This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2016.2566260, IEEE Transactions on Information Forensics and Security



# On the Individual Secrecy Capacity Regions of the General, Degraded and Gaussian Multi-Receiver Wiretap Broadcast Channel

Ahmed S. Mansour, *Student Member, IEEE*, Rafael F. Schaefer, *Member, IEEE*, and Holger Boche, *Fellow, IEEE*

***Abstract*—In this paper, secure communication over a broadcast channel with multiple legitimate receivers and an external eavesdropper is investigated. Two different secrecy measures are considered: The first criterion is a conservative one known as joint secrecy, where the mutual leakage of all confidential messages must be small. The second criterion is a less conservative constraint known as individual secrecy, where the individual leakage of each confidential message must be small. At first, we consider the degraded multi-receiver wiretap broadcast channel and manage to establish the individual secrecy capacity region. Our encoding scheme applies a careful combination of the standard techniques of wiretap random coding and Shannon's one time pad encoding, where the confidential messages of the weak receivers are used as secret keys for the stronger ones. The validity of this technique is due to the properties of the degraded broadcast channel and the secrecy requirements of the individual secrecy criterion. Our result indicates that, the individual secrecy capacity region is in fact larger than the joint one established in earlier literature. The established capacity region is then used to derive the individual secrecy capacity regions of the Gaussian SISO and degraded Gaussian MIMO multi-receiver wiretap broadcast channels. Furthermore, we present an achievable rate region for the general two-receiver wiretap broadcast channel under both the joint and the individual secrecy criterion. Comparing these two rate regions suggests that even for the general case, the individual secrecy criterion might be able to provide a larger rate region compared to the joint one.**

***Index Terms*—multi-receiver wiretap channel, joint secrecy, individual secrecy, degraded broadcast channel, secrecy capacity region, Gaussian SISO, degraded Gaussian MIMO.**

## I. Introduction

Nowadays wireless systems are required to provide both reliable and secure communication. However, due to the open nature of the wireless medium, transmitted signals are not only received by legitimate receivers but eavesdroppers as well. In order to overcome this problem and guarantee a secure information transmission, different secrecy techniques are used either on the physical layer or on higher layers. Recently, physical layer security also known as *information theoretic security* has become increasingly attractive because it does not impose any assumptions on the computational power of the eavesdroppers. Information theoretic security was first introduced by Shannon in [3], where he showed that secure communication between the transmitter and the receiver can be achieved using a shared secret key, whose entropy must be greater than or equal to the entropy of the message to be transmitted, as a one-time pad. In [4], Wyner showed that secure communication is still achievable in the absence of a secret key by exploiting the noisiness of the channel. He considered a secure communication scenario, in which the eavesdropper receives a degraded version of the legitimate receiver's observation. He named this setup the degraded wiretap channel and managed to establish its secrecy capacity. In [5] Wyner's result was extended to the Gaussian scalar wiretap channel, while in [6], it was extended to the general –not necessarily degraded– wiretap channel. In [7], secure communication over a wiretap channel in the presence of a shared secret key was investigated. The authors established the secrecy capacity region by combining Wyner's wiretap coding technique along with Shannon's one time pad principle. Due to the rapid growth in the area of networks security, the problem of secure communication over wiretap channels has become of high significance, see for example recent textbooks [8–10], where the last one in particular highlights the main results and various unsolved issues.

Recently, the problem of secure communication over a wiretap broadcast channel (BC) with more than one legitimate receiver has captured a lot of attention. In spite of the tremendous efforts, the secrecy capacity region of the general multi-receiver wiretap BC is still unknown. It is worth mentioning that even the capacity region of the general BC without any secrecy constraints is still an open problem. Nevertheless, researchers managed to establish the secrecy capacity of some special cases. One of the main special cases that has been investigated by many researchers is the degraded multi-receiver wiretap BC. The class of degraded BCs is very important in particular for wireless communication, because the Gaussian single-input single-output (SISO) BC is inherently degraded. Also since the class of degraded BC contains the degraded Gaussian multiple-input multiple-output (MIMO) BC as well. In [11], the degraded two-receiver wiretap BC was investigated, where the authors succeeded in establishing the



This work was presented in part at IEEE-ICC, London, United Kingdom, June 2015 [1] and at IEEE-SPAWC, Stockholm, Sweden, July 2015 [2].

Ahmed S. Mansour and Holger Boche are with the Lehrstuhl für Theoretische Informationstechnik, Technische Universität München, 80290 München, Germany (e-mail:ahmed.mansour@tum.de; boche@tum.de). Rafael F. Schaefer is with the Information Theory and Applications Group, Technische Universität Berlin, 10587 Berlin, Germany (email: rafael.schaefer@tu-berlin.de).

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

secrecy capacity region. This result played an important role in establishing the secrecy capacity region for the Gaussian SISO two-receiver wiretap BC in [12] and the degraded Gaussian MIMO two-receiver wiretap BC in [13]. In [14], Ekrem and Ulukus extended the secrecy capacity region in [11] to the degraded wiretap BC with an arbitrary number of receivers. Finally, in [12], the secrecy capacity regions for both Gaussian SISO and Gaussian MIMO –not necessarily degraded– multi-receiver wiretap BCs were established. However, all these works only considered the so-called *joint secrecy* criterion.

The *joint secrecy* criterion is a very conservative secrecy constraint, in which each legitimate receiver makes sure that its confidential message is protected even if the confidential messages of the other legitimate receivers are compromised. This implies that the legitimate receivers do not trust each other. Differently from the joint secrecy criterion, we will consider a less conservative secrecy criterion known as *individual secrecy*. This criterion is based on the mutual trust among the legitimate receivers, such that they can cooperate together to protect their confidential messages against eavesdropping. The effect of relaxing the secrecy constraint –from the joint secrecy criterion to the individual one– on the secrecy capacity region was previously investigated for the wiretap BC with receiver side information in [15–18] and with some slight differences for the wiretap multiple access channel in [19]. In particular, it was shown in [18] that the individual secrecy capacity region for some classes of the wiretap BC with receiver side information is larger than the joint secrecy one. This increase in the capacity region arises from the fact that under the individual secrecy criterion the confidential message of one receiver, which is available as side information at the other receiver, can be considered as a secret key shared between the transmitter and the receiver. Thus, instead of only using wiretap random coding as in the joint secrecy case, the individual secrecy approach combines the two encoding techniques: wiretap random coding and secret key encoding, which consequently leads to a larger capacity region.

In this paper we will study the multi-receiver wiretap BC under the *individual secrecy* criterion. During our investigation, we will compare the newly established individual secrecy capacity regions versus the joint secrecy ones established in previous literature. It is important to note that, the capability of the individual secrecy to provide a larger secrecy capacity region for wiretap BC with receiver side information relies on the usage of the available side information to impose secret key encoding. This means that, it is not obvious whether individual secrecy can provide a larger capacity region in the absence of this side information as in the general multi-receiver wiretap BC or not. However, we will show that even in the absence of the receiver side information, individual secrecy is still capable of providing a larger capacity region. In a parallel and independent work [20, 21], individual secrecy for two-user wiretap BC were investigated, where different achievable rate regions are established and compared to the corresponding joint secrecy regions.

The rest of this paper is organized as follows: In Section II, we describe the model of the general multi-receiver wiretap channel and discuss in detail the differences between the joint and the individual secrecy criteria, by comparing their secrecy capacity regions for some special cases. In Section III, we establish the individual secrecy capacity region of the class of degraded multi-receiver wiretap BC. The results presented in this section are related to our conference paper [1]. We then use the established capacity region to derive the individual secrecy capacity regions of the Gaussian SISO and degraded Gaussian MIMO multi-receiver wiretap BC in Section IV and Section V respectively. These two sections contain the same results established in [2] and are presented here for the sake of completeness. Finally, in Section VI, we derive an achievable rate region for the general two-receiver wiretap BC under both the joint and the individual secrecy criteria, using the principle of Marton coding with superposition variable.

### *Notation*

In this paper, random variables are denoted by capital letters and their realizations by the corresponding lower case letters, while calligraphic letters are used to denote sets. $\mathrm{X}^n$ denotes the sequence of variables $(\mathrm{X}_1, \ldots, \mathrm{X}_n)$, where $\mathrm{X}_i$ is the $i^{th}$ variable in the sequence. Additionally, we use $\tilde{\mathrm{X}}^i$ to denote the sequence $(\mathrm{X}_i, \ldots, \mathrm{X}_n)$. A probability distribution for the random variable X is denoted by $Q(x)$. $\mathrm{U} - \mathrm{V} - \mathrm{X}$ denotes a Markov chain of the random variables U, V and X in this order. Bold letters are used to denote matrices, where $\mathbf{A} \succ \mathbf{0}$ indicates that $\mathbf{A}$ is a positive definite matrix and $\mathbf{A} \succeq \mathbf{0}$ implies that $\mathbf{A}$ is a positive semi-definite matrix. $\mathbb{R}_+$ is used to denote the set of nonnegative real numbers. $\mathbb{H}(\cdot)$ and $\mathbb{I}(\cdot;\cdot)$ are the traditional entropy and mutual information respectively, while $|\cdot|$ is used to denote the determinant of a matrix. The probability of an event is given by $\mathbb{P}[\cdot]$. Moreover, $[\![a; b]\!]$ is used to represent the set of natural numbers between $a$ and $b$. We further use $f(x)$ to indicate a scaled and shifted logarithmic function, such that $f(x) = \frac{1}{2}\log(1+x)$ also known as the capacity function.

## II. Secrecy in Multi-Receiver Wiretap BC

In this section, we will investigate the multi-receiver wiretap BC under two different secrecy constraints: Joint secrecy and individual secrecy. We compare these two criteria and show that the individual secrecy can provide a larger secrecy capacity region compared to the joint one.

### *A. System Model and Secrecy Criteria*

The multi-receiver wiretap BC consists of a transmitter with an input alphabet $\mathcal{X}$, $k$ legitimate receivers with output alphabets $\mathcal{Y}_j$, where $j \in [\![1; k]\!]$[1] and an external eavesdropper with output alphabet $\mathcal{Z}$. 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 $z^n$, such that the discrete memoryless multi-receiver wiretap BC is defined as:

$$Q^n(x^n, y_1^n, \ldots, y_k^n, z^n) = \prod_{i=1}^{n} Q(x_i, y_{1i}, \ldots, y_{ki}, z_i). \quad (1)$$

[1]Through the whole paper $j$ is taken to be in $[\![1; k]\!]$, unless stated otherwise.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2016.2566260, IEEE Transactions on Information Forensics and Security



We assume that the transmitter and all receivers have perfect channel knowledge and all our results are limited to this case. For a short discussion, please refer to the discussion in the last section.

**Definition 1.** *A $(2^{nR_1},\dots,2^{nR_k},n)$ 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 $\mathcal{R}$, a stochastic encoder at the transmitter*

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

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

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

*that maps each channel observation at the respective receiver to the corresponding required message or an error message $\{?\}$.*

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

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

where $\hat{\mathrm{M}}_j$ is the estimated message at the $j^{th}$ legitimate receiver. On the other hand, the secrecy performance of $\mathcal{C}_n$ is measured with respect to two different criteria as follows:

**1. Joint Secrecy:** This criterion requires the leakage of the confidential message of one user to the eavesdropper given the confidential messages of all other users to be small. For our model, this requirement can be expressed as follows:

$$\mathbb{I}(\mathrm{M}_j;\mathrm{Z}^n|\mathrm{M}_1\dots\mathrm{M}_{j-1}\mathrm{M}_{j+1}\dots\mathrm{M}_k)\leq\tau_{jn}\quad\text{where }\lim_{n\to\infty}\tau_{jn}=0.\tag{3}$$

This criterion guarantees that the information leaked to the eavesdropper from one user is small even if all the other confidential messages are compromised and known by the eavesdropper. This implies that this criterion does not account for the mutual trust between the legitimate receivers. In most literature, the joint secrecy criterion is defined such that, the mutual leakage of all confidential messages to the eavesdropper is small as follows:

$$\mathbb{I}(\mathrm{M}_1\dots\mathrm{M}_k;\mathrm{Z}^n)\leq\tau_n\quad\text{where}\quad\lim_{n\to\infty}\tau_n=0.\tag{4}$$

Although this definition is simpler than the one in (3), and it can be shown that both definitions are equivalent for some $\tau_n\geq\sum_{j=1}^k\tau_{jn}$ cf. [18], we prefer the one in (3). This is because it provides a better understanding to the interpretation of the relation between the legitimate receivers under the joint secrecy criterion. It also highlights the reason that makes the joint secrecy immune against compromised receivers.

**2. Individual Secrecy:** This criterion requires the leakage of the confidential message of each user to the eavesdropper to be small without conditioning on the confidential messages of the others users. This requirement can be formulated as follows:

$$\mathbb{I}(\mathrm{M}_j;\mathrm{Z}^n)\leq\tau_{jn}\tag{5}$$

and the $\tau_{jn}$ are defined as before. Differently from the conservative joint secrecy constraint in (3), the individual secrecy constraint takes the mutual trust between the legitimate receivers into consideration. This allows the legitimate receivers to cooperate in protecting their messages against eavesdropping. It is important to note that, for $\tau_n$ as defined before, the conditions in (5) can be combined into one condition:

$$\sum_{i=1}^k\mathbb{I}(\mathrm{M}_i;\mathrm{Z}^n)\leq\tau_n.\tag{6}$$

**Definition 2.** *A rate tuple $(R_1,\dots,R_k)\in\mathbb{R}_+^k$ is achievable for the multi-receiver wiretap BC, if there exists a sequence of $(2^{nR_1},\dots,2^{nR_k},n)$ codes $\mathcal{C}_n$, a sequence $\epsilon_n$ and $k$ sequences $\tau_{jn}$, where $n$ is large enough, such that:*

$$P_e(\mathcal{C}_n)\leq\epsilon_n,\quad\textit{and}\quad\lim_{n\to\infty}\epsilon_n,\tau_{jn}=0.\tag{7}$$

*Depending on the selected secrecy criterion, the conditions in* (3) *or* (5) *are fulfilled.*

**Remark 1.** *It is worth mentioning that the joint and individual secrecy constraints are defined according to the notation of strong secrecy criterion [22, 23], in which the total amount of information leaked to the eavesdropper should be small.*

### *B. Secrecy Capacity Regions: Joint Vs Individual*

In this subsection, we will highlight the differences between the joint and the individual secrecy criterion. To do so, we will compare the secrecy capacity regions of both criteria for the degraded two-receiver wiretap BC and the Gaussian two-receiver wiretap BC.

**Proposition 1.** *Consider a degraded two-receiver wiretap BC, i.e. $\mathrm{X}-\mathrm{Y}_1-\mathrm{Y}_2-\mathrm{Z}$ forms a Markov chain. Then the joint secrecy capacity region is given by the set of all rate pairs $(R_1,R_2)\in\mathbb{R}_+^2$, that satisfy*

$$R_2\leq\mathbb{I}(\mathrm{U};\mathrm{Y}_2)-\mathbb{I}(\mathrm{U};\mathrm{Z})\tag{8a}$$

$$R_1\leq\mathbb{I}(\mathrm{X};\mathrm{Y}_1|\mathrm{U})-\mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U})\tag{8b}$$

*where the union is taken over all random variables $(\mathrm{U},\mathrm{X})$, 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 region was first established in [11]. The achievability follows from the technique of random coding with product structure as in [6]. A detailed achievability proof for a more general case from which this result follows as a special case will be provided in Section VI-A. On the other hand, the converse follows using the standard techniques and procedures for degraded BC in [24], and will be provided for the multi-receiver case in Section III-A. The cardinality bound follows by the Fenchel-Bunt strengthening of the Carathéodory's theorem [25, Appendix C]. ■

**Proposition 2.** *Consider a degraded two-receiver wiretap BC as in the previous proposition. The individual secrecy capacity*

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2016.2566260, IEEE Transactions on Information Forensics and Security



*region is given by the set of all rate pairs* $(R_1, R_2) \in \mathbb{R}_+^2$ *that satisfy*

$$R_2 \leq \mathbb{I}(\mathrm{U};\mathrm{Y}_2) - \mathbb{I}(\mathrm{U};\mathrm{Z}) \tag{9a}$$
$$R_1 \leq \mathbb{I}(\mathrm{X};\mathrm{Y}_1|\mathrm{U}) + \mathbb{I}(\mathrm{U};\mathrm{Z}) \tag{9b}$$
$$R_1 \leq \mathbb{I}(\mathrm{X};\mathrm{Y}_1|\mathrm{U}) - \mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}) + R_2 \tag{9c}$$

*where the union is taken over all random variables* $(\mathrm{U}, \mathrm{X})$*, 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:* The achievability combines the techniques of wiretap random coding [6] along with Shannon's one time pad cipher system introduced in [3] as follows: Wiretap random coding is used to protect the message of the weaker receiver from eavesdropping, while the message of the stronger receiver is protected by a combination of wiretap random coding and Shannon's secret key encoding as in [7]. A detailed achievability proof for a more general case from which this result follows as a special case will be provided in Section VI-B. On the other hand, the converse follows by adapting the standard techniques and procedures for degraded BC in [24] to the individual secrecy constraint. The detailed steps of the converse for the multi-receiver case will be presented in Section III-A. ∎

