# Discrete Memoryless Interference and Broadcast Channels with Confidential Messages

Ruoheng Liu, Ivana Marić, Predrag Spasojević, and Roy D. Yates

*Abstract*— **Discrete memoryless interference and broadcast channels in which independent confidential messages are sent to two receivers are considered. Confidential messages are transmitted to each receiver with perfect secrecy, as measured by the equivocation at the other receiver. In this paper, we derive inner and outer bounds for the achievable rate regions for these two communication systems.**

## I. Introduction

We first consider a discrete memoryless *interference channel* in which two transmitters wish to send independent, confidential messages to their respective receivers. We refer to such a channel as the *interference channel with confidential messages* (IC-CM) and denote it $(\mathcal{X}_1 \times \mathcal{X}_2, p(y_1, y_2|x_1, x_2), \mathcal{Y}_1 \times \mathcal{Y}_2)$. This communication model is shown in Figure 1. We also consider the *broadcast channel with confidential messages* (BC-CM), denoted $(\mathcal{X}, p(y_1, y_2|x), \mathcal{Y}_1 \times \mathcal{Y}_2)$, in which confidential messages from a single transmitter are to be communicated to two receivers. The corresponding broadcast communication model is shown in Figure 2. The ignorance of a user with respect to the message intended for the other receiver is measured by equivocation. This approach was introduced by Wyner [1] for the wiretap channel, a scenario in which a single source-destination communication is eavesdropped. Under the assumption that the channel to the wire-tapper is a degraded version of that to the receiver, Wyner determined the capacity-secrecy tradeoff. This result was generalized by Csiszár and Körner who determined the capacity region of the broadcast channel with confidential messages [2] in which a message intended for one of the receivers is confidential.

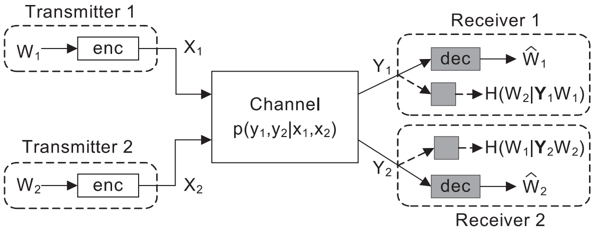

Fig. 1. Interference Channel with Confidential Messages.

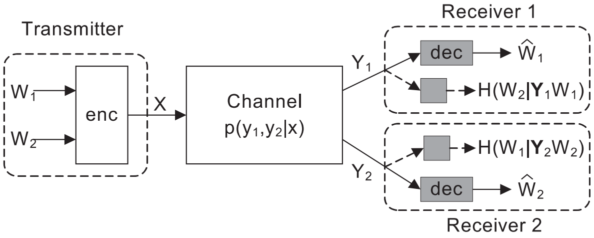

Fig. 2. Broadcast Channel with Confidential Messages.

In this paper, we study inner and outer bounds for achievable secrecy regions of both the broadcast and the interference channel under the requirement of *perfect secrecy*. That is, each receiver is kept in total ignorance with respect to the messages intended for the other receiver. We first derive outer bounds which have an identical mutual information expressions that apply for the broadcast channel when one sender jointly encodes both messages and for the interference channel when two senders offer independent inputs to the channel. The difference is that the optimization is over different input probability distributions, as will be specified in the next section. Next, we derive an inner bound for the interference channel with confidential messages. Since we require a perfect security for confidential messages, no partial decoding of the other transmitter's message is allowed at a receiver. It precludes rate-splitting schemes used by Carleial [3] and Han and Kobayashi [4] for the classical interference channel. Finally, we investigate the inner bound for the BC-CM based on the *Slepian-Wolf binning* technique [5]. We notice that no common message in the sense of Marton [6] is conveyed to the receivers since we only consider sending confidential messages in the broadcast channel. Furthermore, we employ *double binning* technique to proof the perfect security requirement.

The remainder of this paper is organized as follows: we introduce the channel model and state our main results in Sec. II. We derive outer bounds in Sec. III. We establish inner bounds for IC-CM in Sec. IV and for BC-CM in Sec. V, respectively.

## II. Channel Model and Statement of the Result

### A. The Interference Channel

A discrete memoryless interference channel with confidential messages is described by finite sets $\mathcal{X}_1$, $\mathcal{X}_2$, $\mathcal{Y}_1$, $\mathcal{Y}_2$ and a conditional probability distribution $p(y_1, y_2|x_1, x_2)$. As shown in Fig. 1, symbols $(x_1, x_2) \in (\mathcal{X}_1 \times \mathcal{X}_2)$ are channel inputs at transmitters 1 and 2, and $(y_1, y_2) \in (\mathcal{Y}_1 \times \mathcal{Y}_2)$ are channel outputs at receivers 1 and 2, respectively.

This work was supported by NSF Grant ANI 0338805.

R. Liu, P. Spasojević, and R. D. Yates are with WINLAB, Electrical and Computer Engineering, Rutgers University, North Brunswick, NJ 08902 USA (email: {liurh,spasojev,ryates}@winlab.rutgers.edu).

I. Marić is with Department of Electrical Engineering, Stanford University, Stanford, CA 94305 (email: ivanam@wsl.stanford.edu).

Each transmitter $t$, $t = 1, 2$, intends to send an independent message $W_t \in \{1, \ldots, M_t\}$ to the receiver $t$ in $n$ channel uses with perfect secrecy. The channel is memoryless in the sense that

$$p(\mathbf{y}_1, \mathbf{y}_2|\mathbf{x}_1, \mathbf{x}_2) = \prod_{i=1}^{n} p(y_{1,i}, y_{2,i}|x_{1,i}, x_{2,i}) \qquad (1)$$

where $\mathbf{x}_t = \big[x_{t,1}, \quad \ldots, \quad x_{t,n}\big]$. A stochastic encoder $f_t$ for the transmitter $t$ is specified by a matrix of conditional probabilities $f_t(\mathbf{x}_t|w_t)$, where $\mathbf{x}_t \in \mathcal{X}_t^n$, $w_t \in \mathcal{W}_t$, and

$$\sum_{\mathbf{x}_t \in \mathcal{X}_t^n} f_t(\mathbf{x}_t|w_t) = 1. \qquad (2)$$

Decoding functions are mappings $\psi_t : \mathcal{Y}_t \rightarrow \mathcal{W}_t$. Secrecy levels at receivers 1 and 2 are measured by normalized equivocations

$$\frac{1}{n}H(W_2|\mathbf{Y}_1, W_1) \quad \text{and} \quad \frac{1}{n}H(W_1|\mathbf{Y}_2, W_2). \qquad (3)$$

An $(M_1, M_2, n, P_e)$ code for the interference channel consists of described of two encoding function $f_1$, $f_2$, two decoding function $\psi_1$, $\psi_2$, and a maximum average error probability

$$P_e \triangleq \max\{P_{e,1},\, P_{e,2}\} \qquad (4)$$

where for $t = 1, 2$,

$$\begin{aligned} P_{e,t} &= \sum_{w_1,w_2} \frac{1}{M_1 M_2} P\big[\psi_t(\mathbf{Y}_t) \neq w_t|(w_1, w_2) \text{ sent}\big] \qquad (5)\\ &= \sum_{w_1,w_2} \frac{1}{M_1 M_2} \sum_{\mathbf{x}_1 \in \mathcal{X}_1^n} \sum_{\mathbf{x}_2 \in \mathcal{X}_2^n} f_t(\mathbf{x}_t|w_t)\times \\ &\qquad P\big[\psi_t(\mathbf{Y}_t) \neq w_t|(w_1, w_2, \mathbf{x}_1, \mathbf{x}_2) \text{ sent}\big]. \qquad (6) \end{aligned}$$

A rate pair $(R_1,\, R_2)$ is said to be achievable for the interference channel with confidential messages if, for any $\epsilon_0 > 0$, there exists a $(M_1, M_2, n, P_e)$ code such that

$$M_t \geq 2^{nR_t}, \quad P_e \leq \epsilon_0 \quad \text{for } t = 1, 2 \qquad (7)$$

and

$$\begin{aligned} H(W_1) - H(W_1|\mathbf{Y}_2, W_2) &\leq n\epsilon_0 \qquad (8)\\ H(W_2) - H(W_2|\mathbf{Y}_1, W_1) &\leq n\epsilon_0. \qquad (9) \end{aligned}$$

