On the Achievable Individual-Secrecy Rate Region for Broadcast Channels with Receiver Side Information

Yanling Chen*, O. Ozan Koyluoglu†, Aydin Sezgin*
* Chair of Communication Systems, Ruhr University Bochum, Germany. Email: {yanling.chen-q5g, aydin.sezgin}@rub.de.
† Department of Electrical and Computer Engineering, The University of Arizona. Email: ozan@email.arizona.edu.

***Abstract*—In this paper, we study the problem of secure communication over the broadcast channel with receiver side information, under the lens of individual secrecy constraints (i.e., information leakage from each message to an eavesdropper is made vanishing). Several coding schemes are proposed by extending known results in broadcast channels to this secrecy setting. In particular, individual secrecy provided via one-time pad signal is utilized in the coding schemes. As a result, we obtain an achievable rate region together with a characterization of the capacity region for special cases of either a *weak* or *strong* eavesdropper (compared to both legitimate receivers). Interestingly, the capacity region for the former corresponds to a line and the latter corresponds to a square with missing corners; a phenomenon occurring due to the coupling between user's rates. At the expense of having a weaker notion of security, positive secure transmission rates are always guaranteed, unlike the case of the joint secrecy constraint.**

I. Introduction

The broadcast channel is a fundamental communication model that involves transmission of independent messages to different users. The broadcast nature makes the communication very susceptible to eavesdropping. Therefore, it is desirable to offer a reliable communication with a certain level of security guarantee. In this paper, we consider an extension of the broadcast channel with an external eavesdropper as shown in Fig. 1. In this communication 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 due to previous communications) as side information. This setup is also related to the two-way relay channel for which partial capacity results (without an eavesdropper) are derived in [1].

The model of the broadcast channel with receiver side information (BC-RSI) with an external eavesdropper has been studied in [2]. The authors proposed achievable rate regions and outer bounds for 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. Although individual secrecy constraints are by definition weaker than the joint one, they nevertheless provide an acceptable security strength that keeps each legitimate receiver away from an invasion of secrecy. In addition, a joint secrecy constraint can be difficult or even impossible to fulfill in certain cases (for instance, as the eavesdropper has the same or better channel observation than at least one of the legitimate receivers). So, in this paper, our main concern is to characterize the fundamental limits of secure communications under the individual secrecy constraints for the BC-RSI model.

This work is supported by the German Research Foundation, Deutsche Forschungsgemeinschaft (DFG), Germany, under grant SE 1697/11.

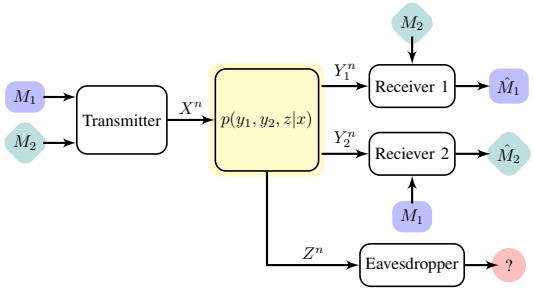

Fig. 1: Wiretap channel with receiver side information.

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. The transmitter aims to send messages m_1, m_2 to receiver $1, 2$, respectively. Suppose x^n is the channel input, 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. (Unless otherwise specified, we use capital letters for random variables and corresponding small cases for their realizations.)

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 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 (3) corresponds to the *individual* secrecy constraints. If the coding

scheme fulfills a stronger condition that

$$\frac{1}{n}I(M_1, M_2; Z^n) \leq \epsilon, \tag{4}$$

then it is said to satisfy the *joint* secrecy constraint.

