

# Fading Cognitive Multiple-Access Channels With Confidential Messages

Ruoheng Liu, Yingbin Liang and H. Vincent Poor

## Abstract

The fading cognitive multiple-access channel with confidential messages (CMAC-CM) is investigated, in which two users attempt to transmit common information to a destination and user 1 also has confidential information intended for the destination. User 1 views user 2 as an eavesdropper and wishes to keep its confidential information as secret as possible from user 2. The multiple-access channel (both the user-to-user channel and the user-to-destination channel) is corrupted by multiplicative fading gain coefficients in addition to additive white Gaussian noise. The channel state information (CSI) is assumed to be known at both the users and the destination. A parallel CMAC-CM with independent subchannels is first studied. The secrecy capacity region of the parallel CMAC-CM is established, which yields the secrecy capacity region of the parallel CMAC-CM with degraded subchannels. Next, the secrecy capacity region is established for the parallel Gaussian CMAC-CM, which is used to study the fading CMAC-CM. When both users know the CSI, they can dynamically change their transmission powers with the channel realization to achieve the optimal performance. The closed-form power allocation function that achieves every boundary point of the secrecy capacity region is derived.

## Index Terms

Secure communication, fading channel, multiple-access channel, equivocation, secrecy capacity.

## I. INTRODUCTION

Wireless transmissions lack physical boundaries and so any adversary within range can receive them. Thus, security is one of the most important issues in wireless communications. One approach to security involves applying encryption algorithms to make messages unintelligible to adversaries. Unfortunately, these security methods are often designed without consideration of the specific properties of wireless networks. More specifically, encryption

The work of R. Liu and H. V. Poor was supported by the National Science Foundation under Grant CNS-09-05398, and by the Air Force Office of Scientific Research under Grant FA9550-08-1-0480, and the work of Y. Liang was supported by a National Science Foundation CAREER Award under Grant CCF-08-46028 and under Grant CCF-09-15772.

Ruoheng Liu and H. Vincent Poor are with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA (email: {rliu, poor}@princeton.edu).

Yingbin Liang is with the Department of Electrical Engineering and Computer Science, Syracuse University, Syracuse, NY 13244, USA (email: yliang06@syr.edu).

methods tend to be layer-specific and ignore the most fundamental communication layer, i.e., the physical-layer, whereby devices communicate through the encoding and modulation of information into waveforms.

The first study of secure communication via physical layer approaches was captured by a basic wiretap channel introduced by Wyner in [1]. In this model, a single source-destination communication link is eavesdropped upon by an eavesdropper via a degraded channel. The source node wishes to send confidential information to the destination node in a reliable manner as well as to keep the eavesdropper as ignorant of this information as possible. The performance measure of interest is the secrecy capacity which characterizes the largest possible communication rate from the source node to the destination node with the eavesdropper obtaining no source information. Wyner's formulation was generalized by Csiszár and Körner who determined the secrecy capacity region of a more general model referred to as the broadcast channel with confidential messages (BCC) [2].

More recently, multi-terminal communication with confidential messages has been studied intensively. (See [3] for a recent survey of progress in this area.) Among these studies, a generalization of both the wiretap channel and the classical multiple-access channel (MAC) was studied in [4], in which each user also receives channel outputs, and hence may obtain the confidential information sent by the other user from the channel output it receives. In this communication scenario, each user views the other user as an eavesdropper, and wishes to keep its confidential information as secret as possible from the other user. The authors of [4] investigated the rate-equivocation region and secrecy capacity region for this channel. Some other related studies on secure communication over multiple access channels can be found in [5]–[7].

Fading has traditionally been considered to be an obstacle to providing reliable wireless communication. However, over the past decade, it has been demonstrated that fading can help improve capacity, reliability, and confidentiality of wireless networks. The impact of fading on secure communication was studied in, e.g., [8]–[10]. More specifically, [8] studied the secrecy capacity of ergodic fading BCCs when the channel state information (CSI) is known at all communicating nodes; [9] considered the ergodic scenario of fading wiretap channel in which the transmitter has no CSI about the eavesdropper channel; and [10] studied the outage preference of secure communication over wireless channels, in which the transmitter has no CSI about either the legitimate receiver's channel or the eavesdropper's channel.

In this paper, we investigate the fading cognitive multiple-access channel with both common and confidential messages, a problem which is inspired by the studies of secure communication over MACs in [4]. In our communication scenario, we assume that two users (users 1 and 2) have common information, while user 1 has confidential information intended for a destination and treats user 2 as an eavesdropper. Hence, user 1 wishes to keep its confidential messages as secret as possible from user 2. We refer to this model as the cognitive MAC with one confidential message (CMAC-CM); (see Fig. 1.(a)), because this channel also models cognitive communication

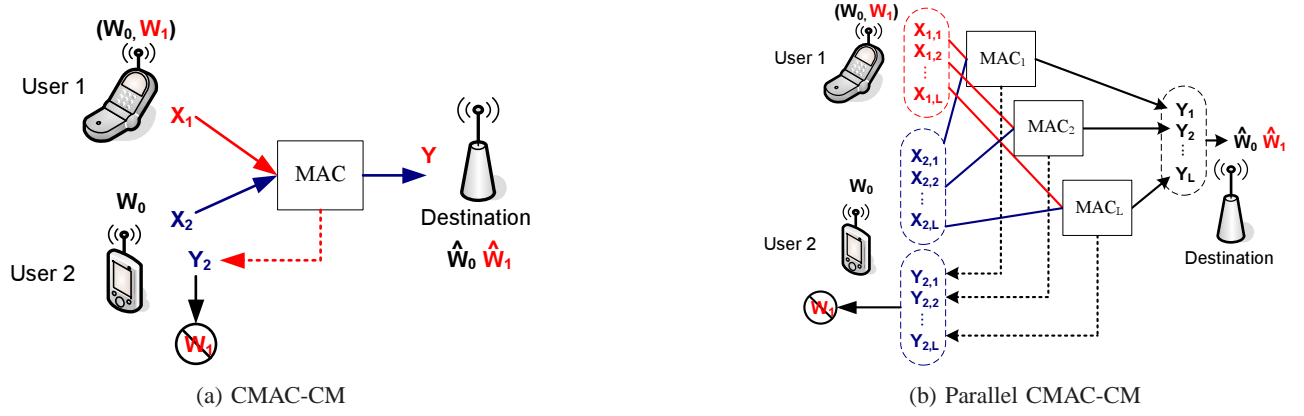


Fig. 1. Cognitive multiple-access channel with confidential messages.

in which the secondary user (user 1) helps the primary user (user 2) to send a common message  $W_0$ , and also has a confidential message  $W_1$  intended for the destination, which needs to be kept secret from the primary user. Furthermore, we consider the situation in which both the user-to-user and the user-to-destination channels are corrupted by multiplicative fading gain coefficients in addition to additive white Gaussian noise. The fading CMAC-CM model captures the basic time-varying and superposition properties of wireless channels, and thus, understanding this channel plays an important role in solving security issue in wireless application. For the fading CMAC-CM, we assume that the fading gain coefficients are stationary and ergodic over time and that the CSI is known at both users and the destination. Note that knowledge of the user-to-destination CSI is necessary in order to cooperatively transmit the common message, and thus should be provided through state feedback from the destination terminal to the user terminals. Knowledge of CSI between the user terminals can be obtained via the reciprocity property of those channels. Users are motivated to do so in order to enable better cooperation for sending the common message.

To solve the fading CMAC-CM problem, we first consider a general information-theoretic model, i.e., the parallel MAC with  $L$  independent subchannels. As shown in Fig. 1.(b), the two users communicate with the destination over  $L$  parallel links and each of the  $L$  links is eavesdropped upon by user 2. We establish the secrecy capacity region for the parallel CMAC-CM. In particular, we provide a converse proof to show that having independent inputs for each subchannel is optimal to achieve the secrecy capacity region. The secrecy capacity region of the parallel CMAC-CM further gives the secrecy capacity region of the parallel CMAC-CM with degraded subchannels. Next, we consider the parallel Gaussian CMAC-CM, which is an example parallel CMAC-CM with degraded subchannels. Based on the maximum-entropy theorem [11] and the extremal inequality [12], we show that the secrecy capacity region of the parallel Gaussian CMAC-CM is achievable by using jointly Gaussian inputs and optimizing power allocations at two users among the parallel subchannels. We then apply this result to investigate the fading CMAC-CM. We study the ergodic performance, where no delay constraint on message transmission is assumed and the secrecy

capacity region is averaged over all channel states. In fact, the fading CMAC-CM can be viewed as the parallel Gaussian CMAC-CM with each fading state corresponding to one subchannel. Hence, the secrecy capacity region of the parallel Gaussian CMAC-CM applies to the fading CMAC-CM. Since both users know the CSI, users can dynamically change their transmission powers with the channel realization to achieve the optimal performance. The optimal power allocation that achieves every boundary point of the secrecy capacity region can be characterized as a solution to a non-convex problem. The Karush-Kuhn-Tucker (KKT) conditions (as necessary conditions) greatly facilitate exploitation of the specific structure of the problem, and enable us to obtain a closed-form solution for the optimal power allocation strategy for the two users.

