The Individual Secrecy Capacity of Degraded Multi-Receiver Wiretap Broadcast Channels

Ahmed S. Mansour*, Rafael F. Schaefer†, and Holger Boche*

* Lehrstuhl für Theoretische Informationstechnik
Technische Universität München
Munich 80290, Germany
Email:{ahmed.mansour, boche}@tum.de

† Department of Electrical Engineering
Princeton University
Princeton, NJ 08544, USA
Email: rafaelfs@princeton.edu

***Abstract*—We study secure communication over a degraded wiretap broadcast channel with multiple receivers and an eavesdropper. We consider two different secrecy measures: the traditional joint secrecy where the mutual information leakage of all messages must be small; and individual secrecy where the sum of the information leakage of each individual message must be small. At first, we investigate the joint secrecy criterion, where we present the capacity region established before and provide a simpler converse proof. We then consider the individual secrecy criterion and establish its capacity region, by combining the techniques of wiretap random coding and Shannon's one time pad principle. Our results indicate that the individual secrecy capacity region is bigger than the joint one. Further, we show that the established capacity regions are valid for any degraded wiretap broadcast channel, regardless of the degradedness order of the eavesdropper. Finally, we extend our results to Gaussian channels.**

I. Introduction

The wireless medium is characterized by an open nature that allows transmitted signals to be received not only by legitimate receivers but eavesdroppers as well. To overcome this problem, physical or higher layers secrecy techniques are used. Recently, physical layer security also known as *information theoretic security* is becoming more attractive because it is not based on any assumptions regarding the computational power of the eavesdroppers. Information theoretic security was first introduced by Shannon in [1], where he showed that secure communication between the transmitter and the receiver can be achieved using a shared secret key, whose entropy is greater than or equal the entropy of the message. In [2], Wyner studied the degraded wiretap channel and proved that secure transmission is still achievable in the absence of a secret key. In [3], this result was extended to the Gaussian wiretap channel and in [4], it was extended to the general wiretap broadcast channel (BC). In [5], Wyner's and shannon's results were combined by investigating secure communication over a wiretap channel in the presence of a shared secret key. The secrecy capacity was established by combining the wiretap coding principle along with Shannon's ciphering technique.

Recently, the problem of secure communication in wiretap BC with more than one receiver has captured a lot of attention. Researchers found it very challenging to establish the secrecy capacity for the general multi-receiver wiretap BC, but they managed to solve different special cases. In [6], the degraded two-receiver wiretap BC was investigated, where the authors succeeded in establishing the secrecy capacity. In [7], this result was extended to the degraded wiretap BC with arbitrary number of receivers. The importance of the class of degraded channels lies in the fact that scalar Gaussian channels are inherently degraded. In [8], the secrecy capacities for both scalar and vector Gaussian multi-receiver wiretap BC were established. However, all these works only considered the *joint secrecy* requirement, where the legitimate receivers do not trust each other. In this paper, we will study the degraded multi-receiver wiretap BC under another secrecy criterion known as the *individual secrecy*. Differently from the joint secrecy, the individual secrecy is based on the mutual trust between the legitimate receivers. To the best of our knowledge, previous literature never investigated individual secrecy for the general wiretap BC. It was only considered for wiretap multiple access channels in [9] and for wiretap BC with receiver side information in [10, 11], where it was shown that individual secrecy can provide a larger secrecy capacity using the available side information to apply secret key encoding.

This paper is organized as follows: In Section II, we describe the model of the degraded multi-receiver wiretap channel and explain the differences between joint and individual secrecy. In Section III, we briefly present the joint secrecy capacity of the degraded multi-receiver wiretap BC and present a simpler converse proof. We then establish the individual secrecy capacity for the same channel. Our results indicate that even in the absence of the receiver side information, the individual secrecy can provide a larger capacity region as compared to joint one. Finally, we extend our results to the Gaussian channels in Section IV.

II. Degraded Multi-Receiver Wiretap BC

The degraded multi-receiver wiretap BC consists of a transmitter with an input alphabet $\mathcal{X}$, k legitimate receivers with output alphabets $\mathcal{Y}_j$, where $j \in [\![1,k]\!]$ and an external eavesdropper with output alphabet $\mathcal{Z}$, such that the following Markov chain holds

$$\mathrm{X} - \mathrm{Y}_1 - \mathrm{Y}_2 - \cdots - \mathrm{Y}_k - \mathrm{Z}. \tag{1}$$

We consider the standard model of a block code of arbitrary but fixed length n with input and output sequences x^n, y_j^n and z^n. Through the whole paper j is taken to be in $[\![1,k]\!]$, unless stated otherwise.

Definition 1. *A $(2^{nR_1}, \ldots, 2^{nR_k}, n)$ code $\mathcal{C}_n$ for the multi-receiver wiretap BC consists of: k independent message sets $\mathcal{M}_j = [\![1, 2^{nR_j}]\!]$, a source of local randomness $\mathcal{R}$, an encoding function at the transmitter*

$$E : \mathcal{M}_1 \times \cdots \times \mathcal{M}_k \times \mathcal{R} \to \mathcal{X}^n,$$

978-1-4673-6432-4/15/$31.00 ©2015 IEEE

which maps the k confidential messages $(m_1, \ldots, m_k) \in \mathcal{M}_1 \times \cdots \times \mathcal{M}_k$ and a realization of the local randomness $r \in \mathcal{R}$ to a codeword $x^n(m_1, \ldots, m_k, r)$, and k decoders

$$\varphi_j : \mathcal{Y}_j^n \to \mathcal{M}_j \cup \{?\},$$

that maps each channel observation at the respective receiver to the corresponding required message or an error message.

We assume that the messages $\mathrm{M}_1, \ldots, \mathrm{M}_k$ are chosen uniformly at random. The reliability performance of $\mathcal{C}_n$ is measured in terms of its average probability of error

$$P_e(\mathcal{C}_n) \triangleq \mathbb{P}\big[\hat{\mathrm{M}}_1 \neq \mathrm{M}_1 \text{ or } \ldots \text{ or } \hat{\mathrm{M}}_k \neq \mathrm{M}_k\big], \tag{2}$$

where $\hat{\mathrm{M}}_j$ is the estimated message at the j^{th} legitimate receiver. It is important to note that one of the consequences of the Markov chain in (1) is that each legitimate receiver is not only capable of decoding its own message, but it can also decode the messages of the receivers degraded from it because these channels are worse than its own channel.

The secrecy performance of the code that assures the ignorance of the eavesdropper about the confidential messages, can be measured with respect to two different secrecy criteria.

