SECRECY RATE REGION IN THE INTERFERENCE CHANNEL WITH COMMON INFORMATION

Hamid G. Bafghi [1], Somayeh Salimi [2], Babak Seyfe[3], Mohammad R. Aref [4]

[1, 3] Department of Electrical Engineering of Shahed Univ. Tehran, Iran,
Email :{ ghanizade, seyfe}@shahed.ac.ir
[2,4] ISSL Laboratory, Electrical Engineering Department, Sharif Univ. of Technology, Tehran, Iran,
Email: {salimi@ee.sharif, aref@sharif}.edu

ABSTRACT

In this paper interference channel with common information and two confidential messages is investigated. There are two senders that need deliver their privative messages and a certain common message. The private messages must be confidential in their corresponding receivers.

An achievable rate region and an outer bound for such a channel are obtained and it is shown that these rate regions include some existing results for some related channels.

Index Terms—Capacity-equivocation region, common information, confidential messages, secrecy rate region, rate-equivocation region

1. INTRODUCTION

INTERFERENCE channel (IC) is a fundamental building block in communication networks which appears when signals intended for one receiver, supposed as interference for the other receivers. A key question in this setting is how to conquest of interfering signal which is made in simultaneous transmissions; despite many attempts is an open problem in general case. For more detail see, e.g., [1] and the references therein. One of the problems caused of the nature of these channels is secrecy issues. It is because of the fact that the information can be extracted by the other nodes that are not destined. In this case it is decided to minimize the leakage of information in non-destination nodes i.e., eavesdroppers. It is also needed to assess the security level of the confidential information for the IC and study the achievable communication rates under a specific secrecy constraint [2].

A special scenario in which both senders intend to transmit not only their privative information but also certain common information to their corresponding destination is recently considered. Interference channel with common information (ICC) was first studied by Tan in his original paper [3], where outer and inner bounds on the capacity region have been derived and some prior results was extended. In [1] an achievable rate region for general two-user ICC is derived. Also the authors in [1] proposed an encoding scheme that extended the Carleial's successive encoding for ICC in [3], which allowed common information to be conveyed through the channel in a cooperative channel.

In this paper, we consider two-user interference channel with common message in which each senders' have private message that must be secure in unintended receiver (Fig. 1). We establish the capacity-equivocation region for ICC channel and we show that the capacity-equivocation region reduces to the capacity region of ICC in [1]. Furthermore we show that in a special case, our region reduces to the capacity of cognitive interference channel with secrecy that was studied in [2].

The rest of the paper is organized as follows. In Section 2 we introduce the model of ICC channel with confidential messages. In Section 3, we present the capacity-equivocation region and discuss the relations between our achievable rate region and several existing results in [1] and [2]. Finally we conclude in Section IV.

2. CHANNEL MODELS

In this section we present the channel models of the ICC based on the models introduced in [1].

Definition 1: Let $\mathcal{C}$ denotes a discrete memoryless interference channel consists of finite alphabets $(\mathcal{X}_1, \mathcal{X}_2, \mathcal{Y}_1, \mathcal{Y}_2)$ where $\mathcal{X}_t$ and $\mathcal{Y}_t$, $t = 1, 2$, denote channel input and output respectively and $\mathcal{P}$ denotes the collection of the conditional probapilities $p(y_1, y_2|x_1, x_2)$ on $(\mathrm{y}_1, \mathrm{y}_2) \in \mathcal{Y}_1 \times \mathcal{Y}_2$ given $(x_1, x_2) \in \mathcal{X}_1 \times \mathcal{X}_2$. The channel is memoryless and for n channel uses, we have

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

where $\mathbf{x}_\mathrm{t} = (x_{t1}, \dots, x_{tn}) \in \mathcal{X}_t^n$ and $\mathbf{y}_\mathrm{t} = (y_{t1}, \dots, y_{tn}) \in \mathcal{Y}_t^n$ for $t = 1, 2$. The marginal distribution of y_t given by

$$p_t(y_\mathrm{t}|x_1, x_2) = \sum_{y_{\tilde{\mathrm{t}}} \in \mathcal{Y}_{\tilde{\mathrm{t}}}} p_t(y_\mathrm{t}, y_{\tilde{\mathrm{t}}}|x_1, x_2) \qquad (2)$$

where t is one of the numbers 1 or 2 and $\tilde{t}$ is the other one.

In this scenario each sender has a private message $w_t \in \mathcal{M}_t\{1, 2, \dots, M_t\}$ with a common message $w_0 \in \mathcal{M}_0\{1, 2, \dots, M_0\}$, $t = 1, 2$. All these messages are assumed to be independent and uniformly generated over their respective ranges.

Definition 2: An (M_0, M_1, M_2, P_e, n) code exists for the channel $\mathcal{C}$, if and only if there exist two coding and two decoding functions in which

$$f_t: \mathcal{M}_0 \times \mathcal{M}_t \to \mathcal{X}_t^n \quad (3)$$

$$g_t: \mathcal{Y}_t^n \to \mathcal{M}_0 \times \mathcal{M}_t \quad (4)$$

Such that $max\left\{P_{e,t}^{(n)}\right\} \le P_e$ for $t = 1,2$, where $P_{e,t}^{(n)}$ denotes the average decoding error probability of decoder t, and is computed as follows

$$P_{e,t}^{(n)} = \frac{1}{M_0 M_1 M_2} \sum_{M_0 M_1 M_2} p((\hat{w}_0, \hat{w}_t) \neq (w_0, w_t) | (w_0, w_{1,}, w_2)) \quad (5)$$

