha} \right) \geq 0.$$ (46)

We will resort to the known series expansion of the log:

$$\log \left( \frac{1 + \alpha}{1 - \alpha} \right) = 2 \sum_{k=1}^{\infty} \frac{\alpha^k}{k},$$

and thus we must show that:

$$a \cdot \alpha = 1 - 2(p * x) \quad \text{and} \quad a_2 \cdot \alpha = 1 - 2(p_2 * x).$$ (242)

Moreover:

$$h'_2(x) = \log_2 \left( \frac{1 - x}{x} \right) = \log_2 \left( \frac{1 + \alpha}{1 - \alpha} \right),$$

$$h''_2(x) = - \frac{1}{x(1 - x)} = - \frac{4}{1 - \alpha^2}.$$ (44)

Then, to show the desired inequality (238), since:

$$h''_2(p * x) h''_2(p_2 * x) h''_2(x) \leq 0,$$ (45)

one only has to show, after some simplifications, that:

$$(1 - e) \left( a^2 - a_2^2 \right) \log_2 \left( \frac{1 + \alpha}{1 - \alpha} \right) + a \left( 1 - (a \alpha)^2 \right) \left[ a_2^2 - 1 + e \left( 1 - (a_2 \alpha)^2 \right) \right] \log_2 \left( \frac{1 + a_2 \alpha}{1 - a_2 \alpha} \right)$$

$$- a_2 \left( 1 - (a_2 \alpha)^2 \right) \left[ a_2^2 - 1 + e \left( 1 - (a_2 \alpha)^2 \right) \right] \log_2 \left( \frac{1 + a_2 \alpha}{1 - a_2 \alpha} \right) \geq 0.$$ (46)

We will resort to the known series expansion of the log:

$$\log \left( \frac{1 + \alpha}{1 - \alpha} \right) = 2 \sum_{k=1}^{\infty} \frac{\alpha^k}{k},$$

and thus we must show that:

$$a \cdot \alpha = 1 - 2(p * x) \quad \text{and} \quad a_2 \cdot \alpha = 1 - 2(p_2 * x).$$ (242)
\[(a^2 - a^2) \sum_{k=5}^{\infty} k \left[ \left( \frac{1}{k - 2} - \frac{1}{k} \right) T_k - \left( \frac{1}{k - 4} - \frac{1}{k - 2} \right) V_k \right] \geq -\frac{2}{3} \alpha^3 T_3 , \quad (248)\]

for all \( \alpha \in [0 : 1] \), where

\[T_k = (1 - e) \left( 1 - \frac{a^k_{k+1} - a^{k+1}}{a^2 - a^2} \right) + a^2 a^2 \frac{a^k_{k-1} - a^{k-1}}{a^2 - a^2} , \quad (249)\]

\[V_k = e a^2 a_2 \frac{a^k_{3-k} - a^{3-k}}{a^2 - a^2} . \quad (250)\]

By hypothesis \( p_2 \leq p \) and hence \( a^2 - a^2 \geq 0 \). We are thus left with only the analysis of the summation. In the sequel, we show the following results on summation operand.

**Lemma 7** (Properties of some series).

1) *The sequence \((T_k)_k\) dominates the sequence \((V_k)_k\) in that:*

\[(\forall k \in \mathbb{N}_{\text{odd}}) , \ T_k \geq V_k \geq 0 . \quad (251)\]

2) *If \( a^2 + a^2 \leq 1 \), then \((V_k)_{k \geq 5} \) for \( k \) odd is a decreasing sequence.*

3) *The following identity holds:*

\[-\frac{2}{3} \alpha^3 T_3 = \sum_{k=5}^{\infty} \alpha^3 T_3 \left( \frac{1}{k - 2} - \frac{1}{k} - \frac{1}{k - 4} + \frac{1}{k - 2} \right) . \quad (252)\]

