On the Individual Secrecy for Gaussian Broadcast Channels with Receiver Side Information

Yanling Chen, O. Ozan Koyluoglu, Aydin Sezgin

***Abstract*—This paper studies the individual secrecy capacity region of the broadcast channel with receiver side information. First, an achievable rate region is established for the discrete memoryless case by employing superposition coding. Further, it is extended to the corresponding Gaussian case, where the individual secrecy capacity region is characterized in case of a weak or strong eavesdropper (compared to two legitimate receivers). For the case left, inner and outer bounds are established and the individual secrecy capacity region is characterized for the low and high SNR regimes. Note that the last case is distinctive due to the individual secrecy constraint, in the sense that positive rate pair is still possible although the eavesdropper may have the advantage against at least one of the legitimate receivers over the channel, unlike the situation if the joint secrecy constraint is imposed.**

I. Introduction

In this paper, we consider the problem of secure communication over the broadcast channel with receiver side information (BC-RSI) as shown in Fig. 1. In this model, the transmitter wants to send two independent messages to two receivers which have, respectively, the desired message of the other receiver (already available in their possession, e.g., due to previous communications) as side information.

Note that the broadcasting capacity region of BC-RSI (Fig. 1 without an eavesdropper) is completely characterized in [1]. For BC-RSI with an external eavesdropper, the authors in [2] proposed achievable rate regions and outer bounds subject to a *joint* secrecy constraint (whereby the information leakage from *both* messages to the eavesdropper is made vanishing). Differently from [2], we focus on the problem under *individual* secrecy constraints that aims to minimize the information leakage from *each* message to the eavesdropper [3]. A parallel work [4] has considered both the joint secrecy and individual secrecy aspects of BC-RSI. Nevertheless, both [3] and [4] considered only the discrete memoryless case.

This work is a continuation of our previous study on BC-RSI with individual secrecy constraints [3]. As mentioned in [3], the concept of *individual secrecy* is motivated by the fact that a joint secrecy constraint can be difficult or even impossible to fulfill in certain cases. For instance, if the eavesdropper has the same or a better channel observation than at least one of the legitimate receivers, then under joint secrecy constraint, positive rate pair for both legitimate receivers is not possible at all. In such cases, the individual secrecy serves as a more realistic and affordable security solution.

The work of Yanling Chen and Aydin Sezgin is supported by the German Research Foundation, Deutsche Forschungsgemeinschaft (DFG), Germany, under grant SE 1697/11.

The main contributions of the paper are as follows. First, we propose an achievable individual secrecy rate region (which generalizes the results provided in [3], [4]) by employing superposition coding. Further, the coding scheme is extended to Gaussian case to characterize the individual secrecy capacity region in case of a weak or strong eavesdropper (compared to two legitimate receivers), and to derive an inner bound in case that the eavesdropper's channel is stronger than one receiver but weaker than the other. In particular, for the last case, we also provide an outer bound, which together with the inner bound, gives the individual secrecy capacity region for the low and high SNR regimes.

II. System model

Consider a discrete memoryless broadcast channel given by $p(y_1, y_2, z|x)$ with two legitimate receivers and one passive eavesdropper, as shown in Fig. 1. The transmitter aims to send messages m_1, m_2 to the legitimate receiver $1, 2$, respectively. Suppose x^n is the channel input to convey m_1, m_2 in n channel uses, whilst y_1^n (at receiver 1), y_2^n (at receiver 2) and z^n (at eavesdropper), are the channel outputs. Besides, m_2 (available at receiver 1) and m_1 (available at receiver 2), serve also as side information that may help to decode the desired message.

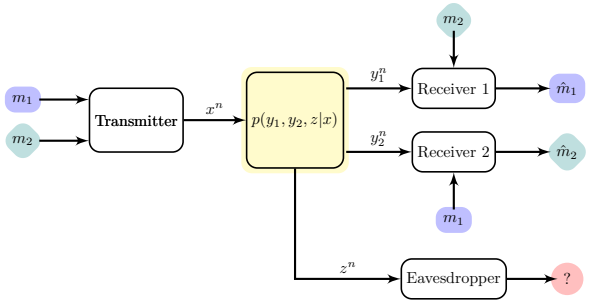

Fig. 1: BC-RSI with an external eavesdropper.

Denote the average probability of decoding error at receiver i as $P_{e,i}$. The rate pair (R_1, R_2) is said to be *achievable*, if for any $\epsilon > 0$, there exists an encoder-decoder

pair such that

$$\frac{1}{n}H(M_i) \geq R_i - \epsilon \tag{1}$$

$$P_{e,i} \leq \epsilon \tag{2}$$

$$\frac{1}{n}I(M_i; Z^n) \leq \epsilon, \tag{3}$$

for $i = 1, 2$ and for sufficiently large n. Note that (1) corresponds to the targeted transmission *rate*; (2) corresponds to the *reliability* constraint at the legitimate receivers; while (3) corresponds to the *individual* secrecy constraints against the eavesdropper.

III. Discrete memoryless BC-RSI with an external eavesdropper

Theorem 1. *An achievable individual secrecy rate region for BC-RSI is given by the set of non-negative rate pairs* (R_1, R_2) *such that*

$$R_1 \leq \min\left\{ \begin{array}{l} I(V;Y_1|U) + \min\{I(U;Y_1), I(U;Y_2)\}, \\ I(V;Y_1|U) - I(V;Z|U) + R_2 \end{array} \right\},$$

$$R_2 \leq \min\left\{ \begin{array}{l} I(V;Y_2|U) + \min\{I(U;Y_1), I(U;Y_2)\}, \\ I(V;Y_2|U) - I(V;Z|U) + R_1 \end{array} \right\},$$

over all $p(u)p(v|u)p(x|v)$ *subject to* $I(V;Y_i|U) \geq I(V;Z|U)$ *for* $i = 1, 2$.