**Proposition 3.** *Consider a Gaussian two-receiver wiretap BC, i.e.* $\mathrm{Y}_1 = \mathrm{X} + \mathrm{N}_1$*,* $\mathrm{Y}_2 = \mathrm{X} + \mathrm{N}_2$ *and* $\mathrm{Z} = \mathrm{X} + \mathrm{N}_Z$*, where the channel input* $\mathrm{X}$ *is under a power constraint such that,* $\mathbb{E}[\mathrm{X}^2] \leq P$ *and the variances of the Gaussian noises are of the following order* $\sigma_1^2 \leq \sigma_2^2 \leq \sigma_Z^2$*. The joint secrecy capacity is given by the union of all rate pairs* $(R_1, R_2) \in \mathbb{R}_+^2$ *that satisfy*

$$R_2 \leq f\left(\frac{\bar{\alpha}P}{\alpha P + \sigma_2^2}\right) - f\left(\frac{\bar{\alpha}P}{\alpha P + \sigma_Z^2}\right) \tag{10a}$$
$$R_1 \leq f\left(\frac{\alpha P}{\sigma_1^2}\right) - f\left(\frac{\alpha P}{\sigma_Z^2}\right) \tag{10b}$$

*where the union is taken over all values of* $\alpha \in [0, 1]$*, such that* $\bar{\alpha} = 1 - \alpha$*.*

*Proof:* This region was first established in [12]. The achievability follows by selecting $(\mathrm{U}, \mathrm{X})$ to be jointly Gaussian in Proposition 1, where $\mathrm{X} = \mathrm{U} + \mathrm{V}$ can be viewed as the summation of two independent zero-mean Gaussian random variables U and V, with respective variances $\bar{\alpha}P$ and $\alpha P$. On the other hand, the converse follows due to the optimality of Gaussian signaling. This optimality was proved in [12] by adapting the relation between the MMSE and the mutual information established in [26] and [27], to the situation with secrecy constraints. For further information regarding the properties and behaviors of the capacity achieving codes, please refer to [28]. ∎

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

$$R_2 \leq f\left(\frac{\bar{\alpha}P}{\alpha P + \sigma_2^2}\right) - f\left(\frac{\bar{\alpha}P}{\alpha P + \sigma_Z^2}\right) \tag{11a}$$
$$R_1 \leq f\left(\frac{\alpha P}{\sigma_1^2}\right) + f\left(\frac{\bar{\alpha}P}{\alpha P + \sigma_Z^2}\right) \tag{11b}$$
$$R_1 \leq f\left(\frac{\alpha P}{\sigma_1^2}\right) - f\left(\frac{\alpha P}{\sigma_Z^2}\right) + R_2 \tag{11c}$$

*where the union is taken over all values of* $\alpha \in [0, 1]$*, such that* $\bar{\alpha} = 1 - \alpha$*.*

*Proof:* The achievability follows by selecting $(\mathrm{U}, \mathrm{X})$ to be jointly Gaussian in Proposition 2, where the total power is divided among two Gaussian variables U and V as in the previous proposition. The weak receiver decodes his own message from the variable U while considering V as noise. On the other hand, the strong receiver can decode both messages and thus the message of the weak receiver can be used as a shared secret key between the transmitter and the strong receiver. Finally, the converse follows by adapting the techniques used in [12] to the individual secrecy constraint. A detailed proof for a more general case will be provided in Section IV. ∎

In order to visualize the difference between the joint and individual secrecy capacity region for Gaussian two-receiver wiretap BC given by (10) and (11) respectively, we calculate the secrecy rates $R_1$ and $R_2$ at different values of $\alpha$. In this calculation, we set the other parameters as follow: $P = 1$, $\sigma_1^2 = 0.05$, $\sigma_2^2 = 0.1$ and $\sigma_Z^2 = 0.15$. The normalized rates are plotted in Figure 1.

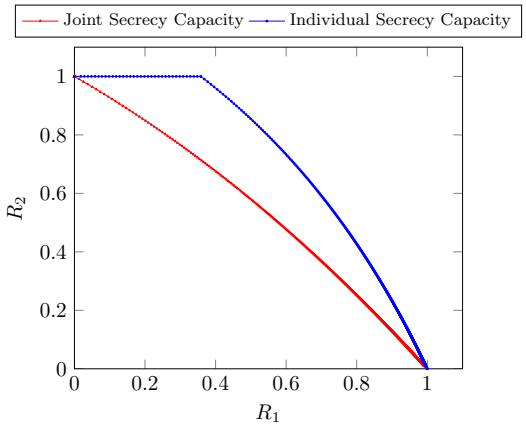


Fig. 1. Joint and Individual secrecy capacity regions of a Gaussian BC.

### C. Discussion

The previous results for the two-receiver wiretap BC are very helpful for understanding the differences between the joint and individual secrecy criteria. It also helps to capture the advantages and disadvantages of each criterion. This can be summarized in the following points:

1. Individual secrecy is a less conservative secrecy measure as compared to the joint one. This implies that, any code that fulfils the joint secrecy constraint should also satisfy

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2016.2566260, IEEE Transactions on Information Forensics and Security



the individual secrecy constraint as well. This is because the condition in (4) implies the one in (6), but not vise versa.

2. The individual secrecy criterion provides a larger capacity region as compared to the joint one. This result can be illustrated by comparing the rate constraint for $R_1$ in (10b) versus the ones in (11b) and (11c) as shown in Figure 1. This comparison shows that there is an increase in the rate $R_1$ accompanied with the individual secrecy criterion. The value of this increase is directly proportional with $R_2$, i.e. the size of the message of the weaker user used as secret key or the size of the total randomization index.

3. The joint secrecy criterion is a very conservative secrecy measure. Even if one of the confidential messages is revealed to the eavesdropper in a genie-aided way –because this receiver is compromised–, the other message is still protected which can be shown as follows:

$$\begin{aligned}\mathbb{I}(\mathrm{M}_1;\mathrm{Z}^n\mathrm{M}_2) &= \mathbb{I}(\mathrm{M}_1;\mathrm{M}_2)+\mathbb{I}(\mathrm{M}_1;\mathrm{Z}^n|\mathrm{M}_2)\\ &\overset{(a)}{=} \mathbb{I}(\mathrm{M}_1;\mathrm{Z}^n|\mathrm{M}_2)\leq \tau_n,\end{aligned} \tag{12}$$

where $(a)$ follows because $\mathrm{M}_1$ and $\mathrm{M}_2$ are independent. The previous equation shows that the leakage of $\mathrm{M}_1$ to the eavesdropper when $\mathrm{M}_2$ is revealed to it is still small.

4. On the other hand, the individual secrecy criterion is based on the mutual trust between the legitimate receivers. Thus, if one of the receivers is compromised such that, its full message or part of it is revealed to the eavesdropper, this might also affects the secrecy of the other one. In order to understand this property, imagine that in the previous example, $\mathrm{M}_2$ was revealed to the eavesdropper as follows:

$$\mathbb{I}(\mathrm{M}_1;\mathrm{Z}^n\mathrm{M}_2)=\mathbb{H}(\mathrm{M}_1)-\mathbb{H}(\mathrm{M}_1|\mathrm{Z}^n\mathrm{M}_2). \tag{13}$$

The term $\mathbb{H}(\mathrm{M}_1|\mathrm{Z}^n\mathrm{M}_2)$ is related to the amount of information about $\mathrm{M}_1$ that is still kept hidden from the eavesdropper $\mathrm{Z}^n$, when the message $\mathrm{M}_2$ is given to the eavesdropper. Under the individual secrecy constraint there is no guarantee that the value of this term is equal to $\mathbb{H}(\mathrm{M}_1)$. In particular, since conditioning decreases entropy, it might be strictly less than $\mathbb{H}(\mathrm{M}_1)$. This means that a part of $\mathrm{M}_1$ might be leaked to the eavesdropper upon revealing $\mathrm{M}_2$.

5. The preference in choosing among these two secrecy criteria is a trade-off between a conservative secrecy measure and a larger capacity region and the decision should always be based on whether the legitimate receivers can trust each other or not.

## III. Degraded Multi-Receiver Wiretap BC

In this section, we investigate the degraded multi-receiver wiretap BC under the joint and individual secrecy constraints. Secrecy in degraded wiretap BC was investigated in [11], where the authors establish the joint secrecy capacity region for the degraded two-receiver wiretap BC. This result was then extended to an arbitrary number of receivers in [14]. We present this result and in particular, provide a simpler proof for the converse, that will help us in deriving the converse for the individual secrecy case. We then establish the individual secrecy capacity region of the degraded multi-receiver wiretap BC, showing that it is bigger than the joint secrecy capacity region. Finally, we show that the established characterizations of the capacity regions under both secrecy criteria are valid for any degraded wiretap BC regardless of the degradedness order of the eavesdropper.

Before we present our results, we need to give a quick introduction about degraded multi-receiver wiretap BC and its main properties. A degraded multi-receiver wiretap BC is a class of multi-receiver wiretap BC, such that

$$\mathrm{X}-\mathrm{Y}_1-\mathrm{Y}_2-\cdots-\mathrm{Y}_k-\mathrm{Z}. \tag{14}$$

The previous Markov chain is the main feature of a degraded multi-receiver wiretap BC. It implies that each legitimate receiver is capable of not only decoding its own message, but also the messages of all the receivers degraded from it.

### 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*

$$R_j\leq \mathbb{I}(\mathrm{U}_j;\mathrm{Y}_j|\mathrm{U}_{j+1})-\mathbb{I}(\mathrm{U}_j;\mathrm{Z}|\mathrm{U}_{j+1}), \tag{15}$$

*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. Further, it suffices to have* $|\mathcal{U}_j|\leq \mathrm{UB}(|\mathcal{U}_{j+1}|)(|\mathcal{X}|+2j-1)$*, where* $\mathrm{UB}(|\mathcal{A}|)$ *is the upper-bound of the cardinality of the set* $\mathcal{A}$ *and* $\mathrm{UB}(|\mathcal{U}_{k+1}|)=1$.

**Remark 2.** *It is worth mentioning that the previous theorem generalizes the joint secrecy capacity region of the degraded two-receiver wiretap BC given in Proposition 1.*

*Proof:* This capacity region was established in [14] under the weak secrecy criterion by combining Cover's superposition coding scheme [29] for the degraded multi-receiver BC as in [30] and the principle of wiretap random coding introduced in [4]. Using the strong secrecy techniques introduced in [31–33], one can show that the previous region is also achievable under the strong secrecy criterion.

For the converse, we present a simpler proof than the one given in [14]. Our new proof is based on standard converse techniques in addition to the properties of the degraded BC, in particular the Markov chain in (14). We start by using *Fano's inequality* [34] to derive an upper-bound for a reliable transmission. We use $\ddot{\mathrm{M}}_{j+1}\triangleq(\mathrm{M}_{j+1},\ldots,\mathrm{M}_k)$, thus we have

$$\begin{aligned}R_j&=\frac{1}{n}\mathbb{H}(\mathrm{M}_j)=\frac{1}{n}\mathbb{H}(\mathrm{M}_j|\ddot{\mathrm{M}}_{j+1})\\ &\leq\frac{1}{n}\Big[\mathbb{H}(\mathrm{M}_j|\ddot{\mathrm{M}}_{j+1})-\mathbb{H}(\mathrm{M}_j|\mathrm{Y}_j^n\ddot{\mathrm{M}}_{j+1})\Big]+\tilde{\gamma}_j(\epsilon_n)\\ &=\frac{1}{n}\mathbb{I}(\mathrm{M}_j;\mathrm{Y}_j^n|\ddot{\mathrm{M}}_{j+1})+\tilde{\gamma}_j(\epsilon_n),\end{aligned} \tag{16}$$

where $\tilde{\gamma}_j(\epsilon_n)=1/n+\epsilon_n R_j$. We then consider the secrecy constraint and let $\mathrm{U}_{ji}\triangleq(\mathrm{M}_j,\mathrm{Y}_{j-1}^{i-1},\tilde{\mathrm{Z}}^{i+1},\mathrm{U}_{(j+1)i})$, where

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2016.2566260, IEEE Transactions on Information Forensics and Security



$\mathrm{Y}_0^{i-1} = \mathrm{U}_{(k+1)i} = \emptyset$ and $\tilde{\mathrm{Z}}^{i+1} = (\mathrm{Z}_{i+1}, \ldots, \mathrm{Z}_n)$. We have

$$\begin{aligned} R_j &\overset{(a)}{\leq} \frac{1}{n}\Big[\mathbb{I}(\mathrm{M}_j; \mathrm{Y}_j^n|\ddot{\mathrm{M}}_{j+1}) - \mathbb{I}(\mathrm{M}_j; \mathrm{Z}^n|\ddot{\mathrm{M}}_{j+1})\Big] + \gamma_j(\epsilon_n, \tau_n) \\ &\overset{(b)}{=} \frac{1}{n}\sum_{i=1}^{n}\Big[\mathbb{I}(\mathrm{M}_j; \mathrm{Y}_{ji}|\ddot{\mathrm{M}}_{j+1}\mathrm{Y}_j^{i-1}\tilde{\mathrm{Z}}^{i+1}) \\ &\quad - \mathbb{I}(\mathrm{M}_j; \mathrm{Z}_i|\ddot{\mathrm{M}}_{j+1}\mathrm{Y}_j^{i-1}\tilde{\mathrm{Z}}^{i+1})\Big] + \gamma_j(\epsilon_n, \tau_n) \\ &\overset{(c)}{=} \frac{1}{n}\sum_{i=1}^{n}\Big[\mathbb{I}(\mathrm{M}_j; \mathrm{Y}_{ji}|\ddot{\mathrm{M}}_{j+1}\mathrm{Y}_j^{i-1}\ldots\mathrm{Y}_{k-1}^{i-1}\tilde{\mathrm{Z}}^{i+1}) \\ &\quad - \mathbb{I}(\mathrm{M}_j; \mathrm{Z}_i|\ddot{\mathrm{M}}_{j+1}\mathrm{Y}_j^{i-1}\ldots\mathrm{Y}_{k-1}^{i-1}\tilde{\mathrm{Z}}^{i+1})\Big] + \gamma_j(\epsilon_n, \tau_n) \\ &\overset{(d)}{\leq} \frac{1}{n}\sum_{i=1}^{n}\Big[\mathbb{I}(\mathrm{U}_{ji}; \mathrm{Y}_{ji}|\mathrm{U}_{(j+1)i}) - \mathbb{I}(\mathrm{U}_{ji}; \mathrm{Z}_i|\mathrm{U}_{(j+1)i})\Big] \\ &\quad + \gamma_j(\epsilon_n, \tau_n) \end{aligned} \tag{17}$$

where $(a)$ follows from (3) and (16) as $\gamma_j(\epsilon_n, \tau_n) = \tau_n/n + \tilde{\gamma}_j(\epsilon_n)$; $(b)$ follows from the Csiszár sum identity [6, Lemma 7]; $(c)$ follows because $(\mathrm{Y}_{j+1}, \ldots, \mathrm{Y}_k)$ are degraded from $\mathrm{Y}_j$, while $(d)$ follows because $\mathrm{Z}_i$ is degraded from $\mathrm{Y}_{ji}$, which implies that $\mathbb{I}(\mathrm{Y}_{j+1}^{i-1}; \mathrm{Y}_{ji}|\mathrm{U}_{(j+1)i}) \geq \mathbb{I}(\mathrm{Y}_{j+1}^{i-1}; \mathrm{Z}_i|\mathrm{U}_{(j+1)i})$.

Now, If we introduce an independent and uniformly distributed time sharing random variable to (17), then take the limit as $n \to \infty$, which implies that $\gamma_j(\epsilon_n, \tau_n) \to 0$, our converse is complete. The cardinality bounds follow by the Fenchel-Bunt strengthening of the Carathéodory's theorem as in [25, Appendix C]. ∎

**Remark 3.** *It is worth mentioning, that the following Markov chain* $\mathrm{U}_k - \cdots - \mathrm{U}_2 - \mathrm{X}$ *can be validated in the converse using the principle of functional dependence graph [9].*

### *B. Individual Secrecy Capacity Region*

**Theorem 2.** *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*

$$R_j \leq \mathbb{I}(\mathrm{U}_j; \mathrm{Y}_j|\mathrm{U}_{j+1}) - \mathbb{I}(\mathrm{U}_j; \mathrm{Z}|\mathrm{U}_{j+1}) + \sum_{l=j+1}^{k} R_l \tag{18a}$$

$$R_j \leq \mathbb{I}(\mathrm{U}_j; \mathrm{Y}_j|\mathrm{U}_{j+1}) + \mathbb{I}(\mathrm{U}_{j+1}; \mathrm{Z}) \tag{18b}$$

$$\sum_{l=j}^{k} R_l \leq \sum_{l=j}^{k} \mathbb{I}(\mathrm{U}_l; \mathrm{Y}_l|\mathrm{U}_{l+1}) \tag{18c}$$

*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. Further, it suffices to have* $|\mathcal{U}_j| \leq \mathrm{UB}(|\mathcal{U}_{j+1}|)(|\mathcal{X}| + 2j - 1)$*, where* $\mathrm{UB}(|\mathcal{A}|)$ *is the upper-bound of the cardinality of the set* $\mathcal{A}$ *and* $\mathrm{UB}(|\mathcal{U}_{k+1}|) = 1$.

Before we present our proof, we need to explain what each bound represents. The bound in (18a) implies that the individual secrecy rate of any receiver is bounded by the summation of the randomly encoded rate and the secret key encoded rate, where the secret key encoded rate is bounded by the rates of the weaker receivers. On the other hand, the bound in (18b) enforces another restriction on the secret key encoded rate by assuring that it is less than the randomization rate that can be decoded by each receiver . Finally, the bound in (18c) guarantees two different requirements. The first is a secrecy one, that assures that any randomization rate that is used to carry a secret key encoded message for a certain user can only be used once. The second requirement is a reliability one, which implies that the total sum rate is bounded by the summation of the information encoded in each layer for the corresponding receiver.

*Proof:* The achievability follows by combining the superposition coding technique used for the degraded multi-receiver BC in [30] and the mixture of wiretap random coding [4] and Shannon one time pad secret encoding [3] used for wiretap channel with secret key in [7], along with the strong secrecy techniques introduced in [31–33].