The remainder of this paper is organized as follows. We first study the parallel CMAC-CM with independent subchannels and its special case of the parallel CMAC-CM with degraded subchannels in Section II. Next, we investigate the secrecy capacity region of the parallel Gaussian CMAC-CM in Section III and the ergodic performance of the fading CMAC-CM in Section IV. We then provide some numerical examples in Section V. Finally, we summarize our results in Section VI.

## II. PARALLEL CMAC-CM

### A. Channel Model

We consider the discrete memoryless parallel CMAC-CM with  $L$  independent subchannels (see Fig. 1.(b)). Each subchannel is assumed to connect users 1 and 2 to the destination, and user 2 can also receive the channel output from each subchannel, and hence may obtain information sent by user 1. The channel transition probability distribution is given by

$$p(y_{[1,L]}, y_{2,[1,L]} | x_{1,[1,L]}, x_{2,[1,L]}) = \prod_{j=1}^L p(y_j, y_{2,j} | x_{1,j}, x_{2,j}), \quad (1)$$

where  $y_{[1,L]} := (y_1, \dots, y_L)$ .

In this model, a common message  $W_0$  is known to both the primary user (user 2) and the secondary user (user 1), and hence both users cooperate to transmit  $W_0$  to the destination. Moreover, the secondary user (user 1) also has confidential message  $W_1$  intended for the destination. User 1 views user 2 as an eavesdropper and wishes to keep its confidential information as secret as possible from user 2. In this paper, we focus on the case in which perfect secrecy is achieved, i.e., user 2 should not obtain any information about the message  $W_1$ . More formally, this condition is characterized by (e.g., see [1], [2], [4]):

$$\frac{1}{n} I(W_1; Y_2^n, X_2^n, W_0) \rightarrow 0 \quad (2)$$

where  $X_2^n := (X_{2,1}, \dots, X_{2,n})$  and  $Y_2^n := (Y_{2,1}, \dots, Y_{2,n})$  are the input and output sequences of user 2, respectively,

and the limit is taken as the block length  $n \rightarrow \infty$ . The goal is to characterize the *secrecy capacity region*  $\mathcal{C}_s$  that contains rate pairs achievable by some coding scheme (more detailed definitions for the rates of the messages and encoding and decoding schemes can be found in [4]).

### B. Secrecy Capacity Region of the Parallel CMAC-CM

For the parallel CMAC-CM, we obtain the following secrecy capacity region.

*Theorem 1:* For the parallel CMAC-CM, the secrecy capacity region is given by

$$\mathcal{C}_s^{[P]} = \bigcup_{\substack{\prod_j p(q_j, x_{2,j}) p(u_j | q_j) p(x_{1,j} | u_j) \\ p(y_j, y_{2,j} | x_{1,j}, x_{2,j})}} \left\{ \begin{array}{l} (R_0, R_1) : \\ R_0 \geq 0, R_1 \geq 0; \\ R_1 \leq \sum_{j=1}^L [I(U_j; Y_j | X_{2,j}, Q_j) - I(U_j; Y_{2,j} | X_{2,j}, Q_j)] \\ R_0 \leq \sum_{j=1}^L I(Q_j, X_{2,j}; Y_j) \end{array} \right\} \quad (3)$$

where  $Q_j$  and  $U_j$ 's are auxiliary random variables, and  $Q_j$  can be chosen to be a deterministic function of  $U_j$  for  $j = 1, \dots, L$ .

*Proof:* See Appendix A. ■

Theorem 1 implies that having independent inputs for each subchannel is optimal. This fact does not follow directly from the single-letter result on the secrecy capacity region of the CMAC-CM given in [4]. Hence, a converse proof is needed, which is provided in Appendix A.

### C. Parallel CMAC-CM with Degraded Subchannels

We consider the parallel CMAC-CM with degraded subchannels, in which each subchannel is either degraded such that given the input of user 2, the output at user 2 is a conditionally degraded version of the output at the destination, or reversely degraded such that given the input of user 2, the output at the destination is a conditionally degraded version of the output at user 2.

Following [4], we define the conditionally degraded subchannels as follows. Let  $\mathcal{A}$  denote the index set that includes all indices of subchannels such that given  $x_{2,j}$ , the output at user 2 is a conditionally degraded version of the output at the destination, i.e., for  $j \in \mathcal{A}$ ,

$$p(y_j, y_{2,j} | x_{1,j}, x_{2,j}) = p(y_j | x_{1,j}, x_{2,j}) p(y_{2,j} | y_j, x_{2,j}). \quad (4)$$

We further define  $\bar{\mathcal{A}}$  to be the complement of the set  $\mathcal{A}$ , and  $\bar{\mathcal{A}}$  includes all indices of subchannels such that given  $x_{2,j}$ , the output at the destination is a conditionally degraded version of the output at user 2, i.e., for  $j \in \bar{\mathcal{A}}$ ,

$$p(y_j, y_{2,j} | x_{1,j}, x_{2,j}) = p(y_{2,j} | x_{1,j}, x_{2,j}) p(y_j | y_{2,j}, x_{2,j}). \quad (5)$$

Hence, the channel transition probability distribution is given by

$$\begin{aligned}
& p(y_{[1,L]}, y_{2,[1,L]} | x_{1,[1,L]}, x_{2,[1,L]}) \\
&= \prod_{j \in \mathcal{A}} p(y_j | x_{1,j}, x_{2,j}) p(y_{2,j} | y_j, x_{2,j}) \prod_{j \in \bar{\mathcal{A}}} p(y_{2,j} | x_{1,j}, x_{2,j}) p(y_j | y_{2,j}, x_{2,j}). \tag{6}
\end{aligned}$$

For the parallel CMAC-CM with degraded subchannels, we apply Theorem 1 and obtain the following secrecy capacity region.

*Theorem 2:* For the parallel CMAC-CM with degraded subchannels, the secrecy capacity region is given by

$$\mathcal{C}_s^{[D]} = \bigcup_{\substack{\prod_j p(q_j, x_{2,j}) p(x_{1,j} | q_j) \\ p(y_j, y_{2,j} | x_{1,j}, x_{2,j})}} \left\{ \begin{array}{l} (R_0, R_1) : \\ R_0 \geq 0, R_1 \geq 0; \\ R_1 \leq \sum_{j \in \mathcal{A}} [I(X_{1,j}; Y_j | X_{2,j}, Q_j) - I(X_{1,j}; Y_{2,j} | X_{2,j}, Q_j)] \\ R_0 \leq \sum_{j \in \mathcal{A}} I(Q_j, X_{2,j}; Y_j) + \sum_{j \in \bar{\mathcal{A}}} I(X_{1,j}, X_{2,j}; Y_j) \end{array} \right\} \tag{7}$$

where  $Q_j$ , for  $j = 1, \dots, L$ , are auxiliary random variables that satisfy the Markov chain relationship

$$Q_j \rightarrow (X_{1,j}, X_{2,j}) \rightarrow (Y_j, Y_{2,j}). \tag{8}$$

*Proof:* See Appendix B. ■

It can be seen that the common message  $W_0$  is sent over all subchannels, and the confidential message  $W_1$  of user 1 is sent only over the subchannels for which the output at user 2 is a *conditionally degraded* version of the output at the destination. Furthermore, user 1 sends the common message  $W_0$  and the confidential message  $W_1$  by using superposition encoding.

