Individual Secrecy for the Broadcast Channel

Yanling Chen *, O. Ozan Koyluoglu †, Aydin Sezgin ‡
* Institute of Digital Signal Processing, University of Duisburg-Essen, Germany.
† Department of Electrical and Computer Engineering, The University of Arizona, USA.
‡ Institute of Digital Communication Systems, Ruhr University Bochum, Germany.
Email: yanling.chen@uni-due.de, ozan@email.arizona.edu, aydin.sezgin@rub.de.

***Abstract*—This paper studies the problem of secure communication over broadcast channels under the *individual* secrecy constraints. That is, the transmitter wants to send two independent messages to two legitimate receivers in the presence of an eavesdropper, while keeping the eavesdropper ignorant of *each* message. A general achievable rate region is established by utilizing Marton's coding together with techniques such as rate splitting, Carleial-Hellman's secrecy coding, Wyner's secrecy coding and indirect decoding. Moreover, the individual secrecy capacity regions for some special cases are characterized, and an linear deterministic instance is exhibited to provide insights into the capacity regions under different secrecy constraints.**

I. Introduction

The broadcast channel (BC) involves the simultaneous communication of information from one transmitter to multiple receivers. For the two-receiver BC with two independent messages, the capacity region is yet unknown. Nevertheless, if one receiver's channel is degraded to the other, then the capacity region is fully characterized and it is shown that superposition coding is optimal [1]–[3]. In general, the best known achievable rate region is obtained by Marton's coding in [4].

Due to the very broadcast nature of the communications, adversaries may overhear the transmissions, resulting in data leakage. Secure broadcasting refers to the situation where one transmitter communicates with several legitimate receivers in the presence of an adversary (external eavesdropper). Inspired by the pioneering works [5]–[7] that studied the point-to-point secure communication, there has been a growing body of literature that investigate the problem of secure broadcasting with two or more receivers [8]–[15]. So far, most works focus on a *joint* secrecy constraint (i.e., to the eavesdropper, the information leakage rate of *all* the private messages is made vanishing). Although the work of [13] studies the *individual* secrecy (i.e., to the eavesdropper, the information leakage rate of *each* private message is made vanishing) for the broadcast channel, however, it assumes that one legitimate receiver is less noisy than the other, and a general treatment is missing.

In this work, we take advantages of the insights gained from the previous studies. Instead of superposition coding employed by [13], we utilize the framework of Marton's coding for the general setting of BC with an external eavesdropper. Wyner's secrecy coding [6] continues to play an important role here. Besides, we find that Carleial-Hellman's secrecy coding [16] is also essential for the individual secrecy setting, which main idea is to regard one message as (partial) randomness for ensuring the secrecy of the others. As a result, we establish a general achievable individual secrecy rate region with characterization of the individual secrecy capacity region for some special cases. It is worth mentioning that a relevant research direction to our problem is the secure multiplex coding (SMC) [17], [18], which aims to attain the channel capacity while keeping each message individually secret (when sending plural messages over wiretap channels).

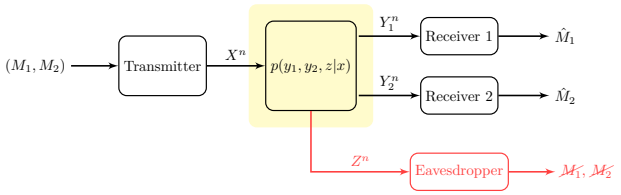


Fig. 1: DM-BC with an external eavesdropper.

The rest of the paper is organized as follows. Section II introduces the system model; Section III gives the main result, i.e., the achievable individual secrecy rate region, which proof is provided in Section IV. Section V looks into a linear deterministic model, where numerical results are presented to illustrate the impact of different secrecy constraints on the respective capacity regions. Finally, Section VI concludes the paper. To enhance the flow, some details are relegated to the appendix.

