Joint and Individual Secrecy in Broadcast Channels with Receiver Side Information

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

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

† Department of Electrical Engineering
Princeton University
Princeton, NJ 08540, USA
Email: rafaelfs@princeton.edu

***Abstract*—We study secure communication in which two confidential messages are transmitted over a broadcast channel to two legitimate receivers, while keeping an eavesdropper ignorant. Each legitimate receiver is interested in decoding one confidential message, while having the other one as side information. In order to measure the secrecy of the communication, we investigate two different secrecy criteria: joint secrecy and individual secrecy. For both criteria, we provide an achievable rate region and a matching multi-letter outer bound presenting a multi-letter description for the capacity region. We further investigate the class of more capable channels and provide a single-letter converse establishing the secrecy capacity region, not only for more capable channels but less noisy and degraded channels as well. Our results indicate that the secrecy capacity for individual secrecy is higher than the one for joint secrecy, as one message can be used as a secret key for the other one.**

I. Introduction

The wireless medium is characterized by an exposed nature that allows transmitted signals to be received not only by legitimate users but eavesdroppers as well. In [1], Shannon studied the problem of secure communication and proved that it can be achieved by a secret key shared between the transmitter and the receiver if the entropy of this key is greater than or equal to the entropy of the message to be transmitted. This condition is a consequence of the assumption that both the receiver and the eavesdropper have an equal access to the transmitted signal. In [2], Wyner studied the degraded wiretap channel and proved that secure transmission is still achievable in the absence of a secret key. In [3], Csiszár and Körner extended Wyner's result to the general broadcast channel (BC) with confidential messages. In [4], Kang and Liu generalized the previous two approaches by studying the presence of a shared secret key in the wiretap channel. They derived the secrecy capacity for this scenario by combining the wiretap coding principle along with Shannon's one-time pad idea.

The problem of secure communication in BC with more than two receivers remains an open topic. In [5], Chia and El Gamal investigated the secrecy capacity for transmitting a confidential common message over a BC with two receivers and one eavesdropper. In [6], Bagherikaram, Motahri, and Khandani studied the same channel but with two confidential messages; one for each receiver. They managed to characterize the secrecy capacity only if the channel is degraded. In this paper, we study a related problem. We consider a BC with two legitimate receivers and one eavesdropper. The transmitter broadcasts two independent confidential messages to the two legitimate receivers while keeping the eavesdropper ignorant about them. The setup has an additional feature, that each legitimate receiver is interested in merely one message while having the other one as side information as shown in Figure 1. This brings the name: BC with receiver side information. This problem is motivated by the concept of two-phase decode-and-forward bidirectional relaying in a three-node network [7]. In the first phase, node 1 and 2 transmit their messages to the relay node which decodes them, while keeping the eavesdropper unable to intercept any information about the transmission. This problem was investigated in [8, 9], where the latter discusses different secrecy criteria. Our work focuses on the succeeding broadcast, where the relay encodes and transmits both messages such that, the two legitimate receivers can decode their intended message using their own message as a side information, while keeping the eavesdropper ignorant. This problem was investigated in [10], where different achievable rate regions and an outer bound were provided. Differently from [10], we differentiate between joint and individual secrecy and propose a new encoding technique for the individual secrecy criterion.

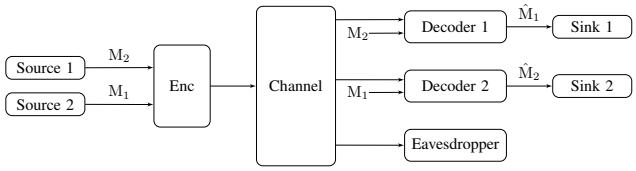

Fig. 1. Broadcast channel with two legitimate receivers and one eavesdropper, where side information is available at the two legitimate receivers

This paper is organized as follows. In Section II, we state the problem and present the two secrecy criteria that we study: joint secrecy and individual secrecy. In Sections III and IV, we provide achievable rate regions and multi-letter converses for each secrecy criteria. We also establish the secrecy capacity for more capable channels which includes both less noisy and degraded ones. Our results indicate that individual secrecy can provide a larger capacity region as compared to joint secrecy.

II. BC With Receiver Side Information

We consider the standard model with a block code of arbitrary but fixed length n. For input and output sequences x^n, y_1^n, y_2^n, and z^n of length n, the discrete memoryless BC is given by

$$W^n(y_1^n, y_2^n, z^n|x^n) = \prod_{k=1}^{n} W(y_{1,k}, y_{2,k}, z_k|x_k).$$

978-1-4799-4903-8/14/$31.00 ©2014 IEEE

Definition 1. *A $(2^{nR_1}, 2^{nR_2}, n)$ code $\mathcal{C}_n$ for the BC with receiver side information consists of: two independent message sets $\mathcal{M}_1$ and $\mathcal{M}_2$, an independent randomization message set $\mathcal{M}_r$, an encoding function at the relay node*

$$E : \mathcal{M}_1 \times \mathcal{M}_2 \times \mathcal{M}_r \to \mathcal{X}^n$$

which maps a message pair $(m_1, m_2) \in \mathcal{M}_1 \times \mathcal{M}_2$ and a realization of the randomization message $m_r \in \mathcal{M}_r$, chosen uniformly at random, to a codeword $x^n(m_1, m_2, m_r)$, and two decoders, one for each node

$$\varphi_1 : \mathcal{Y}_1^n \times \mathcal{M}_2 \to \mathcal{M}_1$$
$$\varphi_2 : \mathcal{Y}_2^n \times \mathcal{M}_1 \to \mathcal{M}_2$$

that maps each channel observation at the respective node and its own message to the corresponding required message.

