Rate Splitting and Sharing for Degraded Broadcast Channel with Secrecy Outside a Bounded Range

Shaofeng Zou
Department of EECS
Syracuse University
Email: szou02@syr.edu

Yingbin Liang
Department of EECS
Syracuse University
Email: yliang06@syr.edu

Lifeng Lai
Department of ECE
Worcester Poly Insistitute
Email: llai@wpi.edu

Shlomo Shamai (Shitz)
Department of EE
Technion
Email: sshlomo@ee.technion.ac.il

***Abstract*—A four-receiver degraded broadcast channel with secrecy outside a bounded range is studied, over which a transmitter sends four messages to four receivers. In the model considered, the channel quality gradually degrades from receiver 4 to receiver 1, and receiver k is required to decode the first k messages for $k = 1, \ldots, 4$. Furthermore, message 3 is required to be secured from receiver 1, and message 4 is required to be secured from receivers 1 and 2. The secrecy capacity region is established. The achievable scheme includes not only superposition, binning and embedded coding used in previous studies, but also rate splitting and sharing particularly designed for this model, which is shown to be critical to further enlarge the achievable region and enable the development of the converse proof.**

***Keywords*—Broadcast channel, rate splitting, rate sharing, secrecy capacity.**

I. Introduction

Security arises as an important issue in wireless communications due to the broadcast nature. Such a practical issue was modeled as a degraded wiretap channel (i.e., a degraded broadcast channel) in Wyner's seminal work [1], in which a transmitter wishes to send a message to a legitimate receiver, and wishes to keep the message secure from an eavesdropper. For such a channel, a physical layer approach was designed in [1] to satisfy the reliability and secrecy requirements. The model was further generalized by Csiszár and Körner in [2] to be the general broadcast channel (not necessarily degraded) with an additional common message intended for both receivers to decode in addition to the confidential message that should be kept secure from the eavesdropper.

More recently, broadcast channels with various decoding and secrecy constraints have been studied (see [3], [4] for recent surveys for these studies). A multi-receiver extension of the Wyner's model was studied in [5], [6], in which a transmitter broadcasts to a number of receivers, and all messages need to be secured from an eavesdropper. Another class of extensions can be viewed as degraded broadcast channels with layered decoding and layered secrecy constraints [6]–[10], in which the receiver with one-level better channel quality is required to decode one more message, and this message needs to be secured from the receivers with worse channel quality. In [11], a further extension of the model in [8] was studied, in which the message is required to be secure from the receiver with two-level worse channel quality, but not from the immediate downstream receiver. Such a model is more practical when the channel has continuous channel quality. It is more reasonable to require the message to be secured from the receivers with a certain amount of worse channel quality, instead of being secured from the receiver with one level worse channel quality, which is not even well defined for continuous channel state. To be more explicit, we use an example to illustrate the motivation of such a model. Consider a degraded broadcast channel with infinite number of receivers, in which h denotes the amplitude of the channel gain (the larger h, the better the channel). In this case, it is impossible to require that the message intended for receivers with $h \geq h_0$ to be secured from receivers with $h < h_0$, because no positive secrecy rate can be achieved. Instead, it is more nature to require that the messages intended for receivers with $h \geq h_0$ to be secured from receivers with $h \leq h_0 - \Delta$, where $\Delta > 0$. We refer to such secrecy requirements as secrecy outside a bounded range.

In this paper, we generalize the three-receiver model studied in [11] to the four-receiver degraded broadcast channel with secrecy outside a bounded range. Our main result is the establishment of the secrecy capacity region for the model of interest. Although our proof of the result may seem to only likely follow techniques developed in [11], our exploration turns out to show that the achievable techniques in [11] and in previous studies of broadcast models in [6]–[9] are not sufficient for establishing the secrecy capacity region. The main technical novelty of this paper lies in designing rate splitting and sharing to enlarge the achievable region, for which we are able to develop the converse proof to establish the secrecy capacity region. Furthermore, the techniques of rate splitting and sharing provide us more insight into the general model with arbitrary number of receivers, which cannot be concluded from the three-receiver case.