II. System model

Consider a discrete memoryless broadcast channel (DM-BC) with two legitimate receivers and one passive eavesdropper defined by $p(y_1, y_2, z|x)$. The model is shown in Fig. 1. The transmitter aims to send messages m_1, m_2 to receiver $1, 2$, respectively. Suppose that x^n is the channel input, whilst y_1^n, y_2^n and z^n, are the channel outputs at receiver 1, receiver 2 and the eavesdropper, respectively. By the *discrete memoryless* nature of the channel, we have

$$p(y_1^n, y_2^n, z^n|x^n) = \prod_{i=1}^{n} p(y_{1i}, y_{2i}, z_i|x_i).$$

A $(2^{nR_1}, 2^{nR_2}, n)$ secrecy code for the DM-BC $p(y_1, y_2, z|x)$ consists of

- Two message sets $\mathcal{M}_1$ and $\mathcal{M}_2$, where $m_1 \in \mathcal{M}_1 = [1 : 2^{nR_1}]$ and $m_2 \in \mathcal{M}_2 = [1 : 2^{nR_2}]$;
- a (randomized) encoder that assigns a codeword x^n to each message pair (m_1, m_2); and
- two decoders, where decoder i (at the legitimate receiver i) assigns an estimate of m_i, say $\hat{m}_i$, or an error to each received sequence y_i^n.

Assume that the messages M_1, M_2 are uniformly distributed over their corresponding message sets. Therefore, we have

$$R_i = \frac{1}{n} H(M_i), \quad \text{for } i = 1, 2. \tag{1}$$

Associated with an $(2^{nR_1}, 2^{nR_2}, n)$ secrecy code, the *individual* information leakage rates are defined as $R_{L,i} = \frac{1}{n} I(M_i; Z^n)$ for $i = 1, 2$, while the *joint* information leakage rate is defined as $R_L = \frac{1}{n} I(M_1, M_2; Z^n)$. Denote the *average probability of decoding error* at receiver i as $P_{e,i}^n = \Pr(M_i \neq \hat{M}_i)$. The rate pair (R_1, R_2) is said to be *achievable* under individual secrecy, if there exists a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes such that

$$P_{e,i}^n \leq \epsilon_n, \quad \text{for } i = 1, 2 \tag{2}$$

$$R_{L,i} \leq \tau_n, \quad \text{for } i = 1, 2 \tag{3}$$

$$\lim_{n\to\infty} \epsilon_n = 0 \quad \text{and} \quad \lim_{n\to\infty} \tau_n = 0. \tag{4}$$

Note that, (3) corresponds to the *individual* secrecy constraints. If the coding schemes fulfill (2), (4) and

$$R_L \leq \tau_n, \tag{5}$$

then the rate pair (R_1, R_2) is said to be achievable under *joint secrecy*. Clearly, the joint secrecy constraint (5) implies the individual secrecy (3).

III. Main Results

The main results of the paper are given as follows.

Theorem 1. *For the DM-BC with an external eavesdropper, an achievable individual secrecy rate region is given by the union of rate pairs $(R_1, R_2) \in \mathcal{R}_+^2$ with $R_1 = R_{1s} + R_{1k}$ and $R_2 = R_{2s} + R_{2k}$, where $(R_{1k}, R_{1s}, R_{2k}, R_{2s}) \in \mathcal{R}_+^4$, that satisfies*

$$\begin{aligned} R_{1s} &\leq I(V_1; Y_1|U) - I(V_1; Z|U), \\ R_{2s} &\leq I(V_2; Y_2|U) - I(V_2; Z|U), \\ R_k + R_{1s} &\leq I(U, V_1; Y_1) - I(V_1; Z|U), \\ R_k + R_{2s} &\leq I(U, V_2; Y_2) - I(V_2; Z|U), \end{aligned} \tag{6}$$

with

$$R_k = \max\left\{R_{1k} + R_{2k}, \max\{R_{1k}, R_{2k}\} + I(U; Z)\right\}, \tag{7}$$

over all $p(u)p(v_1, v_2|u)p(x|v_1, v_2)$ subject to $I(V_1; V_2|U) + I(V_1, V_2; Z|U) \leq I(V_1; Z|U) + I(V_2; Z|U)$.

Proof: See the detailed proof in Section IV. ∎

The coding approach we utilize here is built on the framework of Marton's coding with embedded Carleial-Hellman's secrecy coding and Wyner's secrecy coding. That is, we split M_i into $M_i = (M_{ik}, M_{is})$, for $i = 1, 2$. In particular, (M_{1k}, M_{2k}) are encoded into the cloud codeword U^n, where individual secrecy is guaranteed by employing Carleial-Hellman's secrecy coding; moreover, additional information M_{1s}, M_{2s} are carried by individual satellite codewords V_1^n, V_2^n, respectively, where the secrecy of M_{is} for $i = 1, 2$, is ensured by employing Wyner's secrecy coding. Finally, following the spirit of Marton's coding, (V_1^n, V_2^n) is chosen jointly, and corresponding codeword X^n is sent to the channel.