**Proof:** Proof is given in Appendix F.

Indeed, Lemma 7 motivates our choice \( a^2 + a^2 \leq 1 \) in the sequel and thus allows us to write:

\[
\sum_{k=5}^{\infty} \alpha^k \left[ \left( \frac{1}{k - 2} - \frac{1}{k} \right) T_k - \left( \frac{1}{k - 4} - \frac{1}{k - 2} \right) V_k \right] + \frac{2}{3} \alpha^3 T_3
\]

\[= \sum_{k=5}^{\infty} \left( \frac{1}{k - 2} - \frac{1}{k} \right) (\alpha^k T_k - \alpha^3 T_3) - \left( \frac{1}{k - 4} - \frac{1}{k - 2} \right) (\alpha^k V_k - \alpha^3 T_3) \quad (254)\]

\[= \sum_{k=5}^{\infty} \left( \frac{1}{k - 2} - \frac{1}{k} \right) (\alpha^k V_k - \alpha^3 T_3) - \left( \frac{1}{k - 4} - \frac{1}{k - 2} \right) (\alpha^k V_k - \alpha^3 T_3) \quad (255)\]

\[= \sum_{k=5}^{\infty} \left( \frac{1}{k - 2} - \frac{1}{k} - \frac{1}{k - 4} + \frac{1}{k - 2} \right) (\alpha^k V_k - \alpha^3 T_3) \quad (256)\]

\[\geq 0 , \quad (257)\]
where (a) comes from claim (3) in Lemma 7 and (b) results from claim (1) in Lemma 7 while (c) comes from the fact that
\[
\frac{1}{k-2} - \frac{1}{k} - \frac{1}{k-4} + \frac{1}{k-2} \leq 0 , \tag{258}
\]
and hence, since \((V_k)_{k \geq 5}\) is a decreasing sequence, then for all \(\alpha \in [0:1]\) we can write that:
\[
(\forall k \geq 5) \quad \alpha^k V_k \leq \alpha^k V_5 \leq \alpha^3 V_5 , \tag{259}
\]
and since:
\[
T_3 - V_5 = (1 - e)(1 - a^2 - a^2 + a^2) \geq 0 , \tag{260}
\]
then,
\[
(\forall k \geq 5) \quad \alpha^k V_k - \alpha^3 T_3 \leq 0 . \tag{261}
\]
It is worth mentioning that the assumption \(a^2 + a^2 \leq 1\) was used only in the monotony of the sequence \((V_k)\).

**APPENDIX F**

**PROOF OF LEMMA 7**

In this section, we prove the claims stated in Lemma 7. We start by showing claim (1) which consists to show that \(\forall k \in \mathbb{N}_{\text{odd}}, T_k \geq V_k \geq 0\). Let the sequence \((S_k)_{k \in \mathbb{N}_{\text{odd}}}\) defined as follows:
\[
S_k = \frac{a_{k-1}^2 - a^{k-1}}{a_2^2 - a^2} , \tag{262}
\]
with \(k - 1 \triangleq 2s\), then one can write that for all \(k \geq 3\),
\[
S_k = \sum_{j=0}^{s-1} a_2^j a^{2(s-1-j)} . \tag{263}
\]
Now, we know that:
\[
T_k = (1 - e)(1 - S_{k+2}) + a_2 a^2 S_k , \tag{264}
\]
\[
V_k = e a_2^2 a_2 S_{k-2} . \tag{265}
\]
Let \(k \geq 3\) for which we have that:
\[
T_k - V_k = (1 - e)(1 - S_{k+2}) + a_2^2 a^2 (S_k - e S_{k-2}) . \tag{266}
\]
It is easy to check that:

\[ S_k = a^{k-3} + a_2^2 S_{k-2} \]  \hspace{1cm} (267)

\[ S_{k+2} = a_2^{k-1} + a^{k-1} + a_2^2 a_2 S_{k-2} \]  \hspace{1cm} (268)

Thus, by substituting these expressions in (266), we end up with the next equality:

\[ T_k - V_k = (1 - e) \left( 1 - a_2^{k-1} - a^{k-1} \right) + a_2^2 a^2 \left( a^{k-3} + (a_2^2 - 1) S_{k-2} \right) \]  \hspace{1cm} (269)

\[ = (1 - e) \left( 1 - a_2^{k-1} - a^{k-1} \right) + a_2^2 a^2 \left( a^{k-3} + (a_2^2 - 1) S_{k-2} \right) \]  \hspace{1cm} (270)