More specifically, in the model we study (see Figure 1), a transmitter sends four messages W_1, W_2, W_3, W_4 to four receivers over a degraded broadcast channel with the channel quality gradually degrading from receiver 4 to receiver 1. Receiver k is required to decode $W_1, \ldots, W_k$, for $k = 1, 2, 3, 4$. Furthermore, the message W_3 is required to be secured from receiver 1, and the message W_4 is required to be secured from receivers 1 and 2. Hence, in this network, each message is secured from the receiver with two-level worse channel quality.

Our achievable scheme includes (1) superposition coding, which encodes each message into one layer in order to satisfy the layered decoding requirements at the four receivers; (2) embedded coding [12], [13], which exploits the secrecy requirement outside a bounded range to use lower-layer messages as random sources to secure higher-layer messages; (3) random binning, which provides further randomness to secure

each message at its corresponding layer; and (4) rate splitting and sharing, which turns out to be critical for this model to further enlarge the achievable region. Since the first three techniques are developed and utilized in previous studies, we next illustrate why rate splitting and sharing is useful here. Consider the case where layer 3 is sufficient to secure layer 4. Random binning is then not necessary in layer 4. Hence, simply using techniques for three-receiver model yields the rate of W_4 to be bounded by the decoding capability of receiver 4 given decoding of the three other messages. It turns out to be very difficult to develop the converse proof for the resulting achievable region, which suggests that such an achievable region may not be large enough. Indeed, the previous achievable scheme ignores the fact that under assumption of this case, part of layer 3 (say W_{31}) is good enough to secure the remaining part of layer 3 (say W_{32}) and layer 4 from receiver 2. Hence, W_{32} can be counted towards either the rate R_3 or the rate R_4, which provides the flexibility to enlarge R_4 and correspondingly the achievable region. Such an idea motivates our development of splitting W_3 into two parts W_{31} and W_{32} and sharing W_{32} between R_3 and R_4. The converse for this resulting achievable region can be developed, suggesting that rate splitting and sharing are important for establishing the secrecy capacity region.

The remainder of this paper is organized as follows. In Section II, we introduce our system model. In Section III, we present our main results and describe the main idea of the achievable scheme. In Section IV, we provide outline of the proofs of achievability and converse. Finally, in Section V, we conclude our paper.

II. Channel Model

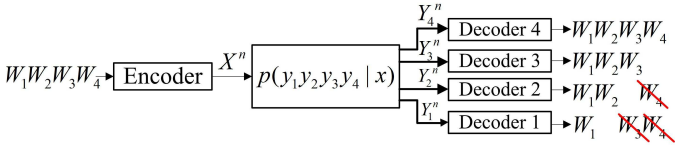

Fig. 1. The four-receiver degraded broadcast channel with secrecy outside a bounded range.

In this paper, we consider a four-receiver degraded broadcast channel with secrecy outside of a bounded range (see Figure 1). Here, a transmitter sends information to four receivers over a discrete memoryless channel with the channel transition probability given by $P_{Y_1Y_2Y_3Y_4|X}$, in which $X \in \mathcal{X}$ denotes the channel input, and $Y_k \in \mathcal{Y}_k$ denotes the channel output at receiver k, for $k = 1, 2, 3, 4$. The channel is assumed to satisfy the degraded condition, i.e., the following Markov chain holds:

$$X \to Y_4 \to Y_3 \to Y_2 \to Y_1. \tag{1}$$

Hence, the channel quality gradually degrades from receiver 4 to receiver 1.

The transmitter has four messages W_1, W_2, W_3, W_4 intended for the four receivers with the following decoding and secrecy requirements. For $k = 1, 2, 3, 4$, receiver k is required to decode the messages $W_1, \ldots, W_k$. Furthermore, the message W_3 needs to be kept secure from receiver 1, and the message W_4 needs to be kept secure from receivers 1 and 2 (see Figure 1).