As reflected in the obtained region in (6), R_k (as defined in (7)) is contributed by Carleial-Hellman's secrecy coding in the cloud layer on (M_{1k}, M_{2k}) to obtain their individual secrecy; the first two inequalities are contributed by employing Wyner's secrecy coding in the individual satellite layer to ensure the secrecy of the extra message M_{is} to each legitimate receiver i. The last two inequalities in (6) come from the fact that receiver i, $i = 1, 2$, uses indirect decoding to decode $m_i = (m_{ik}, m_{is})$ and there is a rate loss of $I(V_i; Z|U)$ (as randomness added in Wyner's secrecy coding) for the sake of the secrecy individually.

Letting $V_2 = U$ (i.e., $R_{2s} = 0$), for the case that Y_1 is less noisy than Y_2, the region reduces to the one in [14, Theorem 1] by the superposition approach. Remarkably, Theorem 1 provides a general individual secrecy achievable region without imposing any degradedness/less noisiness order among the legitmate receiver and the eavesdropper.

Theorem 2. *For the DM-BC with an external eavesdropper such that Y_2 is a deterministic function of X, in addition, Y_1 is more capable than Y_2 and Z is a degraded version of Y_2, then the individual secrecy capacity region is given by the union of rate pairs $(R_1, R_2) \in \mathcal{R}_+^2$ satisfying*

$$\begin{aligned} R_2 &\leq H(Y_2|Z), \\ R_1 &\leq I(X; Y_1) - I(X; Z), \\ R_1 + R_2 &\leq I(X; Y_1), \end{aligned} \tag{8}$$

over all $p(x)$.

Proof: The achievability follows from Theorem 1 by taking $V_2 = U = Y_2$ (thus $R_{2s} = 0$) and $V_1 = X$, replacing R_{1k} by $R_1 - R_{1s}$, R_{2k} by R_2 and then eliminating R_{1s}. Note that in case that Y_2 is a deterministic function of X and Z is a degraded version of Y_2, we have $I(X; Z|Y_2) = 0$, $H(Y_2) = I(X; Y_2)$ and $I(Y_2; Z) = I(X; Z)$. For the converse, the first two inequalities for R_1, R_2, respectively, follow directly from the classical results of wiretap channel by simply ignoring the other legitimate receiver [7]. And, the last inequality follows directly from the upper bound on the sum rate for the relaxed setting without any secrecy constraints. ∎

IV. Achievability Proof of Theorem 1

Rate splitting: 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 rate nR_{1k}, nR_{2k}, respectively; while M_{1s}, M_{2s} of rate nR_{1s}, nR_{2s}, respectively. Therefore, we have

$$R_1 = R_{1k} + R_{1s}, \quad R_2 = R_{2k} + R_{2s}. \tag{9}$$

Codebook generation: Fix $p(u), p(v_1, v_2|u)$.

First, randomly generate $2^{n[R_{1k}+R_{2k}+R_r]}$ i.i.d. sequences $u^n(m_{2k}, m_{1k}, m_r)$, with $(m_{2k}, m_{1k}, m_r) \in [1 : 2^{nR_{2k}}] \times [1 : 2^{nR_{1k}}] \times [1 : 2^{nR_r}]$, according to $p(u)$.

For each fixed $u^n(m_{2k}, m_{1k}, m_r)$, randomly generate $2^{n[R_{1s}+R_{1r}+R_{1c}]}$ sequences $v_1^n(m_{2k}, m_{1k}, m_r, m_{1s}, m_{1r}, m_{1c})$ with $(m_{1s}, m_{1r}, m_{1c}) \in [1 : 2^{nR_{1s}}] \times [1 : 2^{nR_{1r}}] \times [1 : 2^{nR_{1c}}]$, according to $p(v_1|u)$; and similarly, randomly generate $2^{n[R_{2s}+R_{2r}+R_{2c}]}$ sequences $v_2^n(m_{2k}, m_{1k}, m_r, m_{2s}, m_{2r}, m_{2c})$ with $(m_{2s}, m_{2r}, m_{2c}) \in [1 : 2^{nR_{2s}}] \times [1 : 2^{nR_{2r}}] \times [1 : 2^{nR_{2c}}]$, according to $p(v_2|u)$.

Encoding: To send messages (m_1, m_2), with $m_1 = (m_{1k}, m_{1s})$, $m_2 = (m_{2k}, m_{2s})$, randomly choose $m_r \in [1 : 2^{nR_r}]$ and find $u^n(m_{2k}, m_{1k}, m_r)$.