Definition 3: A nonnegative rate quintuple $(R_0, R_1, R_2, R_{e1}, R_{e2})$ is said to be achievable for cannel $\mathcal{C}$ if for any given $0 < P_e < 1$, and for sufficiently large$n$, there exist message sets $\mathcal{M}_0, \mathcal{M}_1, \mathcal{M}_2$ and encoders-decoders (f_1, f_2, g_1, g_2), where

$$R_{e1}^{(n)} \le lim_{n\to\infty} \frac{1}{n} H(W_1|Y_2^n) \quad (6)$$

$$R_{e2}^{(n)} \le lim_{n\to\infty} \frac{1}{n} H(W_2|Y_1^n) \quad (7)$$

The rate-equivocation region for ICC channel is closure of the union of all the achievable rate quintuples $(R_0, R_1, R_2, R_{e1}, R_{e2})$.

3. MAIN RESULTS

We first introduce an achievable rate-equivocation region for the ICC in the following lemma.

Theorem 1: Let $\mathcal{R}(p)$ denotes the set of all nonnegative rate tuple $(R_0, R_{11}, R_{12}, R_{21}, R_{22}, R_{e1}, R_{e2})$ and three auxiliary random variables U_0, U_1 and U_2 are defined over arbitrary finite sets $\mathcal{U}_0$, $\mathcal{U}_1$ and $\mathcal{U}_2$, respectively. The following region is achievable for the ICC with two confidential messages:

$$\mathfrak{R}^{II} = Conv \bigcup_{P(u_0)P(u_1|u_0)P(u_2|u_0)P(x_1|u_0u_1)P(x_2|u_0u_2)P(y_1y_2|x_1x_2)} \left\{ \begin{array}{c} (R_0, R_{11}, R_{12}, R_{21}, R_{22}, R_{e1}, R_{e2}): \\ R_0 \ge 0, R_{11} \ge 0, R_{12} \ge 0, R_{21} \ge 0, R_{22} \ge 0 \\ R_{11} \le I(X_1; Y_1|U_0U_1U_2), \\ R_{11} + R_{12} \le I(X_1; Y_1|U_0U_2), \\ R_{11} + R_{21} \le I(X_1U_2; Y_1|U_0U_1), \\ R_{11} + R_{12} + R_{21} \le I(X_1U_2; Y_1|U_0), \\ R_0 + R_{11} + R_{12} + R_{21} \le I(U_0X_1U_2; Y_1), \\ R_{22} \le I(X_2; Y_2|U_0U_1U_2), \\ R_{21} + R_{22} \le I(X_2; Y_2|U_0U_2), \\ R_{21} + R_{22} \le I(X_2U_1; Y_2|U_0U_1), \\ R_{21} + R_{12} + R_{22} \le I(X_2U_1; Y_2|U_0), \\ R_0 + R_{22} + R_{12} + R_{21} \le I(U_0X_2U_1; Y_2), \\ (R_{e1}, R_{e2}) \in \mathfrak{S}_e(R_0, R_{11}, R_{12}, R_{21}, R_{22}) \end{array} \right\} \quad (8)$$

where $Conv(\mathfrak{R})$ indicates the convex hull of the region $\mathfrak{R}$, and

$$\mathfrak{S}_e(R_0, R_{11}, R_{12}, R_{21}, R_{22}) = \bigcup_{(R'_{11}, R'_{12}, R'_{21}, R'_{22}) \in \mathcal{A}(R_0, R_{11}, R_{12}, R_{21}, R_{22})}$$

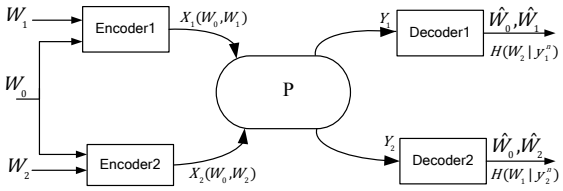

Fig. 1. The interference channel with common message and two confidential messages.

$$\left\{ \begin{array}{c} (R_{e1}, R_{e2}): \\ 0 \le R_{e1} \le R_{11} \\ R_{e1} \le [R'_{11} - I(Y_2; X_1|U_1X_2)]^+ \\ 0 \le R_{e2} \le R_{21} \\ R_{e2} \le [R'_{22} - I(Y_1; X_2|U_2X_1)]^+ \end{array} \right\} \quad (9)$$

where $[x]^+ = max\{x, 0\}$, and

$$\mathcal{A}(R_0, R_{11}, R_{12}, R_{21}, R_{22}) = \left\{(R'_{11}, R'_{12}, R'_{21}, R'_{22}): (R'_{11}, R'_{12}, R'_{21}, R'_{22}) \in \mathcal{C}_{ICC}^p, R_{11} \le R'_{11}, R_{12} \le R'_{12}, R_{21} \le R'_{21}, R_{22} \le R'_{22}\right\} \quad (10)$$