A $(2^{nR_1}, 2^{nR_2}, 2^{nR_3}, 2^{nR_4}, n)$ code for the channel consists of

- Four message sets: $W_k \in \mathcal{W}_k = \{1, \cdots, 2^{nR_k}\}$ for $k = 1, 2, 3, 4$, which are independent from each other and each message is uniformly distributed over the corresponding message set;
- A (possibly stochastic) encoder f^n: $\mathcal{W}_1 \times \mathcal{W}_2 \times \mathcal{W}_3 \times \mathcal{W}_4 \to \mathcal{X}^n$;
- Four decoders $g_k^n : \mathcal{Y}_k^n \to (\mathcal{W}_1, \cdots, \mathcal{W}_k)$ for $k = 1, 2, 3, 4$.

A secrecy rate tuple (R_1, R_2, R_3, R_4) is *achievable* if there exists a sequence of $(2^{nR_1}, 2^{nR_2}, 2^{nR_3}, 2^{nR_4}, n)$ code such that both the average error probability

$$P_e^n = \Pr\left(\cup_{k=1}^4 \{(W_1, \cdots, W_k) \neq g_k^n(Y_k^n)\}\right) \tag{2}$$

and the leakage rate at receivers 1 and 2

$$\frac{1}{n} I(W_3, W_4; Y_1^n | W_1) \tag{3}$$

$$\frac{1}{n} I(W_4; Y_2^n | W_1, W_2) \tag{4}$$

go to zero as n goes to infinity.

Our goal is to characterize the *secrecy capacity region* that contains all achievable rate tuples.

III. Main Results

Our main result in this paper is the following characterization of the secrecy capacity region for the model of interest.

Theorem 1. *Consider the four-receiver degraded broadcast channel with secrecy outside a bounded range as described in Section II. The secrecy capacity region consists of rate tuples (R_1, R_2, R_3, R_4) satisfying*

$$\begin{aligned}
R_1 &\le I(U_1; Y_1), \\
R_2 &\le I(U_2; Y_2 | U_1), \\
R_3 &\le I(U_3; Y_3 | U_2) \\
&\quad + \min\Big(0, I(U_2; Y_2 | U_1) - I(U_3; Y_1 | U_1)\Big), \\
R_4 &\le I(X; Y_4 | U_3) + I(U_3; Y_3 | U_2) - I(X; Y_2 | U_2), \\
R_3 + R_4 &\le I(U_3; Y_3 | U_2) + I(X; Y_4 | U_3) \\
&\quad + \min\Big(0, I(U_2; Y_2 | U_1) - I(X; Y_1 | U_1)\Big),
\end{aligned} \tag{5}$$

for some $P_{U_1U_2U_3X}$ such that the following Markov chain holds

$$U_1 \to U_2 \to U_3 \to X \to Y_4 \to Y_3 \to Y_2 \to Y_1. \tag{6}$$

The major technical challenge for establishing the above secrecy capacity region lies in providing an achievable region good enough to enable the proof of converse. Here, we briefly introduce our idea of the achievable scheme, which highlights the technical novelty of our design. We provide more detailed proofs in Section IV.

Our achievable scheme includes the following ingredients:

1. Superposition coding: Due to the requirement of layered decoding, the messages are encoded using superposition coding with each layer corresponding to one message, i.e., layer k corresponds to W_k for $k = 1, 2, 3, 4$.

2. Joint embedded coding and binning: Since the messages do not need to be kept secure from its immediate downstream receiver, such a receiver's message can serve as a random source for securing the higher layer message in addition to stochastic binning. In fact, if such random source is sufficient for securing the message, binning is not necessary. More specifically, W_3 serves as a random source to secure W_4 from receiver 2 jointly with random binning designed at layer 4 (if necessary). Similarly, W_2 at layer 2 serves as a random source to secure W_3 and W_4 from receiver 1 jointly with binning at layers 3 and 4 (if necessary).