### III. PARALLEL GAUSSIAN CMAC-CM

#### A. Channel Model

In this section, we consider the parallel Gaussian CMAC-CM in which the channel outputs at the destination and user 2 are corrupted by additive Gaussian noise terms. The channel input-output relationship is given by

$$\begin{aligned}
& Y_{j,i} = X_{1,j,i} + X_{2,j,i} + Z_{j,i} \\
& \text{and} \quad Y_{2,j,i} = X_{1,j,i} + X_{2,j,i} + Z_{2,j,i} \tag{9}
\end{aligned}$$

where  $i$  is the time index, and for  $j = 1, \dots, L$ , the noise processes  $\{Z_{j,i}\}$  and  $\{Z_{2,j,i}\}$  are independent and identically distributed (i.i.d.) with the components being zero-mean Gaussian random variables with variances  $\nu_j$  and  $\mu_j$ , respectively. We assume  $\nu_j < \mu_j$  for  $j \in \mathcal{A}$  and  $\nu_j \geq \mu_j$  for  $j \in \bar{\mathcal{A}}$ . The channel input sequences  $X_{1,[1,L]}^n$

and  $X_{2,[1,L]}^n$  are subject to average power constraints  $P_1$  and  $P_2$ , respectively, i.e.,

$$\begin{aligned} & \frac{1}{n} \sum_{i=1}^n \sum_{j=1}^L \mathbb{E}[X_{1,j,i}^2] \leq P_1 \\ \text{and} \quad & \frac{1}{n} \sum_{i=1}^n \sum_{j=1}^L \mathbb{E}[X_{2,j,i}^2] \leq P_2. \end{aligned} \quad (10)$$

### B. Secrecy Capacity Region

We now apply Theorem 2 to obtain the secrecy capacity region of the parallel Gaussian MAC. It can be seen from (9) that the subchannels of the parallel Gaussian MAC are not physically degraded. We consider the following subchannels, for  $j \in \mathcal{A}$ :

$$Y_{j,i} = X_{1,j,i} + X_{2,j,i} + Z_{j,i}, \quad Y_{2,j,i} = Y_{j,i} + Z'_{2,j,i}; \quad (11)$$

and, for  $j \in \bar{\mathcal{A}}$ :

$$Y_{j,i} = Y_{2,j,i} + Z'_{j,i}, \quad Y_{2,j,i} = X_{1,j,i} + X_{2,j,i} + Z_{2,j,i} \quad (12)$$

where  $\{Z'_{j,i}\}$  and  $\{Z'_{2,j,i}\}$  are i.i.d. random processes with components being zero-mean Gaussian random variables with variances  $\nu_j - \mu_j$  for  $j \in \bar{\mathcal{A}}$  and  $\mu_j - \nu_j$  for  $j \in \mathcal{A}$ , respectively. Moreover,  $\{Z'_{j,i}\}$  is independent of  $\{Z_{2,j,i}\}$ , and  $\{Z'_{2,j,i}\}$  is independent of  $\{Z_{j,i}\}$ . We notice that the channel defined in (11)-(12) is a parallel Gaussian MAC with physically degraded subchannels. Since the channel (11)-(12) has the same marginal distributions  $p(y|x_1, x_2)$  and  $p(y_2|x_1, x_2)$  as the parallel Gaussian MAC defined in (9), these two channels have the same secrecy capacity region.<sup>1</sup>

For the channel defined in (11)-(12), we can apply Theorem 2 to obtain the following secrecy capacity region. In particular, the degradedness of the subchannels allows the use of the entropy power inequality in the proof of the converse. We can thus obtain the secrecy capacity region for the parallel Gaussian CMAC-CM.

*Theorem 3:* For the parallel Gaussian CMAC-CM, the secrecy capacity region is given by

$$\mathcal{C}_s^{[G]} = \bigcup_{\underline{p} \in \mathcal{P}} \left\{ \begin{array}{l} (R_0, R_1) : \\ R_0 \geq 0, R_1 \geq 0; \\ R_1 \leq \sum_{j \in \mathcal{A}} \left[ \frac{1}{2} \log \left( 1 + \frac{b_j}{\nu_j} \right) - \frac{1}{2} \log \left( 1 + \frac{b_j}{\mu_j} \right) \right] \\ R_0 \leq \sum_{j \in \mathcal{A}} \frac{1}{2} \log \left( 1 + \frac{a_j + p_{2,j} + 2\sqrt{a_j p_{2,j}}}{b_j + \nu_j} \right) \\ \quad + \sum_{j \in \bar{\mathcal{A}}} \frac{1}{2} \log \left( 1 + \frac{a_j + p_{2,j} + 2\sqrt{a_j p_{2,j}}}{\nu_j} \right) \end{array} \right\} \quad (13)$$

<sup>1</sup>This argument is in fact identical to the so-called *degraded, same-marginals* technique; e.g., see [4] for further details.

where  $\underline{p}$  is the power allocation vector, which consists of  $(a_j, b_j, p_{2,j})$  for  $j \in \mathcal{A}$  and  $(a_j, 0, p_{2,j})$  for  $j \in \bar{\mathcal{A}}$  as components, and the set  $\mathcal{P}$  includes all power allocation vectors  $\underline{p}$  that satisfy the power constraint

$$\mathcal{P} := \left\{ \underline{p} : \sum_{j=1}^L (a_j + b_j) \leq P_1 \text{ and } \sum_{j=1}^L p_{2,j} \leq P_2 \right\}. \quad (14)$$

*Proof:* See Appendix C. ■

We notice that  $\underline{p}$  denotes the power allocation among all subchannels. In particular, for  $j \in \mathcal{A}$ , since user 1 needs to transmit both common and confidential information, the pair  $(a_j, b_j)$  controls the power allocation between the common message  $W_0$  and the confidential message  $W_1$ . For  $j \in \bar{\mathcal{A}}$ , user 1 transmits only the common information, and  $b_j = 0$  indicates that the power is allocated to transmit the common message  $W_0$  only.

### C. Optimal Power Allocation

To characterize the secrecy capacity region of the parallel Gaussian CMAC-CM given in (13), we need to characterize every boundary point and the power allocation vector that achieve each boundary point. Since the secrecy capacity region  $\mathcal{C}_s^{[G]}$  is convex, for every boundary point  $(R_0^*, R_1^*)$ , there exists  $\gamma_1 \geq 0$  such that  $(R_0^*, R_1^*)$  is the solution to the optimization problem

$$\max_{(R_0, R_1) \in \mathcal{C}_s^{[G]}} [R_0 + \gamma_1 R_1]. \quad (15)$$

Note that the optimization problem (15) serves as a complete characterization of the corresponding boundary of the secrecy capacity region, and the solution to (15) provides the power allocations that achieve the boundary of the secrecy capacity region. Let  $(x)^+ = \max(0, x)$ . We obtain the optimal power allocation  $\underline{p}$  that solves (15).

*Theorem 4:* Let  $\underline{p}^*$  be an optimal solution to the optimization problem of (15) that achieves the boundary of the secrecy capacity region of the parallel Gaussian CMAC-CM. Then,  $\underline{p}^*$  can be written as follows.

For  $j \in \mathcal{A}$ , if

$$\frac{2\lambda_1^2 \ln 2}{\lambda_1 + \lambda_2} < \frac{\gamma_1(\mu_j - \nu_j) - \mu_j}{\mu_j \nu_j}, \quad (16)$$

then

$$\begin{aligned} a_j^* &= \frac{\lambda_2^2}{(\lambda_1 + \lambda_2)^2} (s_{1,j} - \phi_j)^+, \\ b_j^* &= (\min[s_{2,j}, \phi_j])^+ \\ \text{and } p_{2,j}^* &= \frac{\lambda_1^2}{(\lambda_1 + \lambda_2)^2} (s_{1,j} - \phi_j)^+; \end{aligned} \quad (17)$$

alternatively, if

$$\frac{2\lambda_1^2 \ln 2}{\lambda_1 + \lambda_2} \geq \frac{\gamma_1(\mu_j - \nu_j) - \mu_j}{\mu_j \nu_j}, \quad (18)$$

then

$$\begin{aligned} a_j^* &= \frac{\lambda_2^2}{(\lambda_1 + \lambda_2)^2} (s_{1,j})^+, \\ b_j^* &= 0 \\ \text{and } p_{2,j}^* &= \frac{\lambda_1^2}{(\lambda_1 + \lambda_2)^2} (s_{1,j})^+; \end{aligned} \quad (19)$$

for  $j \in \bar{\mathcal{A}}$ ,

$$a_j^* = \frac{\lambda_2^2}{(\lambda_1 + \lambda_2)^2} (s_{1,j})^+ \quad \text{and} \quad p_{2,j}^* = \frac{\lambda_1^2}{(\lambda_1 + \lambda_2)^2} (s_{1,j})^+; \quad (20)$$

where  $\gamma_1 \geq 0$ ,

$$\begin{aligned} s_{1,j} &= \frac{\lambda_1 + \lambda_2}{2\lambda_1\lambda_2 \ln 2} - \nu_j, \\ s_{2,j} &= \frac{1}{2} \left[ \sqrt{(\mu_j - \nu_j) \left( \mu_j - \nu_j + \frac{2\gamma_1}{\lambda_1 \ln 2} \right)} - (\mu_j + \nu_j) \right], \\ \phi_j &= -\frac{1}{2} \left( \mu_j + \nu_j + \frac{1}{\omega} \right) + \frac{1}{2} \sqrt{\left( \mu_j + \nu_j + \frac{1}{\omega} \right)^2 - 4 \left[ \mu_j \nu_j - \frac{\gamma_1(\mu_j - \nu_j) - \mu_j}{\omega} \right]}, \\ \omega &= (2 \ln 2) \frac{\lambda_1^2}{\lambda_1 + \lambda_2} \end{aligned} \quad (21)$$

and the pair  $(\lambda_1, \lambda_2)$  is chosen to satisfy the power constraint

$$\sum_{j=1}^L (a_j + b_j) \leq P_1 \quad \text{and} \quad \sum_{j=1}^L p_{2,j} \leq P_2. \quad (22)$$

