Secrecy Measures for Broadcast Channels With Receiver Side Information: Joint vs Individual

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 the transmission of a common message and three confidential messages over a broadcast channel with two legitimate receivers and an eavesdropper. Each legitimate receiver is interested in decoding two of the three confidential messages, while having the third one as side information. In order to measure the ignorance of the eavesdropper about the confidential messages, we investigate two different secrecy criteria: joint secrecy and individual secrecy. For both criteria, we provide a general achievable rate region. We establish both the joint and individual secrecy capacity if the two legitimate receivers are less noisy than the eavesdropper. We further investigate the scenario where the eavesdropper is less noisy than the two legitimate receivers. It is known that the joint secrecy constraints can not be fulfilled under this scenario, however, we manage to establish a non vanishing capacity region for the individual secrecy case.**

I. Introduction

Shannon [1] studied the problem of secure communication and proved that it can only 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 one common and one confidential message over a BC with two receivers and one eavesdropper. They provided a general achievable region and managed to establish the capacity when the two receivers are less noisy than the eavesdropper. In this paper, we study a related problem. However, in stead of having only one confidential message to both legitimate receivers, we extend the system such that each legitimate receiver has an extra individual confidential message. This extension allows us to differentiate between joint and individual secrecy. Our setup has an additional feature, that each legitimate receiver possesses the individual confidential message of the other one as side information as shown in Figure 1. In [6] the problem of BC with receiver side information also known as BC with message cognition was investigated but without any secrecy requirements. The authors provided an achievable region and establish the capacity for some special cases. Secure communication over BC with receiver side information 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 for multiple access channels. Our work focuses on the succeeding broadcast phase, where the relay encodes and transmits the previously received confidential messages in addition to another confidential message to both legitimate receivers and a common message for all three nodes. A simpler version of this problem was investigated in [10], where different achievable rate regions and an outer bound were provided.

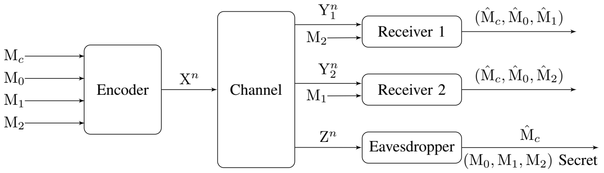

Fig. 1. Broadcast channel with two legitimate receivers and one eavesdropper, where side information is available at the two legitimate receivers

This paper is organized as follows. In Section II, we state the problem then present and discuss the two secrecy criteria that we study: joint secrecy and individual secrecy. In Sections III and IV, we provide achievable rate regions for each secrecy criterion. We also establish the secrecy capacity for some classes of less noisy channels. Our results indicate that individual secrecy can provide a larger capacity region even if the joint secrecy capacity is zero.

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 in Figure 1 is given by

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

978-1-4799-5999-0/14/$31.00 ©2014 IEEE

Definition 1. *A* $(2^{nR_c}, 2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n)$ *code* $\mathcal{C}_n$ *for the BC with receiver side information consists of: four independent message sets* $\mathcal{M}_c$*,* $\mathcal{M}_0$*,* $\mathcal{M}_1$*, and* $\mathcal{M}_2$*, a source of local randomness* $\mathcal{R}$ *at the encoder, an encoding function at the relay node*

$$E : \mathcal{M}_c \times \mathcal{M}_0 \times \mathcal{M}_1 \times \mathcal{M}_2 \times \mathcal{R} \to \mathcal{X}^n$$

which maps a common message $m_c \in \mathcal{M}_c$*, a confidential message triple* $(m_0, m_1, m_2) \in \mathcal{M}_0 \times \mathcal{M}_1 \times \mathcal{M}_2$ *and a realization of the local randomness* $r \in \mathcal{R}$ *to a codeword* $x^n(m_c, m_0, m_1, m_2, r)$*, and three decoders, one for each node*

$$\begin{aligned}
&\varphi_1 : \mathcal{Y}_1^n \times \mathcal{M}_2 \to \mathcal{M}_c \times \mathcal{M}_0 \times \mathcal{M}_1 \cup \{?\}\\
&\varphi_2 : \mathcal{Y}_2^n \times \mathcal{M}_1 \to \mathcal{M}_c \times \mathcal{M}_0 \times \mathcal{M}_2 \cup \{?\}\\
&\varphi_3 : \mathcal{Z}^n \to \mathcal{M}_c \cup \{?\}
\end{aligned}$$

that maps each channel observation at the respective node and its own message to the corresponding required messages or an error message $\{?\}$.

The $(2^{nR_c}, 2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n)$ code $\mathcal{C}_n$ is known to the two legitimate receivers and the eavesdropper as well. We assume that the messages $\mathrm{M_c}$, $\mathrm{M_0}$, $\mathrm{M_1}$ and $\mathrm{M_2}$ are chosen uniformly at random. The reliability performance of the code $\mathcal{C}_n$ is measured in terms of its average probability of error

$$\begin{aligned}
P_e(\mathcal{C}_n) \triangleq &\mathbb{P}\big[\check{\mathrm{M}}_\mathrm{c} \neq \mathrm{M_c} \text{ or } (\hat{\mathrm{M}}_\mathrm{c}, \hat{\mathrm{M}}_0, \hat{\mathrm{M}}_1) \neq (\mathrm{M_c}, \mathrm{M_0}, \mathrm{M_1})\\
&\text{or } (\tilde{\mathrm{M}}_\mathrm{c}, \tilde{\mathrm{M}}_0, \tilde{\mathrm{M}}_2) \neq (\mathrm{M_c}, \mathrm{M_0}, \mathrm{M_2}) | \mathcal{C}_n\big], \qquad (1)
\end{aligned}$$

where $(\hat{\mathrm{M}}_\mathrm{c}, \hat{\mathrm{M}}_0, \hat{\mathrm{M}}_1)$, $(\tilde{\mathrm{M}}_\mathrm{c}, \tilde{\mathrm{M}}_0, \tilde{\mathrm{M}}_2)$ and $\check{\mathrm{M}}_\mathrm{c}$ are the estimated messages at the two legitimate receivers and the eavesdropper respectively. In order to measure the ignorance of the eavesdropper about the confidential messages $\mathrm{M_0}$, $\mathrm{M_1}$ and $\mathrm{M_2}$, we consider two different secrecy criteria.

