Broadcast Channel with Receiver Side Information: Achieving Individual Secrecy

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

***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 preliminary result, we obtain a general achievable region together with a characterization of the capacity region for the case of a degraded eavesdropper.**

I. Introduction

The broadcast channel is a fundamental communication model that involves transmission of independent messages to different users. In this paper, we consider the secure transmission of independent messages to two receivers which have, respectively, the desired message of the other receiver as side information. The model is shown in Fig. 1. The problem (without an eavesdropper) was originally motivated by the concept of the bidirectional relay channel, where two nodes exchange messages via a relay node. If the relay node decodes both messages, then it can broadcast a common codeword to both nodes each having their own message as side information. In [1], the broadcasting capacity region (without an eavesdropper) has been completely characterized.

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 review the problem under *individual* secrecy constraints that aim 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. 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.

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.)

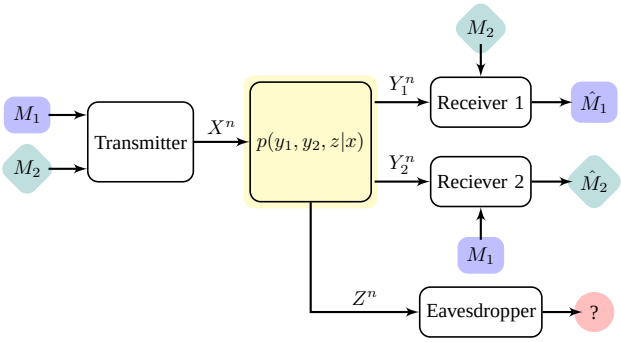

Fig. 1: Wiretap channel with receiver side information.

Denote the average probability of decoding error at receiver i to be $P_{e,i}$. 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. Equation (3) corresponds to *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.

We recall the capacity region of the discrete memoryless broadcast channel with receiver side information, when none of the secrecy constraints are taken into account.

Theorem 1. *([1, Theorem 1]) The capacity region of the discrete memoryless broadcast channel $p(y_1, y_2|x)$ with receiver side information is the set of the rate pairs (R_1, R_2) such that*

$$R_1 \leq I(X; Y_1) \quad \textit{and} \quad R_2 \leq I(X; Y_2) \tag{5}$$

over all possible pmf $p(x)$.

III. 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*

$$R_1 = R_2 \quad \leq \quad \min\{I(X;Y_1), I(X;Y_2)\} \tag{6}$$

for any $p(x)$ is achievable.

Proof: Randomly generate 2^{nR} codewords x^n according to $\prod_{i=1}^n p(x_i)$. 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 constraint, we have for $i = 1, 2$,

$$I(M_i; Z^n) \leq I(M_i; Z^n, M_k) = I(M_i; M_k) = 0, \tag{7}$$

where the 1st equality is due to Markov chain $M_i \to M_k \to Z^n$; and the 2nd is since M_k is a one-time pad of M_i. ■

Note that the above achievable region is limited by the worse channel. In the following, we consider other coding schemes to enlarge the achievable region beyond the one stated above.

B. Secrecy coding approach

Consider those channel inputs $p(x)$ such that $I(X;Z) \leq \min\{I(X;Y_1), I(X;Y_2)\}$. Assume that $I(X;Y_2) \leq I(X;Y_1)$. For such cases, we 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 in a one-time pad (thus M_2 is also secured). We obtain the following.

Proposition 3. *Any $(R_1, R_2) \in \mathbb{R}^+$ satisfying*

$$I(X;Z) \leq R_1 \leq I(X;Y_1);\ I(X;Z) \leq R_2 \leq I(X;Y_2) \tag{8}$$

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 $\prod_{i=1}^n p(x_i)$. Throw them into $2^{n(R_1-R_2)}$ bins [3] and index $x^n(i_k, i_{1s})$ with $(i_k, i_{1s}) \in [1 : 2^{nR_2}] \times [1 : 2^{n(R_1-R_2)}]$.

Given (m_1, m_2), send $x^n(m_k, m_{1s})$ with $m_k = m_{1k} \oplus m_2$ to the channel. Receiver 2 can decode m_k reliably using typical set decoding if $R_2 < I(X;Y_2)$ with the help 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 given m_2.