*Proof:* The optimization problem is non-convex. Our proof technique involves applying KKT conditions (as necessary conditions), which help express the Lagrangian in the form of an integral. This specific structure of the problem is then exploited to obtain a closed-form solution for the optimal power allocation strategy. The details can be found in Appendix D. ■

#### IV. FADING CMAC-CM

In this section, we study the fading CMAC-CM, where both the user-to-destination and the user-to-user channels are corrupted by multiplicative fading gain processes in addition to additive white Gaussian processes. The channel

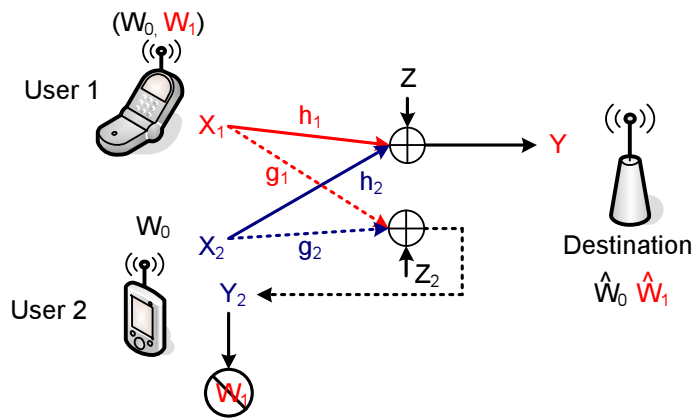


Fig. 2. Fading CMAC-CM.

input-output relationship is given by

$$Y_i = h_{1,i}X_{1,i} + h_{2,i}X_{2,i} + Z_i$$

and  $Y_{2,i} = g_{1,i}X_{1,i} + g_{2,i}X_{2,i} + Z_{2,i}$  (23)

where  $i$  is the time index,  $X_{1,i}$  and  $X_{2,i}$  are channel inputs at the time instant  $i$  from user 1 and user 2, respectively,  $Y_i$  and  $Y_{2,i}$  are channel outputs at the time instant  $i$  at the destination and the receiver of user 2, respectively;  $\underline{h}_i := (h_{1,i}, h_{2,i})$  and  $\underline{g}_i := (g_{1,i}, g_{2,i})$  are proper complex random channel attenuation pairs imposed on the destination and the receiver of user 2; and the noise processes  $\{Z_i\}$  and  $\{Z_{2,i}\}$  are i.i.d. with the components being zero-mean proper complex Gaussian random variables with variances  $\nu$  and  $\mu$ , respectively. The input sequences  $\{X_{1,i}\}$  and  $\{X_{2,i}\}$  are subject to the average power constraint  $P_1$  and  $P_2$ , i.e.,

$$\frac{1}{n} \sum_{i=1}^n \mathbb{E}[X_{1,i}^2] \leq P_1 \quad \text{and} \quad \frac{1}{n} \sum_{i=1}^n \mathbb{E}[X_{2,i}^2] \leq P_2. \quad (24)$$

We assume that the CSI (i.e., the realization of  $(\underline{h}, \underline{g})$ ) is known at both the transmitters and the receivers instantaneously. Depending on the CSI, each user can dynamically change its transmission power and rate to achieve better performance. In this section, we assume that there is no delay constraint on the transmitted messages, and that the secrecy capacity region is an average over all channel states, which is referred to as the *ergodic* secrecy capacity region.

We notice that for a given fading state, i.e., a realization of  $(\underline{h}, \underline{g})$ , the fading CMAC-CM is a Gaussian CMAC-CM. Hence, the fading CMAC-CM can be viewed as a parallel Gaussian CMAC-CM with each fading state corresponding to one subchannel. Thus, the following secrecy capacity region of the fading CMAC-CM follows from Theorem 3.

In the following, for each channel state  $(\underline{h}, \underline{g})$ , we use  $p_1(\underline{h}, \underline{g})$  and  $p_2(\underline{h}, \underline{g})$  to denote the powers allocated at

users 1 and 2, respectively. We further define

$$p(\underline{h}, \underline{g}) := (a(\underline{h}, \underline{g}), b(\underline{h}, \underline{g}), p_2(\underline{h}, \underline{g})). \quad (25)$$

Let  $\mathcal{P}$  denote the set that includes all power allocations that satisfy the power constraint

$$\mathcal{P} := \{p(\underline{h}, \underline{g}) : \mathbb{E}[a(\underline{h}, \underline{g}) + b(\underline{h}, \underline{g})] \leq P_1 \quad \text{and} \quad \mathbb{E}[p_2(\underline{h}, \underline{g})] \leq P_2\}, \quad (26)$$

and  $\mathcal{A}$  denote the set of channel states as follows:

$$\mathcal{A} := \left\{ (\underline{h}, \underline{g}) : \frac{|h_1|^2}{\nu} > \frac{|g_1|^2}{\mu} \right\}. \quad (27)$$

*Corollary 1:* The secrecy capacity region of the fading CMAC-CM is given by (28)

$$\mathcal{C}_s^{[F]} = \bigcup_{p(\underline{h}, \underline{g}) \in \mathcal{P}} \left\{ \begin{array}{l} (R_0, R_1) : \\ R_0 \geq 0, R_1 \geq 0; \\ R_1 \leq \mathbb{E}_{(\underline{h}, \underline{g}) \in \mathcal{A}} \left[ \log \left( 1 + \frac{b(\underline{h}, \underline{g})|h_1|^2}{\nu} \right) - \log \left( 1 + \frac{b(\underline{h}, \underline{g})|g_1|^2}{\mu} \right) \right] \\ R_0 \leq \mathbb{E}_{(\underline{h}, \underline{g}) \in \mathcal{A}} \log \left( 1 + \frac{\chi(\underline{h}, \underline{g})}{b(\underline{h}, \underline{g})|h_1|^2 + \nu} \right) + \mathbb{E}_{(\underline{h}, \underline{g}) \in \bar{\mathcal{A}}} \log \left( 1 + \frac{\chi(\underline{h}, \underline{g})}{\nu} \right) \end{array} \right\} \quad (28)$$

where

$$\chi(\underline{h}, \underline{g}) = \left[ \sqrt{a(\underline{h}, \underline{g})|h_1|} + \sqrt{p_2(\underline{h}, \underline{g})|h_2|} \right]^2 \quad (29)$$

and the random vector pair  $(\underline{h}, \underline{g})$  has the same distribution as the marginal distribution of the process  $\{(\underline{h}_i, \underline{g}_i)\}$  at a single time instant.

The secrecy capacity region given in Corollary 1 is established for fading processes  $(\underline{h}, \underline{g})$  where only ergodic and stationary conditions are assumed. The fading process  $(\underline{h}, \underline{g})$  can be correlated across time, and is not necessarily Gaussian.

Since users are assumed to know the CSI, they can allocate their powers according to the instantaneous channel realization to achieve the optimal performance, i.e., the boundary of the secrecy capacity region. The optimal power allocation that achieves the boundary of the secrecy capacity region for the fading CMAC-CM can be derived from Theorem 4 and is given in the following.