1. *Joint Secrecy:* This criterion requires the leakage of the confidential messages of one user to the eavesdropper given the individual message of the other user to be small.
$$L(\mathcal{C}_n) \triangleq \mathbb{I}(\mathrm{M_0M_1}; \mathrm{Z}^n | \mathrm{M_2M_c}) + \mathbb{I}(\mathrm{M_0M_2}; \mathrm{Z}^n | \mathrm{M_1M_c}). \qquad (2)$$
2. *Individual Secrecy:* This criterion requires the leakage of the confidential message of each user to the eavesdropper to be small as follows:
$$L(\mathcal{C}_n) \triangleq \mathbb{I}(\mathrm{M_0M_1}; \mathrm{Z}^n | \mathrm{M_c}) + \mathbb{I}(\mathrm{M_0M_2}; \mathrm{Z}^n | \mathrm{M_c}) \qquad (3)$$

Definition 2. *A rate quadruple* $(R_c, R_0, R_1, R_2) \in \mathbb{R}_+^4$ *is achievable for the BC with receiver side information, if there exists a sequence of* $(2^{nR_c}, 2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n)$ *codes* $\{\mathcal{C}_n\}_n$*, where* n *is large enough, such that*

$$P_e(\mathcal{C}_n) \leq \epsilon_n \qquad \text{and} \qquad L(\mathcal{C}_n) \leq \tau_n, \qquad (4)$$
$$\text{where } \lim_{n\to\infty} \epsilon_n, \tau_n = 0.$$

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

The difference between the two criteria in (2) and (3) is that, in the joint secrecy the two legitimate receivers do not trust each other and every one is responsible for protecting his own message, while in the individual secrecy the two legitimate receivers cooperate to protect their messages. This implies that the joint secrecy is a more conservative criterion. In fact any code that satisfies the joint secrecy criterion also satisfies the individual one. This is because

$$\mathbb{I}(\mathrm{M_0M_1}; \mathrm{Z}^n | \mathrm{M_c}) \leq \mathbb{I}(\mathrm{M_0M_1}; \mathrm{Z}^n | \mathrm{M_2M_c}),$$

as long as the messages are independent. However, we will show that, individual secrecy has some interesting features as compared to the joint one. In particular, we will show that the individual secrecy can provide non negative secrecy rate when the joint secrecy capacity is zero. While in general it has a bigger achievable region compared to the joint one.

III. The Joint Secrecy Capacity Region

A. Achievable Secrecy Rate Region

Lemma 1. *An achievable joint secrecy rate region for the BC with receiver side information is given by the set of all rates* $(R_c, R_0, R_1, R_2) \in \mathbb{R}_+^4$ *that satisfy*

$$\begin{aligned}
R_c &\leq \min\Big[\mathbb{I}(\mathrm{U}; \mathrm{Y_1}), \mathbb{I}(\mathrm{U}; \mathrm{Y_2}), \mathbb{I}(\mathrm{U}; \mathrm{Z})\Big]\\
R_0 + R_1 &\leq \mathbb{I}(\mathrm{V_0V_1}; \mathrm{Y_1}|\mathrm{U}) - \mathbb{I}(\mathrm{V_0V_1}; \mathrm{Z}|\mathrm{U})\\
R_0 + R_2 &\leq \mathbb{I}(\mathrm{V_0V_2}; \mathrm{Y_2}|\mathrm{U}) - \mathbb{I}(\mathrm{V_0V_2}; \mathrm{Z}|\mathrm{U})\\
2R_0 + R_1 + R_2 &\leq \mathbb{I}(\mathrm{V_0V_1}; \mathrm{Y_1}|\mathrm{U}) + \mathbb{I}(\mathrm{V_0V_2}; \mathrm{Y_2}|\mathrm{U})\\
&-\mathbb{I}(\mathrm{V_0}; \mathrm{Z}|\mathrm{U}) - \mathbb{I}(\mathrm{V_0V_1V_2}; \mathrm{Z}|\mathrm{U}) - \mathbb{I}(\mathrm{V_1}; \mathrm{V_2}|\mathrm{V_0}) \qquad (5)
\end{aligned}$$

for random variables with joint probability distribution $Q(u)$ $Q(v_0|u)$ $Q(v_1, v_2|v_0)$ $Q(x|v_1, v_2)$ $W(y_1, y_1, z|x)$.

Proof: The proof combines the techniques of superposition random coding [3] in addition to Marton coding as in [5] along with different strong secrecy techniques [11, 12]. We consider two groups of message sets. The first group contains the sets of common and confidential messages $\mathcal{M}_c$, $\mathcal{M}_0$, $\mathcal{M}_1$ and $\mathcal{M}_2$. Additionally we use $\mathcal{M} = \mathcal{M}_0 \times \mathcal{M}_1 \times \mathcal{M}_2$. The second group contains the sets of randomization indices $\mathcal{M}_r$, $\mathcal{M}_{r_1}$, and $\mathcal{M}_{r_2}$ in addition to the sets $\mathcal{M}_{t_1}$ and $\mathcal{M}_{t_2}$ needed for Marton coding. In general, any message set $\mathcal{M}_a$ is identified as $\mathcal{M}_a = [\![1, 2^{nR_a}]\!]$.

