

# Degraded Broadcast Channel: Secrecy Outside of 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 three-receiver degraded broadcast channel with secrecy outside of a bounded range is studied, in which the channel quality gradually degrades from receiver 3 to receiver 1. The transmitter has three messages intended for the receivers with receiver 3 decoding all messages, receiver 2 decoding the first two messages, and receiver 1 decoding only the first message. Furthermore, the third message should be kept secure from receiver 1. The discrete memoryless channel is studied and the secrecy capacity region is characterized. The achievable scheme is based on superposition coding and random binning, in which one superposition layer and random binning together provide secrecy. The converse proof is derived based on the insight obtained from the achievable scheme so that manipulations of terms yield tight rate bounds.

## I. INTRODUCTION

The broadcast nature is one of the major reasons that challenge secure communications in wireless networks. In the seminal work by Wyner [1], a physical layer approach to secrecy was proposed and studied for a degraded broadcast channel. This approach guarantees secure transmission from a sender to a legitimate receiver and keeps the transmission secure from an eavesdropper. Csiszár and Körner further extended this model to the case, in which the sender also wants to transmit a common message to both the legitimate receiver and the eavesdropper [2] in addition to the confidential message, and the secrecy capacity region was fully characterized.

Following the initial studies in [1], [2], broadcast channels with various decoding and secrecy constraints have been studied intensively (see [3], [4] for recent surveys for these studies). For example, the broadcast channel with two legitimate receivers and one eavesdropper was studied in [5], in which the sender transmits two messages to two legitimate receivers respectively, and wants to keep both messages confidential from the eavesdropper. The secrecy capacity region was derived when the channel is degraded. The same channel but with layered decoding and secrecy constraints was studied in [6], [7], in which the receiver with the better channel quality is required to decode one more message compared to the receiver with the worse channel quality, and this message should be kept confidential from the receiver with the worse channel quality, and both messages should be kept confidential from the eavesdropper. In [8], [9], the above model was generalized to the case with more than two receivers.

We note that for the model with layered decoding and secrecy, the additional message decoded by a better receiver needs to be kept confidential from the receiver with only

one level worse channel quality (layered secrecy, zero secrecy range). Although such a model is feasible for broadcast channels with discrete states (i.e., quality of receivers can be captured by discrete channel states), it cannot capture the scenarios with receivers' channel quality varying continuously. For such a case, 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 quality. 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 a secrecy requirement as *secrecy outside of a bounded range*.

In this paper, we focus on the three-receiver degraded broadcast channel (see Fig. 1) to convey the central idea of the design of the achievable scheme and development of the converse proof for the capacity region. More specifically, we study the three-receiver broadcast channel that satisfies the degraded condition, i.e., the channel quality gradually degrades from receiver 3 to receiver 1. The transmitter has three messages, i.e.,  $W_1, W_2$  and  $W_3$  for the receivers with receiver 3 decoding all messages, receiver 2 decoding two messages  $W_1$  and  $W_2$ , and receiver 1 decoding only  $W_1$ . Furthermore, the message  $W_3$  should be kept secure from receiver 1. Hence, the secrecy is outside of a bounded range, i.e., the secrecy is required from a receiver with two-level worse channel quality.

We characterize the secrecy capacity region for the three-receiver degraded broadcast channel with secrecy outside of a bounded range. Our novelty in this paper lies in both the design of the joint binning and embedded secrecy scheme and the derivation of the converse proof. More specifically, in order to design an achievable scheme, it is natural to apply superposition coding for encoding three messages, and to apply binning scheme in the level of  $W_3$  to keep  $W_3$  secure from receive 1. However, such a natural scheme turns out to be suboptimal because it misses an important fact that the random message  $W_2$ , which is not required to be detected

at receiver 1, can also serve as a random source to protect  $W_3$  from receiver 1. The novelty of our achievable scheme lies in exploiting the superposition layer of  $W_2$  as embedded coding in addition to the binning scheme for protecting  $W_3$ . Consequently, in the case when  $W_2$  is sufficient to protect  $W_3$ , no binning scheme is needed. Otherwise, joint embedded coding and binning is applied, and hence  $W_3$  is protected via the second superposition layer and random binning in the third layer.

