Secrecy Rate Region in the Interference Channel with Common Information

Hamid G. Bafghi*, Somayeh Salimi†, Babak Seyfe*, Mohammad R. Aref†.

*Department of Electrical Engineering of Shahed Univ. Tehran, Iran, 
Email: {ghanizade, seyfe}@shahed.ac.ir

†ISSL Laboratory, Electrical Engineering Department, Sharif University of Technology, Tehran, Iran. 
Email: {salami@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 private 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

I. INTRODUCTION

INTERFERENCE channel (IC) is a fundamental building blocks in communication networks which is appear when signals intended for one receiver, supposed as interference for the other receivers. A key question in this setting is how to conquer 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 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 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 private 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 it has been shown that the results includes some prior results. 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 special case our region reduces to capacity of cognitive interference channel with secrecy was studied in [2].

The rest of the paper is organized as follows. In Section II we introduce the model of ICC channel with confidential messages. In Section III, 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.

II. CHANNEL MODELS

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

Definition 1: Let \( C \) denotes a discrete memoryless interference channel consists of finite alphabets \( (X_1, X_2, Y_1, Y_2) \) where \( X_t \) and \( Y_t, t = 1, 2, \) denote channel input and output respectively and \( P \) denotes the collection of the conditional probabilities \( p(y_1, y_2|x_1, x_2) \) on \( (y_1, y_2) \in Y_1 \times Y_2 \) given \( (x_1, x_2) \in X_1 \times X_2 \). The channel is memoryless and for \( n \) channel uses, we have

\[
p(y_{1}, y_{2}|x_{1}, x_{2}) = \prod_{t=1}^{n} p(y_{t1}, y_{t2}|x_{t1}, x_{t2})
\]

where \( x_t = (x_{t1}, ..., x_{tn}) \in X_t^n \) and \( y_t = (y_{t1}, ..., y_{tn}) \in Y_t^n \) for \( t = 1, 2 \). The marginal distribution of \( y_t \) given by

\[
p_t(y_t|x_1, x_2) = \sum_{y_t \in Y_t} p_t(y_t, y_t, x_1, x_2)
\]
where $t$ is one of the numbers 1 or 2 and $\bar{t}$ is the other one.

In this scenario each sender have a private message $w_t \in \mathcal{M}_t \{1, 2, \ldots, M_t\}$ with a common message $w_0 \in \mathcal{M}_0 \{1, 2, \ldots, M_0\}$, $t = 1, 2$. 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

$$f_t: \mathcal{M}_t \times \mathcal{T} \to \mathcal{X}_t^n$$

and

$$g_t: \mathcal{Y}_t^n \to \mathcal{M}_t \times \mathcal{T}$$

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

$$p_{e,t}(n) = \frac{1}{M_0 M_1 M_2} \sum_{M_0 M_1 M_2} p((\tilde{w}_0, \tilde{w}_t) \neq (w_0, w_t)|(w_0, w_1, w_2))$$

**Definition 3:** A nonnegative rate quintuple $(R_0, R_1, R_2, R_{e1}, R_{e2})$ is said to be achievable for channel $\mathcal{C}$ 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