Random Codebook and Encoder: Fix an input distribution $Q(u, v_0, v_1, v_2, x)$. Construct the codewords $u^n(m_c)$ for $m_c \in \mathcal{M}_c$ by generating symbols $u_i(m_c)$ with $i \in [\![1, n]\!]$ independently according to $Q(u)$. For every $u^n(m_c)$, generate codewords $v_0^n(m_c, m, m_r)$ for $m \in \mathcal{M}$ and $m_r \in \mathcal{M}_r$ by generating symbols $v_{0_i}(m_c, m, m_r)$ independently at random according to $Q(v_0|u_i(m_c))$. Next, for each $v_0^n(m_c, m, m_r)$ generate the codewords $v_1^n(m_c, m, m_r, m_{r_1}, m_{t_1})$ and $v_2^n(m_c, m, m_r, m_{r_2}, m_{t_2})$ for $m_{r_1} \in \mathcal{M}_{r_1}$, $m_{r_2} \in \mathcal{M}_{r_2}$, $m_{t_1} \in \mathcal{M}_{t_1}$ and $m_{t_2} \in \mathcal{M}_{t_2}$ by generating symbols $v_{1_i}(m_c, m, m_r, m_{r_1}, m_{t_1})$ and $v_{2_i}(m_c, m, m_r, m_{r_2}, m_{t_2})$ independently at random according to $Q(v_1|v_{0_i}(m_c, m, m_r))$ and $Q(v_2|v_{0_i}(m_c, m, m_r))$ respectively. To transmit a message pair (m_c, m), the encoder 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 $v_1^n(m_c, m, m_r, m_{r_1}, m_{t_1})$ and $v_2^n(m_c, m, m_r, m_{r_2}, m_{t_2})$ are jointly typical. Finally, it generates a codeword x^n independently at random according to $\Pi_{i=1}^n Q(x_i|v_{1_i}, v_{2_i})$ and transmits it.

Decoders: The decoding is based on joint typicality as follows: The first decoder outputs $(\hat{m}_c, \hat{m}_0, \hat{m}_1, \hat{m}_r, \hat{m}_{r_1}, \hat{m}_{t_1})$, if

$\big(u^n(\hat{m}_c), v_0^n(\hat{m}_c, \hat{m}, \hat{m}_r), v_1^n(\hat{m}_c, \hat{m}, \hat{m}_r, \hat{m}_{r_1}, \hat{m}_{t_1}), y_1^n\big)$ are jointly typical, where $\hat{m} = (\hat{m}_0, \hat{m}_1, m_2)$. The second decoder functions in a similar way, while the third decoder outputs $\check{m}_c$, if $\big(u^n(\check{m}_c), z^n\big)$ are jointly typical.

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

$$\begin{aligned}\hat{P}_e(\mathcal{C}_n) \triangleq \mathbb{P}\big[&\check{\mathrm{M}}_c \neq \mathrm{M}_c \text{ or } (\hat{\mathrm{M}}_c, \hat{\mathrm{M}}_0, \hat{\mathrm{M}}_1, \hat{\mathrm{M}}_{r_1}, \hat{\mathrm{M}}_{t_1}) \neq \\ &(\mathrm{M}_c, \mathrm{M}_0, \mathrm{M}_1, \mathrm{M}_{r_1}, \mathrm{M}_{t_1}) \text{ or } (\tilde{\mathrm{M}}_c, \tilde{\mathrm{M}}_0, \tilde{\mathrm{M}}_2, \tilde{\mathrm{M}}_{r_2}, \tilde{\mathrm{M}}_{t_2}) \\ &\neq (\mathrm{M}_c, \mathrm{M}_0, \mathrm{M}_2, \mathrm{M}_{r_2}, \mathrm{M}_{t_2})\big]. \end{aligned} \tag{6}$$

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

$$\begin{aligned} R_c &\leq \min\Big[\mathbb{I}(\mathrm{U};\mathrm{Y}_1), \mathbb{I}(\mathrm{U};\mathrm{Y}_2), \mathbb{I}(\mathrm{U};\mathrm{Z})\Big] - \delta_n(\epsilon_n) \\ R_0 + R_1 + R_r + R_{r_1} + R_{t_1} &\leq \mathbb{I}(\mathrm{V}_0\mathrm{V}_1;\mathrm{Y}_1|\mathrm{U}) - \delta_n(\epsilon_n) \\ R_0 + R_2 + R_r + R_{r_2} + R_{t_2} &\leq \mathbb{I}(\mathrm{V}_0\mathrm{V}_2;\mathrm{Y}_2|\mathrm{U}) - \delta_n(\epsilon_n) \\ R_{t_1} + R_{t_2} &\geq \mathbb{I}(\mathrm{V}_1;\mathrm{V}_2|\mathrm{V}_0) + \delta_n(\epsilon_n). \end{aligned} \tag{7}$$

On the other hand, based on strong secrecy approaches in [11, 12], for a sufficiently large n and $\tau_n > 0$, the joint leakage given in (2) is with high probability smaller than τ_n if

$$\begin{aligned} R_r &\geq \mathbb{I}(\mathrm{V}_0;\mathrm{Z}|\mathrm{U}) + \delta_n(\tau_n) \\ R_r + R_{r_1} + R_{t_1} &\geq \mathbb{I}(\mathrm{V}_0\mathrm{V}_1;\mathrm{Z}|\mathrm{U}) + \delta_n(\tau_n) \\ R_r + R_{r_2} + R_{t_2} &\geq \mathbb{I}(\mathrm{V}_0\mathrm{V}_2;\mathrm{Z}|\mathrm{U}) + \delta_n(\tau_n) \\ R_r + R_{r_1} + R_{r_2} &\geq \mathbb{I}(\mathrm{V}_0\mathrm{V}_1\mathrm{V}_2;\mathrm{Z}|\mathrm{U}) + \delta_n(\tau_n). \end{aligned} \tag{8}$$