The $(2^{nR_1}, 2^{nR_2}, n)$ code $\mathcal{C}_n$ is known to the two legitimate receivers and the eavesdropper. We assume that messages M_1 and M_2 are chosen uniformly at random. The reliability performance of the code $\mathcal{C}_n$ is measured in terms of its average probability of error

$$P_e(\mathcal{C}_n) \triangleq \mathbb{P}\left[\hat{\mathrm{M}}_1 \neq \mathrm{M}_1 \text{ or } \hat{\mathrm{M}}_2 \neq \mathrm{M}_2 | \mathcal{C}_n\right], \tag{1}$$

where $\hat{\mathrm{M}}_1$ and $\hat{\mathrm{M}}_2$ are the estimated messages at nodes 1 and 2 respectively. In order to measure the ignorance of the eavesdropper about the transmitted messages M_1 and M_2, we consider two different secrecy criteria.

1. *Joint Secrecy:* the secrecy performance of the code $\mathcal{C}_n$ is measured in terms of the joint leakage of M_1 and M_2 to the eavesdropper:

$$\begin{aligned} L(\mathcal{C}_n) &\triangleq \mathbb{I}(\mathrm{M}_1\mathrm{M}_2; \mathrm{Z}^n) \\ &= \mathbb{I}(\mathrm{M}_1; \mathrm{Z}^n) + \mathbb{I}(\mathrm{M}_2; \mathrm{Z}^n | \mathrm{M}_1). \end{aligned} \tag{2}$$

2. *Individual Secrecy:* the secrecy performance of the code $\mathcal{C}_n$ is measured as the sum of the individual leakages of M_1 and M_2 to the eavesdropper:

$$L(\mathcal{C}_n) \triangleq \mathbb{I}(\mathrm{M}_1; \mathrm{Z}^n) + \mathbb{I}(\mathrm{M}_2; \mathrm{Z}^n). \tag{3}$$

Definition 2. *A secrecy rate pair $(R_1, R_2) \in \mathbb{R}_+^2$ is achievable for the BC with receiver side information, if for any ϵ_n and τ_n in the form of $e^{-\alpha n}$, where $\alpha > 0$, there exists a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes $\{\mathcal{C}_n\}_{n\geq 1}$, such that*

$$P_e(\mathcal{C}_n) \leq \epsilon_n, \qquad L(\mathcal{C}_n) \leq \tau_n. \tag{4}$$

Depending on the selected secrecy criteria, $L(\mathcal{C}_n)$ is given by (2) *or* (3)*.*

In order to have a deeper look into the two criteria in (2) and (3), we need to investigate and compare their secrecy performance and the accompanied capacities. To the best of our knowledge, previous literature on BC only considered the joint secrecy criterion. This might be because any code that satisfies the joint secrecy criterion also satisfies the individual one. We can deduce this easily by comparing (2) and (3), knowing that

$$\mathbb{I}(\mathrm{M}_2; \mathrm{Z}^n) \leq \mathbb{I}(\mathrm{M}_2; \mathrm{Z}^n | \mathrm{M}_1),$$

since M_1 and M_2 are independent. This implies that the joint secrecy is stronger than the individual one. Another point that advocates the strength of the joint criterion over the individual one is that; revealing one message to the eavesdropper might threaten the secrecy of the other message in case of the individual secrecy, while the joint secrecy guarantees the secrecy of the unrevealed message. The previous comparison tells us why most researchers only considered joint secrecy. However, we will show that, individual secrecy has some interesting features as compared to the joint one. In particular, we will show that, loosening the secrecy criterion from the joint to the individual one can increase the secrecy capacity of the BC with receiver side information significantly.

III. The Joint Secrecy Capacity Region

In this section we investigate the joint secrecy criterion in the BC with receiver side information. First, we present an achievable secrecy rate region for the general case. We then derive a multi-letter outer bound that matches the achievable region. Finally, we establish the joint secrecy capacity region when the two legitimate receivers are more capable than the eavesdropper.

A. Achievable Rate Region

Lemma 1. *An achievable joint secrecy rate region for the BC with receiver side information is given by the set of all rate pairs $(R_1, R_2) \in \mathbb{R}_+^2$ that satisfy*

$$R_j \leq \mathbb{I}(\mathrm{V}; \mathrm{Y}_j) - \mathbb{I}(\mathrm{V}; \mathrm{Z}), \qquad j = 1, 2 \tag{5}$$

for random variables with joint probability distribution $Q_{\mathrm{V}}(v)\ Q_{\mathrm{X}|\mathrm{V}}(x|v)\ Q_{\mathrm{Y}_1\mathrm{Y}_2\mathrm{Z}|\mathrm{X}}(y_1, y_1, z|x)$.

