Broadcast Channel with Confidential Messages and Secret Keys

Krishnamoorthy Iyer

***Abstract*—We consider the problem of transmitting confidential messages over a two receiver broadcast channel. Two private messages are to be communicated, one to each of the two receivers. Each message is to be kept secret from the unintended receiver. Secret keys are available at fixed rates between each receiver and the transmitter. Various regimes of the key rates are described and achievable schemes are presented for each. Our schemes involve double random binning, key-dependent codebooks, and a technique called sectioning. Interestingly, double encryption on time-sharing sequences enhances the achievable region in certain regimes. The model subsumes several other models in the literature.**

***Index Terms*—broadcast channel, secrecy capacity region, confidential messages, secret keys**

I. Introduction

We study a discrete-memoryless broadcast channel (DM-BC) with two receivers. The transmitter needs to send separate messages to each receiver, and the message intended for each receiver is to be kept secret from the other. In addition, each transmitter-receiver pair has a secret key available at a fixed rate unknown to the other receiver. These can assist in achieving secrecy. We present an inner bound of the capacity region for this problem. We also state an outer bound.

Security of transmitted messages is of prime concern in broadcast networks. Even if no external eavesdropper is present, it is sometimes necessary to secure the messages of the receivers against each other. One example of this is the model studied by [1], where secrecy-rate regions were obtained by using double-random binning. [2] extended this model by requiring the transmission of a common message, and obtained an achievable rate-equivocation region.

To the best of our knowledge, [3] was the first to develop a coherent scheme that unified channel coding techniques and the use of secret keys to increase secrecy/equivocation rates for a (degraded/less-noisy) DM-BC. More recently, [4] extended the result of [3] to a general BC – they introduced the notion of key-dependent codebooks, which was crucial to their scheme. In both [3] and [4], the legitimate information flow is point-to-point, and the eavesdropper is external. The scheme in [4] also involved, in some regimes, encoding encrypted data inside a sequence decoded by both the eavesdropper and the legitimate user.

In [1], two legitimate information flows are present, and both receivers also eavesdrop on the others' message. While the underlying broadcast model is similar to [1], the presence of of secret keys introduces a degree of freedom that changes the dynamics significantly, requiring the application of a novel technique (used in [4]) to exploit them fully. In order to achieve (weak) secrecy, the achievable scheme of [1] incurs two separate rate penalties on each individual data stream due to double random binning.

We show that the availability of secret keys can be used to progressively dispense with this double penalty. We develop a unified scheme naturally integrating double-random binning [1], key-dependent codebooks [4], and sectioning [5]. This seamlessly gives the rate-region corresponding to Marton's region with high enough secret key rates. Furthermore, in the extreme cases where there are no secret keys or there is only one legitimate receiver, the region respectively simplifies to the regions of [1] and [4], which can be seen as special cases of our model.

As already noted in [4], surprisingly, it is often beneficial to encrypt information into a common sequence, which is decoded by both the receivers. Though the sequence is commonly received, encryption ensures secrecy. Our method of encrypting to a common sequence differs significantly from the scheme of [4, Section IV, Case 2]. We show that a simple, but appropriate, one-time pad (OTP) idea is enough to encrypt the data contained in the common sequence, thereby also simplifying the coding scheme of [4].

In other relevant work, [6] and [7] considered BCs with common and confidential messages with feedback used to generate secret keys. [8] and [9] respectively study two models with two legitimate receivers and an external eavesdropper, and a secret key shared between each transmitter and legitimate receiver pair. However, there is no confidentiality requirement between the legitimate receivers.

The paper is organized as follows. In Section II, the model is described. In Section III, the main theorem and various cases are enumerated. Section IV details the achievable schemes. In Section V, we state the outer bound(s). In section VI, we summarize the results obtained.

II. The Model

We assume a two-receiver discrete memoryless BC with two confidential messages and two secret keys. The finite sets $\mathcal{X}$, $\mathcal{Y}_1$, $\mathcal{Y}_2$ represent the channel's input and the two output alphabets respectively. The channel is described by the conditional probability distribution $P_{Y_1,Y_2|X}(y_1, y_2|x)$, where RVs $X \in \mathcal{X}$, $Y_1 \in \mathcal{Y}_1$, $Y_2 \in \mathcal{Y}_2$. In addition, we assume the availability of secret keys, denoted by RVs $K_1 \in \mathcal{K}_1$ and $K_2 \in \mathcal{K}_2$, between each respective transmitter-receiver pair 1 and 2 unknown to the other receiver, at rates R_{k_1} and R_{k_2} respectively. The transmitter intends to send an independent

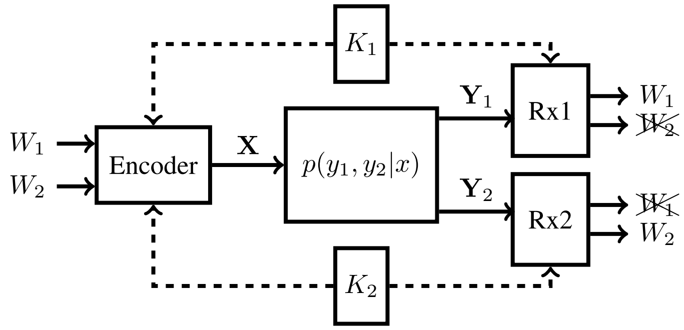

Fig. 1. Two Receiver Broadcast Channel with Two Confidential Messages and Two Secret Keys

message $W_t \in \{1, 2 \ldots, 2^{nR_t}\} \triangleq \mathcal{W}_t$ to the respective receiver $t \in \{1, 2\}$ in n channel uses while ensuring information theoretic secrecy, defined below. The channel is memoryless and without feedback i.e. $\forall \mathbf{x} \in \mathcal{X}^n$, $\mathbf{y}_t \in \mathcal{Y}_t^n$, $t = 1, 2$

$$P(\mathbf{y}_1, \mathbf{y}_2|\mathbf{x}) = \prod_{i=1}^{n} P_{Y_1,Y_2|X}(y_{1i}, y_{2i}|x_i)$$

A stochastic encoder is specified by a matrix of conditional probabilities $f(\mathbf{x}|w_1, k_1, w_2, k_2)$, $\forall w_t \in \mathcal{W}_t$, $k_t \in \mathcal{K}_t$, and

$$\sum_{\mathbf{x} \in \mathcal{X}^n} f(\mathbf{x}|w_1, k_1, w_2, k_2) = 1$$

$f(\mathbf{x}|w_1, k_1, w_2, k_2)$ is the probability that the quadruple of messages and keys (w_1, k_1, w_2, k_2) are encoded as the channel input $\mathbf{x}$. The decoding function at the receiver $t = 1, 2$ is a mapping $\phi_t : \mathcal{K}_t \times \mathcal{Y}_t^n \to \mathcal{W}_t$. A $(2^{nR_1}, 2^{nR_2}, 2^{nR_{k_1}}, 2^{nR_{k_2}}, n, P_e^{(n)})$ code for the broadcast channel consists of the encoding function f, decoding functions ϕ_1, ϕ_2, and the error probability defined as

$$P_e^{(n)} \triangleq \max\{P_{e,1}^{(n)}, P_{e,2}^{(n)}\},$$

where for $t = 1, 2$,

$$P_{e,t}^{(n)} = \sum_{w_1,w_2,k_1,k_2} \frac{P[\phi_t(K_t, \mathbf{Y}_t) \neq w_t|(w_1, w_2, k_1, k_2)]}{2^{nR_1} \times 2^{nR_2} \times 2^{nR_{k_1}} \times 2^{nR_{k_2}}}$$

A rate pair (R_1, R_2) is said to be achievable for the broadcast channel with confidential messages and two secret keys at rates (R_{k_1}, R_{k_2}) if, for any $\epsilon_0 > 0$, there exists a $(2^{nR_1}, 2^{nR_2}, 2^{nR_{k_1}}, 2^{nR_{k_2}}, n, P_e^{(n)})$ code which satisfies both

- reliability requirement: $P_e^{(n)} \leq \epsilon_0$
- secrecy constraint: $nR_t - H(W_t|\mathbf{Y}_{\bar{t}}, K_{\bar{t}}) \leq n\epsilon_0, t = 1, 2.$

This definition corresponds to the so-called *weak secrecy-key rate* [1]. We use the notation $\bar{t} \triangleq \{1, 2\} \setminus \{t\}$. We define a class π_{BC} of distributions $P(u, v_1, v_2, x, y_1, y_2)$ that factor as $P(u)P(v_1, v_2|u)P(x|v_1, v_2)P(y_1, y_2|x)$.

III. Inner Bound

The main result of our paper is presented below.

Theorem 1. *Let $\mathbb{R}_{BC}(\pi_{BC})$ denote the union of all $(R_1, R_2) \in \mathbb{R}_+^2$ satisfying*

$$\begin{aligned} R_1 &\leq I(V_1; Y_1|U) + \min\Big\{R_{k_1} - I(V_1; Y_2|V_2, U) \\ &\quad - I(V_1; V_2|U), I(U; Y_1), I(U; Y_2)\Big\} \\ R_2 &\leq I(V_2; Y_2|U) + \min\Big\{R_{k_2} - I(V_2; Y_1|V_1, U) \\ &\quad - I(V_2; V_1|U), I(U; Y_1), I(U; Y_2)\Big\} \\ R_1 + R_2 &\leq I(V_1; Y_1|U) + I(V_2; Y_2|U) - I(V_1; V_2|U) \\ &\quad + \min\{I(U; Y_1), I(U; Y_2)\}. \end{aligned} \tag{1}$$

where the union is over all distributions $P(u, v_1, v_2, x, y_1, y_2)$ in π_{BC}. Every rate pair $(R_1, R_2) \in \mathbb{R}_{BC}(\pi_{BC})$ is achievable.

The key rates determine the achievable scheme. We enumerate eight different regimes and present their achievable schemes in Section IV.