Combining (7) and (8), while using the Fourier-Motzkin elimination procedure and 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 quadrupole (R_c, R_0, R_1, R_2) satisfying (5). ■

B. Secrecy Capacity For Less Noisy Channels

Definition 3. *The channel $W(y|x)$ is said to be less noisy than the channel $W(z|x)$ denoted as $(\mathrm{Y} \succeq \mathrm{Z})$, if for every random variable V such that $\mathrm{V} - \mathrm{X} - (\mathrm{Y},\mathrm{Z})$ forms a Markov chain, we have*

$$\mathbb{I}(\mathrm{V};\mathrm{Y}) \geq \mathbb{I}(\mathrm{V};\mathrm{Z}).$$

Proposition 1. *Let $W(y,z|x)$ be a discrete memoryless BC, where $\mathrm{Y} \succeq \mathrm{Z}$. Consider two independent random variables M and W, such that $(\mathrm{M},\mathrm{W}) - \mathrm{X}^n - (\mathrm{Y}^n,\mathrm{Z}^n)$ forms a Markov chain. Then the following holds: $\mathbb{I}(\mathrm{M};\mathrm{Y}^n|\mathrm{W}) \geq \mathbb{I}(\mathrm{M};\mathrm{Z}^n|\mathrm{W})$.*

Proof: We start by defining $\Delta = \frac{1}{n}\big[\mathbb{I}(\mathrm{M};\mathrm{Z}^n|\mathrm{W}) - \mathbb{I}(\mathrm{M};\mathrm{Y}^n|\mathrm{W})\big]$ and prove that if $\mathrm{Y} \succeq \mathrm{Z}$, then $\Delta \leq 0$, this directly implies our proposition. Let $\mathrm{U}_i \triangleq (\mathrm{W}, \tilde{\mathrm{Z}}^{i+1}, \mathrm{Y}^{i-1})$ and $\mathrm{V}_i \triangleq (\mathrm{M}, \mathrm{U}_i)$, where $\tilde{\mathrm{Z}}^{i+1} = (\mathrm{Z}_{i+1}, \dots, \mathrm{Z}_n)$. We have

$$\begin{aligned} \Delta &= \frac{1}{n}\sum_{i=1}^{n} \mathbb{I}(\mathrm{M};\mathrm{Z}_i|\mathrm{W}\tilde{\mathrm{Z}}^{i+1}) - \mathbb{I}(\mathrm{M};\mathrm{Y}_i|\mathrm{W}\mathrm{Y}^{i-1}) \\ &\overset{(a)}{=} \frac{1}{n}\sum_{i=1}^{n} \mathbb{I}(\mathrm{M};\mathrm{Z}_i|\mathrm{W}\tilde{\mathrm{Z}}^{i+1}\mathrm{Y}^{i-1}) - \mathbb{I}(\mathrm{M};\mathrm{Y}_i|\mathrm{W}\tilde{\mathrm{Z}}^{i+1}\mathrm{Y}^{i-1}) \\ &= \frac{1}{n}\sum_{i=1}^{n} \mathbb{I}(\mathrm{V}_i;\mathrm{Z}_i|\mathrm{U}_i) - \mathbb{I}(\mathrm{V}_i;\mathrm{Y}_i|\mathrm{U}_i) \\ &\overset{(b)}{=} \mathbb{I}(\mathrm{V};\mathrm{Z}|\mathrm{U}) - \mathbb{I}(\mathrm{V};\mathrm{Y}|\mathrm{U}) \overset{(c)}{\leq} \mathbb{I}(\mathrm{V}^*;\mathrm{Z}) - \mathbb{I}(\mathrm{V}^*;\mathrm{Y}) \overset{(d)}{\leq} 0 \end{aligned}$$

where (a) follows from the Csiszár sum identity [3, Lemma 7]; (b) follows by using an independent uniformly distributed randomization variable; (c) follows as V^* is distributed as $Q(v|u = u^*)$, where u^* is the value of U that maximizes the difference and (d) follows since $\mathrm{V}^* - \mathrm{X} - (\mathrm{Y},\mathrm{Z})$ forms a Markov chain and $\mathrm{Y} \succeq \mathrm{Z}$. ■

Theorem 1. *The joint secrecy capacity region of the BC with receiver side information if $\mathrm{Y}_1 \succeq \mathrm{Z}$ and $\mathrm{Y}_2 \succeq \mathrm{Z}$ is the set of all rate quadrupole $(R_c, R_0, R_1, R_2) \in \mathbb{R}_+^4$ that satisfy*

$$\begin{aligned} R_c &\leq \mathbb{I}(\mathrm{U};\mathrm{Z}) \\ R_0 + R_1 &\leq \mathbb{I}(\mathrm{X};\mathrm{Y}_1|\mathrm{U}) - \mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}) \\ R_0 + R_2 &\leq \mathbb{I}(\mathrm{X};\mathrm{Y}_2|\mathrm{U}) - \mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}) \end{aligned}$$

for some (U,X), such that $\mathrm{U} - \mathrm{X} - (\mathrm{Y}_1,\mathrm{Y}_2,\mathrm{Z})$ forms a Markov chain. Further it suffices to have $|\mathrm{U}| \leq |\mathrm{X}| + 3$.