Proof: The proof combines the technique of random coding with product structure as in [3] along with the usage of resolvability to achieve secrecy [11–13]. We first show that the rate region given by the set of all rate pairs $(R_1, R_2) \in \mathbb{R}_+^2$ satisfying

$$R_j \leq \mathbb{I}(\mathrm{X}; \mathrm{Y}_j) - \mathbb{I}(\mathrm{X}; \mathrm{Z}), \qquad j = 1, 2 \tag{6}$$

is achievable. Then, the region in (5) with prefixed random variable V follows immediately as in [3, Lemma 4].

1. *Random Codebook $\mathcal{C}_n$*: Fix an input distribution $Q_{\mathrm{X}}(x)$ and construct $x^n(m_1, m_2, m_r)$ for $m_j \in \mathcal{M}_j = [\![1, 2^{nR_j}]\!]$, $j = 1, 2$, and $m_r \in \mathcal{M}_r = [\![1, 2^{nR_r}]\!]$ by generating symbols $x_i(m_1, m_2, m_r)$ with $i \in [\![1, n]\!]$, independently at random according to $Q_{\mathrm{X}}(x)$.
2. *Encoder E*: Given a message pair (m_1, m_2), it chooses a randomization message m_r uniformly at random from the set $\mathcal{M}_r$ and transmits $x^n(m_1, m_2, m_r)$.
3. *First Decoder* φ_1: Given y_1^n and its own message m_2, outputs $(\hat{m}_1, \hat{m}_r)$; if it is the unique pair, such that $(x^n(\hat{m}_1, m_2, \hat{m}_r), y_1^n)$ is jointly typical. Otherwise declares an error.
4. *Second Decoder* φ_2: Given y_2^n and its own message m_1, outputs $(\tilde{m}_2, \tilde{m}_r)$; if it is the unique pair, such that $(x^n(m_1, \tilde{m}_2, \tilde{m}_r), y_2^n)$ is jointly typical. Otherwise declares an error.

Reliability and Secrecy Analysis: We define the error probability of this scheme as

$$\begin{aligned} \hat{P}_e(\mathcal{C}_n) \triangleq\ & \mathbb{P}\big[(\hat{\mathrm{M}}_1, \hat{\mathrm{M}}_r) \neq (\mathrm{M}_1, \mathrm{M}_r) \text{ or} \\ & (\tilde{\mathrm{M}}_2, \tilde{\mathrm{M}}_r) \neq (\mathrm{M}_2, \mathrm{M}_r) | \mathcal{C}_n\big]. \end{aligned} \tag{7}$$

We then observe that $\hat{P}_e(\mathcal{C}_n) \geq P_e(\mathcal{C}_n)$, cf. (1). Using the standard analysis of random coding we can prove that for a sufficiently large n, with high probability $\hat{P}_e(\mathcal{C}_n) \leq \epsilon_n$ if

$$R_j + R_r < \mathbb{I}(\mathrm{X};\mathrm{Y}_j) - \delta_n(\epsilon_n) \qquad j = 1, 2. \tag{8}$$

The validity of (8) follows from the product structure of the codebook and the availability of the side information at the receiver as in [7, 14]. On the other hand, for a sufficiently large n and $\tau_n > 0$, the joint leakage given in (2) is with high probability smaller than τ_n if

$$R_r \geq \mathbb{I}(\mathrm{X};\mathrm{Z}) + \delta_n(\tau_n). \tag{9}$$

This follows from Hou's and Kramer's work in [12], or other strong secrecy approaches as for example [11, 13]. Combining (8) and (9), then taking the limit as $n \to \infty$, which implies that $\delta_n(\epsilon_n)$ and $\delta_n(\tau_n) \to 0$ gives the achievability of any rate pair (R_1, R_2) satisfying (6). ∎

B. Multi-Letter Converse

Proposition 1. *The joint secrecy capacity region of the BC with receiver side information is upper bounded as follows*

$$R_j \leq \lim_{n\to\infty} \frac{1}{n}\Big[\mathbb{I}(\mathrm{V};\mathrm{Y}_j^n) - \mathbb{I}(\mathrm{V};\mathrm{Z}^n)\Big], \qquad j = 1, 2 \tag{10}$$

for random variables satisfying the Markov chain $\mathrm{V} - \mathrm{X}^n - (\mathrm{Y}_1^n, \mathrm{Y}_2^n, \mathrm{Z}^n)$.

Proof: Suppose that for some $\epsilon_n, \tau_n > 0$ and sufficiently large n, there exists a $(2^{nR_1}, 2^{nR_2}, n)$ code $\mathcal{C}_n$ such that (4) is satisfied, where $L(\mathcal{C}_n)$ satisfies (2). We have

$$\begin{aligned}
R_1 &= \frac{1}{n}\,\mathbb{H}(\mathrm{M}_1) \overset{(a)}{=} \frac{1}{n}\,\mathbb{H}(\mathrm{M}_1|\mathrm{M}_2) \\
&= \frac{1}{n}\Big[\mathbb{I}(\mathrm{M}_1;\mathrm{Y}_1^n|\mathrm{M}_2) + \mathbb{H}(\mathrm{M}_1|\mathrm{Y}_1^n\mathrm{M}_2)\Big] \\
&\overset{(b)}{\leq} \frac{1}{n}\,\mathbb{I}(\mathrm{M}_1;\mathrm{Y}_1^n|\mathrm{M}_2) + \gamma(\epsilon_n) \\
&\overset{(c)}{\leq} \frac{1}{n}\,\mathbb{I}(\mathrm{M}_1\mathrm{M}_2;\mathrm{Y}_1^n) + \gamma(\epsilon_n) \qquad (11) \\
&\overset{(d)}{\leq} \frac{1}{n}\Big[\mathbb{I}(\mathrm{M}_1\mathrm{M}_2;\mathrm{Y}_1^n) - \mathbb{I}(\mathrm{M}_1\mathrm{M}_2;\mathrm{Z}^n)\Big] + \gamma(\epsilon_n, \tau_n) \qquad (12)
\end{aligned}$$