Given $u^n(m_{2k}, m_{1k}, m_r)$, randomly choose $(m_{1r}, m_{2r}) \in [1 : 2^{nR_{1r}}] \times [1 : 2^{nR_{2r}}]$, and pick (m_{1c}, m_{2c}) such that $v_1^n(m_{2k}, m_{1k}, m_r, m_{1s}, m_{1r}, m_{1c})$ and $v_1^n(m_{2k}, m_{1k}, m_r, m_{2s}, m_{2r}, m_{2c})$ are jointly typical. (If there is more than one such jointly typical pair, choose one of them uniformly at random.) This is possible with high probability, if

$$R_{1c} + R_{2c} > I(V_1; V_2|U) \tag{10}$$

(refer to [19] for the proof).

Finally, for the chosen jointly typical pair (v_1^n, v_2^n), generate a codeword x^n at random according to $p(x|v_1, v_2)$ and transmit it.

Decoding: Receiver 1, upon receiving y_1^n, finds a unique tuple $(\hat{m}_{2k}, \hat{m}_{1k}, \hat{m}_r, \hat{m}_{1s}, \hat{m}_{1r})$ such that $(u^n(\hat{m}_{2k}, \hat{m}_{1k}, \hat{m}_r), v_1^n(\hat{m}_{2k}, \hat{m}_{1k}, \hat{m}_r, \hat{m}_{1s}, \hat{m}_{1r}, \hat{m}_{1c}))$ is jointly typical with y_1^n for some $\hat{m}_{1c}$. And, receiver 2, upon receiving y_2^n, finds a unique tuple $(\tilde{m}_{2k}, \tilde{m}_{1k}, \tilde{m}_r, \tilde{m}_{2s}, \tilde{m}_{2r})$ such that $(u^n(\tilde{m}_{2k}, \tilde{m}_{1k}, \tilde{m}_r), v_2^n(\tilde{m}_{2k}, \tilde{m}_{1k}, \tilde{m}_r, \tilde{m}_{2s}, \tilde{m}_{2r}, \tilde{m}_{2c}))$ is jointly typical with y_2^n for some $\tilde{m}_{2c}$.

Analysis of the error probability of decoding: Assume that $m_1 = (m_{1k}, m_{1s})$, $m_2 = (m_{2k}, m_{2s})$ is sent.

For $P_{e,1}$, a decoding error happens if receiver 1's estimate is $(u^n(\hat{m}_{2k}, \hat{m}_{1k}, \hat{m}_r), v_1^n(\hat{m}_{2k}, \hat{m}_{1k}, \hat{m}_r, \hat{m}_{1s}, \hat{m}_{1r}, \hat{m}_{1c}))$ with $(\hat{m}_{2k}, \hat{m}_{1k}, \hat{m}_r, \hat{m}_{1s}, \hat{m}_{1r}) \neq (m_{2k}, m_{1k}, m_r, m_{1s}, m_{1r})$. In more details, the error event can be partitioned into the followings:

1) Error event corresponds to $(\hat{m}_{2k}, \hat{m}_{1k}, \hat{m}_r) \neq (m_{2k}, m_{1k}, m_r)$. Note that this event occurs with arbitrarily small probability (e.g.: $\epsilon_n/2$) if

$$R_{1k} + R_{2k} + R_r + R_{1s} + R_{1r} + R_{1c} \leq I(U, V_1; Y_1) - \delta_n(\epsilon_n). \tag{11}$$

2) Error event corresponds to $(\hat{m}_{2k}, \hat{m}_{1k}, \hat{m}_r) = (m_{2k}, m_{1k}, m_r)$ but $(\hat{m}_{1s}, \hat{m}_{1r}) \neq (m_{1s}, m_{1r})$. This event occurs with arbitrarily small probability (e.g.: $\epsilon_n/2$) if

$$R_{1s} + R_{1r} + R_{1c} \leq I(V_1; Y_1|U) - \delta_n(\epsilon_n). \tag{12}$$

Similar analysis can be done at the receiver 2, from which the decoding error probability $P_{e,2}$ can be made arbitrarily small (e.g.: ϵ_n) if

$$R_{1k} + R_{2k} + R_r + R_{2s} + R_{2r} + R_{2c} \leq I(U, V_2; Y_2) - \delta_n(\epsilon_n), \tag{13}$$

$$R_{2s} + R_{2r} + R_{2c} \leq I(V_2; Y_2|U) - \delta_n(\epsilon_n). \tag{14}$$

Analysis of individual secrecy: For the individual secrecy (3), i.e., $R_{L,i} \leq \tau_n$, for $i = 1, 2$, it suffices to show that $H(M_1|Z^n) + H(M_2|Z^n) \geq H(M_1) + H(M_2) - n\tau_n = n[R_1 + R_2] - n\tau_n$.