III. An illustrative example

Consider a general model which consists of one transmitter, k legitimate receivers and one passive eavesdropper. The transmitter aims to broadcast k information bits $U^k = (U_1, U_2, \cdots, U_k)$ to k legitimate receivers with $U_i \sim \text{Bern}(1/2)$; whilst each receiver i holds already one piece of information U_i as side information. Suppose that the channels involved are all noiseless and U^k is encoded into $X^n = (X_1, X_2, \cdots, X_n)$ in the transmission. Then, for the purpose of broadcasting, each legitimate receiver i (which holds U_i and receives X^n) shall be able to recover the $k-1$ information bits $U^k \backslash \{U_i\}$, i.e.,

$$H(U^k|X^n, U_i) = 0. \tag{5}$$

Thus, we have

$$\begin{aligned} H(U^k|X^n) &= H(U^k, U_i|X^n) = H(U_i|X^n) + H(U^k|X^n, U_i) \\ &\overset{(6)}{=} H(U_i|X^n). \end{aligned} \tag{6}$$

Let us now consider the secrecy aspect of broadcasting. We note that the eavesdropper also receives a perfect copy of X^n.

1) For the *joint* secrecy constraint, we have that

$$H(U^k|X^n) = H(U^k). \tag{7}$$

Recall (6). We obtain

$$H(U^k|X^n) = H(U_i|X^n) \leq H(U_i) < H(U^k),$$

where the last inequality follows since $U_i \sim \text{Bern}(1/2)$. Thus, equality in (7) is not possible. That is, for this example, no broadcasting scheme could fulfill the *joint* secrecy constraint.

2) For the *individual* secrecy constraints, we have that

$$H(U_i|X^n) = H(U_i), \quad \text{for } 1 \leq i \leq k. \tag{8}$$

Suppose there is a coding scheme that fulfills both purposes of broadcasting, i.e., (5), and the individual secrecy, i.e., (8). Then, we have

$$\begin{aligned} H(U^k, X^n) &= H(U_i, X^n) + H(U_1^{i-1}, U_{i+1}^n|U_i, X^n) \\ &\overset{(a)}{=} H(X^n) + H(U_i|X^n) \\ &\overset{(b)}{=} H(X^n) + H(U_i), \end{aligned} \tag{9}$$

where (a) is due to (5); and (b) is due to (8). In addition to the fact that $H(U^k, X^n) \geq H(U^k)$, we have from (9) that

$$H(X^n) \geq H(U^k) - H(U_i) = k - 1.$$

So to say, the optimal encoding scheme (with respect to the overall transmission rate k/n) from U^k to X^n is such that $H(X^n) = k - 1$. Thus, to obtain the optimal rate, one shall take $n = k-1$. This is feasible. In fact, there are many coding schemes that could achieve this. One of the options is to take

$$x_i = u_1 \oplus u_{i+1}, \quad \text{for} \quad 1 \leq i \leq k-1.$$

The decoding at each receiver i is straightforward. And, the transmission rate R_i to each receiver i, for $1 \leq i \leq k$, is equal to 1, since $k-1$ bits are received in $n = k-1$ channel uses. Note that 1 is the capacity for a binary noiseless channel. This implies that the above scheme actually achieves the individual-secrecy capacity for all receivers.

We summarize the followings from this specific example:

- joint secrecy might be impossible to achieve;
- individual secrecy could be the highest secrecy level to offer (as shown in (6) on the equivocation at the eavesdropper);
- individual secrecy could be achieved without any penalty on the capacity-approaching rate region!

In fact, joint secrecy is impossible for a more general setup.

Proposition 1. *For the communication model as shown in Fig. 1 under the joint secrecy constraint, any rate pair $(R_1, R_2) \in \mathbb{R}^+$ is infeasible if the channel to at least one of the receivers is degraded with respect to the channel to the eavesdropper.*

Proof: Assume that receiver 2 receives Y_2^n as a degraded version of Z^n, the channel output at the eavesdropper. From the following analysis, we show that $R_2 > 0$ is not possible.

$$\begin{aligned} H(M_2) &= I(M_2; Y_2^n, M_1) + H(M_2|M_1, Y_2^n) \\ &\overset{(a)}{\leq} I(M_2; Y_2^n|M_1) + n\epsilon' \leq I(M_1, M_2; Y_2^n) + n\epsilon' \\ &\overset{(b)}{\leq} I(M_1, M_2; Z^n) + n\epsilon' \overset{(c)}{\leq} n(\epsilon + \epsilon'), \end{aligned}$$

where (a) is due to Fano's inequality; (b) is due to the channel degradedness, i.e., Markov chain $(M_1, M_2) \to Z^n \to Y_2^n$; and (c) is due to the joint secrecy constraint (4). This implies that $R_2 \leq \epsilon + \epsilon'$, which is arbitrarily small for an arbitrarily small $P_{e,2}$ (i.e., ϵ') and an arbitrarily small secrecy level ϵ. ■

For the BC-RSI under joint secrecy constraint, an achievable rate region was established in [2]. In the following sections, we will focus on deriving the achievable individual-secrecy rate regions for the BC-RSI model.