where (a) follows from the independence of M_1 and M_2; (b) follows from Fano's inequality with $\gamma(\epsilon_n) = 1/n + \epsilon_n R_1$; (c) follows by the chain rule and (d) follows from (2) and (4), where $\gamma(\epsilon_n, \tau_n) = \tau_n/n + \gamma(\epsilon_n)$. Following the same steps we can achieve a similar bound for R_2:

$$R_2 \leq \frac{1}{n}\Big[\mathbb{I}(\mathrm{M}_1\mathrm{M}_2;\mathrm{Y}_2^n) - \mathbb{I}(\mathrm{M}_1\mathrm{M}_2;\mathrm{Z}^n)\Big] + \gamma(\epsilon_n, \tau_n). \tag{13}$$

Now, if we use $\mathrm{V} \triangleq (\mathrm{M}_1, \mathrm{M}_2)$ and take the limit as $n \to \infty$, such that $\gamma(\epsilon_n, \tau_n) \to 0$, where the convergence of the limit is guaranteed by the Fekete's lemma [15], cf. also [13, Lemma 5], we reach the upper bound in (10). ∎

Remark: Since the multi-letter upper bound in (10) matches the achievable rate region in (5) applied to the n-fold product of the BC, this establishes a multi-letter description for the capacity region. However, a single-letter description is desirable because the former multi-letter one is not efficiently computable.

C. More Capable Channels

Since finding a single-letter converse for the general BC with receiver side information is hard, we focused our attention on the special case of more capable channels.

Definition 3. *The two legitimate receivers are said to be more capable than the eavesdropper in a BC, if for every input* X*, we have*

$$\mathbb{I}(\mathrm{X};\mathrm{Y}_j) \geq \mathbb{I}(\mathrm{X};\mathrm{Z}), \qquad j = 1, 2. \tag{14}$$

The class of more capable channels is a wide class. It contains physically and stochastically degraded channels as well as less noisy channels cf. for example [16]. This implies that establishing secrecy capacity for more capable channels provides the capacity region for these channels as well.

Theorem 1. *The joint secrecy capacity region of the more capable BC with receiver side information is the set of all rate pairs* $(R_1, R_2) \in \mathbb{R}_+^2$ *that satisfy*

$$R_j \leq \mathbb{I}(\mathrm{X};\mathrm{Y}_j) - \mathbb{I}(\mathrm{X};\mathrm{Z}), \qquad j = 1, 2 \tag{15}$$

for random variables with joint probability distribution $Q_{\mathrm{X}}(x)\; Q_{\mathrm{Y_1Y_2Z|X}}(y_1, y_1, z|x)$.

Proof: The achievability follows as in the proof of Lemma 1. Now for the converse, we start by R_1 and let $\mathrm{U}_i^1 \triangleq (\mathrm{Y}_1^{i-1}, \mathrm{Z}_{i+1}^n)$, and $\mathrm{V}_i^1 \triangleq (\mathrm{M}_1, \mathrm{M}_2, \mathrm{U}_i^1)$. Using (12), we have

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

where $\mathrm{U}_i^1 - \mathrm{V}_i^1 - \mathrm{X}_i - (\mathrm{Y}_{1i}, \mathrm{Z}_i)$ forms a Markov chain. Step (a) follows from the chain rule and (b) follows from the Csiszár sum identity [3, Lemma 7]. Introducing a random variable T independent of all others and uniformly distributed over $[\![1, n]\!]$, then letting $\mathrm{U}^1 = (\mathrm{U}_T^1, \mathrm{T})$, $\mathrm{V}^1 = \mathrm{V}_T^1$, $\mathrm{Y}_1 = \mathrm{Y}_{1T}$ and $\mathrm{Z} = \mathrm{Z}_T$, we have

$$R_1 \leq \mathbb{I}(\mathrm{V}^1;\mathrm{Y}_1|\mathrm{U}^1) - \mathbb{I}(\mathrm{V}^1;\mathrm{Z}|\mathrm{U}^1) + \gamma(\epsilon_n, \tau_n). \tag{16}$$

Similarly, let $\mathrm{U}_i^2 \triangleq (\mathrm{Y}_2^{i-1}, \tilde{\mathrm{Z}}^{i+1})$, and $\mathrm{V}_i^2 \triangleq (\mathrm{M}_1, \mathrm{M}_2, \mathrm{U}_i^2)$ such that $\mathrm{U}_i^2 - \mathrm{V}_i^2 - \mathrm{X}_i - (\mathrm{Y}_{2i}, \mathrm{Z}_i)$. Using (13), we can derive a similar bound for R_2 as

$$R_2 \leq \mathbb{I}(\mathrm{V}^2;\mathrm{Y}_2|\mathrm{U}^2) - \mathbb{I}(\mathrm{V}^2;\mathrm{Z}|\mathrm{U}^2) + \gamma(\epsilon_n, \tau_n). \tag{17}$$