The coding scheme is as follows: the messages of the weak receivers are encoded as cloud centers for the satellite codewords that carry the messages of the stronger ones. Further, the Shannon's ciphered messages are constructed by *Xoring* the messages of the weak receivers that act as secret keys with the messages of the stronger receivers. Finally, those *Xored* messages are used as part of the randomization indexes needed to confuse the eavesdropper in both the cloud centers and the satellite codewords. A detailed achievability proof will be provided for a more general case in Section VI.

For the converse, we start by letting $\mathrm{U}_{ji} \triangleq (\mathrm{M}_j, \mathrm{Y}_{j-1}^{i-1}, \tilde{\mathrm{Z}}^{i+1}, \mathrm{U}_{(j+1)i})$, where $\mathrm{Y}_0^{i-1} = \emptyset$ and $\mathrm{U}_{(k+1)i} = \emptyset$. We also use $\ddot{\mathrm{M}}_{j+1}$ to represent the following random variable $\ddot{\mathrm{M}}_{j+1} \triangleq (\mathrm{M}_{j+1}, \ldots, \mathrm{M}_k)$. We have

$$\begin{aligned} R_j &\overset{(a)}{\leq} \frac{1}{n}\Big[\mathbb{I}(\mathrm{M}_j; \mathrm{Y}_j^n) - \mathbb{I}(\mathrm{M}_j; \mathrm{Z}^n)\Big] + \gamma_j(\epsilon_n, \tau_n) \\ &\overset{(b)}{\leq} \frac{1}{n}\Big[\mathbb{I}(\mathrm{M}_j; \mathrm{Y}_j^n|\ddot{\mathrm{M}}_{j+1}) - \mathbb{I}(\mathrm{M}_j; \mathrm{Z}^n|\ddot{\mathrm{M}}_{j+1}) \\ &\quad + \mathbb{I}(\ddot{\mathrm{M}}_{j+1}; \mathrm{Z}^n|\mathrm{M}_j)\Big] + \gamma_j(\epsilon_n, \tau_n) \\ &\overset{(c)}{\leq} \frac{1}{n}\Big[\mathbb{I}(\mathrm{M}_j; \mathrm{Y}_j^n|\ddot{\mathrm{M}}_{j+1}) - \mathbb{I}(\mathrm{M}_j; \mathrm{Z}^n|\ddot{\mathrm{M}}_{j+1})\Big] + \sum_{l=j+1}^{k} R_l \\ &\quad + \gamma_j(\epsilon_n, \tau_n) \\ &\overset{(d)}{\leq} \frac{1}{n}\sum_{i=1}^{n}\Big[\mathbb{I}(\mathrm{U}_{ji}; \mathrm{Y}_{ji}|\mathrm{U}_{(j+1)i}) - \mathbb{I}(\mathrm{U}_{ji}; \mathrm{Z}_i|\mathrm{U}_{(j+1)i})\Big] \\ &\quad + \sum_{l=j+1}^{k} R_l + \gamma_j(\epsilon_n, \tau_n), \end{aligned} \tag{19}$$

where $(a)$ follows by using Fano's inequality as in (16), in addition to the individual secrecy constraint in (5); $(b)$ follows because $\mathbb{I}(\mathrm{M}_j; \mathrm{Z}^n) \geq \mathbb{I}(\mathrm{M}_j; \mathrm{Z}^n|\ddot{\mathrm{M}}_{j+1}) - \mathbb{I}(\ddot{\mathrm{M}}_{j+1}; \mathrm{Z}^n|\mathrm{M}_j)$; $(c)$ follows because $n\sum_{l=j+1}^{k} R_l \geq \mathbb{I}(\ddot{\mathrm{M}}_{j+1}; \mathrm{Z}^n|\mathrm{M}_j)$; while $(d)$ follows as in (17). Now, if we use Eq. (16) in addition to the individual secrecy constraint in (5), we have

$$\begin{aligned} R_j &\leq \frac{1}{n}\Big[\mathbb{I}(\mathrm{M}_j; \mathrm{Y}_j^n|\ddot{\mathrm{M}}_{j+1}) + \mathbb{I}(\ddot{\mathrm{M}}_{j+1}; \mathrm{Z}^n)\Big] + \tilde{\gamma}_j(\epsilon_n) \\ &\leq \frac{1}{n}\sum_{i=1}^{n}\Big[\mathbb{I}(\mathrm{M}_j; \mathrm{Y}_{ji}|\ddot{\mathrm{M}}_{j+1}\mathrm{Y}_j^{i-1}\tilde{\mathrm{Z}}^{i+1}) + \mathbb{I}(\ddot{\mathrm{M}}_{j+1}; \mathrm{Z}_i|\tilde{\mathrm{Z}}^{i+1}) \end{aligned}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2016.2566260, IEEE Transactions on Information Forensics and Security



$$+\mathbb{I}(\tilde{\mathrm{Z}}^{i+1};\mathrm{Y}_{ji}|\ddot{\mathrm{M}}_{j+1}\mathrm{Y}_j^{i-1})\Big]+\tilde{\gamma}_j(\epsilon_n)$$
$$\overset{(a)}{=}\frac{1}{n}\sum_{i=1}^{n}\Big[\mathbb{I}(\mathrm{M}_j;\mathrm{Y}_{ji}|\mathrm{U}_{(j+1)i})+\mathbb{I}(\ddot{\mathrm{M}}_{j+1}\mathrm{Y}_j^{i-1};\mathrm{Z}_i|\tilde{\mathrm{Z}}^{i+1})\Big]+\tilde{\gamma}_j(\epsilon_n)$$
$$\leq\frac{1}{n}\sum_{i=1}^{n}\Big[\mathbb{I}(\mathrm{U}_{ji};\mathrm{Y}_{ji}|\mathrm{U}_{(j+1)i})+\mathbb{I}(\mathrm{U}_{(j+1)i};\mathrm{Z}_i)\Big]+\tilde{\gamma}_j(\epsilon_n) \tag{20}$$

where $(a)$ follows from the Csiszár sum identity [6, Lemma 7] as $\mathbb{I}(\tilde{\mathrm{Z}}^{i+1};\mathrm{Y}_{ji}|\ddot{\mathrm{M}}_{j+1}\mathrm{Y}_j^{i-1})=\mathbb{I}(\mathrm{Y}_j^{i-1};\mathrm{Z}_i|\ddot{\mathrm{M}}_{j+1}\tilde{\mathrm{Z}}^{i+1})$. Finally, for the sum rate, we have

$$\sum_{l=j}^{k}R_l\overset{(a)}{\leq}\frac{1}{n}\Bigg[\sum_{l=j+1}^{k}\Big[\mathbb{I}(\mathrm{M}_l;\mathrm{Y}_l^n|\ddot{\mathrm{M}}_{l+1})-\mathbb{I}(\mathrm{M}_l;\mathrm{Z}^n|\ddot{\mathrm{M}}_{l+1})\Big]+\mathbb{I}(\ddot{\mathrm{M}}_{j+1};\mathrm{Z}^n)+\mathbb{I}(\mathrm{M}_j;\mathrm{Y}_j^n|\ddot{\mathrm{M}}_{j+1})\Bigg]+\sum_{l=j}^{k}\tilde{\gamma}_l(\epsilon_n)$$
$$\overset{(b)}{=}\frac{1}{n}\sum_{i=1}^{n}\Bigg[\sum_{l=j+1}^{k}\Big[\mathbb{I}(\mathrm{U}_{li};\mathrm{Y}_{li}|\mathrm{U}_{(l+1)i})-\mathbb{I}(\mathrm{U}_{li};\mathrm{Z}_i|\mathrm{U}_{(l+1)i})\Big]+\mathbb{I}(\mathrm{U}_{ji};\mathrm{Y}_{ji}|\mathrm{U}_{(j+1)i})+\mathbb{I}(\mathrm{U}_{(j+1)i};\mathrm{Z}_i)\Bigg]+\sum_{l=j}^{k}\tilde{\gamma}_l(\epsilon_n)$$
$$\overset{(c)}{=}\frac{1}{n}\sum_{i=1}^{n}\sum_{l=j}^{k}\mathbb{I}(\mathrm{U}_{li};\mathrm{Y}_{li}|\mathrm{U}_{(l+1)i})+\sum_{l=j}^{k}\tilde{\gamma}_l(\epsilon_n) \tag{21}$$

where $\tilde{\gamma}_l(\epsilon_n)=1/n+\epsilon_n R_l$. $(a)$ follows from Eq. (16) and the fact that $\mathbb{I}(\ddot{\mathrm{M}}_{j+1};\mathrm{Z}^n)=\sum_{l=j+1}^{k}\mathbb{I}(\mathrm{M}_l;\mathrm{Z}^n|\ddot{\mathrm{M}}_{l+1})$; $(b)$ follows as in (17) and (20); while $(c)$ follows because $\sum_{l=j+1}^{k}\mathbb{I}(\mathrm{U}_{li};\mathrm{Z}_i|\mathrm{U}_{(l+1)i})=\mathbb{I}(\mathrm{U}_{(j+1)i};\mathrm{Z}_i)$. Now, if we introduce an independent and uniformly distributed randomization index to the bounds in (19), (20) and (21), 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

Theorems 1 and 2 were derived for degraded multi-receiver wiretap BCs in which the eavesdropper is the weakest receiver. In general, any degraded wiretap BC –whether it is physically or statistically degraded– is characterized by a Markov chain with a certain degradedness order among the legitimate receivers and the eavesdropper. This degradedness order plays an important role in proving the converse of the secrecy capacity region. It was shown in [15, Theorem 3] that changing this order affects the individual secrecy capacity region of the wiretap BC with receiver side information. Thus, it is important to investigate how changing the degradedness order of the eavesdropper affects the joint and individual secrecy capacity regions established in Theorems 1 and 2 respectively.

We start by dividing the $k$ legitimate receivers into two groups. The first group contains the legitimate receivers degraded from the eavesdropper, i.e. the eavesdropper is stronger than those receivers. This group contains the legitimate receivers numbered from $d$ to $k$, where $d\in[\![1;k]\!]$. On the other hand, the second group contains the remaining legitimate receivers from which the eavesdropper is degraded. The receivers of this group are numbered from 1 to $d-1$.

**1. Joint Secrecy Capacity Region** (15)**:** Although this region was established under the condition of having the eavesdropper as the weakest receiver, it can be shown that it is valid for the other scenarios as well.

• *Achievability:* Since the randomization needed to confuse the eavesdropper is bigger than the decoding capability of the legitimate receivers of the first group, i.e. $\mathbb{I}(\mathrm{U}_j;\mathrm{Y}_j|\mathrm{U}_{j+1})\leq\mathbb{I}(\mathrm{U}_j;\mathrm{Z}|\mathrm{U}_{j+1})$ for $j\in[\![d;k]\!]$, the achievable joint secrecy rates for the legitimate receivers in this group are zeros. However, for the second group of receivers, nothing changes. Thus, the region in (15) can be reformulated as follows:

$$R_j=0\qquad j\in[\![d;k]\!]$$
$$R_j\leq\mathbb{I}(\mathrm{U}_j;\mathrm{Y}_j|\mathrm{U}_{j+1})-\mathbb{I}(\mathrm{U}_j;\mathrm{Z}|\mathrm{U}_{j+1})\qquad j\in[\![1;d-1]\!].$$

• *Converse:* It was shown in [9, Proposition 3.4] that the joint secrecy capacity vanishes if the legitimate receiver is degraded from the eavesdropper. This implies that, for the confidential rate of any legitimate receiver that belongs to the first group is upper bounded by zero. On the other hand, the converse of the confidential rates of the legitimate receivers of the second group follows as in (17), where $k$ is replaced by $d-1$.

**2. Individual Secrecy Capacity Region** (18)**:** Like the joint secrecy case, this region was established under the condition of having the eavesdropper as the weakest receiver. The main challenge is that, in [17, Lemma 2], it was shown for the BC with receiver side information that the optimum coding technique for the individual secrecy criterion depends on the degradedness order of the eavesdropper. However, this result has not been generalized for other channels so far. So in order to prove that the region in (18) is valid regardless of the degradedness order of the eavesdropper, we need to modify our achievability and converse proofs.

• *Achievability:* Since the following condition $\mathbb{I}(\mathrm{U}_j;\mathrm{Y}_j|\mathrm{U}_{j+1})\leq\mathbb{I}(\mathrm{U}_j;\mathrm{Z}|\mathrm{U}_{j+1})$ for $j\in[\![d;k]\!]$ still holds, the individual secrecy achievable rates for the legitimate receivers of the first group vanish. This implies that, we need just to modify our coding scheme as if we only have a degraded $(d-1)$-receiver wiretap BC instead of $k$-receiver. Thus, for $j\in[\![d;k]\!]$, we have $R_j=0$, while for $j\in[\![1;d-1]\!]$, the region in (18) implies:

$$R_j\leq\mathbb{I}(\mathrm{U}_j;\mathrm{Y}_j|\mathrm{U}_{j+1})-\mathbb{I}(\mathrm{U}_j;\mathrm{Z}|\mathrm{U}_{j+1})+\sum_{l=j+1}^{d-1}R_l$$
$$R_j\leq\mathbb{I}(\mathrm{U}_j;\mathrm{Y}_j|\mathrm{U}_{j+1})+\mathbb{I}(\mathrm{U}_{j+1};\mathrm{Z})$$
$$\sum_{l=j}^{d-1}R_l\leq\sum_{l=j}^{d-1}\mathbb{I}(\mathrm{U}_l;\mathrm{Y}_l|\mathrm{U}_{l+1}).$$

• *Converse:* We start by the first group of legitimate receivers. It was shown in [15, Proposition 1], that if Y is degraded from Z, then $\mathbb{I}(\mathrm{M};\mathrm{Y}^n)\leq\mathbb{I}(\mathrm{M};\mathrm{Z}^n)$. Since the subtraction of these two terms is the first step in (19), thus $R_j$ is upper-bounded by zero for $j\in[\![d,k]\!]$. On the other

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2016.2566260, IEEE Transactions on Information Forensics and Security



hand, the converse of the confidential rates of the legitimate receivers of the second group follows as in (19), (20) and (21), where $k$ is replaced by $d-1$.

The previous argument advocates that Theorems 1 and 2 establish a characterization of the joint and individual secrecy capacity regions for any degraded multi-receiver wiretap BC regardless of the degradedness order of the eavesdropper.

## IV. Gaussian SISO Multi-Receiver Wiretap BC

In this section, we study the Gaussian SISO multi-receiver wiretap BC under the joint and individual secrecy constraints. We present the joint secrecy capacity region established in [12], then establish the individual secrecy capacity region. We start by defining the Gaussian SISO multi-receiver wiretap BC:

$$\mathrm{Y}_j = \mathrm{X} + \mathrm{N}_j \tag{22a}$$
$$\mathrm{Z} = \mathrm{X} + \mathrm{N}_Z, \tag{22b}$$

where the channel input X is subject to a power constraint $\mathbb{E}[\mathrm{X}^2] \leq P$. The $\mathrm{N}_j$ and $\mathrm{N}_Z$ are zero-mean Gaussian random variables, whose variances are given by $\sigma_j^2$ and $\sigma_Z^2$ respectively.

The Gaussian SISO multi-receiver wiretap BC belongs to the class of degraded multi-receiver wiretap BCs, where the variances (power) of the Gaussian noises $\mathrm{N}_j$ and $\mathrm{N}_Z$ define the degradedness order of the channel. We will assume without loss of generality that the variances of the Gaussian noises satisfy the following order:

$$\sigma_1^2 \leq \sigma_2^2 \leq \cdots \leq \sigma_k^2 \leq \sigma_Z^2. \tag{23}$$

It was shown at the end of the previous section that the capacity regions in (15) and (18) establishes the joint and individual secrecy capacity of any degraded multi-receiver wiretap BC respectively, regardless of the degradedness order of the eavesdropper. Thus, we can use Theorem 1 and Theorem 2 to derive the joint and individual secrecy capacity for the Gaussian SISO multi-receiver wiretap BC.

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

$$R_j \leq f\left(\frac{\alpha_j P}{\sum_{i=1}^{j-1}\alpha_i P + \sigma_j^2}\right) - f\left(\frac{\alpha_j P}{\sum_{i=1}^{j-1}\alpha_i P + \sigma_Z^2}\right), \tag{24}$$

*while the individual secrecy capacity region is given by the union of all rate tuples $(R_1, \ldots, R_k) \in \mathbb{R}_+^k$ that satisfy*

$$R_j \leq f\left(\frac{\alpha_j P}{\sum_{i=1}^{j-1}\alpha_i P + \sigma_j^2}\right) - f\left(\frac{\alpha_j P}{\sum_{i=1}^{j-1}\alpha_i P + \sigma_Z^2}\right) + \sum_{l=j+1}^{k} R_l \tag{25a}$$

$$R_j \leq f\left(\frac{\alpha_j P}{\sum_{i=1}^{j-1}\alpha_i P + \sigma_j^2}\right) + f\left(\frac{\sum_{i=j+1}^{k}\alpha_i P}{\sum_{i=1}^{j}\alpha_i P + \sigma_Z^2}\right) \tag{25b}$$

$$\sum_{l=j}^{k} R_l \leq \sum_{l=j}^{k} f\left(\frac{\alpha_l P}{\sum_{i=1}^{l-1}\alpha_i P + \sigma_l^2}\right) \tag{25c}$$

*where the unions are taken over all values of $\alpha_j \in [0,1]$ such that $\sum_{i=1}^{k}\alpha_i \leq 1$.*

Before we present our proof, we need to highlight the following lemma as it will play a vital role in establishing our converse.