- **Case** 1:
$$R_{k_1} \leq I(V_1; Y_2|V_2, U); \;\; R_{k_2} \leq I(V_2; Y_1|V_1, U).$$
- **Case** 2:
$$\begin{aligned} R_{k_2} &\leq I(V_2; Y_1|V_1, U) \\ I(V_1; Y_2|V_2, U) < R_{k_1} &\leq I(V_1; Y_2|V_2, U) + I(V_1; V_2|U). \end{aligned}$$
- **Case** 3**:** This is identical to Case 2 with the roles of the receivers switched.
- **Case** 4**:**
$$\begin{aligned} I(V_1; Y_2|V_2, U) < R_{k_1} &\leq I(V_1; Y_2|V_2, U) + I(V_1; V_2|U) \\ I(V_2; Y_1|V_1, U) < R_{k_2} &\leq I(V_2; Y_1|V_1, U) + I(V_2; V_1|U). \end{aligned}$$
- **Case** 5**:**
$$\begin{aligned} R_{k_1} &> I(V_1; Y_2|V_2, U) + I(V_1; V_2|U) \\ I(V_2; Y_1|V_1, U) < R_{k_2} &\leq I(V_2; Y_1|V_1, U) + I(V_2; V_1|U). \end{aligned}$$
- **Case** 6**:** This is identical to Case 5 with the roles of the receivers switched.
- **Case** 7**:**
$$\begin{aligned} R_{k_1} &> I(V_1; Y_2|V_2, U) + I(V_1; V_2|U) \\ R_{k_2} &> I(V_2; Y_1|V_1, U) + I(V_2; V_1|U). \end{aligned}$$
- **Case** 8**:** The remaining cases (where key rate mismatch large) and $5 - 7$ have achievable schemes etc. similar to Case 4.

IV. Achievability Schemes

For ease of exposition, we will distinguish between the terms *code* and *codebook*. Also, $R^\dagger \triangleq I(V_1; V_2|U) + \epsilon_1'$ where $\epsilon_1' > 0$ is a small positive constant.

A. Case 1:

The proposed achievable region becomes

$$R_1 \leq I(V_1;Y_1|U) - I(V_1;V_2|U) - I(V_1;Y_2|V_2,U) + R_{k_1}$$
$$R_2 \leq I(V_2;Y_2|U) - I(V_2;V_1|U) - I(V_2;Y_1|V_1,U) + R_{k_2}$$

Our achievability scheme melds the techniques of *double random binning* [1] and *code consisting of multiple key-dependent codebooks* [4, Section IV, Case 1]. Double binning, in turn, combines Gelfand-Pinker binning and random binning (to satisfy mutual covering and to confuse the other receiver to maintain perfect secrecy).

The employed coding structure is shown below. A joint encoder generates two equivocation codewords $\mathbf{v}_1$ and $\mathbf{v}_2$, one for each message-key pair (W_1, K_1) and (W_2, K_2). The pair $(\mathbf{v}_1, \mathbf{v}_2)$ is stochastically mapped into $\mathbf{x}$. The details follow.

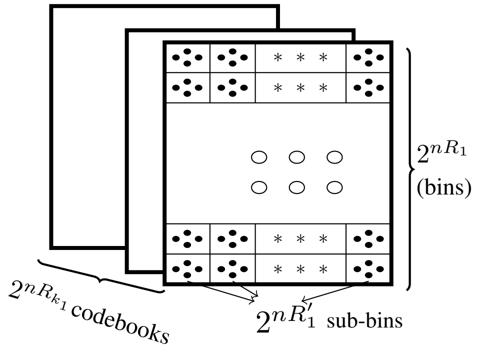

Fig. 2. Case 1: Code for receiver 1

1) Code Construction: Fix $P(u)$, $P(v_1|u)$ and $P(v_2|u)$ as well as $P(x|v_1, v_2)$ and define

$$R'_1 \triangleq I(V_1;Y_2|V_2,U) - \epsilon'_1 - R_{k_1}$$
$$R'_2 \triangleq I(V_2;Y_1|V_1,U) - \epsilon'_1 - R_{k_2}$$

Randomly generate a sequence $\mathbf{u} \sim P(\mathbf{u}) = \prod_{i=1}^{n} P(u_i)$. For $t = 1, 2$, generate code $\mathcal{C}_t$ with $2^{(R_{k_t}+R_t+R'_t+R^\dagger)}$ (conditionally) 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 $\mathbf{v}_t(k_t, w_t, s_t, r_t)$ for $k_t \in \{1, \ldots, 2^{nR_{k_t}}\}$, $w_t \in \{1, \ldots, 2^{nR_t}\}$, $s_t \in \{1, \ldots, 2^{nR'_t}\}$, $r_t \in \{1, \ldots, 2^{nR^\dagger}\}$. W.l.o.g, $2^{nR_{k_t}}$, 2^{nR_t}, $2^{nR'_t}$, $2^{nR^\dagger}$ are considered to be integers.

The code $\mathcal{C}_1$ for receiver 1 consists of $2^{nR_{k_1}}$ codebooks [4, Section IV, Case 1]. Each codebook of $\mathcal{C}_1$ is doubly binned, as in [1], with 2^{nR_1} bins, each containing $2^{nR'_1} = 2^{n[I(V_1;Y_2|V_2,U)-R_{k_1}-\epsilon'_1]}$ sub-bins. Receiver 2's code $\mathcal{C}_2$ is similar.

In all codebooks, each sub-bin contains $2^{nR^\dagger} = 2^{n[I(V_1;V_2|U)+\epsilon'_1]}$ codewords. Furthermore, each codebook in code $\mathcal{C}_t$ contains $2^{n[I(V_t;Y_t|U)-\epsilon'_1]}$ codewords. Please see Figure 2.

The sequence $\mathbf{u}$ and code $\mathcal{C} = \{\mathcal{C}_1, \mathcal{C}_2\}$ is commmunicated to all parties.

2) Encoding: Given key pair $(k_1, k_2) \in \mathcal{K}_1 \times \mathcal{K}_2$, the encoder chooses the appropriate codebooks $\mathcal{C}_1(k_1)$ and $\mathcal{C}_2(k_2)$ in the respective codes $\mathcal{C}_1$ and $\mathcal{C}_2$. To send $(w_1, w_2) \in \mathcal{W}_1 \times \mathcal{W}_2$, the transmitter randomly chooses a sub-bin $\mathcal{C}_t(k_t, w_t, s_t)$ from the bin $\mathcal{C}_t(k_t, w_t)$, for $t = 1, 2$. Next, a pair (r_1, r_2) is chosen such that $(\mathbf{v}_1(k_1, w_1, s_1, r_1), \mathbf{v}_2(k_2, w_2, s_2, r_2)) \in A_\epsilon^{(n)}(V_1, V_2|\mathbf{u})$, where $A_\epsilon^{(n)}(V_1, V_2|\mathbf{u})$ indicates the set of jointly typical sequences $(\mathbf{v}_1, \mathbf{v}_2, \mathbf{u})$ for the given realization $\mathbf{u}$, according to $P_{V_1,V_2|U}$. By mutual covering [10], such a pair exists with high probability. If more than one jointly typical pair exists, one is randomly chosen. We now employ the stochastic encoder which generates $\mathbf{x} \sim \prod_{i=1}^{n} p(x_i|v_{1i}, v_{2i})$ for transmission. *Note that the* $\mathbf{x}$ *codewords are not part of the code* $\mathcal{C}$. *They are generated at the time of transmission after choosing an appropriate* $(\mathbf{v}_1, \mathbf{v}_2)$ *pair.*

3) Decoding: The decoder t has access to the shared key k_t and so the decoding at decoder t for $t = 1, 2$ has to be done from among $2^{n(R_t+R'_t+R^\dagger)} \approx 2^{n[I(V_t;Y_t|U)]}$ sequences $\mathbf{v}_t$ in the codebook $\mathcal{C}_t(k_t)$, see Fig 2. Decoder t chooses w_t such that $(\mathbf{v}_t(k_t, w_t, s_t, r_t), \mathbf{y}_t, \mathbf{u}) \in A_\epsilon^{(n)}(V_t, Y_t, U)$ for some (s_t, r_t), if a unique such w_t exists, else an error is declared.

4) Error Probability Analysis: While the codewords here are quadruply indexed to reflect the codebook index as shown in Fig 2, the rest of the details are standard, omitted here due to space limitations [11].

5) Equivocation calculation for Case 1: We prove that secrecy holds. It is worth mentioning that the calculations below have subtle differences from a similar calculation in [4], improving the robustness. We first express the equivocation as

$$H(W_1|\mathbf{Y}_2, K_2) = \sum_{k_2 \in \mathcal{K}_2} P(K_2 = k_2) H(W_1|\mathbf{Y}_2, k_2) \qquad (2)$$

We will now show that $\forall K_2 = k_2$,

$$H(W_1|\mathbf{Y}_2, k_2) \geq nR_1 - n\tilde{\epsilon}, \qquad (3)$$

implying secrecy of Receiver 1's messages.

$$\begin{aligned} &H(W_1|\mathbf{Y}_2, k_2) && (4) \\ &\quad \geq H(W_1|\mathbf{Y}_2, k_2, \mathbf{V}_2, \mathbf{U}) \\ &\quad = H(W_1, \mathbf{Y}_2|k_2, \mathbf{V}_2, \mathbf{U}) - H(\mathbf{Y}_2|k_2, \mathbf{V}_2, \mathbf{U}) \\ &\quad = H(W_1, \mathbf{V}_1, \mathbf{Y}_2|k_2, \mathbf{V}_2, \mathbf{U}) \\ &\qquad - H(\mathbf{V}_1|k_2, \mathbf{Y}_2, \mathbf{V}_2, \mathbf{U}, W_1) - H(\mathbf{Y}_2|k_2, \mathbf{V}_2, \mathbf{U}) \\ &\quad = H(W_1, \mathbf{V}_1|k_2, \mathbf{V}_2, \mathbf{U}) + H(\mathbf{Y}_2|k_2, \mathbf{V}_1, \mathbf{V}_2, \mathbf{U}, W_1) \\ &\qquad - H(\mathbf{Y}_2|k_2, \mathbf{V}_2, \mathbf{U}) - H(\mathbf{V}_1|k_2, \mathbf{Y}_2, \mathbf{V}_2, \mathbf{U}, W_1) \end{aligned}$$