IV. Individual-Secrecy Rate Region

A. Secret key approach

Consider the symmetric secret rate region where $R_1 = R_2 = R$, i.e., M_1 and M_2 are of the same entropy. One can apply a one-time pad approach as proposed in [2]. With this scheme, the following rate region is achievable.

Proposition 2. *Any $(R_1, R_2) \in \mathbb{R}^+$ satisfying*

$$R_1 = R_2 \leq \min\{I(X; Y_1), I(X; Y_2)\}, \tag{10}$$

for any $p(x)$ is achievable.

Proof: Randomly generate 2^{nR} codewords x^n according to $p(x)$. Given (m_1, m_2), send $x^n(m_k)$ with $m_k = m_1 \oplus m_2$

to the channel. Both receivers can decode reliably by utilizing their side information to extract intended messages if $R_1 = R_2 \leq \min\{I(X;Y_1), I(X;Y_2)\}$.

For the secrecy of M_i, $i = 1, 2$ we have

$$I(M_i; Z^n) \leq I(M_i; Z^n, M_k) = I(M_i; M_k) = 0, \qquad (11)$$

where the 1st equality is due to Markov chain $M_i \to M_k \to Z^n$ by the coding scheme; and the 2nd follows as M_i is secured with a one-time pad M_j ($j \neq i$) in M_k. ■

Note that the above achievable region is limited by the capacity of the worse channel of the legitimate receivers. Nevertheless, it serves as the individual-secrecy capacity region in case that the eavesdropper has an advantage on the channel over both legitimate receivers.

Proposition 3. *If both channels to the legitimate receivers are degraded with respect to the channel to the eavesdropper, then the individual-secrecy capacity region is given by the union of $(R_1, R_2) \in \mathbb{R}^+$ pairs satisfying*

$$R_1 = R_2 \leq \min\{I(X;Y_1), I(X;Y_2)\}, \qquad (12)$$

where the union is taken over $p(x)$. See Fig. 2.

Proof: The achievablity follows from the proof of Proposition 2. Here, we detail the converse.

$$\begin{aligned} nR_1 = H(M_1) &= I(M_1; Y_1^n, M_2) + H(M_1|M_2, Y_1^n) \\ &\overset{(a)}{\leq} I(M_1; Y_1^n|M_2) + n\epsilon' \leq I(M_1, M_2; Y_1^n) + n\epsilon'; \\ &\overset{(b)}{\leq} I(X^n; Y_1^n) + n\epsilon' \overset{(c)}{=} \sum_{i=1}^{n} I(X_i; Y_{1,i}) + n\epsilon' \\ &\overset{(d)}{=} nI(X_Q; Y_{1,Q}|Q) + n\epsilon' \overset{(e)}{\leq} nI(X;Y_1) + n\epsilon'; \end{aligned}$$

Moreover, we have

$$\begin{aligned} nR_1 = H(M_1) &\leq I(M_1, M_2; Y_1^n) + n\epsilon' \\ &\overset{(f)}{\leq} I(M_1, M_2; Z^n) + n\epsilon' \\ &\overset{(g)}{\leq} I(M_2; Z^n|M_1) + n(\epsilon' + \epsilon) \\ &\leq H(M_2) + n(\epsilon' + \epsilon) \overset{(h)}{=} nR_2 + n(\epsilon' + \epsilon) \\ &\overset{(i)}{\leq} nI(X;Y_2) + n(\epsilon' + \epsilon) \end{aligned}$$