First consider $H(M_1|Z^n)$. We have

$$\begin{aligned}
&H(M_1|Z^n) = H(M_{1k}, M_{1s}|Z^n) \\
=&H(M_{1k}, M_{2k}, M_r, U^n, M_{1s}|Z^n) \\
&- H(M_{2k}, M_r, U^n|M_{1k}, M_{1s}, Z^n) \\
\overset{(a)}{\geq}&H(U^n|Z^n) + H(M_{1s}|U^n, Z^n) - H(U^n|M_{1k}, Z^n) - n\tau_n/9 \\
\overset{(b)}{\geq}&H(U^n|Z^n) + H(M_{1s}|U^n, Z^n) - n\tau_n/9 \\
&- n[R_{2k} + R_r - I(U; Z)] - n\tau_n/9 \\
=&H(U^n|Z^n) + H(V_1^n, M_{1s}|U^n, Z^n) - H(V_1^n|M_{1s}, U^n, Z^n) \\
&- n[R_{2k} + R_r - I(U; Z)] - 2n\tau_n/9 \\
\overset{(c)}{\geq}&H(U^n|Z^n) + H(V_1^n|U^n, Z^n) - n[R_{1r} + R_{1c} - I(V_1; Z|U)] \\
&- n[R_{2k} + R_r - I(U; Z)] - n\tau_n/3 \\
=&H(U^n, V_1^n|Z^n) - n[R_{1r} + R_{1c} - I(V_1; Z|U)] \\
&- n[R_{2k} + R_r - I(U; Z)] - n\tau_n/3,
\end{aligned} \tag{15}$$

where (a) follows from the fact that conditioning reduces entropy and $H(M_{2k}, M_r|M_{1k}, M_{1s}, U^n, Z^n) \leq n\tau_n/9$ by data processing inequality (due to the Markov chain $(M_{1k}, M_{2k}, M_r) \to U^n \to Y_1^n$) and Fano's inequality (if (11) is fulfilled):

$$\begin{aligned}
H(M_{2k}, M_r|M_{1k}, M_{1s}, U^n, Z^n) \leq&H(M_{1k}, M_{2k}, M_r|U^n) \\
\leq&H(M_{1k}, M_{2k}, M_r|Y_1^n) \\
\leq&n\tau_n/9;
\end{aligned}$$

(b) and (c) follow from [11, Lemma 1] that

- $H(U^n|M_{1k}, Z^n) \leq n[R_{2k} + R_r - I(U; Z)] + n\tau_n/9$ if taking
$$R_{2k} + R_r \geq I(U; Z) + \delta_n(\tau_n); \tag{16}$$
- $H(V_1^n|M_{1s}, U^n, Z^n) \leq n[R_{1r} + R_{1c} - I(V_1; Z|U)] + n\tau_n/9$ if taking
$$R_{1r} + R_{1c} \geq I(V_1; Z|U) + \delta_n(\tau_n). \tag{17}$$

Similarly, we could show that

$$\begin{aligned}
H(M_2|Z^n) \geq&H(U^n, V_2^n|Z^n) - n[R_{2r} + R_{2c} - I(V_2; Z|U)] \\
&- n[R_{1k} + R_r - I(U; Z)] - n\tau_n/3
\end{aligned} \tag{18}$$

if taking

$$R_{1k} + R_r \geq I(U; Z) + \delta_n(\tau_n), \tag{19}$$

$$R_{2r} + R_{2c} \geq I(V_2; Z|U) + \delta_n(\tau_n). \tag{20}$$

Note that

$$\begin{aligned}
&H(U^n, V_1^n|Z^n) + H(U^n, V_2^n|Z^n)\\
=&2H(U^n|Z^n) + H(V_1^n|U^n, Z^n) + H(V_2^n|U^n, Z^n)\\
\geq&2H(U^n) - 2I(U^n; Z^n)\\
&+ H(V_1^n, V_2^n|U^n) - I(V_1^n, V_2^n; Z^n|U^n)\\
\overset{(d)}{\geq}&H(U^n) + H(U^n, V_1^n, V_2^n) - 2nI(U; Z)\\
&- nI(V_1, V_2; Z|U) - n\tau_n/6\\
\overset{(e)}{\geq}&2n[R_{2k} + R_{1k} + R_r] + n[R_{1s} + R_{1r} + R_{2s} + R_{2r}]\\
&- 2nI(U; Z) - nI(V_1, V_2; Z|U) - n\tau_n/3, \qquad (21)
\end{aligned}$$