3. Rate splitting and sharing: We split W_3 into two parts, i.e., W_{31} and W_{32}. Such splitting exploits the opportunity (see case 1 in the proof of achievability), that W_{31} is sufficient to secure both W_{32} and W_4 from receiver 2, and thus the rate of W_{32} can be counted towards the rate of either W_3 or W_4. In this way, the rate region may be enlarged.

We note that joint embedded coding and binning is necessary here to exploit the secrecy requirements only outside the bounded range (i.e., the secrecy is not imposed for the immediate downstream receiver). Thus, messages intended for receivers inside the bounded range can serve as random sources for secrecy purpose. Such a scheme cannot be used for the model in [9] where the secrecy is imposed for the immediate downstream receiver. We further note that the embedded coding here uses messages across superposition layers as random sources for secrecy, which is different from the original embedded coding [6] where the messages serving as random sources are at the same layers as the messages being protected.

In fact, using only the superposition and joint embedded coding and binning is shown to be optimal (i.e., achieve the secrecy capacity region) for the three-receiver model in [11]. However, for the four-receiver model, such an achievable scheme is not in a sufficiently good form for which the machinery of a converse proof is difficult to develop. The major novelty of our scheme lies in developing rating splitting and sharing, which helps to potentially enlarge the achievable region (at least enlarge the region for a given distribution of auxiliary random variables). Consequently, the proof of converse can be developed for such an achievable region, and thus the secrecy capacity region is established.

More specifically, without rate splitting and sharing, superposition and joint embedded coding and binning yields an achievable region with rates satisfying

$$\begin{aligned}
R_1 &\le I(U_1;Y_1),\\
R_2 &\le I(U_2;Y_2;U_1),\\
R_3 &\le I(U_3;Y_3|U_2)\\
&\quad + \min\Big(0, I(U_2;Y_2|U_1) - I(U_3;Y_1|U_1)\Big),\\
R_4 &\le I(X;Y_4|U_3),\\
R_4 &\le I(X;Y_4|U_3) + I(U_3;Y_3|U_2) - I(X;Y_2|U_2),\\
R_3 + R_4 &\le I(U_3;Y_3|U_2) + I(X;Y_4|U_3)\\
&\quad + I(U_2;Y_2|U_1) - I(X;Y_1|U_1) \qquad (7)
\end{aligned}$$

As we comment in Section IV-B, it is very difficult to develop the converse proof for the bound $R_4 \le I(X;Y_4|U_3)$ in the above region. However, by using rate splitting and sharing, this bound is replaced by the bound $R_3 + R_4 \le I(U_3;Y_3|U_2) + I(X;Y_4|U_3)$, and the resulting region (5) is larger than the above region (7) (for a given distribution of auxiliary random variables). Furthermore, the converse proof for the new bound on $R_3 + R_4$ in (5) can be derived, and thus establishes the region (5) as the secrecy capacity region.

IV. Technical Proof

In the following two subsections, we outline the achievability and converse proofs. Further details can be found in [14].

A. Proof of Achievability (Outline)

Fix a distribution $P_{U_1}P_{U_2|U_1}P_{U_3|U_2}P_{X|U_3}P_{Y_1,Y_2,Y_3,Y_4|X}$. We design the achievable schemes for two cases.

1) Case 1: $I(U_3;Y_3|U_2) > I(X;Y_2|U_2)$.