Based on functional dependence graphs, we can show that $\forall K_2 = k_2, W_1 \rightarrow (\mathbf{V}_1, \mathbf{V}_2, \mathbf{U}) \rightarrow \mathbf{Y}_2$ forms a Markov Chain. Thus the second term becomes

$$H(\mathbf{Y}_2|k_2, \mathbf{V}_1, \mathbf{V}_2, \mathbf{U}, W_1) = H(\mathbf{Y}_2|k_2, \mathbf{V}_1, \mathbf{V}_2, \mathbf{U})$$

Making the replacement, we now have

$$\begin{aligned}
&H(W_1|\mathbf{Y}_2,k_2)\\
&\quad\geq H(W_1,\mathbf{V}_1|k_2,\mathbf{V}_2,\mathbf{U})+H(\mathbf{Y}_2|k_2,\mathbf{V}_1,\mathbf{V}_2,\mathbf{U})\\
&\qquad-H(\mathbf{Y}_2|k_2,\mathbf{V}_2,\mathbf{U})-H(\mathbf{V}_1|k_2,\mathbf{Y}_2,\mathbf{V}_2,\mathbf{U},W_1)\\
&\quad=H(W_1,\mathbf{V}_1|k_2,\mathbf{V}_2,\mathbf{U})-I(\mathbf{V}_1;\mathbf{Y}_2|k_2,\mathbf{V}_2,\mathbf{U})\\
&\qquad\qquad-H(\mathbf{V}_1|k_2,\mathbf{Y}_2,\mathbf{V}_2,\mathbf{U},W_1). \qquad (5)
\end{aligned}$$

By a calculation analogous to [1, Lemma 2], we can show that

$$H(\mathbf{V}_1|k_2,\mathbf{Y}_2,\mathbf{V}_2,\mathbf{U},W_1)\leq n\epsilon_3', \qquad (6)$$

where ϵ_3' is small for sufficiently large n. This can be interpreted to mean that there is no uncertainty left in $\mathbf{V}_1$ given $(k_2,\mathbf{Y}_2,\mathbf{V}_2,\mathbf{U},W_1)$. If there were, the randomness can be included in W_1 to improve the rate R_1.

To compute $H(\mathbf{V}_1|k_2,\mathbf{Y}_2,\mathbf{V}_2,\mathbf{U},W_1)$, we proceed as follows. Suppose $W_1=w_1$, Receiver 2 (acting as the eavesdropper) tries to decode $\mathbf{v}_1(k_1,w_1,s_1,r_1)$ based on its received sequence $\mathbf{y}_2$ (of course it already has knowledge of its own key k_2). Since Decoder 2 knows w_1, let $\lambda_{k_2}(w_1)$ denote the average probability of error of decoding the indices (k_1,s_1,r_1) at Receiver 2 (given that its key is k_2). Joint typicality enables us to show that

Lemma 2. *$\lambda_{k_2}(w_1)\leq\epsilon_0'$ for sufficiently large n.*

Proof. For a given time-sharing sequence $\mathbf{u}$, let $A_\epsilon^{(n)}(P_{V_1,V_2,Y_2|U})$ denote the set of jointly typical sequences $\mathbf{v}_1$ and $(\mathbf{v}_2,\mathbf{y}_2)$ with respect to $P(v_1,v_2,y_2|u)$. For a given $W_1=w_1$, Decoder 2 chooses (k_1,s_1,r_1) with

$$(\mathbf{v}_1,\mathbf{v}_2,\mathbf{y}_2)\in A_\epsilon^{(n)}(P_{V_1,V_2,Y_2|U}), \qquad (7)$$

if such a pair (k_1,s_1,r_1) exists and is unique; else an error is declared.

We define the event

$$\hat{E}(k_1,s_1,r_1)=(\mathbf{v}_1(k_1,w_1,s_1,r_1),\mathbf{v}_2,\mathbf{y}_2)\in A_\epsilon^{(n)}(P_{V_1,V_2,Y_2|U}) \qquad (8)$$

W.l.o.g, we assume that $\mathbf{v}_1(k_1=1,w_1,s_1=1,r_1=1)$ was chosen, and define the event

$$\mathcal{B}_{w_1}=\{\mathbf{v}_1(1,w_1,1,1)\text{ chosen}\} \qquad (9)$$

Hence

$$\begin{aligned}
\lambda_{k_2}(w_1)&\leq P\{\hat{E}^c(k_1=1,s_1=1,r_1=1)|\mathcal{B}_{w_1}\}\\
&\quad+\sum_{(k_1,s_1,r_1)\neq(1,1,1)}P\{\hat{E}((k_1,s_1,r_1))|\mathcal{B}_{w_1}\} \qquad (10)
\end{aligned}$$

where $\hat{E}^c(k_1=1,s_1=1,r_1=1)$ denotes the event

$$\{(\mathbf{v}_1(1,w_1,1,1),\mathbf{v}_2,\mathbf{y}_2)\notin A_\epsilon^{(n)}(P_{V_1,V_2,Y_2|U})\} \qquad (11)$$

By the joint AEP,

$$P\{\hat{E}^c(k_1=1,s_1=1,r_1=1)\}\leq\epsilon \qquad (12)$$

and for $(k_1,s_1,r_1)\neq(1,1,1)$,

$$P\{\hat{E}((k_1,s_1,r_1))|\mathcal{B}_{w_1}\}\leq 2^{-n[I(V_1;V_2,Y_2|U)-\epsilon]} \qquad (13)$$

We upper bound $\lambda_{k_2}(w_1)$ as

$$\epsilon+2^{nR_{k_1}}2^{nR_1'}2^{nR^\dagger}2^{-n[I(V_1;V_2,Y_2|U)-\epsilon]} \qquad (14)$$

Now since $R_{k_1}+R_1'+R^\dagger=I(V_1;V_2,Y_2|U)$, we finally have

$$\lambda_{k_2}(w_1)\leq\epsilon_0' \qquad (15)$$

where ϵ_0' small for n sufficiently large. □

By Fano's inequality

$$\begin{aligned}
&\frac{1}{n}H(\mathbf{V}_1|k_2,\mathbf{Y}_2,\mathbf{V}_2,\mathbf{U},W_1=w_1)\leq\\
&\qquad\frac{1}{n}[1+\lambda_{k_2}(w_1)\log[2^{nR_{k_1}}2^{nR_1'}2^{nR^\dagger}]]\triangleq\epsilon_3' \qquad (16)
\end{aligned}$$

We conclude that

$$\begin{aligned}
&\frac{1}{n}H(\mathbf{V}_1|k_2,\mathbf{Y}_2,\mathbf{V}_2,\mathbf{U},W_1)\\
&=\frac{1}{n}\sum_{w_1\in\mathcal{W}_1}P(W_1=w_1)H(\mathbf{V}_1|k_2,\mathbf{Y}_2,\mathbf{V}_2,\mathbf{U},W_1=w_1)\\
&\leq\epsilon_3' \qquad (17)
\end{aligned}$$

The above is an application of the technique from [4] whereby the key index $(K_t,t=1,2)$ introduces an extra degree of randomness which increases equivocation only at the receiver for which the message is not intended. The secret keys ensure that the randomness requirement (the RV that chooses the subbin) for the transmitter-receiver t pair is reduced by the respective key rate R_{k_t} from $I(V_t;Y_{\bar{t}}|V_{\bar{t}},U)$ to $I(V_t;Y_{\bar{t}}|V_{\bar{t}},U)-R_{k_t}$ for $t=1,2$.

We have shown that

$$H(\mathbf{V}_1|k_2,\mathbf{Y}_2,\mathbf{V}_2,\mathbf{U},W_1)\leq n\epsilon_3' \qquad (18)$$

Substituting the above inequality in (5), we get

$$\begin{aligned}
H(W_1|\mathbf{Y}_2,k_2)&\geq H(W_1,\mathbf{V}_1|k_2,\mathbf{V}_2,\mathbf{U})\\
&\quad-I(\mathbf{V}_1;\mathbf{Y}_2|k_2,\mathbf{V}_2,\mathbf{U})-n\epsilon_3'. \qquad (19)
\end{aligned}$$

Now, in the first term on the RHS above, the equivocation of $(W_1,\mathbf{V}_1)$ is the logarithm of the total number of cells in the code $\mathcal{C}_1$, which is $2^{n[I(V_1;Y_1|U)+R_{k_1}]}$. Next, we note that in the random codebook $\mathcal{C}$, our coding scheme only requires that we find a codeword $\mathbf{V}_2$ that is jointly typical with $\mathbf{V}_1$, *thus the choice of key k_2 does not play a role*. Conditioning by $\mathbf{V}_2$ causes a reduction by a factor of $2^{I(\mathbf{V}_1;\mathbf{V}_2|\mathbf{U})}$, to give $2^{n[I(V_1;Y_1|U)+R_{k_1}]}2^{-I(\mathbf{V}_1;\mathbf{V}_2|\mathbf{U})}$. Taking logs, we get $n[I(V_1;Y_1|U)+R_{k_1}]-I(\mathbf{V}_1;\mathbf{V}_2|\mathbf{U})$. Thus we have

$$\begin{aligned}
H(W_1|\mathbf{Y}_2,k_2)&\geq n[I(V_1;Y_1|U)+R_{k_1}]-I(\mathbf{V}_1;\mathbf{V}_2|\mathbf{U})\\
&\quad-I(\mathbf{V}_1;\mathbf{Y}_2|k_2,\mathbf{V}_2,\mathbf{U})-n\epsilon_3' \qquad (20)
\end{aligned}$$

Now, by a calculation (omitted due to space limitations) (see [11]), we can obtain the following inequalities:

$$I(\mathbf{V}_1;\mathbf{V}_2|\mathbf{U})\leq nI(V_1;V_2|U)+n\epsilon_2' \qquad (21)$$

and

$$I(\mathbf{V}_1;\mathbf{Y}_2|k_2,\mathbf{V}_2,\mathbf{U})\leq nI(V_1;Y_2|V_2,U)+n\epsilon_4' \qquad (22)$$

Substituting (21) and (22) in (20), we get

$$\begin{aligned} &H(W_1|\mathbf{Y}_2, k_2) \\ &\quad \geq n[I(V_1;Y_1|U) + R_{k_1}] - nI(V_1;V_2) - nI(V_1;Y_2|V_2,U) \\ &\qquad\qquad\qquad\qquad - n(\epsilon_2' + \epsilon_3' + \epsilon_4') \\ &\quad = nR_1 - n(\epsilon_2' + \epsilon_3' + \epsilon_4') \end{aligned} \tag{23}$$

which gives us (3), as desired.

