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).

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 \( y^n_1, y^n_2 \) 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

\[
p(y^n_1, y^n_2, z^n|x^n) = \prod_{i=1}^{n} p(y_{i1}, y_{i2}, z_i|x_i).
\]
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 $M_1$ and $M_2$, where $m_1 \in M_1 = [1: 2^{nR_1}]$ and $m_2 \in M_2 = [1: 2^{nR_2}]$;
- 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 $y^n_i$.

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

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

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 $P^n_{\text{err}, i} = \Pr(M_i \neq \hat{m}_i)$. 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

$$P^n_{\text{err}, i} \leq \epsilon_n, \quad \text{for } i = 1, 2 \quad (2)$$
$$R_{L,i} \leq \tau_n, \quad \text{for } i = 1, 2 \quad (3)$$
$$\lim_{n \to \infty} \epsilon_n = 0 \quad \text{and} \quad \lim_{n \to \infty} \tau_n = 0. \quad (4)$$

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

$$R_L \leq \tau_n, \quad (5)$$

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 $(R_1, R_2) \in \mathbb{R}_1^2$ with $R_1 = R_{1s} + R_{1k}$ and $R_2 = R_{2s} + R_{2k}$, where $(R_{1s}, R_{1k}, R_{2s}, R_{2k}) \in \mathbb{R}_1^4$, that satisfies

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

with

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

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

**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 $U^n$, while 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 $m_i = (m_{is}, m_{ik})$ 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 legitimate 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 $(R_1, R_2) \in \mathbb{R}_1^2$ satisfying

$$R_2 \leq H(Y_2 | Z),$$
$$R_1 \leq I(X; Y_1) - I(X; Z), \quad (8)$$
$$R_1 + R_2 \leq I(X; Y_1),$$

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 $R_{1s} + R_{1k}$ 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

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

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

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

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

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

Given $u^n(m_{2k}, m_{1k}, m_r)$, randomly choose $(m_{1r}, m_{2r}) \in [1 : 2^{R_{2s}}] \times [1 : 2^{R_{2s}}]$, and pick $(m_{1s}, m_{2s})$ such that $v_1^n(m_{2k}, m_{1k}, m_r, m_{1s}, m_{1r}, m_{1c})$ and $v_2^n(m_{2k}, m_{1k}, m_r, m_{2s}, m_{2r}, m_{2c})$ 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

$$R_{1c} + R_{2c} > I(V_1; V_2|U)$$  \hfill (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 $(\hat{m}_{2k}, \hat{m}_{1k}, \hat{m}_r, \hat{m}_{1s}, \hat{m}_{1r}, \hat{m}_{1c})$ such that $(u^n(\hat{m}_{2k}, \hat{m}_{1k}, \hat{m}_r, \hat{m}_{1s}, \hat{m}_{1r}, \hat{m}_{1c}))$ is jointly typical with $y_1^n$ for some $\hat{m}_{1c}$. And, receiver 2, upon receiving $y_2^n$, finds a unique tuple $(\hat{m}_{2k}, \hat{m}_{1k}, \hat{m}_r, \hat{m}_{2s}, \hat{m}_{2r})$ such that $(u^n(\hat{m}_{2k}, \hat{m}_{1k}, \hat{m}_r, \hat{m}_{2s}, \hat{m}_{2r}))$ is jointly typical with $y_2^n$ for some $\hat{m}_{2s}$.

**Analysis of the error probability of decoding:** Assume that $m_1 = (m_{1k}, m_{1s}, m_r) = (m_{2k}, m_{1k}, m_r)$. Note that this event occurs with arbitrarily small probability (e.g.: $\epsilon_n/2$) if

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

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

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

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

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

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

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

$$H(M_1|Z^n) = H(M_{1k}, M_{1s}, U^n|Z^n)$$

$$= H(M_{1k}, M_{2k}, M_r, U^n|Z^n)$$

$$- H(M_{2k}, M_r, U^n|M_{1k}, M_{1s}, Z^n)$$

$$\geq H(U^n|Z^n) + H(M_{1s}, U^n, Z^n) - H(U^n|M_{1k}, Z^n) - n\tau_n/9$$

$$\geq H(U^n|Z^n) + H(M_{1s}, U^n, Z^n) - n\tau_n/9$$

$$- n[R_{2k} + R_r - I(U; Z)] - n\tau_n/9$$

$$= H(U^n|Z^n) + H(V_1^n, M_{1s}, U^n, Z^n) - H(V_1^n|M_{1s}, U^n, Z^n)$$

$$- n[R_{2k} + R_r - I(U; Z)] - 2n\tau_n/9$$

$$\geq H(U^n|Z^n) + H(V_1^n, U^n, Z^n) - n[R_{1r} + R_{1c} - I(V_1; Z|U)]$$

$$- n[R_{2k} + R_r - I(U; Z)] - n\tau_n/3$$

$$= H(U^n, V_1^n|Z^n) - n[R_{1r} + R_{1c} - I(V_1; Z|U)]$$

$$- n[R_{2k} + R_r - I(U; Z)] - n\tau_n/3.$$  \hfill (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 $(M_{1k}, M_{2k}, M_r) \rightarrow U^n \rightarrow Y^n_1$) and Fano’s inequality (if (11) is fulfilled):

$$H(M_{2k}, M_r, M_{1k}, M_{1s}, U^n, Z^n) \leq H(M_{1k}, M_{2k}, M_r|U^n)$$

$$\leq H(M_{1k}, M_{2k}, M_r|Y_1^n)$$

$$\leq n\tau_n/9;$$

(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

$$R_{2k} + R_r \geq I(U; Z) + \delta_n(\tau_n);$$  \hfill (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

$$R_{1r} + R_{1c} \geq I(V_1; Z|U) + \delta_n(\tau_n).$$  \hfill (17)