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

and

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

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

### III. 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:

$$\mathcal{R}^{11} = \text{Conv} \bigcup_{\mathcal{R}_0, \mathcal{R}_1, \mathcal{R}_2, \mathcal{R}_{e1}, \mathcal{R}_{e2}} \mathbb{E}_e(R_0, R_{11}, R_{12}, R_{21}, R_{22}) = \bigcup_{R_0, R_{11}, R_{12}, R_{21}, R_{22}, R_{e1}, R_{e2}} \left\{ (R_0, R_{11}, R_{12}, R_{21}, R_{22}) = \begin{cases} R_0 \geq 0, R_{11} \geq 0, R_{12} \geq 0, R_{21} \geq 0, R_{22} \geq 0, \\
R_{11} \leq I(X_1; Y_1; U_0 U_1 U_2), \\
R_{12} \leq I(X_1; Y_1; U_0 U_2), \\
R_{21} \leq I(X_1; Y_2; U_1 U_0), \\
R_{22} \leq I(X_2; Y_2; U_1 U_2), \\
R_{e1} \leq I(U_0; Y_1 U_1 U_2), \\
R_{e2} \leq I(U_0; Y_2 U_1 U_2), \\
R_{e1} + R_{e2} \leq I(U_0; Y_1 U_1 U_2), \\
R_{e2} + R_{e1} \leq I(U_0; Y_2 U_1 U_2) \bigg\} \right.$$
\[
\mathcal{L}_1(R_0, R_{11}, R_{12}, R_{21}, R_{22}) = \begin{cases}
(R_{e1}, R_{e2}): \\
0 \leq R_{e1} \leq R_{11} \\
0 \leq R_{e2} \leq R_{21} \\
R_{e1} \leq [I(X_1; Y_1 U_1 U_2) - I(Y_2; X_1 X_2)]^+ \\
R_{e2} \leq [I(X_2; Y_2 U_1 U_2) - I(Y_2; X_1 X_2)]^+ \\
R_{e1} \leq [I(U_1; X_1 U_2) - R_{12} - R_{21} - I(Y_2; X_1 X_2)]^+ \\
R_{e2} \leq [I(U_2; X_2 U_1) - R_{12} - R_{21} - I(Y_1; X_1 X_2)]^+ \\
R_{e1} \leq [I(U_2; X_2 U_1; Y_0) - R_{12} - R_{21} - I(Y_1; X_1 X_2)]^+ \\
R_{e2} \leq [I(U_1; X_1 U_2; Y_0) - R_{12} - R_{21} - I(Y_1; X_1 X_2)]^+ \\
\end{cases}
\]

\[
\mathcal{L}_2(R_0, R_{11}, R_{12}, R_{21}, R_{22}) = \begin{cases}
(R_{e1}, R_{e2}): \\
0 \leq R_{e1} \leq R_{11} + R_{12} \\
R_{e2} = 0 \\
R_{e1} \leq [I(X_1; Y_1 U_1 U_2) - I(Y_2; X_1 X_2)]^+ \\
R_{e2} \leq [I(X_2; Y_2 U_1 U_2) - I(Y_1; X_1 X_2)]^+ \\
R_{e1} \leq [I(X_1; Y_1 U_1 U_2) - I(Y_2; X_1 X_2)]^+ \\
R_{e2} \leq [I(X_2; Y_2 U_1 U_2) - I(Y_1; X_1 X_2)]^+ \\
R_{e1} \leq [I(X_1; Y_1 U_1 U_2) - I(Y_2; X_1 X_2)]^+ \\
R_{e2} \leq [I(X_2; Y_2 U_1 U_2) - I(Y_1; X_1 X_2)]^+ \\
R_{e1} \leq [I(U_2; X_2 U_1; Y_0) - R_{12} - R_{21} - I(Y_1; X_1 X_2)]^+ \\
R_{e2} \leq [I(U_1; X_1 U_2; Y_0) - R_{12} - R_{21} - I(Y_1; X_1 X_2)]^+ \\
\end{cases}
\]

\[
\mathcal{L}_3(R_0, R_{11}, R_{12}, R_{21}, R_{22}) = \begin{cases}
(R_{e1}, R_{e2}): \\
0 \leq R_{e1} \leq R_{21} + R_{22} \\
R_{e2} = 0 \\
R_{e1} \leq [I(X_1; Y_1 U_1 U_2) - I(Y_2; X_1 X_2)]^+ \\
R_{e2} \leq [I(X_2; Y_2 U_1 U_2) - I(Y_1; X_1 X_2)]^+ \\
R_{e1} \leq [I(X_1; Y_1 U_1 U_2) - I(Y_2; X_1 X_2)]^+ \\
R_{e2} \leq [I(X_2; Y_2 U_1 U_2) - I(Y_1; X_1 X_2)]^+ \\
R_{e1} \leq [I(X_1; Y_1 U_1 U_2) - I(Y_2; X_1 X_2)]^+ \\
R_{e2} \leq [I(X_2; Y_2 U_1 U_2) - I(Y_1; X_1 X_2)]^+ \\
\end{cases}
\]

The equivocation-rates are proved in Appendix B.

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 the \( p(.) \). The equivocation-rates are proved in Appendix B.