Random codebook generation: Randomly generate the codebook as follows:

- Generate 2^{nR_1} independent and identically distributed (i.i.d.) u_1^n with distribution $\prod_{i=1}^n p(u_{1,i})$. Index these codewords as $u_1^n(w_1)$, $w_1 \in [1, 2^{n\widetilde{R}_1}]$.
- For each $u_1^n(w_1)$, generate 2^{nR_2} i.i.d. u_2^n with distribution $\prod_{i=1}^n p(u_{2,i}|u_{1,i})$. Index these codewords as $u_2^n(w_1, w_2)$, $w_2 \in [1, 2^{n\widetilde{R}_2}]$.
- For each $u_2^n(w_1, w_2)$, generate $2^{n\widetilde{R}_3}$ i.i.d. u_3^n with distribution $\prod_{i=1}^n p(u_{3,i}|u_{2,i})$. Partition these codewords into $2^{nR_{31}}$ bins. We further partition each bin into $2^{nR_{32}}$ sub-bins. Hence, there are $2^{n(\widetilde{R}_3 - R_{31} - R_{32})}$ u_3^n in each sub-bin. We use $w_{31} \in [1 : 2^{nR_{31}}]$ to denote the bin number, $w_{32} \in [1 : 2^{nR_{32}}]$ to denote the sub-bin number, and $l_3 \in [1 : 2^{n(\widetilde{R}_3 - R_{31} - R_{32})}]$ to denote the index within the bin. Hence, each u_3^n is indexed by $(w_1, w_2, w_{31}, w_{32}, l_3)$.
- For each $u_3^n(w_1, w_2, w_{31}, w_{32}, l_3)$, generate $2^{n\widetilde{R}_4}$ i.i.d. x^n with distribution $\prod_{i=1}^n p(x_i|u_{3,i})$. Partition these codewords into $2^{n\overline{R}_4}$ bins. We use $w_4 \in [1 : 2^{n\overline{R}_4}]$ to denote the bin number, $l_4 \in [1 : 2^{n(\widetilde{R}_4 - \overline{R}_4)}]$ to denote the index inside the sub-bin. Index those codewords as $x^n(w_1, w_2, w_{31}, w_{32}, l_3, w_4, l_4)$, $w_4 \in [1, 2^{n\widetilde{R}_4}]$.

The chosen codebook is revealed to both the transmitter and receivers.

Encoding: To send a message tuple $(w_1, w_2, w_{31}, w_{32}, w_4)$, the transmitter randomly and uniformly generates $l_3 \in [1 : 2^{n(\widetilde{R}_3 - R_{31} - R_{32})}]$ and $l_4 \in [1 : 2^{n(\widetilde{R}_4 - \overline{R}_4)}]$, and sends $x^n(w_1, w_2, w_{31}, w_{32}, l_3, w_4, l_4)$.

Decoding:

- Receiver 1 claims that $\widehat{w}_1$ is sent, if there exists a unique $\widehat{w}_1$ such that

$$\Big(u_1^n(\widehat{w}_1), y_1^n\Big) \in T_\epsilon^n(P_{U_1Y_1}).$$

Otherwise, it declares an error.

- Receiver 2 claims that $(\widehat{w}_1, \widehat{w}_2)$ is sent, if there exists a unique pair $(\widehat{w}_1, \widehat{w}_2)$ such that

$$\left(u_1^n(\widehat{w}_1), u_2^n(\widehat{w}_1, \widehat{w}_2), y_2^n\right) \in T_\epsilon^n(P_{U_1U_2Y_2}).$$

Otherwise, it declares an error.

- Receiver 3 claims that $(\widehat{w}_1, \widehat{w}_2, \widehat{w}_{31}, \widehat{w}_{32})$ is sent, if there exists a unique tuple $(\widehat{w}_1, \widehat{w}_2, \widehat{w}_{31}, \widehat{w}_{32}, \widehat{l}_3)$ such that

$$\left(u_1^n(\widehat{w}_1), u_2^n(\widehat{w}_1, \widehat{w}_2), u_3^n(\widehat{w}_1, \widehat{w}_2, \widehat{w}_{31}, \widehat{w}_{32}, \widehat{l}_3), y_3^n\right) \in T_\epsilon^n(P_{U_1U_2U_3Y_3}).$$

Otherwise, it declares an error.