1. Joint Secrecy: This criterion requires the mutual leakage of the confidential messages to the eavesdropper to be small. This condition can be formulated as follows:

$$\begin{aligned} L(\mathcal{C}_n) &\triangleq \mathbb{I}(\mathrm{M}_1, \ldots, \mathrm{M}_k; \mathrm{Z}^n) \leq \tau_n \\ &\triangleq \sum_{j=1}^{k} \mathbb{I}(\mathrm{M}_j; \mathrm{Z}^n | \mathrm{M}_{j+1}, \ldots, \mathrm{M}_k) \leq \tau_n. \end{aligned} \tag{3}$$

2. Individual Secrecy: This criterion requires the sum of the individual leakage of each confidential message to the eavesdropper to be small. This requirement can be expressed as follows:

$$L(\mathcal{C}_n) \triangleq \sum_{j=1}^{k} \mathbb{I}(\mathrm{M}_j; \mathrm{Z}^n) \leq \tau_n. \tag{4}$$

In order to differentiate between these two criteria, we need to understand the degree of secrecy each one provides. The joint secrecy criterion is a conservative secrecy constraint, where the legitimate receivers do not trust each other, so it guarantees that the confidential message of each receiver is secure, even if the confidential messages of the other receivers were revealed to the eavesdropper. On the other hand, the individual secrecy criterion is based on the mutual trust between the legitimate receivers, thus the legitimate receivers cooperate together to protect their messages against eavesdropping. This implies that revealing the confidential message of any receiver to the eavesdropper might threaten the secrecy of all other messages. It is important to note that, any code that satisfies the joint secrecy criterion also satisfies the individual one. This is because, as long the confidential messages are independent,

$$\sum_{j=1}^{k} \mathbb{I}(\mathrm{M}_j; \mathrm{Z}^n) \leq \mathbb{I}(\mathrm{M}_1, \ldots, \mathrm{M}_k; \mathrm{Z}^n).$$

Although the previous argument might advocates the joint secrecy over the individual one, there is another feature that promotes the usage of individual secrecy. It was shown in [10, 11] that, the individual secrecy can provide a bigger achievable region compared to the joint one for the wiretap BC with receiver side information. Although this result was based on using the available side information as secret keys, we will show that even in the absence of the receiver side information the individual secrecy can still provide a larger capacity region.

Definition 2. *A rate tuple $(R_1, \ldots, R_k) \in \mathbb{R}_+^k$ is achievable for the multi-receiver wiretap BC, if there exists a sequence of $(2^{nR_1}, \ldots, 2^{nR_k}, n)$ codes $\mathcal{C}_n$ and two sequence ϵ_n and τ_n, where $\lim_{n\to\infty} \epsilon_n, \tau_n = 0$ such that, for n is large enough, the following holds:*

$$P_e(\mathcal{C}_n) \leq \epsilon_n \qquad \textit{and} \qquad L(\mathcal{C}_n) \leq \tau_n. \tag{5}$$

Depending on the selected secrecy criteria, $L(\mathcal{C}_n)$ is given by (3) *or* (4)*.*

Regardless of the selected secrecy criteria, we can reformulate the reliability constraint by using Fano's inequality as follows:

$$\begin{aligned} \mathbb{H}(\mathrm{M}_j | \mathrm{Y}_j^n \mathrm{M}_{j+1} \ldots \mathrm{M}_k) &\leq \mathbb{H}(\mathrm{M}_j | \mathrm{Y}_j^n) \leq \mathbb{H}(\mathrm{M}_j | \hat{\mathrm{M}}_j) \\ &\leq 1 + P_e \mathbb{H}(\mathrm{M}_j) \leq 1 + \epsilon_n n R_j. \end{aligned}$$

Now if we let $\tilde{\gamma}_j(\epsilon_n) = 1/n + \epsilon_n R_j$, we have

$$\begin{aligned} R_j &= \frac{1}{n} \mathbb{H}(\mathrm{M}_j | \mathrm{M}_{j+1} \ldots \mathrm{M}_k) \\ &\leq \frac{1}{n} \Big[\mathbb{H}(\mathrm{M}_j | \mathrm{M}_{j+1} \ldots \mathrm{M}_k) - \mathbb{H}(\mathrm{M}_j | \mathrm{Y}_j^n \mathrm{M}_{j+1} \ldots \mathrm{M}_k) \Big] \\ &\quad + \tilde{\gamma}_j(\epsilon_n) \\ &= \frac{1}{n} \mathbb{I}(\mathrm{M}_j; \mathrm{Y}_j^n | \mathrm{M}_{j+1} \ldots \mathrm{M}_k) + \tilde{\gamma}_j(\epsilon_n). \end{aligned} \tag{6}$$

III. Secrecy Capacity of Degraded Wiretap BC: Joint Vs Individual

In this section, we will present the joint secrecy capacity region of the degraded multi-receiver wiretap BC. This region was established in [6] for $k = 2$ and extended to arbitrary number of receivers in [7]. In particular, we will provide a simpler converse proof for the previously established region, which will be used later to establish the individual secrecy capacity. We will then establish the individual secrecy capacity for the degraded two-receiver wiretap BC and the multi-receiver case as well, showing that the individual secrecy provides a larger capacity region. Finally, we will show that the established capacity regions for the two criteria establish the secrecy capacity of any degraded wiretap BC regardless of the degradedness order of the eavesdropper.

A. Joint Secrecy Capacity Region

Theorem 1. *The joint secrecy capacity region of the degraded multi-receiver wiretap BC is given by the union of all rate tuples $(R_1, \ldots, R_k) \in \mathbb{R}_+^k$ that satisfy*

$$R_j \leq \mathbb{I}(\mathrm{U}_j; \mathrm{Y}_j | \mathrm{U}_{j+1}) - \mathbb{I}(\mathrm{U}_j; \mathrm{Z} | \mathrm{U}_{j+1}), \tag{7}$$

where $\mathrm{U}_1 = \mathrm{X}$, $\mathrm{U}_{k+1} = \emptyset$ and the union is taken over all random variables $(\mathrm{U}_k, \ldots, \mathrm{U}_2, \mathrm{X})$ such that, $\mathrm{U}_k - \cdots - \mathrm{U}_2 - \mathrm{X} - \mathrm{Y}_1 - \mathrm{Y}_2 - \cdots - \mathrm{Y}_k - \mathrm{Z}$ forms a Markov chain.

Proof: This capacity region was established in [7]. The achievability is based on Cover's superposition coding scheme in addition to the random binning technique. For

the converse, we present a simpler proof that will be later adapted to the individual secrecy criterion. We start by letting $\mathrm{U}_j^i \triangleq (\mathrm{M}_j, \mathrm{Y}_{j-1}^{i-1}, \tilde{\mathrm{Z}}^{i+1}, \mathrm{U}_{j+1}^i)$, where $\tilde{\mathrm{Z}}^{i+1} = (\mathrm{Z}_{i+1}, \ldots, \mathrm{Z}_n)$, $\mathrm{Y}_0^{i-1} = \emptyset$ and $\mathrm{U}_{k+1}^i = \emptyset$. For R_k, we have