Now, from the choice of the system parameters (66), we see that:

\[ \max\{a, a_2^2\} \leq 1 - e \leq a_2 \]  \hspace{1cm} (271)

Then, to lower bound \( T_k - V_k \) we split into the following cases:

- If \( 1 - a_2^{k-1} - a^{k-1} \geq 0 \), then

\[ T_k - V_k = (1 - e) \left( 1 - a_2^{k-1} - a^{k-1} \right) + a_2^2 a^2 \left( a^{k-3} + (a_2^2 - 1) S_{k-2} \right) \]  \hspace{1cm} (272)

\[ \geq a_2^2 \left( 1 - a_2^{k-1} - a^{k-1} \right) + a_2^2 a^2 \left( a^{k-3} + (a_2^2 - 1) S_{k-2} \right) \]  \hspace{1cm} (273)

\[ = a_2^2 \left( 1 - a_2^{k-1} + (a_2^2 - 1) a^2 S_{k-2} \right) \]  \hspace{1cm} (274)

\[ = a_2^2 (1 - a_2^2) \left( 1 - a_2^{k-1} - a^{k-1} \right) \]  \hspace{1cm} (275)

\[ \overset{(a)}{=} a_2^2 (1 - a_2^2) \left( \sum_{j=0}^{s-1} a_2^j a^2 \sum_{j=0}^{s-2} a_2^j a_2^2 (s-2-j) \right) \]  \hspace{1cm} (276)

\[ = a_2^2 (1 - a_2^2) \left( \sum_{j=0}^{s-1} a_2^j - a^2 \sum_{j=0}^{s-2} a_2^j a_2^2 (s-1-j) \right) \]  \hspace{1cm} (277)

\[ = a_2^2 (1 - a_2^2) \left( a_2^{k-3} + \sum_{j=0}^{s-2} a_2^j \left( 1 - a_2^2 (s-1-j) \right) \right) \geq 0 \]  \hspace{1cm} (278)

where \( (a) \) comes from (263) and some standard manipulations of multinomial coefficients.
• If $1 - a_2^{k-1} - a^{k-1} \leq 0$, then

\[
T_k - V_k = (1 - e) \left(1 - a_2^{k-1} - a^{k-1}\right) + a_2^2 a^2 (a^{k-3} + (a_2^2 - 1) S_{k-2})
\]

\[
\geq (1 - a_2^{k-1} - a^{k-1}) + a_2^2 a^2 (a^{k-3} + (a_2^2 - 1) S_{k-2})
\]

\[
= 1 - a_2^{k-1} - a^{k-1} (1 - a_2^2) - a_2^2 a^2 (1 - a_2^2) S_{k-2}
\]

\[
= (1 - a_2^2) \left( \frac{1 - a_2^{k-1}}{1 - a_2^2} - a^{k-1} - a_2^2 a^2 S_{k-2} \right)
\]

\[
\geq (1 - a_2^2) \left( \frac{1 - a_2^{k-1}}{1 - a_2^2} - a^{k-1} - a_2^4 S_{k-2} \right)
\]

\[
= (1 - a_2^2) \left( \sum_{j=0}^{s-1} a_2^2 - a^{k-1} - a_2^2 \sum_{j=0}^{s-2} a_2^2 j a^2 (s-2-j) \right)
\]

\[
= (1 - a_2^2) \left( \sum_{j=0}^{s-1} a_2^2 - a^{k-1} - \sum_{j=0}^{s-2} a_2^2 (j+2) a^2 (s-2-j) \right)
\]

\[
= (1 - a_2^2) \left( \sum_{j=0}^{s-1} a_2^2 - a^{k-1} - \sum_{j=2}^{s} a_2^2 j a^2 (s-j) \right)
\]

\[
= (1 - a_2^2) \left( \sum_{j=0}^{s-1} a_2^2 - a^{k-1} + a_2^2 - a_2^2 s + \sum_{j=2}^{s-1} a_2^2 j (1 - a^2 (s-j)) \right)
\]

\[
\geq 0
\]

where (a) comes from that $a_2 \geq a \geq 0$.