where (a) is due to Fano's inequality; (b) is due to Markov chain $(M_1, M_2) \to X^n \to Y_1^n$; (c) is since the channel is memoryless; (d) is by introducing a time-sharing random variable Q which is uniform over $1, 2, \ldots, n$; (e) is by taking $X = X_Q, Y_1 = Y_{1,Q}$; (f) is due to the channel degradedness, i.e., Markov chain $(M_1, M_2) \to Z^n \to Y_1^n$; (g) is by the individual secrecy constraint (3); (h) is due to $H(M_2) = nR_2$ and (i) is derived by applying a proof similar to $H(M_1) \leq nI(X;Y_1) + n\epsilon'$ and by taking $Y_2 = Y_{2,Q}$. As a conclusion, we have by (h) $R_1 \leq R_2$; and

$$R_1 \leq \min\{I(X;Y_1), I(X;Y_2)\}.$$

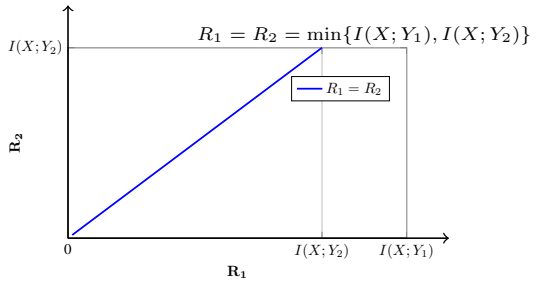

Fig. 2: Individual-secrecy capacity region in case of a strong eavesdropper.

By symmetry, we have $R_2 \leq R_1$ and $R_2 \leq \min\{I(X;Y_1), I(X;Y_2)\}$. Thus, we establish that $R_1 = R_2 \leq \min\{I(X;Y_1), I(X;Y_2)\}$, i.e., the converse. ■

B. Secrecy coding approach

Consider channel inputs $p(x)$ such that $I(X;Z) \leq \min\{I(X;Y_1), I(X;Y_2)\}$. Assume wlog that $I(X;Y_2) \leq I(X;Y_1)$. For such cases, we can split M_1 into two parts: one of entropy $n(I(X;Y_1) - I(X;Y_2))$ which is secured by using secrecy coding for classical wiretap channels; and the other of entropy $nI(X;Y_2)$ which is secured by capsuling with M_2 as a one-time pad (thus M_2 is also secured as in Section IV-A). In general, we have the following.

Proposition 4. *Any $(R_1, R_2) \in \mathbb{R}^+$ satisfying*

$$I(X;Z) \leq R_t \leq I(X;Y_t), \quad \textit{for} \quad t \in \{1, 2\}, \qquad (13)$$

for $p(x)$ such that $I(X;Z) \leq \min\{I(X;Y_1), I(X;Y_2)\}$ is achievable.

Proof: Assume that $R_2 \leq R_1$. We split M_1 into two parts, i.e., $M_1 = (M_{1k}, M_{1s})$ with M_{1k} of entropy nR_2, the same as M_2; whilst M_{1s} of entropy $n(R_1 - R_2)$.

Randomly generate 2^{nR_1} codewords x^n according to $p(x)$. Throw them into $2^{n(R_1 - R_2)}$ bins [3] and index $x^n(i_k, i_{1s})$ with $(i_k, i_{1s}) \in [1 : 2^{nR_2}] \times [1 : 2^{n(R_1 - R_2)}]$.

To send messages (m_1, m_2), choose $x^n(m_k, m_{1s})$ with $m_k = m_{1k} \oplus m_2$ and transmit it to the channel. Receiver 2 can decode m_k reliably using typical set decoding if $R_2 < I(X;Y_2)$ with the knowledge of m_1, and thus extract m_2. Receiver 1 can decode both m_k and m_{1s} if $R_1 < I(X;Y_1)$, and extract m_{1k} from the former with the knowledge of m_2.