Back to R_1, Eq. (16) can be further simplified as

$$\begin{aligned}
R_1 &\leq \mathbb{E}\big[\mathbb{I}(\mathrm{V}^1;\mathrm{Y}_1|\mathrm{U}^1 = \mathrm{u}^1) - \mathbb{I}(\mathrm{V}^1;\mathrm{Z}|\mathrm{U}^1 = \mathrm{u}^1)\big] + \gamma(\epsilon_n, \tau_n) \\
&\overset{(a)}{\leq} \mathbb{I}(\mathrm{V}^1;\mathrm{Y}_1|\mathrm{U}^1 = \mathrm{u}^{1*}) - \mathbb{I}(\mathrm{V}^1;\mathrm{Z}|\mathrm{U}^1 = \mathrm{u}^{1*}) + \gamma(\epsilon_n, \tau_n) \\
&\overset{(b)}{=} \mathbb{I}(\mathrm{V}^{1*};\mathrm{Y}_1) - \mathbb{I}(\mathrm{V}^{1*};\mathrm{Z}) + \gamma(\epsilon_n, \tau_n) \qquad (18)
\end{aligned}$$

where $\mathrm{V}^{1*} - \mathrm{X} - (\mathrm{Y}_1, \mathrm{Z})$ forms a Markov chain. Step (a) follows as u^{1*} is the value of U^1 that maximizes the difference in (16) and (b) follows because V^{1*} is distributed as $Q_{\mathrm{V}^1|\mathrm{U}^1=u^{1*}}$. Similarly for R_2, we have

$$R_2 \leq \mathbb{I}(\mathrm{V}^{2*};\mathrm{Y}_2) - \mathbb{I}(\mathrm{V}^{2*};\mathrm{Z}) + \gamma(\epsilon_n,\tau_n), \tag{19}$$

where $\mathrm{V}^{2*} - \mathrm{X} - (\mathrm{Y}_2, \mathrm{Z})$ forms a Markov chain, such that V^{2*} is distributed as $Q_{\mathrm{V}^2|\mathrm{U}^2=u^{2*}}$ and u^{2*} is the value of U^2 that maximizes the difference in (17). Because of the Markov chains and the fact that if Y_1 and Y_2 are more capable than Z, $\mathbb{I}(\mathrm{X};\mathrm{Y}_1|\mathrm{V}^{1*}) \geq \mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{V}^{1*})$ and $\mathbb{I}(\mathrm{X};\mathrm{Y}_2|\mathrm{V}^{2*}) \geq \mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{V}^{2*})$. The bounds in (18) and (19) can be simplified to

$$\begin{aligned} R_1 &\leq \mathbb{I}(\mathrm{X};\mathrm{Y}_1) - \mathbb{I}(\mathrm{X};\mathrm{Z}) + \gamma(\epsilon_n,\tau_n) \\ R_2 &\leq \mathbb{I}(\mathrm{X};\mathrm{Y}_2) - \mathbb{I}(\mathrm{X};\mathrm{Z}) + \gamma(\epsilon_n,\tau_n). \end{aligned} \tag{20}$$

Before finalizing our converse, we need to illustrate an important point. One might argue that getting rid of the conditional random variables U^1 and U^2 using the previous procedure can not be done for R_1 and R_2 simultaneously because U^1 and U^2 might be dependent, such that u^{1*} and u^{2*} can not occur concurrently. This fact does not affect our converse because it only implies that the derived upper bounds are loose. Yet, our result assures that for the more capable case, these bounds are tight enough. Now taking the limit as $n \to \infty$, which implies that $\gamma(\epsilon_n,\tau_n) \to 0$, Equation (15) is satisfied. ∎

IV. The Individual Secrecy Capacity Region

In this section we investigate the individual secrecy criterion for the BC with receiver side information. We first provide an achievable rate region for the general case, then we derive a multi-letter outer bound that matches this region. Finally we establish the individual secrecy capacity region for the more capable case.

A. Achievable Rate Region

Lemma 2. *An achievable individual secrecy rate region for the BC with receiver side information is given by the set of all rate pairs $(R_1, R_2) \in \mathbb{R}_+^2$ that satisfy*

$$\begin{aligned} R_1 &\leq \min\Big[\mathbb{I}(\mathrm{V};\mathrm{Y}_1) - \mathbb{I}(\mathrm{V};\mathrm{Z}) + R_2\ ,\ \mathbb{I}(\mathrm{V};\mathrm{Y}_1)\Big] \\ R_2 &\leq \min\Big[\mathbb{I}(\mathrm{V};\mathrm{Y}_2) - \mathbb{I}(\mathrm{V};\mathrm{Z}) + R_1\ ,\ \mathbb{I}(\mathrm{V};\mathrm{Y}_2)\Big] \end{aligned} \tag{21}$$

for random variables with joint probability distribution $Q_{\mathrm{V}}(v)\ Q_{\mathrm{X}|\mathrm{V}}(x|v)\ Q_{\mathrm{Y}_1\mathrm{Y}_2\mathrm{Z}|\mathrm{X}}(y_1,y_1,z|x)$, such that $\mathbb{I}(\mathrm{V};\mathrm{Y}_1)$ and $\mathbb{I}(\mathrm{V};\mathrm{Y}_2)$ are greater than $\mathbb{I}(\mathrm{V};\mathrm{Z})$.