where $\mathcal{C}_{ICC}^p$ is defined as

$$\mathcal{C}_{ICC}^p = \left\{ \begin{array}{c} (R_0, R_{11}, R_{12}, R_{21}, R_{22}): \\ R_0 \ge 0, R_{11} \ge 0, R_{12} \ge 0, R_{21} \ge 0, R_{22} \ge 0 \\ R_{11} \le I(X_1; Y_1|U_0U_1U_2), \\ R_{11} + R_{12} \le I(X_1; Y_1|U_0U_2), \\ R_{11} + R_{21} \le I(X_1U_2; Y_1|U_0U_1), \\ R_{11} + R_{12} + R_{21} \le I(X_1U_2; Y_1|U_0), \\ R_0 + R_{11} + R_{12} + R_{21} \le I(U_0X_1U_2; Y_1), \\ R_{22} \le I(X_2; Y_2|U_0U_1U_2), \\ R_{21} + R_{22} \le I(X_2; Y_2|U_0U_1), \\ R_{21} + R_{22} \le I(X_2U_1; Y_2|U_0U_2), \\ R_{21} + R_{12} + R_{22} \le I(X_2U_1; Y_2|U_0), \\ R_0 + R_{22} + R_{12} + R_{21} \le I(U_0X_2U_1; Y_2) \end{array} \right\} \quad (11)$$

for some fixed joint probability distribution $p(.)$ that factor as

$$p(u_0, u_1, u_2, x_1, x_2, y_1, y_2) = p(u_0)p(u_1|u_0)p(u_2|u_0)p(x_1|u_0u_1) p(x_2|u_0u_2)p(y_1, y_2|x_1, x_2) \quad (12)$$

Remark 1: The details of the proof and computation of the equivocation rates are relegated to Appendix A. We delineate the proof in the following. The main idea of the proof was derived in [1], where the achievable rate region for ICC without secrecy was obtained.

Remark 2: The intuitive interpretation of the rate–equivocation region in Theorem 1 is like the description which is taken in [4, Thm 1].

Corollary 1: The rate region of the ICC without secrecy reduces to the rate region introduced in [1]. In the introduced region, by renunciation of the equivocation rates, region of [1] is obtained.

Corollary 2: As a minor result, in this bound by letting $R_1 = \emptyset$, $U_1 = X_1$ and $R_{e1} = \emptyset$, the rate-equivocation region for cognitive radio introduced in [2] is obtained.

Theorem 2: The set $\mathfrak{S}_e(R_0, R_{11}, R_{12}, R_{21}, R_{22})$ in (9) can be expressed in the following form:

$$\mathfrak{S}_e(R_0, R_{11}, R_{12}, R_{21}, R_{22}) = \mathcal{L}_1(R_0, R_{11}, R_{12}, R_{21}, R_{22}) \cup \mathcal{L}_2(R_0, R_{11}, R_{12}, R_{21}, R_{22}) \cup \mathcal{L}_3(R_0, R_{11}, R_{12}, R_{21}, R_{22}) \quad (13)$$

where $\mathcal{L}_1$, $\mathcal{L}_2$ and $\mathcal{L}_3$ are defined in (14)-(16) in the following of the page.

Theorem 3: The nonnegative rate quintuple $(R_0, R_1, R_2, R_{e1}, R_{e2})$ satisfying

$$R_{e1} \le R_1 \quad (17)$$

$$R_{e2} \le R_2 \quad (18)$$

$$R_0 \le min\{I(U;Y_1), I(U;Y_2)\} \quad (19)$$

$$R_0 + R_1 \le I(V_1;Y_1|U) + min\{I(U;Y_1), I(U;Y_2)\} \quad (20)$$

$$R_0 + R_2 \le I(V_2;Y_2|U) + min\{I(U;Y_1), I(U;Y_2)\} \quad (21)$$

$$R_0 + R_1 + R_2 \le I(V_1;Y_1|U) + I(V_2;Y_2|V_1U) + min\{I(U;Y_1), I(U;Y_2)\} \quad (22)$$

$$R_0 + R_1 + R_2 \le I(V_1;Y_1|V_2U) + I(V_2;Y_2|U) + min\{I(U;Y_1), I(U;Y_2)\} \quad (23)$$

$$R_{e1} \le \begin{Bmatrix} [I(V_1;Y_1|U) - I(V_1;Y_2|U)]^+ \\ [I(V_1;Y_1|V_2U) - I(V_1;Y_2|V_2U)]^+ \end{Bmatrix} \quad (24)$$

$$R_{e1} \le \begin{Bmatrix} [I(V_2;Y_2|U) - I(V_2;Y_1|U)]^+ \\ [I(V_2;Y_2|V_1U) - I(V_2;Y_1|V_1U)]^+ \end{Bmatrix} \quad (25)$$

over all the distributions $p(.)$ that factors as (12), is an outer bound for the ICC.

Proof: See Appendix B.

Remark 3: We consider that (19)-(23) have been driven in [5] as the outer bound for the broadcast channel. The difference is the factorization of $p(.)$. The equivocation-rates are proved in Appendix B.

CONCLUSIONS

In this paper we considered the interference channel with common message and two confidential messages. We have shown that our derived achievable rate region reduces to the one for ICC without confidential messages established in [1]. On the other hand, we have shown that our region reduces to the one in [2] for the cognitive interference channel with secrecy. Moreover, the outer bound for this channel was derived.