where (d) follows from the fact that $I(U^n; Z^n) \leq nI(U; Z) + n\tau_n/18$ and $I(V_1^n, V_2^n; Z^n|U^n) \leq nI(V_1, V_2; Z|U) + n\tau_n/18$, the proofs of which follow similarly to the proof of [20, Lemma 3]; (e) follows by data processing inequality and Fano's inequality that

- $H(U^n) \geq n[R_{2k} + R_{1k} + R_r] - n\tau_n/12$ (if (11) is fulfilled):

$$\begin{aligned}
H(U^n) \geq I(U^n; Y_1^n) \geq& I(M_{1k}, M_{2k}, M_r; Y_1^n)\\
\geq& n[R_{2k} + R_{1k} + R_r] - n\tau_n/12;
\end{aligned}$$

- $H(U^n, V_1^n, V_2^n) \geq n[R_{2k}+R_{1k}+R_r+R_{1s}+R_{1r}+R_{2s}+R_{2r}] - n\tau_n/12$ (if (11), (12), (13), (14) are fulfilled):

$$\begin{aligned}
&H(U^n, V_1^n, V_2^n) \geq I(U^n, V_1^n, V_2^n; Y_1^n, Y_2^n)\\
\geq& I(M_{1k}, M_{2k}, M_r, M_{1s}, M_{1r}, M_{2s}, M_{2r}; Y_1^n, Y_2^n)\\
\geq& n[R_{1k} + R_{2k} + R_r + R_{1s} + R_{1r} + R_{2s} + R_{2r}] - n\tau_n/12.
\end{aligned}$$

Combining (15) and (18), we obtain

$$\begin{aligned}
&H(M_1|Z^n) + H(M_2|Z^n)\\
\overset{(f)}{\geq}&H(U^n, V_1^n|Z^n) - n[R_{1r} + R_{1c} - I(V_1; Z|U)]\\
&- n[R_{2k} + R_r - I(U; Z)] - n\tau_n/3\\
&+ H(U^n, V_2^n|Z^n) - n[R_{2r} + R_{2c} - I(V_2; Z|U)]\\
&- n[R_{1k} + R_r - I(U; Z)] - n\tau_n/3\\
\overset{(g)}{\geq}&n[R_1 + R_2] - n\tau_n - n[R_{1c} + R_{2c}]\\
&+ n[I(V_1; Z|U) + I(V_2; Z|U) - I(V_1, V_2; Z|U)]\\
\overset{(h)}{\geq}&n[R_1 + R_2] - n\tau_n,
\end{aligned}$$

where (f) is due to (15) and (18); (g) is according to (21) and the fact that $R_1 = R_{1k} + R_{1s}$ and $R_2 = R_{2k} + R_{2s}$ as defined in (9); and (h) is by taking

$$R_{1c}+R_{2c} \leq I(V_1; Z|U)+I(V_2; Z|U)-I(V_1, V_2; Z|U). \quad (22)$$

Achievable rate region: We summarize the rate requirements in order to guarantee a reliable communication to both legitimate receivers and to satisfy the individual secrecy constraints at the eavesdropper as follows:

- the non-negativity for rates;
- the rate relations imposed by rate splitting, i.e., (9);
- the conditions for a reliable communication to both legitimate receivers, i.e., (10), (11), (12), (13), (14);
- the conditions for individual secrecy of the messages at the eavesdropper, i.e., (16), (17), (19), (20), (22).

Eliminating $R_r, R_{1r}, R_{2r}, R_{1c}, R_{2c}$ by applying Fourier-Motzkin procedure [21], we obtain the region of $(R_1, R_2) = (R_{1k} + R_{1s}, R_{2k} + R_{2s})$ in terms of $(R_{1k}, R_{1s}, R_{2k}, R_{2s})$ as given in (6) in Theorem 1. Note that a sketch of this Fourier-Motzkin procedure is provided in [22].