At the eavesdropper, the secrecy of M_2 follows by

$$I(M_2; Z^n) \leq I(M_2; Z^n, M_k, M_{1s}) = I(M_2; M_k, M_{1s}) = 0.$$

Further, the secrecy of M_1 is shown as follows. Since $R_2 \geq I(X;Z)$, for a fixed i_{1s}, one can further bin the codewords x^n and index them as $x^n(i_{kx}, i_{ks}, i_{1s})$ with $i_k = (i_{kx}, i_{ks}) \in [1 : 2^{n(I(X;Z) - \epsilon)}] \times [1 : 2^{n(R_2 - I(X;Z) + \epsilon)}]$. Correspondingly, split $M_k = (M_{kx}, M_{ks})$. We have

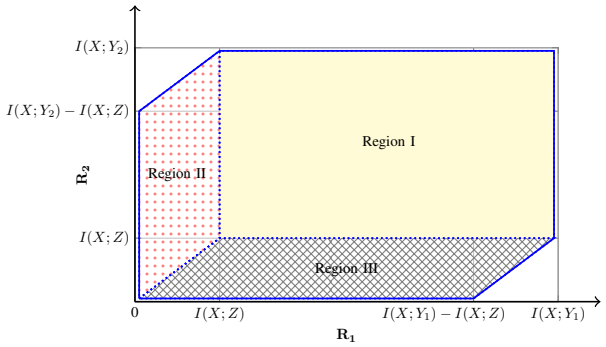

Fig. 3: Individual-secrecy capacity region in case of a weak eavesdropper.

$$
\begin{aligned}
&H(M_{1s}, M_{ks}|Z^n)\\
&\quad = H(M_{1s}, M_{ks}, X^n|Z^n) - H(X^n|M_{1s}, M_{ks}, Z^n)\\
&\quad \overset{(a)}{\geq} H(M_{1s}, M_{ks}, X^n, Z^n) - H(Z^n) - n\epsilon_1\\
&\quad = H(X^n) + H(Z^n|X^n) - H(Z^n) - n\epsilon_1\\
&\quad \overset{(b)}{\geq} nR_1 + nH(Z|X) - nH(Z) - n\epsilon_1\\
&\quad \overset{(c)}{\geq} H(M_{1s}, M_{ks}) - n\delta(\epsilon),
\end{aligned}
$$

where (a) follows as $H(X^n|M_{1s}, M_{ks}, Z^n) \leq n\epsilon_1$ due to Fano's inequality and that the eavesdropper can decode X^n reliably, given (M_{ks}, M_{1s}, Z^n); (b) is due to the fact that $H(X^n) = nR_1$; $H(Z^n|X^n) = nH(Z|X)$ since the channel is memoryless; and $H(Z^n) = \sum_{i=1}^n H(Z_i|Z_1^{i-1}) \leq \sum_{i=1}^n H(Z_i) = nH(Z)$; (c) follows that $H(M_{1s}, M_{ks}) = n(R_1 - R_2) + n(R_2 - I(X;Z) + \epsilon)$ and $\delta(\epsilon) = \epsilon_1 + \epsilon$.

Above inequality implies $I(M_{1s}; Z^n) \leq n\delta(\epsilon)$. In addition, we can bound $I(M_{1k}; Z^n|M_{1s}) \leq I(M_{1k}; Z^n, M_{1s}, M_k) = I(M_{1k}; M_k, M_{1s}) = 0$ due to Markov chain $M_{1k} \to (M_k, M_{1s}) \to Z^n$. Therefore, we obtain

$$I(M_1; Z^n) = I(M_{1s}; Z^n) + I(M_{1k}; Z^n|M_{1s}) \leq n\delta(\epsilon).$$

This concludes the proof of the individual secrecy. ■

Proposition 5. *If the channel to the eavesdropper is degraded with respect to the channels to both legitimate receivers, then the individual-secrecy capacity region is given by the union of* $(R_1, R_2) \in \mathbb{R}^+$ *pairs satisfying*

$$
\begin{aligned}
R_1 &\leq \min\{I(X;Y_1) - I(X;Z) + R_2, I(X;Y_1)\};\\
R_2 &\leq \min\{I(X;Y_2) - I(X;Z) + R_1, I(X;Y_2)\},
\end{aligned}
$$

where the union is taken over $p(x)$.