Proof: To establish the achievability of the above region, we utilize the superposition coding with embedded one-time pad and secrecy coding approaches.

Rate splitting: We split $M_1 = (M_{1k}, M_{1sk}, M_{1s})$ and $M_2 = (M_{2k}, M_{2sk}, M_{2s})$, with both M_{1k} and M_{2k} of entropy nR_k, both M_{1sk} and M_{2sk} of entropy nR_{sk}, M_{1s} of entropy nR_{1s} and M_{2s} of entropy nR_{2s}. Thus we have $R_1 = R_k + R_{sk} + R_{1s}$ and $R_2 = R_k + R_{sk} + R_{2s}$.

Codebook generation: Fix $p(u), p(v|u)$. First, randomly generate 2^{nR_k} i.i.d sequences $u^n(k)$, $k \in [1 : 2^{nR_k}]$, according to $p(u)$. Secondly, for each $u^n(k)$, according to $p(v|u)$, randomly generate i.i.d sequences $v^n(k, sk, 1s, 2s, r)$ with $(sk, 1s, 2s, r) \in [1 : 2^{nR_{sk}}] \times [1 : 2^{nR_{1s}}] \times [1 : 2^{nR_{2s}}] \times [1 : 2^{nR_r}]$.

Encoding: To send messages (m_1, m_2), choose $u^n(k)$, where $k = m_k \triangleq m_{1k} \oplus m_{2k}$. Given $u^n(k)$, randomly choose $r \in [1 : 2^{nR_r}]$ and find $v^n(k, m_{sk}, m_{1s}, m_{2s}, r)$, where $m_{sk} \triangleq m_{1sk} \oplus m_{2sk}$. Generate x^n according to $p(x|v)$, and transmit it over the channel.

Decoding: Receiver 2, upon receiving y_2^n, finds $u^n(\hat{k})$ such that $(u^n(\hat{k}), y_2^n)$ is jointly typical. With the knowledge of m_{1k}, decode $\hat{m}_{2k} = m_{1k} \oplus \hat{k}$. Corresponding to $u^n(\hat{k})$, with the knowledge of m_1, further find $v^n(\hat{k}, \hat{m}_{sk}, m_{1s}, \hat{m}_{2s}, \hat{r})$ which is jointly typical with y_2^n; and decode $\hat{m}_{2sk} = (m_{1sk} \oplus \hat{m}_{sk})$. Thus, $\hat{m}_2 = (\hat{m}_{2k}, \hat{m}_{2sk}, \hat{m}_{2s})$.

Receiver 1, upon receiving y_1^n, finds $u^n(\tilde{k})$ such that $(u^n(\tilde{k}), y_1^n)$ is jointly typical. Corresponding to $u^n(\tilde{k})$, further find $v^n(\tilde{k}, \tilde{m}_{sk}, \tilde{m}_{1s}, m_{2s}, \tilde{r})$ which is jointly typical with y_1^n. With the knowledge of $m_2 = (m_{2k}, m_{2sk}, m_{2s})$, decode $\tilde{m}_1 = (m_{2k} \oplus \tilde{k}, m_{2sk} \oplus \tilde{m}_{sk}, \tilde{m}_{1s})$.

Analysis of the error probability of decoding: Assume that $(M_1, M_2) = (m_1, m_2)$ is sent. First consider $P_{e,2}$ at receiver 2. A decoding error happens iff one or more of the following events occur:

$$\begin{aligned}
\mathcal{E}_{21} =& \{(u^n(m_{1k} \oplus m_{2k}), y_2^n) \notin \mathcal{T}_\epsilon^{(n)}\}, \\
\mathcal{E}_{22} =& \{(u^n(m_{1k} \oplus m'_{2k}), y_2^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } m'_{2k} \neq m_{2k}\}, \\
\mathcal{E}_{23} =& \{(v^n(m_{1k} \oplus m_{2k}, m_{1sk} \oplus m_{2sk}, m_{1s}, m_{2s}, r), y_2^n) \notin \mathcal{T}_\epsilon^{(n)}\}, \\
\mathcal{E}_{24} =& \{(v^n(m_{1k} \oplus m_{2k}, m'_{sk}, m_{1s}, m'_{2s}, r'), y_2^n) \in \mathcal{T}_\epsilon^{(n)}, \\
& (m'_{sk}, m'_{2s}, r') \neq (m_{1sk} \oplus m_{2sk}, m_{2s}, r)\}.
\end{aligned}$$

Thus $P_{e,2}$ can be upper bounded by $P_{e,2} \leq \Pr(\mathcal{E}_{21}) + \Pr(\mathcal{E}_{22}) + \Pr(\mathcal{E}_{23}) + \Pr(\mathcal{E}_{24})$. By the LLN, $\Pr(\mathcal{E}_{21})$ and $\Pr(\mathcal{E}_{23})$ tends to zero as $n \to \infty$. For $\Pr(\mathcal{E}_{22})$, since $u^n(m'_{2k} \oplus m_{1k})$ is independent of $(u^n(m_{2k} \oplus m_{1k}), y_2^n)$ for $m'_{2k} \neq m_{2k}$, by the packing lemma [5], $\Pr(\mathcal{E}_{22})$ tends to zero as $n \to \infty$ if