*Corollary 2:* Let  $p(\underline{h}, \underline{g})^*$  be an optimal power allocation that achieves the boundary of the secrecy capacity region of the fading CMAC-CM. Then,  $p(\underline{h}, \underline{g})^*$  is given as follows:

- for  $(\underline{h}, \underline{g}) \in \mathcal{A}$ , if

$$\frac{\lambda_1^2 |h_2|^2 \ln 2}{\lambda_1 |h_2|^2 + \lambda_2 |h_1|^2} < \frac{\gamma_1 (\mu |h_1|^2 - \nu |g_1|^2) - \mu |h_1|^2}{\mu \nu}, \quad (30)$$

then

$$\begin{aligned}
a^*(\underline{h}, \underline{g}) &= \frac{\lambda_2^2 |h_1|^2}{(\lambda_1 |h_2|^2 + \lambda_2 |h_1|^2)^2} [s_1(\underline{h}, \underline{g}) - \phi(\underline{h}, \underline{g})]^+, \\
b^*(\underline{h}, \underline{g}) &= (\min [s_2(\underline{h}, \underline{g}), \phi(\underline{h}, \underline{g})])^+ \\
\text{and } p_2^*(\underline{h}, \underline{g}) &= \frac{\lambda_1^2 |h_2|^2}{(\lambda_1 |h_2|^2 + \lambda_2 |h_1|^2)^2} [s_1(\underline{h}, \underline{g}) - \phi(\underline{h}, \underline{g})]^+;
\end{aligned} \tag{31}$$

alternatively, if

$$\frac{\lambda_1^2 |h_2|^2 \ln 2}{\lambda_1 |h_2|^2 + \lambda_2 |h_1|^2} \geq \frac{\gamma_1 (\mu |h_1|^2 - \nu |g_1|^2) - \mu |h_1|^2}{\mu \nu}, \tag{32}$$

then

$$\begin{aligned}
a^*(\underline{h}, \underline{g}) &= \frac{\lambda_2^2 |h_1|^2}{(\lambda_1 |h_2|^2 + \lambda_2 |h_1|^2)^2} [s_1(\underline{h}, \underline{g})]^+, \\
b^*(\underline{h}, \underline{g}) &= 0 \\
\text{and } p_2^*(\underline{h}, \underline{g}) &= \frac{\lambda_1^2 |h_2|^2}{(\lambda_1 |h_2|^2 + \lambda_2 |h_1|^2)^2} [s_1(\underline{h}, \underline{g})]^+;
\end{aligned} \tag{33}$$

- for  $(\underline{h}, \underline{g}) \in \bar{\mathcal{A}}$ ,

$$\begin{aligned}
a^*(\underline{h}, \underline{g}) &= \frac{\lambda_2^2 |h_1|^2}{(\lambda_1 |h_2|^2 + \lambda_2 |h_1|^2)^2} [s_1(\underline{h}, \underline{g})]^+ \\
\text{and } p_2^*(\underline{h}, \underline{g}) &= \frac{\lambda_1^2 |h_2|^2}{(\lambda_1 |h_2|^2 + \lambda_2 |h_1|^2)^2} [s_1(\underline{h}, \underline{g})]^+;
\end{aligned} \tag{34}$$

where  $\gamma_1 \geq 0$ ,

$$\begin{aligned}
s_1(\underline{h}, \underline{g}) &= \frac{\lambda_1 |h_2|^2 + \lambda_2 |h_1|^2}{\lambda_1 \lambda_2 \ln 2} - \nu, \\
s_2(\underline{h}, \underline{g}) &= \frac{1}{2} \left[ \sqrt{\left( \frac{\mu}{|g_1|^2} - \frac{\nu}{|h_1|^2} \right) \left( \frac{\mu}{|g_1|^2} - \frac{\nu}{|h_1|^2} + \frac{2\gamma_1}{\lambda_1 \ln 2} \right)} - \left( \frac{\mu}{|g_1|^2} + \frac{\nu}{|h_1|^2} \right) \right], \\
\phi(\underline{h}, \underline{g}) &= -\frac{1}{2} \left( \frac{\mu}{|g_1|^2} + \frac{\nu}{|h_1|^2} + \frac{1}{\omega(\underline{h}, \underline{g})} \right) \\
&\quad + \frac{1}{2} \sqrt{\left( \frac{\mu}{|g_1|^2} + \frac{\nu}{|h_1|^2} + \frac{1}{\omega(\underline{h}, \underline{g})} \right)^2 - 4 \left[ \frac{\mu}{|g_1|^2} \frac{\nu}{|h_1|^2} - \frac{\gamma_1 \left( \frac{\mu}{|g_1|^2} - \frac{\nu}{|h_1|^2} \right) - \frac{\mu}{|g_1|^2}}{\omega(\underline{h}, \underline{g})} \right]} \\
\omega(\underline{h}, \underline{g}) &= (\ln 2) \frac{\lambda_1^2 |h_2|^2}{\lambda_1 |h_2|^2 + \lambda_2 |h_1|^2}
\end{aligned} \tag{35}$$

and the pair  $(\lambda_1, \lambda_2)$  is chosen to satisfy the power constraint

$$\mathbb{E}[a(\underline{h}, \underline{g}) + b(\underline{h}, \underline{g})] \leq P_1 \quad \text{and} \quad \mathbb{E}[p_2(\underline{h}, \underline{g})] \leq P_2. \tag{36}$$

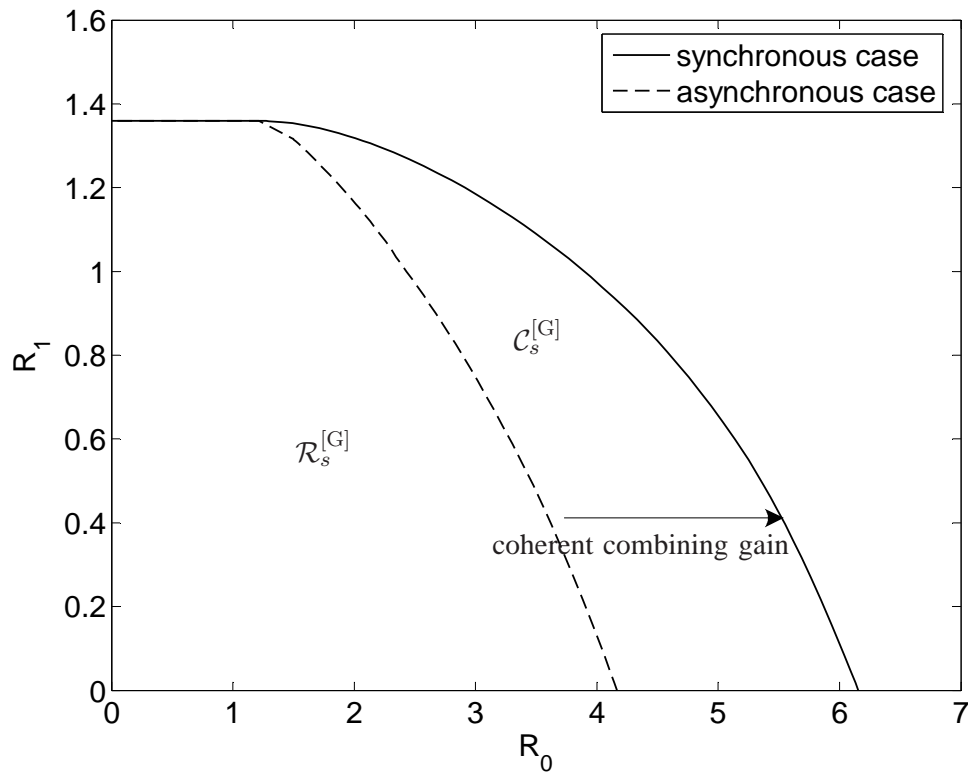


Fig. 3. Secrecy capacity region vs. asynchronous secrecy rate region for the example  $L = 10$  parallel Gaussian CMAC-CM.

## V. NUMERICAL EXAMPLES

In this section, we study two numerical examples to illustrate the secrecy capacity regions of the parallel Gaussian CMAC-CM and the fading CMAC-CM, respectively.

We first consider an  $L = 10$  parallel Gaussian CMAC-CM. We assume that the source power constraints of users 1 and 2 are

$$P_1 = 12 \text{ dB} \quad \text{and} \quad P_2 = 10 \text{ dB},$$

and the noise variances at the receivers of the destination and of user 2 are given by

$$\underline{\nu} = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10]$$

$$\text{and} \quad \underline{\mu} = [5, 3, 4, 9, 1, 10, 8, 7, 2, 6].$$

Fig. 3 illustrates the boundary of the secrecy capacity region for this channel. For comparison, we also consider the asynchronous case, in which users 1 and 2 send the common message  $W_0$  in a asynchronous transmission mode.