Proof: The proof combines the techniques used in the previous section along with the Shannon's cipher system, where the Shannon ciphered message is used as a part of the randomization index for wiretap encoding. We started by dividing each message set $\mathcal{M}_j$ with $j = 1,2$ into two independent parts $\mathcal{M}_{jk} = [\![1, 2^{nR_{jk}}]\!]$, $k = 1,2$ such that $\mathcal{M}_{12}$ and $\mathcal{M}_{21}$ are of the same size. We construct $\mathcal{M}_\otimes = [\![1, 2^{nR_\otimes}]\!]$ by *Xoring* the corresponding elements of $\mathcal{M}_{12}$ and $\mathcal{M}_{21}$. Thus, we have

$$\begin{aligned} R_1 = R_{11} + R_{12}, \qquad R_2 = R_{22} + R_{21}, \\ R_\otimes = R_{12} = R_{21} \leq \min(R_1, R_2). \end{aligned} \tag{22}$$

1. *Random Codebook $\mathcal{C}_n$:* Fix an input distribution $Q_{\mathrm{X}}(x)$ and construct $x^n(m_{11}, m_{22}, m_\otimes, m_r)$ for $m_{jj} \in \mathcal{M}_{jj}$ $j = 1,2$, $m_\otimes \in \mathcal{M}_\otimes$, and $m_r \in \mathcal{M}_r = [\![1, 2^{nR_r}]\!]$ by generating symbols $x_i(m_{11}, m_{22}, m_\otimes, m_r)$ with $i \in [\![1,n]\!]$, independently at random according to $Q_{\mathrm{X}}(x)$.
2. *Encoder E:* Given a message pair (m_1, m_2), it calculates the triple $(m_{11}, m_{22}, m_\otimes)$ then chooses a message m_r uniformly at random from the set $\mathcal{M}_r$ and transmits $x^n(m_{11}, m_{22}, m_\otimes, m_r)$.
3. *First Decoder φ_1:* Given y_1^n and $m_2 = (m_{21}, m_{22})$, outputs $(\hat{m}_1, \hat{m}_r)$; where $\hat{m}_1$ is the concatenation of $\hat{m}_{11}$ and $\hat{m}_{12}$. First, it finds the unique triple $(\hat{m}_{11}, \hat{m}_\otimes, \hat{m}_r)$ such that $(x^n(\hat{m}_{11}, m_{22}, \hat{m}_\otimes, \hat{m}_r), y_1^n)$ is jointly typical. Then, it computes $\hat{m}_{12}$ by *Xoring* m_{21} and $\hat{m}_\otimes$.
4. *Second Decoder φ_2:* Given y_2^n and $m_1 = (m_{11}, m_{12})$, outputs $(\tilde{m}_2, \tilde{m}_r)$; where $\tilde{m}_2$ is the concatenation of $\tilde{m}_{22}$ and $\tilde{m}_{21}$. First, it finds the unique triple $(\tilde{m}_{22}, \tilde{m}_\otimes, \tilde{m}_r)$ such that $(x^n(m_{11}, \tilde{m}_{22}, \tilde{m}_\otimes, \tilde{m}_r), y_2^n)$ is jointly typical. Then, it computes $\tilde{m}_{21}$ by *Xoring* m_{12} and $\tilde{m}_\otimes$.

Reliability and Secrecy Analysis: We define the error probability for this scheme as

$$\begin{aligned} \tilde{P}_e(\mathcal{C}_n) \triangleq \mathbb{P}\Big[&(\hat{\mathrm{M}}_{11}, \hat{\mathrm{M}}_\otimes, \hat{\mathrm{M}}_\mathrm{r}) \neq (\mathrm{M}_{11}, \mathrm{M}_\otimes, \mathrm{M}_\mathrm{r}) \text{ or} \\ &(\tilde{\mathrm{M}}_{22}, \tilde{\mathrm{M}}_\otimes, \tilde{\mathrm{M}}_\mathrm{r}) \neq (\mathrm{M}_{22}, \mathrm{M}_\otimes, \mathrm{M}_\mathrm{r}) | \mathcal{C}_n\Big], \end{aligned} \tag{23}$$

where $\tilde{P}_e(\mathcal{C}_n) \geq P_e(\mathcal{C}_n)$, cf. (1). Now following the same procedures used in the previous section, we can prove that for a sufficiently large n, with high probability $\tilde{P}_e(\mathcal{C}_n) \leq \epsilon_n$ if

$$R_{jj} + R_\otimes + R_r < \mathbb{I}(\mathrm{X};\mathrm{Y}_j) - \delta_n(\epsilon_n) \qquad j = 1,2. \tag{24}$$

Because of the new message sets structure, the random variable M_1 is identified as the product of two independent and uniformly distributed random variables M_{11} and M_{12}. Thus, the leakage of M_1 to the eavesdropper becomes

$$\mathbb{I}(\mathrm{M}_1;\mathrm{Z}^n|\mathcal{C}_n) = \mathbb{I}(\mathrm{M}_{11};\mathrm{Z}^n|\mathcal{C}_n) + \mathbb{I}(\mathrm{M}_{12};\mathrm{Z}^n|\mathrm{M}_{11}\mathcal{C}_n). \tag{25}$$