$$\mathcal{L}_1(R_0, R_{11}, R_{12}, R_{21}, R_{22}) = \left\{ \begin{array}{c} (R_{e1}, R_{e2}): \\ 0 \le R_{e1} \le R_{11} \\ 0 \le R_{e2} \le R_{21} \\ R_{e1} \le [I(X_1;Y_1|U_0U_1U_2) - I(Y_2;X_1|U_1X_2)]^+ \\ R_{e1} \le [I(X_1;Y_1|U_0U_2) - R_{12} - I(Y_2;X_1|U_1X_2)]^+ \\ R_{e1} \le [I(X_1U_2;Y_1|U_0U_1) - R_{21} - I(Y_2;X_1|U_1X_2)]^+ \\ R_{e1} \le [I(X_1U_2;Y_1|U_0) - R_{12} - R_{21} - I(Y_2;X_1|U_1X_2)]^+ \\ R_{e1} \le [I(U_0X_1U_2;Y_1) - R_0 - R_{12} - R_{21} - I(Y_2;X_1|U_1X_2)]^+ \\ R_{e2} \le [I(X_2;Y_2|U_0U_1U_2) - I(Y_1;X_2|U_2X_1)]^+ \\ R_{e2} \le [I(X_2;Y_2|U_0U_1) - R_{21} - I(Y_1;X_2|U_2X_1)]^+ \\ R_{e2} \le [I(X_2U_1;Y_2|U_0U_2) - R_{12} - I(Y_1;X_2|U_2X_1)]^+ \\ R_{e2} \le [I(X_2U_1;Y_2|U_0) - R_{12} - R_{21} - I(Y_1;X_2|U_2X_1)]^+ \\ R_{e2} \le [I(U_0X_2U_1;Y_2) - R_0 - R_{12} - R_{21} - I(Y_1;X_2|U_2X_1)]^+ \end{array} \right\} \quad (14)$$

$$\mathcal{L}_2(R_0, R_{11}, R_{12}, R_{21}, R_{22}) = \left\{ \begin{array}{c} (R_{e1}, R_{e2}): \\ 0 \le R_{e1} \le R_{11} + R_{12} \\ R_{e1} \le [I(X_1;Y_1|U_0U_1U_2) - I(Y_2;X_1|U_1X_2)]^+ \\ R_{e1} \le [I(X_1;Y_1|U_0U_2) - R_{12} - I(Y_2;X_1|U_1X_2)]^+ \\ R_{e1} \le [I(X_1U_2;Y_1|U_0U_1) - R_{21} - I(Y_2;X_1|U_1X_2)]^+ \\ R_{e1} \le [I(X_1U_2;Y_1|U_0) - R_{12} - R_{21} - I(Y_2;X_1|U_1X_2)]^+ \\ R_{e1} \le [I(U_0X_1U_2;Y_1) - R_0 - R_{12} - R_{21} - I(Y_2;X_1|U_1X_2)]^+ \\ R_{e2} = 0 \end{array} \right\} \quad (15)$$

$$\mathcal{L}_3(R_0, R_{11}, R_{12}, R_{21}, R_{22}) = \left\{ \begin{array}{c} (R_{e1}, R_{e2}): \\ R_{e1} = 0 \\ 0 \le R_{e2} \le R_{21} + R_{22} \\ R_{e2} \le [I(X_2;Y_2|U_0U_1U_2) - I(Y_1;X_2|U_2X_1)]^+ \\ R_{e2} \le [I(X_2;Y_2|U_0U_1) - R_{21} - I(Y_1;X_2|U_2X_1)]^+ \\ R_{e2} \le [I(X_2U_1;Y_2|U_0U_2) - R_{12} - I(Y_1;X_2|U_2X_1)]^+ \\ R_{e2} \le [I(X_2U_1;Y_2|U_0) - R_{12} - R_{21} - I(Y_1;X_2|U_2X_1)]^+ \\ R_{e2} \le [I(U_0X_2U_1;Y_2) - R_0 - R_{12} - R_{21} - I(Y_1;X_2|U_2X_1)]^+ \end{array} \right\} \quad (16)$$

APPENDIX A

Our equivocation rate region introduced in *Theorem 1* is established on the one of [1]. First, we introduce our code construction like [1].

CodeBook Generation: For fixed distribution $p(.)$ that factors as (12), with rate splitting we have

$$\begin{aligned} W_0 &\in \{1,\cdots,2^{nR_0}\} \\ W_{12} &\in \{1,\cdots,2^{nR_{12}}\} \\ W_{11} &\in \{1,\cdots,2^{nR_{11}}\} \\ W_{21} &\in \{1,\cdots,2^{nR_{21}}\} \\ W_{22} &\in \{1,\cdots,2^{nR_{22}}\} \end{aligned} \tag{26}$$

where $R_{12}+R_{11}=R_1$ and $R_{21}+R_{22}=R_2$. Now we consider the following codebook:

$$\mathbb{C}=\begin{cases} \mathbf{u}_0(i) & i\in\{1,\dots,2^{nR_0}\} \\ \mathbf{u}_1(i,j) & j\in\{1,2,\dots,2^{nR_{12}}\} \\ \mathbf{u}_2(i,l) & l\in\{1,2,\dots,2^{nR_{21}}\} \\ \mathbf{x}_1(i,j,a,b) & a\in\{1,2,\dots,A\}, b\in\{1,2,\dots,B\} \\ \mathbf{x}_2(i,l,c,d) & c\in\{1,2,\dots,C\}, d\in\{1,2,\dots,D\} \end{cases} \tag{27}$$

where all code words are strongly typical, i.e.,

$$\begin{aligned} &\mathbf{u}_0(i)\in T_\epsilon^n\left(P_{U_0}\right), \\ &\mathbf{u}_1(i,j)\in T_\epsilon^n\left(P_{U_1|U_0}|\mathbf{u}_0(i)\right), \\ &\mathbf{u}_2(i,l)\in T_\epsilon^n\left(P_{U_2|U_0}|\mathbf{u}_0(i)\right), \\ &\mathbf{x}_1(i,j,a,b)\in T_\epsilon^n\left(P_{X_1|U_0U_1}|\mathbf{u}_0(i),\mathbf{u}_1(i,j)\right), \\ &\mathbf{x}_2(i,l,c,d)\in \mathrm{T}_\epsilon^{\mathrm{n}}\left(\mathrm{P}_{\mathrm{X}_2|\mathrm{U}_0\mathrm{U}_2}|\mathbf{u}_0(\mathrm{i}),\mathbf{u}_2(\mathrm{i,l})\right), \end{aligned} \tag{28}$$