We further show that the above scheme is optimal by developing an outer bound on the capacity region that matches the achievable region. The novelty lies in bounding  $R_3$  by exploiting the intuitions in the two cases of the achievable scheme. For the case that  $W_2$  is sufficient to protect  $W_3$ ,  $R_3$  can be bounded directly by the decoding capability of receiver 3. For the case that  $W_2$  is not sufficient to protect  $W_3$ , the key idea is to bound the difference between the rate  $R_3$  of  $W_3$  and the rate  $R_2$  of  $W_2$  rather than bounding  $R_3$  directly, because  $R_3$  is closely related to  $R_2$  due to the fact that  $W_2$  is utilized to protect  $W_3$  in the achievable scheme. Furthermore, in order to derive a tight bound, a critical step is to identify a useful term that corresponds to receiver 1's knowledge of  $W_2$  given  $W_1$  and  $W_3$ , which vanishes in this case and hence discarding it does not loosen the bound.

This paper is organized as follows. In Section II, we introduce our system model. In section III, we present our main results with outlined achievable and converse proofs. Finally, in Section IV, we conclude our paper.

## II. CHANNEL MODEL

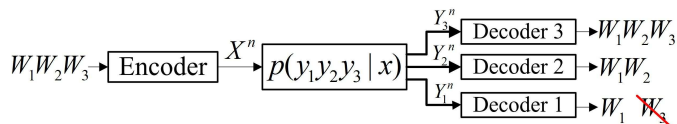


Fig. 1. System Model

In this paper, we consider the degraded broadcast channel with secrecy outside of a bounded range (see Fig. 1 for an illustration), in which a transmitter sends information to three receivers. The channel is discrete memoryless with the channel transition probability given by  $P_{Y_1, Y_2, Y_3 | X}$ , 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  $k = 1, 2, 3$ . It is assumed that the channel satisfies the degraded condition with the following Markov chain condition being satisfied:

$$X \rightarrow Y_3 \rightarrow Y_2 \rightarrow Y_1. \quad (1)$$

Hence, the quality of channels gradually degrades from receiver 3 to receiver 1.

The transmitter have three messages  $W_1, W_2, W_3$  intended for the three receivers with receiver 1 being required to decode  $W_1$ , receiver 2 being required to decode  $W_1, W_2$ , and receiver 3 being required to decode  $W_1, W_2, W_3$ . The system is also required to satisfy the secrecy constraint that the message  $W_3$  is kept secure from receiver 1.

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

- Three message sets:  $W_k \in \mathcal{W}_k = \{1, \dots, 2^{nR_k}\}$  for  $k = 1, 2, 3$ , which are independent from each other and each

message is uniformly distributed over the corresponding message set;

- An (possibly stochastic) encoder  $f^n: \mathcal{W}_1 \times \mathcal{W}_2 \times \mathcal{W}_3 \rightarrow \mathcal{X}^n$ ;
- Three decoders  $g_k^n: \mathcal{Y}_k^n \rightarrow (\mathcal{W}_1, \dots, \mathcal{W}_k)$  for  $k = 1, 2, 3$ .

Hence, a secrecy rate tuple  $(R_1, R_2, R_3)$  is said to be *achievable*, if there exists a sequence of  $(2^{nR_1}, 2^{nR_2}, 2^{nR_3}, n)$  codes such that both the average error probability

$$P_e^n = \Pr(\cup_{k=1}^3 \{(W_1, \dots, W_k) \neq g_k^n(Y_k^n)\}) \quad (2)$$

and the leakage rate at receiver 1

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

approach zero as  $n$  goes to infinity.

The asymptotically small probability of error in (2) implies that receiver  $k$  can decode  $W_1, \dots, W_k$  for  $k = 1, 2, 3$ . And the asymptotically small leakage rate in (3) implies that receiver 1 is kept ignorant of the message  $W_3$ .