One can prove that the second term in (25) vanishes as

$$\begin{aligned} \mathbb{I}(\mathrm{M}_{12};\mathrm{Z}^n|\mathrm{M}_{11}) &= \mathbb{H}(\mathrm{M}_{12}|\mathrm{M}_{11}) - \mathbb{H}(\mathrm{M}_{12}|\mathrm{Z}^n\mathrm{M}_{11}) \\ &\overset{(a)}{=} \mathbb{H}(\mathrm{M}_{12}) - \mathbb{H}(\mathrm{M}_{12}|\mathrm{Z}^n\mathrm{M}_{11}) \\ &\overset{(b)}{\leq} \mathbb{H}(\mathrm{M}_{12}) - \mathbb{H}(\mathrm{M}_{12}|\mathrm{M}_{11}\mathrm{M}_{22}\mathrm{M}_\otimes\mathrm{M}_r) \\ &\overset{(c)}{=} \mathbb{H}(\mathrm{M}_{12}) - \mathbb{H}(\mathrm{M}_{12}|\mathrm{M}_\otimes) \overset{(d)}{=} 0 \end{aligned} \tag{26}$$

where (a) follows because M_{12} and M_{11} are independent; (b) follows because $(\mathrm{M}_{11}, \mathrm{M}_{22}, \mathrm{M}_\otimes, \mathrm{M}_r) - \mathrm{X}^n - \mathrm{Z}^n$ forms a Markov chain; (c) follows because M_{12} is independent from $\mathrm{M}_{11}, \mathrm{M}_{22}$ and M_r and (d) follows because of the Shannon's cipher system as $\mathbb{H}(\mathrm{M}_{12}) = \mathbb{H}(\mathrm{M}_{21})$. It is worth mentioning that, revealing M_2 to the eavesdropper might threaten the validity of this result. Since the eavesdropper may succeed in inferring some information about M_{12} using M_2 and Z^n. On the other hand, for a sufficiently large n and $\tau_n > 0$, the first term in (25) is with high probability smaller than τ_n, if

$$R_\otimes + R_r \geq \mathbb{I}(\mathrm{X};\mathrm{Z}) + \delta_n(\tau_n). \tag{27}$$

Thus the whole expression in (25) is with high probability smaller than τ_n. Repeating the same steps for M_2, we can show that with high probability the individual leakage given by (3)

is also smaller than some τ_n. Now using Fourier-Motzkin elimination on the rate constraints given in (22), (24) and (27), followed by replacing X by a prefixed random variable V as in Lemma 1 and [3, Lemma 4] and taking the limit as $n \to \infty$, which implies that $\delta_n(\epsilon_n) \to 0$ and $\delta_n(\tau_n) \to 0$, leads the achievability of any rate pair (R_1, R_2) satisfying (21). ■

B. Multi-Letter Converse

Proposition 2. *The individual secrecy capacity region of the BC with receiver side information is upper bounded as follows*

$$R_1 \leq \lim_{n\to\infty} \frac{1}{n} \min \Big[\mathbb{I}(\mathrm{V};\mathrm{Y}_1^n) - \mathbb{I}(\mathrm{V};\mathrm{Z}^n) + nR_2, \mathbb{I}(\mathrm{V};\mathrm{Y}_1^n)\Big]$$
$$R_2 \leq \lim_{n\to\infty} \frac{1}{n} \min \Big[\mathbb{I}(\mathrm{V};\mathrm{Y}_2^n) - \mathbb{I}(\mathrm{V};\mathrm{Z}^n) + nR_1, \mathbb{I}(\mathrm{V};\mathrm{Y}_2^n)\Big]$$

for random variables satisfying the Markov chain $\mathrm{V} - \mathrm{X}^n - (\mathrm{Y}_1^n, \mathrm{Y}_2^n, \mathrm{Z}^n)$.

Proof: Suppose that for some $\epsilon_n, \tau_n > 0$ and sufficiently large n, there exists a $(2^{nR_1}, 2^{nR_2}, n)$ code $\mathcal{C}_n$ such that (4) is satisfied, where $L(\mathcal{C}_n)$ satisfies (3). We have

$$\begin{aligned} R_1 &\overset{(a)}{\leq} \frac{1}{n}\Big[\mathbb{I}(\mathrm{M}_1\mathrm{M}_2;\mathrm{Y}_1^n) - \mathbb{I}(\mathrm{M}_1;\mathrm{Z}^n)\Big] + \gamma(\epsilon_n,\tau_n) \\ &= \frac{1}{n}\Big[\mathbb{I}(\mathrm{M}_1\mathrm{M}_2;\mathrm{Y}_1^n) - \mathbb{I}(\mathrm{M}_1\mathrm{M}_2;\mathrm{Z}^n) + \mathbb{I}(\mathrm{M}_2;\mathrm{Z}^n|\mathrm{M}_1)\Big] \\ &\quad + \ \gamma(\epsilon_n,\tau_n) \\ &\overset{(b)}{\leq} \frac{1}{n}\Big[\mathbb{I}(\mathrm{M}_1\mathrm{M}_2;\mathrm{Y}_1^n) - \mathbb{I}(\mathrm{M}_1\mathrm{M}_2;\mathrm{Z}^n)\Big] + R_2 + \gamma(\epsilon_n,\tau_n) \end{aligned} \tag{28}$$