for all i, j, l, a, b, c, d, where $T_\epsilon^{(n)}$ denotes the typical sets of the respective joint distributions, and

$$\begin{aligned} \frac{1}{n}\log A &= R'_{11}-I(X_1;Y_2|U_1,X_2) \\ \frac{1}{n}\log B &= I\left(X_1;Y_2|U_1,X_2\right) \\ \frac{1}{n}\log C &= R'_{22}-I(X_2;Y_1|U_2,X_1) \\ \frac{1}{n}\log D &= I(X_2;Y_1|U_2,X_1) \end{aligned} \tag{29}$$

Encoding: In the following we consider the case in which $R'_{11}\geq\frac{1}{n}\log A$ and $R'_{22}\geq\frac{1}{n}\log C$ and compute the equivocation rate for this case, then we derive the other case similarly. First we define the following sets

$$\begin{aligned} &\mathcal{A}=\{1,2,\dots,A\},\mathcal{B}=\{1,2,\dots,B\}, \\ &\mathcal{C}=\{1,2,\dots,C\},\mathcal{D}=\{1,2,\dots,D\}, \end{aligned} \tag{30}$$

where A, B, C and D are defined in (29). We let

$$\begin{aligned} \mathcal{W}_{11} &= \mathcal{A}\times\mathcal{S} \\ \mathcal{W}_{22} &= \mathcal{C}\times\mathcal{T} \end{aligned} \tag{31}$$

where $\mathcal{S}=\{1,2,\dots,S\}$ and $\mathcal{T}=\{1,2,\dots,T\}$ and

$$\begin{aligned} \frac{1}{n}\log S &= R_{11}-\frac{1}{n}logA \\ \frac{1}{n}\log T &= R_{22}-\frac{1}{n}logC \end{aligned} \tag{32}$$

We define

$$\begin{aligned} f&:\mathcal{B}\longrightarrow\mathcal{S} \\ g&:\mathcal{D}\longrightarrow\mathcal{T} \end{aligned}$$

where mapping f is partitioning $\mathcal{B}$ into $\mathcal{S}$ subsets and mapping g is partitioning $\mathcal{D}$ into $\mathcal{T}$ subsets. Both these functions are nearly equal size, i.e.

$$\begin{aligned} \|f^{-1}(s_1)\|\leq 2\|f^{-1}(s_2)\|, &\qquad \forall s_1,s_2\in\mathcal{S} \\ \|g^{-1}(t_1)\|\leq 2\|g^{-1}(t_2)\|, &\qquad \forall t_1,t_2\in\mathcal{T} \end{aligned}$$

Now we generate source messages in both senders. By using $W_{11}=(a,s)\longrightarrow(a,b)$ and $W_{22}=(c,t)\longrightarrow(c,d)$ where b and d are chosen randomly from the sets $f^{-1}(s)\subset\mathcal{B}$ and $g^{-1}(t)\subset\mathcal{D}$ respectively, sender 1 transmits $\mathbf{x}_1(i,j,a,b)$ and sender 2 transmits $\mathbf{x}_2(i,l,c,d)$ and transmissions are assumed synchronized.

Decoding: Each receiver receives an n-length channel output sequence, $\mathbf{y}_1$ and $\mathbf{y}_2$ for receiver 1 and 2 respectively. Decoder 1 declares $\left(\hat{\imath},\hat{\jmath},\hat{a},\hat{b}\right)$ which is the unique triple that satisfy $\left(\mathbf{u}_0(\hat{\imath}),\mathbf{u}_1(\hat{\imath},\hat{\jmath}),\mathbf{u}_2(\hat{\imath},l),\mathbf{x}_1\left(\hat{\imath},\hat{\jmath},\hat{a},\hat{b}\right),\mathbf{y}_1\right)\in T_\epsilon^{(n)}$ for some l. Similarly the decoder 2 declares $\left(\hat{\imath},\hat{l},\hat{m}\right)$ which is the unique triple that satisfies $\left(\mathbf{u}_0(\hat{\imath}),\ \mathbf{u}_1(\hat{\imath},j),\ \mathbf{u}_2\left(\hat{\imath},\hat{l}\right),\ \mathbf{x}_2\left(\hat{\imath},\hat{l},\hat{c},\hat{d}\right),\ \mathbf{y}_2\right)\in T_\epsilon^{(n)}$ for some j.

Otherwise, an error was notified.