Proof: Under the *degradedness* condition, we have that $I(X;Z) \leq \min\{I(X;Y_1), I(X;Y_2)\}$ holds for any $p(x)$. Utilizing the scheme in Proposition 4, the region I in Fig.3 is achievable. To show region II is achievable, one can employ Wyner's secrecy coding to achieve rate pairs (R_1, R_2) such that $R_1 = 0$ and $R_2 \leq I(X;Y_2) - I(X;Z)$. Then, applying time sharing with the west boundary rate pairs of region I, one obtains the achievablity of other rate pairs in region II. A similar proof applies to the achievability of region III.

The converse follows from the fact that the achievable region is equal to the intersection of upper bounds given in [1, Theorem 1], which is the capacity region of the BC-RSI without an eavesdropper, and the upper bound given in Proposition 7, which is a partial upper bound by applying the results for wiretap channel with shared key for one receiver while ignoring the requirement of reliable and secure communication for the other. ■

As shown in Fig. 3, the individual-secrecy capacity region for a weak eavesdropper is a rectangle with missing corners. In particular, for this scenario, one may not claim that if (R_1, R_2) is achievable, then $(R_1 - c_1, R_2 - c_2)$ is achievable for any $c_1 \leq R_1, c_2 \leq R_2$. This follows as the individual-secrecy rates are *coupled* in the BC-RSI setting.

C. Superposition coding

Consider a degraded broadcast channel where $X \to Y_1 \to Y_2$ forms a Markov chain. Then, one can utilize superposition coding to transmit a cloud center to the weak receiver and both the cloud center and satellite codewords to the strong receiver [3]. By utilizing the one-time pad message as the cloud center, one can readily achieve the following region.

Proposition 6. *The individual-secrecy rate region for BC-RSI is achievable for the set of the rate pairs* (R_1, R_2) *such that*

$$
\begin{aligned}
R_2 &\leq I(U;Y_2), &(14)\\
R_1 &\leq I(V;Y_1|U) - I(V;Z|U) + R_2, &(15)
\end{aligned}
$$

over all $p(u)p(v|u)p(x|v)$.

Proof: Assume that $R_2 \leq R_1$ (since V can be always chosen such that $I(V;Y_1|U) - I(V;Z|U)$ is non-negative). Represent M_1 by (M_{1k}, M_{1s}), with M_{1k} of entropy nR_2, the same as that of M_2 and M_{1s} of entropy $n(R_1 - R_2)$.

Codebook generation: Fix $p(u), p(v|u)$. First, randomly generate 2^{nR_2} i.i.d sequences $u^n(k)$, $k \in [1 : 2^{nR_2}]$, according to $p(u)$. Secondly, for each $u^n(k)$, according to $p(v|u)$, randomly generate i.i.d sequences $v^n(k, s, r)$ with $(s, r) \in [1 : 2^{n(R_1 - R_2)}] \times [1 : 2^{n(I(V;Z|U) - \epsilon)}]$.

Encoding: To send messages (m_1, m_2), choose $u^n(k)$, where $k = m_k \triangleq m_{1k} \oplus m_2$. Given $u^n(k)$, randomly choose $r \in [1 : 2^{n(I(V;Z|U) - \epsilon)}]$ and find $v^n(k, m_{1s}, r)$. Generate x^n according to $p(x|v)$, and transmit it to 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. (It is necessary that $R_2 < I(U;Y_2)$.) With the knowledge of m_1, decode $\hat{m}_2 = m_{1k} \oplus \hat{k}$.

Receiver 1, upon receiving y_1^n, finds $u^n(\hat{k})$ such that $(u^n(\hat{k}), y_1^n)$ is jointly typical. (This is possible since $R_2 < I(U;Y_2) \leq I(U;Y_1)$.) Corresponding to $u^n(\hat{k})$, further find $v^n(\hat{k}, \hat{m}_{1s}, \hat{r})$ which is jointly typical with y_1^n. With the knowledge of m_2, decode $\hat{m}_1 = (m_2 \oplus \hat{k}, \hat{m}_{1s})$.