### B. The Broadcast Channel

A discrete memoryless broadcast channel with confidential messages is described by finite sets $\mathcal{X}$, $\mathcal{Y}_1$, $\mathcal{Y}_2$, and a conditional probability distribution $p(y_1, y_2|x)$. Symbols $x \in \mathcal{X}$ are channel inputs and $(y_1, y_2) \in (\mathcal{Y}_1 \times \mathcal{Y}_2)$ are channel outputs at receivers 1 and 2, respectively. The transmitter intends to send independent message $W_t \in \{1, \ldots, M_t\} \triangleq \mathcal{W}_t$ to respective receivers $t \in \{1, 2\}$ in $n$ channel uses with perfect secrecy, as measured by equivocation at the other receiver. The channel is memoryless in the sense that

$$p(\mathbf{y}_1, \mathbf{y}_2|\mathbf{x}) = \prod_{i=1}^{n} p(y_{1,i}, y_{2,i}|x_i). \qquad (10)$$

A stochastic encoder $f$ is specified by a matrix of conditional probabilities $f(\mathbf{x}|w_1, w_2)$, where $\mathbf{x} \in \mathcal{X}^n$, $w_t \in \mathcal{W}_t$, and

$$\sum_{\mathbf{x} \in \mathcal{X}^n} f(\mathbf{x}|w_1, w_2) = 1. \qquad (11)$$

Note that $f(\mathbf{x}|w_1, w_2)$ is the probability that the messages $(w_1, w_2)$ are encoded as channel input $\mathbf{x}$. The decoding function at the receiver $t$ is a mapping $\phi_t : \mathcal{Y}_t \rightarrow \mathcal{W}_t$. The secrecy levels with respect to the confidential messages $W_1$ and $W_2$ are measured, respectively, at receivers 1 and 2 by the normalized equivocations (3).

An $(M_1, M_2, n, P_e)$ code for the broadcast channel consists of the encoding function $f$, two decoding functions $\phi_1$, $\phi_2$, and the average error probability given by (4), where for $t = 1, 2$,

$$\begin{aligned} P_{e,t} &= \sum_{w_1,w_2} \frac{1}{M_1 M_2} P\big[\phi_t(\mathbf{Y}_t) \neq w_t|(w_1, w_2) \text{ sent}\big] \qquad (12)\\ &= \sum_{w_1,w_2} \frac{1}{M_1 M_2} \sum_{\mathbf{x} \in \mathcal{X}^n} f(\mathbf{x}|w_1, w_2)\times \\ &\qquad P\big[\phi_t(\mathbf{Y}_t) \neq w_t|(w_1, w_2, \mathbf{x}) \text{ sent}\big]. \qquad (13) \end{aligned}$$

A rate pair $(R_1,\, R_2)$ is said to be achievable for the broadcast channel with confidential messages if, for any $\epsilon_0 > 0$, there exists a $(M_1, M_2, n, P_e)$ code which satisfies (7)-(9).

### C. Statement of the Result

The following theorems are the main results of this paper. The theorems give the outer and inner bounds on capacity regions of interference and broadcast channels with confidential messages.

We define $\pi$ as a class of joint distributions and $\mathcal{R}(\pi)$ as the union over all distributions in $\pi$ of all $(R_1, R_2)$ satisfying

$$\begin{aligned} 0 \leq R_1 &\leq I(V_1; Y_1|U) - I(V_1; Y_2|U)\\ 0 \leq R_2 &\leq I(V_2; Y_2|U) - I(V_2; Y_1|U) \qquad (14) \end{aligned}$$

where $U$, $V_1$, and $V_2$ are auxiliary random variables. In particular, we consider the following three classes of joint distributions. For the interference channel, let $\pi_{\text{IC}-\text{O}}$ be the class of distributions $p(u, v_1, v_2, x_1, x_2, y_1, y_2)$ that factor as

$$p(u)p(v_1, v_2|u)p(x_1|v_1)p(x_2|v_2)p(y_1, y_2|x_1, x_2) \qquad (15)$$

and $\pi_{\text{IC}-\text{I}}$ be the class of distributions that factor as

$$p(u)p(v_1|u)p(v_2|u)p(x_1|v_1)p(x_2|v_2)p(y_1, y_2|x_1, x_2). \qquad (16)$$

For broadcast channel, let $\pi_{\text{BC}}$ denote the class of distributions $p(u, v_1, v_2, x, y_1, y_2)$ that factor as

$$p(u)p(v_1, v_2|u)p(x|v_1, v_2)p(y_1, y_2|x). \qquad (17)$$

*Theorem 1: (Outer Bound)* For the interference channel $(\mathcal{X}_1 \times \mathcal{X}_2, p(y_1, y_2|x_1, x_2), \mathcal{Y}_1 \times \mathcal{Y}_2)$ with confidential messages, the capacity region

$$\mathcal{C}_{\text{IC}} \subseteq \mathcal{R}(\pi_{\text{IC}-\text{O}}).$$

For the broadcast channel $(\mathcal{X}, p(y_1, y_2|x), \mathcal{Y}_1 \times \mathcal{Y}_2)$ with confidential messages, the capacity region

$$\mathcal{C}_{\text{BC}} \subseteq \mathcal{R}(\pi_{\text{BC}}).$$

We provide the proof of outer bounds in Sec. III.

Let $\mathcal{R}_{\mathrm{IC-I}}(\pi_{\mathrm{IC-I}})$ denote the union over all distributions in $\pi_{\mathrm{IC-I}}$ of all $(R_1, R_2)$ satisfying

$$\begin{aligned} 0 &\le R_1 \le I(V_1;Y_1|U) - I(V_1;Y_2|V_2,U)\\ 0 &\le R_2 \le I(V_2;Y_2|U) - I(V_2;Y_1|V_1,U). \end{aligned} \tag{18}$$

*Theorem 2: (Inner Bound for IC-CM)* Any rate pair

$$(R_1, R_2) \in \mathcal{R}_{\mathrm{IC-I}}(\pi_{\mathrm{IC-I}})$$

is achievable for the interference channel with confidential messages.

We provide the proof in Sec. IV.

Let $\mathcal{R}_{\mathrm{BC}}(\pi_{\mathrm{BC}})$ denote the union over all distributions in $\pi_{\mathrm{BC}}$ of all $(R_1, R_2)$ satisfying

$$\begin{aligned} 0 &\le R_1 \le I(V_1;Y_1|U) - I(V_1;Y_2|V_2,U) - I(V_1;V_2|U)\\ 0 &\le R_2 \le I(V_2;Y_2|U) - I(V_2;Y_1|V_1,U) - I(V_1;V_2|U). \end{aligned} \tag{19}$$

*Theorem 3: (Inner Bound for BC-CM)* Any rate pair $(R_1, R_2) \in \mathcal{R}_{\mathrm{BC}}(\pi_{\mathrm{BC}})$ is achievable for the broadcast channel with confidential messages.

We prove Theorem 3 in Sec. V.

We note that, for BC-CM, we can employ joint encoding at the transmitter. However, to preserve confidentiality, each achievable rate is with a penalty in terms of $I(V_1;V_2|U)$.

## III. Outer Bound

We now prove Theorem 1 and derive the outer bound for $R_1$. The outer bound for $R_2$ will follow by symmetry. Fano's inequality implies that

$$H(W_1|\mathbf{Y}_1) \le \epsilon_0 \log(M_1 - 1) + h(\epsilon_0) \triangleq n\delta_1 \tag{20}$$

where $h(x)$ is the binary entropy function.

The secrecy requirement (8) implies that

$$nR_1 = H(W_1) \le H(W_1|\mathbf{Y}_2, W_2) + n\epsilon_0. \tag{21}$$

First, we write

$$H(W_1|\mathbf{Y}_2, W_2)$$
$$\le H(W_1|\mathbf{Y}_2) \tag{22}$$
$$= H(W_1) - I(W_1;\mathbf{Y}_2) \tag{23}$$
$$= I(W_1;\mathbf{Y}_1) - I(W_1;\mathbf{Y}_2) + H(W_1|\mathbf{Y}_1) \tag{24}$$
$$\le I(W_1;\mathbf{Y}_1) - I(W_1;\mathbf{Y}_2) + n\delta_1 \tag{25}$$

where the last step follows from Fano's inequality (20).