$$\begin{aligned}
R_k &\overset{(a)}{\leq} \frac{1}{n}\Big[\mathbb{I}(\mathrm{M}_k;\mathrm{Y}_k^n) - \mathbb{I}(\mathrm{M}_k;\mathrm{Z}^n)\Big] + \gamma_k(\epsilon_n,\tau_n)\\
&\overset{(b)}{=} \frac{1}{n}\sum_{i=1}^n \Big[\mathbb{I}(\mathrm{M}_k;\mathrm{Y}_{ki}|\mathrm{Y}_k^{i-1}\tilde{\mathrm{Z}}^{i+1}) - \mathbb{I}(\mathrm{M}_k;\mathrm{Z}_i|\mathrm{Y}_k^{i-1}\tilde{\mathrm{Z}}^{i+1})\Big]\\
&\quad + \gamma_k(\epsilon_n,\tau_n)\\
&\overset{(c)}{\leq} \frac{1}{n}\sum_{i=1}^n \Big[\mathbb{I}(\mathrm{M}_k\mathrm{Y}_k^{i-1}\tilde{\mathrm{Z}}^{i+1};\mathrm{Y}_{ki}) - \mathbb{I}(\mathrm{M}_k\mathrm{Y}_k^{i-1}\tilde{\mathrm{Z}}^{i+1};\mathrm{Z}_i)\Big]\\
&\quad + \gamma_k(\epsilon_n,\tau_n)\\
&\overset{(c)}{\leq} \frac{1}{n}\sum_{i=1}^n \Big[\mathbb{I}(\mathrm{U}_k^i\mathrm{Y}_k^{i-1};\mathrm{Y}_{ki}) - \mathbb{I}(\mathrm{U}_k^i\mathrm{Y}_k^{i-1};\mathrm{Z}_i)\Big] + \gamma_k(\epsilon_n,\tau_n)\\
&\overset{(d)}{=} \frac{1}{n}\sum_{i=1}^n \Big[\mathbb{I}(\mathrm{U}_k^i;\mathrm{Y}_{ki}) - \mathbb{I}(\mathrm{U}_k^i;\mathrm{Z}_i)\Big] + \gamma_k(\epsilon_n,\tau_n) \qquad (8)
\end{aligned}$$

where $\gamma_k(\epsilon_n,\tau_n) = \tau_n/n + \tilde{\gamma}_k(\epsilon_n)$. (a) follows from (3) and (6); (b) follows from the Csiszár sum identity [4, Lemma 7]; (c) follows because Z_i is degraded from Y_{ki}, which implies that $\mathbb{I}(\mathrm{Y}_k^{i-1}\tilde{\mathrm{Z}}^{i+1};\mathrm{Y}_{ki}) \geq \mathbb{I}(\mathrm{Y}_k^{i-1}\tilde{\mathrm{Z}}^{i+1};\mathrm{Z}_i)$ and $\mathbb{I}(\mathrm{Y}_{k-1}^{i-1};\mathrm{Y}_{ki}|\mathrm{M}_k\mathrm{Y}_k^{i-1}\tilde{\mathrm{Z}}^{i+1}) \geq \mathbb{I}(\mathrm{Y}_{k-1}^{i-1};\mathrm{Z}_i|\mathrm{M}_k\mathrm{Y}_k^{i-1}\tilde{\mathrm{Z}}^{i+1})$; and (d) follows because Y_k is degraded from Y_{k-1}, leading $\mathbb{I}(\mathrm{Y}_k^{i-1};\mathrm{Y}_{ki}|\mathrm{M}_k\mathrm{Y}_{k-1}^{i-1}\tilde{\mathrm{Z}}^{i+1})$ and $\mathbb{I}(\mathrm{Y}_k^{i-1};\mathrm{Z}_i|\mathrm{M}_k\mathrm{Y}_{k-1}^{i-1}\tilde{\mathrm{Z}}^{i+1})$ to vanish. On the other hand, for R_j as $j \in [\![1, k-1]\!]$, we have

$$\begin{aligned}
R_j &\overset{(a)}{\leq} \frac{1}{n}\Big[\mathbb{I}(\mathrm{M}_j;\mathrm{Y}_j^n|\mathrm{M}_{j+1}\ldots\mathrm{M}_k) - \mathbb{I}(\mathrm{M}_j;\mathrm{Z}^n|\mathrm{M}_{j+1}\ldots\mathrm{M}_k)\Big]\\
&\quad + \gamma_j(\epsilon_n,\tau_n)\\
&\overset{(b)}{=} \frac{1}{n}\sum_{i=1}^n \Big[\mathbb{I}(\mathrm{M}_j;\mathrm{Y}_{ji}|\mathrm{M}_{j+1}\ldots\mathrm{M}_k\mathrm{Y}_j^{i-1}\tilde{\mathrm{Z}}^{i+1})\\
&\quad - \mathbb{I}(\mathrm{M}_j;\mathrm{Z}_i|\mathrm{M}_{j+1}\ldots\mathrm{M}_k\mathrm{Y}_j^{i-1}\tilde{\mathrm{Z}}^{i+1})\Big] + \gamma_j(\epsilon_n,\tau_n)\\
&\overset{(c)}{=} \frac{1}{n}\sum_{i=1}^n \Big[\mathbb{I}(\mathrm{M}_j;\mathrm{Y}_{ji}|\mathrm{M}_{j+1}\mathrm{Y}_j^{i-1}\ldots\mathrm{M}_k\mathrm{Y}_{k-1}^{i-1}\tilde{\mathrm{Z}}^{i+1})\\
&\quad - \mathbb{I}(\mathrm{M}_j;\mathrm{Z}_i|\mathrm{M}_{j+1}\mathrm{Y}_j^{i-1}\ldots\mathrm{M}_k\mathrm{Y}_{k-1}^{i-1}\tilde{\mathrm{Z}}^{i+1})\Big] + \gamma_j(\epsilon_n,\tau_n)\\
&\overset{(d)}{\leq} \frac{1}{n}\sum_{i=1}^n \Big[\mathbb{I}(\mathrm{U}_j^i;\mathrm{Y}_{ji}|\mathrm{U}_{j+1}^i) - \mathbb{I}(\mathrm{U}_j^i;\mathrm{Z}_i|\mathrm{U}_{j+1}^i)\Big]\\
&\quad + \gamma_j(\epsilon_n,\tau_n) \qquad (9)
\end{aligned}$$

where (a) follows from (3) and (6) as $\gamma_j(\epsilon_n,\tau_n) = \tau_n/n + \tilde{\gamma}_j(\epsilon_n)$; (b) follows from the Csiszár sum identity [4, Lemma 7]; (c) follows because $(\mathrm{Y}_{j+1}, \ldots, \mathrm{Y}_k)$ are degraded from Y_j, while (d) follows because Z_i is degraded from Y_{ji}, which implies that $\mathbb{I}(\mathrm{Y}_{j+1}^{i-1};\mathrm{Y}_{ji}|\mathrm{U}_{j+1}^i) \geq \mathbb{I}(\mathrm{Y}_{j+1}^{i-1};\mathrm{Z}_i|\mathrm{U}_{j+1}^i)$. If we introduce an independent uniformly distributed time sharing sequence to (8) and (9), then take the limit as $n \to \infty$ such that $\gamma_j(\epsilon_n,\tau_n) \to 0$, our converse is complete. ∎

Remark 1. *It worth mentioning, that the following Markov chain* $\mathrm{U}_k - \cdots - \mathrm{U}_2 - \mathrm{X}$ *was validated in the converse using the principle of functional dependence graph [12].*