Similarly, we could show that

$$H(M_2|Z^n) \geq H(U^n, V_2^n|Z^n) - n[R_{2c} + R_{2c} - I(V_2; Z|U)]$$

$$- n[R_{1k} + R_r - I(U; Z)] - n\tau_n/3$$  \hfill (18)

if taking

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

$$R_{2c} + R_{2c} \geq I(V_2; Z|U) + \delta_n(\tau_n).$$  \hfill (20)
Note that
\[ H(U^n, V^n_1|Z^n) + H(U^n, V^n_2|Z^n) \]
\[
= 2H(U^n|Z^n) + H(V^n_1|U^n, Z^n) + H(V^n_2|U^n, Z^n)
\]
\[
\geq 2H(U^n) - 2I(U^n; Z^n)
\]
\[
+ H(V^n_1, V^n_2|U^n) - I(V^n_1, V^n_2; Z^n|U^n)
\]
\[
\geq H(U^n) + H(U^n, V^n_1, V^n_2) - 2nI(U; Z)
\]
\[
- nI(V_1, V_2; Z|U) - n\tau_n/6
\]
\[
\geq 2n[R_{2k} + R_{1k} + R_x] + n[R_{1s} + R_{1r} + R_{2s} + R_{2r}]
\]
\[
- 2nI(U; Z) - nI(V_1, V_2; Z|U) - n\tau_n/3,
\]
where \(d\) follows from the fact that \(I(U^n; Z^n) \leq nI(U; Z) + n\tau_n/18\) and \(I(V^n_1, V^n_2; Z^n|U^n) \leq nI(V_1, V_2; Z|U) + n\tau_n/18\), the proofs of which follow similarly to the proof of [20, Lemma 3]; \(e\) follows by data processing inequality and Fano’s inequality that
\[
H(U^n) \geq n[R_{2k} + R_{1k} + R_x] - n\tau_n/12 \text{ (if } (11) \text{ is fulfilled)};
\]
\[
H(U^n, V^n_1, V^n_2) \geq n[R_{2k} + R_{1k} + R_x + R_{1s} + R_{1r} + R_{2s} + R_{2r}] - n\tau_n/12 \text{ (if } (11), (12), (13), (14) \text{ are fulfilled)};
\]
\[
H(U^n, V^n_1, V^n_2) \geq I(U^n, V^n_1, V^n_2; Y^n_1, Y^n_2)
\]
\[
\geq I(M_{1k}, M_{2k}, M_r, M_{1s}, M_{1r}, M_{2s}, M_{2r}; Y^n_1, Y^n_2)
\]
\[
\geq n[R_{1k} + R_{2k} + R_x + R_{1s} + R_{1r} + R_{2s} + R_{2r}] - n\tau_n/12.
\]

Combining (15) and (18), we obtain
\[
H(M_1|Z^n) + H(M_2|Z^n)
\]
\[
\geq H(U^n, V^n_1|Z^n) - n[R_{1r} + R_{1c} - I(V_1; Z|U)]
\]
\[
- n[R_{2k} + R_x - I(U; Z)] - n\tau_n/3
\]
\[
+ H(U^n, V^n_2|Z^n) - n[R_{2r} + R_x - I(V_2; Z|U)]
\]
\[
- n[R_{1k} + R_x - I(U; Z)] - n\tau_n/3
\]
\[
\geq n[R_3 + R_2 - n\tau_n - n[R_{1c} + R_{2c}]
\]
\[
+ n[I(V_1; Z|U) + I(V_2; Z|U) - I(V_1, V_2; Z|U)]
\]
\[
\geq n[R_1 + R_2 - n\tau_n],
\]
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
\[
R_{1c} + R_{2c} \leq I(V_1; Z|U) + I(V_2; Z|U) - I(V_1, V_2; Z|U).
\]

\textbf{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 \(R_{r_1}, R_{r_2}, R_{c_1}, R_{c_2}\) 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].

\textbf{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
\[
Y_1 = D^{n_{1s}}X,
\]
\[
Y_2 = D^{n_{2s}}X,
\]
\[
Z = D^{n_{e}}X,
\]
where \(X\) is the binary input vector of length \(q = n_1 + n_2 + n_e\); \(D\) 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:

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

\[ R_2 \leq n_2, \quad R_1 + R_2 \leq n_1; \]

- under joint secrecy constraint:
\[
R_2 \leq n_2 - n_e^+; \quad R_1 + R_2 \leq n_1 - n_e^+\;
\]

- under individual secrecy constraint:
\[
R_1 \leq n_1 - n_e^+; \quad R_2 \leq n_2 - n_e^+ \quad \text{and}
\]
\[
R_1 + R_2 \leq n_1,
\]
where \([a]^+ = \max\{0, a\}\).

\textbf{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 \(0 \leq n_e \leq n_e^+\), 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...
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.

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