Analysis of the probability error: 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 both of the following events occur:

$$\mathcal{E}_{21} = \{(u^n(m_2 \oplus m_{1k}), y_2^n) \notin \mathcal{T}_\epsilon^{(n)}\},$$
$$\mathcal{E}_{22} = \{(u^n(m_2' \oplus m_{1k}), y_2^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } m_2' \neq m_2\}.$$

Thus $P_{e,2}$ can be upper bounded as

$$P_{e,2} \leq \Pr(\mathcal{E}_{21}) + \Pr(\mathcal{E}_{22}).$$

By the LLN, $\Pr(\mathcal{E}_{21})$ tends to zero as $n \to \infty$. For $\Pr(\mathcal{E}_{22})$, since $u^n(m_2' \oplus m_{1k})$ is independent of $(u^n(m_2 \oplus m_{1k}), y_2^n)$ for $m_2' \neq m_2$, by the packing lemma, $\Pr(\mathcal{E}_{22})$ tends to zero as $n \to \infty$ if $R_2 < I(U; Y_2) - \delta(\epsilon)$.

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

$$\mathcal{E}_{11} = \{(u^n(m_2 \oplus m_{1k}, y_1^n) \notin \mathcal{T}_\epsilon^{(n)}\},$$
$$\mathcal{E}_{12} = \{(v^n(k, m_{1s}, r), y_1^n) \notin \mathcal{T}_\epsilon^{(n)}\},$$
$$\mathcal{E}_{13} = \{(v^n(k, m_{1s}', r'), y_1^n) \in \mathcal{T}_\epsilon^{(n)}, (m_{1s}', r') \neq (m_{1s}, r)\}.$$

So $P_{e,1}$ can be upper bounded by

$$P_{e,1} \leq \Pr(\mathcal{E}_{11}) + \Pr(\mathcal{E}_{12}|\mathcal{E}_{11}^c) + \Pr(\mathcal{E}_{13}|\mathcal{E}_{11}^c).$$

By the LLN, $\Pr(\mathcal{E}_{11})$ and $\Pr(\mathcal{E}_{12}|\mathcal{E}_{11}^c)$ tends to zero as $n \to \infty$. For $\Pr(\mathcal{E}_{13}|\mathcal{E}_{11}^c)$, note that if $(m_{1s}', r') \neq (m_{1s}, r)$, then given $u^n(k)$, $v^n(k, m_{1s}', r')$ is independent of $(v^n(k, m_{1s}, r), y_1^n)$. By the packing lemma, it tends to zero as $n \to \infty$ if $R_1 < I(V; Y_1|U) - I(V; Z|U) + R_2 - \delta(\epsilon)$.

Analysis of individual secrecy: For the secrecy of M_2, due to the Markov chain $M_2 \to (M_k, M_{1s}) \to Z^n$, we have $I(M_2; Z^n) \leq I(M_2; Z^n, M_k, M_{1s}) = I(M_2; M_k, M_{1s}) = 0$, where the last equality is due to the fact that $M_k = M_2 \oplus M_{1k}$, is independent of M_2 as its one-time pad encryption.

For the secrecy of M_1, we have

$$\begin{aligned}
I(M_1; Z^n) =& I(M_{1k}, M_{1s}; Z^n) \\
=& I(M_{1k}; Z^n) + I(M_{1s}; Z^n|M_{1k}) \\
\overset{(a)}{=}& I(M_{1s}; Z^n|M_{1k}) \\
\leq& I(M_{1s}; Z^n, M_{1k}, M_k) \\
=& I(M_{1s}; Z^n, M_k) + I(M_{1s}; M_{1k}|Z^n, M_k) \\
\overset{(b)}{=}& I(M_{1s}; Z^n, M_k) \\
=& H(M_{1s}) - H(M_{1s}|M_k, Z^n) \\
=& n(R_1 - R_2) - H(M_{1s}|M_k, Z^n),
\end{aligned}$$

where (a) is due to the fact that $I(M_{1k}; Z^n) = 0$ by following a similar proof of $I(M_2; Z^n) = 0$; (b) follows that $I(M_{1s}; M_{1k}|Z^n, M_k) \geq 0$ and that $H(M_{1k}|Z^n, M_k, M_{1s}) = H(M_{1k}|M_k, M_{1s}) = H(M_{1k}) \geq H(M_{1k}|Z^n, M_k)$.