At the eavesdropper, for the secrecy of M_2, we have

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

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

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

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) is due to the fact that $H(M_{1s}, M_{ks}) = n(R_1 - R_2) + n(R_2 - I(X;Z) + \epsilon)$.

Above inequality implies $I(M_{1s}; Z^n) \leq n\delta(\epsilon)$. In addition, we 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 individual secrecy proof. ■

Proposition 4. *If the channel to the eavesdropper is degraded with respect to the channels of both legitimate receivers, then the individual-secrecy capacity region is given by the union of $(R_1, R_2) \in \mathbb{R}^+$ pairs satisfying*

$$\begin{aligned}
R_1 &\leq \min\{I(X;Y_1) - I(X;Z) + R_2, I(X;Y_1)\}; \\
R_2 &\leq \min\{I(X;Y_2) - I(X;Z) + R_1, I(X;Y_2)\},
\end{aligned} \tag{9}$$

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

Proof: With the *degraded* condition, we have $I(X;Z) \leq \min\{I(X;Y_1), I(X;Y_2)\}$ for any $p(x)$. Denote $\mathcal{R}_1$ to be the region achievable by Proposition 3, as defined in (8) . Further, denote $\mathcal{R}_2 = \{(R_1, R_2) : R_1 = 0, R_2 \leq I(X;Y_2) - I(X;Z)\}$ and $\mathcal{R}_3 = \{(R_1, R_2) : R_1 \leq I(X;Y_1) - I(X;Z), R_2 = 0\}$, which are achievable by employing Wyner's secrecy coding. The achievability of the region in (9) follows from the convex hull of $\mathcal{R}_1 \cup \mathcal{R}_2 \cup \mathcal{R}_3$. The converse follows directly from Theorem 1 together with Proposition 7 provided below. ■

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

$$R_t = I(U;Y_t);\ R_{\bar{t}} \leq I(V;Y_{\bar{t}}|U) - I(V;Z|U) + R_t, \tag{10}$$

over all $p(u)p(v|u)p(x|v)$*, where* $t = \arg\min_{i\in\{1,2\}} \{I(U;Y_i)\}$ *and* $\bar{t} = \{1,2\}\backslash\{t\}$.

Proof: Assume that $R_2 \le R_1$. (This corresponds to the case $t = 2$ in which $I(U;Y_2) \le I(U;Y_1)$, since V can be always chosen such that $I(V;Y_{\bar{t}}|U) - I(V;Z|U)$ 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 $\prod_{i=1}^n p(u_i)$. Secondly, for each $u^n(k)$, according to $\prod_{i=1}^n p(v_i|u_i)$, 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 $\prod_{i=1}^n p(x_i|v_i)$, and transmit it to the channel.

Decoding: Receiver 2, upon receiving y_2^n, finds $u^n(\hat{k})$ such that $(u^n(\hat{k}), y_1^n)$ 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 $R_2 < I(U;Y_2) \le I(U;Y_1)$.) 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: Similar to the analysis of the superposition coding for general discrete memoryless broadcast channels, we have $P_{e,1}, P_{e,2} \to 0$ as $n \to \infty$ if $R_2 < I(U;Y_2) - \epsilon$ and $R_1 < I(V;Y_1|U) - I(V;Z|U) + R_2 - \epsilon$.

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

$$\begin{aligned}
I(M_1;Z^n) &= I(M_{1k}, M_{1s}; Z^n) && (11)\\
&= I(M_{1k};Z^n) + I(M_{1s};Z^n|M_{1k}) && (12)\\
&\overset{(a)}{=} I(M_{1s};Z^n|M_{1k}) && (13)\\
&\le I(M_{1s}; Z^n, M_{1k}, M_k) && (14)\\
&= I(M_{1s}; Z^n, M_k) + I(M_{1s}; M_{1k}|Z^n, M_k) && (15)\\
&\overset{(b)}{=} I(M_{1s}; Z^n, M_k) && (16)\\
&= H(M_{1s}) - H(M_{1s}|M_k, Z^n) && (17)\\
&= n(R_1 - R_2) - H(M_{1s}|M_k, Z^n), && (18)
\end{aligned}$$

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 $I(M_{1s}; M_{1k}|Z^n, M_k) \ge 0$ and that $H(M_{1k}|Z^n, M_k, M_{1s}) = H(M_{1k}|M_k, M_{1s}) = H(M_{1k}) \ge H(M_{1k}|Z^n, M_k)$.