V. Numerical results

Consider a linear deterministic broadcast channel that is inspired by [23], in which the received signals at the legitimate receivers and the eavesdropper are given by

$$Y_1 = D^{q-n_1}X, \qquad (23)$$

$$Y_2 = D^{q-n_2}X, \qquad (24)$$

$$Z = D^{q-n_e}X, \qquad (25)$$

where X is the binary input vector of length $q = \max\{n_1, n_2, n_e\}$; D is the $q \times q$ down-shift matrix; n_1, n_2 and n_e are the integer channel gains of the channels from the transmitter to receiver 1, receiver 2, and the eavesdropper, respectively. Without loss of generality, we assume that $n_1 \geq n_2$. Under this assumption, Y_2 is a degraded version of Y_1 according to the channel definition. In this case, we have the following theorem:

Theorem 3. *For the linear deterministic broadcast channel with an external eavesdropper, its capacity region is the set of the rate pairs $(R_1, R_2) \in \mathcal{R}_+^2$ defined by*

- *without secrecy constraint:*

$$R_2 \leq n_2, \quad R_1 + R_2 \leq n_1; \qquad (26)$$

- *under joint secrecy constraint:*

$$R_2 \leq [n_2 - n_e]^+, \quad R_1 + R_2 \leq [n_1 - n_e]^+; \qquad (27)$$

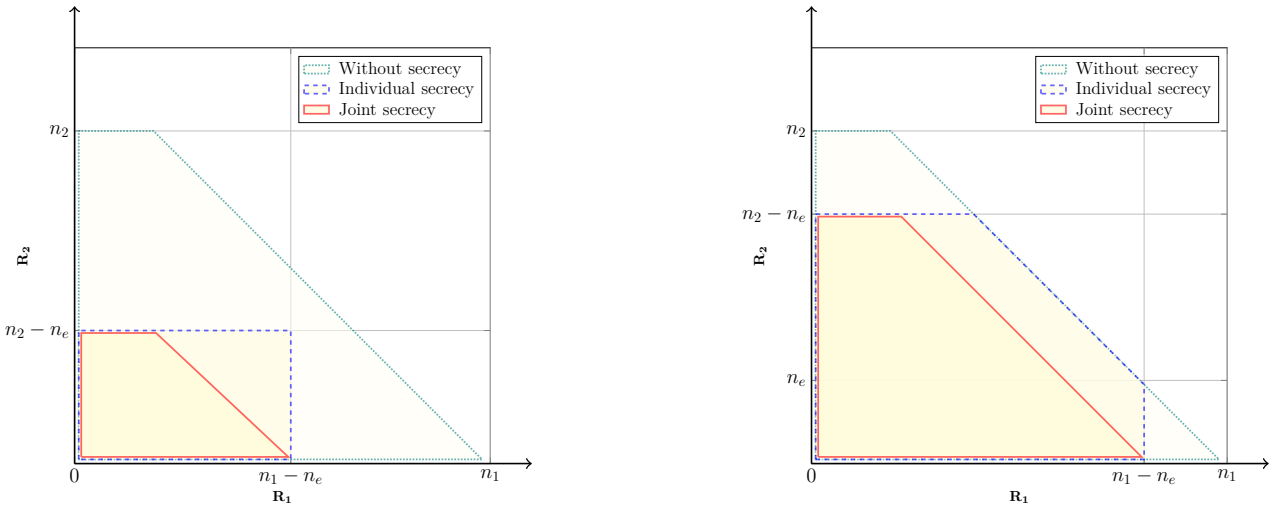
- *under individual secrecy constraint:*

$$\begin{aligned}
&R_1 \leq [n_1 - n_e]^+, \quad R_2 \leq [n_2 - n_e]^+ \quad \textit{and}\\
&R_1 + R_2 \leq n_1,
\end{aligned} \qquad (28)$$

where $[a]^+ = \max\{0, a\}$.

Proof: (26) follows from [2], [3], [21]; (27) follows from [8, Corollary 2] or [15, Theorem 4]; and (28) follows from Theorem 2. ∎

Non-degenerate individual/joint secrecy rate regions are possible only for the case as $n_1 \geq n_2 \geq n_e$. Its capacity regions under different secrecy constraints are depicted in Fig. 2. Note that the individual secrecy capacity region is a *rectangle* in case of $0 \leq n_2 - n_e \leq n_e$, as shown in Fig. 2a; but a *rectangle with one missing corner* in case of $n_2 - n_e > n_e$, as shown in Fig. 2b. Compared to the capacity region without any secrecy constraints, there is n_e bits loss for the maximal transmission rates R_1, R_2, respectively, due to the individual secrecy constraint. However, for the case under the joint secrecy constraint, compared to the capacity region with no secrecy constraint, there is not only a loss of n_e bits for the maximal transmission rates



(a) $0 < n_2 - n_e \leq n_e$ (b) $n_2 - n_e > n_e$

Fig. 2: Capacity regions of deterministic BC.