Proof: The achievability follows directly from Lemma 1 by letting $\mathrm{V}_0 = \mathrm{V}_1 = \mathrm{V}_2 = \mathrm{X}$ in (5) in addition to the properties of less noisy channels. For the converse, we start by the common rate R_c and let $\mathrm{U}_i \triangleq (\mathrm{M}_c, \tilde{\mathrm{Z}}^{i+1})$, we have

$$\begin{aligned} R_c &\overset{(a)}{\leq} \frac{1}{n}\min\Big[\mathbb{I}(\mathrm{M}_c;\mathrm{Y}_1^n|\mathrm{M}_2), \mathbb{I}(\mathrm{M}_c;\mathrm{Y}_2^n|\mathrm{M}_1), \mathbb{I}(\mathrm{M}_c;\mathrm{Z}^n)\Big] \\ &\quad + \gamma_c(\epsilon_n) \\ &\overset{(b)}{=} \frac{1}{n}\mathbb{I}(\mathrm{M}_c;\mathrm{Z}^n) + \gamma_c(\epsilon_n) \\ &\leq \frac{1}{n}\sum_{i=1}^{n}\mathbb{I}(\mathrm{M}_c\tilde{\mathrm{Z}}^{i+1};\mathrm{Z}_i) + \gamma_c(\epsilon_n) \\ &= \frac{1}{n}\sum_{i=1}^{n}\mathbb{I}(\mathrm{U}_i;\mathrm{Z}_i) + \gamma_c(\epsilon_n) \end{aligned} \tag{9}$$

where (a) follows from Fano's inequality as $\gamma_c(\epsilon_n) = 1/n + \epsilon_n R_c$ while (b) follows from Proposition 1 and the independence of the messages. Now consider $R_0 + R_1$ and let $\mathrm{M} \triangleq (\mathrm{M}_0, \mathrm{M}_1, \mathrm{M}_2)$, we can show that

$$\begin{aligned} R_0 + R_1 &\overset{(a)}{\leq} \frac{1}{n}\ \mathbb{I}(\mathrm{M}_0\mathrm{M}_1;\mathrm{Y}_1^n|\mathrm{M}_2\mathrm{M}_c) + \gamma_1(\epsilon_n) \\ &\leq \frac{1}{n}\ \mathbb{I}(\mathrm{M}_0\mathrm{M}_1\mathrm{M}_2;\mathrm{Y}_1^n|\mathrm{M}_c) + \gamma_1(\epsilon_n) \\ &\overset{(b)}{\leq} \frac{1}{n}\Big[\mathbb{I}(\mathrm{M};\mathrm{Y}_1^n|\mathrm{M}_c) - \mathbb{I}(\mathrm{M};\mathrm{Z}^n|\mathrm{M}_c)\Big] + \gamma_1(\epsilon_n, \tau_n) \end{aligned}$$

where (a) follows from Fano's inequality as $\gamma_1(\epsilon_n) = 1/n + \epsilon_n(R_0 + R_1)$ and (b) follows from (4) and (2), where $\gamma_1(\epsilon_n, \tau_n) = \big(\tau_n + \gamma_c(\epsilon_n)\big)/n + \gamma_1(\epsilon_n)$. Using the same steps we can drive a similar bound for $R_0 + R_2$ as:

$$R_0 + R_2 \leq \frac{1}{n}\Big[\mathbb{I}(\mathrm{M};\mathrm{Y}_2^n|\mathrm{M}_c) - \mathbb{I}(\mathrm{M};\mathrm{Z}^n|\mathrm{M}_c)\Big] + \gamma_2(\epsilon_n, \tau_n).$$

Using the same procedure used in [5] for less noisy channel, we have

$$\begin{aligned} R_0 + R_1 &\leq \frac{1}{n}\sum_{i=1}^{n}\Big[\mathbb{I}(\mathrm{X}_i;\mathrm{Y}_{1i}|\mathrm{U}_i) - \mathbb{I}(\mathrm{X}_i;\mathrm{Z}_i|\mathrm{U}_i)\Big] + \gamma_1(\epsilon_n, \tau_n) \\ R_0 + R_2 &\leq \frac{1}{n}\sum_{i=1}^{n}\Big[\mathbb{I}(\mathrm{X}_i;\mathrm{Y}_{2i}|\mathrm{U}_i) - \mathbb{I}(\mathrm{X}_i;\mathrm{Z}_i|\mathrm{U}_i)\Big] + \gamma_2(\epsilon_n, \tau_n). \end{aligned}$$

Now using an independent uniformly distributed randomization, then take the limit as $n \to \infty$ such that $\gamma_c(\epsilon_n)$, $\gamma_1(\epsilon_n, \tau_n)$ and $\gamma_2(\epsilon_n, \tau_n) \to 0$, completes our converse. ■

IV. The Individual Secrecy Capacity Region

A. Achievable Secrecy Rate Region

Lemma 2. *An achievable individual secrecy rate region for the BC with receiver side information is given by the set of all rates $(R_c, R_0, R_1 = R_{11} + R_{12}, R_2 = R_{21} + R_{22}) \in \mathbb{R}_+^4$ that satisfy*

$$\begin{aligned} R_c &\leq \min\Big[\mathbb{I}(\mathrm{U};\mathrm{Y}_1), \mathbb{I}(\mathrm{U};\mathrm{Y}_2), \mathbb{I}(\mathrm{U};\mathrm{Z})\Big] \\ R_{12} = R_{21} &\leq \min\Big[R_1, R_2, \mathbb{I}(\mathrm{V}_\otimes;\mathrm{Y}_1|\mathrm{U}), \mathbb{I}(\mathrm{V}_\otimes;\mathrm{Y}_2|\mathrm{U})\Big] \\ R_0 + R_{11} &\leq \Big[\mathbb{I}(\mathrm{V}_0\mathrm{V}_1;\mathrm{Y}_1|\mathrm{V}_\otimes) - \mathbb{I}(\mathrm{V}_0\mathrm{V}_1;\mathrm{Z}|\mathrm{V}_\otimes)\Big]^+ \\ R_0 + R_{22} &\leq \Big[\mathbb{I}(\mathrm{V}_0\mathrm{V}_2;\mathrm{Y}_2|\mathrm{V}_\otimes) - \mathbb{I}(\mathrm{V}_0\mathrm{V}_2;\mathrm{Z}|\mathrm{V}_\otimes)\Big]^+ \\ 2R_0 + R_{11} + R_{22} &\leq \Big[\mathbb{I}(\mathrm{V}_0\mathrm{V}_1;\mathrm{Y}_1|\mathrm{V}_\otimes) + \mathbb{I}(\mathrm{V}_0\mathrm{V}_2;\mathrm{Y}_2|\mathrm{V}_\otimes) \\ -\mathbb{I}(\mathrm{V}_1;\mathrm{V}_2|\mathrm{V}_0) &- \mathbb{I}(\mathrm{V}_0\mathrm{V}_1\mathrm{V}_2;\mathrm{Z}|\mathrm{V}_\otimes) - \mathbb{I}(\mathrm{V}_0;\mathrm{Z}|\mathrm{V}_\otimes)\Big]^+ \quad (10) \end{aligned}$$