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

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

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; $H(V^n|U^n, M_{1s}, Z^n) \le n\epsilon$ due to Fano's inequality and that the eavesdropper can decode V^n reliably, given (U^n, M_{1s}, Z^n); and $H(Z^n|U^n) = \sum_{i=1}^n H(Z_i|Z^{i-1}, U^n) \le \sum_{i=1}^n H(Z_i|U_i) = nH(Z|U)$. ■

D. Marton's coding

A universal approach is to apply Marton's coding for the general broadcast channels, utilizing the one-time pad message as common message to transmit secure messages to both users.

Proposition 6. *The rate region is given by* $(R_1 = R_k + R_{1s}, R_2 = R_k + R_{2s})$ *pairs such that* (R_k, R_{1s}, R_{2s}) *belongs to the region given by the union of rate tuples*

$$\begin{aligned}
R_k &\le \min\{I(U;Y_1), I(U;Y_2)\}\\
R_{1s} &\le \min\{I(V_1,V_2;Y_1|U) - R_0, I(V_1;Y_1,V_2|U)\}\\
R_{2s} &\le \min\{I(V_1,V_2;Y_2|U) - R_0, I(V_2;Y_2,V_1|U)\}\\
R_{1s} + R_{2s} &\le I(V_1;Y_1,V_2|U) + I(V_2;Y_2,V_1|U) - R_0
\end{aligned}$$

over any pmf $p(u)p(v_1,v_2|u)p(x|v_1,v_2)$*, where* $R_0 = I(V_1;V_2|U) + I(V_1,V_2;Z|U)$.

Proof: Represent M_1, M_2 by $M_1 = (M_{1k}, M_{1s})$ and $M_2 = (M_{2k}, M_{2s})$ with M_{1k}, M_{2k} of entropy nR_k; whilst M_{1s} of entropy nR_{1s} and M_{2s} of entropy nR_{2s}.

Codebook generation: Fix $p(u), p(v_1|u), p(v_2|u)$ and $p(x|v_1,v_2)$. First, randomly generate 2^{nR_k} i.i.d sequences $u^n(k)$, $k \in [1 : 2^{nR_k}]$, according to $\prod_{i=1}^n p(u_i)$.

For each $u^n(k)$, randomly generate $2^{n(R_{1s}+R_{1c}+R_{1r})}$ i.i.d sequences $v_1^n(k, s_1, c_1, r_1)$ with $(s_1, c_1, r_1) \in [1 : 2^{nR_{1s}}] \times [1 : 2^{nR_{1c}}] \times [1 : 2^{nR_{1r}}]$, according to $\prod_{i=1}^n p(v_{1i}|u_i)$; and similarly generate $2^{n(R_{2s}+R_{2c}+R_{2r})}$ i.i.d sequences $v_2^n(k, s_2, c_2, r_2)$, $(s_2, c_2, r_2) \in [1 : 2^{nR_{2s}}] \times [1 : 2^{nR_{2c}}] \times [1 : 2^{nR_{2r}}]$, according to $\prod_{i=1}^n p(v_{2i}|u_i)$. For a fixed (k, s_1, s_2), we denote the product $V_1 \times V_2$ codebook to be $\mathcal{C}_{V_1,V_2|U}(k, s_1, s_2)$.

Encoding: To send messages (m_1, m_2), choose $u^n(k)$, where $k = m_k \triangleq m_{1k} \oplus m_{2k}$. Given $u^n(k)$, find in the product codebook $\mathcal{C}_{V_1,V_2|U}(k, m_{1s}, m_{2s})$ a jointly typical $(v_1^n(k, m_{1s}, c_1, r_1), v_2^n(k, m_{2s}, c_2, r_2))$ pair. (This is possible if $R_{1c} + R_{2c} > I(V_1;V_2|U)$). Generate and transmit $x^n(v_1^n, v_2^n)$ according to $\prod_{i=1}^n p(x_i|v_{1i}, v_{2i})$.