The equivocation calculation for receiver 2 in this case is similar.

B. Case 2:

The key idea for this case is to employ the *sectioning* technique of [5]. We have to show that the rate-pairs

$$\begin{aligned} R_1 &\leq I(V_1;Y_1|U) - I(V_1;V_2|U) - I(V_1;Y_2|V_2,U) + R_{k_1} \\ R_2 &\leq I(V_2;Y_2|U) - I(V_2;V_1|U) - I(V_2;Y_1|V_1,U) + R_{k_2}, \end{aligned}$$

are achievable. We split the message $W_1 \triangleq (\tilde{W}_1, W_1^{otp})$ and define

$$\begin{aligned} R_{k_1}' &\triangleq I(V_1;Y_2|V_2,U) - \epsilon_1'; \; R_{k_1}^{otp} \triangleq R_{k_1} - R_{k_1}' \\ \tilde{R}_1 &\triangleq I(V_1;Y_1|U) - I(V_1;V_2|U) - \epsilon_1' \end{aligned}$$

Total secure achievable rate for Receiver 1 in this regime consists of $\tilde{W}_1$ at $\tilde{R}_1$ by channel coding techniques, and W_1^{otp} at rate $R_1^{otp} = R_{k_1}^{otp}$.

1) Code Construction: Fix $P(u)$, $P(v_1|u)$, $P(v_2|u)$,$P(x|v_1,v_2)$ and (re-)define

$$R_1' \triangleq I(V_1;Y_2|V_2,U) - \epsilon_1' - R_{k_1}' = 0$$

(R_2' as in Case 1). Randomly generate $\mathbf{u} \sim \prod_{i=1}^n P(u_i)$. The code $\mathcal{C}_1$ for receiver 1 consists of $2^{nR_{k_1}'}$ codebooks. A codebook contains $2^{n\tilde{R}_1}$ bins, each containing $2^{nR^\dagger} = 2^{n[I(V_1;V_2|U)+\epsilon_1']}$ codewords $\mathbf{v}_1 \sim \prod_{i=1}^n P_{V_1|U}(v_{1i}|u_i)$. The notion of *sub-bins* in Fig 2 are replaced by *sections* for user 1 in this case. Each bin is divided evenly into $2^{nR_{k_1}^{otp}}$ sections. If $w_1 = (\tilde{w}_1, w_1^{otp})$, $\tilde{w}_1$ is encoded as the bin index. The pair (w_1^{otp}, k_1^{otp}) picks the section $w_1^{otp} \oplus k_1^{otp}$, as in [5], securing w_1^{otp} by an OTP.

The code $\mathcal{C}_2$ of receiver 2 is identical to that in Case 1. The code-construction for receiver 1 is summarized. Generate a code with $2^{(R_{k_1}'+\tilde{R}_1+R^\dagger)}$ (conditionally) independent sequences $\mathbf{v}_1$ each with probability $P(\mathbf{v}_1|\mathbf{u}) = \prod_{i=1}^n P(v_{1,i}|u_i)$ and label them $\mathbf{v}_1(k_1', \tilde{w}_1, r_1)$ for $k_1' \in \{1, \ldots, 2^{nR_{k_1}'}\}$, $\tilde{w}_1 \in \{1, \ldots, 2^{n\tilde{R}_1}\}$, $r_1 \in \{1, \ldots, 2^{nR^\dagger}\}$. W.l.o.g, $2^{nR_{k_1}'}$, $2^{nR_{k_1}^{otp}}$,$2^{nR_{k_2}}$,$2^{n\tilde{R}_1}$,2^{nR_2}, $2^{nR_2'}$, $2^{nR^\dagger}$ are considered to be integers. The sequence $\mathbf{u}$ and code $\mathcal{C} = \{\mathcal{C}_1, \mathcal{C}_2\}$ is communicated to all parties.

2) Encoding: Given key pair $(k_1, k_2) \in \mathcal{K}_1 \times \mathcal{K}_2$, where $k_1 = (k_1', k_1^{otp})$, the encoder chooses the codebooks $\mathcal{C}_1(k_1')$ and $\mathcal{C}_2(k_2)$. To send $(w_1, w_2) \in \mathcal{W}_1 \times \mathcal{W}_2$, where $w_1 = (\tilde{w}_1, w_1^{otp})$, the encoder chooses the section $w_1^{otp} \oplus k_1^{otp}$ from the bin $\mathcal{C}_1(k_1', \tilde{w}_1)$. It randomly chooses a sub-bin $\mathcal{C}_2(k_2, w_2, s_2)$ from $\mathcal{C}_2(k_2, w_2)$. Since this contains $2^{n[I(V_1;V_2|U)+\epsilon_1']}$ codewords, the number of available pairs $(\mathbf{v}_1, \mathbf{v}_2)$ is $\geq 2^{n[I(V_1;V_2|U)+\epsilon_1']}$, so that, by mutual covering [10], with very high probability, jointly typical pairs exist. One is chosen randomly. Generate $\mathbf{x} \sim \prod_{i=1}^n P_{X|V_1,V_2}(x_i|v_{1i}, v_{2i})$ (*stochastic encoding*) and transmit.

3) Decoding: Receiver 1 knows the codebook $\mathcal{C}_1(k_1')$, and so decodes $\mathbf{v}_1$ from among $\approx 2^{n[I(V_1;Y_1|U)]}$ possibilities by joint typicality with $\mathbf{y}_1$ and $\mathbf{u}$. Clearly $\mathbf{v}_1$, and so $w_1 = (\tilde{w}_1, w_1^{otp})$ can be decoded with low error probability. Receiver 2 proceeds as in Case 1.

4) Error Probability Analysis: For receiver 2, the analysis is the same as in Case 1. For receiver 1, analysis similar to Case 1, but the sub-bin index s_1 is not used.

5) Equivocation for Case 2*:* With the replacements $W_1 \leftarrow \tilde{W}_1$ and $R_1 \leftarrow \tilde{R}_1$, the calculation is similar to Case 1. The message portion w_1^{otp} is secured by OTP, and is perfectly, and hence weakly secure [11].

C. Case 3:

The achievable region similar to Case 2 with roles of the receivers reversed.

D. Case 4:

The proposed achievable region becomes

$$R_1 \leq I(V_1;Y_1|U) - I(V_1;V_2|U) - I(V_1;Y_2|V_2,U) + R_{k_1} \tag{24}$$

$$\begin{aligned} R_2 &\leq I(V_2;Y_2|U) - I(V_2;V_1|U) - I(V_2;Y_1|V_1,U) + R_{k_2} \\ R_1 + R_2 &\leq I(V_1;Y_1|U) + I(V_2;Y_2|U) - I(V_1;V_2|U) \\ &\qquad + \min\{I(U;Y_1), I(U;Y_2)\}. \end{aligned}$$

1) Code Construction: Equations (25) to (28) hold for $t = 1, 2$. Split $W_t \triangleq \left(\tilde{W}_t, W_t^{otp}, W_t^u\right)$ and $\mathcal{K}_t \triangleq \left(\mathcal{K}_t', \mathcal{K}_t^{otp}, \mathcal{K}_t^u\right)$. R_t and R_{k_t} are split as

$$R_t = \left(\tilde{R}_t, R_t^{otp}, R_t^u\right) \text{ s.t } R_t = \tilde{R}_t + R_t^{otp} + R_t^u \tag{25}$$

$$R_{k_t} = \left(R_{k_t}', R_{k_t}^{otp}, R_{k_t}^u\right) \text{ s.t } R_{k_t} = R_{k_t}' + R_{k_t}^{otp} + R_{k_t}^u. \tag{26}$$

Let us first choose

$$\begin{aligned} \tilde{R}_t &= I(V_t;Y_t|U) - I(V_1;V_2|U) - \epsilon_1' \\ R_{k_t}' &= I(V_t;Y_{\bar{t}}|V_{\bar{t}},U) - \epsilon_1' \end{aligned} \tag{27}$$

With this choice, and by (24)

$$R_t - \tilde{R}_t \leq R_{k_t} - R_{k_t}'. \tag{28}$$

Now a pair (R_1^{otp}, R_2^{otp}) is chosen such that

$$\begin{aligned} 0 \leq R_1^{otp} &\leq R_{k_1} - R_{k_1}'; \;\; 0 \leq R_2^{otp} \leq R_{k_2} - R_{k_2}' \\ 0 \leq R_1^{otp} &+ R_2^{otp} \leq I(V_1;V_2|U) + \epsilon_1'. \end{aligned} \tag{29}$$

Let us set

$$R_{k_t}^{otp} = R_t^{otp}, \; t = 1, 2. \tag{30}$$

For $t = 1, 2$, let R_t^u and $R_{k_t}^u$ respectively denote the remaining parts of the message and key rates, which can be empty depending on the choice in (29). Clearly, by (28), $R_t^u \leq R_{k_t}^u$ by our rate choices. We also constrain

$$R_1^u + R_2^u \leq \min\{I(U;Y_1), I(U;Y_2)\}. \tag{31}$$

Generate $2^{n(R_1^u+R_2^u)}$ sequences $\mathbf{u}(l_1, l_2)$, for $t = 1, 2$, $l_t = 0, 1, 2, \ldots, 2^{nR_t^u} - 1$. For each $\mathbf{u}$, generate a satellite code $\mathcal{C}(\mathbf{u}) = \{\mathcal{C}_1(\mathbf{u}), \mathcal{C}_2(\mathbf{u})\}$. For $t = 1, 2$, $\mathcal{C}_t(\mathbf{u})$ has $2^{nR'_{k_t}}$ codebooks, with $\mathbf{v}_t \sim \prod_{i=1}^n P_{V_t|U}(v_{ti}|u_i)$. A codebook is divided into $2^{n\tilde{R}_t}$ bins, each with $2^{nR^\dagger}$ codewords. A bin is divided evenly into $2^{nR_t^{otp}}$ sections. This gives (29), as every pair of sections – one each from $\mathcal{C}_1$ and $\mathcal{C}_2$ – must contain $\geq 2^{n[I(V_1;V_2|U)+\epsilon'_1]}$ $(\mathbf{v}_1, \mathbf{v}_2)$ pairs to satisfy mutual covering [10], and so we require

$$[R^\dagger - R_1^{otp}] + [R^\dagger - R_2^{otp}] \geq I(V_1;V_2|U) + \epsilon'_1,$$

which gives (29) on simplification.