In this case, the secrecy rate region is given by

$$\mathcal{R}_s^{[G]} = \bigcup_{\underline{p} \in \mathcal{P}} \left\{ \begin{array}{l} (R_0, R_1) : \\ R_0 \geq 0, R_1 \geq 0; \\ R_1 \leq \sum_{j \in \mathcal{A}} \left[ \frac{1}{2} \log \left( 1 + \frac{b_j}{\nu_j} \right) \frac{1}{2} \log \left( 1 + \frac{b_j}{\mu_j} \right) \right] \\ R_0 \leq \sum_{j \in \mathcal{A}} \frac{1}{2} \log \left( 1 + \frac{a_j + p_{2,j}}{b_j + \nu_j} \right) + \sum_{j \in \bar{\mathcal{A}}} \frac{1}{2} \log \left( 1 + \frac{a_j + p_{2,j}}{\nu_j} \right) \end{array} \right\} \quad (37)$$

where  $\underline{p}$  is the power allocation vector, which consists of  $(a_j, b_j, p_{2,j})$  for  $j \in \mathcal{A}$  and  $(a_j, 0, p_{2,j})$  for  $j \in \bar{\mathcal{A}}$  as components, and the set  $\mathcal{P}$  includes all power allocation vector  $\underline{p}$  that satisfy the power constraint (22). We observe that the synchronous transmission mode significantly increases the rate  $R_0$  of the common message since coherent combining detection can be employed at the destination.

Next, we consider the Rayleigh-fading CMAC-CM, where  $h_1, h_2$  and  $g_1$  are zero-mean proper complex Gaussian random variables. Hence,  $|h_1|^2, |h_2|^2$  and  $|g_1|^2$  are exponentially distributed with means  $\sigma_1, \sigma_2$  and  $\sigma_3$ . We assume that the power constraints of users 1 and 2 are  $P_1 = P_2 = 10$  dB, and the noise variances at the receivers of the destination and of user 2 are  $\nu = \mu = 2$ . In Fig. 4, we plot the boundaries of the secrecy capacity regions corresponding to  $\sigma_1 = 0.5, 1, 2$  and fixed  $\sigma_2 = \sigma_3 = 1$ . It can be seen that as  $\sigma_1$  increases, both the secrecy rate  $R_1$  of the confidential message  $W_1$  and the rate  $R_0$  of the common message  $W_0$  improve. This is because larger  $\sigma_1$  implies a better channel from user 1 to the destination. In Fig. 5, we plot the boundaries of the secrecy capacity regions corresponding to  $\sigma_2 = 0.5, 1, 2$  and fixed  $\sigma_1 = \sigma_3 = 1$ . It can be seen that as  $\sigma_2$  increases, only the rate  $R_0$  of the common message  $W_0$  improves. In Fig. 6, we plot the boundaries of the secrecy capacity regions corresponding to  $\sigma_3 = 0.5, 1, 2$  and fixed  $\sigma_1 = \sigma_2 = 1$ . It can be seen that as  $\sigma_3$  decreases, only the rate  $R_1$  of the confidential message  $W_1$  improves.

## VI. CONCLUSION

We have established the secrecy capacity region of the parallel CMAC-CM, in which it is seen that having independent inputs to each subchannel is optimal. From this result, we have derived the secrecy capacity region for the parallel Gaussian CMAC-CM and the ergodic secrecy capacity region for the fading CMAC-CM. We have illustrated that, when both users know the CSI, they can dynamically adapt their transmission powers with the channel realization to achieve the optimal performance.

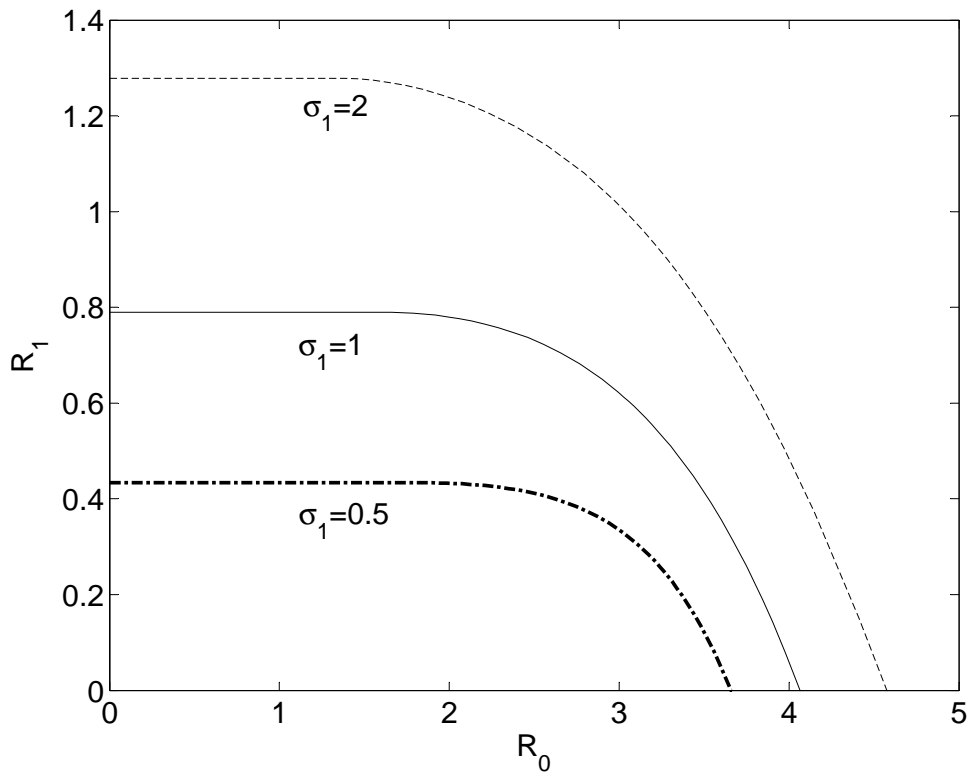


Fig. 4. Secrecy capacity regions for the example fading CMAC-CMs ( $P_1 = P_2 = 10$  dB,  $\nu = \mu = 2$ , and  $\sigma_2 = \sigma_3 = 1$ ).

## APPENDIX

### A. Proof of Theorem 1

*Achievability:* The achievability follows from [4, Corollary 3] by setting

$$\begin{aligned}
 Q &:= (Q_1, \dots, Q_L), & U &:= (U_1, \dots, U_L) \\
 X_1 &:= (X_{1,1}, \dots, X_{1,L}), & X_2 &:= (X_{2,1}, \dots, X_{2,L}) \\
 Y &:= (Y_1, \dots, Y_L), & \text{and } Y_2 &:= (Y_{2,1}, \dots, Y_{2,L})
 \end{aligned} \tag{38}$$

with  $Q$ ,  $U$ ,  $X_1$ , and  $X_2$  having independent components. Furthermore, we choose the components of these random vectors to satisfy the condition

$$p(q_j, u_j, x_{1,j}, x_{2,j}, y_j, y_{2,j}) = p(q_j, x_{2,j})p(u_j|q_j)p(x_{1,j}|u_j)p(y_j, y_{2,j}|x_{1,j}, x_{2,j}) \quad \text{for } j = 1, \dots, L. \tag{39}$$

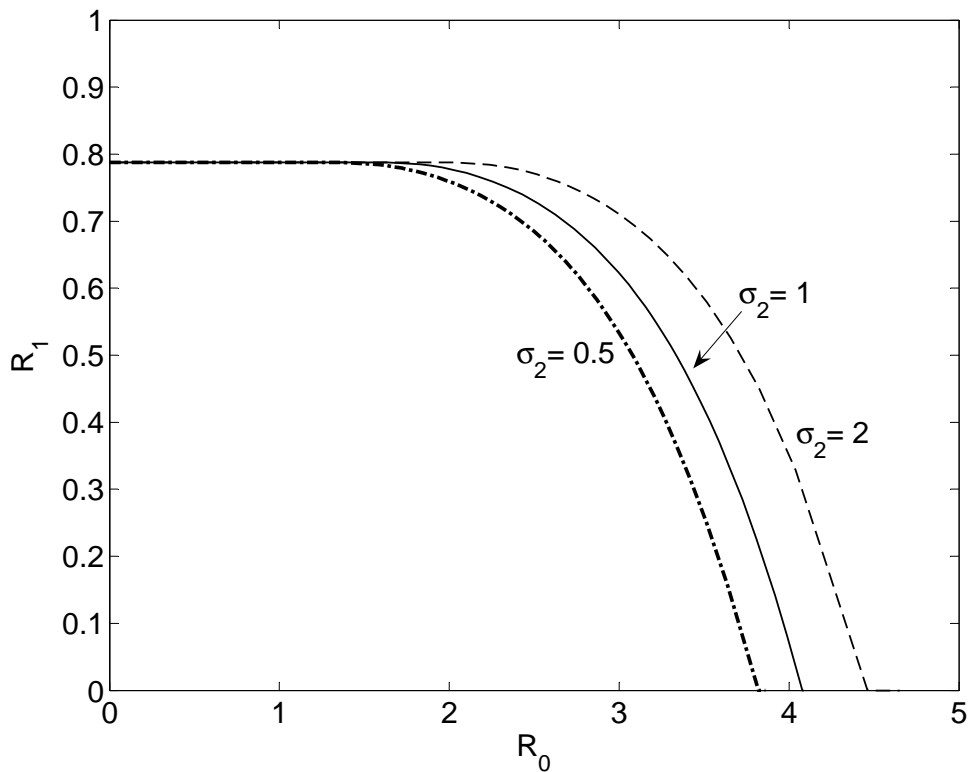


Fig. 5. Secrecy capacity regions for the example fading CMAC-CMs ( $P_1 = P_2 = 10$  dB,  $\nu = \mu = 2$ , and  $\sigma_1 = \sigma_3 = 1$ ).