**Lemma 1.** *Consider a Gaussian SISO multi-receiver wiretap channel as defined in* (22)*, where $\mathbb{E}[\mathrm{X}^2] \leq P$ and the variances of the Gaussian noises satisfy the order in* (23)*. If the following inequality holds*

$$\mathbb{I}(\mathrm{U}_j;\mathrm{Y}_j|\mathrm{U}_{j+1}) - \mathbb{I}(\mathrm{U}_j;\mathrm{Z}|\mathrm{U}_{j+1}) \leq f\left(\frac{\alpha_j P}{\sum_{i=1}^{j-1}\alpha_i P + \sigma_j^2}\right) - f\left(\frac{\alpha_j P}{\sum_{i=1}^{j-1}\alpha_i P + \sigma_Z^2}\right), \tag{26}$$

*where $\mathrm{U}_{k+1} = \emptyset$, $\mathrm{U}_1 = \mathrm{X}$, $\mathrm{U}_k - \cdots - \mathrm{U}_2 - \mathrm{X} - \mathrm{Y}_1 - \mathrm{Y}_2 - \cdots - \mathrm{Y}_k - \mathrm{Z}$ forms a Markov chain and $\sum_{i=1}^{k}\alpha_i = 1$, then $\mathbb{E}[\mathrm{U}_j^2] \leq \sum_{i=j}^{k}\alpha_i P$.*

*Proof:* We start by letting $\mathrm{U}_k$ be a Gaussian random variable such that, $\mathbb{E}[\mathrm{U}_k^2] = (\alpha_k + \gamma)P$ because according to [12], the expression in (27) is maximized by Gaussian signalling. Now, if we let $\mathrm{X} = \mathrm{U}_k + \bar{\mathrm{V}}_k$, where $\bar{\mathrm{V}}_k$ is a Gaussian random variable independent from $\mathrm{U}_k$, we have

$$\mathbb{I}(\mathrm{U}_k;\mathrm{Y}_k) - \mathbb{I}(\mathrm{U}_k;\mathrm{Z}) = f\left(\frac{(\alpha_k+\gamma)P}{(\sum_{i=1}^{k-1}\alpha_i - \gamma)P + \sigma_k^2}\right) - f\left(\frac{(\alpha_k+\gamma)P}{(\sum_{i=1}^{k-1}\alpha_i - \gamma)P + \sigma_Z^2}\right). \tag{27}$$

This conditions contradicts the one in (26) at $j = k$, unless $\gamma \leq 0$ which consequently implies that $\mathbb{E}[\mathrm{U}_k^2] \leq \alpha_k P$. Now, repeating the previous steps recursively until we reach $\mathrm{U}_j$, we can show that $\mathbb{E}[\mathrm{U}_j^2] \leq \sum_{i=j}^{k}\alpha_i P$. ∎

*Proof of Theorem 3:* The achievability of the two regions follows by choosing $\mathrm{U}_j = \mathrm{U}_{j+1} + \mathrm{V}_j$, where the $\mathrm{V}_j$ are independent Gaussian random variables with variance $\alpha_j$ and $\mathrm{U}_{k+1} = 0$. The decoder at a certain receiver $\mathrm{Y}_i$, where $i \in [\![1,k]\!]$, can decode all $\mathrm{V}_j$ for $j \geq i$ because of the order of the variances of the Gaussian noises in (23), while handling the remaining $\mathrm{V}_j$ for $j < i$ as interfering noise. The previous coding structure implies that, $(\mathrm{U}_k, \ldots, \mathrm{U}_2, \mathrm{X})$ are characterized by a joint Gaussian distribution. This implies that the rates in (24) and (25) are achievable.

Now, for the converse, we focus mainly on the individual secrecy case as the joint secrecy converse can be established using the same steps. We start with the bound in (18a) and consider the $k^{th}$ user first. We have

$$\begin{aligned} R_k &\leq \mathbb{I}(\mathrm{U}_k;\mathrm{Y}_k) - \mathbb{I}(\mathrm{U}_k;\mathrm{Z}) \\ &\overset{(a)}{=} \Big[\mathbb{I}(\mathrm{X};\mathrm{Y}_k) - \mathbb{I}(\mathrm{X};\mathrm{Z})\Big] - \Big[\mathbb{I}(\mathrm{X};\mathrm{Y}_k|\mathrm{U}_k) - \mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}_k)\Big] \\ &\overset{(b)}{\leq} \left[f\left(\frac{P}{\sigma_k^2}\right) - f\left(\frac{P}{\sigma_Z^2}\right)\right] - \Big[\mathbb{I}(\mathrm{X};\mathrm{Y}_k|\mathrm{U}_k) - \mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}_k)\Big] \\ &\overset{(c)}{=} \left[f\left(\frac{P}{\sigma_k^2}\right) - f\left(\frac{P}{\sigma_Z^2}\right)\right] - \left[f\left(\frac{\bar{\alpha}_k P}{\sigma_k^2}\right) - f\left(\frac{\bar{\alpha}_k P}{\sigma_Z^2}\right)\right] \end{aligned}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2016.2566260, IEEE Transactions on Information Forensics and Security



$$\overset{(d)}{=} f\left(\frac{\alpha_k P}{\sum_{i=1}^{k-1}\alpha_i P+\sigma_k^2}\right)-f\left(\frac{\alpha_k P}{\sum_{i=1}^{k-1}\alpha_i P+\sigma_Z^2}\right), \quad (28)$$

where $(a)$ follows by using the chain rule and the Markov chain $\mathrm{U}_k-\mathrm{X}-(\mathrm{Y}_k,\mathrm{Z})$; $(b)$ follows because $\mathbb{I}(\mathrm{X};\mathrm{Y}_k)-\mathbb{I}(\mathrm{X};\mathrm{Z})$ is maximized by a Gaussian X [5]; $(c)$ follows because $0\leq \mathbb{I}(\mathrm{X};\mathrm{Y}_k|\mathrm{U}_k)-\mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}_k)\leq f(P/\sigma_k^2)-f(P/\sigma_Z^2)$, which implies that for any pair $(\mathrm{U}_k,\mathrm{X})$, there exists an $\bar{\alpha}_k\in[0,1]$ such that, $\mathbb{I}(\mathrm{X};\mathrm{Y}_k|\mathrm{U}_k)-\mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}_k)=f(\bar{\alpha}_k P/\sigma_k^2)-f(\bar{\alpha}_k P/\sigma_Z^2)$; and $(d)$ follows by letting $\alpha_k=1-\bar{\alpha}_k$ and $\bar{\alpha}_k=\sum_{i=1}^{k-1}\alpha_i$. Now, we consider the $(k-1)^{th}$ user under the same bound, we have

$$\begin{aligned}
R_{k-1} &\leq \mathbb{I}(\mathrm{U}_{k-1};\mathrm{Y}_{k-1}|\mathrm{U}_k)-\mathbb{I}(\mathrm{U}_{k-1};\mathrm{Z}|\mathrm{U}_k)+R_k\\
&\overset{(a)}{=} \Big[\mathbb{I}(\mathrm{X};\mathrm{Y}_{k-1}|\mathrm{U}_k)-\mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}_k)\Big]\\
&\quad-\Big[\mathbb{I}(\mathrm{X};\mathrm{Y}_{k-1}|\mathrm{U}_{k-1})-\mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}_{k-1})\Big]+R_k\\
&\overset{(b)}{\leq} \left[f\left(\frac{\bar{\alpha}_k P}{\sigma_{k-1}^2}\right)-f\left(\frac{\bar{\alpha}_k P}{\sigma_Z^2}\right)\right]\\
&\quad-\Big[\mathbb{I}(\mathrm{X};\mathrm{Y}_{k-1}|\mathrm{U}_{k-1})-\mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}_{k-1})\Big]+R_k\\
&\overset{(c)}{=} \left[f\left(\frac{\bar{\alpha}_k P}{\sigma_{k-1}^2}\right)-f\left(\frac{\bar{\alpha}_k P}{\sigma_Z^2}\right)\right]\\
&\quad-\left[f\left(\frac{\bar{\alpha}_{k-1} P}{\sigma_k^2}\right)-f\left(\frac{\bar{\alpha}_{k-1} P}{\sigma_Z^2}\right)\right]+R_k\\
&\overset{(d)}{=} f\left(\frac{\alpha_{k-1}P}{\sum_{i=1}^{k-2}\alpha_i P+\sigma_k^2}\right)-f\left(\frac{\alpha_{k-1}P}{\sum_{i=1}^{k-2}\alpha_i P+\sigma_Z^2}\right)+R_k,
\end{aligned} \quad (29)$$

where $(a)$ follows by using the chain rule and the Markov chain $\mathrm{U}_k-\mathrm{U}_{k-1}-\mathrm{X}-(\mathrm{Y}_{k-1},\mathrm{Z})$; $(b)$ follows because under the constraint $\mathbb{I}(\mathrm{X};\mathrm{Y}_k|\mathrm{U}_k)-\mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}_k)=f(\bar{\alpha}_k P/\sigma_k^2)-f(\bar{\alpha}_k P/\sigma_Z^2)$, the expression $\mathbb{I}(\mathrm{X};\mathrm{Y}_{k-1}|\mathrm{U}_k)-\mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}_k)$ is maximized by a joint Gaussian distribution on the pair $(\mathrm{U}_k,\mathrm{X})$ [12]; $(c)$ follows because $0\leq \mathbb{I}(\mathrm{X};\mathrm{Y}_{k-1}|\mathrm{U}_{k-1})-\mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}_{k-1})\leq f(\bar{\alpha}_k P/\sigma_{k-1}^2)-f(\bar{\alpha}_k P/\sigma_Z^2)$, which implies that for any triple $(\mathrm{U}_k,\mathrm{U}_{k-1},\mathrm{X})$, there exists an $\bar{\alpha}_{k-1}\in[0,\bar{\alpha}_k]$ such that, $\mathbb{I}(\mathrm{X};\mathrm{Y}_{k-1}|\mathrm{U}_{k-1})-\mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}_{k-1})=f(\bar{\alpha}_{k-1}P/\sigma_{k-1}^2)-f(\bar{\alpha}_{k-1}P/\sigma_Z^2)$; and $(d)$ follows by letting $\alpha_{k-1}=\bar{\alpha}_k-\bar{\alpha}_{k-1}$ and $\bar{\alpha}_{k-1}=\sum_{i=1}^{k-2}\alpha_i$.

Now, if we apply the same steps in (29) to the remaining users, we can show that the bound in (25a) holds. These calculations establish two additional constraints: the first is $\sum_{i=1}^{k}\alpha_i=1$, while the second is the bound in (26) and its consequence $\mathbb{E}[\mathrm{U}_j^2]\leq\sum_{i=j}^{k}\alpha_i P$ which follows from Lemma 1. We now consider the bound in (18b) as follows:

$$\begin{aligned}
R_j &\leq \mathbb{I}(\mathrm{U}_j;\mathrm{Y}_j|\mathrm{U}_{j+1})+\mathbb{I}(\mathrm{U}_{j+1};\mathrm{Z})\\
&\overset{(a)}{=} \mathbb{I}(\mathrm{U}_j;\mathrm{Y}_j|\mathrm{U}_{j+1})-\mathbb{I}(\mathrm{U}_j;\mathrm{Z}|\mathrm{U}_{j+1})+\mathbb{I}(\mathrm{U}_j;\mathrm{Z})\\
&\overset{(b)}{\leq} f\left(\frac{\alpha_j P}{\sum_{i=1}^{j-1}\alpha_i P+\sigma_j^2}\right)-f\left(\frac{\alpha_j P}{\sum_{i=1}^{j-1}\alpha_i P+\sigma_Z^2}\right)\\
&\quad+\mathbb{I}(\mathrm{U}_j;\mathrm{Z})\\
&\overset{(c)}{\leq} f\left(\frac{\alpha_j P}{\sum_{i=1}^{j-1}\alpha_i P+\sigma_j^2}\right)-f\left(\frac{\alpha_j P}{\sum_{i=1}^{j-1}\alpha_i P+\sigma_Z^2}\right)\\
&\quad+f\left(\frac{\sum_{i=j}^{k}\alpha_i P}{\sum_{i=1}^{j-1}\alpha_i P+\sigma_Z^2}\right)\\
&= f\left(\frac{\alpha_j P}{\sum_{i=1}^{j-1}\alpha_i P+\sigma_j^2}\right)+f\left(\frac{\sum_{i=j+1}^{k}\alpha_i P}{\sum_{i=1}^{j}\alpha_i P+\sigma_Z^2}\right),
\end{aligned} \quad (30)$$

where $(a)$ follows by using the chain rule and the Markov chain $\mathrm{U}_{j+1}-\mathrm{U}_j-\mathrm{Z}$; $(b)$ follows by the same steps used to establish (25a); while $(c)$ follows because under the power constraint on $\mathrm{U}_j$ and X, in addition to the Markov chain $\mathrm{U}_j-\mathrm{X}-\mathrm{Z}$, $\mathbb{I}(\mathrm{U}_j;\mathrm{Z})$ is maximized by a joint Gaussian distribution on the pair $(\mathrm{U}_j,\mathrm{X})$. Finally, we consider the bound in (18c), for which we have

$$\begin{aligned}
\sum_{l=j}^{k}R_l &\leq \sum_{l=j}^{k}\mathbb{I}(\mathrm{U}_l;\mathrm{Y}_l|\mathrm{U}_{l+1})\\
&\overset{(a)}{=} \sum_{l=j}^{k}\big[\mathbb{I}(\mathrm{U}_l;\mathrm{Y}_l|\mathrm{U}_{l+1})-\mathbb{I}(\mathrm{U}_l;\mathrm{Z}|\mathrm{U}_{l+1})\big]+\mathbb{I}(\mathrm{U}_j;\mathrm{Z})\\
&\overset{(b)}{\leq} \sum_{l=j}^{k}\left[f\left(\frac{\alpha_l P}{\sum_{i=1}^{l-1}\alpha_i P+\sigma_l^2}\right)-f\left(\frac{\alpha_l P}{\sum_{i=1}^{l-1}\alpha_i P+\sigma_Z^2}\right)\right]\\
&\quad+\mathbb{I}(\mathrm{U}_j;\mathrm{Z})\\
&\overset{(c)}{\leq} \sum_{l=j}^{k}\left[f\left(\frac{\alpha_l P}{\sum_{i=1}^{l-1}\alpha_i P+\sigma_l^2}\right)-f\left(\frac{\alpha_l P}{\sum_{i=1}^{l-1}\alpha_i P+\sigma_Z^2}\right)\right]\\
&\quad+f\left(\frac{\sum_{i=j}^{k}\alpha_i P}{\sum_{i=1}^{j-1}\alpha_i P+\sigma_Z^2}\right)\\
&= \sum_{l=j}^{k}f\left(\frac{\alpha_l P}{\sum_{i=1}^{l-1}\alpha_i P+\sigma_l^2}\right),
\end{aligned} \quad (31)$$

where $(a)$ follows by using the chain rule and the Markov chain $\mathrm{U}_k-\mathrm{U}_{k-1}-\cdots-\mathrm{U}_j-\mathrm{Z}$; while $(b)$ and $(c)$ follows as in (30). Now, our converse is complete. ■

## V. Degraded Gaussian MIMO Multi-Reciever Wiretap Channel

In this section, we will study the degraded Gaussian MIMO multi-receiver wiretap BC under the joint and individual secrecy criteria and present the joint and individual secrecy capacity regions. We start by defining the degraded Gaussian MIMO multi-receiver wiretap BC as:

$$\mathbf{Y}_j=\mathbf{X}+\mathbf{N}_j \quad (32a)$$

$$\mathbf{Z}=\mathbf{X}+\mathbf{N}_Z, \quad (32b)$$

where $\mathbf{X}$, $\mathbf{Y}_j$, $\mathbf{N}_j$, $\mathbf{Z}$ and $\mathbf{N}_Z$ are column vectors of length $m$, where $m$ is the number of antennas available at the transmitter and each receiver. The channel input $\mathbf{X}$ is subject to a covariance constraint $\mathbb{E}[\mathbf{X}\mathbf{X}^\top]\preceq\mathbf{S}$, where $\mathbf{S}$ is a positive definite matrix, i.e. $\mathbf{S}\succ\mathbf{0}$. $\mathbf{N}_j$ and $\mathbf{N}_Z$ are zero-mean Gaussian random vectors, whose covariance matrices are given by $\mathbf{\Sigma}_j$ and $\mathbf{\Sigma}_Z$, such that

$$\mathbf{0}\prec\mathbf{\Sigma}_1\preceq\mathbf{\Sigma}_2\preceq\cdots\preceq\mathbf{\Sigma}_k\preceq\mathbf{\Sigma}_Z. \quad (33)$$

The semi-definite ordering of the noise covariance matrices in (33) implies that $\mathbf{X}-\mathbf{Y}_1-\cdots-\mathbf{Y}_k-\mathbf{Z}$ forms a Markov

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2016.2566260, IEEE Transactions on Information Forensics and Security



chain, where changing the order of the covariance matrix will change the position of the receiver in the Markov chain. This implies that, the degraded Gaussian MIMO wiretap BC belongs to the class of degraded wiretap BCs and its joint and individual secrecy capacity regions can be computed by finding the optimal joint distribution on $(\mathrm{U}_k, \ldots, \mathrm{U}_2, \mathbf{X})$ that traces the boundary of the capacity regions in (15) and (18) respectively.