Equivocation: Now, we prove the bound on equivocation-rates.

$$\begin{aligned} &H(W_{21},W_{22}|Y_1^n)\overset{(a)}{\geq}H(W_{22}|Y_1^n,W_1,U_0^n,W_{21}) \\ &=H(W_{22},Y_1^n|W_1,U_0^n,W_{21})-H(Y_1^n|W_1,U_0^n,W_{21}) \\ &=H(W_{22},Y_1^n,X_2^n|W_1,U_0^n,W_{21}) \\ &-H(X_2^n|W_1,U_0^n,W_{21},W_{22},Y_1^n)-H(Y_1^n|W_1,U_0^n,W_{21}) \\ &=H(W_{22},X_2^n|W_1,U_0^n,W_{21})+H(Y_1^n|W_1,U_0^n,W_2,X_2^n) \\ &-H(X_2^n|W_1,U_0^n,W_{21},W_{22},Y_1^n)-H(Y_1^n|W_1,U_0^n,W_{21}) \\ &\overset{(b)}{\geq}H(X_2^n|W_1,U_0^n,W_{21})+H(Y_1^n|U_0^n,U_1^n,U_2^n,X_1^n,X_2^n) \\ &-H(X_2^n|W_1,U_0^n,W_{21},W_{22},Y_1^n)-H(Y_1^n|W_1,U_0^n,W_{21}) \end{aligned} \tag{33}$$

where (a) follows from the fact that conditioning does not increase the entropy and (b) is because that Y_1^n is independent of (W_1,W_2) given $(U_0^nU_1^n,U_2^n,X_1^n,X_2^n)$.

Now, we consider each term in (33). To compute the first term, just like [7], we have:

Lemma 1: consider a discrete random variable X taking values in $\{x_1,\dots,x_m\}$ and the probability mass function satisfying

$$\frac{P_X(x_i)}{P_X(x_j)} \leq 2^{\delta} \text{ for } \delta \geq 1, \quad \forall i,j \in [1,\dots,m] \tag{34}$$

Then

$$H(X) \geq \log m - \delta \tag{35}$$

For the first term in (33), by using (35) we have

$$\frac{P_{x_2^n}(x_2^n)}{P_{x_2^n}(\bar{x}_2^n)} \leq 2, \ \forall x_2^n, \bar{x}_2^n \epsilon \{x_2^n\} \tag{36}$$

So we obtain

$$\frac{1}{n}H(X_2^n|U_0^n,W_1,W_{21}) =^{(c)} \frac{1}{n}H(X_2^n|U_0^n,W_{21}) \geq \frac{1}{n}\log C + \frac{1}{n}logD - \frac{1}{n} = R'_{22} - \frac{1}{n} \tag{37}$$

where (c) is because of the fact that X_2 is independent of W_1. For the second and the third terms in (33), using the approach taken in [2], we have

$$\frac{1}{n}H(Y_1^n|U_0^n,U_1^n,U_2^n,X_1^n,X_2^n) \geq H(Y|U_0,U_1,U_2,X_1,X_2) \tag{38}$$

For the third term of (33) following same approach as that in Lemma 3 of [6], using Fano's inequality we have

$$\frac{1}{n}H(X_2^n|U_0^n,Y_1^n,W_1,W_{21},W_{22}) < \epsilon \tag{39}$$

To compute the forth term in (33), first we define

$$\hat{Y}_1^n = \begin{cases} Y_1^n & if\ (\mathbf{u}_0,\ \mathbf{u}_1,\ \mathbf{u}_2,\ \mathbf{x}_2,\ \mathbf{y}_2) \in T_{\epsilon}^{(n)} \\ Z^n & else \end{cases}$$

where Z^n is an arbitrary sequence that is constructed in Y_1^n. Now we have

$$\begin{aligned}
&\frac{1}{n}H(Y_1^n|W_1,W_{21},U_0^n) \\
&= \frac{1}{n}\sum_{W_1,W_{21}} \Pr\{W_1=\omega_1,W_{21}=\omega_{21}\}H(Y_1^n|W_1=\omega_1,W_{21}=\omega_{21},U_0^n) \\
&\leq \frac{1}{n}\sum_{W_1,W_{21}} \Pr\{W_1=\omega_1,W_{21}=\omega_{21}\}H(\hat{Y}_1^n,Y_1^n|W_1=\omega_1,W_{21}=\omega_{21},U_0^n) \\
&= \frac{1}{n}\sum_{W_1,W_{21}} \Pr\{W_1=\omega_1,W_{21}=\omega_{21}\}\times \\
&\left(H(\hat{Y}_1^n|W_1=\omega_1,W_{21}=\omega_{21},U_0^n)+H(Y_1^n|W_1=\omega_1,W_{21}=\omega_{21},U_0^n)\right)
\end{aligned} \tag{40}$$

For the first term in (40) we can write

$$\begin{aligned}
&\frac{1}{n}\sum_{W_1,W_{21}} \Pr\{W_1=\omega_1,W_{21}=\omega_{21}\}H(\hat{Y}_1^n|W_1=\omega_1,W_{21}=\omega_{21},U_0^n) \\
&\leq \frac{1}{n}\sum_{W_1,W_{21}} \Pr\{W_1=\omega_1,W_{21}=\omega_{21}\}\times\log\left\|T_{\varepsilon}^{(n)}(P_{Y_1|U_0U_1U_2X_1}|U_0^nU_1^nU_2^nX_1^n)\right\| \\
&\leq \frac{1}{n}\sum_{W_1,W_{21}} \Pr\{W_1=\omega_1,W_{21}=\omega_{21}\}H(Y_1|U_0U_1U_2X_1) \\
&\leq H(Y_1|U_0U_1U_2X_1)+\varepsilon
\end{aligned} \tag{41}$$