Let

$$\begin{aligned} \mathbf{Y}_1^{i-1} &= [y_{1,i}, \dots, y_{1,i-1}]\\ \text{and} \quad \tilde{\mathbf{Y}}_2^{i+1} &= [y_{2,i+1}, \dots, y_{2,n}]. \end{aligned}$$

We use the chain rule to expand $I(W_1;\mathbf{Y}_1)$ as

$$I(W_1;\mathbf{Y}_1)$$
$$= \sum_{i=1}^{n} [I(W_1;Y_{1,i}|\mathbf{Y}_1^{i-1}) \tag{26}$$
$$\begin{aligned} = \sum_{i=1}^{n} [&I(W_1, \tilde{\mathbf{Y}}_2^{i+1};Y_{1,i}|\mathbf{Y}_1^{i-1})\\ &- I(\tilde{\mathbf{Y}}_2^{i+1};Y_{1,i}|\mathbf{Y}_1^{i-1}, W_1)] \end{aligned} \tag{27}$$
$$\begin{aligned} = \sum_{i=1}^{n} [&I(W_1;Y_{1,i}|\mathbf{Y}_1^{i-1}, \tilde{\mathbf{Y}}_2^{i+1}) + I(\tilde{\mathbf{Y}}_2^{i+1};Y_{1,i}|\mathbf{Y}_1^{i-1})\\ &- I(\tilde{\mathbf{Y}}_2^{i+1};Y_{1,i}|\mathbf{Y}_1^{i-1}, W_1)] \end{aligned} \tag{28}$$
$$= \sum_{i=1}^{n} I(W_1;Y_{1,i}|\mathbf{Y}_1^{i-1}, \tilde{\mathbf{Y}}_2^{i+1}) + \Theta_1 - \Theta_2 \tag{29}$$

where

$$\Theta_1 = \sum_{i=1}^{n} I(\tilde{\mathbf{Y}}_2^{i+1};Y_{1,i}|\mathbf{Y}_1^{i-1}), \tag{30}$$
$$\Theta_2 = \sum_{i=1}^{n} I(\tilde{\mathbf{Y}}_2^{i+1};Y_{1,i}|\mathbf{Y}_1^{i-1}, W_1). \tag{31}$$

Similarly, we can expand the term $I(W_1;\mathbf{Y}_2)$ as

$$I(W_1;\mathbf{Y}_2)$$
$$= \sum_{i=1}^{n} I(W_1;Y_{2,i}|\tilde{\mathbf{Y}}_2^{i+1}) \tag{32}$$
$$\begin{aligned} = \sum_{i=1}^{n} [&I(W_1, \mathbf{Y}_1^{i-1};Y_{2,i}|\tilde{\mathbf{Y}}_2^{i+1})\\ &- I(\mathbf{Y}_1^{i-1};Y_{2,i}|\mathbf{Y}_1^{i-1}, \tilde{\mathbf{Y}}_2^{i+1})] \end{aligned} \tag{33}$$
$$\begin{aligned} = \sum_{i=1}^{n} [&I(W_1;Y_{2,i}|\mathbf{Y}_1^{i-1}, \tilde{\mathbf{Y}}_2^{i+1}) + I(\mathbf{Y}_1^{i-1};Y_{2,i}|\tilde{\mathbf{Y}}_2^{i+1})\\ &- I(\mathbf{Y}_1^{i-1};Y_{2,i}|\tilde{\mathbf{Y}}_2^{i+1}, W_1)] \end{aligned} \tag{34}$$
$$= \sum_{i=1}^{n} I(W_1;Y_{2,i}|\mathbf{Y}_1^{i-1}, \tilde{\mathbf{Y}}_2^{i+1}) + \Theta_3 - \Theta_4 \tag{35}$$

where

$$\Theta_3 = \sum_{i=1}^{n} I(\mathbf{Y}_1^{i-1};Y_{2,i}|\tilde{\mathbf{Y}}_2^{i+1}), \tag{36}$$
$$\Theta_4 = \sum_{i=1}^{n} I(\mathbf{Y}_1^{i-1};Y_{2,i}|\tilde{\mathbf{Y}}_2^{i+1}, W_1). \tag{37}$$

The relationships between $\Theta_1$ and $\Theta_3$, and $\Theta_2$ and $\Theta_4$ are given in the following lemma.

*Lemma 1:* $\Theta_1 = \Theta_3$ and $\Theta_2 = \Theta_4$.

Lemma 1 follows from [2, Lemma 7]. We provide its proof in Appendix for completeness.

Combining (21), (25), (29), and (35), Lemma 1 implies that

$$\begin{aligned} nR_1 - n(\delta_1 + \epsilon_0) \le \sum_{i=1}^{n} [&I(W_1;Y_{1,i}|\mathbf{Y}_1^{i-1}, \tilde{\mathbf{Y}}_2^{i+1})\\ &- I(W_1;Y_{2,i}|\mathbf{Y}_1^{i-1}, \tilde{\mathbf{Y}}_2^{i+1})]. \end{aligned} \tag{38}$$

Now, for $\delta \triangleq \delta_1 + \epsilon_0$, we have

$$\begin{aligned} R_1 \le \frac{1}{n}\sum_{i=1}^{n} &[I(W_1;Y_{1,i}|\mathbf{Y}_1^{i-1},\tilde{\mathbf{Y}}_2^{i+1}) \\ &- I(W_1;Y_{2,i}|\mathbf{Y}_1^{i-1},\tilde{\mathbf{Y}}_2^{i+1})] + \delta. \end{aligned} \tag{39}$$

Following the method of [7, Chapter 14], we introduce a random variable $Q$ uniformly distributed over $\{1,2,\ldots,n\}$ and independent of $(W_1,W_2,\mathbf{X}_1,\mathbf{X}_2,\mathbf{Y}_1,\mathbf{Y}_2)$. Now we can bound $R_1$ as follows

$$\begin{aligned} R_1 &\le \frac{1}{n}\sum_{i=1}^{n}[I(W_1;Y_{1,i}|\mathbf{Y}_1^{i-1},\tilde{\mathbf{Y}}_2^{i+1},Q=i) \\ &\qquad - I(W_1;Y_{2,i}|\mathbf{Y}_1^{i-1},\tilde{\mathbf{Y}}_2^{i+1},Q=i)] + \delta && (40) \\ &= \sum_{i=1}^{n} p(Q=i)[I(W_1;Y_{1,Q}|\mathbf{Y}_1^{Q-1},\tilde{\mathbf{Y}}_2^{Q+1},Q=i) \\ &\qquad - I(W_1;Y_{2,Q}|\mathbf{Y}_1^{Q-1},\tilde{\mathbf{Y}}_2^{Q+1},Q=i)] + \delta && (41) \\ &= I(W_1;Y_{1,Q}|\mathbf{Y}_1^{Q-1},\tilde{\mathbf{Y}}_2^{Q+1},Q) \\ &\qquad - I(W_1;Y_{2,Q}|\mathbf{Y}_1^{Q-1},\tilde{\mathbf{Y}}_2^{Q+1},Q) + \delta && (42) \end{aligned}$$

For

$$U \triangleq (\mathbf{Y}_1^{Q-1},\tilde{\mathbf{Y}}_2^{Q+1},Q) \tag{43}$$

$$Y_1 \triangleq Y_{1,Q} \quad \text{and} \quad Y_2 \triangleq Y_{2,Q}, \tag{44}$$

(42) becomes

$$\begin{aligned} R_1 &\le I(W_1;Y_1|U) - I(W_1;Y_2|U) + \delta && (45) \\ &= I(W_1,U;Y_1|U) - I(W_1,U;Y_2|U) + \delta. && (46) \end{aligned}$$

Lastly, we define

$$V_1 \triangleq (W_1,U) \quad \text{and} \quad V_2 \triangleq (W_2,U) \tag{47}$$

to obtain

$$R_1 \le I(V_1;Y_1|U) - I(V_1;Y_2|U) + \delta. \tag{48}$$

Similarly, we can bound $R_2$ as

$$R_2 \le I(V_2;Y_2|U) - I(V_2;Y_1|U) + \delta. \tag{49}$$

Note that, due to (47), the joint distribution $p(u,v_1,v_2,x,y_1,y_2)$ factors as (17) for a broadcast channel and factors as (15) for an interference channel.

## IV. Inner Bound for the Interference Channel with Confidential Messages

In this section we consider the achievable rate region for the interference channel. We prove that the region $\mathcal{R}(\pi_{I-IC})$ is achievable. The coding structure for the IC-CM is illustrated in Fig. 3. We employ a time-sharing parameter $U$ in the sense of Han-Kobayashi [4] and two equivocation codebooks (stochastic encoders), one for each message $W_1$ and $W_2$. Each encoder $t$ will map $\mathbf{v}_t$ into a channel input $\mathbf{x}_t$. The detail of random code generation is described as follows.