**Theorem 4.** *Consider a degraded Gaussian MIMO multi-receiver wiretap BC, then the joint secrecy capacity region is given by the union of all rate tuples $(R_1, \ldots, R_k) \in \mathbb{R}_+^k$ that satisfy*

$$R_j \leq \frac{1}{2}\log\frac{\left|\sum_{i=1}^{j}\mathbf{K}_i+\mathbf{\Sigma}_j\right|}{\left|\sum_{i=1}^{j-1}\mathbf{K}_i+\mathbf{\Sigma}_j\right|}-\frac{1}{2}\log\frac{\left|\sum_{i=1}^{j}\mathbf{K}_i+\mathbf{\Sigma}_Z\right|}{\left|\sum_{i=1}^{j-1}\mathbf{K}_i+\mathbf{\Sigma}_Z\right|} \tag{34}$$

*while the individual secrecy capacity region is given by the union of all rate tuples $(R_1, \ldots, R_k) \in \mathbb{R}_+^k$ that satisfy*

$$R_j \leq \frac{1}{2}\log\frac{\left|\sum_{i=1}^{j}\mathbf{K}_i+\mathbf{\Sigma}_j\right|}{\left|\sum_{i=1}^{j-1}\mathbf{K}_i+\mathbf{\Sigma}_j\right|}-\frac{1}{2}\log\frac{\left|\sum_{i=1}^{j}\mathbf{K}_i+\mathbf{\Sigma}_Z\right|}{\left|\sum_{i=1}^{j-1}\mathbf{K}_i+\mathbf{\Sigma}_Z\right|} + \sum_{l=j+1}^{k} R_l \tag{35a}$$

$$R_j \leq \frac{1}{2}\log\frac{\left|\sum_{i=1}^{j}\mathbf{K}_i+\mathbf{\Sigma}_j\right|}{\left|\sum_{i=1}^{j-1}\mathbf{K}_i+\mathbf{\Sigma}_j\right|}+\frac{1}{2}\log\frac{\left|\sum_{i=1}^{k}\mathbf{K}_i+\mathbf{\Sigma}_Z\right|}{\left|\sum_{i=1}^{j}\mathbf{K}_i+\mathbf{\Sigma}_Z\right|} \tag{35b}$$

$$\sum_{l=j}^{k} R_l \leq \sum_{l=j}^{k}\frac{1}{2}\log\frac{\left|\sum_{i=1}^{l}\mathbf{K}_i+\mathbf{\Sigma}_l\right|}{\left|\sum_{i=1}^{l-1}\mathbf{K}_i+\mathbf{\Sigma}_l\right|} \tag{35c}$$

*where the unions are taken over all positive semi-definite matrices $\mathbf{K}_j \succeq \mathbf{0}$, such that $\sum_{i=1}^{k}\mathbf{K}_i \preceq \mathbf{S}$.*

*Proof:* The achievablity of the previous regions follows by using a Gaussian random vector realization for the auxiliary random variables in Theorem 1 and Theorem 2 respectively. These vectors are constructed recursively as follows: $\mathbf{U}_j = \mathbf{U}_{j+1} + \mathbf{V}_j$, where $\mathbf{V}_j$ are independent Gaussian random vectors with covariance matrices $\mathbf{K}_j$ and $\mathbf{U}_{k+1}$ is a zero vector.

Now, for the converse, we start by highlighting the upper-bound established in [12] for the degraded Gaussian MIMO wiretap BC under the joint secrecy constraint

$$\mathbb{I}(\mathrm{U}_j;\mathbf{Y}_j|\mathrm{U}_{j+1}) - \mathbb{I}(\mathrm{U}_j;\mathbf{Z}|\mathrm{U}_{j+1}) \leq \frac{1}{2}\log\frac{\left|\sum_{i=1}^{j}\mathbf{K}_i+\mathbf{\Sigma}_j\right|}{\left|\sum_{i=1}^{j-1}\mathbf{K}_i+\mathbf{\Sigma}_j\right|}-\frac{1}{2}\log\frac{\left|\sum_{i=1}^{j}\mathbf{K}_i+\mathbf{\Sigma}_Z\right|}{\left|\sum_{i=1}^{j-1}\mathbf{K}_i+\mathbf{\Sigma}_Z\right|}. \tag{36}$$

Using the previous bound and adapting the technique used in deriving the converse of the Gaussian SISO case in Theorem 3 to the degraded MIMO case, the converse can be shown accordingly. ∎

## VI. General Achievable Rate Regions

In this section, we derive achievable rate regions for the general two-receiver wiretap BC under both the joint secrecy criterion and the individual secrecy criterion. We then highlight that the established regions recover the capacity regions of the degraded two-receiver wiretap BC for both secrecy criteria. Finally, we compare the two established rate regions under the joint and individual secrecy constraints showing that there are some scenarios, in which the individual secrecy rate region outperforms the joint secrecy one.

### A. The Joint Secrecy Rate Region

The general two-receiver wiretap BC was first investigated under the joint secrecy constraint in [11]. The authors established a general rate region in [11, Theorem 1] by adapting the classical technique of Marton coding introduced in [35] to the two-receiver wiretap BC. The main issue of the region given therein is that it fails to recover the joint secrecy capacity region of the degraded two-receiver wiretap BC, where the optimal coding strategy is superposition encoding. This implies that in order to provide a better achievable rate region for the general two-receiver wiretap BC, we need to use a coding scheme that combines both Marton coding and superposition encoding. This agrees with the result presented in [36, 37] that, Marton coding is in general not optimal without a superposition variable. With this in mind, we provide the following rate region:

**Theorem 5.** *An achievable joint secrecy rate region for the two-receiver wiretap BC is given by the set of all rate pairs $(R_1, R_2) \in \mathbb{R}_+^2$ that satisfy*

$$\begin{aligned}
R_1 &\leq \mathbb{I}(\mathrm{V}_0\mathrm{V}_1;\mathrm{Y}_1) - \mathbb{I}(\mathrm{V}_0\mathrm{V}_1;\mathrm{Z})\\
R_2 &\leq \mathbb{I}(\mathrm{V}_0\mathrm{V}_2;\mathrm{Y}_2) - \mathbb{I}(\mathrm{V}_0\mathrm{V}_2;\mathrm{Z})\\
R_1+R_2 &\leq \mathbb{I}(\mathrm{V}_0\mathrm{V}_1;\mathrm{Y}_1) + \mathbb{I}(\mathrm{V}_0\mathrm{V}_2;\mathrm{Y}_2) - \mathbb{I}(\mathrm{V}_0;\mathrm{Z}) - R_{\mathrm{CE}}\\
R_1+R_2 &\leq \mathbb{I}(\mathrm{V}_0\mathrm{V}_1;\mathrm{Y}_1) + \mathbb{I}(\mathrm{V}_2;\mathrm{Y}_2|\mathrm{V}_0) - R_{\mathrm{CE}}\\
R_1+R_2 &\leq \mathbb{I}(\mathrm{V}_1;\mathrm{Y}_1|\mathrm{V}_0) + \mathbb{I}(\mathrm{V}_0\mathrm{V}_2;\mathrm{Y}_2) - R_{\mathrm{CE}}
\end{aligned} \tag{37}$$

*where $R_{\mathrm{CE}} = \max\big[\mathbb{I}(\mathrm{V}_0\mathrm{V}_1;\mathrm{Z}) + \mathbb{I}(\mathrm{V}_2;\mathrm{Z}|\mathrm{V}_0), \mathbb{I}(\mathrm{V}_0\mathrm{V}_2;\mathrm{Z}) + \mathbb{I}(\mathrm{V}_1;\mathrm{Z}|\mathrm{V}_0), \mathbb{I}(\mathrm{V}_0\mathrm{V}_1\mathrm{V}_2;\mathrm{Z}) + \mathbb{I}(\mathrm{V}_1;\mathrm{V}_2|\mathrm{V}_0)\big]$. The random variables that define the previous region are characterized by the following joint distribution $Q(v_0)\,Q(v_1,v_2|v_0)\,Q(x|v_1,v_2)\,Q(y_1,y_2,z|x)$, i.e., $\mathrm{V}_0 - (\mathrm{V}_1,\mathrm{V}_2) - \mathrm{X} - (\mathrm{Y}_1,\mathrm{Y}_2,\mathrm{Z})$.*

**Remark 4.** *One can show that, the rate constraints in* (37) *simplify to the ones in* (8)*, if we let $\mathrm{V}_0 = \mathrm{V}_2 = \mathrm{U}$ and $\mathrm{V}_1 = \mathrm{X}$. This implies that the joint secrecy rate region established in Theorem 5 recovers the joint secrecy capacity region of the two-receiver degraded wiretap BC given in Proposition 1*

*Proof:* The proof combines the principle of Marton coding with a superposition variable for wiretap encoding as in [38], in addition to the usage of strong secrecy techniques described in [31–33].

**1. Message sets:** We consider the following sets: Two sets of confidential messages $\mathcal{M}_1$ and $\mathcal{M}_2$, three sets of randomization messages for secrecy $\mathcal{M}_r$, $\mathcal{M}_{r_1}$ and $\mathcal{M}_{r_2}$, and finally two additional sets $\mathcal{M}_{t_1}$ and $\mathcal{M}_{t_2}$ needed for the construction of Marton coding, where any message set is of the form $\mathcal{M}_a = [\![1, 2^{nR_a}]\!]$. Additionally we divide each confidential

message into two parts as follows: $\mathcal{M}_1 = \mathcal{M}_{11} \times \mathcal{M}_{12}$ and $\mathcal{M}_2 = \mathcal{M}_{21} \times \mathcal{M}_{22}$. Based up on this structure, we have

$$R_1 = R_{11} + R_{12} \quad \text{and} \quad R_2 = R_{21} + R_{22}. \tag{38}$$

The aim of this division is to use $\mathcal{M}_{11}$ and $\mathcal{M}_{21}$ to play the role of a common confidential message, which both legitimate receivers have to decode, while $\mathcal{M}_{12}$ and $\mathcal{M}_{22}$ are the actual individual confidential messages which are only decoded by the intended receiver. This principle is motivated by the combination of Marton coding and superposition encoding.

**2. Random Codebook $\mathcal{C}_n^J$:** Fix an input distribution $Q(v_0, v_1, v_2, x)$. Construct the codewords $v_0^n(m_0)$, where $m_0 = (m_{11}, m_{21}, m_r)$ by generating the symbols $v_{0i}(m_0)$ independently at random according to $Q(v_0)$. Next, for each $v_0^n(m_0)$ generate the codewords $v_1^n(m_0, m_{12}, m_{r_1}, m_{t_1})$ and $v_2^n(m_0, m_{22}, m_{r_2}, m_{t_2})$ by generating symbols $v_{1i}(m_0, m_{12}, m_{r_1}, m_{t_1})$ and $v_{2i}(m_0, m_{22}, m_{r_2}, m_{t_2})$ independently at random according to $Q(v_1|v_{0i}(m_0))$ and $Q(v_2|v_{0i}(m_0))$ respectively. This agrees with the fact that $(m_{11}, m_{21})$ simulate a common confidential message, so they are encoded in the superposition variable $v_0$. On the other hand, $m_{12}$ and $m_{22}$ are encoded in the Marton coding variables $v_1$ and $v_2$ as they represent the individual confidential messages for the first and second legitimate receivers respectively.

**3. Encoder $E$:** Given a message pair $(m_1, m_2)$, where $m_1 = (m_{11}, m_{12})$ and $m_2 = (m_{21}, m_{22})$, the transmitter chooses three randomization messages $m_r$, $m_{r_1}$ and $m_{r_2}$ uniformly at random from the sets $\mathcal{M}_r$, $\mathcal{M}_{r_1}$ and $\mathcal{M}_{r_2}$ respectively. Then, it finds a pair $(m_{t_1}, m_{t_2})$ such that $v_1^n(m_0, m_{12}, m_{r_1}, m_{t_1})$ and $v_2^n(m_0, m_{22}, m_{r_2}, m_{t_2})$ are jointly typical. According to Marton coding technique [35], with high probability such pair exists if

$$R_{t_1} + R_{t_2} > \mathbb{I}(\mathrm{V}_1; \mathrm{V}_2|\mathrm{V}_0). \tag{39}$$

Finally, the encoder generates a codeword $x^n$ independently at random according to $\prod_{i=1}^n Q(x_i|v_{1i}, v_{2i})$ and transmits it.

**4. First Legitimate Decoder $\varphi_1$:** Given $y_1^n$, it outputs $\hat{m}_1 = (\hat{m}_{11}, \hat{m}_{12})$ by finding the unique messages $(\hat{m}_0, \hat{m}_{12}, \hat{m}_{r_1}, \hat{m}_{t_1})$, where $\hat{m}_0 = (\hat{m}_{11}, \hat{m}_{21}, \hat{m}_r)$ such that, $v_0^n(\hat{m}_0)$, $v_1^n(\hat{m}_0, \hat{m}_{12}, \hat{m}_{r_1}, \hat{m}_{t_1})$ and $y_1^n$ are jointly typical. Otherwise declares an error.

**5. Second Legitimate Decoder $\varphi_2$:** Given $y_2^n$, it outputs $\tilde{m}_2 = (\tilde{m}_{21}, \tilde{m}_{22})$ by finding the unique messages $(\tilde{m}_0, \tilde{m}_{22}, \tilde{m}_{r_2}, \tilde{m}_{t_2})$, where $\tilde{m}_0 = (\tilde{m}_{11}, \tilde{m}_{21}, \tilde{m}_r)$ such that $v_0^n(\tilde{m}_0)$, $v_2^n(\tilde{m}_0, \tilde{m}_{22}, \tilde{m}_{r_2}, \tilde{m}_{t_2})$ and $y_2^n$ are jointly typical. Otherwise declares an error.

**7. Reliability Analysis:** We define the average error probability of this scheme as

$$\begin{aligned}\hat{P}_e(\mathcal{C}_n^J) \triangleq \mathbb{P}\big[&(\hat{\mathrm{M}}_{11}, \hat{\mathrm{M}}_{21}, \hat{\mathrm{M}}_{12}, \hat{\mathrm{M}}_r, \hat{\mathrm{M}}_{r_1}, \hat{\mathrm{M}}_{t_1}) \\ &\neq (\mathrm{M}_{11}, \mathrm{M}_{21}, \mathrm{M}_{12}, \mathrm{M}_r, \mathrm{M}_{r_1}, \mathrm{M}_{t_1}) \\ &\text{or } (\tilde{\mathrm{M}}_{11}, \tilde{\mathrm{M}}_{21}, \tilde{\mathrm{M}}_{22}, \tilde{\mathrm{M}}_r, \tilde{\mathrm{M}}_{r_2}, \tilde{\mathrm{M}}_{t_2}) \\ &\neq (\mathrm{M}_{11}, \mathrm{M}_{21}, \mathrm{M}_{22}, \mathrm{M}_r, \mathrm{M}_{r_2}, \mathrm{M}_{t_2})\big].\end{aligned}$$

We then observe that $\hat{P}_e(\mathcal{C}_n^J) \geq P_e(\mathcal{C}_n)$, cf. (2). Now according to our encoding and decoding procedure, the average error probability $\hat{P}_e(\mathcal{C}_n^J)$ can be expressed as the union of the following error events:

$$\begin{aligned}
\text{a)}\ \mathcal{E}_{11} :&(\hat{\mathrm{M}}_{11}, \hat{\mathrm{M}}_{21}, \hat{\mathrm{M}}_r) \neq (\mathrm{M}_{11}, \mathrm{M}_{21}, \mathrm{M}_r), \\
&(\hat{\mathrm{M}}_{12}, \hat{\mathrm{M}}_{r_1}, \hat{\mathrm{M}}_{t_1}) = (\mathrm{M}_{12}, \mathrm{M}_{r_1}, \mathrm{M}_{t_1}). \\
\text{b)}\ \mathcal{E}_{12} :&(\hat{\mathrm{M}}_{11}, \hat{\mathrm{M}}_{21}, \hat{\mathrm{M}}_r) = (\mathrm{M}_{11}, \mathrm{M}_{21}, \mathrm{M}_r), \\
&(\hat{\mathrm{M}}_{12}, \hat{\mathrm{M}}_{r_1}, \hat{\mathrm{M}}_{t_1}) \neq (\mathrm{M}_{12}, \mathrm{M}_{r_1}, \mathrm{M}_{t_1}). \\
\text{c)}\ \mathcal{E}_{13} :&(\hat{\mathrm{M}}_{11}, \hat{\mathrm{M}}_{21}, \hat{\mathrm{M}}_r) \neq (\mathrm{M}_{11}, \mathrm{M}_{21}, \mathrm{M}_r), \\
&(\hat{\mathrm{M}}_{12}, \hat{\mathrm{M}}_{r_1}, \hat{\mathrm{M}}_{t_1}) \neq (\mathrm{M}_{12}, \mathrm{M}_{r_1}, \mathrm{M}_{t_1}). \\
\text{d)}\ \mathcal{E}_{21} :&(\tilde{\mathrm{M}}_{11}, \tilde{\mathrm{M}}_{21}, \tilde{\mathrm{M}}_r) \neq (\mathrm{M}_{11}, \mathrm{M}_{21}, \mathrm{M}_r), \\
&(\tilde{\mathrm{M}}_{22}, \tilde{\mathrm{M}}_{r_2}, \tilde{\mathrm{M}}_{t_2}) = (\mathrm{M}_{22}, \mathrm{M}_{r_2}, \mathrm{M}_{t_2}). \\
\text{e)}\ \mathcal{E}_{22} :&(\tilde{\mathrm{M}}_{11}, \tilde{\mathrm{M}}_{21}, \tilde{\mathrm{M}}_r) = (\mathrm{M}_{11}, \mathrm{M}_{21}, \mathrm{M}_r), \\
&(\tilde{\mathrm{M}}_{22}, \tilde{\mathrm{M}}_{r_2}, \tilde{\mathrm{M}}_{t_2}) \neq (\mathrm{M}_{22}, \mathrm{M}_{r_2}, \mathrm{M}_{t_2}). \\
\text{f)}\ \mathcal{E}_{23} :&(\tilde{\mathrm{M}}_{11}, \tilde{\mathrm{M}}_{21}, \tilde{\mathrm{M}}_r) \neq (\mathrm{M}_{11}, \mathrm{M}_{21}, \mathrm{M}_r), \\
&(\tilde{\mathrm{M}}_{22}, \tilde{\mathrm{M}}_{r_2}, \tilde{\mathrm{M}}_{t_2}) \neq (\mathrm{M}_{22}, \mathrm{M}_{r_2}, \mathrm{M}_{t_2}).
\end{aligned}$$

Let us consider the first error event $\mathcal{E}_{11}$ and assume that the following messages $(m_{11}, m_{21}, m_r, m_{12}, m_{r_1}, m_{t_1})$ were selected for transmission. Based on the structure of the codebook in addition to the definitions of the encoder and first legitimate decoder, this error event will happen if one of the following conditions occurs:

1. The sequences $v_0^n(m_{11}, m_{21}, m_r)$ and $v_1^n(m_{11}, m_{21}, m_r, m_{12}, m_{r_1}, m_{t_1})$ produced by the encoder are not jointly typical with the received $y_1^n$.
2. There exists a message tuple $(\bar{m}_{11}, \bar{m}_{21}, \bar{m}_r) \neq (m_{11}, m_{21}, m_r)$, such that $v_0^n(\bar{m}_{11}, \bar{m}_{21}, \bar{m}_r)$, $v_1^n(\bar{m}_{11}, \bar{m}_{21}, \bar{m}_r, m_{12}, m_{r_1}, m_{t_1})$ and $y_1^n$ are jointly typical.