To bound the second term in (40) we use the Fano's inequality and obtain

$$\begin{aligned}
&\frac{1}{n}\sum_{W_1,W_{21}} \Pr\{W_1=\omega_1,W_{21}=\omega_{21}\}H(Y_1^n|W_1=\omega_1,W_{21}=\omega_{21},U_0^n,\hat{Y}_1^n) \\
&\leq \frac{1}{n}\sum_{W_1,W_{21}} \Pr\{W_1=\omega_1,W_{21}=\omega_{21}\} \\
&\times\left(1+\Pr\{\hat{Y}_1^n \neq Y_1^n|W_1=\omega_1,W_{21}=\omega_{21},U_0^n\}\log|Y|^n\right) \\
&\frac{1}{n}+\sum_{W_1,W_{21}} \Pr\{W_1=\omega_1,W_{21}=\omega_{21}\} \\
&\times\left(1+\Pr\left\{\left(U_0^n,U_1^n,U_2^n,X_1^n,Y_1^n\right)\notin T_{\varepsilon}^{(n)}\right\}\log|Y|\right) \leq \varepsilon
\end{aligned} \tag{42}$$

Hence (40) is bounded as

$$\frac{1}{n}H(Y_1^n|W_1,W_{21},U_0^n) \leq H(Y_1|U_0U_1U_2X_1)+\varepsilon \tag{43}$$

in which ε is negligible for sufficiently large n. Substituting (37), (38), (39) and (43) in (33) we obtain

$$H(W_{21},W_{22}|Y_1^n) \geq R'_{22} - \frac{1}{n} + H(Y_1|U_0,U_1,U_2,X_1,X_2) - H(Y_1|U_0,U_1,U_2,X_1) = R'_{22} - I(Y_1;X_2|U_2,X_1) - \frac{1}{n} \tag{44}$$

By the definition of R_{e2} , we conclude

$$R_{e2} \leq R'_{22} - I(Y_1;X_2|U_2,X_1) \tag{45}$$

■

APPENDIX B

In this section we prove Theorem 3. From the Fano's Lemma we have

$$H(W_0W_1|Y_1^n) \leq n\delta_n \tag{46}$$

$$H(W_0W_2|Y_2^n) \leq n\delta_n \tag{47}$$

Now we check the bounds. First we consider R_0, following the approach taken in [5]

$$\begin{aligned}
nR_0 &= H(W_0) = I(W_0;Y_1^n) + H(W_0|Y_1^n) \\
&\leq \sum_{i=1}^n I\left(W_0;Y_{1i}|Y_1^{i-1}\right) + n\delta_n \\
&= \sum_{i=1}^n I\left(W_0Y_1^{i-1};Y_{1i}\right) - I\left(Y_1^{i-1};Y_{1i}\right) + n\delta_n \\
&\leq \sum_{i=1}^n \left[I\left(W_0Y_1^{i-1}\tilde{Y}_2^{i+1};Y_{1i}\right) - I\left(\tilde{Y}_2^{i+1};Y_{1i}|W_0Y_1^{i-1}\right)\right] + n\delta_n \\
&\leq \sum_{i=1}^n I\left(W_0Y_1^{i-1}\tilde{Y}_2^{i+1};Y_{1i}\right) + n\delta_n
\end{aligned} \tag{48}$$

Similarly we can obtain

$$nR_0 \leq \sum_{i=1}^n I\left(W_0Y_1^{i-1}\tilde{Y}_2^{i+1};Y_{2i}\right) + n\delta_n \tag{49}$$

For the some rate bounds $R_0 + R_1$ we have

$$\begin{aligned}
n(R_0+R_1) &= H(W_0W_1) \\
&= H(W_0) + I(W_1;Y_1^n|W_0) + H(W_1|Y_1^nW_0) \\
&\quad + H(W_1|Y_1^nW_0) \\
&\leq H(W_0) + I(W_1;Y_1^n|W_0) + n\delta_n
\end{aligned} \tag{50}$$

For the second term in (50) we can write

$$I(W_1; Y_1^n|W_0) = \sum_{i=1}^n I\left(W_1; Y_{1i}|Y_1^{i-1}W_0\right)$$

$$= \sum_{i=1}^n \left[I\left(W_1\tilde{Y}_2^{i+1}; Y_{1i}|Y_1^{i-1}W_0\right) - I\left(\tilde{Y}_2^{i+1}; Y_{1i}|Y_1^{i-1}W_0W_1\right)\right]$$

$$\leq \sum_{i=1}^n I\left(W_1; Y_{1i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0\right) + n\delta_n \quad (51)$$

From (50) and (51) we have

$$n(R_0 + R_1) \leq \sum_{i=1}^n I\left(W_0Y_1^{i-1}\tilde{Y}_2^{i+1}; Y_{1i}\right) + \sum_{i=1}^n I\left(W_1; Y_{1i}|W_0Y_1^{i-1}\tilde{Y}_2^{i+1}\right) + 2n\delta_n \quad (52)$$

Similarly we have

$$n(R_0 + R_1) \leq \sum_{i=1}^n I\left(W_0Y_1^{i-1}\tilde{Y}_2^{i+1}; Y_{2i}\right) + \sum_{i=1}^n I\left(W_1; Y_{1i}|W_0Y_1^{i-1}\tilde{Y}_2^{i+1}\right) + 2n\delta_n \quad (53)$$

So (20) is proved. The bounds in (21) are obtained similarly.