for random variables with joint probability distribution $Q(u)$ $Q(v_\otimes|u)$ $Q(v_0|v_\otimes)$ $Q(v_1, v_2|v_0)$ $Q(x|v_1, v_2)$ $W(y_1, y_1, z|x)$ and $[a]^+$ is defined as the maximum between 0 and a.

Proof: The proof combines the techniques used in the previous section along with Shannon's cipher system. We consider the same message sets as in the previous section. Additionally, we divided each confidential individual messages set into two sets as follows: $\mathcal{M}_1 = \mathcal{M}_{11} \times \mathcal{M}_{12}$ and $\mathcal{M}_2 = \mathcal{M}_{21} \times \mathcal{M}_{22}$. We make sure that $\mathcal{M}_{12}$ and $\mathcal{M}_{21}$ to be of the same size and use them to construct $\mathcal{M}_\otimes$ by *Xoring* the corresponding elements of each. Further, we use $\mathcal{M} = \mathcal{M}_0 \times \mathcal{M}_{11} \times \mathcal{M}_{22} \times \mathcal{M}_\otimes$.

$$R_\otimes = R_{12} = R_{21} = \min[R_1, R_2]. \quad (11)$$

Random Codebook and Encoder: Fix an input distribution $Q(u, v_\otimes, v_0, v_1, v_2, x)$. Construct the codewords $u^n(m_c)$ for $m_c \in \mathcal{M}_c$ by generating symbols $u_i(m_c)$ with $i \in [\![1, n]\!]$ independently according to $Q(u)$. For every $u^n(m_c)$, generate codewords $v_\otimes^n(m_c, m_\otimes)$ for $m_\otimes \in \mathcal{M}_\otimes$ by generating symbols $v_{\otimes_i}(m_c, m_\otimes)$ independently at random according to $Q(v_\otimes|u_i(m_c))$. Next, continue with constructing the codebook using the same steps in Lemma 1. Now given a message pair (m_c, m), the encoder produces a codeword x^n using the same procedure in Lemma 1 as well.

Decoders: The first decoder outputs $(\hat{m}_c, \hat{m}_0, \hat{m}_1, \hat{m}_r, \hat{m}_{r_1}, \hat{m}_{t_1})$. First it finds the unique messages such that, $\big(u^n(\hat{m}_c), v_\otimes^n(\hat{m}_c, \hat{m}_\otimes), v_0^n(\hat{m}_c, \hat{m}, \hat{m}_r), v_1^n(\hat{m}_c, \hat{m}, \hat{m}_r, \hat{m}_{r_1}, \hat{m}_{t_1}), y_1^n\big)$ are jointly typical. Then, it computes $\hat{m}_{12}$ by *Xoring* m_{21} and $\hat{m}_\otimes$. The second decoder works in a similar way, while the third decoder is kept the same as in Lemma 1.

Reliability and Secrecy Analysis: Using the same average probability of error defined in (6) and the structure of the new codebook, the reliability conditions in (7) shall be modified such that any conditioning on U is replaced by conditioning on $\mathrm{V}_\otimes$ in addition to the following

$$R_\otimes \leq \min\Big[\mathbb{I}(\mathrm{V}_\otimes;\mathrm{Y}_1|\mathrm{U}), \mathbb{I}(\mathrm{V}_\otimes;\mathrm{Y}_2|\mathrm{U})\Big] - \delta_n(\epsilon_n). \quad (12)$$

This assures that for a sufficiently large n, with high probability $\hat{P}_e(\mathcal{C}_n) \leq \epsilon_n$. On the other hand, modifying the secrecy conditions in (8) by changing every conditioning on U to conditioning on $\mathrm{V}_\otimes$ guarantees that for a sufficiently large n, with high probability $\mathbb{I}(\mathrm{M}_0\mathrm{M}_{11};\mathrm{Z}^n) + \mathbb{I}(\mathrm{M}_0\mathrm{M}_{22};\mathrm{Z}^n) \leq \tau_n$. However, in order to prove that the individual secrecy given by (3) is $\leq \tau_n$, we need to prove that $\mathbb{I}(\mathrm{M}_{12};\mathrm{Z}^n|\mathrm{M}_0\mathrm{M}_{11})$ and $\mathbb{I}(\mathrm{M}_{21};\mathrm{Z}^n|\mathrm{M}_0\mathrm{M}_{22})$ are also small. This can be shown as follows:

$$\begin{aligned} \mathbb{I}(\mathrm{M}_{12};\mathrm{Z}^n|\mathrm{M}_0\mathrm{M}_{11}) &= \mathbb{H}(\mathrm{M}_{12}|\mathrm{M}_0\mathrm{M}_{11}) - \mathbb{H}(\mathrm{M}_{12}|\mathrm{Z}^n\mathrm{M}_0\mathrm{M}_{11}) \\ &\overset{(a)}{=} \mathbb{H}(\mathrm{M}_{12}) - \mathbb{H}(\mathrm{M}_{12}|\mathrm{Z}^n\mathrm{M}_0\mathrm{M}_{11}) \\ &\overset{(b)}{=} \mathbb{H}(\mathrm{M}_{12}) - \mathbb{H}(\mathrm{M}_{12}|\mathrm{M}_\otimes) \overset{(c)}{=} 0 \end{aligned}$$

where (a) follows because the messages are independent; (b) follows because the best the eavesdropper can do is to decode $\mathrm{M}_\otimes$; while (c) follows because of the 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 $\mathbb{H}(\mathrm{M}_{12})$. Using the same steps, we can prove that $\mathbb{I}(\mathrm{M}_{21};\mathrm{Z}^n|\mathrm{M}_0\mathrm{M}_{22}) = 0$.
Now combining (11), (12) and the modified versions of (7) and (8), 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 quadruple (R_c, R_0, R_1, R_2) satisfying (10). ■