2) Encoding: (w_1^u, w_2^u) is protected by OTP by picking $\mathbf{u}(w_1^u \oplus k_1^u, w_2^u \oplus k_2^u)$. It searches inside the pair of sections $\mathcal{C}_t(\mathbf{u}(w_1^u \oplus k_1^u, w_2^u \oplus k_2^u), k'_t, \tilde{w}_t, w_t^{otp} \oplus k_t^{otp})$ for $t = 1, 2$ for a $(\mathbf{v}_1, \mathbf{v}_2)$ pair that is jointly typical $\in A_{\epsilon'_1}^{(n)}(V_1, V_2|\mathbf{u}(w_1^u \oplus k_1^u, w_2^u \oplus k_2^u))$. By construction, the number of $(\mathbf{v}_1, \mathbf{v}_2)$ pairs $\geq 2^{n[I(V_1;V_2|U)+\epsilon'_1]}$, so a jointly typical pair exists with very high probability, by mutual covering, [10]. The encoder generates and transmits $\mathbf{x} \sim \prod_{i=1}^n P_{X|V_1,V_2}(x_i|v_{1i}, v_{2i})$.

3) Decoding: By (31), $\mathbf{u}$ are generated at a rate $\leq \min\{I(U;Y_1), I(U;Y_2)\}$, so both receivers can decode $\mathbf{u}$ with arbitrarily low error probability error by joint typicality with $\mathbf{y}_t$. *Decoding now proceeds exactly as in previous cases.*

4) Error Probability Analysis: The analysis for both receivers is similar to that for receiver 1 in Case 2.

5) Equivocation Calculation: For $t = 1, 2$, W_t^{otp}, W_t^u are protected by OTPs and are secure. $\tilde{W}_t$ is protected by the scheme developed for $\tilde{W}_1$ of receiver 1 in Case 2.

6) Cases $5, 6, 7$ and Other Cases: In Case 5, individual $\mathbf{v}_1$ sequences can be used to encode a different message, consequently rates $R_1 > I(V_1;Y_1|U)$ attainable and individual rate constraints become active. In Case 6, the same holds for $\mathbf{v}_2$. Details omitted [11].

V. Outer Bound(s)

We state the outer bound(s) without proof.

Theorem 3. *Consider $P \in \pi_{BC}$ such that*

$$U \to V_1 \to X, \; U \to V_2 \to X$$

Let $R_o(P)$ be the set of all $(R_1, R_2) \in \mathbb{R}_+^2$ s.t.

$$\begin{aligned} R_1 \leq \min\Big\{ & \qquad I(V_1;Y_1|U)+ \\ & \min\{R_{k_1} - I(V_1;Y_2|U), I(U;Y_1), I(U;Y_2)\}, \\ & \qquad I(V_1;Y_1|V_2,U)+ \\ & \min\{R_{k_1} - I(V_1;Y_2|V_2,U), I(U;Y_1), I(U;Y_2)\}\Big\} \\ R_2 \leq \min\Big\{ & \qquad I(V_2;Y_2|U)+ \\ & \min\{R_{k_2} - I(V_2;Y_1|U), I(U;Y_1), I(U;Y_2)\}, \\ & \qquad I(V_2;Y_2|V_1,U)+ \\ & \min\{R_{k_2} - I(V_2;Y_1|V_1,U), I(U;Y_1), I(U;Y_2)\}\Big\} \end{aligned}$$

Then the capacity region

$$\mathbb{C}_{BC} \subseteq \cup_{P \in \pi_{BC}: U \to V_t \to X \textit{ for } t=1,2} R_o(P) \tag{32}$$

VI. Conclusion

For confidential message transmission over a two receiver broadcast channel, we have proposed an inner and an outer bound. The achievable schemes proposed use different techniques for different key rates. We plan to consider common messages and the rate-equivocation region in future work.

VII. Acknowledgements

The author would like to express his gratitude to S. R. B. Pillai and B. K. Dey for many detailed discussions and constructive comments.

References

[1] R. Liu, I. Maric, P. Spasojevic, and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2493–2507, June 2008.

[2] J. Xu, Y. Cao, and B. Chen, "Capacity bounds for broadcast channels with confidential messages," *Information Theory, IEEE Transactions on*, vol. 55, no. 10, pp. 4529–4542, Oct 2009.

[3] H. Yamamoto, "Rate-distortion theory for the shannon cipher system," *Information Theory, IEEE Transactions on*, vol. 43, no. 3, pp. 827–835, May 1997.

[4] W. Kang and N. Liu, "Wiretap channel with shared key," in *Information Theory Workshop (ITW), 2010 IEEE*, Aug 2010, pp. 1–5.

[5] E. Ardestanizadeh, M. Franceschetti, T. Javidi, and Y.-H. Kim, "Wiretap channel with secure rate-limited feedback," *Information Theory, IEEE Transactions on*, vol. 55, no. 12, pp. 5353–5361, Dec 2009.

[6] X. Yin, L. Pang, Z. Xue, and Y. Zhou, "Degraded broadcast channels with rate-limited feedback," in *Communications and Networking in China (CHINACOM), 2013 8th International ICST Conference on*, Aug 2013, pp. 911–916.

[7] B. Dai, A. Vinck, Y. Luo, and Z. Zhuang, "Capacity region of non-degraded wiretap channel with noiseless feedback," in *Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on*, July 2012, pp. 244–248.

[8] R. Schaefer, A. Khisti, and H. Boche, "On the use of secret keys in broadcast channels with receiver side information," in *Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on*, May 2014, pp. 1582–1586.

[9] R. Schaefer and A. Khisti, "Secure broadcasting of a common message with independent secret keys," in *Information Sciences and Systems (CISS), 2014 48th Annual Conference on*, March 2014, pp. 1–6.

[10] A. E. Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge University Press, 2011.

[11] K. Iyer, "Broadcast channel with confidential messages and secret keys," *Online at http://www.ee.iitb.ac.in/course/~krishna/krishnaBCCMSKs.pdf*, 2015.

[12] I. Csiszar and J. Korner, *Information Theory: Coding Theorems for Discrete Memoryless Systems.* London, U.K.: Academic, 1981.

VIII. Appendix

A. *Error Probability Analysis for Case* 1

The error probability analysis similar to [1], with the main difference that the the codewords here are quadruply indexed to reflect the codebook index.

W.l.o.g, assume that the transmitter sends the message pair $(w_1 = 1, w_2 = 1)$ and $(s_1 = 1, s_2 = 1)$ and in addition, the secret keys are $(k_1 = 1, k_2 = 1)$. Consider the (encoding) error event $\mathcal{T}$ that the encoder cannot find an appropriately jointly typical pair, i.e. $\forall r_1, r_2$

$$\mathcal{T} \triangleq \{(\mathbf{V}_1(1,1,1,r_1), \mathbf{V}_2(1,1,1,r_2)) \notin A_\epsilon^{(n)}(V_1, V_2|\mathbf{u})\}.$$

Since $R^\dagger > I(V_1; V_2|U)$, by the mutual covering lemma, [10], $P\{T\} \leq \delta$ where $\delta > 0$ is small enough for large n. Let us assume that $(\mathbf{V}_1(1,1,1,1), \mathbf{V}_2(1,1,1,1))$ is chosen for tranmission, and define the event

$$\mathcal{T}^c \triangleq \{(\mathbf{V}_1(1,1,1,1), \mathbf{V}_2(1,1,1,1)) \in A_\epsilon^{(n)}(V_1, V_2|\mathbf{u})\}.$$

The decoding error probability at receiver 1 is then bounded as

$$\begin{aligned} P_{e,1}^{(n)} &\leq P\{\mathcal{T}\} + (1 - P\{\mathcal{T}\})[P\{\bigcap_{s_1,r_1} E_1^c(1,1,s_1,r_1)|\mathcal{T}^c\} \\ &\qquad + \sum_{w_1 \neq 1} \sum_{s_1,r_1} P\{E_1(1,w_1,s_1,r_1)|\mathcal{T}^c\}] \qquad (33) \\ &\leq P\{\mathcal{T}\} + P\{E_1^c(1,1,1,1)|\mathcal{T}^c\} \\ &\qquad + \sum_{w_1 \neq 1} \sum_{s_1,r_1} P\{E_1(1,w_1,s_1,r_1)|\mathcal{T}^c\} \qquad (34) \end{aligned}$$

where

$$E_t(1,w_t,s_t,r_t) = \{(\mathbf{v}_t(1,w_t,s_t,r_t), \mathbf{y}_t) \in A_\epsilon^{(n)}(V_t, Y_t|\mathbf{u})\}.$$

Since $P\{E_1(1,w_1,s_1,r_1)|\mathcal{T}^c\} \leq 2^{-n[I(V_1;Y_1|U)-\epsilon]}$, by using joint typicality lemma [10], the probability of error can be bounded as

$$P_{e,1}^{(n)} \leq \delta + \epsilon + 2^{nR_1} 2^{nR'_1} 2^{nR^\dagger} 2^{-n[I(V_1;Y_1|U)-\epsilon]}. \qquad (35)$$

Thus, if $R_1 + R'_1 + R^\dagger < I(V_1; Y_1|U)$ then, $P_{e,1}^{(n)} < \epsilon_0$ for sufficiently large n. Similar calculations for receiver 2 shows that if $R_2 + R'_2 + R^\dagger < I(V_2; Y_2|U)$, then $P_{e,2}^{(n)} \to 0$.