IV. 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 cognitive interference channel with secrecy. Moreover, the outer bound for this channel was derived.

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

\[
\begin{aligned}
W_0 & \in [1, \ldots, 2^{nR_0}] \\
W_{12} & \in [1, \ldots, 2^{nR_{12}}] \\
W_{11} & \in [1, \ldots, 2^{nR_{11}}] \\
W_{21} & \in [1, \ldots, 2^{nR_{21}}] \\
W_{22} & \in [1, \ldots, 2^{nR_{22}}] 
\end{aligned}
\]

(26)
where \( R_{12} + R_{13} = R_1 \) and \( R_{21} + R_{22} = R_2 \). Now we consider the following codebook:

\[
\mathcal{C} = \begin{cases} 
\mathbf{u}_0(i), & i \in \{1, \ldots, 2^nR_0\} \\
\mathbf{u}_1(i, j), & j \in \{1, 2, \ldots, 2^nR_2\} \\
\mathbf{u}_2(i, l), & l \in \{1, 2, \ldots, 2^nR_1\} \\
x_1(i, j, a, b), & a \in \{1, 2, \ldots, A\}, b \in \{1, 2, \ldots, B\} \\
x_2(i, l, c, d), & c \in \{1, 2, \ldots, C\}, d \in \{1, 2, \ldots, D\}
\end{cases}
\] (27)

where all codewords are strongly typical, i.e.,

\[
\begin{align*}
\mathbf{u}_0(i) & \in \mathcal{T}_n^m(\mathbb{P}_{u_0}), \\
\mathbf{u}_1(i, j) & \in \mathcal{T}_n^m(\mathbb{P}_{u_1|u_0} \mathbf{u}_0(i)), \\
\mathbf{u}_2(i, l) & \in \mathcal{T}_n^m(\mathbb{P}_{u_2|u_1} \mathbf{u}_1(i, j)), \\
x_1(i, j, a, b) & \in \mathcal{T}_n^m(\mathbb{P}_{x_1|u_1} \mathbf{u}_1(i, j)), \\
x_2(i, l, c, d) & \in \mathcal{T}_n^m(\mathbb{P}_{x_2|u_2} \mathbf{u}_2(i, l))
\end{align*}
\] (28)

for all \( i, j, l, a, b, c, d \), where \( \mathcal{T}_n^m \) denotes the typical sets of the respective joint distributions, and

\[
\frac{1}{n} \log A = R_{11} - I(X_1; Y_2 | U_1, X_2) \\
\frac{1}{n} \log B = I(X_1; Y_1 | U_1, X_2) \\
\frac{1}{n} \log C = R_{22} - I(X_2; Y_1 | U_2, X_1) \\
\frac{1}{n} \log D = I(X_2; Y_1 | U_2, X_1)
\] (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

\[
\mathcal{A} = \{1, 2, \ldots, A\}, \mathcal{B} = \{1, 2, \ldots, B\}, \\
\mathcal{C} = \{1, 2, \ldots, C\}, \mathcal{D} = \{1, 2, \ldots, D\},
\] (30)

where \( \mathcal{A}, \mathcal{B}, \mathcal{C} \) and \( \mathcal{D} \) are defined in (41). We let

\[
W_{11} = \mathcal{A} \times S \\
W_{22} = \mathcal{C} \times T
\] (31)

where \( S = \{1, 2, \ldots, S\} \) and \( T = \{1, 2, \ldots, T\} \) and

\[
\frac{1}{n} \log S = R_{11} - \frac{1}{n} \log A \\
\frac{1}{n} \log T = R_{22} - \frac{1}{n} \log C
\] (32)

We define

\[
\begin{align*}
f: & \mathcal{B} \to S \\
g: & \mathcal{D} \to T
\end{align*}
\]

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

\[
\|f^{-1}(s_1)\| \leq 2\|f^{-1}(s_2)\|, \quad \forall s_1, s_2 \in S \\
\|g^{-1}(t_1)\| \leq 2\|g^{-1}(t_2)\|, \quad \forall t_1, t_2 \in T
\]

Now we generate source messages in both senders. By using \( W_{11} = (a, s) \to (a, b) \) and \( W_{22} = (c, t) \to (c, d) \) where \( a \) and \( d \) are chosen randomly from the sets \( f^{-1}(s) \subseteq \mathcal{B} \) and \( g^{-1}(t) \subseteq \mathcal{D} \) respectively, sender 1 transmits \( x_1(i, j, a, b) \) and sender 2 transmits \( x_2(i, l, c, d) \) and transmissions are assumed synchronized.