R_1, R_2, respectively, but also n_e bits loss for the sum rate $R_1 + R_2$. This additional loss on the sum rate $R_1 + R_2$ illustrates the fundamental difference between the *joint* secrecy (3) and the *individual* secrecy (5) constraints.

VI. Conclusion

In this paper, we studied the problem of secure communication over the broadcast channel under the individual secrecy constraint. As a general result, we derived an achievable rate region and characterized the individual secrecy capacity region for some special case. Unlike previous studies, our treatment is general by not requiring any less noisiness/degradedness order among receivers, and with a focus on the key scenario for secure broadcasting in the sense that two confidential messages are dedicated to two legitimate receivers, respectively.

References

[1] T. Cover, "Broadcast channels," *IEEE Trans. Inf. Theory*, vol. 18, no. 1, pp. 2–14, Jan. 1972.

[2] P. Bergmans, "Random coding theorem for broadcast channels with degraded components," *IEEE Trans. Inf. Theory*, vol. 19, no. 2, pp. 197–207, Mar. 1973.

[3] R. G. Gallager, "Coding and capacity for degraded broadcast channels," *Problemy Peridachi Informatsi*, vol. 10, no. 3, pp. 3–14, 1974.

[4] K. Marton, "A coding theorem for the discrete memoryless broadcast channel," *IEEE Trans. Inf. Theory*, vol. 25, no. 3, pp. 306–311, May 1979.

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

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

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

[8] E. Ekrem and S. Ulukus, "Secrecy capacity of a class of broadcast channels with an eavesdropper," *EURASIP Journal on Wireless Communications and Networking*, Jan. 2009.

[9] ——, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2083–2114, Apr. 2011.

[10] ——, "Degraded compound multi-receiver wiretap channels," *IEEE Trans. Inf. Theory*, vol. 58, no. 9, pp. 5681–5698, Sep. 2012.

[11] 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.

[12] E. Ekrem and S. Ulukus, "Multi-receiver wiretap channel with public and confidential messages," *IEEE Trans. Inf. Theory*, vol. 59, no. 4, pp. 2165–2177, Apr. 2013.

[13] 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.

[14] ——, "On the individual secrecy rate region for the broadcast channel with an external eavesdropper," in *Proc. 2015 IEEE International Symposium on Information Theory (ISIT 2015)*, Jun. 2015, pp. 1347–1351.

[15] M. Benammar and P. Piantanida, "Secrecy capacity region of some classes of wiretap broadcast channels," *IEEE Transactions on Information Theory*, vol. 61, no. 10, pp. 5564–5582, Oct 2015.

[16] A. Carleial and M. Hellman, "A note on Wyner's wiretap channel (Corresp.)," *IEEE Trans. Inf. Theory*, vol. 23, no. 3, pp. 387–390, May 1977.

[17] D. Kobayashi, H. Yamamoto, and T. Ogawa, "Secure multiplex coding attaining channel capacity in wiretap channels," *IEEE Transactions on Information Theory*, vol. 59, no. 12, pp. 8131–8143, Dec 2013.

[18] M. Hayashi and R. Matsumoto, "Secure multiplex coding with dependent and non-uniform multiple messages," *IEEE Transactions on Information Theory*, vol. 62, no. 5, pp. 2355–2409, May 2016.

[19] A. El Gamal and E. Van Der Meulen, "A proof of Marton's coding theorem for the discrete memoryless broadcast channel (Corresp.)," *IEEE Trans. Inf. Theory*, vol. 27, no. 1, pp. 120–122, Jan. 1981.

[20] R. Liu, I. Maric, P. Spasojević, and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.

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

[22] Y. Chen, O. O. Koyluoglu, and A. Sezgin, "Individual secrecy for the broadcast channel," *CoRR*, Nov. 2015. [Online]. Available: http://arxiv.org/abs/1511.09070

[23] A. S. Avestimehr, S. N. Diggavi, and D. N. Tse, "Wireless network information flow: A deterministic approach," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 1872–1905, Apr. 2011.