We fix $p(u)$, $p(v_1|u)$ and $p(v_2|u)$, as well as $p(x_1,x_2|v_1,v_2) = p(x_1|v_1)p(x_2|v_2)$. Let

$$R_1' \triangleq I(V_1;Y_2|V_2,U) - \epsilon_1 \tag{50}$$

$$R_2' \triangleq I(V_2;Y_1|V_1,U) - \epsilon_1 \tag{51}$$

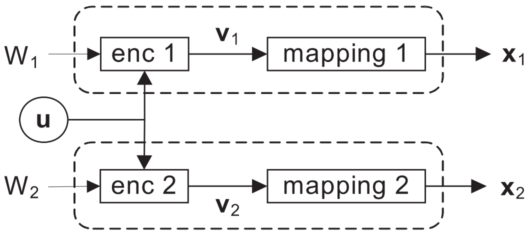

Fig. 3. Code construction for the IC-CM

where $\epsilon_1 > 0$ and $\epsilon_1 \to 0$ as $n \to \infty$.

- **Codebook generation:** We generate randomly a typical sequence $\mathbf{u}$ with probability $p(\mathbf{u}) = \prod_{i=1}^{n} p(u_i)$. We assume that both the transmitters and the receivers know the sequence $\mathbf{u}$.

  For transmitter $t$, $t = 1,2$, we generate $Q_t = 2^{n(R_t+R_t')}$ independent sequences $\mathbf{v}_t$ each with probability

  $$p(\mathbf{v}_t|\mathbf{u}) = \prod_{i=1}^{n} p(v_{t,i}|u_i)$$

  and label them

  $$\mathbf{v}_t(w_t,k_t),\ w_t \in \{1,\ldots,M_t\} \text{ and } k_t \in \{1,\ldots,M_t'\} \tag{52}$$

  where $M_t = 2^{nR_t}$ and $M_t' = 2^{nR_t'}$. Without loss of generality, $M_t$, $M_t'$, and $Q_t$ are assumed to be integers. Let's denote the transmitter $t$ codebook as

  $$\mathcal{C}_t \triangleq \{\mathbf{v}_t(w_t,k_t),\ \text{for all } (w_t,k_t)\}$$

  and its $w_t$-th sub-codebook (bin)

  $$\mathcal{C}_t(w_t) \triangleq \{\mathbf{v}_t(w_t,k_t),\ \text{for } k_t = 1,\ldots,M_t'\}$$

  is defined by the labeling in (52).
- **Encoding:** To send a message pair $(w_1,w_2) \in \mathcal{W}_1 \times \mathcal{W}_2$, each transmitter employs a stochastic encoder. Encoder $t$ randomly chooses an element $\mathbf{v}_t(w_t,k_t)$ from the sub-codebook $\mathcal{C}_t(w_t)$. Each transmitter generates the channel input sequences based on the mapping $p(x_1|v_1)$ and $p(x_2|v_2)$ respectively.
- **Decoding:** For a given typical sequence $\mathbf{u}$, let $A_\epsilon^{(n)}(V_t,Y_t|\mathbf{u})$ denote the set of jointly typical sequences $\mathbf{v}_t$ and $\mathbf{y}_t$ with respect to $p(v_t,y_t|u)$ [7, Chapter 14.2]. Given a sequence $\mathbf{u}$, decoder $t$ chooses $w_t$ such that $(\mathbf{v}_t(w_t,k_t),\mathbf{y}_t) \in A_\epsilon^{(n)}(V_t,Y_t|\mathbf{u})$ if such $w_t$ exists and and is unique; otherwise, an error is declared.

### A. Error Probability Analysis

To bound the probability of error, we define the event

$$E_t(w_t,k_t) \triangleq \{(\mathbf{v}_t(w_t,k_t),\mathbf{y}_t|\mathbf{u}) \in A_\epsilon^{(n)}(V_t,Y_t|\mathbf{u})\}. \tag{53}$$

Without loss of generality, we can assume that transmitter 1 sends the message $w_1 = 1$ associated with the codeword $\mathbf{v}_1(1,1)$, and define the corresponding event

$$K_1 \triangleq \{\mathbf{v}_1(1,1) \text{ sent}\}. \tag{54}$$

The union bound on the error probability of receiver 1 is as follows

$$\begin{aligned} P_{e1} &\le P\left\{\bigcap_{k_1} E_1^c(1,k_1)\Big|K_1\right\} \\ &\quad + \sum_{w_1\neq 1}\sum_{k_1} P\{E_1(w_1,k_1)|K_1\} \\ &\le P\{E_1^c(1,1)|K_1\} + \sum_{w_1\neq 1}\sum_{k_1} P\{E_1(w_1,k_1)|K_1\} \end{aligned} \tag{55}$$

where $E_1^c(1,k_1)$ denotes the event

$$\{(\mathbf{v}_1(1,k_1),\mathbf{y}_1) \notin A_\epsilon^{(n)}(V_1,Y_1|\mathbf{u})\}.$$

Following the joint asymptotic equipartition property (AEP) [7], we have

$$P\{E_1^c(1,1)|K_1\} \le \epsilon, \tag{56}$$

and, for $w_1 \neq 1$,

$$\begin{aligned} &P\{E_1(w_1,k_1)|K_1\} \\ &= \sum_{(\mathbf{v}_1(w_1,k_1),\mathbf{y}_1)\in A_\epsilon^{(n)}(V_1,Y_1|\mathbf{u})} p(\mathbf{v}_1(w_1,k_1),\mathbf{y}_1|\mathbf{u}) \\ &= \sum_{(\mathbf{v}_1(w_1,k_1),\mathbf{y}_1)\in A_\epsilon^{(n)}(V_1,Y_1|\mathbf{u})} p(\mathbf{v}_1(w_1,k_1)|\mathbf{u})p(\mathbf{y}_1|\mathbf{u}) \\ &\le 2^{n[H(V_1,Y_1|U)+\epsilon]}\, 2^{-n[H(V_1|U)-\epsilon]}\, 2^{-n[H(Y_1|U)-\epsilon]} \\ &= 2^{-n[I(V_1;Y_1|U)-3\epsilon]}. \end{aligned} \tag{57}$$

Note that (57) follows from the code generation process, namely, for a given $\mathbf{u}$, codewords $\mathbf{v}_1(1,1)$ and $\mathbf{v}_1(w_1,k_1)$ (where $w_1 \neq 1$) are independent, and $\mathbf{y}_1$ is the result of sending the codeword $\mathbf{v}_1(1,1)$ over the channel, so $\mathbf{y}_1$ and $\mathbf{v}_1(w_1,k_1)$ are independent, for $w_1 \neq 1$ and given $\mathbf{u}$. Hence, we can bound the probability of error as

$$\begin{aligned} P_{e1} &\le \epsilon + Q_1 2^{-n[I(V_1;Y_1|U)-3\epsilon]} \\ &= \epsilon + 2^{n(R_1+R_1')}\, 2^{-n[I(V_1;Y_1|U)-3\epsilon]} \end{aligned} \tag{58}$$

So, if

$$R_1 + R_1' < I(V_1;Y_1|U), \tag{59}$$

then for any $\epsilon_0 > 0$, $P_{e1} \le \epsilon_0$ as $n \to \infty$. Similar, for receiver 2 if

$$R_2 + R_2' < I(V_2;Y_2|U), \tag{60}$$

the probability error at receiver 2 can be made to arbitrary small, i.e., $P_{e2} \le \epsilon_0$ as $n \to \infty$. Hence, (4), (50), and (59)-(60) imply that $P_e \to 0$ as long as $n \to \infty$ and the rate pair $(R_1,R_2) \in \mathcal{R}(\pi_{I-IC})$.

### B. Equivocation

To show that secrecy requirements (8) and (9) hold, we will use the following lemma.