Decoding: Receiver 1, upon receiving y_1^n, finds $u^n(\hat{k})$ such that $(u^n(\hat{k}), y_1^n)$ is jointly typical. (It is necessary that $R_k < I(U;Y_1)$). With the knowledge of m_2 and $u^n(\hat{k})$, further find $(v_1^n(\hat{k}, \hat{m}_{1s}, \hat{c}_1, \hat{r}_1), v_2^n(\hat{k}, m_{2s}, \hat{c}_2, \hat{r}_2))$, which is jointly typical with y_1^n. Decode $\hat{m}_1 = (m_{2k} \oplus \hat{k}, \hat{m}_{1s})$.

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 $R_k < I(U;Y_2)$). With the knowledge of m_1 and $u^n(\hat{k})$, further find $(v_1^n(\hat{k}, m_{1s}, \hat{c}_1, \hat{r}_1)), v_2^n(\hat{k}, \hat{m}_{2s}, \hat{c}_2, \hat{r}_2))$, which is jointly typical with y_2^n. Decode $\hat{m}_2 = (m_{1k} \oplus \hat{k}, \hat{m}_{2s})$.

Analysis of decoding error: For $P_{e,1}$ (similar for $P_{e,2}$), a decoding error happens iff ≥ 1 of the following events occur:

$$\begin{aligned}
\mathcal{E}_{11} =& \{(u^n(k), y_1^n) \notin \mathcal{T}_\epsilon^{(n)}\},\\
\mathcal{E}_{12} =& \{(v_1^n(k, m_{1s}, c_1, r_1), v_2^n(k, m_{2s}, c_2, r_2)) \notin \mathcal{T}_\epsilon^{(n)}\},\\
\mathcal{E}_{13} =& \{(v_1^n(k, m_{1s}, c_1, r_1), v_2^n(k, m_{2s}, c_2, r_2), y_1^n) \notin \mathcal{T}_\epsilon^{(n)})\},\\
\mathcal{E}_{14} =& \{(v_1^n(k, m'_{1s}, c'_1, r'_1), v_2^n(k, m_{2s}, c'_2, r'_2), y_1^n) \in \mathcal{T}_\epsilon^{(n)},\\
& m'_{1s} \neq m_{1s}\}.
\end{aligned}$$

The probability of error $P_{e,1}$ is upper bounded as $P_{e,1} \leq \Pr(\mathcal{E}_{11}) + \Pr(\mathcal{E}_{12}|\mathcal{E}_{11}^c) + \Pr(\mathcal{E}_{13}|\mathcal{E}_{11}^c, \mathcal{E}_{12}^c) + \Pr(\mathcal{E}_{14}|\mathcal{E}_{11}^c)$. By the LLN, $\Pr(\mathcal{E}_{11})$ and $\Pr(\mathcal{E}_{13}|\mathcal{E}_{11}^c, \mathcal{E}_{12}^c)$ tend to zero as $n \to \infty$; $\Pr(\mathcal{E}_{12}|\mathcal{E}_{11}^c)$, by the mutual covering lemma [3] , tends to zero as $n \to \infty$ since $R_{1c} + R_{2c} > I(V_1; V_2|U) + \epsilon$; The 4th term, $\Pr(\mathcal{E}_{14}|\mathcal{E}_{11}^c)$, by the packing lemma [3], tends to zero as $n \to \infty$ if $R_{1s} + R_{1c} + R_{2c} + R_{1r} + R_{2r} < I(V_1, V_2; Y_1|U) - \epsilon$, and $R_{1s} + R_{1c} + R_{1r} < I(V_1; Y_1, V_2|U) - \epsilon$.