$$R_k < I(U; Y_2). \tag{4}$$

For $\Pr(\mathcal{E}_{24})$, note that if $(m'_{sk}, m'_{2s}, r') \neq (m_{1sk} \oplus m_{2sk}, m_{2s}, r)$, then for given $u^n(k)$ with $k = m_{1k} \oplus m_{2k}$, $v^n(k, m'_{sk}, m_{1s}, m'_{2s}, r')$ is independent of $(v^n(k, m_{1sk} \oplus m_{2sk}, m_{1s}, m_{2s}, r), y_1^n)$. By the packing lemma [5], $\Pr(\mathcal{E}_{24})$ tends to zero as $n \to \infty$ if

$$R_{sk} + R_{2s} + R_r < I(V; Y_2|U). \tag{5}$$

At receiver 1, the decoder makes an error iff one or more of the following events occur:

$$\begin{aligned}
\mathcal{E}_{11} =& \{(u^n(m_{1k} \oplus m_{2k}, y_1^n) \notin \mathcal{T}_\epsilon^{(n)}\}, \\
\mathcal{E}_{12} =& \{(u^n(m'_{1k} \oplus m_{2k}), y_1^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } m'_{1k} \neq m_{1k}\}, \\
\mathcal{E}_{13} =& \{(v^n(m_{1k} \oplus m_{2k}, m_{1sk} \oplus m_{2sk}, m_{1s}, m_{2s}, r), y_1^n) \notin \mathcal{T}_\epsilon^{(n)}\}, \\
\mathcal{E}_{14} =& \{(v^n(m_{1k} \oplus m_{2k}, m'_{sk}, m'_{1s}, m_{2s}, r'), y_1^n) \in \mathcal{T}_\epsilon^{(n)}, \\
& (m'_{sk}, m'_{1s}, r') \neq (m_{1sk} \oplus m_{2sk}, m_{1s}, r)\}.
\end{aligned}$$

So $P_{e,1}$ can be upper bounded by $P_{e,1} \leq \Pr(\mathcal{E}_{11}) + \Pr(\mathcal{E}_{12}) + \Pr(\mathcal{E}_{13}) + \Pr(\mathcal{E}_{14})$. By the LLN, $\Pr(\mathcal{E}_{11})$ and $\Pr(\mathcal{E}_{13})$ tend to zero as $n \to \infty$. For $\Pr(\mathcal{E}_{12})$, since $u^n(m_{2k} \oplus m'_{1k})$ is independent of $(u^n(m_{2k} \oplus m_{1k}), y_2^n)$ for $m'_{1k} \neq m_{1k}$, by the packing lemma [5], $\Pr(\mathcal{E}_{12})$ tends to zero as $n \to \infty$ if

$$R_k < I(U; Y_1). \tag{6}$$

For $\Pr(\mathcal{E}_{14})$, note that if $(m'_{sk}, m'_{1s}, r') \neq (m_{1sk} \oplus m_{2sk}, m_{1s}, r)$, then for given $u^n(k)$ with $k = m_{1k} \oplus m_{2k}$, $v^n(k, m'_{sk}, m'_{1s}, m_{2s}, r')$ is independent of $(v^n(k, m_{1sk} \oplus m_{2sk}, m_{1s}, m_{2s}, r), y_1^n)$. By the packing lemma [5], it tends to zero as $n \to \infty$ if

$$R_{sk} + R_{1s} + R_r < I(V; Y_1|U) \tag{7}$$

Analysis of individual secrecy: Due to the symmetric roles of receiver 1 and receiver 2, we only need to prove the secrecy of one message (e.g., M_1). The other (e.g., the secrecy of M_2) follows by a similar proof.

For the secrecy of M_1, we have

$$\begin{aligned}
I(M_1;Z^n) =& I(M_{1k}, M_{1sk}, M_{1s}; Z^n) \\
=& I(M_{1k};Z^n) + I(M_{1sk}, M_{1s}; Z^n|M_{1k}) \\
\overset{(a)}{=}& I(M_{1sk}, M_{1s}; Z^n|M_{1k}) \\
=& I(M_{1sk};Z^n|M_{1k}) + I(M_{1s};Z^n|M_{1k}, M_{1sk}) \\
\overset{(b)}{=}& I(M_{1s};Z^n|M_{1k}, M_{1sk}) \\
=& H(M_{1s}) - H(M_{1s}|M_{1k}, M_{1sk}, Z^n) \\
\overset{(c)}{\leq}& nR_{1s} - H(M_{1s}|M_k, Z^n),
\end{aligned}$$

where (a) is due to the fact that $I(M_{1k};Z^n) = 0$ by $I(M_{1k};Z^n) \leq I(M_{1k};Z^n, M_k) = I(M_{1k};M_k) = 0$, which follows by the Markov chain $M_{1k} \to M_k \to Z^n$; (b) follows from the fact that $I(M_{1sk};Z^n|M_{1k}) = 0$ by

$$\begin{aligned}
H(M_{1sk}|Z^n, M_{1k}) \geq& H(M_{1sk}|Z^n, M_{1k}, M_k, M_{sk}) \\
=& H(M_{1sk}|M_k, M_{sk}) \\
=& H(M_{1sk}) = H(M_{1sk}|M_{1k});
\end{aligned}$$

(c) is due to the fact that $H(M_{1s}|M_{1k}, M_{1sk}, Z^n) \geq H(M_{1s}|M_{1k}, M_k, M_{1sk}, Z^n) = H(M_{1s}|M_k, Z^n)$, where the last equality is because M_{1k}, M_{1sk} are independent of M_{1s} given M_k, Z^n, which is due to the Markov chain $M_{1s} \to (Z^n, M_k) \to (M_{1k}, M_{1sk})$.