*Lemma 2:* The random code generation implies that the following form Markov chains hold

$$\begin{aligned} &W_2 \to (\mathbf{V}_2,\mathbf{U}) \to (\mathbf{Y}_2,W_1) \\ &W_1 \to (\mathbf{V}_1,\mathbf{V}_2,\mathbf{U}) \to \mathbf{Y}_2 \end{aligned}$$

*Proof:* The result follows easily by the problem definition and the random code construction. ■

Markov chains in Lemma 2 yield

$$I(W_1;W_2|\mathbf{Y}_2,\mathbf{V}_2,\mathbf{U}) = 0 \tag{61}$$

$$I(W_1;\mathbf{Y}_2|\mathbf{V}_1,\mathbf{V}_2,\mathbf{U}) = 0 \tag{62}$$

We next consider the following equivocation bound

$$\begin{aligned} &H(W_1|\mathbf{Y}_2,W_2) \\ &\quad \ge H(W_1|\mathbf{Y}_2,W_2,\mathbf{V}_2,\mathbf{U}) && (63) \\ &\quad = H(W_1|\mathbf{Y}_2,\mathbf{V}_2,\mathbf{U}) && (64) \\ &\quad = H(W_1,\mathbf{Y}_2|\mathbf{V}_2,\mathbf{U}) - H(\mathbf{Y}_2|\mathbf{V}_2,\mathbf{U}) \\ &\quad = H(W_1,\mathbf{V}_1,\mathbf{Y}_2|\mathbf{V}_2,\mathbf{U}) - H(\mathbf{V}_1|\mathbf{Y}_2,\mathbf{V}_2,\mathbf{U},W_1) \\ &\qquad - H(\mathbf{Y}_2|\mathbf{V}_2,\mathbf{U}) \\ &\quad = H(W_1,\mathbf{V}_1|\mathbf{V}_2,\mathbf{U}) - H(\mathbf{V}_1|\mathbf{Y}_2,\mathbf{V}_2,\mathbf{U},W_1) \\ &\qquad - [H(\mathbf{Y}_2|\mathbf{V}_2,\mathbf{U}) - H(\mathbf{Y}_2|\mathbf{V}_1,\mathbf{V}_2,\mathbf{U},W_1)] \\ &\quad = H(W_1,\mathbf{V}_1|\mathbf{V}_2,\mathbf{U}) - H(\mathbf{V}_1|\mathbf{Y}_2,\mathbf{V}_2,\mathbf{U},W_1) \\ &\qquad - [H(\mathbf{Y}_2|\mathbf{V}_2,\mathbf{U}) - H(\mathbf{Y}_2|\mathbf{V}_1,\mathbf{V}_2,\mathbf{U})] && (65) \\ &\quad = H(W_1,\mathbf{V}_1|\mathbf{V}_2,\mathbf{U}) - H(\mathbf{V}_1|\mathbf{Y}_2,\mathbf{V}_2,\mathbf{U},W_1) \\ &\qquad - I(\mathbf{V}_1;\mathbf{Y}_2|\mathbf{V}_2,\mathbf{U}) \\ &\quad \ge H(\mathbf{V}_1|\mathbf{V}_2,\mathbf{U}) - H(\mathbf{V}_1|\mathbf{Y}_2,\mathbf{V}_2,\mathbf{U},W_1) \\ &\qquad - I(\mathbf{V}_1;\mathbf{Y}_2|\mathbf{V}_2,\mathbf{U}) && (66) \end{aligned}$$

where inequality (63) is due to the fact that conditioning reduces entropy, and (64) and (65) follow from (61) and (62), respectively.

Now, we consider the first term in (66). Note that given $\mathbf{U} = \mathbf{u}$, $\mathbf{V}_1$ and $\mathbf{V}_2$ are independent and $\mathbf{V}_1$ has $Q_1$ possible values with equal probability. Hence, we have

$$\begin{aligned} H(\mathbf{V}_1|\mathbf{U},\mathbf{V}_2) &= H(\mathbf{V}_1|\mathbf{U}) \\ &= \log Q_1 \\ &= n(R_1 + R_1'). \end{aligned} \tag{67}$$

We next show that $H(\mathbf{V}_1|\mathbf{Y}_2,\mathbf{V}_2,\mathbf{U},W_1) \le n\epsilon_2$, where $\epsilon_2 \to 0$ as $n \to \infty$. In order to calculate the conditional entropy $H(\mathbf{V}_1|\mathbf{Y}_2,\mathbf{V}_2,\mathbf{U},W_1)$, we consider the following situation. Let's fix $W_1 = w_1$, and assume that transmitter 1 sends a codeword $\mathbf{v}_1(w_1,k_1) \in \mathcal{C}_1(w_1)$, for $1 \le k_1 \le M_1'$, to the channel and receiver 2 knows the sequence $\mathbf{V}_2 = \mathbf{v}_2$ and $\mathbf{U} = \mathbf{u}$. Given index $W_1 = w_1$, receiver 2 decodes the codeword $\mathbf{v}_1(w_1,k_1)$ based on the received sequence $\mathbf{y}_2$. Let $\lambda(w_1)$ denote the average probability of error of decoding the index $k_1$ at receiver 2. Based on joint typicality [7, Chapter 8], we have the following lemma.

*Lemma 3:* $\lambda(w_1) \le \epsilon_0$ as $n \to \infty$.

Proof of Lemma 3 is in the Appendix.

Fano's inequality implies that

$$\begin{aligned}\frac{1}{n}H(\mathbf{V}_1|\mathbf{Y}_2,\mathbf{V}_2,\mathbf{U},W_1=w_1) &\le \frac{1}{n}[1+\lambda(w_1)\log M_1']\\ &\le \frac{1}{n}+\epsilon_0 I(V_1;Y_2|V_2,U)\\ &\triangleq \epsilon_2 \qquad (68)\end{aligned}$$

where the second inequality follows from Lemma 3 and (50). Consequently,

$$\begin{aligned}&\frac{1}{n}H(\mathbf{V}_1|\mathbf{Y}_2,\mathbf{V}_2,\mathbf{U},W_1)\\ &\quad=\frac{1}{n}\sum_{w_1\in\mathcal{W}_1}p(W_1=w_1)H(\mathbf{V}_1|\mathbf{Y}_2,\mathbf{V}_2,\mathbf{U},W_1=w_1)\\ &\quad\le \epsilon_2. \qquad (69)\end{aligned}$$

Finally, the third term in (66) can be bounded based on the following lemma.

*Lemma 4:*

$$I(\mathbf{V}_1;\mathbf{Y}_2|\mathbf{V}_2,\mathbf{U}) \le nI(V_1;Y_2|V_2,U)+n\epsilon_3 \qquad (70)$$

where $\epsilon_3 \to 0$ as $n \to 0$.
The proof is given in the Appendix.

Therefore, by using (67), (69), and (70), we can rewrite (66) as

$$\begin{aligned}&\frac{1}{n}H(W_1|\mathbf{Y}_2,\mathbf{X}_2,W_2)\\ &\qquad\ge R_1+R_1'-I(V_1;Y_2|V_2,U)-\epsilon_2-\epsilon_3.\end{aligned}$$

By the definition of $R_1'$ (50), we have

$$R_1-\frac{1}{n}H(W_1|\mathbf{Y}_2,\mathbf{X}_2,W_2) \le \epsilon_4 \qquad (71)$$

where $\epsilon_4 \triangleq \epsilon_1+\epsilon_2+\epsilon_3$, and, thus, the security condition (8) is satisfied. Following the same approach, we can prove that (9) is satisfied. ■

## V. Inner Bound for the Broadcast Channel with Confidential Messages

We now prove Theorem 3 based on the Slepian-Wolf *binning* [5] and *double binning*. In this section we redefine the parameters $R_1$, $R_2$, $R_1'$, $R_2'$, $Q_1$, $Q_2$, $M_1$, and $M_2$. The coding structure for the BC-CM is shown in Fig. 4. We employ a joint encoder generating two equivocation codewords $\mathbf{v}_1$ and $\mathbf{v}_2$, one for each message $W_1$ and $W_2$. The equivocation codewords are mapped into the channel input $\mathbf{x}$. The detail of random code generation is described as follows.

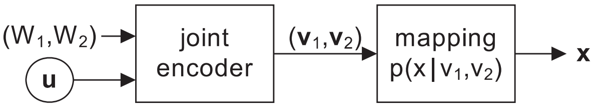

Fig. 4. Code construction for the BC-CM

We fix $p(u)$, $p(v_1|u)$ and $p(v_2|u)$, as well as $p(x|v_1,v_2)$. Let $0 \le \alpha \le 1$,

$$\begin{aligned}R_1' &\triangleq I(V_1;Y_2|V_2,U)-\epsilon_1'\\ R_2' &\triangleq I(V_2;Y_1|V_1,U)-\epsilon_1' \qquad (72)\end{aligned}$$

and

$$R^\dagger = I(V_1;V_2|U) \qquad (73)$$

where $\epsilon_1' > 0$ and $\epsilon_1' \to 0$ as $n \to \infty$.