where (a) follows from (3) and (4); while (b) follows as $\mathbb{I}(\mathrm{M}_2;\mathrm{Z}^n|\mathrm{M}_1) = \mathbb{H}(\mathrm{M}_2|\mathrm{M}_1) - \mathbb{H}(\mathrm{M}_2|\mathrm{M}_1\mathrm{Z}^n) \leq nR_2$. If we use $\mathrm{V} \triangleq (\mathrm{M}_1, \mathrm{M}_2)$ in (11) and (28), then take the limit as $n \to \infty$, so $\gamma(\epsilon_n)$ and $\gamma(\epsilon_n, \tau_n) \to 0$, where the convergence of the limit is guaranteed by the Fekete's lemma [15], we reach the upper bound of R_1. Repeating the same steps for R_2 completes our proof and establishes a multi-letter description for the capacity region similarly as in Section III-B. ■

C. More Capable Channels

Theorem 2. *The individual secrecy capacity region of the more capable BC with receiver side information is the set of all rate pairs* $(R_1, R_2) \in \mathbb{R}_+^2$ *that satisfy*

$$\begin{aligned} R_1 &\leq \min\Big[\mathbb{I}(\mathrm{X};\mathrm{Y}_1) - \mathbb{I}(\mathrm{X};\mathrm{Z}) + R_2 \ , \ \mathbb{I}(\mathrm{X};\mathrm{Y}_1)\Big] \\ R_2 &\leq \min\Big[\mathbb{I}(\mathrm{X};\mathrm{Y}_2) - \mathbb{I}(\mathrm{X};\mathrm{Z}) + R_1 \ , \ \mathbb{I}(\mathrm{X};\mathrm{Y}_2)\Big] \end{aligned} \tag{29}$$

for random variables with joint probability distribution $Q_{\mathrm{X}}(x)\ Q_{\mathrm{Y}_1\mathrm{Y}_2\mathrm{Z}|\mathrm{X}}(y_1, y_1, z|x)$.

Proof: The achievability follows as in the proof of Lemma 2, while for the converse, we start by highlighting the standard single-letter bound

$$R_j \leq \mathbb{I}(\mathrm{X};\mathrm{Y}_j) + \gamma(\epsilon_n), \qquad j = 1, 2. \tag{30}$$

We then compare (12) and (28). Now using the same steps used in the converse of the more capable channel in the previous section for both R_1 and R_2, we reach the following

$$\begin{aligned} R_1 &\leq \mathbb{I}(\mathrm{X};\mathrm{Y}_1) - \mathbb{I}(\mathrm{X};\mathrm{Z}) + R_2 + \gamma(\epsilon_n,\tau_n) \\ R_2 &\leq \mathbb{I}(\mathrm{X};\mathrm{Y}_2) - \mathbb{I}(\mathrm{X};\mathrm{Z}) + R_1 + \gamma(\epsilon_n,\tau_n). \end{aligned} \tag{31}$$

Combining (30) and (31), then take the limit as $n \to \infty$, such that $\gamma(\epsilon_n)$ and $\gamma(\epsilon_n, \tau_n) \to 0$ completes our converse. ■

V. Conclusion

We studied the broadcast channel with receiver side information, where the transmitter sends confidential messages to the legitimate receivers while keeping the eavesdropper ignorant. We measured this ignorance by two secrecy criteria: the joint secrecy and the individual one. For each criterion we derived an achievable rate region and a corresponding multi-letter converse. We established the secrecy capacity of the class of more capable channels which includes both less noisy and degraded ones by providing a single-letter converse. Our analysis illustrated that loosening the secrecy criterion from the joint to the individual one, induces an increase on the secrecy capacity. This increase arises from using one message as a secret key for the other one. However, doing so might threaten the secrecy of each message upon revealing the other one to the eavesdropper.

References

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

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

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

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

[5] 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.

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

[7] T. J. Oechtering, C. Schnurr, I. Bjelaković, and H. Boche, "Broadcast capacity region of two-phase bidirectional relaying," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 454–458, Jan. 2008.

[8] X. Tang, R. Liu, P. Spasojevic, and H. Poor, "Multiple access channels with generalized feedback and confidential messages," in *IEEE Inf. Theory Workshop*, Bergen, Norway, Sep. 2007, pp. 608–613.

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

[10] R. F. Wyrembelski, A. Sezgin, and H. Boche, "Secrecy in broadcast channels with receiver side information," in *Signals, Systems and Computers (ASILOMAR), 2011 Conference Record of the Forty Fifth Asilomar Conference on*, Nov. 2011, pp. 290–294.

[11] 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.

[12] J. Hou and G. Kramer, "Effective secrecy: Reliability, confusion and stealth," Nov. 2013, available online at arxiv.org.

[13] 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.

[14] R. F. Wyrembelski, T. J. Oechtering, and H. Boche, "MIMO Gaussian bidirectional broadcast channels with common messages," *IEEE Trans. Wireless Commun.*, vol. 10, no. 9, pp. 2950–2959, Sep. 2011.

[15] M. Fekete, "Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten," *Math. Z.*, vol. 17, no. 1, pp. 228–249, 1923.

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