## III. MAIN RESULTS

Our main result in this paper is the full characterization of the secrecy capacity region of the degraded broadcast channel with secrecy outside of a bounded range as presented in the following theorem.

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

$$\begin{aligned} R_1 &\leq I(U_1; Y_1), \\ R_2 &\leq I(U_2; Y_2 | U_1), \\ R_3 &\leq \min\{0, I(U_2; Y_2 | U_1) - I(X; Y_1 | U_1)\} + I(X; Y_3 | U_2) \end{aligned} \quad (4)$$

for some  $P_{U_1 U_2 X}$  such that the following Markov chain holds

$$U_1 \rightarrow U_2 \rightarrow X \rightarrow Y_3 \rightarrow Y_2 \rightarrow Y_1. \quad (5)$$

The achievable scheme we design applies superposition coding to encode the messages  $W_1, W_2$  and  $W_3$  in order into three layers, respectively. Furthermore, in order to keep  $W_3$  secure from receive 1, the second layer of  $W_2$  first serves as a random source to protect  $W_3$ . If this is not sufficient to protect  $W_3$ , a random binning scheme is adopted at layer 3 of  $W_3$  to further protect  $W_3$  from being known by receiver 1. The novelty of our achievable scheme lies in exploiting the superposition layer of  $W_2$  as embedded coding in addition to the binning scheme for protecting  $W_3$ .

Such a scheme is also reflected in the expression of the above capacity region. The minimum of two bounds on  $R_3$  corresponds to the two cases whether or not the second layer of  $W_2$  is sufficient to protect  $W_3$ . If  $I(U_2; Y_2 | U_1) > I(X; Y_1 | U_1)$ , the randomness of  $W_2$  is sufficient to exhaust receiver 1's decoding capability, and hence is good enough for protecting  $W_3$ . Hence, in this case, no binning is required in layer 3, and  $R_3 \leq I(X; Y_3 | U_2)$ . On the other hand, if  $I(U_2; Y_2 | U_1) \leq I(X; Y_1 | U_1)$ , binning is required at layer 3 to protect  $W_3$  jointly with randomness of  $W_2$ , and hence,  $R_3 \leq I(U_2; Y_2 | U_1) - I(X; Y_1 | U_1) + I(X; Y_3 | U_2)$ . This can also be

written as  $R_3 \leq I(X; Y_3|U_2) - I(X; Y_1|U_2) + I(U_2; Y_2|U_1) - I(U_2; Y_1|U_1)$ , which has a clear intuitive interpretation. If receiver 1 know the message  $W_1, W_2$  (i.e.,  $U_1, U_2$ ), the secrecy rate of  $W_3$  will be  $I(U_2; Y_2|U_1) - I(X; Y_1|U_1)$ . But part of  $U_2$  is secure from receiver 1 with rate  $I(U_2; Y_2|U_1) - I(U_2; Y_1|U_1)$ , which can be used to convey further secrecy rate for  $W_3$ .

In the converse proof, the key idea to bound  $R_3$  is to exploit the intuitions gathered in the two cases of the achievable scheme. For the case that  $W_2$  is sufficient to protect  $W_3$ ,  $R_3$  can be bounded directly by the decoding capability of receiver 3. For the case that  $W_2$  is not sufficient to protect  $W_3$ , our novelty lies in bounding  $R_3 - R_2$  rather than bounding  $R_3$  directly, because  $R_3$  is closely related to  $R_2$  due to the fact that  $W_2$  is utilized to protect  $W_3$  in the achievable scheme, and hence  $R_3$  should be bounded by decoding the capability of receiver  $Y_2$  as shown in the bound of  $R_3$ . However, directly bounding  $R_3$  would involve only the decoding and secrecy constraints on  $W_3$  and hence  $Y_1$  and  $Y_3$ , but it is challenging to introduce  $Y_2$  to the bound of  $R_3$ . In this case, bounding  $R_3 - R_2$  naturally incorporates the decoding capability of receiver  $Y_2$  into the bound. Furthermore, in order to derive a tight bound, a critical step is to identify a useful term that corresponds to receiver 1's knowledge of  $W_2$  given  $W_1$  and  $W_3$ , which vanishes in this case and hence discarding it does not loosen the bound.