**Decoding:** Each receiver, receives an \( n \)-length channel output sequence, \( y_1 \) and \( y_2 \) for receiver 1 and 2 respectively. Decoder 1 declares \((\hat{i}, \hat{j}, \hat{a}, \hat{b})\) which is the unique triple that satisfy \((u_0(\hat{i}), u_1(\hat{i}, \hat{j}), u_2(\hat{i}, \hat{l}), x_1(\hat{i}, \hat{j}, \hat{a}, \hat{b}), y_1) \in \mathcal{T}_n^{(n)}\) for some \( i \). Similarly decoder 2 declares \((\hat{i}, \hat{l}, \hat{c}, \hat{d})\), which is the unique triple that satisfies \((u_0(\hat{i}), u_1(\hat{i}, \hat{j}), u_2(\hat{i}, \hat{l}), x_2(\hat{i}, \hat{l}, \hat{c}, \hat{d}), y_2) \in \mathcal{T}_n^{(n)}\) for some \( j \). Otherwise, an error was notified.

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

\[
\begin{align*}
H\left(W_{21}, W_{22} | Y_1^n\right) & \geq H\left(W_{22} | Y_1^n, W_1^n, U_0^n, W_2^n\right) \\
& = H\left(W_{22} | Y_1^n, U_0^n, W_2^n\right) - H\left(Y_1^n | W_1^n, U_0^n, W_2^n\right) \\
& = H\left(W_{22}, X_2^n | W_1^n, U_0^n, W_2^n\right) - H\left(Y_1^n | W_1^n, U_0^n, W_2^n\right) \\
& \geq H\left(W_{22}, X_2^n | W_1^n, U_0^n, W_2^n\right) + H\left(Y_1^n | U_0^n, U_1^n, U_2^n, X_1^n\right) \\
& - H\left(W_{22}, X_2^n | W_1^n, U_0^n, W_2^n\right) - H\left(Y_1^n | W_1^n, U_0^n, W_2^n\right)
\end{align*}
\] (33)

where \((a)\) follows from the fact that conditioning does not increase the entropy and \((b)\) is because that \( Y_1^n \) independent of \((W_1^n, U_0^n, W_2^n)\) given \((U_0^n, U_1^n, U_2^n, X_1^n, X_2^n)\).

Now, we consider each term in (33). To compute the first term, just like [2] and its references we have:

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

\[
\frac{\mathbb{P}(x)_{\delta}}{\mathbb{P}(x_{\delta})} \leq 2^\delta \quad \forall x \in \{x_1, \ldots, x_m\}
\]

Then

\[
H(X) \geq \log m - \delta
\]

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

\[
\frac{\mathbb{P}(x_{\delta})}{\mathbb{P}(x)} \leq 2, \quad \forall x, x_{\delta} \in \{x_1, \ldots, x_m\}
\]

So we obtain

\[
\frac{1}{n} H(X_2^n | U_0^n, W_1^n, W_2^n) = (c) \frac{1}{n} H(Y_2^n | U_0^n, W_1^n, W_2^n)
\]

\[
\geq \frac{1}{n} \log C + \frac{1}{n} \log D - \frac{1}{n}
\]

\[
= R_{22} - \frac{1}{n}
\]

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

\[
\frac{1}{n} H(Y_1^n | U_0^n, U_1^n, U_2^n, X_1^n, X_2^n) \geq H(Y_1^n | U_0^n, U_1^n, U_2^n, X_1^n, X_2^n)
\]

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

\[
\frac{1}{n} H(X_2^n | U_0^n, Y_1^n, W_1^n, W_2^n) < \varepsilon
\]

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

\[
\Phi_i^n = \begin{cases} Y_1^n & \text{if } (u_0, u_1, u_2, x_2, y_2) \in \mathcal{T}_n^{(n)} \\
\Phi_i^n & \text{else}
\end{cases}
\]

where \( Z^n \) is an arbitrary sequence that is constructed in \( Y_1^n \).