- **Codebook generation:** We generate randomly a typical sequence $\mathbf{u}$ with probability $p(\mathbf{u})=\prod_{i=1}^n p(u_i)$. We assume that both the transmitter and the receivers know the sequence $\mathbf{u}$.
  We generate $Q_t = 2^{n(R_t+R_t'+R^\dagger)}$ independent sequences $\mathbf{v}_t$ each with probability
  $$p(\mathbf{v}_t|\mathbf{u})=\prod_{i=1}^n p(v_{t,i}|u_i)$$
  and label them
  $$\begin{aligned}&\mathbf{v}_t(w_t,s_t,k_t),\ \text{for } w_t\in\{1,\dots,M_t\},\\ &\quad s_t\in\{1,\dots,J_t\},\ \text{and } k_t\in\{1,\dots,G_t\}. \qquad (74)\end{aligned}$$
  where $M_t=2^{nR_t}$, $J_t=2^{nR_t'}$, and $G_t=2^{nR^\dagger}$. Without loss of generality $Q_t$, $M_t$, $J_t$, and $G_t$ are considered to be integers.

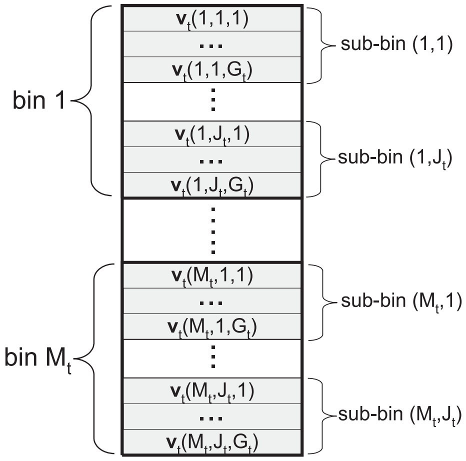

Fig. 5. Double binning for $\mathbf{v}_t$ sequences

Let's denote the transmitter $t$ codebook as

$$\mathcal{C}_t \triangleq \big\{\mathbf{v}_t(w_t,s_t,k_t),\ \text{for all } (w_t,s_t,k_t)\big\}.$$

Based on the labeling in (74), the codebook $\mathcal{C}_t$ is partitioned into $M_t$ bins, and the $w_t$-th bin is

$$\begin{aligned}\mathcal{C}_t(w_t) \triangleq \{&\mathbf{v}_t(w_t,s_t,k_t),\ \text{for } s_t\in\{1,\dots,J_t\}\\ &\text{and } k_t\in\{1,\dots,G_t\}. \qquad (75)\end{aligned}$$

Furthermore, each bin $\mathcal{C}_t(w_t)$ is divided into $J_t$ sub-bins, and the $(w_t,s_t)$-th sub-bin is

$$\mathcal{C}_t(w_t,s_t) \triangleq \big\{\mathbf{v}_t(w_t,s_t,k_t),\ \text{for } k_t\in\{1,\dots,G_t\}\big\}. \qquad (76)$$

The double binning structure for $\mathbf{v}_t$ sequences is shown in Fig. 5.

- **Encoding:** To send the message pair $(w_1, w_2) \in \mathcal{W}_1 \times \mathcal{W}_2$, the transmitter employs a stochastic encoder. We randomly chooses an sub-bin $\mathcal{C}_t(w_t, s_t)$ from the bin $\mathcal{C}_t(w_t)$, for $t = 1, 2$. Next, we select a pair $(k_1, k_2)$ such that
$$\big(\mathbf{v}_1(w_1, s_t, k_1), \mathbf{v}_2(w_2, s_2, k_2)\big) \in A_\epsilon^{(n)}(V_1, V_2|\mathbf{u}),$$
where $A_\epsilon^{(n)}(V_1, V_2|\mathbf{u})$ denotes, for a given typical sequence $\mathbf{u}$, the set of jointly typical sequences $\mathbf{v}_1$ and $\mathbf{v}_2$ with respect to $p(v_1, v_2|u)$. If there are more than one such pair, then randomly select one. Generate the channel input sequence $\mathbf{x}$ according to the mapping $p(x|v_1, v_2)$.
- **Decoding:** For a given typical sequence $\mathbf{u}$, let $A_\epsilon^{(n)}(V_t, Y_t|\mathbf{u})$ denote the set of jointly typical sequences $\mathbf{v}_t$ and $\mathbf{y}_t$ with respect to $p(v_t, y_t|u)$. Decoder $t$ chooses $w_t$ such that $(\mathbf{v}_t(w_t, s_t, k_t), \mathbf{y}_t) \in A_\epsilon^{(n)}(V_t, Y_t|\mathbf{u})$ if such $w_t$ exists and and is unique; otherwise, an error is declared.

### A. Error Probability Analysis

Without loss of generality, we assume that the transmitter sends the message pair $(w_1 = 1, w_2 = 1)$ and $s_1 = s_2 = 1$. First, we consider the error event $T$ that the encoder can not find an appropriate jointly typical pair, i.e.,
$$\begin{aligned}T \triangleq \{&\big(\mathbf{v}_1(1,1,k_1), \mathbf{v}_2(1,1,k_2)\big) \notin A_\epsilon^{(n)}(V_1, V_2|\mathbf{u}),\\ &\text{for } s_t = 1, \dots, J_t,\ k_t = 1, \dots, G_t, \text{ and } t = 1, 2\}. \quad (77)\end{aligned}$$

The definition of $R^\dagger$ in (73) implies that
$$2R^\dagger > I(V_1, V_2|U). \quad (78)$$

Hence, following the approach of [8], we have that
$$P\{T\} \leq \delta_3 \quad (79)$$
where $\delta_3 > 0$ and $\delta_3 \to 0$ as $n \to \infty$. In other word, the encoding is successful with probability close to 1 as long as $n$ is large.

In the following, we assume that $(v_1(1,1,1), v_2(1,1,1))$ is sent and define the event
$$K_2 \triangleq \{(\mathbf{v}_1(1,1,1), \mathbf{v}_2(1,1,1)) \in A_\epsilon^{(n)}(V_1, V_2|\mathbf{u})\}.$$

Now, the error probability at receiver 1 is bounded as follows
$$\begin{aligned}P_{e1} \leq{}& P\{T\} + (1 - P\{T\})\Bigg[P\Bigg\{\bigcap_{s_1,k_1} E_1^c(1, s_1, k_1)\Bigg|K_2\Bigg\}\\ &+ \sum_{w_1 \neq 1}\sum_{s_1,k_1} P\{E_1(w_1, s_1, k_1)|K_2\}\Bigg]\\ \leq{}& P\{T\} + P\{E_1^c(1,1,1)|K_2\}\\ &+ \sum_{w_1 \neq 1}\sum_{s_1,k_1} P\{E_1(w_1, s_1, k_1)|K_2\} \quad (80)\end{aligned}$$
where
$$E_t(w_t, s_t, k_t) = \{(\mathbf{v}_t(w_t, s_t, k_t), \mathbf{y}_t) \in A_\epsilon^{(n)}(V_t, Y_t|\mathbf{u})\}.$$

Joint typicality [7, Chapter 14] implies that
$$\begin{aligned}&P\{E_1^c(1,1,1)|K_2\} \leq \epsilon,\\ &P\{E_1(w_1, s_1, k_1)|K_2\} \leq 2^{-n[I(V_1;Y_1|U)-\epsilon]} \quad \text{for } w_1 \neq 1.\end{aligned}$$

Hence, we can bound the probability of error as
$$\begin{aligned}P_{e1} &\leq \delta_3 + \epsilon + Q_1 2^{-n[I(V_1;Y_1|U)-\epsilon]}\\ &= \delta_3 + \epsilon + 2^{n(R_1+R_1'+R^\dagger)}\, 2^{-n[I(V_1;Y_1|U)-\epsilon]} \quad (81)\end{aligned}$$

So, if
$$R_1 + R_1' + R^\dagger < I(V_1; Y_1|U), \quad (82)$$
then for any $\epsilon_0 > 0$, $P_{e1} \leq \epsilon_0$ as $n \to \infty$. Similarly, for receiver 2, if
$$R_2 + R_2' + R^\dagger < I(V_2; Y_2|U), \quad (83)$$
then $P_{e2} \leq \epsilon_0$ as $n \to \infty$. Hence, (4), (72), (73), (82), and (83) imply that $P_e \to 0$ as long as $n \to \infty$ and the rate pair $(R_1, R_2) \in \mathcal{R}_{\mathrm{BC}}(\pi_{\mathrm{BC}})$.