This proves our claim. Next, we show that if $a^2 + a_2^2 \leq 1$ then $(V_k)_{k \geq 5}$ is decreasing for $k$ odd.

Let $k$ be an odd integer such that $k \geq 5$. We have that:

\[
\frac{V_{k+2} - V_k}{ea^2a_2^2} = S_{k+2} - S_k
\]

We check our last claim by induction, i.e., assuming $S_7 - S_5 \leq 0$ and

\[
\forall k \geq 5, S_{k+2} - S_k \leq 0 \quad \text{then} \quad S_{k+4} - S_{k+2} \leq 0
\]

To this end, we have that:

\[
S_7 - S_5 = a_2^2 (a^2 + a_2^2 - 1) \leq 0
\]
Let then $k \geq 5$, such that $S_{k+2} - S_k \leq 0$, thus:

\[ S_{k+4} - S_{k+2} = a_2^{k+1} + (a^2 - 1)S_{k+2} \]
\[ = a_2^{k+1} + (a^2 - 1)\left(a_2^{k-1} + a^2S_k\right) \]
\[ = a_2^{k+1} - a_2^{k-1} + a^2\left(a_2^{k-1} + (a^2 - 1)S_k\right) \]
\[ = a_2^{k+1} - a_2^{k-1} + a^2\left(S_{k+2} - S_k\right) \]
\[ \leq 0 , \]

which proves the claim. Finally, it is easy to verify that:

\[-\frac{2}{3} \alpha^3 T_3 = \sum_{k=5}^{\infty} \alpha^3 T_3 \left(\frac{1}{k-2} - \frac{1}{k} - \frac{1}{k-4} + \frac{1}{k-2}\right) , \]

by noticing

\[ \sum_{k=5}^{\infty} \left(\frac{1}{k-2} - \frac{1}{k} - \frac{1}{k-4} + \frac{1}{k-2}\right) = -\frac{2}{3} . \]

**APPENDIX G**

**PROOF OF THEOREM 8**

In this section, we prove the result on the product of the two inversely less-noisy BC with a more-noisy eavesdropper.

**A. Proof of the achievability**

The achievability easily follows by evaluating the region:

\[ \begin{align*}
R_1 & \leq I(QU_1; Y) - I(QU_1; Z) , \\
R_2 & \leq I(QU_2; T) - I(QU_2; Z) , \\
R_1 + R_2 & \leq I(U_1; Y|Q) + I(QU_2; T) - I(QU_1U_2|Z; Y) - I(U_1; U_2|Q) , \\
R_1 + R_2 & \leq I(QU_1; Y) + I(U_2; T|Q) - I(QU_1U_2|Z) - I(U_1; U_2|Q) , \\
R_1 + R_2 & \leq I(QU_1; Y) - I(QU_1; Z) + I(QU_2; T) - I(QU_2; Z) - I(U_1; U_2|ZQ) ,
\end{align*} \]

based on the choices: $Q = (U_1, U_2)$ and $U_1 = X_1$ and $U_2 = X_2$ such that $P_{U_1X_1U_2X_2} = P_{U_1X_1}P_{U_2X_2}$. 

July 22, 2014
The single rate constraints write thus as:

\[ R_1 \leq I(X_1; Y_1) - I(X_1; Z_1) + I(U_2; Y_2) - I(U_2; Z_2) \]  
\[ \overset{(a)}{=} I(X_1; Y_1|Z_1) + I(U_2; Y_2) - I(U_2; Z_2) , \]  

where \((a)\) is a result of that \(Z_1\) is degraded towards \(Y_1\). The sum-rates follow in a similar fashion, however the last sum-rate is redundant since:

\[ I(X_1; X_2|Z_1 Z_2 U_1 U_2) \leq I(X_1; X_2|U_1 U_2) = 0 . \]  

\[ \text{(302)} \]

\[ \text{B. Proof of the converse} \]

Let us concatenate the two outputs \(Y = (Y_1, Y_2)\), \(Z = (Z_1, Z_2)\) and \(T = (T_1, T_2)\). We start by single rate constraints.