B. *Equivocation for Case* 2

Replacing $W_1 \leftarrow \tilde{W}_1$ in the expression (4), and by similar steps as in (5) – (19), along with Markov chain $\tilde{W}_1 \to (\mathbf{V}_1, \mathbf{V}_2, \mathbf{U}) \to \mathbf{Y}_2$ which holds for all $K_2 = k_2$, we get in place of (19),

$$\begin{aligned} H(\tilde{W}_1|\mathbf{Y}_2, k_2) \geq & H(\tilde{W}_1, \mathbf{V}_1|\mathbf{V}_2, \mathbf{U}, k_2) \\ & - I(\mathbf{V}_1; \mathbf{Y}_2|\mathbf{V}_2, \mathbf{U}, k_2) - n\epsilon'_3 \qquad (36) \end{aligned}$$

Expansion of the first term gives

$$\begin{aligned} H(\tilde{W}_1, \mathbf{V}_1|\mathbf{V}_2, \mathbf{U}, k_2) = & H(\tilde{W}_1|\mathbf{V}_2, \mathbf{U}, k_2) \\ & + H(\mathbf{V}_1|\mathbf{V}_2, \mathbf{U}, \tilde{W}_1, k_2). \qquad (37) \end{aligned}$$

Notice that

$$H(\tilde{W}_1|\mathbf{V}_2, \mathbf{U}, k_2) = n\tilde{R}_1. \qquad (38)$$

To compute the second term, we note that the total number of entries in the code $\mathcal{C}_1$ is $2^{n[I(V_1;Y_1|U)+R'_{k_1}]}$. Conditioning by the message $\tilde{W}_1$ causes a reduction of possible transmitted $\mathbf{V}_1$ sequences by a factor of $2^{n\tilde{R}_1}$. Furthermore, conditioning by $\mathbf{V}_2$ causes a further reduction by a factor of $2^{I(\mathbf{V}_1;\mathbf{V}_2|\mathbf{U})}$. *Note that, as in Case* 1, *key K_2's value plays no role*. So the remaining number of possible $\mathbf{V}_1$ sequences are

$$\begin{aligned} \tilde{N}_1 &= \frac{2^{n[I(V_1;Y_1|U)+R'_{k_1}]} 2^{-I(\mathbf{V}_1;\mathbf{V}_2|\mathbf{U})}}{2^{n[I(V_1;Y_1|U)-I(V_1;V_2|U)-\epsilon'_1]}} \\ &= \frac{2^{n[I(V_1;Y_1|U)+I(V_1;Y_2|V_2,U)-\epsilon'_1]} 2^{-I(\mathbf{V}_1;\mathbf{V}_2|\mathbf{U})}}{2^{n[I(V_1;Y_1|U)-I(V_1;V_2|U)-\epsilon'_1]}} \end{aligned}$$

Thus

$$\begin{aligned} & H(\mathbf{V}_1|\mathbf{V}_2, \mathbf{U}, \tilde{W}_1, k_2) \\ & \quad = \log \tilde{N}_1 \\ & \quad = nI(V_1; Y_2|U, V_2) + nI(V_1; V_2|U) - I(\mathbf{V}_1; \mathbf{V}_2|\mathbf{U}) \\ & \quad \geq n\left(I(V_1; Y_2|U, V_2) - \epsilon'_2\right) \qquad (39) \end{aligned}$$

where the last inequality follows by [1, Lemma 3]. From (36) – (39), it follows that

$$\begin{aligned} H(\tilde{W}_1|\mathbf{Y}_2, K_2) = & \sum_{k_2 \in \mathcal{K}_2} P(K_2 = k_2) H(\tilde{W}_1|\mathbf{Y}_2, k_2) \\ & \geq n\tilde{R}_1 + nI(V_1; Y_2|U, V_2) \\ & \quad - I(\mathbf{V}_1; \mathbf{Y}_2|\mathbf{V}_2, \mathbf{U}, k_2) - n(\epsilon'_2 + \epsilon'_3) \\ & \geq n\tilde{R}_1 - n\epsilon \end{aligned}$$

where the last inequality again follows from [1, Lemma 3]. The other portion of the message of receiver 1, namely, w_1^{otp} is secured by an OTP, and so is perfectly, and hence weakly secure. Equivocation calculation for receiver 2 in this case is exactly the same as in Case 1.

C. *Case* 3*:*

This is similar to Case 2 with the roles of the receivers reversed. Hence the code structure and the achievable region are similar to Case 2, with the roles reversed.

D. *Cases* $5 - 7$ *and Other Cases:*

The code construction, encoding, decoding, probability of error analysis, and the equivocation calculation are exactly the same in these cases as in Case 4. In Case 5 (resp. 6), the individual rate constraint on R_1 (resp. R_2) also appears, and in Case 7, both individual rate constraints and the sum-rate constraint are active. The achievable region becomes the region described in Theorem 1. For details, see the appendix. *When the key rate mismatch is very large, achievability schemes can be designed using discussed techniques.* We discuss these Cases $5 - 7$ briefly below.

E. Case 5*:*

The code construction, encoding, decoding, probability of error analysis, and the equivocation calculation are exactly the same as this Case 4. The proposed achievable region becomes

$$\begin{aligned}
&R_1 \geq 0, R_2 \geq 0\\
&R_1 \leq I(V_1;Y_1|U) + \min\Big\{R_{k_1} - I(V_1;Y_2|V_2,U)\\
&\qquad\qquad - I(V_1;V_2|U), I(U;Y_1), I(U;Y_2)\Big\}\\
&R_2 \leq I(V_2;Y_2|U) - I(V_2;V_1|U) - I(V_2;Y_1|V_1,U) + R_{k_2}\\
&R_1 + R_2 \leq I(V_1;Y_1|U) + I(V_2;Y_2|U) - I(V_1;V_2|U)\\
&\qquad\qquad + \min\{I(U;Y_1), I(U;Y_2)\} \qquad (40)
\end{aligned}$$

In this regime, since we have $R_{k_1} > I(V_1;V_2|U) + I(V_1;Y_2|V_2,U)$, we can achieve individual rate $R_1 > I(V_1;Y_1|U)$ as follows. We set aside a portion $\hat{R}_{k_1} = I(V_1;Y_2|V_2,U) + I(V_1;V_2|U)$. As in Case 4, we split this into two parts, as $R'_{k_1} = I(V_1;Y_2|V_2,U) - \epsilon'_1$ and a portion $R^{otp}_{k_1} = I(V_1;V_2|U) + \epsilon'_1$. Each section inside $\mathcal{C}_1$ contains exactly one $\mathbf{v}_1$. This ensures that every individual $\mathbf{v}_1$ sequence encodes a different tuple $(\tilde{w}_1, w^{otp}_1)$, and hence a different message, which gives us a rate $I(V_1;Y_1|U)$. Now, (unlike in Case 4), we still have a portion of key at rate $R^u_{k_1} = R_{k_1} - \hat{R}_{k_1} > 0$ which can be used to encrypt messages inside the time-sharing sequence, and so now rates $R_1 > I(V_1;Y_1|U)$ are attainable and so the individual rate constraint for receiver 1 becomes active.

F. Case 6*:*

This is symmetric to Case 5 with the roles of the receivers reversed, and hence the achievable region is obtained from the previous case by appropriate role reversal.

G. Case 7*:*

$$\begin{aligned}
R_{k_1} &> I(V_1;Y_2|V_2,U) + I(V_1;V_2|U)\\
R_{k_2} &> I(V_2;Y_1|V_1,U) + I(V_2;V_1|U) \qquad (41)
\end{aligned}$$

The code construction, encoding, decoding, error probability analysis, and equivocation are exactly the same as in the previous cases $5, 6$. Both individual rate constraints $I(V_i;Y_i|U) + \min\{I(U;Y_1), I(U;Y_2)\}$ for $i = 1, 2$ are active, as also the sum-rate constraint. The achievable region becomes the region described in Theorem 1.

H. Outer Bound Proofs

Consider R_1 in (32). The first term inside the outer minimization corresponds to the receiver 2 attempting to eavesdrop without having decoded its own message, hence no conditioning on V_2. The second term inside the minimization occurs when receiver 2 attempts to decode the message of receiver 1 after decoding its own message, hence the terms are conditioned on V_2. The proof for the first term inside each outer minimization follows closely the associated converse proof in [4]. The proof for the second term inside each outer minimization is more involved, and uses the technique employed in the second outer bound obtained in [1, Section IV-B], where a genie gives receiver 1 the message and key (W_2, K_2), while receiver 2 attempts to evaluate the equivocation with (W_2, K_2) as side information.

We will only prove the bounds for R_1. The corresponding inequality for R_2 follows by symmetry.

1) First Bound: The other receiver attempts to eavesdrop without first decoding its own message/codeword: Unlike in the case of achievability proofs, where we followed the techniques in [1] with appropriate changes due to the presence of secret keys as in [4], here we primarily follow the proof technique in [4], with modifications appropriate to our model. The modifications play an important role in obtaining the second outer bound, as they are suggested by the second bound obtained by [1].

We restate the following inequalities [4, equations (8) and (9)] in terms of our notation where $Y \leftarrow Y_1$ and $Z \leftarrow Y_2$ Note that the inequalities in [4] are themselves taken from [12, p. 314, equation (3.34)]

For ease of reference, we (re-)derive the following equality

$$\begin{aligned}
&H(\mathbf{Y}^n_{1,1}) - H(\mathbf{Y}^n_{2,1}) =\\
&\sum_{i=1}^{n}[H(\mathbf{Y}_{1i}|\mathbf{Y}^n_{1,i+1}, \mathbf{Y}^{i-1}_{2,1}) - H(\mathbf{Y}_{2i}|\mathbf{Y}^n_{1,i+1}, \mathbf{Y}^{i-1}_{2,1})] \quad (42)
\end{aligned}$$

To the LHS of (42) above, we add and subtract $H(\mathbf{Y}_{2,1}, \mathbf{Y}^n_{1,2})$ and get

$$\begin{aligned}
&H(\mathbf{Y}^n_{1,1}) - H(\mathbf{Y}^n_{2,1}) =\\
&H(\mathbf{Y}^n_{1,1}) - H(\mathbf{Y}_{2,1}, \mathbf{Y}^n_{1,2}) + H(\mathbf{Y}_{2,1}, \mathbf{Y}^n_{1,2}) - H(\mathbf{Y}^n_{2,1}) =\\
&\big(H(\mathbf{Y}_{1,1}|\mathbf{Y}^n_{1,2}) + \cancel{H(\mathbf{Y}^n_{1,2})}\big) - \big(H(\mathbf{Y}_{2,1}|\mathbf{Y}^n_{1,2})) + \cancel{H(\mathbf{Y}^n_{1,2})}\big) +\\
&\big(H(\mathbf{Y}^n_{1,2}|\mathbf{Y}_{2,1}) + \cancel{H(\mathbf{Y}_{2,1})}\big) - \big(\cancel{H(\mathbf{Y}_{2,1})} + H(\mathbf{Y}^n_{2,2}|\mathbf{Y}_{2,1})\big)\\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (43)
\end{aligned}$$

thus obtaining

$$\begin{aligned}
&H(\mathbf{Y}^n_{1,1}) - H(\mathbf{Y}^n_{2,1}) =\\
&\big(H(\mathbf{Y}_{1,1}|\mathbf{Y}^n_{1,2}) - H(\mathbf{Y}_{2,1}|\mathbf{Y}^n_{1,2}) +\\
&H(\mathbf{Y}^n_{1,2}|\mathbf{Y}_{2,1}) - H(\mathbf{Y}^n_{2,2}|\mathbf{Y}_{2,1}) \qquad (44)
\end{aligned}$$