Corollary 1. *The joint secrecy capacity region of the degraded two-receiver wiretap BC is given by the union of all rate pairs* $(R_1, R_2) \in \mathbb{R}_+^2$ *that satisfy*

$$R_2 \leq \mathbb{I}(\mathrm{U};\mathrm{Y}_2) - \mathbb{I}(\mathrm{U};\mathrm{Z}) \qquad (10a)$$
$$R_1 \leq \mathbb{I}(\mathrm{X};\mathrm{Y}_1|\mathrm{U}) - \mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}) \qquad (10b)$$

where the union is taken over all random variables (U, X)*, such that* $\mathrm{U} - \mathrm{X} - \mathrm{Y}_1 - \mathrm{Y}_2 - \mathrm{Z}$ *forms a Markov chain. Further it suffices to have* $|\mathcal{U}| \leq |\mathcal{X}| + 3$*.*

Proof: This capacity region was established in [6]. It can be derived from Theorem 1 by letting $k = 2$, where the cardinality argument follows by the Fenchel-Bunt strengthening of the Carathéodory's theorem [13, Appendix C]. ∎

B. Individual Secrecy Capacity Region

Theorem 2. *The individual secrecy capacity region of the degraded two-receiver wiretap BC is given by the union of all rate pairs* $(R_1, R_2) \in \mathbb{R}_+^2$ *that satisfy*

$$R_2 \leq \mathbb{I}(\mathrm{U};\mathrm{Y}_2) - \mathbb{I}(\mathrm{U};\mathrm{Z}) \qquad (11a)$$
$$R_1 \leq \mathbb{I}(\mathrm{X};\mathrm{Y}_1|\mathrm{U}) + \mathbb{I}(\mathrm{U};\mathrm{Z}) \qquad (11b)$$
$$R_1 \leq \mathbb{I}(\mathrm{X};\mathrm{Y}_1|\mathrm{U}) - \mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}) + R_2 \qquad (11c)$$

where the union is taken over all random variables (U, X)*, such that* $\mathrm{U} - \mathrm{X} - \mathrm{Y}_1 - \mathrm{Y}_2 - \mathrm{Z}$ *forms a Markov chain. Further it suffices to have* $|\mathcal{U}| \leq |\mathcal{X}| + 3$*.*

Remark 2. *The difference between this capacity region and the joint capacity region in* (10) *is that, the individual secrecy constraint allows the usage of* M_2 *as a secret key for* Y_1*, which leads to a higher rate* R_1*.*

Proof: The proof combines the technique of superposition coding with random binning and Shannon's ciphering system, where the Shannon ciphered message is interpreted as a part of the randomization index used to confuse the eavesdropper.

1. Message Sets: We start by dividing each message set $\mathcal{M}_j$, for $j = 1, 2$ into three independent parts $\mathcal{M}_{jl} = [\![1, 2^{nR_{jl}}]\!]$, for $l = 1, 2, 3$. In this division, we force $\mathcal{M}_{11}$ and $\mathcal{M}_{21}$ to be of the same size and use them to construct $\mathcal{M}_{\otimes_1} = [\![1, 2^{nR_{\otimes_1}}]\!]$ by *Xoring* their corresponding elements. We also make sure that $\mathcal{M}_{12}$ and $\mathcal{M}_{22}$ are of the same size and use them to construct $\mathcal{M}_{\otimes_2} = [\![1, 2^{nR_{\otimes_2}}]\!]$, such that

$$R_{\otimes_1} = R_{11} = R_{21} \quad \text{and} \quad R_{\otimes_2} = R_{12} = R_{22},$$
$$R_{\otimes_1} + R_{\otimes_2} \leq R_2. \qquad (12)$$

2. Random Codebook $\mathcal{C}_n$: Fix an input distribution $Q_{\mathrm{UX}}(u,x)$. Construct the codewords $u^n(m_2, m_{\otimes_1}, m_{r_1})$ for $m_2 \in \mathcal{M}_2$, $m_{\otimes_1} \in \mathcal{M}_{\otimes_1}$ and $m_{r_1} \in \mathcal{M}_{r_1} = [\![1, 2^{nR_{r_1}}]\!]$ by generating symbols $u_i(m_c, m_{\otimes_1}, m_{r_1})$ with $i \in [\![1, n]\!]$ independently according to $Q(u)$. For every $u^n(m_2, m_{\otimes_1}, m_{r_1})$ generate codewords $x^n(m_2, m_{\otimes_1}, m_{r_1}, m_{13}, m_{\otimes_2}, m_{r_2})$ for $m_{13} \in \mathcal{M}_{13}$, $m_{\otimes_2} \in \mathcal{M}_{\otimes_2}$, and $m_{r_2} \in \mathcal{M}_{r_2} = [\![1, 2^{nR_{r_2}}]\!]$ by generating symbols $x_i(m_2, m_{\otimes_1}, m_{r_1}, m_{13}, m_{\otimes_2}, m_{r_2})$ with $i \in [\![1, n]\!]$, independently at random according to $Q_{\mathrm{X|U}}(x|u(m_c, m_{\otimes_1}, m_{r_1}))$.

3. Encoder E: Given a message pair (m_1, m_2), it calculates the triple $(m_{13}, m_{\otimes_1}, m_{\otimes_2})$ then chooses a message pair (m_{r_1}, m_{r_2}) uniformly at random from the sets $\mathcal{M}_{r_1}$ and $\mathcal{M}_{r_2}$. Finally, it transmits the codeword $x^n(m_2, m_{\otimes_1}, m_{r_1}, m_{13}, m_{\otimes_2}, m_{r_2})$.

4. First Decoder φ_1: Given y_1^n, it outputs $\hat{m}_1$; where $\hat{m}_1$ is the concatenation of $\hat{m}_{11}$, $\hat{m}_{12}$ and $\hat{m}_{13}$. First, it finds the unique messages $\hat{m}_2$, $\hat{m}_{\otimes_1}$, $\hat{m}_{r_1}$, $\hat{m}_{13}$, $\hat{m}_{\otimes_2}$ and $\hat{m}_{r_2}$ such that $u^n(\hat{m}_2, \hat{m}_{\otimes_1}, \hat{m}_{r_1})$, $x^n(\hat{m}_2, \hat{m}_{\otimes_1}, \hat{m}_{r_1}, \hat{m}_{13}, \hat{m}_{\otimes_2}, \hat{m}_{r_2})$ and y_1^n are jointly typical. Then, it computes the pair $(\hat{m}_{11}, \hat{m}_{12})$ by *Xoring* $(\hat{m}_{21}, \hat{m}_{22})$ and $(\hat{m}_{\otimes_1}, \hat{m}_{\otimes_2})$ respectively.

5. Second Decoder φ_2: Given y_2^n, it outputs $\tilde{m}_2$ by finding the unique triple $(\tilde{m}_2, \tilde{m}_{\otimes_1}, \tilde{m}_{r_1})$ such that $u^n(\tilde{m}_2, \tilde{m}_{\otimes_1}, \tilde{m}_{r_1})$ and y_2^n are jointly typical.