According to the properties of typical sequences, for a sufficiently large $n$ and some constant $\alpha > 0$ such that, $\epsilon_n = 2^{-\alpha n}$, the probability of the first condition is always less than $\epsilon_n$. On the other hand, the probability of the second condition is less than $\epsilon_n$, if the condition in (40a) holds.

Now, applying this error analysis procedure to all the previous error events, we can show that for a sufficiently large $n$ , the probability of each of these events is less than $\epsilon_n$, if

$$\begin{aligned}
R_{11}+R_{21}+R_r &\leq \mathbb{I}(\mathrm{V}_0\mathrm{V}_1; \mathrm{Y}_1) - \delta_n(\epsilon_n) && \text{(40a)}\\
R_{12}+R_{r_1}+R_{t_1} &\leq \mathbb{I}(\mathrm{V}_1; \mathrm{Y}_1|\mathrm{V}_0) - \delta_n(\epsilon_n) && \text{(40b)}\\
R_1+R_{21}+R_r+R_{r_1}+R_{t_1} &\leq \mathbb{I}(\mathrm{V}_0\mathrm{V}_1; \mathrm{Y}_1) - \delta_n(\epsilon_n) && \text{(40c)}\\
R_{11}+R_{21}+R_r &\leq \mathbb{I}(\mathrm{V}_0\mathrm{V}_2; \mathrm{Y}_2) - \delta_n(\epsilon_n) && \text{(40d)}\\
R_{22}+R_{r_2}+R_{t_2} &\leq \mathbb{I}(\mathrm{V}_2; \mathrm{Y}_2|\mathrm{V}_0) - \delta_n(\epsilon_n) && \text{(40e)}\\
R_2+R_{11}+R_r+R_{r_2}+R_{t_2} &\leq \mathbb{I}(\mathrm{V}_0\mathrm{V}_2; \mathrm{Y}_2) - \delta_n(\epsilon_n), && \text{(40f)}
\end{aligned}$$

where $\delta_n(\epsilon_n) \to 0$ as $n \to \infty$. Each rate constraint in (40) guarantees that the probability of a corresponding error event is less than $\epsilon_n$. It is important to note that the constraints in (40a) and (40d) can be ignored as they are included in the ones in (40c) and (40f). Another important point is that in calculating the average error probability $\hat{P}_e(\mathcal{C}_n^J)$, we ignored the events where the sequences $v_0^n$, $v_1^n$, $v_2^n$ and $x^n$ being atypical sequences, because according to the properties

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2016.2566260, IEEE Transactions on Information Forensics and Security



of typical sequences, the probability of such events for a sufficiently large $n$ is small as well.

**8. Secrecy Analysis:** For our secrecy analysis, we adapted some of the strong secrecy techniques in [31–33], which are related to the concept of resolvability to the Marton coding technique as in [39]. We start by identifying all the virtual channels that exist between the confidential messages and the eavesdropper. Based on the codebook structure, we can define six possible channels as follow: $\mathrm{Q}_1 : \mathcal{V}_0 \to \mathcal{P}(\mathcal{Z})$, $\mathrm{Q}_2 : \mathcal{V}_0 \times \mathcal{V}_1 \to \mathcal{P}(\mathcal{Z})$, $\mathrm{Q}_3 : \mathcal{V}_1 \to \mathcal{P}(\mathcal{Z})$, $\mathrm{Q}_4 : \mathcal{V}_0 \times \mathcal{V}_2 \to \mathcal{P}(\mathcal{Z})$, $\mathrm{Q}_5 : \mathcal{V}_2 \to \mathcal{P}(\mathcal{Z})$, and $\mathrm{Q}_6 : \mathcal{V}_0 \times \mathcal{V}_1 \times \mathcal{V}_2 \to \mathcal{P}(\mathcal{Z})$. According to [32, 33], in order to fulfill the joint strong secrecy criterion in (4), we need to make sure that the randomization rate in the input sequence to each of these virtual channels is at least equivalent to the mutual information between the channel input and the eavesdropper. Thus, for a sufficiently large $n$ and some constant $\beta > 0$ such that, $\tau_n = 2^{-\beta n}$, the joint secrecy constraints given in (4) are with high probability smaller than $\tau_n$, if

$$\begin{aligned}
R_r &\geq \mathbb{I}(\mathrm{V}_0;\mathrm{Z}) + \delta_n(\tau_n)\\
R_r + R_{r_1} + R_{t_1} &\geq \mathbb{I}(\mathrm{V}_0\mathrm{V}_1;\mathrm{Z}) + \delta_n(\tau_n)\\
R_{r_1} + R_{t_1} &\geq \mathbb{I}(\mathrm{V}_1;\mathrm{Z}|\mathrm{V}_0) + \delta_n(\tau_n)\\
R_r + R_{r_2} + R_{t_2} &\geq \mathbb{I}(\mathrm{V}_0\mathrm{V}_2;\mathrm{Z}) + \delta_n(\tau_n)\\
R_{r_2} + R_{t_2} &\geq \mathbb{I}(\mathrm{V}_2;\mathrm{Z}|\mathrm{V}_0) + \delta_n(\tau_n)\\
R_r + R_{r_1} + R_{r_2} &\geq \mathbb{I}(\mathrm{V}_0\mathrm{V}_1\mathrm{V}_2;\mathrm{Z}) + \delta_n(\tau_n). \qquad (41)
\end{aligned}$$

It is important to note that, although $R_{t_1}$ is considered as part of the randomization index for channels $(\mathrm{Q}_2, \mathrm{Q}_3)$, and $R_{t_2}$ is considered as part of the randomization index for channels $(\mathrm{Q}_4, \mathrm{Q}_5)$, neither $R_{t_1}$ nor $R_{t_2}$ plays a role in the randomization index of channel $\mathrm{Q}_6$. This is due to the structure of Marton coding.

Now, if we combine (39), (40) and (41), and let $R_{11} = R_{21} = 0$, then apply the Fourier-Motzkin elimination procedure, followed by taking the limit as $n \to \infty$, which implies that $\delta_n(\epsilon_n)$ and $\delta_n(\tau_n) \to 0$, we prove the achievability of any rate pair $(R_1, R_2)$ satisfying (37). ■

Marton coding with a superposition variable was first introduced in [40] to establish an achievable rate region for the two-receiver BC with a common message and two private messages. The idea was to use the superposition variable $\mathrm{V}_0$ to encode the common message, while the two private messages are encoded using the classical Marton coding in $\mathrm{V}_1$ and $\mathrm{V}_2$. In [36], it was shown that even for the two-receiver BC without a common message, $\mathrm{V}_0$ is still needed to provide a more general coding scheme than the classical Marton coding. This result also holds to our scenario as follows: Although we let $R_{11} = R_{21} = 0$, which implies that $\mathrm{V}_0$ does not carry any information, we still need $\mathrm{V}_0$ and without it we can not show that the rate region established in Theorem 5 includes the joint secrecy capacity region of the degraded two-receiver wiretap BC. This implies that $\mathrm{V}_0$ can be interpreted as a virtual common layer that assures the optimality of our coding scheme for the scenarios, where superposition encoding is needed.

### *B. The Individual Secrecy Rate Region*

In order to establish an achievable rate region for the general two-receiver wiretap BC under the individual secrecy criterion, we need to make use of the fact that individual secrecy allows the usage of the whole or a part of the individual message of one user as a secret key for the other user. Since secret key encoding requires that the key is secretly shared between the transmitter and the receiver, the first user must find a way to acquire a full knowledge about the part of the message of the second user used as secret key. This can be done by possessing a prior knowledge about the second user's message as in BC with receiver side information [15–18] or by obtaining this information from its channel observation. Since, we do not have any prior side information at the receivers, we need to use the second method. With this in mind, we present the following rate region:

**Theorem 6.** *An achievable individual secrecy rate region for the two-receiver wiretap BC is given by the set of all rate pairs* $(R_1 = R_{11} + R_{12}, R_2 = R_{21} + R_{22}) \in \mathbb{R}_+^2$ *that satisfy*

$$\begin{aligned}
R_1 + R_{21} &\leq \mathbb{I}(\mathrm{V}_0\mathrm{V}_1;\mathrm{Y}_1) - \mathbb{I}(\mathrm{V}_0\mathrm{V}_1;\mathrm{Z})\\
&\quad + \min\Big[R_{21}, \mathbb{I}(\mathrm{V}_0\mathrm{V}_1;\mathrm{Z})\Big]\\
R_2 + R_{11} &\leq \mathbb{I}(\mathrm{V}_0\mathrm{V}_2;\mathrm{Y}_2) - \mathbb{I}(\mathrm{V}_0\mathrm{V}_2;\mathrm{Z})\\
&\quad + \min\Big[R_{11}, \mathbb{I}(\mathrm{V}_0\mathrm{V}_2;\mathrm{Z})\Big]\\
R_1 + R_2 &\leq \mathbb{I}(\mathrm{V}_0\mathrm{V}_1;\mathrm{Y}_1) + \mathbb{I}(\mathrm{V}_2;\mathrm{Y}_2|\mathrm{V}_0) - R_{\mathrm{CE}}\\
&\quad + \min\Big[R_{\mathrm{CE}} - \mathbb{I}(\mathrm{V}_1;\mathrm{V}_2|\mathrm{V}_0),\ R_{11} + R_{12}\Big]\\
R_1 + R_2 &\leq \mathbb{I}(\mathrm{V}_1;\mathrm{Y}_1|\mathrm{V}_0) + \mathbb{I}(\mathrm{V}_0\mathrm{V}_2;\mathrm{Y}_2) - R_{\mathrm{CE}}\\
&\quad + \min\Big[R_{\mathrm{CE}} - \mathbb{I}(\mathrm{V}_1;\mathrm{V}_2|\mathrm{V}_0),\ R_{11} + R_{12}\Big]\\
R_1 + R_2 + R_{11} + R_{12} &\leq \mathbb{I}(\mathrm{V}_0\mathrm{V}_1;\mathrm{Y}_1) + \mathbb{I}(\mathrm{V}_0\mathrm{V}_2;\mathrm{Y}_2) - R_{\mathrm{CE}}\\
-\mathbb{I}(\mathrm{V}_0;\mathrm{Z}) &+ \min\Big[R_{\mathrm{CE}} - \mathbb{I}(\mathrm{V}_1;\mathrm{V}_2|\mathrm{V}_0),\ R_{11} + R_{12}\Big] \qquad (42)
\end{aligned}$$

*where* $R_{\mathrm{CE}}$ *is as defined in Theorem 5. The random variables that define the previous region are characterized by the following joint distribution* $Q(v_0)\ Q(v_1, v_2|v_0)\ Q(x|v_1, v_2)\ Q(y_1, y_2, z|x)$*, i.e.,* $\mathrm{V}_0 - (\mathrm{V}_1, \mathrm{V}_2) - \mathrm{X} - (\mathrm{Y}_1, \mathrm{Y}_2, \mathrm{Z})$.

**Remark 5.** *It can be shown that, the rate constraints in* (42) *simplify to the ones in* (9)*, if we set* $R_{11} = 0$*,* $\mathrm{V}_0 = \mathrm{V}_2 = \mathrm{U}$ *and* $\mathrm{V}_1 = \mathrm{X}$*. This implies that the individual secrecy rate region established in Theorem 6 recovers the individual secrecy capacity region of the two-receiver degraded wiretap BC given in Proposition 2*

*Proof:* The proof combines the techniques used in establishing the achievable joint secrecy region, in addition to one time pad encoding for Shannon's cipher system [3].

**1. Message sets:** We consider the same message sets used in the proof of Theorem 5. However, we divide each confidential message into three parts as follows: $\mathcal{M}_1 = \mathcal{M}_{11} \times \mathcal{M}_{12} \times \mathcal{M}_{13}$ and $\mathcal{M}_2 = \mathcal{M}_{21} \times \mathcal{M}_{22} \times \mathcal{M}_{23}$. In this division, we force $\mathcal{M}_{13}$ and $\mathcal{M}_{21}$ to be of the same size and use them to construct $\mathcal{M}_{\otimes_1}$ by *Xoring* the corresponding elements of both sets. We also force $\mathcal{M}_{23}$ and $\mathcal{M}_{11}$ to be of the same size and use them to construct $\mathcal{M}_{\otimes_2}$ using the same procedure.

Finally we divide the two *Xored* message sets into two parts as follows: $\mathcal{M}_{\otimes_1} = \mathcal{M}_{\otimes_{11}} \times \mathcal{M}_{\otimes_{12}}$ and $\mathcal{M}_{\otimes_2} = \mathcal{M}_{\otimes_{21}} \times \mathcal{M}_{\otimes_{22}}$. Based on this structure, we have

$$\begin{aligned} R_1 = R_{11} + R_{12} + R_{13} \quad \text{and} \quad R_2 = R_{21} + R_{22} + R_{23} \\ R_{\otimes_1} = R_{13} = R_{21} = R_{\otimes_{11}} + R_{\otimes_{12}} \\ R_{\otimes_2} = R_{23} = R_{11} = R_{\otimes_{21}} + R_{\otimes_{22}}. \end{aligned} \tag{43}$$

The previous message structure serves our coding scheme as follows: As in Theorem 5, $\mathcal{M}_{11}$ and $\mathcal{M}_{21}$ represent a common confidential message. However, in this theorem, they play an additional role as well. $\mathcal{M}_{21}$ acts as secret keys for the first legitimate receiver, while $\mathcal{M}_{11}$ acts as secret keys for the second legitimate receiver. On the other hand, $\mathcal{M}_{12}$ and $\mathcal{M}_{13}$ represent the individual confidential message intended for the first legitimate receiver, where $\mathcal{M}_{12}$ is the part of the message protected by wiretap random coding, while $\mathcal{M}_{13}$ is the part of the message protected by secret key encoding. The same holds for $\mathcal{M}_{22}$ and $\mathcal{M}_{23}$, which represent the individual confidential message intended for the second legitimate receiver.

**2. Random Codebook $\mathcal{C}_n^I$:** Fix an input distribution $Q(v_0, v_1, v_2, x)$. Construct the codewords $v_0^n(m_0)$, where $m_0 = (m_{11}, m_{21}, m_r, m_{\otimes_{11}}, m_{\otimes_{21}})$ by generating the symbols $v_{0i}(m_0)$ independently at random according to $Q(v_0)$. Next, for each $v_0^n(m_0)$ generate the codewords $v_1^n(m_0, m_{12}, m_{r_1}, m_{\otimes_{12}}, m_{t_1})$ and $v_2^n(m_0, m_{22}, m_{r_2}, m_{\otimes_{22}}, m_{t_2})$ by generating the symbols $v_{1i}(m_0, m_{12}, m_{r_1}, m_{\otimes_{12}}, m_{t_1})$ and $v_{2i}(m_0, m_{22}, m_{r_2}, m_{\otimes_{22}}, m_{t_2})$ independently at random according to $Q(v_1|v_{0i}(m_0))$ and $Q(v_2|v_{0i}(m_0))$ respectively.

**3. Encoder $E$:** Given a message pair $(m_1, m_2)$, where $m_1 = (m_{11}, m_{12}, m_{13})$ and $m_2 = (m_{21}, m_{22}, m_{23})$, it first calculates the *Xored* messages $(m_{\otimes_{11}}, m_{\otimes_{21}}, m_{\otimes_{12}}, m_{\otimes_{22}})$, then chooses three randomization messages $m_r$, $m_{r_1}$ and $m_{r_2}$ uniformly at random from the sets $\mathcal{M}_r$, $\mathcal{M}_{r_1}$ and $\mathcal{M}_{r_2}$ respectively. Then, it finds a pair $(m_{t_1}, m_{t_2})$, such that $v_1^n(m_0, m_{12}, m_{r_1}, m_{\otimes_{12}}, m_{t_1})$ and $v_2^n(m_0, m_{22}, m_{r_2}, m_{\otimes_{21}}, m_{t_2})$ are jointly typical. According to Marton coding technique [35], with high probability such pair exists if

$$R_{t_1} + R_{t_2} > \mathbb{I}(\mathrm{V}_1; \mathrm{V}_2|\mathrm{V}_0). \tag{44}$$

Finally, it generates a codeword $x^n$ independently at random according to $\prod_{i=1}^n Q(x_i|v_{1i}, v_{2i})$ and transmits it.

**4. First Legitimate Decoder $\varphi_1$:** Given $y_1^n$, it outputs $\hat{m}_1 = (\hat{m}_{11}, \hat{m}_{12}, \hat{m}_{13})$. First, it finds the unique messages $(\hat{m}_0, \hat{m}_{12}, \hat{m}_{r_1}, \hat{m}_{\otimes_{12}}, \hat{m}_{t_1})$, where $\hat{m}_0 = (\hat{m}_{11}, \hat{m}_{21}, \hat{m}_r, \hat{m}_{\otimes_{11}}, \hat{m}_{\otimes_{21}})$ such that, $v_0^n(\hat{m}_0)$, $v_1^n(\hat{m}_0, \hat{m}_{12}, \hat{m}_{r_1}, \hat{m}_{\otimes_{12}}, \hat{m}_{t_1})$ and $y_1^n$ are jointly typical. Then, it estimates $\hat{m}_{13}$ by *Xoring* $\hat{m}_{21}$ and $\hat{m}_{\otimes_1} = (\hat{m}_{\otimes_{11}}, \hat{m}_{\otimes_{12}})$. If one of the previous two steps fails, it declares an error.