Now we have
\[
\frac{1}{n} H(Y_1^n | W_1, W_2, U_0^n) \\
= \frac{1}{n} \sum_{W_1, W_2} \Pr [W_1 = \omega_1, W_2 = \omega_2] H(Y_1^n | W_1 = \omega_1, W_2 = \omega_2, U_0^n) \\
\leq \frac{1}{n} \sum_{W_1, W_2} \Pr [W_1 = \omega_1, W_2 = \omega_2] H(Y_1^n | Y_1^n | W_1 = \omega_1, W_2 = \omega_2, U_0^n) \\
\leq \frac{1}{n} \sum_{W_1, W_2} \Pr [W_1 = \omega_1, W_2 = \omega_2] \times \\
\left( H(Y_1^n | W_1 = \omega_1, W_2 = \omega_2, U_0^n) + H(Y_1^n | W_1 = \omega_1, W_2 = \omega_2, U_0^n) \right) \tag{40}
\]

For the first term in (40) we can write
\[
\frac{1}{n} \sum_{W_1, W_2} \Pr [W_1 = \omega_1, W_2 = \omega_2] H(Y_1^n | W_1 = \omega_1, W_2 = \omega_2, U_0^n) \\
\leq \frac{1}{n} \sum_{W_1, W_2} \Pr [W_1 = \omega_1, W_2 = \omega_2] \times \log \left[ \sum_{Y_1^n} \Pr [Y_1^n | W_1 = \omega_1, W_2 = \omega_2, U_0^n] \right] \tag{41}
\]

\[
\leq \frac{1}{n} \sum_{W_1, W_2} \Pr [W_1 = \omega_1, W_2 = \omega_2] \times \log \left[ \sum_{Y_1^n} \Pr [Y_1^n | W_1 = \omega_1, W_2 = \omega_2, U_0^n] \right] \\
\leq H(Y_1^n | U_0^n, U_1^n, U_2^n, X_1) + \epsilon \\
\]

To bound the second term in (40) we use the Fano’s inequality and obtain
\[
\frac{1}{n} \sum_{W_1, W_2} \Pr [W_1 = \omega_1, W_2 = \omega_2] H(Y_1^n | W_1 = \omega_1, W_2 = \omega_2, U_0^n) \\
\leq \frac{1}{n} \sum_{W_1, W_2} \Pr [W_1 = \omega_1, W_2 = \omega_2] \times \log \left[ \sum_{Y_1^n} \Pr [Y_1^n | W_1 = \omega_1, W_2 = \omega_2, U_0^n] \right] \\
\leq \frac{1}{n} \sum_{W_1, W_2} \Pr [W_1 = \omega_1, W_2 = \omega_2] \times \log \left[ \sum_{Y_1^n} \Pr [Y_1^n | W_1 = \omega_1, W_2 = \omega_2, U_0^n] \right] \\
\leq \epsilon \tag{42}
\]

Hence (40) is bounded as
\[
\frac{1}{n} H(Y_1^n | W_1, W_2, U_0^n) \leq H(Y_1^n | U_0 U_1 U_2 X_1) + \epsilon \tag{43}
\]

in which \( \epsilon \) is negligible for sufficiently large \( n \). Substituting (37), (38), (39) and (43) in (33) we obtained
\[
H(W_1 W_2 | Y_1^n) \\
\geq R_{c_1} - \frac{1}{n} + H \left( Y_1^n | U_0^n, U_1, U_2, X_1, X_2 \right) - H \left( Y_1^n | U_0, U_1, U_2, X_1, X_2 \right) \tag{44}
\]

\[
= R_{c_1} - I \left( Y_1^n | U_1, U_2, X_1, X_2 \right) - \frac{1}{n} \\
\]

By the definition of \( R_{c_1} \) we conclude
\[
R_{c_1} \leq R_{c_1} - I \left( Y_1^n | U_1, U_2, X_1, X_2 \right) - \frac{1}{n} \tag{45}
\]