B. Secrecy Capacity For Less Noisy Channels

Theorem 2. *The individual secrecy capacity region of the BC with receiver side information if $\mathrm{Y}_1 \succeq \mathrm{Z}$ and $\mathrm{Y}_2 \succeq \mathrm{Z}$ is the set of all rate quadruple $(R_c, R_0, R_1, R_2) \in \mathbb{R}_+^4$ that satisfy*

$$\begin{aligned} &R_c \leq \mathbb{I}(\mathrm{U};\mathrm{Z}) \\ &R_0{+}R_1 \leq \mathbb{I}(\mathrm{X};\mathrm{Y}_1|\mathrm{U}){-}\mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}){+}\min\Big[R_1, R_2, \mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U})\Big] \\ &R_0{+}R_2 \leq \mathbb{I}(\mathrm{X};\mathrm{Y}_2|\mathrm{U}){-}\mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}){+}\min\Big[R_1, R_2, \mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U})\Big] \end{aligned}$$

for some (U, X), such that $\mathrm{U} - \mathrm{X} - (\mathrm{Y}_1, \mathrm{Y}_2, \mathrm{Z})$ forms a Markov chain. Further it suffices to have $|\mathrm{U}| \leq |\mathrm{X}| + 3$.

Proof: The achievability proof is based on the same principle used in Lemma 2. We start by modifying the structure of the random codebook as follows: For every $u^n(m_c)$, we generate the codewords $x^n(m_c, m, m_r)$ by generating symbols $x_i(m_c, m, m_r)$ independently at random according to $Q(x|u_i(m_c))$. Now given a message pair (m_c, m), the encoder chooses a message m_r uniformly at random from the set $\mathcal{M}_r$ and transmits $x^n(m_c, m, m_r)$. This changes the decoder at the first legitimate receiver in the following way: It outputs $(\hat{m}_c, \hat{m}, \hat{m}_r)$, if it is the unique triple such that, $\big(u^n(\hat{m}_c), x^n(\hat{m}_c, \hat{m}, \hat{m}_r), y_1^n\big)$ is jointly typical. The decoder at the second legitimate receiver also changes in the same way, while the decoder as the eavesdropper is kept unchanged. Under the less noisy condition and the previous modifications, the reliability conditions in (12) changes as follows:

$$\begin{aligned} R_c &\leq \mathbb{I}(\mathrm{U};\mathrm{Z}) - \delta_n(\epsilon_n) \\ R_0 + R_{11} + R_\otimes + R_r &\leq \mathbb{I}(\mathrm{X};\mathrm{Y}_1|\mathrm{U}) - \delta_n(\epsilon_n) \\ R_0 + R_{22} + R_\otimes + R_r &\leq \mathbb{I}(\mathrm{X};\mathrm{Y}_2|\mathrm{U}) - \delta_n(\epsilon_n). \quad (13) \end{aligned}$$

On the other hand, the secrecy conditions in (8) simplifies to

$$R_\otimes + R_r \geq \mathbb{I}(\mathrm{X};\mathrm{Z}|\mathrm{U}) + \delta_n(\tau_n). \quad (14)$$

Now using Fourier-Motzkin elimination on the rate constraints given in (13) and (14) followed by taking the limit as $n \to \infty$, which implies that $\delta_n(\epsilon_n) \to 0$ and $\delta_n(\tau_n) \to 0$, completes the achievability proof. It is important to highlight the difference between the coding scheme of Lemma 2 and of this theorem. In this theorem, the *Xored* message $\mathcal{M}_\otimes$ is encoded in the same layer with wiretap encoded messages, such that it acts as an additional source of randomization. While in Lemma 2, it was encoded in a different layer. It is worth mentioning that the encoding scheme used in this theorem is only possible if the two legitimate receivers have a statistical advantage over the eavesdropper.

Now for the converse, we start by letting $\mathrm{U}_i \triangleq (\mathrm{M}_c, \tilde{\mathrm{Z}}^{i+1})$ and highlight the standard reliability upper bound when Y_1 and Y_2 are less noisy than Z given by:

$$\begin{aligned} R_0 + R_1 &\leq \frac{1}{n}\sum_{i=1}^{n} \mathbb{I}(\mathrm{X}_i; \mathrm{Y}_{1i}|\mathrm{U}_i) + \gamma_1(\epsilon_n) \\ R_0 + R_2 &\leq \frac{1}{n}\sum_{i=1}^{n} \mathbb{I}(\mathrm{X}_i; \mathrm{Y}_{2i}|\mathrm{U}_i) + \gamma_2(\epsilon_n) \qquad (15) \end{aligned}$$