1) Single-rate constraints: By Fano’s inequality and the secrecy constraint, we have that:

\[ n(R_1 - \epsilon_n) \leq I(W_1; Y^n) - I(W_1; Z^n) \]  
\[ \leq I(W_1; Y^n Z^n_1) - I(W_1; Z^n) \]  
\[ = I(W_1; Y^n|Z^n_1) - I(W_1; Z^n_2|Z^n_1) . \]

Thus, by standard Csiszár & Körner’s sum-identity \(\text{[165]}\) and some basic manipulations, we get that:

\[ n(R_1 - \epsilon_n) \leq \sum_{i=1}^{n} \left[ I(W_1; Y_1^n Z^n_1 Y^{i-1} Z^n_{2,i+1}) - I(W_1; Z_1^n Y^{i-1} Z^n_{2,i+1}) \right] \]  
\[ = \sum_{i=1}^{n} \left[ I(W_1; Y_1 Y_2^n Z^n_1 Y^{i-1} Z^n_{2,i+1}) - I(W_1; Z_2^n Y^{i-1} Z^n_{2,i+1}) \right] \]  
\[ = \sum_{i=1}^{n} \left[ I(W_1; Y_2^n Z^n_1 Y^{i-1} Z^n_{2,i+1}) - I(W_1; Z_2^n Y^{i-1} Z^n_{2,i+1}) \right] \]  
\[ + I(W_1; Y_1^n Y_2^n Z^n_1 Y^{i-1} Z^n_{2,i+1}) \]  
\[ \overset{(a)}{=} \sum_{i=1}^{n} \left[ I(W_1; Y_2^n Z^n_1 Y^{i-1} Z^n_{2,i+1}) - I(W_1; Z_1^n Y^{i-1} Z^n_{2,i+1}) \right] \]  
\[ + I(W_1; Y_1^n Y_2^n Z^n_1 Y^{i-1} Z^n_{2,i+1}) \]  
\[ \leq \sum_{i=1}^{n} \left[ I(W_1; Y_2^n Z^n_1 Y^{i-1} Z^n_{2,i+1}) - I(W_1; Z_2^n Y^{i-1} Z^n_{2,i+1}) \right] \]  
\[ + I(X_1; Y_1^n Z^n_1) , \]  

\[ \text{(310)} \]
where (a) follows from that $Z_1$ is degraded respect to $Y_1$ and (b) comes from the Markov chain:

$$(Z_1^{i-1}, Y^{i-1}, Z_2^n, Y_{2,i}) \rightarrow X_{1,i} \rightarrow (Y_{1,i}, Z_{1,i}) .$$ (311)

Thus, letting $U_{2,i} = W_1$ and $V_2 = (Z_1^n, Y^{i-1}, Z_2^n)$ we can simply get the rate constraint:

$$R_1 \leq I(X_1; Y_1|Z_1) + I(U_2; Y_2|V_2) - I(U_2; Z_2|V_2) .$$ (312)

2) Sum-rate constraint: We start by writing:

$$n(R_1 + R_2 - \epsilon_n) \leq I(W_1; Y^n) - I(W_1; T^nZ^n) + I(W_1W_2; T^nZ^n)$$ (313)

$$\leq I(W_1; Y^nZ^n) - I(W_1; T^nZ^n) + I(W_1W_2; T^nZ^n)$$ (314)

$$\overset{(a)}{=} I(W_1; Y^n|Z^n_1) - I(W_1; T^nZ^n_2|Z^n_1) + I(W_1W_2; T^nZ^n_2|Z^n_1) + n\epsilon_n ,$$ (315)

where (a) follows from the secrecy constraint. By standard manipulations, similarly to those used in the proof of the outer bound in Section [V-B] write that:

$$n(R_1 + R_2 - \epsilon_n) \leq \sum_{i=1}^{n} \left[ I(W_1T^n_{i+1}; Y_{i}|Z^n_1Y^{i-1}Z^n_{2,i+1}) - I(W_1T^n_{i+1}; T_1Z_{2,i}|Z^n_1Y^{i-1}Z^n_{2,i+1}) \right.$$ 

$$+ I(W_1W_2T^n_{i+1}Z^n_{2,i}; T_1Z_{2,i}Z^n_1Y^{i-1}Z^n_{2,i+1}) \right]$$ (316)

$$= \sum_{i=1}^{n} \left[ I(W_1T^n_{i+1}; Y_{1,i}, Y_{2,i}|Z^n_1Y^{i-1}Z^n_{2,i+1}) - I(W_1T^n_{i+1}; T_1T_2Z_{2,i}|Z^n_1Y^{i-1}Z^n_{2,i+1}) \right.$$ 

$$+ I(W_1W_2T^n_{i+1}Z^n_{2,i}; T_1T_2Z_{2,i}Z^n_1Y^{i-1}Z^n_{2,i+1}) \right]$$ (317)

$$= \sum_{i=1}^{n} \left[ I(W_1T^n_{i+1}; Y_{2,i}|Z^n_1Y^{i-1}Z^n_{2,i+1}) - I(W_1T^n_{i+1}; T_2Z_{2,i}|Z^n_1Y^{i-1}Z^n_{2,i+1}) \right.$$ 

$$+ I(W_1W_2T^n_{i+1}Z^n_{2,i}; T_2Z_{2,i}Z^n_1Y^{i-1}Z^n_{2,i+1}) \right.$$ 

$$\leq \sum_{i=1}^{n} \left[ I(W_1T^n_{i+1}; Y_{2,i}|Z^n_1Y^{i-1}Z^n_{2,i+1}) - I(W_1T^n_{i+1}; T_2Z_{2,i}|Z^n_1Y^{i-1}Z^n_{2,i+1}) \right.$$ 

$$+ I(X_{2,i}; T_2Z_{2,i}Z^n_1Y^{i-1}Z^n_{2,i+1}) \right.$$ 

$$+ I(W_1T^n_{i+1}; Y_{1,i}|Y_{2,i}Z^n_1Y^{i-1}Z^n_{2,i+1}) - I(W_1T^n_{i+1}; T_1T_2Z_{2,i}Z^n_1Y^{i-1}Z^n_{2,i+1})$$ 

$$+ I(W_1W_2T^n_{i+1}Z^n_{2,i}; T_1T_2Z_{2,i}Z^n_1Y^{i-1}Z^n_{2,i+1}) \right] .$$ (319)
On one hand, we observe that:

\[
I(W_1 T_{i+1}^n; Y_{1,i} \| Y_{2,i} Z_1^n Y^{i-1} Z_2^n_{i+1}) - I(W_i T_{i+1}^n; T_{1,i} | T_{2,i} Z_2^n Z_1^n Y^{i-1} Z_2^n_{i+1}) \\
+ I(W_1 W_2 T_{i+1}^n Z_2^{i-1}; T_{1,i} | T_{2,i} Z_2^n Z_1^n Y^{i-1} Z_2^n_{i+1}) \\
= I(W_1 T_{i+1}^n; Y_{1,i} \| Y_{2,i} Z_1^n Y^{i-1} Z_2^n_{i+1}) + I(W_2 Z_2^{i-1}; T_{1,i} | T_{2,i} Z_2^n Z_1^n Y^{i-1} Z_2^n_{i+1}) W_1 T_{i+1}^n) \\
= I(W_1 T_{i+1}^n; Y_{1,i} \| Y_{2,i} Z_1^n Y^{i-1} Z_2^n_{i+1}) + I(W_2 Z_2^{i-1}; T_{1,i} | T_{2,i} Z_1^n Y^{i-1} Z_2^n_{i+1}) W_1 T_{i+1}^n) \\
\leq I(W_1 T_{i+1}^n; Y_{1,i} \| Y_{2,i} Z_1^n Y^{i-1} Z_2^n_{i+1}) + I(X_{1,i}; T_{1,i} | T_{2,i} Z_1^n Y^{i-1} Z_2^n_{i+1}) W_1 T_{i+1}^n) ,
\]