To complete the proof that $I(M_1;Z^n) \leq n\delta'(\epsilon)$, we show in the following that $H(M_{1s}, M_{2s}|M_k, Z^n) \geq n(R_{1s}+R_{2s}) - n\delta'(\epsilon)$, which implies that $H(M_{1s}|M_k, Z^n) \geq nR_{1s} - n\delta'(\epsilon)$.

$$\begin{aligned}
& H(M_{1s}, M_{2s}|M_k, Z^n) \overset{(d)}{=} H(M_{1s}, M_{2s}|U^n, Z^n) \\
=& H(M_{1s}, M_{2s}, Z^n|U^n) - H(Z^n|U^n) \\
=& H(M_{1s}, M_{2s}, Z^n, V^n|U^n) - H(V^n|U^n, M_{1s}, M_{2s}, Z^n) \\
& - H(Z^n|U^n) \\
=& H(V^n|U^n) + H(Z^n|U^n, V^n) - H(V^n|U^n, M_{1s}, M_{2s}, Z^n) \\
& - H(Z^n|U^n) \\
\overset{(e)}{\geq}& n(R_{sk} + R_{1s} + R_{2s} + R_e) + nH(Z|U,V) \\
& - nH(Z|U) - n\epsilon \\
\overset{(f)}{=}& n(R_{1s} + R_{2s}) - n\delta'(\epsilon)
\end{aligned}$$

where (d) is due to the fact that U^n is uniquely determined by M_k; (e) follows by $H(V^n|U^n) = n(R_{sk} + R_{1s} + R_{2s} + R_e)$ by the codebook construction and the choice of V^n is randomly chosen based on $M_K, M_{sk}, M_{1s}, M_{2s}$ which are presumed to be uniformly distributed; Moreover, since the channel is discrete memoryless, we have $H(Z^n|U^n, V^n) = \sum_{i=1}^n H(Z_i|U_i, V_i) = nH(Z|U,V)$; and, $H(V^n|U^n, M_{1s}, M_{2s}, Z^n) \leq n\epsilon$ due to Fano's inequality by taking

$$R_{sk} + R_r \leq I(V;Z|U) - \epsilon', \tag{8}$$

since the eavesdropper can decode V^n reliably by using typical set decoding given $(U^n, M_{1s}, M_{2s}, Z^n)$; and

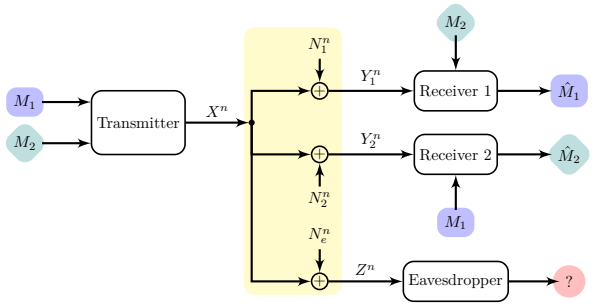

Fig. 2: Gaussian BC-RSI with an external eavesdropper.

$H(Z^n|U^n) = \sum_{i=1}^n H(Z_i|Z^{i-1}, U^n) \leq \sum_{i=1}^n H(Z_i|U_i) = nH(Z|U)$; (f) holds by taking

$$R_{sk} + R_r \geq I(V;Z|U) - 2\epsilon' \tag{9}$$

and $\delta'(\epsilon) = \epsilon + 2\epsilon'$.

Achievable individual secrecy rate region: Recall the non-negativity for rates, the equalities imposed by rate splitting, the conditions for reliable communication at both legitimate receivers, i.e., (4)-(7), and individual-secrecy at the eavesdropper, i.e., (8)-(9).

Eliminating $R_e, R_k, R_{sk}, R_{1s}, R_{2s}$ by applying Fourier-Motzkin procedure [5], we get the desired region. ■

Remark: Interestingly, we observe that:

1) Setting $Y_2 = \emptyset$, i.e., $R_2 = 0$, the region coincides with the secrecy capacity region of the wiretap channel [6].

2) Letting $R_k = 0$ (i.e., $U = \emptyset$) and $R_{sk} = 0$ and applying Fourier-Motzkin procedure, the derived region reduces to an achievable region under the joint-secrecy constraint (indicated by the above secrecy proof), which coincides with the one established in [2].

3) Letting $R_{2s} = 0$ and applying Fourier-Motzkin procedure, the derived region reduces to an achievable region which includes [3, Proposition 6].

4) Taking $U = V = X$, the region reduces to the one in [3, Proposition 3], which turns out to be the capacity region in case of a strong eavesdropper.

5) Taking $U = \emptyset$, the region reduces to the one in [4, Lemma 2]. Further taking $V = X$, it reduces to the one in [3, Proposition 5] and [4, Theorem 2], which turns out to be the capacity region in case of a weak eavesdropper.