### B. Equivocation

Here, we prove that secrecy requirements (8) and (9) hold for BC-CM. Following the same approach as (63)-(66), we have
$$\begin{aligned}H(W_1|\mathbf{Y}_2, W_2) \geq{}& H(\mathbf{V}_1|\mathbf{V}_2, \mathbf{U}) - H(\mathbf{V}_1|\mathbf{Y}_2, \mathbf{V}_2, \mathbf{U}, W_1)\\ &- I(\mathbf{V}_1; \mathbf{Y}_2|\mathbf{V}_2, \mathbf{U}). \quad (84)\end{aligned}$$

Now, we consider the first term in (84)
$$H(\mathbf{V}_1|\mathbf{U}, \mathbf{V}_2) = H(\mathbf{V}_1|\mathbf{U}) - I(\mathbf{V}_1; \mathbf{V}_2|\mathbf{U}) \quad (85)$$

Note that given $\mathbf{U} = \mathbf{u}$, $\mathbf{V}_1$ has $Q_1$ possible values with equal probability. Hence, we have $H(\mathbf{V}_1|\mathbf{U}) = \log Q_1$. Using the same approach as in Lemma 4, we can obtain
$$I(\mathbf{V}_1; \mathbf{V}_2|\mathbf{U}) \leq nI(V_1; V_2|U) + n\epsilon_2' \quad (86)$$

Hence, by the definition of $R^\dagger$ in (73), we have
$$\begin{aligned}H(W_1, \mathbf{V}_1|\mathbf{U}) &\leq \log Q_1 - nI(V_1; V_2|U) - n\epsilon_2'\\ &= n(R_1 + R_1' + R^\dagger) - I(\mathbf{V}_1; \mathbf{V}_2|\mathbf{U}) - n\epsilon_2'\\ &= n(R_1 + R_1' - \epsilon_2'). \quad (87)\end{aligned}$$

Following joint typicality [7], (69) implies
$$H(\mathbf{V}_1|\mathbf{Y}_2, \mathbf{V}_2, \mathbf{U}, W_1) \leq n\epsilon_3'$$
where $\epsilon_3' \to 0$ as $n \to 0$. Applying Lemma 4, the third term in (84) can be bounded as
$$I(\mathbf{V}_1; \mathbf{Y}_2|\mathbf{V}_2, \mathbf{U}) \leq nI(V_1; Y_2|V_2, U) + n\epsilon_4' \quad (88)$$
where $\epsilon_4' \to 0$ as $n \to 0$. Hence, by using (86), (87), and (88), we can rewrite (84) as
$$\frac{1}{n}H(W_1|\mathbf{Y}_2, W_2) \geq R_1 - \epsilon_5' \quad (89)$$
where $\epsilon_5' \triangleq \epsilon_1' + \epsilon_2' + \epsilon_3' + \epsilon_4'$, and thus the security condition (8) is satisfied. Following the same approach, we can prove that (9) also holds. ■

## Appendix

*Proof:* [**Lemma 1**]

$$\begin{aligned}
\Theta_1 &= \sum_{i=1}^{n} I(\tilde{\mathbf{Y}}_2^{i+1}; Y_{1,i}|\mathbf{Y}_1^{i-1}) && (90)\\
&= \sum_{i=1}^{n} \sum_{j=i+1}^{n} I(Y_{2,j}; Y_{1,i}|\mathbf{Y}_1^{i-1}, \tilde{\mathbf{Y}}_2^{j+1}) && (91)\\
&= \sum_{j=2}^{n} \sum_{i=1}^{j-1} I(Y_{2,j}; Y_{1,i}|\mathbf{Y}_1^{i-1}, \tilde{\mathbf{Y}}_2^{j+1}) && (92)\\
&= \sum_{j=2}^{n} I(Y_{2,j}; \mathbf{Y}_1^{j-1}|\tilde{\mathbf{Y}}_2^{j+1}) && (93)\\
&= \sum_{j=1}^{n} I(Y_{2,j}; \mathbf{Y}_1^{j-1}|\tilde{\mathbf{Y}}_2^{j+1}) && (94)\\
&= \Theta_3. && (95)
\end{aligned}$$

Note that (94) follows from $\mathbf{Y}_1^{j-1} = \emptyset$, for $j = 1$.

Similarly, by using $\tilde{\mathbf{Y}}_2^{j+1} = \emptyset$, for $j = n$, we have

$$\begin{aligned}
\Theta_4 &= \sum_{i=1}^{n} I(\mathbf{Y}_1^{i-1}; Y_{2,i}|\tilde{\mathbf{Y}}_2^{i+1}, W_1) && (96)\\
&= \sum_{i=1}^{n} \sum_{j=1}^{i-1} I(Y_{1,j}; Y_{2,i}|\mathbf{Y}_1^{j-1}, \tilde{\mathbf{Y}}_2^{i+1}, W_1) && (97)\\
&= \sum_{j=1}^{n-1} \sum_{i=j+1}^{n} I(Y_{1,j}; Y_{2,i}|\mathbf{Y}_1^{j-1}, \tilde{\mathbf{Y}}_2^{i+1}, W_1) && (98)\\
&= \sum_{j=1}^{n-1} I(Y_{1,i}; \tilde{\mathbf{Y}}_2^{j+1}|\mathbf{Y}_1^{j-1}, W_1) && (99)\\
&= \Theta_2. && (100)
\end{aligned}$$

■

*Proof:* [**Lemma 3**]

For a given typical sequence pair $(\mathbf{v}_2, \mathbf{u})$, let $A_\epsilon^{(n)}(V_1, Y_2|\mathbf{u}, \mathbf{v}_2)$ denote the set of jointly typical sequences $\mathbf{v}_1$ and $\mathbf{y}_2$ with respect to $p(v_1, y_2|v_2, u)$. To simplify notation, we use $A_\epsilon^{(n)}$ represent this set in this proof.

For given $W_1 = w_1$, decoder 2 chooses $k_1$ so that

$$(\mathbf{v}_1(w_1, k_1), \mathbf{y}_2) \in A_\epsilon^{(n)}$$

if such $k_1$ exists and and is unique; otherwise, an error is declared. Define the event

$$\hat{E}(k_1) = \{(\mathbf{v}_1(w_1, k_1), \mathbf{y}_2) \in A_\epsilon^{(n)}\}. \quad (101)$$

Without loss of generality, we assume that $\mathbf{v}_1(w_1, k_1 = 1)$ was sent, and define the event

$$\hat{K}_1 = \big\{\mathbf{v}_1(w_1, 1) \text{ sent}\big\}. \quad (102)$$

Hence

$$\lambda(w_1) \leq P\{\hat{E}^c(k_1 = 1)|\hat{K}_1\} + \sum_{k_1 \neq 1} P\{\hat{E}(k_1)|\hat{K}_1\} \quad (103)$$

where $\hat{E}^c(k_1 = 1)$ denotes the event

$$\{(\mathbf{v}_1(w_1, 1), \mathbf{y}_2) \notin A_\epsilon^{(n)}\}.$$

Following the joint AEP [7], we have

$$P\{\hat{E}^c(k_1 = 1)|\hat{K}_1\} \leq \epsilon, \quad (104)$$

and, for $k_1 \neq 1$,

$$\begin{aligned}
&P\{\hat{E}(k_1)|\hat{K}_1\}\\
&\quad = \sum_{(\mathbf{v}_1(w_1,k_1),\mathbf{y}_2) \in A_\epsilon^{(n)}} p(\mathbf{v}_1(w_1, k_1), \mathbf{y}_2|\mathbf{v}_2, \mathbf{u})\\
&\quad = \sum_{(\mathbf{v}_1(w_1,k_1),\mathbf{y}_2) \in A_\epsilon^{(n)}} p(\mathbf{v}_1(w_1, k_1)|\mathbf{v}_2, \mathbf{u}) p(\mathbf{y}_2|\mathbf{v}_2, \mathbf{u}) && (105)\\
&\quad \leq |A_\epsilon^{(n)}| \cdot 2^{-n[H(V_1|V_2,U)-\epsilon]}\, 2^{-n[H(Y_2|V_2,U)-\epsilon]}\\
&\quad \leq 2^{n[H(V_1,Y_2|V_2,U)+\epsilon]}\, 2^{-n[H(V_1|V_2,U)-\epsilon]}\, 2^{-n[H(Y_2|V_2,U)-\epsilon]}\\
&\quad = 2^{-n[I(V_1;Y_2|V_2,U)-3\epsilon]}. && (106)
\end{aligned}$$