We next outline the proofs of achievability and converse for Theorem 1 in two subsections.

#### A. Proof of Achievability

*Random codebook generation:* Fix a distribution  $P_{U_1}P_{U_2|U_1}P_{X|U_2}P_{Y_1, Y_2, Y_3|X}$ . Randomly generate the codebook as follows:

- Generate  $2^{nR_1}$  independent identically distributed (i.i.d.)  $u_1^n$  with distribution  $\prod_{i=1}^n p(u_{1,i})$ . Index these codewords as  $u_1^n(w_1)$ ,  $w_1 \in [1, 2^{n\tilde{R}_1}]$ .
- 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  $u_2^n(w_1, w_2)$ ,  $w_2 \in [1, 2^{n\tilde{R}_2}]$ .
- For each  $u_2^n(w_1, w_2)$ , generate  $2^{n\tilde{R}_3}$  i.i.d.  $x^n$  with distribution  $\prod_{i=1}^n p(x_i|u_{2,i})$ . Partition these codewords into  $2^{n\tilde{R}_3}$  bins. Hence, there are  $2^{n(\tilde{R}_3 - R_3)}$  number of  $x^n$  in each bin. We use  $w_3 \in [1 : 2^{n\tilde{R}_3}]$  to denote the bin number, and  $l \in [1 : 2^{n(\tilde{R}_3 - R_3)}]$  to denote the index within the bin. Hence, each  $x^n$  is indexed by  $(w_1, w_2, w_3, l)$ .

The chosen codebook is revealed to both the transmitter and the receivers. Since  $w_3$  is superposed on  $w_2$ , the uncertainty that receiver 1 has about  $w_2$  propagates to the uncertainty that receiver 1 has about  $w_3$ . Hence, both  $w_2$  and  $l$  are utilized to protect  $w_3$ .

*Encoding:* To send a message tuple  $(w_1, w_2, w_3)$ , the transmitter randomly and uniformly generates  $l \in [1 : 2^{n(\tilde{R}_3 - R_3)}]$ , and sends  $x^n(w_1, w_2, w_3, l)$ .

*Decoding:*

- Receiver 1 claims that  $\hat{w}_1$  is sent, if there exists a unique  $\hat{w}_1$  such that  $(u_1^n(\hat{w}_1), y_1^n) \in T_\epsilon^n(P_{U_1 Y_1})$ . Otherwise, it declares an error.

- Receiver 2 claims that  $(\hat{w}_1, \hat{w}_2)$  is sent, if there exists a unique pair  $(\hat{w}_1, \hat{w}_2)$  such that  $(u_1^n(\hat{w}_1), u_2^n(\hat{w}_1, \hat{w}_2), y_2^n) \in T_\epsilon^n(P_{U_1 U_2 Y_2})$ . Otherwise, it declares an error.
- Receiver 3 claims that  $(\hat{w}_1, \hat{w}_2, \hat{w}_3)$  is sent, if there exists a unique tuple  $(\hat{w}_1, \hat{w}_2, \hat{w}_3, \hat{l})$  such that  $(u_1^n(\hat{w}_1), u_2^n(\hat{w}_1, \hat{w}_2), u_3^n(\hat{w}_1, \hat{w}_2, \hat{w}_3, \hat{l}), y_3^n) \in T_\epsilon^n(P_{U_1 U_2 U_3 Y_3})$ . Otherwise, it declares an error.

We first analyze the probability of decoding error, and then analyze the leakage rate.