**APPENDIX B**

In this section we prove Theorem 2. From the Fano’s Lemma we have
\[
H \left( W_0 W_1 | Y_1^n \right) \leq n \delta_n \tag{46}
\]

\[
H \left( W_0 W_2 | Y_2^n \right) \leq n \delta_n \tag{47}
\]

Now we check the bounds. First we consider \( R_0 \), following the approach taken in [5]
\[
n R_0 = H(W_0) = I \left( W_0, Y_1^n \right) + H(W_0 | Y_1^n) \\
\leq \sum_{i=1}^n I \left( W_0, Y_1_i | Y_1^{i-1} \right) + n \delta_n \\
\]

Similarly we can obtain
\[
n R_0 \leq \sum_{i=1}^n I \left( W_0, Y_1^n \right) + n \delta_n \tag{48}
\]

For the same rate bounds \( R_0 + R_1 \) we have
\[
n (R_0 + R_1) = H(W_0) + I \left( W_1, Y_1^n | W_0 \right) + H \left( W_0 | Y_1^n W_0 \right) \\
\leq n R_0 + n R_1 + n \delta_n \tag{49}
\]

For the second term in (50) we can write
\[
n R_1 \leq \sum_{i=1}^n I \left( W_0, Y_1^n \right) + n \delta_n \tag{50}
\]

From (50) and (51) we have
\[
n (R_0 + R_1) = n \left( R_0 + R_1 \right) + \sum_{i=1}^n I \left( W_0, Y_1^n \right) + 2n \delta_n \tag{52}
\]

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

Considering sum rate bounds \( R_0 + R_1 + R_2 \), we have
\[
n \left( R_0 + R_1 + R_2 \right) = H(W_0 W_1) + I \left( W_2, Y_1^n | W_1 W_0 \right) + H \left( W_2 | Y_1^n W_1 W_0 \right) \\
\leq H(W_0 W_1) + I \left( W_2, Y_1^n | W_1 W_0 \right) + n \delta_n \tag{53}
\]

Similarly we have
\[
n \left( R_0 + R_1 + R_2 \right) \leq \sum_{i=1}^n I \left( W_0, Y_1^n \right) + 2n \delta_n \tag{54}
\]

Following similarly as previous bounds, we can obtain
\[
n \left( R_0 + R_1 + R_2 \right) = n \left( R_0 + R_1 + R_2 \right) + \sum_{i=1}^n I \left( W_0, Y_1^n \right) + n \delta_n \tag{55}
\]
Combining (54)-(57), (22) and (23) are obtained. For the equivocability rate bounds we have

\[ R_{el} \leq H(W_1|Y^n_2) \]

\[ = H(W_1|Y^n_2W_0) + I(W_1;W_0|Y^n_2) \]

\[ \leq H(W_1|W_0) - I(W_1;Y^n_2|W_0) + H(W_0|Y^n_2) \]

\[ = I(W_1;Y^n_2|W_0) - I(W_1;Y^n_2|W_0) + H(W_1|Y^n_0W_0) \]

\[ + H(W_0|Y^n_2) \]

\[ \leq I(W_1;Y^n_2|W_0) - I(W_1;Y^n_2|W_0) + 2\delta_n \]  

For the second term in (59) we have

\[ I(W_1;Y^n_2|W_0W_2) \]

\[ \leq \sum_{i=1}^{\infty} I(W_1;Y^n_2|W_0W_2) \]

\[ \leq \sum_{i=1}^{\infty} I(W_1;Y^n_2|W_0W_2) \]

Therefore we obtain

\[ R_{el} \leq \sum_{i=1}^{\infty} I(W_1;Y^n_2|W_0W_2) + 2\delta_n \]

By defining following auxiliary random variables (19)-(25) are obtained. \( Q \) is a random variable uniformly distributed over \( \{1,\ldots,n\} \), independent of \( W_0W_1W_2X^n_1X^n_2Y^n_1Y^n_2 \).

\[ U_i \triangleq W_0^{Y^n_1+1}Y^n_2+1Q \]

\[ V_i \triangleq W_iU, V_i \triangleq W_iU \]

\[ Y_1 \triangleq Y^n_1, Y_2 \triangleq Y^n_2 \]