Note that (105) follows from the code generation process, namely, for a given $\mathbf{u}$, codewords $\mathbf{v}_1(w_1, 1)$ and $\mathbf{v}_1(w_1, k_1)$ are independent, and $\mathbf{y}_2$ is the result of sending the codeword $\mathbf{v}_1(w_1, 1)$ over the channel, so $\mathbf{y}_2$ and $\mathbf{v}_1(w_1, k_1)$ are independent, for $k_1 \neq 1$ and given $\mathbf{v}_2$ and $\mathbf{u}$. Now, we can bound the probability of error as

$$\begin{aligned}
\lambda(w_1) &\leq \epsilon + M_1' \cdot 2^{-n[I(V_1;Y_2|V_2,U)-3\epsilon]} && (107)\\
&\leq \epsilon + 2^{nR_1'}\, 2^{-n[I(V_1;Y_2|V_2,U)-3\epsilon]}. && (108)
\end{aligned}$$

Note that $R_1' = I(V_1; Y_2|V_2, U) - \epsilon_1$. Hence, by choosing $\epsilon_1 > 3\epsilon$, we have

$$\lambda(w_1) \leq \epsilon_0 \quad (109)$$

where $\epsilon_0 \to 0$ as $n \to \infty$. ■

*Proof:* [**Lemma 4**]

Let $A_\epsilon^{(n)}(U, V_1, V_2, Y_2)$ denote the set of typical sequences $(\mathbf{u}, \mathbf{v}_1, \mathbf{v}_2, \mathbf{y}_2)$ with respect to $p(u, v_1, v_2, y_2)$. To simplify notation, we use $A_\epsilon^{(n)}$ represent this set in this proof. Let

$$\mu(\mathbf{u}, \mathbf{v}_1, \mathbf{v}_2, \mathbf{y}_2) = \begin{cases} 1, & (\mathbf{u}, \mathbf{v}_1, \mathbf{v}_2, \mathbf{y}_2) \notin A_\epsilon^{(n)}; \\ 0, & \text{otherwise} \end{cases} \quad (110)$$

be the corresponding indicator function.

we expand $I(\mathbf{V}_1; \mathbf{Y}_2|\mathbf{V}_2, \mathbf{U})$ as

$$\begin{aligned}
&I(\mathbf{V}_1; \mathbf{Y}_2|\mathbf{V}_2, \mathbf{U})\\
&\qquad \leq I(\mathbf{V}_1, \mu; \mathbf{Y}_2|\mathbf{V}_2, \mathbf{U})\\
&\qquad = I(\mathbf{V}_1; \mathbf{Y}_2|\mathbf{V}_2, \mathbf{U}, \mu) + I(\mu; \mathbf{Y}_2|\mathbf{V}_2, \mathbf{U})\\
&\qquad = \sum_{j=0}^{1} P(\mu = j) I(\mathbf{V}_1; \mathbf{Y}_2|\mathbf{V}_2, \mathbf{U}, \mu = j)\\
&\qquad\quad + I(\mu; \mathbf{Y}_2|\mathbf{V}_2, \mathbf{U}) && (111)
\end{aligned}$$

Note that

$$\begin{aligned}
&P(\mu=1)I(\mathbf{V}_1;\mathbf{Y}_2|\mathbf{V}_2,\mathbf{U},\mu=1)\\
&\quad\le n\log|\mathcal{Y}_2|\cdot P((\mathbf{u},\mathbf{v}_1,\mathbf{v}_2,\mathbf{y}_2)\notin A_\epsilon^{(n)})\\
&\quad\le n\epsilon\log|\mathcal{Y}_2|\,,
\end{aligned}\tag{112}$$

and

$$I(\mu;\mathbf{Y}_2|\mathbf{V}_2,\mathbf{U})\le H(\mu)\le 1.\tag{113}$$

We only consider the term $P(\mu=0)I(\mathbf{V}_1;\mathbf{Y}_2|\mathbf{V}_2,\mathbf{U},\mu=0)$. Following the sequence joint typicality properties [7], we have

$$\begin{aligned}
&P(\mu=0)I(\mathbf{V}_1;\mathbf{Y}_2|\mathbf{V}_2,\mathbf{U},\mu=0)\\
&\quad\le I(\mathbf{V}_1;\mathbf{Y}_2|\mathbf{V}_2,\mathbf{U},\mu=0)\\
&\quad=\sum_{(\mathbf{u},\mathbf{v}_1,\mathbf{v}_2,\mathbf{y}_2)\in A_\epsilon^{(n)}} p(\mathbf{u},\mathbf{v}_1,\mathbf{v}_2,\mathbf{y}_2)\\
&\qquad\log\frac{p(\mathbf{v}_1,\mathbf{y}_2|\mathbf{v}_2,\mathbf{u})}{p(\mathbf{y}_2|\mathbf{v}_2,\mathbf{u})p(\mathbf{v}_1|\mathbf{v}_2,\mathbf{u})}\\
&\quad=\sum_{(\mathbf{u},\mathbf{v}_1,\mathbf{v}_2,\mathbf{y}_2)\in A_\epsilon^{(n)}} p(\mathbf{u},\mathbf{v}_1,\mathbf{v}_2,\mathbf{y}_2)[-\log p(\mathbf{y}_2|\mathbf{v}_2,\mathbf{u})\\
&\qquad-\log p(\mathbf{v}_1|\mathbf{v}_2,\mathbf{u})+\log p(\mathbf{v}_1,\mathbf{y}_2|\mathbf{v}_2,\mathbf{u})]\\
&\quad\le\sum_{(\mathbf{u},\mathbf{v}_1,\mathbf{v}_2,\mathbf{y}_2)\in A_\epsilon^{(n)}} p(\mathbf{u},\mathbf{v}_1,\mathbf{v}_2,\mathbf{y}_2)\cdot n[H(Y_2|V_2,U)\\
&\qquad+H(V_1|V_2,U)-H(V_1,Y_2|V_2,U)+3\epsilon]\\
&\quad\le n[H(Y_2|V_2,U)+H(V_1|V_2,U)\\
&\qquad-H(V_1,Y_2|V_2,U)+3\epsilon]\\
&\quad=nI(V_1;Y_2|V_2,U)+3\epsilon.
\end{aligned}\tag{114}$$

Combining (111), (112), (113), and (114), we have the desired result

$$\begin{aligned}
&I(\mathbf{V}_1;\mathbf{Y}_2|\mathbf{V}_2\mathbf{U})\\
&\qquad\le nI(V_1;Y_2|V_2,U)+n\Big(\epsilon\log|\mathcal{Y}_2|+3\epsilon+\frac{1}{n}\Big)\\
&\qquad=nI(V_1;Y_2|V_2,U)+n\epsilon_3
\end{aligned}$$

where

$$\epsilon_3\triangleq\epsilon\log|\mathcal{Y}_2|+3\epsilon+\frac{1}{n}.$$

■

## ACKNOWLEDGMENT

The authors would like to thank Shlomo Shamai (Shitz) and Gerhard Kramer for their useful comments about the proof.

## REFERENCES

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

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

[3] A. B. Carleial, "Interference channels," *IEEE Trans. on Inf. Theory*, vol. 24, no. 1, p. 60, Jan. 1978.

[4] T. S. Han and K. Kobayashi, "A new achievable rate region for the interference channel," *IEEE Trans. on Inf. Theory*, vol. 27, no. 1, pp. 49–60, Jan. 1981.

[5] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. on Inf. Theory*, vol. 19, pp. 471–480, 1973.

[6] K. Marton, "A coding theorem for the discrete memoryless broadcast channel," *IEEE Trans. on Inf. Theory*, vol. 25, no. 1, pp. 306–311, May 1979.

[7] T. Cover and J. Thomas, *Elements of Information Theory*. John Wiley Sons, Inc., 1991.

[8] A. El Gamal and E. Van der Meulen, "A proof of Marton's coding theorem for the discrete memoryless broadcast channel," *IEEE Trans. on Inf. Theory*, vol. 27, pp. 120–122, July 1980.