*Analysis of error probability:* By the law of large numbers and the packing lemma, it can be shown that receiver  $k$  decodes the messages  $(w_1, \dots, w_k)$  with asymptotically small probability of error for  $k = 1, 2, 3$ , if the following inequalities are satisfied:

$$\begin{aligned} R_1 &\leq I(U_1; Y_1), \\ R_2 &\leq I(U_2; Y_2|U_1), \\ \tilde{R}_3 &\leq I(X; Y_3|U_2). \end{aligned} \quad (6)$$

*Analysis of leakage rate:* In this model, receiver 1 needs to be kept ignorant of message  $W_3$ . It is sufficient to show that the average leakage rate over the random generated codebook is asymptotically small, because this implies that there must exist one codebook guaranteeing such property.

$$\begin{aligned} &I(W_3; Y_1^n | W_1, C) \\ &= I(W_1, W_2, W_3, L; Y_1^n | C) - I(W_1, W_2, L; Y_1^n | W_3, C) \\ &\quad - H(W_3 | Y_1^n, W_1, C) + H(W_3 | Y_1^n, C) \\ &\leq I(W_1, W_2, W_3, L; Y_1^n | C) - I(W_1, W_2, L; Y_1^n | W_3, C) + n\epsilon_n \\ &= I(X^n; Y_1^n | C) - H(W_1, W_2, L | W_3, C) \\ &\quad + H(W_1, W_2, L | Y_1^n, W_3, C) + n\epsilon_n. \end{aligned} \quad (7)$$

Next, we bound the three terms in (7) one by one. For the first term, we have,

$$\begin{aligned} I(X^n; Y_1^n | C) &= I(U_1^n, X^n; Y_1^n | C) \\ &= I(U_1^n; Y_1^n | C) + I(X^n; Y_1^n | U_1^n, C) \\ &\leq H(U_1^n | C) + H(Y_1^n | U_1^n, C) - H(Y_1^n | X^n, C) \\ &\leq nR_1 + nH(Y_1 | U_1) - nH(Y_1 | X) \\ &= nR_1 + nI(X; Y_1 | U_1). \end{aligned} \quad (8)$$

For the second term, due to the independence of  $W_1, W_2$  and  $L$ , we have

$$H(W_1, W_2, L | W_3, C) = nR_1 + nR_2 + n(\tilde{R}_3 - R_3). \quad (9)$$

For the last term, we have

$$\begin{aligned} &H(W_1, W_2, L | Y_1^n, W_3, C) \\ &= H(W_2, L | Y_1^n, W_3, C) + H(W_1 | Y_1^n, W_2, W_3, C) \\ &\leq H(W_2, L | Y_1^n, W_3, C) + n\epsilon_n \\ &\leq H(W_2, L | Y_1^n, U_1^n, W_3) + 2n\epsilon_n. \end{aligned} \quad (10)$$

Following the techniques in [10, Chapter 22], it can be shown that if  $R_2 + \tilde{R}_3 - R_3 \geq I(X; Y_1 | U_1)$  and  $R_2 \geq I(U_2; Y_1 | U_1)$ , then

$$\begin{aligned} &\lim_{n \rightarrow \infty} \frac{1}{n} H(W_2, L | Y_1^n, U_1^n, W_3) \\ &\leq R_2 + \tilde{R}_3 - R_3 - I(X; Y_1 | U_1) + \delta(\epsilon). \end{aligned}$$

Combining the above analysis of the three terms together, it is clear that  $\frac{1}{n}I(W_3; Y_1^n|W_1, \mathcal{C}) \rightarrow 0$  as  $n \rightarrow \infty$ , if the following inequalities are satisfied:

$$\begin{aligned} R_2 + \tilde{R}_3 - R_3 &\geq I(X; Y_1|U_1), \\ R_2 &\geq I(U_2; Y_1|U_1). \end{aligned} \quad (11)$$

Combining the bounds in (6) and (11), we conclude that the rate tuple  $(R_1, R_2, R_3)$  is achievable if

$$\begin{aligned} R_1 &\leq I(U_1; Y_1), \\ R_2 &\leq I(U_2; Y_2|U_1), \\ R_3 &\leq \min\{0, I(U_2; Y_2|U_1) - I(X; Y_1|U_1)\} + I(X; Y_3|U_2). \end{aligned}$$

We note that the lower bound on  $R_2$  is redundant due to the fact that if the rate  $R_2 = I(U_2; Y_2|U_1)$  can be achieved, any rate below this value can be achieved by sending certain amount of information independent of  $W_2$ . Since the second layer is utilized to protect  $W_3$ , we generate  $2^{nI(U_2; Y_2|U_1)}$  of  $u_2^n$  for each  $u_1^n$  such that the secrecy rate  $R_3$  is maximized.