6. Reliability Analysis: We define the average error probability for this scheme as

$$\tilde{P}_e(\mathcal{C}_n) \triangleq \mathbb{P}\Big[(\hat{\mathrm{M}}_2, \hat{\mathrm{M}}_{\otimes_1}, \hat{\mathrm{M}}_{\mathrm{r}_1}, \hat{\mathrm{M}}_{13}, \hat{\mathrm{M}}_{\otimes_2}, \hat{\mathrm{M}}_{\mathrm{r}_2}) \neq (\mathrm{M}_2, \mathrm{M}_{\otimes_1}, \mathrm{M}_{\mathrm{r}_1}, \mathrm{M}_{13}, \mathrm{M}_{\otimes_2}, \mathrm{M}_{\mathrm{r}_2}) \text{ or } (\tilde{\mathrm{M}}_2, \tilde{\mathrm{M}}_{\otimes_1}, \tilde{\mathrm{M}}_{\mathrm{r}_1}) \neq (\mathrm{M}_2, \mathrm{M}_{\otimes_1}, \mathrm{M}_{\mathrm{r}_1})\Big]. \quad (13)$$

We then observe that $\tilde{P}_e(\mathcal{C}_n) \geq P_e(\mathcal{C}_n)$, cf. (2). Using the standard analysis of random coding, we can prove that for a sufficiently large n, with high probability $\tilde{P}_e(\mathcal{C}_n) \leq \epsilon_n$ if

$$\begin{aligned} R_2 + R_{\otimes_1} + R_{r_1} &\leq \mathbb{I}(\mathrm{U};\mathrm{Y}_2) - \delta_n(\epsilon_n) \\ R_{13} + R_{\otimes_2} + R_{r_2} &\leq \mathbb{I}(\mathrm{X};\mathrm{Y}_1|\mathrm{U}) - \delta_n(\epsilon_n). \end{aligned} \quad (14)$$

7. Secrecy Analysis: Based on different the strong secrecy approaches cf. [14, 15], for a sufficiently large n, the individual leakage of M_2 to the eavesdropper is with high probability smaller than τ_n if

$$R_{\otimes_1} + R_{r_1} \geq \mathbb{I}(\mathrm{U};\mathrm{Z}) + \delta_n(\tau_n). \quad (15)$$

On the other hand, because of the new structure of $\mathcal{M}_1$, M_1 can be defined as a random variable that combines the three independent random variables M_{11}, M_{12} and M_{13}. Thus, the leakage of M_1 to the eavesdropper becomes

$$\begin{aligned} \mathbb{I}(\mathrm{M}_1;\mathrm{Z}^n) &= \mathbb{I}(\mathrm{M}_{13};\mathrm{Z}^n) + \mathbb{I}(\mathrm{M}_{12};\mathrm{Z}^n|\mathrm{M}_{13}) \\ &\quad + \mathbb{I}(\mathrm{M}_{11};\mathrm{Z}^n|\mathrm{M}_{13}\mathrm{M}_{12}). \end{aligned} \quad (16)$$

Based on Shannon's cipher system, one can prove that the second and the third terms in (16) vanish as follows:

$$\begin{aligned} \mathbb{I}(\mathrm{M}_{12};\mathrm{Z}^n|\mathrm{M}_{13}) &= \mathbb{H}(\mathrm{M}_{12}|\mathrm{M}_{13}) - \mathbb{H}(\mathrm{M}_{12}|\mathrm{Z}^n\mathrm{M}_{13}) \\ &\overset{(a)}{=} \mathbb{H}(\mathrm{M}_{12}) - \mathbb{H}(\mathrm{M}_{12}|\mathrm{Z}^n\mathrm{M}_{13}) \\ &\overset{(b)}{\leq} \mathbb{H}(\mathrm{M}_{12}) - \mathbb{H}(\mathrm{M}_{12}|\mathrm{M}_{13}\mathrm{M}_{\otimes_1}\mathrm{M}_{\otimes_2}\mathrm{M}_{r_1}\mathrm{M}_{r_2}) \\ &\overset{(c)}{=} \mathbb{H}(\mathrm{M}_{12}) - \mathbb{H}(\mathrm{M}_{12}|\mathrm{M}_{\otimes_2}) \overset{(d)}{=} 0 \end{aligned} \quad (17)$$

where (a) follows because M_{12} and M_{13} are independent; (b) follows because the best the eavesdropper can extract from Z^n is all the transmitted message except M_2, which is protected by the condition in (15) ; (c) follows because $\mathrm{M}_{\otimes_2}$ is the only message that is related to M_{12} and (d) follows because of the Shannon's cipher system where the entropy of the secret key M_{21} is equivalent to the entropy of the transmitted message M_{12}. Similarly, $\mathbb{I}(\mathrm{M}_{11};\mathrm{Z}^n|\mathrm{M}_{13}\mathrm{M}_{12}) = 0$. On the other hand, the first term in (16) is with high probability smaller than τ_n for a sufficiently large n, if

$$R_{\otimes_2} + R_{r_2} \geq \mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}) + \delta_n(\tau_n). \quad (18)$$

Thus the whole expression in (16) is with high probability smaller than τ_n. Now, if we apply the Fourier-Motzkin elimination to the rate constraints given in (14), (15) and (18), we have

$$\begin{aligned} R_2 &\leq \mathbb{I}(\mathrm{U};\mathrm{Y}_2) - \mathbb{I}(\mathrm{U};\mathrm{Z}) - \delta_n(\epsilon_n, \tau_n) \\ R_{13} &\leq \mathbb{I}(\mathrm{X};\mathrm{Y}_1|\mathrm{U}) - \mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}) - \delta_n(\epsilon_n, \tau_n). \end{aligned} \quad (19)$$

Now keeping in mind that R_1 is the summation of R_{11}, R_{12} and R_{13}, we can use Eqs. (12), (15) and (18) which give some bounds on the rates R_{11} and R_{12} in addition to Eq. (19) to bound R_1. If we do so, then take the limit as $n \to \infty$, which implies that $\delta_n(\epsilon_n, \tau_n) \to 0$, we prove the achievability of any rate pair (R_1, R_2) satisfying (11).