Considering sum rate bounds $R_0 + R_1 + R_2$, we have

$$n(R_0 + R_1 + R_2)$$
$$= H(W_0W_1) + I(W_2; Y_2^n|W_1W_0) + H(W_2|Y_2^nW_1W_0)$$
$$\leq H(W_0W_1) + I(W_2; Y_2^n|W_1W_0) + n\delta_n \quad (54)$$

$$n(R_0 + R_1 + R_2)$$
$$= H(W_0W_2) + I(W_1; Y_1^n|W_2W_0) + H(W_1|Y_1^nW_2W_0)$$
$$\leq H(W_0W_2) + I(W_1; Y_1^n|W_2W_0) + n\delta_n \quad (55)$$

Similarly as previous bounds, we can obtain

$$I(W_1; Y_1^n|W_2W_0) \leq \sum_{i=1}^n I\left(W_1; Y_{1i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0W_1\right) \quad (56)$$

$$I(W_2; Y_2^n|W_1W_0) \leq \sum_{i=1}^n I\left(W_2; Y_{2i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0W_2\right) \quad (57)$$

Combining (54)-(57), (22) and (23) are obtained. For the equivocation rate bounds we have

$$R_{e1} \leq H(W_1|Y_2^n) = H(W_1|Y_2^nW_0) + I(W_0; W_1|Y_2^n) \leq I(W_1; Y_1^n|W_0) - I(W_1; Y_2^n|W_0) + H(W_1|Y_1^nW_0) + H(W_0W_2|Y_2^n) \leq I(W_1; Y_1^n|W_0) - I(W_1; Y_2^n|W_0) + 2\delta_n \quad (58)$$

$$R_{e1} \leq H(W_1|Y_2^n)$$
$$= H(W_1|Y_2^nW_0W_2) + I(W_0; W_1|Y_2^nW_2)$$
$$\leq I(W_1; Y_1^n|W_0W_2) - I(W_1; Y_2^n|W_0W_2) + H(W_1|Y_1^nW_0W_2) + H(W_0W_2|Y_2^n)$$
$$\leq I(W_1; Y_1^n|W_0W_2) - I(W_1; Y_2^n|W_0W_2) + 2\delta_n \quad (59)$$

For the second term in (59) we have

$$I(W_1; Y_2^n|W_0W_2) \leq \sum_{i=1}^n I\left(W_1; Y_{2i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0W_2\right) \quad (60)$$

$$I(W_1; Y_2^n|W_0) \leq \sum_{i=1}^n I\left(W_1; Y_{2i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0\right) \quad (61)$$

Therefore we obtain

$$R_{e1} \leq \sum_{i=1}^n I\left(W_1; Y_{1i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0\right) - \sum_{i=1}^n I\left(W_1; Y_{2i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0\right) + 2n\delta_n \quad (62)$$

$$R_{e1} \leq \sum_{i=1}^n I\left(W_1; Y_{1i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0W_2\right) - \sum_{i=1}^n I\left(W_1; Y_{2i}|Y_1^{i-1}\tilde{Y}_2^{i+1}W_0W_2\right) + 2n\delta_n \quad (63)$$

By defining the following auxiliary random variables (19)-(25) are obtained where Q is a random variable uniformly distributed over $\{1, \dots, n\}$, independent of $W_0, W_1, W_2, X_1^n, X_2^n, Y_1^n, Y_2^n$

$$U_i \triangleq W_0Y_1^{i-1}\tilde{Y}_2^{i+1}Q \quad (63)$$

$$V_1 \triangleq W_1U, V_2 \triangleq W_2U$$

$$Y_1 \triangleq Y_{1Q}, Y_2 \triangleq Y_{1Q} \quad (64)$$

■

4. REFERENCES

[1] J. Jiang, Y. Xin, and H. K. Garg, "Interference channels with common information," *IEEE Trans. Inf. Theory,* vol. 54, no. 1, pp. 171–187, Jan. 2008.

[2] Yingbin Liang, Anelia Somekh-Baruch, H. Vincent Poor, Shlomo Shamai (Shitz) and Sergio Verdú, "Capacity of Cognitive Interference channels with and without secrecy," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 604-618, Feb 2009.

[3] H. H. Tan, "Two-user interference channels with correlated information sources," *Inf. Contr.*, vol. 44, no. 1, pp. 77–104, 1980.

[4] Yingbin Liang, H. Vincent Poor," Multiple-Access Channels With Confidential Messages," *IEEE Trans. Inf. Theory,* vol. 54, no. 3, March 2008.

[5] Jin Xu, Yi Cao and Biao Chen, "Capacity Bound for Broadcast Channel With Confidential Messages," *IEEE Trans. Inf. Theory,* vol. 55, No. 10, Oct. 2009.

[6] R. Liu, I. Maric, P. Spasojevic, and R. D. 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.

[7] Csisz´ar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. on Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[8] E. Shannon, "Two-way communication channels," in *Proc. 4th. Berkeley Symp. Math. Stat. Prob.*, Berkeley, CA, 1961, vol. 1, pp. 611–644.

[9] Aydano B. Carleial, " Interference Channels," *IEEE Trans. Inf. Theory*, vol. IT-24, No. 1, Jan. 1978.

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

[11] H. F. Chong, M. Motani, H. K. Garg, and H. El Gamal, "On simplification of the Han–Kobayashi rate region for the interference channel," submitted for publication *IEEE Trans. Inf. Theory*.

[12] G. Kramer, "Review of rate regions for interference channels," in *Proc. Int. Zurich Seminar on Communications*, Zurich, Switzerland, Feb. 2006, pp. 162–165.

[13] E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–714, 1949.

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

[15] Csisz´ar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. on Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[16] Maric, A. Goldsmith, G. Kramer, and S. Shamai (Shitz), "On the capacity of interference channels with a cognitive transmitter," in *Proc. of Workshop Inf. Theory Appl.*, (UCSD, La Jolla, CA), Jan. Feb. 2007.