- Receiver 4 claims that $\widehat{w}_1, \widehat{w}_2, \widehat{w}_{31}, \widehat{w}_{32}, \widehat{w}_4$ is sent, if there exists a unique tuple $(\widehat{w}_1, \widehat{w}_2, \widehat{w}_{31}, \widehat{w}_{32}, \widehat{l}_3, \widehat{w}_4, \widehat{l}_4)$ such that

$$\left(u_1^n(\widehat{w}_1), u_2^n(\widehat{w}_1, \widehat{w}_2), u_3^n(\widehat{w}_1, \widehat{w}_2, \widehat{w}_{31}, \widehat{w}_{32}, \widehat{l}_3), x^n(\widehat{w}_1, \widehat{w}_2, \widehat{w}_{31}, \widehat{w}_{32}, \widehat{l}_3, \widehat{w}_4, \widehat{l}_4), y_4^n\right) \in T_\epsilon^n(P_{U_1U_2U_3XY_4}).$$

Otherwise, it declares an error.

Analysis of error probability: It can be shown by the law of large number and packing lemma that receiver k decodes the messages $(w_1, \ldots, w_k)$ with asymptotically small probability of error for $k = 1, \ldots, 4$ if the following inequalities are satisfied.

$$\begin{aligned} R_1 &\le I(U_1; Y_1), \\ R_2 &\le I(U_2; Y_2|U_1), \\ \widetilde{R}_3 &\le I(U_3; Y_3|U_2), \\ \widetilde{R}_4 &\le I(X; Y_4|U_3). \end{aligned} \tag{8}$$

Analysis of leakage rate: In this model, W_{31}, W_{32}, W_4 are required to be kept secured from receiver 1, and W_4 is required to be kept secured from receiver 2. We note that under the assumption of case 1, i.e., $I(U_3; Y_3|U_2) > I(X; Y_2|U_2)$, part of W_3 (i.e., W_{31}) is sufficient to secure the remaining part of W_3 (i.e., W_{32}) and W_4 from receiver 2 without the necessity of random binning in layer 4[1]. Thus, we strengthen the secrecy requirements as follows: W_{31}, W_{32}, W_4 are kept secure from receiver 1, and W_{32}, W_4 are kept secure from receiver 2. Therefore, it is sufficient to show

$$\frac{1}{n} I(W_{31}, W_{32}, W_4; Y_1^n|W_1, \mathcal{C}) \to 0, \tag{9}$$

$$\frac{1}{n} I(W_{32}, W_4; Y_2^n|W_1, W_2, \mathcal{C}) \to 0, \tag{10}$$

as $n \to \infty$.

It can be shown that if

$$\begin{aligned} R_2 + \widetilde{R}_3 - R_{31} - R_{32} &\ge I(U_3; Y_1|U_1), \\ R_2 &\ge I(U_2; Y_1|U_1), \\ R_2 + \widetilde{R}_3 - R_{31} - R_{32} + \widetilde{R}_4 - \overline{R}_4 &\ge I(X; Y_1|U_1), \\ \widetilde{R}_3 - R_{32} &\ge I(U_3; Y_2|U_2), \\ \widetilde{R}_3 - R_{32} + \widetilde{R}_4 - \overline{R}_4 &\ge I(U_4; Y_2|U_2), \end{aligned} \tag{11}$$

the conditions (9) and (10) are satisfied.