Now for the converse, we start by R_2 and observe that the joint secrecy bound for R_k at $k = 2$ in (8) holds for the individual secrecy as well. Thus, we focus on R_1 and let $\mathrm{U}_i \triangleq (\mathrm{M}_2, \mathrm{Y}_1^{i-1}, \tilde{\mathrm{Z}}^{i+1})$, we have

$$\begin{aligned} R_1 &\overset{(a)}{\leq} \frac{1}{n}\Big[\mathbb{I}(\mathrm{M}_1;\mathrm{Y}_1^n) - \mathbb{I}(\mathrm{M}_1;\mathrm{Z}^n)\Big] + \gamma_1(\epsilon_n, \tau_n) \\ &\overset{(b)}{\leq} \frac{1}{n}\Big[\mathbb{I}(\mathrm{M}_1;\mathrm{Y}_1^n|\mathrm{M}_2) - \mathbb{I}(\mathrm{M}_1;\mathrm{Z}^n|\mathrm{M}_2) + \mathbb{I}(\mathrm{M}_2;\mathrm{Z}^n|\mathrm{M}_1)\Big] \\ &\quad + \gamma_1(\epsilon_n, \tau_n) \\ &\overset{(c)}{\leq} \frac{1}{n}\Big[\mathbb{I}(\mathrm{M}_1;\mathrm{Y}_1^n|\mathrm{M}_2) - \mathbb{I}(\mathrm{M}_1;\mathrm{Z}^n|\mathrm{M}_2)\Big] + R_2 + \gamma_1(\epsilon_n, \tau_n) \\ &\overset{(d)}{\leq} \frac{1}{n}\sum_{i=1}^{n}\Big[\mathbb{I}(\mathrm{X}_i;\mathrm{Y}_{1i}|\mathrm{U}_i) - \mathbb{I}(\mathrm{X}_i;\mathrm{Z}_i|\mathrm{U}_i)\Big] + R_2 \\ &\quad + \gamma_1(\epsilon_n, \tau_n) \end{aligned} \quad (20)$$

where (a) follows from (4) and (6); (b) follows because $\mathbb{I}(\mathrm{M}_1;\mathrm{Z}^n) \geq \mathbb{I}(\mathrm{M}_1;\mathrm{Z}^n|\mathrm{M}_2) - \mathbb{I}(\mathrm{M}_2;\mathrm{Z}^n|\mathrm{M}_1)$; (c) follows because $nR_2 \geq \mathbb{I}(\mathrm{M}_2;\mathrm{Z}^n|\mathrm{M}_1)$; while (d) follows as in (9). The second bound on R_1 can be derived as follows:

$$\begin{aligned} R_1 &\overset{(a)}{\leq} \frac{1}{n}\Big[\mathbb{I}(\mathrm{M}_1;\mathrm{Y}_1^n|\mathrm{M}_2) + \mathbb{I}(\mathrm{M}_2;\mathrm{Z}^n)\Big] + \tilde{\gamma}_1(\epsilon_n) \\ &\leq \frac{1}{n}\sum_{i=1}^{n}\Big[\mathbb{I}(\mathrm{M}_1;\mathrm{Y}_{1i}|\mathrm{M}_2\mathrm{Y}_1^{i-1}\tilde{\mathrm{Z}}^{i+1}) + \mathbb{I}(\mathrm{M}_2;\mathrm{Z}_i|\tilde{\mathrm{Z}}^{i+1}) \\ &\quad + \mathbb{I}(\tilde{\mathrm{Z}}^{i+1};\mathrm{Y}_{1i}|\mathrm{M}_2\mathrm{Y}_1^{i-1})\Big] + \tilde{\gamma}_1(\epsilon_n) \\ &\overset{(b)}{=} \frac{1}{n}\sum_{i=1}^{n}\Big[\mathbb{I}(\mathrm{M}_1;\mathrm{Y}_{1i}|\mathrm{U}_i) + \mathbb{I}(\mathrm{M}_2\mathrm{Y}_1^{i-1};\mathrm{Z}_i|\tilde{\mathrm{Z}}^{i+1})\Big] \\ &\quad + \tilde{\gamma}_1(\epsilon_n) \\ &\leq \frac{1}{n}\sum_{i=1}^{n}\Big[\mathbb{I}(\mathrm{X}_i;\mathrm{Y}_{1i}|\mathrm{U}_i) + \mathbb{I}(\mathrm{U}_i;\mathrm{Z}_i)\Big] + \tilde{\gamma}_1(\epsilon_n) \end{aligned} \quad (21)$$

where (a) follows from (6); while (b) follows from the Csiszár sum identity [4, Lemma 7]. If we introduce an independent and uniformly distributed time sharing sequence to (8), (20) and (21), then take the limit as $n \to \infty$, such that $\gamma_1(\epsilon_n, \tau_n)$, $\gamma_2(\epsilon_n, \tau_n)$ and $\tilde{\gamma}_1(\epsilon_n) \to 0$; our converse is complete. ■

Theorem 3. *The individual secrecy capacity region of the degraded multi-receiver wiretap BC is given by the union of all rate tuples $(R_1, \ldots, R_k) \in \mathbb{R}_+^k$ that satisfy*

$$R_j \leq \mathbb{I}(\mathrm{U}_j;\mathrm{Y}_j|\mathrm{U}_{j+1}) - \mathbb{I}(\mathrm{U}_j;\mathrm{Z}|\mathrm{U}_{j+1}) + \sum_{l=j+1}^{k} R_l \quad (22a)$$

$$R_j \leq \mathbb{I}(\mathrm{U}_j;\mathrm{Y}_j|\mathrm{U}_{j+1}) + \mathbb{I}(\mathrm{U}_{j+1};\mathrm{Z}) \tag{22b}$$

$$\sum_{l=j}^{k} R_l \leq \sum_{l=j}^{k} \mathbb{I}(\mathrm{U}_l;\mathrm{Y}_l|\mathrm{U}_{l+1}) \tag{22c}$$

where $\mathrm{U}_1 = \mathrm{X}$, $\mathrm{U}_{k+1} = \emptyset$ *and the union runs over all random variables* $(\mathrm{U}_k, \ldots, \mathrm{U}_2, \mathrm{X})$ *such that,* $\mathrm{U}_k - \cdots - \mathrm{U}_2 - \mathrm{X} - \mathrm{Y}_1 - \mathrm{Y}_2 - \cdots - \mathrm{Y}_k - \mathrm{Z}$ *forms a Markov chain.*

At first, we need to point out the interpretation of each bound. The first bound (22a) implies that the achievable secrecy rate of each receiver is less than the summation of the random coded part in its layer and the rates of all receivers degraded from it, which can be used as secret keys. The second bound (22b) assures that the rate of any receiver can not exceed the summation of the information in its layer and all the randomization indexes of the lower layers. The last bound (22c) is only needed for $k \geq 3$, to assure that if any randomization index is used to carry information for a certain user, it can not be used by another one.

Proof: The achievability follows by extending the coding techniques in Theorem 2, where each messages is divided into $k+1$ independent parts and the messages of the weak receivers are used as secret keys for the stronger ones. For the converse, we start by letting $\mathrm{U}_j^i \triangleq (\mathrm{M}_j, \mathrm{Y}_{j-1}^{i-1}, \tilde{\mathrm{Z}}^{i+1}, \mathrm{U}_{j+1}^i)$ and observe that under the individual secrecy Eq. (8) still holds. We then adapt Eq. (9) to the individual secrecy requirement as in (20).