where (a) follows from that $Z_2$ is degraded respect to $T_2$. On the other hand, we have that:

\[
I(X_{1,i}; T_{1,i} | T_{2,i} Z_{1,i}) \overset{(a)}{=} I(X_{1,i}; T_{1,i} | Z_{1,i}) - I(T_{2,i}; T_{1,i} | Z_{1,i}) \\
\overset{(b)}{\leq} I(X_{1,i}; T_{1,i} | Z_{1,i}) - I(Y_{2,i}; T_{1,i} | Z_{1,i}) \\
\overset{(a)}{=} I(X_{1,i}; T_{1,i} | Y_{2,i} Z_{1,i}) ,
\]

where (a) and (b) follow from the Markov chains:

\[
(Y_{2,i}, T_{2,i}) \leadsto X_{1,i} \leadsto (Y_{1,i}, Z_{1,i}) \quad \text{and} \quad (Y_{1,i}, Z_{1,i}) \leadsto X_{2,i} \leadsto (Y_{2,i}, T_{2,i}) ,
\]

and thus this implies that $T_2$ is less-noisy than $Y_2$. From this observation, we have:

\[
I(W_1 T_{i+1}^n; Y_{1,i} \| Y_{2,i} Z_1^n Y^{i-1} Z_2^n_{i+1}) + I(X_{1,i}; T_{1,i} | T_{2,i} Z_1^n Y^{i-1} Z_2^n_{i+1}) W_1 T_{i+1}^n) \\
\leq I(W_1 T_{i+1}^n; Y_{1,i} \| Y_{2,i} Z_1^n Y^{i-1} Z_2^n_{i+1}) + I(X_{1,i}; T_{1,i} | Y_{2,i} Z_1^n Y^{i-1} Z_2^n_{i+1}) W_1 T_{i+1}^n) \\
= I(X_{1,i}; T_{1,i} | Y_{2,i} Z_1^n Y^{i-1} Z_2^n_{i+1}) ,
\]

Then, letting $S_{2,i} = T_{i+1}^n$, the resulting sum-rate reads as:

\[
R_1 + R_2 \leq I(X_1; Y_1 | Z_1) + I(U_2 S_2; Y_2 | V_2) - I(U_2 S_2; T_2 Z_2 | V_2) + I(X_2; T_2 | Z_2 V_2) .
\]

The variable $S_2$ can be eliminated in a similar manner as we already did in Section V-C. Since, $Y_2$ is less-noisy than $Z_2$ and so is $T_1$ towards $Z_1$, then we can show the converse of the region by letting $U_2 \equiv (U_2, V_2)$ and $U_1 \equiv (U_1, V_1)$.
REFERENCES

[1] C. E. Shannon, “Communication theory of secrecy systems,” *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct. 1949. [Online]. Available: [http://dx.doi.org/10.1002/j.1538-7305.1949.tb00928.x](http://dx.doi.org/10.1002/j.1538-7305.1949.tb00928.x)

[2] A. D. Wyner, “The wire-tap channel,” *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[3] I. Csiszar and J. Korner, “Broadcast channels with confidential messages,” *Information Theory, IEEE Transactions on*, vol. 24, no. 3, pp. 339–348, 1978.

[4] O. Ozel and S. Ulukus, “Wiretap channels: Roles of rate splitting and channel prefixing,” in *Information Theory Proceedings (ISIT), 2011 IEEE International Symposium on*, 2011, pp. 628–632.

[5] Y. Liang and H. Poor, “Generalized multiple access channels with confidential messages,” in *Information Theory, 2006 IEEE International Symposium on*, 2006, pp. 952–956.

[6] Y. Liang, H. V. Poor, and S. Shamai (Shitz), “Physical layer security in broadcast networks,” *Security and Communication Networks, Wiley*, vol. 2, no. 5, pp. 227–238, 2009.

[7] R. Liu, I. Maric, P. S, and R. Yates, “Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions,” *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2493–2507, 2008.