Analysis of individual secrecy: For the secrecy of M_1 (similar for M_2), we follow the steps in (11)-(17) and obtain

$$I(M_1; Z^n) \leq nR_{1s} - H(M_{1s}|M_k, Z^n). \tag{19}$$

In the following, we show that $H(M_{1s}, M_{2s}|M_k, Z^n) \geq n(R_{1s} + R_{2s}) - n\delta'(\epsilon)$ holds if we take $R_{1r} + R_{2r} = I(V_1, V_2; Z|U) - \epsilon$. This implies that $H(M_{1s}|M_k, Z^n) \geq nR_{1s} - n\delta(\epsilon)$; and by (19) we obtain $I(M_1; Z^n) \leq n\delta(\epsilon)$.

$$\begin{aligned}
&H(M_{1s}, M_{2s}|M_k, Z^n)\\
=&H(M_{1s}, M_{2s}, Z^n|U^n) - H(Z^n|U^n)\\
\overset{(a)}{\geq}&H(M_{1s}, M_{2s}, Z^n|W_{1c}, W_{2c}, U^n) - H(Z^n|U^n)\\
=&H(M_{1s}, M_{2s}, Z^n, V_1^n, V_2^n|W_{1c}, W_{2c}, U^n) - H(Z^n|U^n)\\
&- H(V_1^n, V_2^n|W_{1c}, W_{2c}, U^n, M_{1s}, M_{2s}, Z^n)\\
\overset{(b)}{\geq}&H(M_{1s}, M_{2s}, Z^n, V_1^n, V_2^n|W_{1c}, W_{2c}, U^n)\\
&- H(Z^n|U^n) - n\epsilon\\
=&H(M_{1s}, M_{2s}, V_1^n, V_2^n|W_{1c}, W_{2c}, U^n) - H(Z^n|U^n) - n\epsilon\\
&+ H(Z^n|W_{1c}, W_{2c}, U^n, M_{1s}, M_{2s}, V_1^n, V_2^n)\\
=&n(R_{1s} + R_{2s} + R_{1r} + R_{2r}) + H(Z^n|U^n, V_1^n, V_2^n)\\
&- H(Z^n|U^n) - n\epsilon\\
\overset{(c)}{\geq}&n(R_{1s} + R_{2s}) - n\delta'(\epsilon)
\end{aligned}$$

where (a) follows by introducing random variable W_{1c}, W_{2c} for the covering indices c_1, c_2; (b) follows from the fact that the eavesdropper can decode V_1^n, V_2^n reliably given $(U^n, M_{1s}, M_{2s}, W_{1c}, W_{2c}, Z^n)$; (c) follows that $H(Z^n|U^n) \leq nH(Z|U)$ and $H(Z^n|U^n, V_1^n, V_2^n) = nH(Z|U, V_1, V_2)$ and additionally by the rate choice $R_{1r} + R_{2r} = I(V_1, V_2; Z|U) - \epsilon$.

Adding those conditions such that $P_{e,1}, P_{e,2} \to 0$ as $n \to \infty$ to the rate choice $R_{1r} + R_{2r} = I(V_1, V_2; Z|U) - \epsilon$, we have

$$\begin{aligned}
R_k \leq& \min\{I(U;Y_1), I(U;Y_2)\}\\
R_{1c} + R_{2c} \geq& I(V_1; V_2|U)\\
R_{is} + R_{1c} + R_{2c} + R_{1r} + R_{2r} \leq& I(V_1, V_2; Y_i|U) \quad \text{for } i = 1, 2\\
R_{1s} + R_{1c} + R_{1r} \leq& I(V_1; Y_1, V_2|U)\\
R_{2s} + R_{2c} + R_{2r} \leq& I(V_2; Y_2, V_1|U)
\end{aligned}$$

Eliminating $R_{1c}, R_{2c}, R_{1r}, R_{2r}$ by applying Fourier-Motzkin procedure [3], we get the desired region of (R_k, R_{1s}, R_{2s}). ■

Remark: Setting $U, Y_2, V_2 = \emptyset$, the region coincides with the secrecy capacity region of the wiretap channel [4]; If we let $U = \emptyset$, it reduces to an achievable region under the joint secrecy constraint (indicated by the above secrecy proof).

E. Upper bounds

For the individual secrecy capacity region of BC-RSI, an obvious upper bound is the capacity region of the BC-RSI without an eavesdropper as given in Theorem 1. Another upper bound follows directly the work of wiretap channel with shared key [5], as stated in the following proposition.

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.*

IV. 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 provide some special case results together with several achievable schemes; whilst the characterization 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)*, pp. 313–318, Sep. 2007.

[2] R. 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] Abbas El Gamal and Young-Han 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)*, pp. 1–5, Sep. 2010.