**5. Second Legitimate Decoder $\varphi_2$:** Given $y_2^n$, it outputs $\tilde{m}_2 = (\tilde{m}_{21}, \tilde{m}_{22}, \tilde{m}_{23})$. First, it finds the unique messages $(\tilde{m}_0, \tilde{m}_{22}, \tilde{m}_{r_2}, \tilde{m}_{\otimes_{22}}, \tilde{m}_{t_2})$, where $\tilde{m}_0 = (\tilde{m}_{11}, \tilde{m}_{21}, \tilde{m}_r, \tilde{m}_{\otimes_{11}}, \tilde{m}_{\otimes_{21}})$ such that $v_0^n(\tilde{m}_0)$, $v_2^n(\tilde{m}_0, \tilde{m}_{22}, \tilde{m}_{r_2}, \tilde{m}_{\otimes_{22}}, \tilde{m}_{t_2})$ and $y_2^n$ are jointly typical. Then, it estimates $\tilde{m}_{23}$ by *Xoring* $\tilde{m}_{11}$ and $\tilde{m}_{\otimes_2} = (\tilde{m}_{\otimes_{21}}, \tilde{m}_{\otimes_{22}})$. If one of the previous two steps fails, it declares an error.

**7. Reliability Analysis:** We define the average error probability of this scheme as

$$\begin{aligned} \ddot{P}_e(\mathcal{C}_n^I) \triangleq \mathbb{P}\big[&(\hat{\mathrm{M}}_{11}, \hat{\mathrm{M}}_{12}, \hat{\mathrm{M}}_{21}, \hat{\mathrm{M}}_{\otimes_1}, \hat{\mathrm{M}}_{\otimes_{21}}, \hat{\mathrm{M}}_r, \hat{\mathrm{M}}_{r_1}, \hat{\mathrm{M}}_{t_1}) \\ &\neq (\mathrm{M}_{11}, \mathrm{M}_{12}, \mathrm{M}_{21}, \mathrm{M}_{\otimes_1}, \mathrm{M}_{\otimes_{21}}, \mathrm{M}_r, \mathrm{M}_{r_1}, \mathrm{M}_{t_1}) \\ &\text{or } (\tilde{\mathrm{M}}_{11}, \tilde{\mathrm{M}}_{21}, \tilde{\mathrm{M}}_{22}, \tilde{\mathrm{M}}_{\otimes_{11}}, \tilde{\mathrm{M}}_{\otimes_2}, \tilde{\mathrm{M}}_r, \tilde{\mathrm{M}}_{r_2}, \tilde{\mathrm{M}}_{t_2}) \\ &\neq (\mathrm{M}_{11}, \mathrm{M}_{21}, \mathrm{M}_{22}, \mathrm{M}_{\otimes_{11}}, \mathrm{M}_{\otimes_2}, \mathrm{M}_r, \mathrm{M}_{r_2}, \mathrm{M}_{t_2})\big]. \end{aligned}$$

We then observe that $\ddot{P}_e(\mathcal{C}_n^I) \geq P_e(\mathcal{C}_n)$, cf. (2). Now according to our encoding and decoding procedure, the average error probability $\ddot{P}_e(\mathcal{C}_n^I)$ can be expressed as the union of the following error events:

a) $\mathcal{E}_{11}$ : $(\hat{\mathrm{M}}_{12}, \hat{\mathrm{M}}_{r_1}, \hat{\mathrm{M}}_{\otimes_{12}}, \hat{\mathrm{M}}_{t_1}) = (\mathrm{M}_{12}, \mathrm{M}_{r_1}, \mathrm{M}_{\otimes_{12}}, \mathrm{M}_{t_1})$, $(\hat{\mathrm{M}}_{11}, \hat{\mathrm{M}}_{21}, \hat{\mathrm{M}}_r, \hat{\mathrm{M}}_{\otimes_{11}}, \hat{\mathrm{M}}_{\otimes_{21}}) \neq (\mathrm{M}_{11}, \mathrm{M}_{21}, \mathrm{M}_r, \mathrm{M}_{\otimes_{11}}, \mathrm{M}_{\otimes_{21}})$

b) $\mathcal{E}_{12}$ : $(\hat{\mathrm{M}}_{12}, \hat{\mathrm{M}}_{r_1}, \hat{\mathrm{M}}_{\otimes_{12}}, \hat{\mathrm{M}}_{t_1}) \neq (\mathrm{M}_{12}, \mathrm{M}_{r_1}, \mathrm{M}_{\otimes_{12}}, \mathrm{M}_{t_1})$, $(\hat{\mathrm{M}}_{11}, \hat{\mathrm{M}}_{21}, \hat{\mathrm{M}}_r, \hat{\mathrm{M}}_{\otimes_{11}}, \hat{\mathrm{M}}_{\otimes_{21}}) = (\mathrm{M}_{11}, \mathrm{M}_{21}, \mathrm{M}_r, \mathrm{M}_{\otimes_{11}}, \mathrm{M}_{\otimes_{21}})$

c) $\mathcal{E}_{13}$ : $(\hat{\mathrm{M}}_{12}, \hat{\mathrm{M}}_{r_1}, \hat{\mathrm{M}}_{\otimes_{12}}, \hat{\mathrm{M}}_{t_1}) \neq (\mathrm{M}_{12}, \mathrm{M}_{r_1}, \mathrm{M}_{\otimes_{12}}, \mathrm{M}_{t_1})$, $(\hat{\mathrm{M}}_{11}, \hat{\mathrm{M}}_{21}, \hat{\mathrm{M}}_r, \hat{\mathrm{M}}_{\otimes_{11}}, \hat{\mathrm{M}}_{\otimes_{21}}) \neq (\mathrm{M}_{11}, \mathrm{M}_{21}, \mathrm{M}_r, \mathrm{M}_{\otimes_{11}}, \mathrm{M}_{\otimes_{21}})$

d) $\mathcal{E}_{21}$ : $(\tilde{\mathrm{M}}_{22}, \tilde{\mathrm{M}}_{r_2}, \tilde{\mathrm{M}}_{\otimes_{22}}, \tilde{\mathrm{M}}_{t_2}) = (\mathrm{M}_{22}, \mathrm{M}_{r_2}, \mathrm{M}_{\otimes_{22}}, \mathrm{M}_{t_2})$, $(\tilde{\mathrm{M}}_{11}, \tilde{\mathrm{M}}_{21}, \tilde{\mathrm{M}}_r, \tilde{\mathrm{M}}_{\otimes_{11}}, \tilde{\mathrm{M}}_{\otimes_{21}}) \neq (\mathrm{M}_{11}, \mathrm{M}_{21}, \mathrm{M}_r, \mathrm{M}_{\otimes_{11}}, \mathrm{M}_{\otimes_{21}})$

e) $\mathcal{E}_{22}$ : $(\tilde{\mathrm{M}}_{22}, \tilde{\mathrm{M}}_{r_2}, \tilde{\mathrm{M}}_{\otimes_{22}}, \tilde{\mathrm{M}}_{t_2}) \neq (\mathrm{M}_{22}, \mathrm{M}_{r_2}, \mathrm{M}_{\otimes_{22}}, \mathrm{M}_{t_2})$, $(\tilde{\mathrm{M}}_{11}, \tilde{\mathrm{M}}_{21}, \tilde{\mathrm{M}}_r, \tilde{\mathrm{M}}_{\otimes_{11}}, \tilde{\mathrm{M}}_{\otimes_{21}}) = (\mathrm{M}_{11}, \mathrm{M}_{21}, \mathrm{M}_r, \mathrm{M}_{\otimes_{11}}, \mathrm{M}_{\otimes_{21}})$

f) $\mathcal{E}_{23}$ : $(\tilde{\mathrm{M}}_{22}, \tilde{\mathrm{M}}_{r_2}, \tilde{\mathrm{M}}_{\otimes_{22}}, \tilde{\mathrm{M}}_{t_2}) \neq (\mathrm{M}_{22}, \mathrm{M}_{r_2}, \mathrm{M}_{\otimes_{22}}, \mathrm{M}_{t_2})$, $(\tilde{\mathrm{M}}_{11}, \tilde{\mathrm{M}}_{21}, \tilde{\mathrm{M}}_r, \tilde{\mathrm{M}}_{\otimes_{11}}, \tilde{\mathrm{M}}_{\otimes_{21}}) \neq (\mathrm{M}_{11}, \mathrm{M}_{21}, \mathrm{M}_r, \mathrm{M}_{\otimes_{11}}, \mathrm{M}_{\otimes_{21}})$

Using the same error analysis procedure highlighted in the proof of Theorem 5, we can show that for a sufficiently large $n$ and some constant $\alpha > 0$ such that, $\epsilon_n = 2^{-\alpha n}$, the probability of each of the previous events is less than $\epsilon_n$ if

$$R_0 \leq \mathbb{I}(\mathrm{V}_0\mathrm{V}_1; \mathrm{Y}_1) - \delta_n(\epsilon_n) \tag{45a}$$
$$R_{12} + R_{r_1} + R_{\otimes_{12}} + R_{t_1} \leq \mathbb{I}(\mathrm{V}_1; \mathrm{Y}_1|\mathrm{V}_0) - \delta_n(\epsilon_n) \tag{45b}$$
$$R_0 + R_{12} + R_{\otimes_{12}} + R_{r_1} + R_{t_1} \leq \mathbb{I}(\mathrm{V}_0\mathrm{V}_1; \mathrm{Y}_1) - \delta_n(\epsilon_n) \tag{45c}$$
$$R_0 \leq \mathbb{I}(\mathrm{V}_0\mathrm{V}_2; \mathrm{Y}_2) - \delta_n(\epsilon_n) \tag{45d}$$
$$R_{22} + R_{r_2} + R_{\otimes_{22}} + R_{t_2} \leq \mathbb{I}(\mathrm{V}_2; \mathrm{Y}_2|\mathrm{V}_0) - \delta_n(\epsilon_n) \tag{45e}$$
$$R_0 + R_{22} + R_{\otimes_{22}} + R_{r_2} + R_{t_2} \leq \mathbb{I}(\mathrm{V}_0\mathrm{V}_2; \mathrm{Y}_2) - \delta_n(\epsilon_n), \tag{45f}$$

where $R_0 = R_{11} + R_{21} + R_r + R_{\otimes_{11}} + R_{\otimes_{21}}$ and $\delta_n(\epsilon_n) \to 0$ as $n \to \infty$. Each rate constraint in (45) guarantees that the probability of the corresponding error event is less than $\epsilon_n$. It is also obvious that the constraints in (45a) and (45d) can be ignored because the ones in (40c) and (40f) are tighter.

**8. Secrecy Analysis:** Because of the new message sets structure, the random variable $\mathrm{M}_1$ is identified as the product of three independent and uniformly distributed random variables $\mathrm{M}_{11}$, $\mathrm{M}_{12}$ and $\mathrm{M}_{13}$. This also applies to $\mathrm{M}_2$ which is the product of the three independent and uniformly distributed random variables $\mathrm{M}_{21}$, $\mathrm{M}_{22}$ and $\mathrm{M}_{23}$. Thus, the individual secrecy constraint given by (5) can be reformulated as follows:

$$\begin{aligned} \mathbb{I}(\mathrm{M}_{11}\mathrm{M}_{12}; \mathrm{Z}^n) + \mathbb{I}(\mathrm{M}_{13}; \mathrm{Z}^n|\mathrm{M}_{11}\mathrm{M}_{12}) \leq \tau_{1n} \\ \mathbb{I}(\mathrm{M}_{21}\mathrm{M}_{22}; \mathrm{Z}^n) + \mathbb{I}(\mathrm{M}_{23}; \mathrm{Z}^n|\mathrm{M}_{21}\mathrm{M}_{22}) \leq \tau_{2n}. \end{aligned} \tag{46}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2016.2566260, IEEE Transactions on Information Forensics and Security



Using the strong secrecy approaches in [31–33] as we did for the joint secrecy criterion, we can show that for a sufficiently large $n$ and some constant $\beta > 0$ such that, $\tau_n = 2^{-\beta n} \geq \max(\tau_{1n}, \tau_{2n})$, the term $\mathbb{I}(\mathrm{M}_{11}\mathrm{M}_{12}\mathrm{M}_{21}\mathrm{M}_{22}; \mathrm{Z}^n)$ is with high probability smaller than $\tau_n$, if

$$\begin{aligned}
R_r + R_{\otimes_{11}} + R_{\otimes_{21}} &\geq \mathbb{I}(\mathrm{V}_0; \mathrm{Z}) + \delta_n(\tau_n) \\
R_r + R_{\otimes_1} + R_{\otimes_{21}} + R_{r_1} + R_{t_1} &\geq \mathbb{I}(\mathrm{V}_0\mathrm{V}_1; \mathrm{Z}) + \delta_n(\tau_n) \\
R_{r_1} + R_{\otimes_{12}} + R_{t_1} &\geq \mathbb{I}(\mathrm{V}_1; \mathrm{Z}|\mathrm{V}_0) + \delta_n(\tau_n) \\
R_r + R_{\otimes_{11}} + R_{\otimes_2} + R_{r_2} + R_{t_2} &\geq \mathbb{I}(\mathrm{V}_0\mathrm{V}_2; \mathrm{Z}) + \delta_n(\tau_n) \\
R_{r_2} + R_{\otimes_{22}} + R_{t_2} &\geq \mathbb{I}(\mathrm{V}_2; \mathrm{Z}|\mathrm{V}_0) + \delta_n(\tau_n) \\
R_r + R_{\otimes_1} + R_{\otimes_2} + R_{r_1} + R_{r_2} &\geq \mathbb{I}(\mathrm{V}_0\mathrm{V}_1\mathrm{V}_2; \mathrm{Z}) + \delta_n(\tau_n),
\end{aligned} \tag{47}$$

where the *Xored* messages are considered part of the randomization index in each virtual channel between the confidential messages and the eavesdropper identified in the secrecy analysis of the joint secrecy region. Since the rate constraints in (47) guarantee that with high probability $\mathbb{I}(\mathrm{M}_{11}\mathrm{M}_{12}\mathrm{M}_{21}\mathrm{M}_{22}; \mathrm{Z}^n) \leq \tau_n$, this implies that both $\mathbb{I}(\mathrm{M}_{11}\mathrm{M}_{12}; \mathrm{Z}^n)$ and $\mathbb{I}(\mathrm{M}_{21}\mathrm{M}_{22}; \mathrm{Z}^n)$ are with high probability smaller than $\tau_n$.

On the other hand, one can show that the term $\mathbb{I}(\mathrm{M}_{13}; \mathrm{Z}^n|\mathrm{M}_{11}\mathrm{M}_{12})$ which represents the leakage of $\mathrm{M}_{13}$ to the eavesdropper given $\mathrm{M}_{11}$ and $\mathrm{M}_{12}$ vanishes as follows:

$$\begin{aligned}
\mathbb{I}(\mathrm{M}_{13}; \mathrm{Z}^n|\mathrm{M}_{11}\mathrm{M}_{12}) &\overset{(a)}{=} \mathbb{H}(\mathrm{M}_{13}) - \mathbb{H}(\mathrm{M}_{13}|\mathrm{Z}^n\mathrm{M}_{11}\mathrm{M}_{12}) \\
&\overset{(b)}{\leq} \mathbb{H}(\mathrm{M}_{13}) - \mathbb{H}(\mathrm{M}_{13}|\mathrm{M}_{\otimes_1}) \overset{(c)}{=} 0,
\end{aligned} \tag{48}$$

where $(a)$ follows because $\mathrm{M}_{13}$, $\mathrm{M}_{11}$ and $\mathrm{M}_{12}$ are independent; $(b)$ follows because the best the eavesdropper can do is to decode $\mathrm{M}_{\otimes_1}$; while $(c)$ follows because of the principle of one time pad in Shannon's cipher system where the entropy of the secret key $\mathbb{H}(\mathrm{M}_{21})$ is equal to the entropy of the transmitted message $\mathbb{H}(\mathrm{M}_{13})$. It is important to highlight here the idea that supports our analysis. In order for the eavesdropper to extract any information about $\mathrm{M}_{13}$, it must possess information about both the *Xored* message $\mathrm{M}_{\otimes_1}$ and the secret key $\mathrm{M}_{21}$. In our analysis, we assumed that the eavesdropper will be able to decode $\mathrm{M}_{\otimes_1}$ correctly from its channel observation. However, Eq. (47) assures that the eavesdropper can not extract any information about $\mathrm{M}_{21}$. This implies that the eavesdropper will not be able to extract any information about $\mathrm{M}_{13}$ as well.

Now, using the same steps, we can proof that the term $\mathbb{I}(\mathrm{M}_{23}; \mathrm{Z}^n|\mathrm{M}_{21}\mathrm{M}_{22})$ which represents the leakage of $\mathrm{M}_{23}$ to the eavesdropper given $\mathrm{M}_{21}$ and $\mathrm{M}_{22}$ also vanishes. This implies that under the previous constraints, the leakage terms in (46) are with high probability smaller than $\tau_n$.