We finally note that it can be easily argued that there exists one codebook that guarantees both asymptotically small probability of error and asymptotically small leakage rate.

### B. Proof of Converse

By Fano's inequality and the secrecy requirement, we have the following inequalities:

$$\begin{aligned} H(W_k|Y_k^n) &\leq n\epsilon_n, \text{ for } 1 \leq k \leq 3, \\ I(W_3; Y_1^n|W_1) &\leq n\epsilon_n. \end{aligned} \quad (12)$$

We set  $U_{1,i} = (W_1, Y_1^{i-1})$ ,  $U_{2,i} = (W_1, W_2, Y_2^{i-1})$ ,  $U_{3,i} = (W_1, W_2, W_3, Y_3^{i-1}, Y_{1,i+1}^n)$ . It can be shown that the following Markov chain is satisfied:

$$U_{1,i} \rightarrow U_{2,i} \rightarrow U_{3,i} \rightarrow X_i \rightarrow Y_{3,i} \rightarrow Y_{2,i} \rightarrow Y_{1,i} \quad (13)$$

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

We first bound the rate  $R_1$  as follows.

$$\begin{aligned} nR_1 &\leq I(W_1; Y_1^n) + n\epsilon_n \\ &= \sum_{i=1}^n I(W_1; Y_{1,i}|Y_1^{i-1}) + n\epsilon_n \\ &\leq \sum_{i=1}^n I(W_1, Y_1^{i-1}; Y_{1,i}) + n\epsilon_n \\ &= \sum_{i=1}^n I(U_{1,i}; Y_{1,i}) + n\epsilon_n. \end{aligned} \quad (14)$$

Similarly, we bound the rate  $R_2$  as follows.

$$\begin{aligned} nR_2 &\leq I(W_2; Y_2^n|W_1) + n\epsilon_n \\ &= \sum_{i=1}^n I(W_2; Y_{2,i}|W_1, Y_2^{i-1}) + n\epsilon_n \\ &= \sum_{i=1}^n I(W_2; Y_{2,i}|W_1, Y_1^{i-1}, Y_2^{i-1}) + n\epsilon_n \\ &\leq \sum_{i=1}^n I(W_2, Y_2^{i-1}; Y_{2,i}|W_1, Y_1^{i-1}) + n\epsilon_n \\ &= \sum_{i=1}^n I(U_{2,i}; Y_{2,i}|U_{1,i}) + n\epsilon_n. \end{aligned} \quad (15)$$

We next derive two bounds on  $R_3$ . Following the steps similar to those in bounding  $R_1$  and  $R_2$ , we derive the following bound.

$$\begin{aligned} nR_3 &\leq I(W_3; Y_3^n|W_1, W_2) + n\epsilon_n \\ &= \sum_{i=1}^n I(W_3; Y_{3,i}|W_1, W_2, Y_3^{i-1}) + n\epsilon \\ &\leq \sum_{i=1}^n I(W_3, Y_3^{i-1}; Y_{3,i}|W_1, W_2, Y_2^{i-1}) + n\epsilon \\ &\leq \sum_{i=1}^n I(W_3, Y_3^{i-1}, Y_{1,i+1}^n; Y_{3,i}|W_1, W_2, Y_2^{i-1}) + n\epsilon \\ &= \sum_{i=1}^n I(U_{3,i}; Y_{3,i}|U_{2,i}) \\ &\leq \sum_{i=1}^n I(X_i; Y_{3,i}|U_{2,i}). \end{aligned} \quad (16)$$