Combining (8) and (11), we obtain the following achievable region:

$$\begin{aligned} R_1 &\le I(U_1; Y_1), \\ R_2 &\le I(U_2; Y_2|U_1), \\ R_{31} + R_{32} &\le I(U_3; Y_3|U_2), \\ \overline{R}_4 &\le I(X; Y_4|U_3), \\ R_{31} + R_{32} &\le I(U_2; Y_2|U_1) + I(U_3; Y_3|U_2) - I(U_3; Y_1|U_1), \\ R_{31} + R_{32} + \overline{R}_4 &\le I(U_2; Y_2|U_1) + I(U_3; Y_3|U_2) + I(X; Y_4|U_3) - I(X; Y_1|U_1), \\ R_{32} &\le I(U_3; Y_3|U_2) - I(U_3; Y_2|U_2), \\ R_{32} + \overline{R}_4 &\le I(U_3; Y_3|U_2) + I(X; Y_4|U_3) - I(X; Y_2|U_2). \end{aligned} \tag{12}$$

We note that the above region use the fact that if $R_2 = I(U_2; Y_2|U_1)$ can be achieved, any rate below this threshold can be achieved by sending certain amount of information independent of W_2.

Rate sharing: It can be observed that W_{32} satisfies the same decoding and secrecy requirements as W_4, and hence its rate can be counted towards R_4 by subtracting the same rate from R_3. Thus, we define $R_3 = R_{31}$, and $R_4 = R_{32} + \overline{R}_4$. By adding these two rates to the above achievable region, and performing the Fourier-Motzkin elimination to remove R_{31}, R_{32}, and $\bar{R}_4$, we obtain the achievable region given in Theorem 1.

2) Case 2: $I(U_3; Y_3|U_2) \le I(X; Y_2|U_2)$.

Randomly generate the codebook as in case 1, and set $R_{32} = 0$, $R_{31} = R_3$, and $\overline{R}_4 = R_4$. The encoding and decoding procedures are similar to those of case 1.

Following steps similar to those in case 1 to analyze the decoding error probability and the leakage rate, we obtain the achievable region characterized by the following bounds:

$$\begin{aligned} R_1 &\le I(U_1; Y_1), \\ R_2 &\le I(U_2; Y_2|U_1), \\ R_3 &\le I(U_3; Y_3|U_2), \\ R_4 &\le I(X; Y_4|U_3), \\ R_3 &\le I(U_2; Y_2|U_1) + I(U_3; Y_3|U_2) - I(U_3; Y_1|U_1), \\ R_3 + R_4 &\le I(U_2; Y_2|U_1) + I(U_3; Y_3|U_2) + I(X; Y_4|U_3) - I(X; Y_1|U_1), \\ R_4 &\le I(U_3; Y_3|U_2) + I(X; Y_4|U_3) - I(X; Y_2|U_2). \end{aligned} \tag{13}$$

Comparing the two bounds on R_4 in the above region, the bound $R_4 \le I(X; Y_4|U_3)$ is redundant and can be removed due to the assumption of case 2, which is $I(U_3; Y_3|U_2) \le I(X; Y_2|U_2)$. Thus, we obtain an achievable region that is the same as the capacity region characterized in Theorem 1.

B. Proof of Converse (Outline)

Here we provide our main insight for proving the converse with the details omitted due to the space limitation. The full proof can be found in [14].

[1]This is only true for securing W_4 from receiver 2. Random binning may still be needed for securing W_3 and W_4 from receiver 1.

To prove the converse, a natural construction of auxiliary random variables is as follows:

$$\begin{aligned} U_{1,i} &= (W_1, Y_1^{i-1}), \\ U_{2,i} &= (W_1, W_2, Y_2^{i-1}), \\ U_{3,i} &= (W_1, W_2, W_3, Y_3^{i-1}, Y_{1,i+1}^n), \\ U_{4,i} &= (W_1, \ldots, W_4, Y_4^{i-1}, Y_{2,i+1}^n), \end{aligned} \tag{14}$$

which satisfy the following Markov chain:

$$\begin{aligned} &U_{1,i} \to U_{2,i} \to U_{3,i} \to U_{4,i} \to X_i \\ &\to Y_{4,i} \to Y_{3,i} \to Y_{2,i} \to Y_{1,i}, \end{aligned} \tag{15}$$

for $i = 1, \ldots, n$.