IV. Gaussian BC-RSI with an external eavesdropper

In this section, we consider the discrete-time Gaussian BC-RSI as shown in Fig. 2. Suppose X is the channel input with a power constraint P and the signals received by both receivers and the eavesdropper are

$$\begin{aligned}
Y_1 &= X + N_1; \\
Y_2 &= X + N_2; \\
Z &= X + N_e,
\end{aligned}$$

where N_1, N_2 and N_e are additive white Gaussian noise (AWGN) independent of X. Without loss of generality,

we assume that $N_1 \sim \mathcal{N}(0, \sigma_1^2)$, $N_2 \sim \mathcal{N}(0, \sigma_2^2)$ and $N_e \sim \mathcal{N}(0, \sigma_e^2)$, respectively. According to the noise level in the channels to both receives and the eavesdropper, the overall channel can be regarded to be *stochastically* degraded in different orders. For simplicity, we only consider their corresponding *physically* degraded instances. The reason is that the same analysis can be easily extended to the stochastically degraded cases. So the following scenarios are of our interest (w.l.o.g., we assume $\sigma_1 < \sigma_2$):

1) $\sigma_e^2 \geq \sigma_2^2 \geq \sigma_1^2$, i.e., $X \to Y_1 \to Y_2 \to Z$ forms a Markov chain,
2) $\sigma_2^2 \geq \sigma_1^2 \geq \sigma_e^2$, i.e., $X \to Z \to Y_1 \to Y_2$ forms a Markov chain, and
3) $\sigma_2^2 \geq \sigma_e^2 \geq \sigma_1^2$, i.e., $X \to Y_1 \to Z \to Y_2$ forms a Markov chain.

The individual secrecy capacity of the first two cases can be derived by extending the aforementioned achievability scheme for discrete memoryless channel model to the Gaussian scenario (and, the converse follows from [3, Proposition 3 & Proposition 5]). For the third case, we show in the following subsections that we can approach the individual secrecy capacity region as $P \gg \sigma_2^2$ or $P \ll \sigma_1^2$.

A. An outer bound

Proposition 2. *An outer bound of the individual secrecy capacity region for the Gaussian BC-RSI when $X \to Y_1 \to Z \to Y_2$ forms a Markov chain is given by the set of the rate pairs (R_1, R_2) satisfying*

$$\begin{aligned} R_2 \leq & C\left(\frac{(1-\gamma\alpha)P}{\gamma\alpha P + \sigma_2^2}\right); \\ R_2 \leq R_1 \leq & C\left(\frac{\alpha P}{\sigma_1^2}\right) - C\left(\frac{\alpha P}{\sigma_e^2}\right) + R_2, \end{aligned}$$

for some $\alpha, \gamma \in [0,1]$, and $C(x) = \frac{1}{2}\log(1+x)$ is the Gaussian capacity function.

Proof: We observe that

$$\begin{aligned} \frac{n}{2}\log 2\pi e\sigma_e^2 &= h(Z^n|X^n) = h(Z^n|M_1, M_2, X^n) \\ &\leq h(Z^n|M_1, M_2) \leq h(Z^n|M_2) \leq h(Z^n) \\ &\overset{(a)}{\leq} \frac{n}{2}\log 2\pi e(P + \sigma_e^2), \end{aligned}$$

where (a) is due to the fact that for a random variable with a fixed variance, Gaussian distribution maximizes the entropy. It implies that there exist $\alpha, \gamma \in [0,1]$, such that

$$h(Z^n|M_2) = \frac{n}{2}\log 2\pi e(\alpha P + \sigma_e^2); \tag{10}$$

$$h(Z^n|M_1, M_2) = \frac{n}{2}\log 2\pi e(\gamma\alpha P + \sigma_e^2). \tag{11}$$

In particular, we have

$$\begin{aligned} h(Z^n|M_1) &= h(Z^n) - I(M_1; Z^n) \overset{(b)}{\geq} h(Z^n) - nO(\epsilon) \\ &\geq h(Z^n|M_2) - nO(\epsilon) \\ &= \frac{n}{2}\log 2\pi e(\alpha P + \sigma_e^2) - nO(\epsilon), \end{aligned} \tag{12}$$

which (b) is due to the individual secrecy constraint.

Similarly, we have

$$\begin{aligned} \frac{n}{2}\log 2\pi e\sigma_2^2 &= h(Y_2^n|X^n) = h(Y_2^n|M_1, M_2, X^n) \\ &\leq h(Y_2^n|M_1, M_2) \leq h(Y_2^n|M_1) \leq H(Y_2^n) \\ &\overset{(a)}{\leq} \frac{n}{2}\log 2\pi e(P + \sigma_2^2). \end{aligned}$$

There must exist a β such that

$$h(Y_2^n|M_1, M_2) = \frac{n}{2}\log 2\pi e(\beta P + \sigma_2^2). \tag{13}$$

Therefore,

$$\begin{aligned} nR_2 = H(M_2) &= H(M_2|M_1) \overset{(c)}{=} I(M_2; Y_2^n|M_1) + nO(\epsilon) \\ &= h(Y_2^n|M_1) - h(Y_2^n|M_1, M_2) + nO(\epsilon) \\ &\overset{(d)}{\leq} \frac{n}{2}\log\frac{P + \sigma_2^2}{\beta P + \sigma_2^2} + nO(\epsilon), \end{aligned} \tag{14}$$

where (c) is by Fano's inequality and (d) is due to (13).

Recall the Markov chain $(M_1, M_2) \to X^n \to Y_1^n \to Z^n \to Y_2^n$. Applying the conditional entropy power inequality (EPI) [5, p.22], we obtain

$$h(Y_2^n|M_1, M_2) \geq \frac{n}{2}\log\left[2^{\frac{2}{n}h(Z^n|M_1,M_2)} + 2\pi e(\sigma_2^2 - \sigma_e^2)\right].$$

In addition to (13), we have

$$h(Z^n|M_1, M_2) \leq \frac{n}{2}\log 2\pi e(\beta P + \sigma_e^2).$$

Comparing to (11) which gives that $h(Z^n|M_1, M_2) = \frac{n}{2}\log 2\pi e(\gamma\alpha P + \sigma_e^2)$, we have $\gamma\alpha \leq \beta$. Further, recall (14) and we obtain

$$\begin{aligned} nR_2 &\leq \frac{n}{2}\log\frac{P + \sigma_2^2}{\beta P + \sigma_2^2} + nO(\epsilon) \leq \frac{n}{2}\log\frac{P + \sigma_2^2}{\gamma\alpha P + \sigma_2^2} + nO(\epsilon) \\ &= nC\left(\frac{(1-\gamma\alpha)P}{\gamma\alpha P + \sigma_2^2}\right) + nO(\epsilon). \end{aligned} \tag{15}$$