Using the above definition, we have the following achievable region

$$\mathcal{R}_s^P := \bigcup_{\substack{\prod_j p(q_j, x_{2,j}) p(u_j | q_j) p(x_{1,j} | u_j) \\ p(y_j, y_{2,j} | x_{1,j}, x_{2,j})}} \left\{ (R_0, R_1) \left| \begin{array}{l} R_0 \geq 0, R_1 \geq 0; \\ R_1 \leq \sum_{j=1}^L [I(U_j; Y_j | X_{2,j}, Q_j) - I(U_j; Y_{2,j} | X_{2,j}, Q_j)] \\ R_0 + R_1 \leq \sum_{j=1}^L [I(U_j, X_{2,j}, Q_j; Y_j) - I(U_j; Y_{2,j} | X_{2,j}, Q_j)] \end{array} \right. \right\}. \quad (40)$$

Note that

$$[I(U_j; Y_j | X_{2,j}, Q_j) - I(U_j; Y_{2,j} | X_{2,j}, Q_j)] + I(X_{2,j}, Q_j; Y_j) = I(U_j, X_{2,j}, Q_j; Y_j) - I(U_j; Y_{2,j} | X_{2,j}, Q_j) \quad (41)$$

and hence, any rate pair  $(R_0, R_1) \in \mathcal{C}_s^P$  must also satisfies  $(R_0, R_1) \in \mathcal{R}_s^P$ . This implies that the secrecy rate region  $\mathcal{C}_s^{[P]}$  is achievable.

*Converse:* By Fano's inequality [11, Chapter 2.11], we have

$$H(W_0, W_1 | Y_{[1,L]}^n) \leq n(R_0 + R_1)\epsilon + 1 := n\delta \quad (42)$$

where  $\delta \rightarrow 0$  if  $\epsilon \rightarrow 0$ . On the other hand, the information theoretic secrecy implies that

$$H(W_1) \leq H(W_1 | Y_{2,[1,L]}^n, X_{2,[1,L]}^n, W_0) + n\epsilon. \quad (43)$$

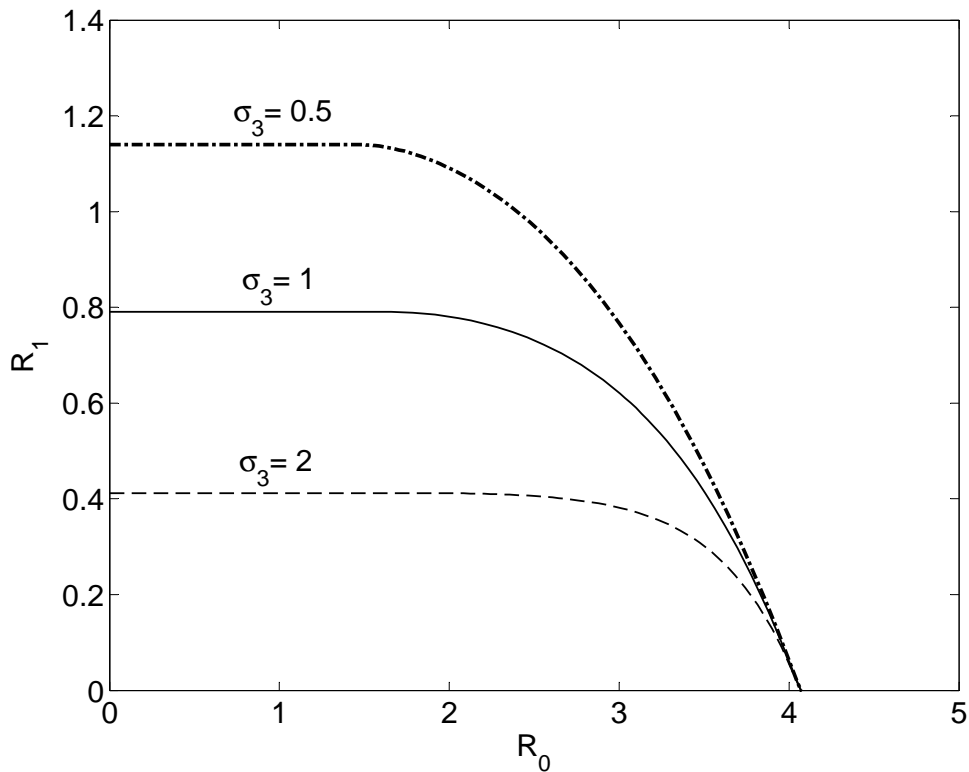


Fig. 6. Secrecy capacity regions for the example fading CMAC-CMs ( $P_1 = P_2 = 10$  dB,  $\nu = \mu = 2$ , and  $\sigma_1 = \sigma_2 = 1$ ).

Now, we consider the upper bound on the secrecy rate  $R_1$  as

$$\begin{aligned} nR_1 &= H(W_1) \\ &\leq H(W_1 | Y_{2,[1,L]}^n, X_{2,[1,L]}^n, W_0) + n\epsilon \end{aligned} \quad (44)$$

$$\leq H(W_1 | Y_{2,[1,L]}^n, X_{2,[1,L]}^n, W_0) - H(W_1 | Y_{[1,L]}^n, X_{2,[1,L]}^n, W_0) + n(\epsilon + \delta) \quad (45)$$

$$= I(W_1; Y_{[1,L]}^n | X_{2,[1,L]}^n, W_0) - I(W_1; Y_{2,[1,L]}^n | X_{2,[1,L]}^n, W_0) + n(\epsilon + \delta)$$

$$= \sum_{j=1}^L \left[ I(W_1; Y_j^n | Y_{[1,j-1]}^n, X_{2,[1,L]}^n, W_0) - I(W_1; Y_{2,j}^n | Y_{2,[j+1,L]}^n, X_{2,[1,L]}^n, W_0) \right] + n(\epsilon + \delta) \quad (46)$$

$$= \sum_{j=1}^L \sum_{i=1}^n \left[ I(W_1; Y_{j,i} | Y_j^{i-1}, Y_{[1,j-1]}^n, X_{2,[1,L]}^n, W_0) - I(W_1; Y_{2,j,i} | Y_{2,j,i+1}^n, Y_{2,[j+1,L]}^n, X_{2,[1,L]}^n, W_0) \right] + n(\epsilon + \delta) \quad (47)$$

where (44) follows from the secrecy constraint (43), (45) follows from Fano's inequality (42), and (46) and (47) follow from the chain rule of mutual information [11, Chapter 2.5]. Let

$$Q_{j,i} := \left( Y_j^{i-1}, Y_{[1,j-1]}^n, Y_{2,j,i+1}^n, Y_{2,[j+1,L]}^n, X_{2,[1,L]}^n, W_0 \right). \quad (48)$$

We notice that this definition implies the Markov chain relationship

$$X_{2,j,i} \rightarrow Q_{j,i} \rightarrow W_1 \rightarrow X_{1,j,i}. \quad (49)$$

Then, following from [2, Lemma 7], we have

$$nR_1 \leq \sum_{j=1}^L \sum_{i=1}^n [I(W_1; Y_{j,i} | X_{2,j,i}, Q_{j,i}) - I(W_1; Y_{2,j,i} | X_{2,j,i}, Q_{j,i})] + n(\epsilon + \delta). \quad (50)$$

We also can write

$$\begin{aligned} nR_0 &= H(W_0) \\ &\leq I(W_0; Y_{[1,L]}^n) + n\delta \end{aligned} \quad (51)$$

$$= \sum_{j=1}^L \sum_{i=1}^n I(W_0; Y_{j,i} | Y_j^{i-1}, Y_{[1,j-1]}^n) + n\delta \quad (52)$$

$$\begin{aligned} &\leq \sum_{j=1}^L \sum_{i=1}^n I(W_0, Y_j^{i-1}, Y_{[1,j-1]}^n, Y_{2,j,i+1}^n, Y_{2,[j+1,L]}^n, X_{2,[1,L]}^n; Y_{j,i}) + n\delta \\ &= \sum_{j=1}^L \sum_{i=1}^n I(Q_{j,i}, X_{2,j,i}; Y_{j,i}) + n\delta \end{aligned} \quad (53)$$

where (51) follows from Fano's inequality (42), (52) follows from the chain rule, and (53) follows from the definition of  $Q_{j,i}$  in (48).