We then consider the confidential rate of the first legitimate receiver $(R_0 + R_1)$ and let $\mathrm{M} = (\mathrm{M}_0, \mathrm{M}_1, \mathrm{M}_2)$. We have

$$\begin{aligned} R_0 + R_1 &\leq \frac{1}{n}\ \mathbb{I}(\mathrm{M}; \mathrm{Y}_1^n|\mathrm{M}_c) + \gamma_1(\epsilon_n) \\ &\overset{(a)}{\leq} \frac{1}{n}\Big[\mathbb{I}(\mathrm{M}; \mathrm{Y}_1^n|\mathrm{M}_c) - \max\big[\mathbb{I}(\mathrm{M}_0\mathrm{M}_1; \mathrm{Z}^n|\mathrm{M}_c), \\ &\quad \mathbb{I}(\mathrm{M}_0\mathrm{M}_2; \mathrm{Z}^n|\mathrm{M}_c)\big]\Big] + \gamma_1(\epsilon_n, \tau_n) \\ &= \frac{1}{n}\Big[\mathbb{I}(\mathrm{M}; \mathrm{Y}_1^n|\mathrm{M}_c) - \mathbb{I}(\mathrm{M}; \mathrm{Z}^n|\mathrm{M}_c) + \min\big[\mathbb{I}(\mathrm{M}_1; \mathrm{Z}^n| \\ &\quad \mathrm{M}_0\mathrm{M}_2\mathrm{M}_c), \mathbb{I}(\mathrm{M}_2; \mathrm{Z}^n|\mathrm{M}_0\mathrm{M}_1\mathrm{M}_c)\big]\Big] + \gamma_1(\epsilon_n, \tau_n) \\ &\overset{(b)}{\leq} \frac{1}{n}\Big[\mathbb{I}(\mathrm{M}; \mathrm{Y}_1^n|\mathrm{M}_c) - \mathbb{I}(\mathrm{M}; \mathrm{Z}^n|\mathrm{M}_c)\Big] \\ &\quad + \min\big[R_1, R_2\big] + \gamma_1(\epsilon_n, \tau_n) \qquad (16) \end{aligned}$$

where (a) follows from (3) and (4); while (b) follows because $R_1 \geq \mathbb{I}(\mathrm{M}_1; \mathrm{Z}^n|\mathrm{M}_0\mathrm{M}_2\mathrm{M}_c)$ and $R_2 \geq \mathbb{I}(\mathrm{M}_2; \mathrm{Z}^n|\mathrm{M}_0\mathrm{M}_1\mathrm{M}_c)$. Repeating the previous steps for $(R_0 + R_2)$, we have

$$\begin{aligned} R_0 + R_2 \leq \frac{1}{n}\Big[\mathbb{I}(\mathrm{M}; \mathrm{Y}_2^n|\mathrm{M}_c) - \mathbb{I}(\mathrm{M}; \mathrm{Z}^n|\mathrm{M}_c)\Big] \\ + \min\big[R_1, R_2\big] + \gamma_1(\epsilon_n, \tau_n) \qquad (17) \end{aligned}$$

Now following the same procedure used in the proof of the converse of Theorem 1 along with (15), followed by using an independent uniformly distributed randomization variable, then take the limit as $n \to \infty$ such that $\gamma_c(\epsilon_n)$, $\gamma_1(\epsilon_n, \tau_n)$ and $\gamma_2(\epsilon_n, \tau_n) \to 0$, completes our converse. ■

Theorem 3. *The individual secrecy capacity region of the BC with receiver side information if* $\mathrm{Z} \succeq \mathrm{Y}_1$ *and* $\mathrm{Z} \succeq \mathrm{Y}_2$ *is the set of all rate triples* $(R_c, R_1, R_2) \in \mathbb{R}_+^3$ *that satisfy*

$$R_c + R_1 = R_c + R_2 \leq \min\Big[\mathbb{I}(\mathrm{X}; \mathrm{Y}_1), \mathbb{I}(\mathrm{X}; \mathrm{Y}_2)\Big]$$

for some X, *such that* $\mathrm{X} - (\mathrm{Y}_1, \mathrm{Y}_2, \mathrm{Z})$ *forms a Markov chain.*

Proof: The achievability follows directly the properties of less noisy channels and Lemma 2 by letting $\mathrm{V}_\otimes = \mathrm{X}$ in (10). Now for the converse, we start by R_0 and proof that if Z is less noisy than Y_1, R_0 vanishes.

$$\begin{aligned} R_0 &\overset{(a)}{\leq} \frac{1}{n}\Big[\mathbb{I}(\mathrm{M}_0\mathrm{M}_2; \mathrm{Y}_1^n|\mathrm{M}_c) - \mathbb{I}(\mathrm{M}_0\mathrm{M}_2; \mathrm{Z}^n|\mathrm{M}_c)\Big] + \gamma_0(\epsilon_n, \tau_n) \\ &\overset{(b)}{\leq} \gamma_0(\epsilon_n, \tau_n) \end{aligned}$$

where (a) follows from (3) and (4) while (b) follows from Proposition 1. On the other hand if Z is less noisy than Y_1 and Y_2, (16) and (17) simplify to

$$R_1 \leq R_2 + \gamma_1(\epsilon_n, \tau_n) \quad \text{and} \quad R_2 \leq R_1 + \gamma_2(\epsilon_n, \tau_n)$$

This implies that $R_1 = R_2$. Now using the trivial upper bound of reliable transmission, completes our converse. ■

V. Conclusion

We studied the transmission of common and confidential messages over a broadcast channel with receiver side information. We measured the secrecy of the transmission by two criteria: the joint secrecy and the individual one. For each criterion we derived a general achievable rate region. Further, we established the secrecy capacity for two classes of less noisy channels. Our results indicates that the individual secrecy has a bigger capacity region as compared to the joint one, this increase arises from the usage of one message as a secret key for the other one which can not be done for the joint secrecy. The individual secrecy can provide a non negative secrecy rates, even if the joint secrecy constraints can not be fulfilled. However, the individual secrecy requires the mutual trust of the legitimate receivers and thus it is more vulnerable.

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] T. J. Oechtering, M. Wigger, and R. Timo, "Broadcast capacity regions with three receivers and message cognition," in *Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on*, Cambridge, MA, USA, July 2012, pp. 388–392.

[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] 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.

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