As we comment in Section III, without rate splitting of R_3 and rate sharing between R_3 and R_4, we have the bound $R_4 \leq I(X; Y_4|U_3)$ in the achievable region (7). However, it is very challenging to derive this bound for the given choice of auxiliary random variable $U_{3,i}$ in (14). More specifically, it is difficult to justify inserting $Y_{1,i+1}^n$ into the conditioning of the mutual information. But such a choice of U_3 appears to be necessary for showing other bounds in the achievable region. Such dilemma motivates us to come up with the scheme of rate splitting and sharing in the achievable scheme to replace this bound by bound on $R_3 + R_4$ so that the converse proof can be established.

V. Conclusion

In this paper, we have studied a four-receiver discrete memoryless degraded broadcast channel with secrecy outside a bounded range. We have characterized the secrecy capacity region of this model. We have designed an achievable scheme based on superposition, joint embedded coding and binning, and rate splitting and sharing. Among the techniques, rate splitting and sharing is critical for deriving a potentially larger achievable region, for which the converse can be established.

In the future, we plan to extend our results to the case with an arbitrary number of receivers. For such a more general model, it is anticipated that rate splitting and sharing is more involved because one layer's message can be split into multiple components in order to be shared by rates corresponding to higher layers. The procedure of Fourier Motzkin elimination to obtain the resulting achievable region will also become more complex. This suggests that new techniques need to be developed to simplify the mathematical manipulations, as well as capturing the essence of the problem.

Acknowledgment

The work of S. Zou and Y. Liang was supported by a National Science Foundation CAREER Award under Grant CCF-10-26565 and by the National Science Foundation under Grants CNS-11-16932. L. Lai was supported by a National Science Foundation CAREER Award under Grant CCF-13-18980 and by the National Science Foundation under Grant CNS-13-21223. The work of S. Shamai (Shitz) was supported by the Israel Science Foundation (ISF), and the European Commission in the framework of the Network of Excellence in Wireless COMmunications NEWCOM#.

References

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

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

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

[4] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4-5, pp. 355–580, Now Publishers, Hanover, MA, USA, 2008.

[5] E. Ekrem and S. Ulukus, "Secrecy capacity of a class of broadcast channels with an eavesdropper," *EURASIP J. Wirel. Commun. Netw.*, vol. 2009, pp. 1:1–1:29, Mar. 2009.

[6] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "A vector generalization of costa's entropy-power inequality with applications," *IEEE Trans. Inform. Theory*, vol. 56, no. 4, pp. 1865 –1879, April 2010.

[7] E. Ekrem and S. Ulukus, "Degraded compound multi-receiver wiretap channels," *IEEE Trans. Inform. Theory*, vol. 58, no. 9, pp. 5681–5698, September 2012.

[8] S. Zou, Y. Liang, L. Lai, and S. Shamai (Shitz), "An information theoretical approach to secrecy sharing," *Submitted to IEEE Transactions on Information Theory*, 2014.

[9] ——, "Layered secure broadcasting over MIMO channels and application in secret sharing," in *Proc. 2014 IEEE International Symposium on Information Theory (ISIT)*, Hawaii, USA, June 2014, pp. 396–400.

[10] ——, "Layered decoding and secrecy over degraded broadcast channels," in *Proc. 2013 IEEE 14th Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, Darmstadt, Germany, June 2013, pp. 679–683.

[11] ——, "Degraded broadcast channel: Secrecy outside of a bounded range," *to appear in Proc. 2015 IEEE Information Theory Workshop (ITW)*, 2015.

[12] H. D. Ly, T. Liu, and Y. Blankenship, "Security embedding codes," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 148–159, Feb 2012.

[13] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Transactions on Information Theory, Special Issue on Information Theoretic Security*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[14] S. Zou, Y. Liang, L. Lai, and S. Shamai (Shitz), "Supplement material of rate splitting and sharing for degraded broadcast channel with secrecy outside of a bounded range," *available at szou02.mysite.syr.edu/conference/supplementisit2015.pdf*, 2015.