Now in order to finalize our proof, we need to define the bounds of the Shannon ciphered messages (secret key encoded messages) i.e $R_{\otimes_1}$ and $R_{\otimes_2}$. In addition to Eq. (43), we have another upper-bound for the ciphered messages which is the randomization index needed to confuse the eavesdropper in each layer (virtual channel). It is important to note that, although $m_{t_1}$ and $m_{t_2}$ are used to confuse the eavesdropper in some sense, they can not be a part of the secret key encoded message. This is because $m_{t_1}$ and $m_{t_2}$ are chosen such that the generated pair $(v_1^n, v_2^n)$ is jointly typical. Thus they can not be preselected by the encoder based on the value of the ciphered message. With this in mind we have the following bounds:

$$\begin{aligned}
R_{\otimes_1} &\leq \mathbb{I}(\mathrm{V}_0\mathrm{V}_1; \mathrm{Z}) \\
R_{\otimes_2} &\leq \mathbb{I}(\mathrm{V}_0\mathrm{V}_2; \mathrm{Z}) \\
R_{\otimes_1} + R_{\otimes_2} &\leq \mathbb{I}(\mathrm{V}_0\mathrm{V}_1; \mathrm{Z}) + \mathbb{I}(\mathrm{V}_2; \mathrm{Z}|\mathrm{V}_0) - \mathbb{I}(\mathrm{V}_1; \mathrm{V}_2|\mathrm{V}_0) \\
R_{\otimes_1} + R_{\otimes_2} &\leq \mathbb{I}(\mathrm{V}_0\mathrm{V}_2; \mathrm{Z}) + \mathbb{I}(\mathrm{V}_1; \mathrm{Z}|\mathrm{V}_0) - \mathbb{I}(\mathrm{V}_1; \mathrm{V}_2|\mathrm{V}_0) \\
R_{\otimes_1} + R_{\otimes_2} &\leq \mathbb{I}(\mathrm{V}_0\mathrm{V}_1\mathrm{V}_2; \mathrm{Z})
\end{aligned} \tag{49}$$

If we combine the bounds in (44) (45), (47), (43) and (49), then apply the Fourier-Motzkin elimination procedure, followed by taking the limit as $n \to \infty$, which implies that $\delta_n(\epsilon_n)$ and $\delta_n(\tau_n) \to 0$, we prove the achievability of any rate pair $(R_1 = R_{11} + R_{12}, R_2 = R_{21} + R_{22})$ satisfying (42). ■

### C. General Rate Region: Joint Vs Individual

In the previous sections, it has been shown that the individual secrecy criterion can provide a bigger rate region compared to the joint secrecy criterion for the degraded, Gaussian SISO and degraded Gaussian MIMO multi-receiver wiretap BC. This result was established by comparing the individual and joint secrecy capacity regions for these channels. Although, we can not establish a similar result for the general multi-receiver wiretap BC, we can still provide some intuitions by comparing the joint secrecy rate region in (37) and the individual secrecy rate region in (42).

Now, consider an encoding scheme for the individual secrecy criterion that divides the confidential messages sets $\mathcal{M}_1$ and $\mathcal{M}_2$ such that, $R_{11} \leq \mathbb{I}(\mathrm{V}_0\mathrm{V}_1; \mathrm{Z})$, $R_{12} \leq \mathbb{I}(\mathrm{V}_0\mathrm{V}_2; \mathrm{Z})$ and $R_{11} + R_{12} \leq R_{\mathrm{CE}} - \mathbb{I}(\mathrm{V}_1; \mathrm{V}_2|\mathrm{V}_0)$. For this scheme the rate region in (42) simplifies to:

$$\begin{aligned}
R_1 &\leq \mathbb{I}(\mathrm{V}_0\mathrm{V}_1; \mathrm{Y}_1) - \mathbb{I}(\mathrm{V}_0\mathrm{V}_1; \mathrm{Z}) \\
R_2 &\leq \mathbb{I}(\mathrm{V}_0\mathrm{V}_2; \mathrm{Y}_2) - \mathbb{I}(\mathrm{V}_0\mathrm{V}_2; \mathrm{Z}) \\
R_1 + R_2 &\leq \mathbb{I}(\mathrm{V}_0\mathrm{V}_1; \mathrm{Y}_1) + \mathbb{I}(\mathrm{V}_0\mathrm{V}_2; \mathrm{Y}_2) - \mathbb{I}(\mathrm{V}_0; \mathrm{Z}) - R_{\mathrm{CE}} \\
R_1 + R_2 &\leq \mathbb{I}(\mathrm{V}_0\mathrm{V}_1; \mathrm{Y}_1) + \mathbb{I}(\mathrm{V}_2; \mathrm{Y}_2|\mathrm{V}_0) - R_{\mathrm{CE}} + R_{11} + R_{12} \\
R_1 + R_2 &\leq \mathbb{I}(\mathrm{V}_1; \mathrm{Y}_1|\mathrm{V}_0) + \mathbb{I}(\mathrm{V}_0\mathrm{V}_2; \mathrm{Y}_2) - R_{\mathrm{CE}} + R_{11} + R_{12}.
\end{aligned}$$

It is obvious that the first three constraints in the previous region are identical to the first three constraints of the joint secrecy rate region in (37). On the other hand, the last two constraints in the previous region are bigger than the last two constraints in (37). Thus, although the joint and individual secrecy rate regions established in Theorem 5 and Theorem 6 are based on the same coding scheme (Marton coding with superposition variable), there exists some scenarios where the individual secrecy rate region can be bigger than the joint secrecy one. This gives us some intuitions that, in general the individual secrecy criterion might be able to provide a rate region bigger than the joint one.

## VII. Conclusion and Open Problems

We studied secure broadcasting over the multi-receiver wiretap BC with respect to two secrecy criteria: joint secrecy and individual secrecy. For both criteria, we presented a general

achievable rate region showing that for some scenarios the individual secrecy can provide a larger rate region as compared to the joint secrecy rate region. We then considered the class of degraded multi-receiver wiretap BC. For this class we established the individual secrecy capacity region and showed that it is in fact larger than the joint secrecy capacity region established in previous literature. This increase is because coding under the individual secrecy criterion combines wiretap random coding with secret key encoding by using the messages of the weak receivers as secret keys for the stronger ones. Further, we extended our results by establishing the individual secrecy capacity region for the Gaussian SISO and degraded Gaussian MIMO multi-receiver wiretap BCs.

It is important to highlight that all the results established in this paper were derived under two main assumptions: We assumed that the transmitter has a perfect channel state information about the channels to the legitimate receivers channel and the eavesdropper channel as well. We also assume that only a passive eavesdropper exists and ignored the existence of an active one. Although these assumptions might seem too ideal, without them it is very hard to establish significant results for the multi-user scenarios. These assumptions are also a necessary step before investigating a more general scenarios.

This have also been the case for the single-user scenarios, where at first the wiretap channel was investigated under perfect channel state information and passive eavesdropper only [4]. The channel uncertainty problem was then investigated in [41, 42] from a compound channel perspective, where the latter further considers the strong secrecy criterion. Following this, wiretap channels with both passive and active eavesdroppers were studied in [43, 44]. This line of research not only helped us to have a better understanding for secure communication under more practical scenarios, but it has also shown that some completely new behaviour can occur for communication scenarios under secrecy constraints [45]. An interesting example of this new behaviour is super-activation, which implies that a communication system consisting of two orthogonal channels, each of them have a zero capacity, can have an overall capacity greater than zero. Super-activation has remained a distinct phenomena for quantum information theory, until it has been shown that it can also happen in the classical non-quantum world [46]. It would be very interesting to investigate how the uncertainty of the transmitter about the state of the channels and the existence of active eavesdroppers will affect the results established in this paper.

## REFERENCES


[1] A. S. Mansour, R. F. Schaefer, and H. Boche, "The individual secrecy capacity of degraded multi-receiver wiretap broadcast channels," in *Communications (ICC), 2015 IEEE International Conference on*, London, United Kingdom, June 2015, pp. 4181–4186.

[2] ——, "The individual secrecy capacity of the Gaussian SISO and degraded Gaussian MIMO multi-receiver wiretap channel," in *Signal Processing Advances in Wireless Communications (SPAWC), 2015 IEEE 16th International Workshop on*, Stockholm, Sweden, June 2015, pp. 365–369.

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

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

[5] 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.

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

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

[8] Y. Liang, H. V. Poor, and S. S. (Shitz), "Information theoretic security," *Found. Trends Commun. Inf. Theory*, vol. 5, no. 4-5, pp. 355–580, April 2009.

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

[10] R. Ahlswede, *Hiding Data - Selected Topics from Rudolf Ahlswede's Lectures on Information Theory 3*, 1st ed., ser. Foundations in Signal Processing, Communications and Networking, A. Ahlswede, I. Althöfer, C. Deppe, and U. Tamm, Eds. Springer International Publishing, 2016, vol. 12.

[11] 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.

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

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

[14] 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.

[15] 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.

[16] Y. Chen, O. Koyluoglu, and A. Sezgin, "On the achievable individual-secrecy rate region for broadcast channels with receiver side information," in *Information Theory (ISIT), 2014 IEEE International Symposium on*, Honolulu, HI, USA, June 2014, pp. 26–30.

[17] A. S. Mansour, R. F. Schaefer, and H. Boche, "Joint and individual secrecy in broadcast channels with receiver side information," in *Signal Processing Advances in Wireless Communications (SPAWC), 2014 IEEE 15th International Workshop on*, Toronto, Canada, June 2014, pp. 369–373.

[18] ——, "Capacity regions for broadcast channels with degraded message sets and message cognition under different secrecy constraints," *CoRR*, 2015, available at: http://arxiv.org/abs/1501.04490.

[19] 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.

[20] Y. Chen, O. O. Koyluoglu, and A. Sezgin, "On the individual secrecy rate region for the broadcast channel with an external eavesdropper," in *Information Theory (ISIT), 2015 IEEE International Symposium on*, June 2015, pp. 1347–1351.

[21] Y. Chen, O. Ozan Koyluoglu, and A. Sezgin, "Individual Secrecy for the Broadcast Channel," *ArXiv e-prints*, November 2015. [Online]. Available: http://adsabs.harvard.edu/abs/2015arXiv151109070C

[22] I. Csiszár, "Almost independence and secrecy capacity," in *Probl. Peredachi Inf.*, vol. 32, no. 1, 1996, pp. 48–57.

[23] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Lecture Notes in Computer Science*, vol. 1807. Springer-Verlag, 2000, pp. 351–368.

[24] R. G. Gallager, "Capacity and coding for degraded broadcast channels," *Probl. Peredachi Inf.*, vol. 10, no. 3, pp. 3–14, 1974.

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

[26] D. Guo, S. Shamai (Shitz), and S. Verdu, "Mutual information and minimum mean-square error in gaussian channels," *IEEE Trans. Inf. Theory*, vol. 51, no. 4, pp. 1261–1282, April 2005.

[27] D. Guo, Y. Wu, S. Shamai (Shitz), and S. Verdu, "Estimation in gaussian noise: Properties of the minimum mean-square error," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2371–2385, April 2011.

[28] R. Bustin, R. F. Schaefer, H. V. Poor, and S. Shamai (Shitz), "On the snr-evolution of the mmse function of codes for the gaussian broadcast and wiretap channels," *IEEE Trans. Inf. Theory*, vol. 61, no. 4, April 2016.

[29] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York, NY, USA: Wiley-Interscience, 1991.

[30] P. Bergmans, "Random coding theorem for broadcast channels with degraded components," *IEEE Trans. Inf. Theory*, vol. 19, no. 2, pp. 197–207, Mar 1973.

[31] 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.

[32] 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.

[33] R. F. Wyrembelski, M. Wiese, and H. Boche, "Strong secrecy in bidirectional broadcast channels with confidential messages," *Information Forensics and Security, IEEE Transactions on*, vol. 8, no. 2, pp. 324–334, February 2013.

[34] R. Fano, *Transmission of Information: A Statistical Theory of Communications*. Cambridge, Massachusetts: The MIT Press, 1961.

[35] K. Marton, "A coding theorem for the discrete memoryless broadcast channel," *IEEE Trans. Inf. Theory*, vol. 25, no. 3, pp. 306–311, May 1979.

[36] A. A. Gohari, A. E. Gamal, and V. Anantharam, "On an outer bound and an inner bound for the general broadcast channel," in *Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on*, Austin, TX, United States, June 2010, pp. 540–544.

[37] V. Jog and C. Nair, "An information inequality for the bssc broadcast channel," in *Information Theory and Applications Workshop (ITA), 2010*, San Diego, United States, Jan 2010, pp. 1–8.

[38] Y.-K. Chia and A. El Gamal, "Three-receiver broadcast channels with common and confidential messages," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 2748–2765, May 2012.

[39] Z. Goldfeld, G. Kramer, H. H. Permuter, and P. Cuff, "Strong secrecy for cooperative broadcast channels," *CoRR*, vol. abs/1601.01286, 2016. [Online]. Available: http://arxiv.org/abs/1601.01286

[40] Y. Liang, *Multiuser Communications with Relaying and User Cooperation*. University of Illinois at Urbana-Champaign, 2005, ph.D. thesis. [Online]. Available: http://hdl.handle.net/2142/80931

[41] Y. Liang, G. Kramer, H. V. Poor, and S. S. (Shitz), "Compound wiretap channels," *EURASIP J. Wirel. Commun. Netw.*, vol. 2009, pp. 1–13, March 2009.

[42] I. Bjelaković, H. Boche, and J. Sommerfeld, "Secrecy results for compound wiretap channels," *Problems of Information Transmission*, vol. 49, no. 1, pp. 73–98, 2013.

[43] M. Wiese, J. Nötzel, and H. Boche, "The arbitrarily varying wiretap channel - deterministic and correlated random coding capacities under the strong secrecy criterion," *CoRR*, vol. abs/1410.8078, 2014. [Online]. Available: http://arxiv.org/abs/1410.8078

[44] J. Nötzel, M. Wiese, and H. Boche, "The arbitrarily varying wiretap channel - secret randomness, stability and super-activation," *CoRR*, vol. abs/1501.07439, 2015. [Online]. Available: http://arxiv.org/abs/1501.07439

[45] R. F. Schaefer, H. Boche, and H. V. Poor, "Secure communication under channel uncertainty and adversarial attacks," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1796–1813, October 2015.

[46] H. Boche and R. F. Schaefer, "Capacity results and super-activation for wiretap channels with active wiretappers," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 9, pp. 1482–1496, September 2013.


**Ahmed S. Mansour** (S'13) received the Master of Science degree in Electrical Engineering and Computer Science in 2012 from Universität Ulm, Germany. He was a recipient of the Best Master Thesis Award from Universität Ulm. Since April 2013, he has been working as a research and teaching assistant with the Lehrstuhl für Theoretische Informationstechnik at the Technische Universität München, Germany. He is currently working towards his Ph.D. degree.

**Rafael F. Schaefer** (S'08–M'12) received the Dipl.-Ing. degree in electrical engineering and computer science in 2007 from the Technische Universität Berlin, Germany and the Dr.-Ing. degree in electrical engineering in 2012 from the Technische Universität München, Germany. From 2007 until 2010 he was a Research and Teaching Assistant at Technische Universität Berlin and from 2010 until 2013 at Technische Universität München. From 2013 until 2015 he was a Post-Doctoral Research Fellow at Princeton University. Since December 2015 he has been an Assistant Professor at Technische Universität Berlin. He was a recipient of the VDE Johann-Philipp-Reis Prize in 2013. He was one of the exemplary reviewers of the IEEE COMMUNICATION LETTERS in 2013. He is currently an Associate Member of the IEEE Information Forensics and Security Technical Committee. He is the General Chair of the *Symposium on Information Theoretic Approaches to Security and Privacy* at IEEE GlobalSIP 2016. Among his publications is the recent book *Information Theoretic Security and Privacy of Information Systems* (Cambridge University Press).

**Holger Boche** (M'04–SM'07–F'11) received the Dipl.-Ing. and Dr.-Ing. degrees in electrical engineering from the Technische Universität Dresden, Germany, in 1990 and 1994, respectively. He graduated in mathematics from the Technische Universität Dresden in 1992. From 1994 to 1997, he did Postgraduate studies in mathematics at the Friedrich-Schiller Universität Jena, Germany. He received his Dr. rer. nat. degree in pure mathematics from the Technische Universität Berlin, Germany, in 1998. In 1997, he joined the Heinrich-Hertz-Institut (HHI) für Nachrichtentechnik Berlin, Germany. Starting in 2002, he was a Full Professor for mobile communication networks with the Institute for Communications Systems, Technische Universität Berlin. In 2003, he became Director of the Fraunhofer German-Sino Lab for Mobile Communications, Berlin, Germany, and in 2004 he became the Director of the Fraunhofer Institute for Telecommunications (HHI), Berlin, Germany. Since October 2010 he has been with the Institute of Theoretical Information Technology and Full Professor at the Technische Universität München, Germany. Since 2014 he has been a member and honorary fellow of the TUM Institute for Advanced Study, Munich, Germany. He was a Visiting Professor with the ETH Zurich, Switzerland, during the 2004 and 2006 Winter terms, and with KTH Stockholm, Sweden, during the 2005 Summer term. Prof. Boche is a Member of IEEE Signal Processing Society SPCOM and SPTM Technical Committee. He was elected a Member of the German Academy of Sciences (Leopoldina) in 2008 and of the Berlin Brandenburg Academy of Sciences and Humanities in 2009. He received the Research Award "Technische Kommunikation" from the Alcatel SEL Foundation in October 2003, the "Innovation Award" from the Vodafone Foundation in June 2006, and the Gottfried Wilhelm Leibniz Prize from the Deutsche Forschungsgemeinschaft (German Research Foundation) in 2008. He was co-recipient of the 2006 IEEE Signal Processing Society Best Paper Award and recipient of the 2007 IEEE Signal Processing Society Best Paper Award. He is the General Chair of the *Symposium on Information Theoretic Approaches to Security and Privacy* at IEEE GlobalSIP 2016. Among his publications is the recent book *Information Theoretic Security and Privacy of Information Systems* (Cambridge University Press).