Now, we keep the first line as it is, and consider the second line of (44), namely

$$H(\mathbf{Y}^n_{1,2}|\mathbf{Y}_{2,1}) - H(\mathbf{Y}^n_{2,2}|\mathbf{Y}_{2,1}) \qquad (45)$$

Note that this resembles what we started with, namely, the LHS of (42) with the changes that we have an extra conditioning on $\mathbf{Y}_{2,1}$, and $\mathbf{Y}^n_{1,1} \leftarrow \mathbf{Y}^n_{1,2}$ and $\mathbf{Y}^n_{2,1} \leftarrow \mathbf{Y}^n_{2,2}$. So, in analogy with (44), we can write

$$\begin{aligned}
&H(\mathbf{Y}^n_{1,2}|\mathbf{Y}_{2,1}) - H(\mathbf{Y}^n_{2,2}|\mathbf{Y}_{2,1}) =\\
&\big(H(\mathbf{Y}_{1,2}|\mathbf{Y}^n_{1,3}, \mathbf{Y}_{2,1}) - H(\mathbf{Y}_{2,2}|\mathbf{Y}^n_{1,3}, \mathbf{Y}_{2,1}) +\\
&H(\mathbf{Y}^n_{1,3}|\mathbf{Y}_{2,2}, \mathbf{Y}_{2,1}) - H(\mathbf{Y}^n_{2,3}|\mathbf{Y}_{2,2}, \mathbf{Y}_{2,1}) \qquad (46)
\end{aligned}$$

As before, we leave the first line as it is, and expand the second line, namely

$$H(\mathbf{Y}^n_{1,3}|\mathbf{Y}_{2,2}, \mathbf{Y}_{2,1}) - H(\mathbf{Y}^n_{2,3}|\mathbf{Y}_{2,2}, \mathbf{Y}_{2,1}) \qquad (47)$$

We proceed iteratively.

Note that

$$\left.[H(\mathbf{Y}_{1i}|\mathbf{Y}_{1,i+1}^n, \mathbf{Y}_{2,1}^{i-1}) - H(\mathbf{Y}_{2i}|\mathbf{Y}_{1,i+1}^n, \mathbf{Y}_{2,1}^{i-1})]\right|_{i=1} \\ = \big(H(\mathbf{Y}_{1,1}|\mathbf{Y}_{1,2}^n) - H(\mathbf{Y}_{2,1}|\mathbf{Y}_{1,2}^n)\big) \quad (48)$$

which was the first line on the RHS of (44).

Similarly

$$\left.[H(\mathbf{Y}_{1i}|\mathbf{Y}_{1,i+1}^n, \mathbf{Y}_{2,1}^{i-1}) - H(\mathbf{Y}_{2i}|\mathbf{Y}_{1,i+1}^n, \mathbf{Y}_{2,1}^{i-1})]\right|_{i=2} \\ = \big(H(\mathbf{Y}_{1,2}|\mathbf{Y}_{1,3}^n, \mathbf{Y}_{2,1}) - H(\mathbf{Y}_{2,2}|\mathbf{Y}_{1,3}^n, \mathbf{Y}_{2,1})\big) \quad (49)$$

which was the first line on the RHS of (46).

Iterating, we finally expand the RHS as

$$\sum_{i=1}^{n}[H(\mathbf{Y}_{1i}|\mathbf{Y}_{1,i+1}^n, \mathbf{Y}_{2,1}^{i-1}) - H(\mathbf{Y}_{2i}|\mathbf{Y}_{1,i+1}^n, \mathbf{Y}_{2,1}^{i-1})]$$

to obtain

$$H(\mathbf{Y}_{1,1}^n) - H(\mathbf{Y}_{2,1}^n) = \\ \sum_{i=1}^{n}[H(\mathbf{Y}_{1i}|\mathbf{Y}_{1,i+1}^n, \mathbf{Y}_{2,1}^{i-1}) - H(\mathbf{Y}_{2i}|\mathbf{Y}_{1,i+1}^n, \mathbf{Y}_{2,1}^{i-1})] \quad (50)$$

which is the same as (42), which was to be proved.

We can also derive the following equality analogously.

$$H(\mathbf{Y}_{1,1}^n|W_1, K_1) - H(\mathbf{Y}_{2,1}^n|W_1, K_1) = \\ \sum_{i=1}^{n}[H(\mathbf{Y}_{1i}|\mathbf{Y}_{1,i+1}^n, \mathbf{Y}_{2,1}^{i-1}, W_1, K_1) \\ - H(\mathbf{Y}_{2i}|\mathbf{Y}_{1,i+1}^n, \mathbf{Y}_{2,1}^{i-1}, W_1, K_1)].$$

We define auxiliary RVs:

$$U_i \triangleq (\mathbf{Y}_{1,i+1}^n, \mathbf{Y}_{2,1}^{i-1}) \quad (51)$$

We also define a time-sharing RV Q, which is independent of everything else, and is uniform on the set $\{1, 2, 3, \dots, n\}$. With this definition of U and Q, we further define the following RVs

$$U \triangleq (U_Q, Q),\ V_1 \triangleq (U, W_1, K_1) \\ X \triangleq X_Q,\ Y \triangleq Y_Q,\ Z \triangleq Z_Q$$

Note that the Markov chain condition $U \to V_1 \to X \to (Y_1, Y_2)$ is satisfied.

Using the above equations and the definitions of the auxiliary random variables, there exist real numbers t_1 and t_2 s.t.

$$\frac{1}{n}H(\mathbf{Y}_{1,1}^n) = H(Y_1|U) + t_1 \quad (52)$$

$$\frac{1}{n}H(\mathbf{Y}_{2,1}^n) = H(Y_2|U) + t_1 \quad (53)$$

and also

$$\frac{1}{n}H(\mathbf{Y}_{1,1}^n|W_1, K_1) = H(Y_1|V_1) + t_2 = H(Y_1|U, V_1) + t_2 \quad (54)$$

$$\frac{1}{n}H(\mathbf{Y}_{2,1}^n|W_1, K_1) = H(Y_2|V_1) + t_2 = H(Y_2|U, V_1) + t_2 \quad (55)$$

where the last equality in both equations (54) and (55) above follows due to the Markov Chain condition $U \to V_1 \to Y_1$ and $U \to V_1 \to Y_2$ where

$$0 \le t_1 \le \min\{I(U; Y_1), I(U; Y_2)\} \quad (56)$$

$$0 \le t_2 \le \min\{I(V_1; Y_1), I(V_1; Y_2)\} \quad (57)$$

Since the code satisfies the information leakage constraint, namely

$$\begin{aligned} n\mu &\ge I(W_1; \mathbf{Y}_{2,1}^n) \\ &= I(W_1, K_1; \mathbf{Y}_{2,1}^n) - I(K_1; \mathbf{Y}_{2,1}^n|W_1) \\ &= H(\mathbf{Y}_{2,1}^n) - H(\mathbf{Y}_{2,1}^n|W_1, K_1) \\ &\qquad - H(K_1|W_1) + H(K_1|\mathbf{Y}_{2,1}^n, W_1) \\ &\ge H(\mathbf{Y}_{2,1}^n) - H(\mathbf{Y}_{2,1}^n|W_1, K_1) - H(K_1|W_1) \\ &\overset{\because K_1 \perp\!\!\!\perp W_1}{=} H(\mathbf{Y}_{2,1}^n) - H(\mathbf{Y}_{2,1}^n|W_1, K_1) - H(K_1) \\ &= H(\mathbf{Y}_{2,1}^n) - H(\mathbf{Y}_{2,1}^n|W_1, K_1) - nR_{k_1} \\ &= n(H(Y_2|U) + t_1 - H(Y_2|V_1) - t_2 - R_{k_1}) \\ &\overset{\because U \to V_1 \to Y_2}{=} n(H(Y_2|U) + t_1 - H(Y_2|V_1, U) - t_2 - R_{k_1}) \\ &= n(I(V_1; Y_2|U) + t_1 - t_2 - R_{k_1}) \end{aligned} \quad (58)$$

Therefore

$$\cancel{n}\mu \ge \cancel{n}(I(V_1; Y_2|U) + t_1 - t_2 - R_{k_1}) \\ \implies t_1 - t_2 \le R_{k_1} - I(V_1; Y_2|U) + \mu \quad (59)$$

We also have

$$t_1 - t_2 \le t_1 \le min\{I(U; Y_1), I(U; Y_2)\} \quad (60)$$

Thus, from (59) and (60), we have

$$t_1 - t_2 \le min\{R_{k_1} - I(V_1; Y_2|U) + \mu, I(U; Y_1), I(U; Y_2)\} \quad (61)$$

Now

$$\begin{aligned} |\mathcal{W}_1| &= H(W_1) \overset{W_1 \perp\!\!\!\perp K_1}{=} H(W_1|K_1) \\ &= H(W_1|\mathbf{Y}_{1,1}^n, K_1) + I(W_1; \mathbf{Y}_{1,1}^n|K_1) \\ &\overset{Fano}{\le} I(W_1; \mathbf{Y}_{1,1}^n|K_1) + n\epsilon_n \\ &\le I(W_1, K_1; \mathbf{Y}_{1,1}^n) + n\epsilon_n \\ &= H(\mathbf{Y}_{1,1}^n) - H(\mathbf{Y}_{1,1}^n|W_1, K_1) + n\epsilon_n \\ &= n\big[H(Y_1|U) + t_1 - H(Y_1|V_1) - t_2 + \epsilon_n\big] \\ &\overset{U \to V_1 \to Y_1}{=} n\big[H(Y_1|U) + t_1 - H(Y_1|V_1, U) - t_2 + \epsilon_n\big] \\ &= n\big[I(Y_1; V_1|U) + (t_1 - t_2) + \epsilon_n\big] \\ &\le n\big[I(Y_1; V_1|U) + \min\{R_{k_1} - I(V_1; Y_2|U) + \mu, \\ &\qquad\qquad I(U; Y_1), I(U; Y_2)\} + \epsilon_n\big] \end{aligned} \quad (62)$$