Letting $\epsilon \to 0$, we obtain the desired upper bound for R_2

Now we proceed to bound R_1. First we show $R_1 \geq R_2$ as follows.

$$\begin{aligned} nR_1 =& H(M_1) = H(M_1|M_2) \\ \geq& I(M_1; Y_1^n|M_2) \\ =& I(M_1; Y_1^n, Z^n|M_2) - I(M_1; Z^n|M_2, Y_1^n) \\ \overset{(e)}{=}& I(M_1; Z^n|M_2) + I(M_1; Y_1^n|M_2, Z^n) \\ =& h(Z^n|M_2) - h(Z^n|M_1, M_2) + I(M_1; Y_1^n|M_2, Z^n) \\ \geq& h(Z^n|M_2) - h(Z^n|M_1, M_2) \\ \overset{(f)}{\geq}& h(Z^n) - h(Z^n|M_1, M_2) - nO(\epsilon) \\ \geq& h(Z^n|M_1) - h(Z^n|M_1, M_2) - nO(\epsilon) \\ =& I(M_2; Z^n|M_1) - nO(\epsilon) \\ \overset{(g)}{\geq}& I(M_2; Y_2^n|M_1) - nO(\epsilon) \\ =& H(M_2|M_1) - H(M_2|M_1, Y_2^n) - nO(\epsilon) \\ \overset{(h)}{\geq}& nR_2 - nO(\epsilon), \end{aligned} \tag{16}$$

where (e) follows by the fact that $I(M_1;Z^n|M_2,Y_1^n)=0$, which is implied by $I(M_1,M_2;Z^n|Y_1^n)=0$ due to the channel degradedness, i.e., the Markov chain $(M_1,M_2)\to X^n\to Y_1^n\to Z^n\to Y_2^n$; (f) is due to the individual secrecy constraint; and (g) is due to the channel degradedness, i.e., $(M_1,M_2)\to X^n\to Y_1^n\to Z^n\to Y_2^n$; (h) is due to the Fano's inequality. Finally, letting $\epsilon\to 0$, we derive $R_1\geq R_2$.

On the other hand, we have

$$\begin{aligned}
nR_1 =&H(M_1)=H(M_1|M_2)\\
\overset{(i)}{\leq}&I(M_1;Y_1^n|M_2)+nO(\epsilon)\\
=&I(M_1;Y_1^n,Z^n|M_2)-I(M_1;Z^n|M_2,Y_1^n)+nO(\epsilon)\\
\overset{(j)}{=}&I(M_1;Z^n|M_2)+I(M_1;Y_1^n|M_2,Z^n)+nO(\epsilon)\\
=&h(Z^n|M_2)-h(Z^n|M_1,M_2)\\
&+I(M_1;Y_1^n|M_2,Z^n)+nO(\epsilon),
\end{aligned}\tag{17}$$

where (i) is due to the Fano's inequality and (j) is due to the channel degradedness. Note that

$$\begin{aligned}
&I(M_1;Y_1^n|M_2,Z^n)\\
&=h(Y_1^n|M_2,Z^n)-h(Y_1^n|M_1,M_2,Z^n)\\
&\leq h(Y_1^n|M_2,Z^n)-h(Y_1^n|M_1,M_2,X^n,Z^n)\\
&=h(Y_1^n|M_2,Z^n)-h(Y_1^n|X^n,Z^n)\\
&=h(Y_1^n,Z^n|M_2)-h(Z^n|M_2)-h(Y_1^n|X^n,Z^n)\\
&\overset{(k)}{=}h(Y_1^n|M_2)+h(Z^n|Y_1^n)-h(Z^n|M_2)\\
&-h(Y_1^n,Z^n|X^n)+h(Z^n|X^n)\\
&\overset{(k)}{=}h(Y_1^n|M_2)+h(Z^n|Y_1^n)-h(Z^n|M_2)\\
&-h(Y_1^n|X^n)-h(Z^n|Y_1^n)+h(Z^n|X^n)\\
&=h(Y_1^n|M_2)-h(Z^n|M_2)-h(Y_1^n|X^n)+h(Z^n|X^n),
\end{aligned}\tag{18}$$

where (k) follows by the fact that $h(Z^n|M_2,Y_1^n)=h(Z^n|Y_1^n)$ and $h(Z^n|X^n,Y_1^n)=h(Z^n|Y_1^n)$ due to the Markov chain $(M_1,M_2)\to X^n\to Y_1^n\to Z^n$.