To complete the proof that $I(M_1; Z^n) \leq n\delta(\epsilon)$, we show in the following that $H(M_{1s}|M_k, Z^n) \geq n(R_1 - R_2) - n\delta(\epsilon)$.

$$\begin{aligned}
H(M_{1s}|M_k, Z^n) \overset{(c)}{=}& H(M_{1s}|U^n, Z^n) \\
=& H(M_{1s}, Z^n|U^n) - H(Z^n|U^n) \\
=& H(M_{1s}, Z^n, V^n|U^n) \\
& - H(V^n|U^n, M_{1s}, Z^n) - H(Z^n|U^n) \\
=& H(V^n|U^n) + H(Z^n|U^n, V^n) \\
& - H(V^n|U^n, M_{1s}, Z^n) - H(Z^n|U^n) \\
\overset{(d)}{\geq}& n(R_1 - R_2) - n\delta(\epsilon),
\end{aligned}$$

where (c) is due to the fact that U^n is uniquely determined by M_k; (d) follows as $H(V^n|U^n) = n(R_1 - R_2) + n(I(V; Z|U) - \epsilon)$ by codebook construction; $H(Z^n|U^n, V^n) = \sum_{i=1}^n H(Z_i|U_i, V_i) = nH(Z|U, V)$ since the channel is discrete memoryless; $H(V^n|U^n, M_{1s}, Z^n) \leq n\epsilon$ due to Fano's inequality and that the eavesdropper can decode V^n reliably, given (U^n, M_{1s}, Z^n); and $H(Z^n|U^n) = \sum_{i=1}^n H(Z_i|Z^{i-1}, U^n) \leq \sum_{i=1}^n H(Z_i|U_i) = nH(Z|U)$. ■

D. Upper bounds

An upper bound on the individual-secrecy capacity region is the capacity region of the BC-RSI without an eavesdropper as given in [1, Theorem 1]. Another upper bound follows directly the work of wiretap channel with shared key [5], as provided below.

Proposition 7. *For any R_2 in the achievable region, R_1 is upper bounded by*

$$\max_{U \to V \to X \to (Y_1, Z)} \min\{I(V; Y_1|U) - I(V; Z|U) + R_2, I(V; Y_1)\}.$$

If the channel is degraded such that $X \to Y_1 \to Z$, then for any R_2 in the achievable region, R_1 is upper bounded by

$$\max_{X \to Y_1 \to Z} \min\{I(X; Y_1) - I(X; Z) + R_2, I(X; Y_1)\}.$$

Similar results hold for interchanging 1 *and* 2 *above.*

V. Conclusion

In this paper, we studied the problem of secure communication over BC-RSI under the individual secrecy constraints. Compared to the joint secrecy constraint, this relaxed setting allows for higher secure communication rates at the expense of having a weaker notion of security. We characterized the individual-secrecy capacity region: 1) in case of a *strong* eavesdropper, to be a line on (R_1, R_2) plane; and 2) in case of a *weak* eavesdropper, to be a rectangle with missing corners. This result is due to the very nature of the problem where the communication rates are coupled. Therefore, one can not arbitrarily decrease one user's rate without sacrificing the rate of the other. We presented several achievable strategies by employing superposition coding, Wyner's secrecy coding and one-time pad, however, the characterization of the capacity region for the general case still remains as an open problem.

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 2007)*, pp. 313–318, Sep. 2007.

[2] R. F. Wyrembelski, A. Sezgin and H. Boche, "Secrecy in broadcast channels with receiver side information," in *Proc. 45th Asilomar Conference on Signals, Systems and Computers (ASILOMAR)*, pp. 290–294, Nov. 2011.

[3] A. El Gamal and Y.-H. Kim, *Network Information Theory*, Cambridge University Press, 2011.

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

[5] W. Kang and N. Liu, "Wiretap channel with shared key," in *Proc. 2010 IEEE Information Theory Workshop (ITW 2010)*, pp. 1–5, Sep. 2010.