$$\begin{aligned}
R_j &\leq \frac{1}{n}\Big[\mathbb{I}(\mathrm{M}_j;\mathrm{Y}_j^n) - \mathbb{I}(\mathrm{M}_j;\mathrm{Z}^n)\Big] + \gamma_j(\epsilon_n,\tau_n) \\
&\leq \frac{1}{n}\Big[\mathbb{I}(\mathrm{M}_j;\mathrm{Y}_j^n|\mathrm{M}_{j+1}\ldots\mathrm{M}_k) - \mathbb{I}(\mathrm{M}_j;\mathrm{Z}^n|\mathrm{M}_{j+1}\ldots\mathrm{M}_k) \\
&\qquad + \mathbb{I}(\mathrm{M}_{j+1}\ldots\mathrm{M}_k;\mathrm{Z}^n|\mathrm{M}_j)\Big] + \gamma_j(\epsilon_n,\tau_n) \\
&\leq \frac{1}{n}\Big[\mathbb{I}(\mathrm{M}_j;\mathrm{Y}_j^n|\mathrm{M}_{j+1}\ldots\mathrm{M}_k) - \mathbb{I}(\mathrm{M}_j;\mathrm{Z}^n|\mathrm{M}_{j+1}\ldots\mathrm{M}_k)\Big] \\
&\qquad + \sum_{l=j+1}^{k} R_l + \gamma_j(\epsilon_n,\tau_n) \\
&\leq \frac{1}{n}\sum_{i=1}^{n}\Big[\mathbb{I}(\mathrm{U}_j^i;\mathrm{Y}_{j,i}|\mathrm{U}_{j+1}^i) - \mathbb{I}(\mathrm{U}_j^i;\mathrm{Z}_i|\mathrm{U}_{j+1}^i)\Big] + \sum_{l=j+1}^{k} R_l \\
&\qquad + \gamma_j(\epsilon_n,\tau_n).
\end{aligned} \tag{23}$$

One the other hand, the bound in (22b) follows easily using the same steps in (21), while the sum rate bound (22c) can be derived as follows:

$$\begin{aligned}
\sum_{l=j}^{k} R_l &\overset{(a)}{\leq} \frac{1}{n}\Bigg[\sum_{l=j+1}^{k}\Big[\mathbb{I}(\mathrm{M}_l;\mathrm{Y}_l^n|\mathrm{M}_{l+1}\ldots\mathrm{M}_k) \\
&\qquad - \mathbb{I}(\mathrm{M}_l;\mathrm{Z}^n|\mathrm{M}_{l+1}\ldots\mathrm{M}_k)\Big] + \mathbb{I}(\mathrm{M}_{j+1}\ldots\mathrm{M}_k;\mathrm{Z}^n) \\
&\qquad + \mathbb{I}(\mathrm{M}_j;\mathrm{Y}_j^n|\mathrm{M}_{j+1}\ldots\mathrm{M}_k)\Bigg] + \sum_{l=j}^{k}\tilde{\gamma}_l(\epsilon_n) \\
&\overset{(b)}{=} \frac{1}{n}\sum_{i=1}^{n}\Bigg[\sum_{l=j+1}^{k}\Big[\mathbb{I}(\mathrm{U}_l^i;\mathrm{Y}_{li}|\mathrm{U}_{l+1}^i) - \mathbb{I}(\mathrm{U}_l^i;\mathrm{Z}_i|\mathrm{U}_{l+1}^i)\Big] \\
&\qquad + \mathbb{I}(\mathrm{U}_j^i;\mathrm{Y}_{ji}|\mathrm{U}_{j+1}^i) + \mathbb{I}(\mathrm{U}_{j+1}^i;\mathrm{Z}_i)\Bigg] + \sum_{l=j}^{k}\tilde{\gamma}_l(\epsilon_n) \\
&\overset{(c)}{=} \frac{1}{n}\sum_{i=1}^{n}\sum_{l=j}^{k}\mathbb{I}(\mathrm{U}_l^i;\mathrm{Y}_{li}|\mathrm{U}_{l+1}^i) + \sum_{l=j}^{k}\tilde{\gamma}_l(\epsilon_n)
\end{aligned} \tag{24}$$

where $\tilde{\gamma}_l(\epsilon_n) = 1/n + \epsilon_n R_l$. (a) follows by applying Fano's inequality to (5) and the fact that $\mathbb{I}(\mathrm{M}_{j+1}\ldots\mathrm{M}_k;\mathrm{Z}^n) = \sum_{l=j+1}^{k}\mathbb{I}(\mathrm{M}_l;\mathrm{Z}^n|\mathrm{M}_{l+1}\ldots\mathrm{M}_k)$; (b) follows as in (9) and (21); while (c) follows because $\sum_{l=j+1}^{k}\mathbb{I}(\mathrm{U}_l^i;\mathrm{Z}_i|\mathrm{U}_{l+1}^i) = \mathbb{I}(\mathrm{U}_{j+1}^i;\mathrm{Z}_i)$. Now, if we introduce an independent and uniformly distributed randomization index to the bounds in (23) and (24) in addition to extending the reliability constraint in (21) to all k receivers, then take the limit as $n \to \infty$ such that $\gamma_j(\epsilon_n,\tau_n)$ and $\tilde{\gamma}_j(\epsilon_n) \to 0$; our converse is complete. ■

C. Eavesdropper Degradedness Order

Proposition 3.4 in [12] states that the joint secrecy capacity vanishes if the legitimate receivers is degraded from the eavesdropper. This implies that investigating the effect of the degradedness order of the eavesdropper on the joint secrecy capacity is not necessary. On the other hand, in [11, Lemma 2], it was shown that for the degraded wiretap BC with receiver side information, the optimum coding technique for the individual secrecy criterion depends on the degradedness order of the eavesdropper. This raises a question about the validity of the individual secrecy capacity region in (11), if the degradedness order of the eavesdropper is changed. In order to answer this question, we need to consider the following scenarios:

1. $\mathrm{X} - \mathrm{Z} - \mathrm{Y}_1 - \mathrm{Y}_2$**:** Under this Markov chain, for any distribution on (U, X), we have $\mathbb{I}(\mathrm{U};\mathrm{Y}_2) \leq \mathbb{I}(\mathrm{U};\mathrm{Z})$ and $\mathbb{I}(\mathrm{X};\mathrm{Y}_1|\mathrm{U}) \leq \mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U})$. This implies that the individual achievable region in (11) simplifies to $R_1 = R_2 = 0$. In order to proof that these rates are the actual capacity, we refer to [10, Proposition 1], which implies that for the given Markov chain $\mathbb{I}(\mathrm{M}_2;\mathrm{Y}_2^n) \leq \mathbb{I}(\mathrm{M}_2;\mathrm{Z}^n)$ and $\mathbb{I}(\mathrm{M}_1;\mathrm{Y}_1^n) \leq \mathbb{I}(\mathrm{M}_1;\mathrm{Z}^n)$. Using these two inequalities in (20) and (8) completes the converse.

2. $\mathrm{X} - \mathrm{Y}_1 - \mathrm{Z} - \mathrm{Y}_2$**:** For this Markov chain, we have $\mathbb{I}(\mathrm{U};\mathrm{Y}_2) \leq \mathbb{I}(\mathrm{U};\mathrm{Z})$. Thus the individual achievable region in (11) simplifies to $R_2 = 0$ and $R_1 \leq \mathbb{I}(\mathrm{X};\mathrm{Y}_1|\mathrm{U}) - \mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U})$. The converse for the bound of R_2 follows as in the previous case because $\mathbb{I}(\mathrm{M}_2;\mathrm{Y}_2^n) \leq \mathbb{I}(\mathrm{M}_2;\mathrm{Z}^n)$, while the converse for bound of R_1 follows as in (20) when $R_2 = 0$.