[8] Y. Zhao, P. Xu, Y. Zhao, W. Wei, and Y. Tang, “Secret communications over semi-deterministic broadcast channels,” in *Communications and Networking in China, 2009. ChinaCOM 2009. Fourth International Conference on*, 2009, pp. 1–4.

[9] W. Kang and N. Liu, “The secrecy capacity of the semi-deterministic broadcast channel,” in *Information Theory, 2009. ISIT 2009. IEEE International Symposium on*, 2009, pp. 2767–2771.

[10] R. Liu and H. Poor, “Secrecy capacity region of a multiple-antenna gaussian broadcast channel with confidential messages,” *Information Theory, IEEE Transactions on*, vol. 55, no. 3, pp. 1235–1249, 2009.

[11] R. Liu, T. Liu, H. Poor, and S. Shamai, “Multiple-input multiple-output gaussian broadcast channels with confidential messages,” *Information Theory, IEEE Transactions on*, vol. 56, no. 9, pp. 4215–4227, 2010.

[12] E. Ekrem and S. Ulukus, “The secrecy capacity region of the gaussian mimo multi-receiver wiretap channel,” *Information Theory, IEEE Transactions on*, vol. 57, no. 4, pp. 2083–2114, 2011.

[13] Y. Liang, H. V. Poor, and S. Shamai (Shitz), *Information Theoretic Security*. Foundations and Trends in Communications and Information Theory, Now Publishers, Hanover, MA, USA, 2008, vol. 5, no. 4-5.

[14] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. Bloch, S. Ulukus, and A. Yener, “Cooperative security at the physical layer: A summary of recent advances,” *Signal Processing Magazine, IEEE*, vol. 30, no. 5, pp. 16–28, 2013.

[15] E. Ekrem and S. Ulukus, “Secrecy capacity of a class of broadcast channels with an eavesdropper,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, pp. 824:235–, 2009. [Online]. Available: [http://jwcn.eurasipjournals.com/content/2009/1/824235](http://jwcn.eurasipjournals.com/content/2009/1/824235)

[16] G. Bagherikaram, A. Motahari, and A. Khandani, “Secrecy capacity region of gaussian broadcast channel,” in *Information Sciences and Systems. CISS 2009. 43rd Annual Conference on*, 2009, pp. 152–157.

[17] C. Nair and A. El Gamal, “An outer bound to the capacity region of the broadcast channel,” in *Information Theory, 2006 IEEE International Symposium on*, 2006, pp. 2205–2209.

[18] K. Marton, “A coding theorem for the discrete memoryless broadcast channel,” *Information Theory, IEEE Transactions on*, vol. 25, no. 3, pp. 306–311, 1979.

[19] A. Wyner and J. Ziv, “A theorem on the entropy of certain binary sequences and applications–I,” *Information Theory, IEEE Transactions on*, vol. 19, no. 6, pp. 769–772, 1973.
[20] S. Shafiee and S. Ulukus, “Achievable rates in gaussian MISO channels with secrecy constraints,” in *Information Theory, 2007. ISIT 2007. IEEE International Symposium on*, 2007, pp. 2466–2470.

[21] A. El Gamal, “Capacity of the product and sum of two unmatched broadcast channels,” *Probl. Peredachi Inf.*, vol. 16, pp. 3–23, 1980.

[22] Y. Geng, A. Gohari, C. Nair, and Y. Yu, “The capacity region for two classes of product broadcast channels,” in *Information Theory Proceedings (ISIT), 2011 IEEE International Symposium on*, 2011, pp. 1544–1548.

[23] C. Nair, “Capacity regions of two new classes of two-receiver broadcast channels,” *Information Theory, IEEE Transactions on*, vol. 56, no. 9, pp. 4207–4214, 2010.

[24] T. Cover and J. Thomas, *Elements of information theory (2nd Ed)*. Wiley-Interscience, 2006.

[25] I. Csiszar and J. Körner, *Information theory: coding theorems for discrete memoryless systems*. Akadémiai Kiado, Budapest, 1982.