Now

$$H(W_1) = nR_1 \quad (63)$$

Equations (62) and (63) together imply that

$$\cancel{n}R_1 \leq \cancel{n}\Big(I(Y_1;V_1|U) + \min\Big\{R_{k_1} - I(V_1;Y_2|U) + \mu, I(U;Y_1), I(U;Y_2)\Big\} + \epsilon_n\Big) \tag{64}$$

which gives (as μ and ϵ_n can be made arbitrarily small)

$$R_1 \leq I(Y_1;V_1|U) + \min\{R_{k_1} - I(V_1;Y_2|U), I(U;Y_1), I(U;Y_2)\} \tag{65}$$

which is the first term inside the outer minimization in (32)

2) Second Bound: Where the other receiver decodes its own codeword before eavesdropping: The bound is obtained by considering that:

- a genie gives receiver 1 message-key pair (W_2, K_2)
- receiver 2 attempts to evaluate the equivocation with (W_2, K_2) as side information

This is inspired by [1]. We rewrite the equations/inequalities used in [4, Equations (18) and (22)] employing these insights.

Consider the inequality (note that this follows very closely the corresponding chain of inequalities in [4] with the crucial change of additional conditioning RVs (W_2, K_2)

$$\begin{aligned} |\mathcal{W}_1| &= H(W_1) \\ &= H(W_1|K_1) && \text{Since } W_1 \perp\!\!\!\perp K_1 \\ &= H(W_1|K_1, W_2, K_2) && \text{Since } (W_1, K_1) \perp\!\!\!\perp (W_2, K_2) \end{aligned} \tag{66}$$

We interpret the last equation above, (66), as a genie giving (W_2, K_2) to receiver 1. We continue

$$\begin{aligned} H(W_1) &= H(W_1|K_1, W_2, K_2) \\ &= H(W_1|K_1, W_2, K_2) - H(W_1|\mathbf{Y}_{1,1}^n, K_1, W_2, K_2) \\ &\qquad + H(W_1|\mathbf{Y}_{1,1}^n, K_1, W_2, K_2) \\ &= I(W_1; \mathbf{Y}_{1,1}^n|K_1, W_2, K_2) \\ &\qquad + H(W_1|\mathbf{Y}_{1,1}^n, K_1, W_2, K_2) \\ &\leq I(W_1; \mathbf{Y}_{1,1}^n|K_1, W_2, K_2) + H(W_1|\mathbf{Y}_{1,1}^n, K_1) \\ &\leq I(W_1; \mathbf{Y}_{1,1}^n|K_1, W_2, K_2) + n\epsilon_n \qquad \text{by Fano} \end{aligned} \tag{67}$$

$$\begin{aligned} &\leq I(W_1, K_1; \mathbf{Y}_{1,1}^n|W_2, K_2) + n\epsilon_n \\ &= H(\mathbf{Y}_{1,1}^n|W_2, K_2) - H(\mathbf{Y}_{1,1}^n|W_1, K_1, W_2, K_2) \\ &\qquad + n\epsilon_n \end{aligned}$$

Analogously to (52) to (53), (54) to (55) it can be shown that there real numbers T_1 and T_2 s.t.

$$\frac{1}{n}H(\mathbf{Y}_{1,1}^n|W_2, K_2) = H(Y_1|V_2) + T_1 \tag{68}$$

$$\frac{1}{n}H(\mathbf{Y}_{2,1}^n|W_2, K_2) = H(Y_2|V_2) + T_1 \tag{69}$$

and also

$$\frac{1}{n}H(\mathbf{Y}_{1,1}^n|W_2, K_2, W_1, K_1) = H(Y_1|V_2, V_1) + T_2 \tag{70}$$

$$\frac{1}{n}H(\mathbf{Y}_{2,1}^n|W_2, K_2, W_1, K_1) = H(Y_2|V_2, V_1) + T_2 \tag{71}$$

We finally have

$$H(W_1) \leq n(H(Y_1|V_2) + T_1 - H(Y_1|V_2, V_1) - T_2 + \epsilon_n)$$

Note that, since $U \to V_2 \to X \to (Y_1, Y_2)$ Markov chain is (trivially) satisfied. So we can rewrite $H(Y_1|V_2) = H(Y_1|V_2, U)$ and $H(Y_1|V_2, V_1) = H(Y_1|V_2, V_1, U)$ due to the appropriate Markov chain conditions. So, now we have

$$\begin{aligned} H(W_1) &\leq n(H(Y_1|V_2, U) + T_1 - H(Y_1|V_2, V_1, U) - T_2 + \epsilon_n) \\ &= n(I(V_1; Y_1|V_2, U) + T_1 - T_2 + \epsilon_n). \end{aligned} \tag{72}$$

Now, since, $H(W_1) = nR_1$, substituting in (72), we get

$$\cancel{n}R_1 \leq \cancel{n}(I(V_1; Y_1|V_2, U) + T_1 - T_2 + \epsilon_n). \tag{73}$$

Since the information leakage condition (58) is satisfied, and the receiver 2 attempts to evaluate the equivocation with (W_2, K_2) as side information, we can write

$$n\mu \geq I(W_1; \mathbf{Y}_{2,1}^n|W_2, K_2) \tag{74}$$

$$\begin{aligned} &= I(W_1, K_1; \mathbf{Y}_{2,1}^n|W_2, K_2) - I(K_1; \mathbf{Y}_{2,1}^n|W_1, W_2, K_2) \\ &= \big(H(\mathbf{Y}_{2,1}^n|W_2, K_2) - H(\mathbf{Y}_{2,1}^n|W_1, K_1, W_2, K_2)\big) \\ &\quad - \big(H(K_1|W_2, K_2, W_1) + H(K_1|\mathbf{Y}_{2,1}^n, W_2, K_2, W_1)\big) \\ &\geq H(\mathbf{Y}_{2,1}^n|W_2, K_2) - H(\mathbf{Y}_{2,1}^n|W_1, K_1, W_2, K_2) \\ &\qquad - H(K_1|W_2, K_2, W_1). \end{aligned} \tag{75}$$

Now we simplify the last term in (75) above in two steps as

$$\begin{aligned} H(K_1|W_2, K_2, W_1) &= H(K_1|W_1) \\ &\quad \text{Since } (W_2, K_2) \perp\!\!\!\perp (W_1, K_1) \\ &= H(K_1) \\ &\quad \text{Since } K_1 \perp\!\!\!\perp W_1. \end{aligned} \tag{76}$$

Inequalities (75) and (76) together imply that

$$\begin{aligned} n\mu &\geq H(\mathbf{Y}_{2,1}^n|W_2, K_2) - H(\mathbf{Y}_{2,1}^n|W_1, K_1, W_2, K_2) - H(K_1) \\ &= n(H(Y_2|V_2) + T_1 - H(Y_2|V_2, V_1) - T_2 - R_{k_1}) \end{aligned} \tag{77}$$

Applying the Markov Chain conditions gives:

$$\begin{aligned} &\cancel{n}\mu \geq \cancel{n}(H(Y_2|V_2, U) + T_1 - H(Y_2|V_2, V_1, U) - T_2 - nR_{k_1}) \\ \implies &\mu \geq I(V_1; Y_2|V_2, U) + T_1 - T_2 - nR_{k_1} \end{aligned} \tag{78}$$

Rearranging the above gives:

$$T_1 - T_2 \leq R_{k_1} - I(V_1; Y_2|V_2, U) + \mu \tag{79}$$

We also have

$$T_1 - T_2 \leq min\{I(U; Y_1), I(U; Y_2)\} \tag{80}$$

Inequalities (79) and (80) together give

$$T_1 - T_2 \leq \min\{R_{k_1} - I(V_1; Y_2|V_2, U) + \mu, I(U; Y_1), I(U; Y_2)\} \tag{81}$$

On substituting (81) into the inequality (73), we get

$$\begin{aligned} R_1 \leq\ &I(V_1; Y_1|V_2, U) + \\ &\min\{R_{k_1} - I(V_1; Y_2|V_2, U) + \mu, I(U; Y_1), I(U; Y_2)\} \end{aligned} \tag{82}$$

which was to be proved.

3) Outer Bounds on Sum-Rates: Now, following [1] we derive outer bounds on the sum-rates $R_1 + R_2$ based on the individual rate outer bounds.

We define

$$\begin{aligned} \triangle_1 &\triangleq I(V_1; Y_1|U)+ \\ &\quad \min\{R_{k_1} - I(V_1; Y_2|U), I(U; Y_1), I(U; Y_2)\} \qquad (83) \\ \triangle_2 &\triangleq I(V_2; Y_2|U)+ \\ &\quad \min\{R_{k_2} - I(V_2; Y_1|U), I(U; Y_1), I(U; Y_2)\} \qquad (84) \\ \Theta_1 &\triangleq I(V_1; Y_1|V_2, U)+ \qquad (85) \\ &\quad \min\{R_{k_1} - I(V_1; Y_2|V_2, U), I(U; Y_1), I(U; Y_2)\}\} \\ \Theta_2 &\triangleq I(V_2; Y_2|V_1, U)+ \qquad (86) \\ &\quad \min\{R_{k_2} - I(V_2; Y_1|V_1, U), I(U; Y_1), I(U; Y_2)\}\} \end{aligned}$$

The bounds on R_1 and R_2 imply the following bounds on the sum-rate

$$R_1 + R_2 \leq \triangle_1 + \triangle_2 \qquad (87)$$

$$R_1 + R_2 \leq \Theta_1 + \Theta_2 \qquad (88)$$

$$R_1 + R_2 \leq \min\{\triangle_1 + \Theta_2, \triangle_2 + \Theta_1\} \qquad (89)$$