We now derive the second bound on  $R_3$  by bounding  $R_3 - R_2$  as follows.

$$\begin{aligned} nR_3 - nR_2 &= H(W_3) - H(W_2) \\ &\leq H(W_3|W_1, W_2) + n\epsilon_n - H(W_3|Y_3^n, W_1, W_2) - H(W_2) \\ &\quad + n\epsilon_n - I(W_3; Y_1^n|W_1) \\ &= I(W_3; Y_3^n|W_1, W_2) - H(W_2) - H(W_3|W_1) \\ &\quad + H(W_3|Y_1^n, W_1) + 2n\epsilon_n \\ &= I(W_3; Y_3^n|W_1, W_2) - H(W_2, W_3|W_1) \\ &\quad + H(W_2, W_3|Y_1^n, W_1) - H(W_2|Y_1^n, W_1, W_3) + 2n\epsilon_n \\ &\stackrel{(a)}{\leq} I(W_3; Y_3^n|W_1, W_2) - I(W_2, W_3; Y_1^n|W_1) + 2n\epsilon_n, \end{aligned} \quad (17)$$

where (a) is due to the fact that the entropy  $H(W_2|Y_1^n, W_1, W_3)$  is nonnegative. Here we note that discarding such an entropy term does not result in a looser bound. This is because if  $H(W_2|Y_1^n, W_1, W_3)$  is not a vanishing term (which implies that  $Y_1$  cannot decode  $W_2$  given  $W_1$  and  $W_3$ ), then  $W_2$  provides enough randomness for protecting  $W_3$ , and hence (16) (which is bounded by the decoding capability of receiver  $Y_3$ ) should already provide a tighter bound on  $R_3$ .

We further bound the two terms in (17) one by one. The first term in (17) is bounded as follows:

$$\begin{aligned} I(W_3; Y_3^n|W_1, W_2) &= \sum_{i=1}^n I(W_3; Y_{3,i}|W_1, W_2, Y_3^{i-1}) \\ &= \sum_{i=1}^n I(W_3, Y_{1,i+1}^n; Y_{3,i}|W_1, W_2, Y_3^{i-1}) \\ &\quad - I(Y_{1,i+1}^n; Y_{3,i}|W_1, W_2, W_3, Y_3^{i-1}) \\ &= \sum_{i=1}^n I(W_3, Y_{1,i+1}^n; Y_{3,i}|W_1, W_2, Y_3^{i-1}) \\ &\quad - I(Y_3^{i-1}; Y_{1,i}|W_1, W_2, W_3, Y_{1,i+1}^n) \\ &\leq \sum_{i=1}^n I(W_3, Y_3^{i-1}, Y_{1,i+1}^n; Y_{3,i}|W_1, W_2, Y_2^{i-1}) \\ &\quad - I(Y_3^{i-1}; Y_{1,i}|W_1, W_2, W_3, Y_{1,i+1}^n). \end{aligned} \quad (18)$$

The second term in (17) is bounded as follows:

$$\begin{aligned}
& -I(W_2, W_3; Y_1^n | W_1) \\
&= \sum_{i=1}^n -I(W_2, W_3; Y_{1,i} | W_1, Y_{1,i+1}^n) \\
&= \sum_{i=1}^n -I(W_2, W_3, Y_3^{i-1}; Y_{1,i} | W_1, Y_{1,i+1}^n) \\
&\quad + I(Y_3^{i-1}; Y_{1,i} | W_1, W_2, W_3, Y_{1,i+1}^n) \\
&= \sum_{i=1}^n -I(Y_3^{i-1}; Y_{1,i} | W_1, Y_{1,i+1}^n) \\
&\quad - I(W_2, W_3; Y_{1,i} | W_1, Y_{1,i+1}^n, Y_3^{i-1}) \\
&\quad + I(Y_3^{i-1}; Y_{1,i} | W_1, W_2, W_3, Y_{1,i+1}^n) \\
&= \sum_{i=1}^n -I(Y_3^{i-1}; Y_{1,i} | W_1, Y_{1,i+1}^n) \\
&\quad - I(W_2, W_3, Y_3^{i-1}, Y_{1,i+1}^n; Y_{1,i} | W_1, Y_1^{i-1}) \\
&\quad + I(Y_3^{i-1}, Y_{1,i+1}^n; Y_{1,i} | W_1, Y_1^{i-1}) \\
&\quad + I(Y_3^{i-1}; Y_{1,i} | W_1, W_2, W_3, Y_{1,i+1}^n) \\
&\stackrel{(a)}{=} \sum_{i=1}^n -I(W_2, W_3, Y_3^{i-1}, Y_{1,i+1}^n; Y_{1,i} | W_1, Y_1^{i-1}) \\
&\quad + I(Y_3^{i-1}; Y_{1,i} | W_1, W_2, W_3, Y_{1,i+1}^n), \tag{19}
\end{aligned}$$