Recall the Markov chain $(M_1,M_2)\to X^n\to Y_1^n\to Z^n\to Y_2^n$. We apply the conditional EPI [5, p.22] and obtain

$$h(Z^n|M_2)\geq\frac{n}{2}\log\left[2^{\frac{n}{2}h(Y_1^n|M_2)}+2\pi e(\sigma_e^2-\sigma_1^2)\right].$$

In addition to (10) which gives that $h(Z^n|M_2)=\frac{n}{2}\log 2\pi e(\alpha P+\sigma_e^2)$, we have

$$h(Y_1^n|M_2)\leq\frac{n}{2}\log 2\pi e(\alpha P+\sigma_1^2).\tag{19}$$

Combining (17) and (18), we have

$$\begin{aligned}
nR_1\leq&h(Z^n|M_2)-h(Z^n|M_1,M_2)+I(M_1;Y_1^n|M_2,Z^n)\\
\leq&h(Y_1^n|M_2)-h(Z^n|M_1,M_2)-h(Y_1^n|X^n)\\
&+h(Z^n|X^n)\\
=&h(Z^n|M_1)-h(Z^n|M_1,M_2)+h(Y_1^n|M_2)\\
&-h(Z^n|M_1)-h(Y_1^n|X^n)+h(Z^n|X^n)\\
=&I(M_2;Z^n|M_1)+h(Y_1^n|M_2)-h(Z^n|M_1)\\
&-h(Y_1^n|X^n)+h(Z^n|X^n)\\
\overset{(l)}{\leq}&nR_2+h(Y_1^n|M_2)-h(Z^n|M_1)-h(Y_1^n|X^n)+h(Z^n|X^n)\\
=&nR_2+h(Y_1^n|M_2)-h(Z^n|M_1)-h(N_1^n)+h(N_e^n)\\
\overset{(m)}{\leq}&nR_2+\frac{n}{2}\log\frac{(\alpha P+\sigma_1^2)\sigma_e^2}{(\alpha P+\sigma_e^2)\sigma_1^2}+nO(\epsilon)\\
=&nR_2+nC\left(\frac{\alpha P}{\sigma_1^2}\right)-nC\left(\frac{\alpha P}{\sigma_e^2}\right)+nO(\epsilon),
\end{aligned}\tag{20}$$

where (l) is due to the fact that $I(M_2;Z^n|M_1)\leq H(M_2)=nR_2$; and (m) is due to (12) and (19). Finally, letting $\epsilon\to 0$, we get the desired upper bound for R_1.

Letting $\epsilon\to 0$, (15), (16) and (20) together establish the outer bound. ∎

Remark: Interestingly, $\gamma=1$ corresponds to the joint secrecy constraint, since $\gamma=1$ implies that $h(Z^n|M_1,M_2)=h(Z^n)$ according to (11). However, in case of $(M_1,M_2)\to Y_1^n\to Z^n\to Y_2^n$, we have, under joint secrecy constraint, that

$$\begin{aligned}
nR_2=H(M_2)=I(M_2;Y_2^n|M_1)\leq I(M_1,M_2;Y_2^n)\\
\leq I(M_1,M_2;Y_2^n,Z^n)=I(M_1,M_2;Z^n)=0.
\end{aligned}$$

That is, only positive R_1 is possible. And, $R_1\leq C\left(P/\sigma_1^2\right)-C\left(P/\sigma_e^2\right)$ is obtained by taking $\alpha=1$ via Wyner's secrecy coding [7]. This is consistent with our observation in [3, Proposition 1].

B. An inner bound

Proposition 3. *An inner bound of the individual secrecy capacity region for the Gaussian BC-RSI in case that $X\to Y_1\to Z\to Y_2$ forms a Markov chain, is given by the set of the rate pairs (R_1,R_2) satisfying*

$$\begin{aligned}
R_2\leq&C\left(\frac{(1-\gamma\alpha)P}{\gamma\alpha P+\sigma_2^2}\right);\\
R_2\leq R_1\leq&C\left(\frac{\gamma\alpha P}{\sigma_1^2}\right)-C\left(\frac{\gamma\alpha P}{\sigma_e^2}\right)+R_2,
\end{aligned}$$

where $\alpha,\gamma\in[0,1]$.

Proof: For a fixed pair $\alpha,\gamma\in[0,1]$, one can derive an inner bound of (R_1,R_2) by applying superposition coding as described in the following.

Codebook generation: Randomly and independently generate 2^{nR_2} sequences $u^n(k)$, $k\in[1:2^{nR_2}]$, each i.i.d. $\mathcal{N}(0,(1-\gamma\alpha)P)$; and $2^{n(R_1-R_2+R_r)}$ sequences $v^n(s,r)$, $(s,r)\in[1:2^{n(R_1-R_2)}]\times[1:2^{nR_r}]$, each i.i.d. $\mathcal{N}(0,\gamma\alpha P)$.

Encoding: To send the message pair (m_1,m_2) with $m_1=(m_{1k},m_{1s})$, where m_{1k} is of the same length as m_2, the encoder encapsulates m_{1k} and m_2 in m_k with $m_k\triangleq m_{1k}\oplus m_2$, randomly chooses $r\in[1:2^{nR_r}]$, and transmits $x^n(m_1,m_2)=u^n(m_k)+v^n(m_{1s},r)$.

Decoding: Receiver 2 decodes m_k from $y_2^n=u^n(m_k)+(v^n(m_{1s},r)+n_2^n)$ while treating $v^n(m_{1s},r)$ as noise, and

further recovers m_2 with his knowledge of m_1. The probability of decoding error tends to zero as $n \to \infty$ if

$$R_2 \leq C\left(\frac{(1-\gamma\alpha)P}{\gamma\alpha P+\sigma_2^2}\right). \tag{21}$$