IV. Gaussian Multi-Receiver Wiretap BC

In this section we will extend our results to Gaussian channels. We will restrict our attention to the two users scenario for simplicity. We define the Gaussian scalar two-receiver wiretap channel as:

$$\begin{aligned}
\mathrm{Y}_j &= \mathrm{X} + \mathrm{N}_j, \qquad j = 1,2 \\
\mathrm{Z} &= \mathrm{X} + \mathrm{N}_Z
\end{aligned} \tag{25}$$

The channel input X is subject to a power constraint $\mathbb{E}[\mathrm{X}^2] \leq P$. N_1, N_2, N_Z are zero-mean Gaussian random variables, whose variances are given by σ_1^2, σ_2^2, σ_Z^2 respectively.

The Gaussian scalar wiretap channel belongs to the class of degraded wiretap BCs, where the variance (power) of the Gaussian noises N_1, N_2 and N_Z defines the degradedness order of the channel. For example, if $\sigma_1^2 \leq \sigma_Z^2 \leq \sigma_2^2$, then

$\mathrm{X} - \mathrm{Y}_1 - \mathrm{Z} - \mathrm{Y}_2$ forms a Markov chain. Since we already showed that the capacity regions in (10) and (11) establishes the joint and individual secrecy capacity of any degraded wiretap BC regardless of the degradedness order of the eavesdropper, we can use Corollary 1 and Theorem 2 to derive the joint and individual secrecy capacity regions for the Gaussian case.

To compute the secrecy capacity region explicitly, we need to find the optimal joint distributions of (U, X) in (10) and (11). In [8], Ekrem and Ulukus computed the joint secrecy capacity of the Gaussian scalar two-receiver wiretap channel, showing that the optimal choice is a jointly Gaussian distribution on (U, X). They showed the optimality of this choice using two converse techniques along with the properties of differential entropy. The first technique is based on the MMSE, while the second one depends on the Fisher information. That is why, we will only focus on extending the individual secrecy result in Theorem 2 to Gaussian channels.

Theorem 4. *The individual secrecy capacity region of the two-receiver Gaussian wiretap BC is given by the union of all rate pairs $(R_1, R_2) \in \mathbb{R}_+^2$ that satisfy*

$$\begin{aligned} R_2 &\leq f\left(1 + \frac{\bar{\alpha}P}{\alpha P + \sigma_2^2}\right) - f\left(1 + \frac{\bar{\alpha}P}{\alpha P + \sigma_Z^2}\right) \\ R_1 &\leq f\left(1 + \frac{\alpha P}{\sigma_1^2}\right) + f\left(1 + \frac{\bar{\alpha}P}{\alpha P + \sigma_Z^2}\right) \\ R_1 &\leq f\left(1 + \frac{\alpha P}{\sigma_1^2}\right) - f\left(1 + \frac{\alpha P}{\sigma_Z^2}\right) + R_2 \end{aligned} \tag{26}$$

where $f(x) = \frac{1}{2}\log(x)$ and the union is taken over all values of $\alpha \in [0, 1]$, such that $\bar{\alpha} = 1 - \alpha$.

Proof: The achievability follows by selecting (U, X) to be jointly Gaussian in Theorem 2, where X can be viewed as the summation of two independent zero-mean Gaussian random variables U and V, with respective variances $\bar{\alpha}P$ and αP. This implies that the total input power P is distributed among the two users, such that $\bar{\alpha}P$ is dedicated for Y_2, while the rest is dedicated for Y_1. On the other hand, the converse follows by adapting the techniques used in [7] to the individual secrecy constraint, keeping in mind that the second bound is just a reliability bound. ∎

In order to visualize the difference between the individual secrecy capacity region for Gaussian channels given by (26) and the joint secrecy capacity region for Gaussian channel given in [7, Theorem 5], we calculate the secrecy rates R_1 and R_2 at different values of α. The parameters used in this calculation were as follows: $P = 1$, $\sigma_1^2 = 0.05$, $\sigma_2^2 = 0.1$ and $\sigma_Z^2 = 0.15$. The results plotted in Figure 1 agree with the fact that the individual secrecy capacity region is larger than the joint one.

V. Conclusion

We studied secure broadcasting over a degraded multi-receiver wiretap BC with respect to two secrecy criteria: joint secrecy and individual secrecy. For both criteria, we established the secrecy capacity for arbitrary number of receivers showing that the individual secrecy has a bigger capacity region. This increase arises from using the messages of the weak receivers as secret keys for the stronger ones. Further, we extended our results to Gaussian channels.

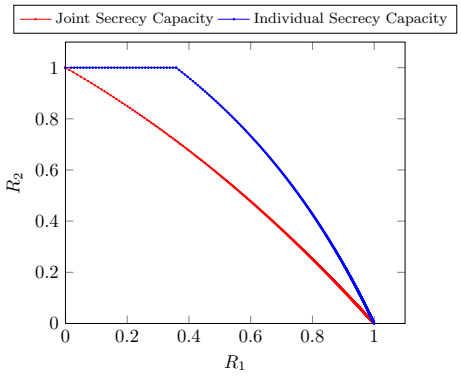

Fig. 1. Joint and Individual secrecy capacity regions of a Gaussian BC.

VI. Acknowledgment

This work of R. F. Schaefer was supported by the German Research Foundation (DFG) under Grant WY 151/2-1.

References

[1] C. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, Oct. 1949.

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

[3] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul 1978.

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

[5] W. Kang and N. Liu, "Wiretap channel with shared key," in *IEEE Inf. Theory Workshop*, Dublin, Ireland, Sep. 2010, pp. 1–5.

[6] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "Secrecy rate region of the broadcast channel with an eavesdropper," in *Forty-Sixth Annual Allerton Conference*, Sep. 2009, pp. 834–841.

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

[8] ——, "The secrecy capacity region of the gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2083–2114, 2011.

[9] E. Tekin and A. Yener, "The gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5747–5755, Dec. 2008.

[10] A. S. Mansour, R. F. Schaefer, and H. Boche, "Secrecy measures for broadcast channels with receiver side information: Joint vs individual," in *IEEE Inf. Theory Workshop*, Hobart, Tasmania, Australia, November 2014, pp. 426–430.

[11] ——, "Joint and individual secrecy in broadcast channels with receiver side information," in *Signal Processing Advances in Wireless Communications (SPAWC), 2014 IEEE 15th International Workshop*, Toronto, Canada, June 2014, pp. 369 – 373.

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

[13] A. El Gamal and Y.-H. Kim, *Network Information Theory*. New York, NY, USA: Cambridge University Press, 2012.

[14] J. Hou and G. Kramer, "Effective secrecy: Reliability, confusion and stealth," in *Information Theory (ISIT), 2014 IEEE International Symposium on*, Honolulu, HI, USA, June 2014, pp. 601–605.

[15] M. R. Bloch and J. N. Laneman, "Strong secrecy from channel resolvability," *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 8077–8098, Dec. 2013.