where (a) is due to the following fact:

$$\begin{aligned}
& \sum_{i=1}^n [-I(Y_3^{i-1}; Y_{1,i} | W_1, Y_{1,i+1}^n) \\
& \quad + I(Y_3^{i-1}, Y_{1,i+1}^n; Y_{1,i} | W_1, Y_1^{i-1})] \\
&= \sum_{i=1}^n [-I(Y_1^{i-1}; Y_{1,i} | W_1, Y_{1,i+1}^n) \\
& \quad - I(Y_3^{i-1}; Y_{1,i} | W_1, Y_1^{i-1}, Y_{1,i+1}^n) \\
& \quad + I(Y_{1,i+1}^n; Y_{1,i} | W_1, Y_1^{i-1}) \\
& \quad + I(Y_3^{i-1}; Y_{1,i} | W_1, Y_1^{i-1}, Y_{1,i+1}^n)] \\
&= 0.
\end{aligned}$$

Combining (18) and (19), we obtain

$$\begin{aligned}
& nR_3 - nR_2 \\
&\leq \sum_{i=1}^n [I(U_{3,i}; Y_{3,i} | U_{2,i}) - I(U_{3,i}; Y_{1,i} | U_{1,i})] + 2n\epsilon_n \\
&\leq \sum_{i=1}^n [I(X_i, Y_{3,i} | U_{2,i}) - I(X_i; Y_{1,i} | U_{1,i})] + 2n\epsilon_n. \tag{20}
\end{aligned}$$

We finally define a uniformly distributed random variable  $Q \in \{1, \dots, n\}$ , and set  $U_k \triangleq (Q, U_{k,Q})$ ,  $Y_k \triangleq (Q, Y_{k,Q})$ , for  $k = 1, 2, 3$ , and  $X \triangleq (Q, X_Q)$ . Then the desired bounds follow from the standard single letter characterization, which concludes the proof.

#### IV. CONCLUSION

In this paper, we have studied a three-receiver discrete memoryless degraded broadcast channel with secrecy outside

of a bounded range. We have characterized the secrecy capacity region for such a model. In particular, we have proposed a novel achievable scheme in which a superposition layer of a message serves as random resource jointly with binning to achieve the secrecy constraint. We have showed that such a scheme is optimal by developing a converse proof, which exploits the idea of the achievable scheme for manipulating terms. The techniques derived in this paper can be further generalized to study the degraded broadcast channel with arbitrary  $K$  receivers and with secrecy outside of an arbitrarily bounded range. In the future, we will also extend the current study to models with receivers having continuously changing channel state parameters.

#### 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] G. Bagherikaram, A. Motahari, and A. Khandani, "The secrecy rate region of the broadcast channel," *arXiv preprint*, 2008.
- [6] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz), "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, 2012.
- [8] S. Zou, Y. Liang, L. Lai, and S. Shamai (Shitz), "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.
- [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] A. El Gamal and Y.-H. Kim, *Network Information Theory*. New York: Cambridge University Press, 2012.
- [11] I. Csiszár and J. Körner, *Information theory: coding theorems for discrete memoryless systems*. Cambridge University Press, 2011.