Receiver 1 uses successive cancellation. It first decodes m_k from $y_1^n = u^n(m_k) + (v^n(m_{1s}, r) + n_1^n)$ while treating $v^n(m_{1s}, r)$ as noise, and recovers part of m_1, i.e., m_{1k}, with the knowledge of m_2. The probability of this decoding error goes to zero as $n \to \infty$ if $R_2 \leq C\left(\frac{(1-\gamma\alpha)P}{\gamma\alpha P+\sigma_2^2}\right)$, since it implies that $R_2 \leq C\left(\frac{(1-\gamma\alpha)P}{\gamma\alpha P+\sigma_1^2}\right)$ by the fact that $\sigma_1^2 \leq \sigma_2^2$. (This implies that $R_2 \leq R_1$.) Then it subtracts off $u^n(m_k)$ and decodes $v^n(m_{1s}, r) + n_1^n$ to recover (m_{1s}, r) and thus m_{1s}, i.e., the rest of m_1. The probability of this decoding error tends to zero as $n \to \infty$ if

$$R_1 - R_2 + R_r \leq C\left(\frac{\gamma\alpha P}{\sigma_1^2}\right). \tag{22}$$

Secrecy: The eavesdropper could decode m_k from $z^n = u^n(m_k)+(v^n(m_{1s}, r)+n_e^n)$. However, m_k does not disclose any information about m_{1s} and m_2, individually. Subtracting off $u^n(m_k)$ from z^n, the eavesdropper gets a better observation $v^n(m_{1s}, r) + n_e^n$, which actually does not help to recover m_{1s} if

$$R_r \approx C\left(\frac{\gamma\alpha P}{\sigma_e^2}\right). \tag{23}$$

In other words, the secrecy of m_{1s} is guaranteed by the embedded secrecy coding in the choice of v^n.

As a conclusion, (R_1, R_2) is achievable under the individual secrecy constraints, once R_1, R_2, R_r satisfy (21), (22) and (23).

Eliminating R_r, we get the desired region of (R_1, R_2), which concludes our proof of achievability. ∎

C. Individual-secrecy capacity region

Proposition 4. *If $\sigma_2^2 \geq \sigma_e^2 \geq \sigma_1^2$, and $P \gg \sigma_e^2$ or $P \ll \sigma_1^2$, the individual secrecy capacity region for the Gaussian BC-RSI is given as the set of (R_1, R_2) satisfying*

$$\begin{aligned} R_2 \leq & C\left(\frac{(1-\gamma\alpha)P}{\gamma\alpha P+\sigma_2^2}\right); \\ R_1 \leq & C\left(\frac{\gamma\alpha P}{\sigma_1^2}\right) - C\left(\frac{\gamma\alpha P}{\sigma_e^2}\right) + R_2, \end{aligned}$$

where $\gamma, \alpha \in [0, 1]$.

Proof: Consider the gap between the inner and outer bounds derived in previous subsections. If we take the same choice of α, γ in both bounds, it is easy to see that the gap occurs only in R_1, which is

$$\begin{aligned} & C\left(\frac{\alpha P}{\sigma_1^2}\right) - C\left(\frac{\alpha P}{\sigma_e^2}\right) - C\left(\frac{\gamma\alpha P}{\sigma_1^2}\right) + C\left(\frac{\gamma\alpha P}{\sigma_e^2}\right) \\ =& \frac{1}{2}\log\frac{(\alpha P+\sigma_1^2)(\gamma\alpha P+\sigma_e^2)}{(\alpha P+\sigma_e^2)(\gamma\alpha P+\sigma_1^2)} \to 0, \end{aligned}$$

as $P \gg \sigma_e^2$ or $P \ll \sigma_1^2$, regardless of the values of α, γ. ∎

As a conclusion, we have the following proposition.

Proposition 5. *The individual secrecy capacity region for the Gaussian BC-RSI is the set of (R_1, R_2) satisfying*

- *as $\sigma_e^2 \geq \sigma_2^2 \geq \sigma_1^2$:*

$$\begin{aligned} R_1 \leq & \min\left\{C\left(\frac{P}{\sigma_1^2}\right) - C\left(\frac{P}{\sigma_e^2}\right) + R_2, C\left(\frac{P}{\sigma_1^2}\right)\right\}; \\ R_2 \leq & \min\left\{C\left(\frac{P}{\sigma_2^2}\right) - C\left(\frac{P}{\sigma_e^2}\right) + R_1, C\left(\frac{P}{\sigma_2^2}\right)\right\}, \end{aligned}$$

- *as $\sigma_2^2 \geq \sigma_1^2 \geq \sigma_e^2$:*

$$R_1 = R_2 \leq C\left(\frac{P}{\sigma_2^2}\right),$$

- *as $\sigma_2^2 \geq \sigma_e^2 \geq \sigma_1^2$, and $P \gg \sigma_e^2$ or $P \ll \sigma_1^2$:*

$$\begin{aligned} R_1 \leq & C\left(\frac{\gamma P}{\sigma_1^2}\right) - C\left(\frac{\gamma P}{\sigma_e^2}\right) + R_2; \\ R_2 \leq & C\left(\frac{(1-\gamma)P}{\gamma P+\sigma_2^2}\right), \quad \text{where } \gamma \in [0, 1]. \end{aligned}$$

V. Conclusion

In this paper, we studied the problem of secure communication over BC-RSI under the individual secrecy constraints. As a general result, we proposed an achievable individual secrecy rate region by employing superposition coding with embedded secret key and secrecy coding approaches. In addition, we investigate the corresponding Gaussian BC-RSI, where the capacity region is characterized not only for a weak or strong eavesdropper (compared to two legitimate receivers), but also for the low and high SNR regimes when the eavesdropper channel is stronger than one receiver but weaker than the other.

References

[1] G. Kramer and S. Shamai, "Capacity for classes of broadcast channels with receiver side information," in *Proc. 2007 IEEE Information Theory Workshop (ITW '07)*, Sep. 2007, pp. 313–318.

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

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

[4] A. Mansour, R. 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*, June 2014, pp. 369–373.

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

[6] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[7] A. D. Wyner, "The wire-tap channel," *Bell Systems Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.