We introduce a time-sharing random variable  $T$  [11, Chapter 14.3] that is independent of all other random variables in the model, and uniformly distributed over  $\{1, \dots, n\}$ . Define  $Q_j = (T, Q_{j,i}, j)$ ,  $U_j = (Q_j, W_1)$ ,  $X_{1,j} = X_{1,T,j}$ ,  $X_{2,j} = X_{2,T,j}$ ,  $Y_{2,j} = X_{2,T,j}$ , and  $Y_j = Y_{T,j}$  for  $j = 1, \dots, L$ . Note that  $(Q_j, X_{1,j}, X_{2,j}, Y_j, Y_{2,j})$  satisfies the following Markov chain relationship

$$Q_j \rightarrow U_j \rightarrow (X_{1,j}, X_{2,j}) \rightarrow (Y_j, Y_{2,j}), \quad \text{for } j = 1, \dots, L. \quad (54)$$

Using the above definition, (50) and (53) become

$$\begin{aligned} R_1 &\leq \sum_{j=1}^L [I(U_j; Y_j | X_{2,j}, Q_j) - I(U_j; Y_{2,j} | X_{2,j}, Q_j)] + (\epsilon + \delta). \\ \text{and } R_0 &\leq \sum_{j=1}^L I(X_{2,j}, Q_j; Y_j) + \delta. \end{aligned} \quad (55)$$

## B. Proof of Theorem 2

The achievability follows from Theorem 1 by setting

$$\begin{aligned} U_j &= X_{1,j} & \text{for } j \in \mathcal{A} \\ \text{and } Q_j &= U_j = X_{1,j} & \text{for } j \in \bar{\mathcal{A}}. \end{aligned} \quad (56)$$

To show the converse, we first consider the upper bound on  $R_0$ . By using (3) in Theorem 1, we have

$$\begin{aligned} R_0 &\leq \sum_{j=1}^L I(Q_j, X_{2,j}; Y_j) \\ &= \sum_{j \in \mathcal{A}} I(Q_j, X_{2,j}; Y_j) + \sum_{j \in \bar{\mathcal{A}}} I(Q_j, X_{2,j}; Y_j) \\ &\leq \sum_{j \in \mathcal{A}} I(Q_j, X_{2,j}; Y_j) + \sum_{j \in \bar{\mathcal{A}}} I(X_{1,j}, X_{2,j}; Y_j) \end{aligned} \quad (57)$$

where (57) follows from the Markov chain relationships

$$Q_j \rightarrow (X_{1,j}, X_{2,j}) \rightarrow Y_j. \quad (58)$$

Now, we consider the upper bound on  $R_1$ . By applying Theorem 1, we obtain

$$\begin{aligned} R_1 &\leq \sum_{j=1}^L [I(U_j; Y_j | X_{2,j}, Q_j) - I(U_j; Y_{2,j} | X_{2,j}, Q_j)] \\ &= \sum_{j \in \mathcal{A}} [I(U_j; Y_j | X_{2,j}, Q_j) - I(U_j; Y_{2,j} | X_{2,j}, Q_j)] + \sum_{j \in \bar{\mathcal{A}}} [I(U_j; Y_j | X_{2,j}, Q_j) - I(U_j; Y_{2,j} | X_{2,j}, Q_j)]. \end{aligned} \quad (59)$$

For  $j \in \bar{\mathcal{A}}$ , the subchannel satisfies

$$p(y_j, y_{2,j} | x_{1,j}, x_{2,j}) = p(y_{2,j} | x_{1,j}, x_{2,j}) p(y_j | y_{2,j}, x_{2,j}), \quad \text{for } j \in \bar{\mathcal{A}}. \quad (60)$$

This implies that

$$\begin{aligned} I(U_j; Y_j | X_{2,j}, Q_j) - I(U_j; Y_{2,j} | X_{2,j}, Q_j) &\leq I(U_j; Y_j | X_{2,j}, Q_j, Y_{2,j}) \\ &\leq I(Q_j, U_j; Y_j | X_{2,j}, Y_{2,j}) \\ &= 0 \quad \text{for } j \in \bar{\mathcal{A}} \end{aligned} \quad (61)$$

where the last equality of (61) follows from the Markov chain relationship

$$(Q_j, U_j) \rightarrow (X_{1,j}, X_{2,j}) \rightarrow (Y_{2,j}, X_{2,j}) \rightarrow Y_j \quad \text{for } j \in \bar{\mathcal{A}}. \quad (62)$$

On the other hand, for  $j \in \mathbf{A}$ , the subchannel satisfies

$$p(y_j, y_{2,j} | x_{1,j}, x_{2,j}) = p(y_j | x_{1,j}, x_{2,j})p(y_{2,j} | y_j, x_{2,j}), \quad \text{for } j \in \mathcal{A}. \quad (63)$$

Hence, we obtain

$$\begin{aligned} I(U_j; Y_j | X_{2,j}, Q_j) - I(U_j; Y_{2,j} | X_{2,j}, Q_j) &\leq I(U_j; Y_j | X_{2,j}, Q_j, Y_{2,j}) \\ &\leq I(U_j, X_{1,j}; Y_j | X_{2,j}, Q_j, Y_{2,j}) \\ &= I(X_{1,j}; Y_j | X_{2,j}, Q_j, Y_{2,j}) \end{aligned} \quad (64)$$

$$= I(X_{1,j}; Y_j, Y_{2,j} | X_{2,j}, Q_j) - I(X_{1,j}; Y_{2,j} | X_{2,j}, Q_j) \quad (65)$$

$$= I(X_{1,j}; Y_j | X_{2,j}, Q_j) - I(X_{1,j}; Y_{2,j} | X_{2,j}, Q_j) \quad \text{for } j \in \mathcal{A} \quad (66)$$

where (64) follows from the Markov chain relationship

$$(Q_j, U_j, Y_{2,j}) \rightarrow (X_{1,j}, X_{2,j}) \rightarrow Y_j, \quad (67)$$

(65) follows from the chain rule of mutual information, and (66) follows from the conditional degradedness (63).

Now, substituting (61) and (66) into (59), we obtain the bound on  $R_1$  given in (7). This concludes the proof of the converse.

### C. Proof of Theorem 3

By the *degraded, same-marginals* argument (see [4]), we need to prove Theorem 3 only for the channel defined by (11)-(12).

*Achievability:* The achievability follows by applying Theorem 2 and choosing the input distribution as follows

$$\begin{aligned} Q_j &= \text{constant}, \quad X_{2,j} \sim \mathcal{N}(0, p_{2,j}), \\ X'_{1,j} &\sim \mathcal{N}(0, (1 - \alpha_j)p_{1,j}), \quad X'_{1,j} \text{ is independent of } X_{2,j} \\ \text{and } X_{1,j} &= \sqrt{\frac{\alpha_j p_{1,j}}{p_{2,j}}} X_{2,j} + X'_{1,j}. \end{aligned} \quad (68)$$

Moreover, by the fact  $\alpha_j = 1$  for  $j \in \bar{\mathcal{A}}$ , we obtain the secrecy rate region  $\mathcal{C}_s^{[G]}$  is achievable.

*Converse:* Here, we derive a tight upper bound on the achievable weighted sum rate

$$R_0 + \gamma_1 R_1$$

using Theorem 2 as the starting point. Since a capacity region is always convex (via a time-sharing argument), an exact characterization of all the achievable weighted sum rates for all nonnegative  $\gamma_1$  provides an exact

characterization of the entire secrecy capacity region. By Theorem 2, any achievable rate pair  $(R_0, R_1)$  must satisfy:

$$R_0 + \gamma_1 R_1 \leq \sum_{j \in \mathcal{A}} [I(Q_j, X_{2,j}; Y_j) + \gamma_1 I(X_{1,j}; Y_j | X_{2,j}, Q_j) - \gamma_1 I(X_{1,j}; Y_{2,j} | X_{2,j}, Q_j)] + \sum_{j \in \bar{\mathcal{A}}} I(X_{1,j}, X_{2,j}; Y_j). \quad (69)$$

For the subchannel  $j \in \bar{\mathcal{A}}$ , we are concerned only with the term

$$I(X_{1,j}, X_{2,j}; Y_j). \quad (70)$$

The maximum-entropy theorem [11] implies that (70) is maximized when  $X_{1,j}$  and  $X_{2,j}$  are jointly Gaussian with variance  $p_{1,j}$  and  $p_{2,j}$  repetitively, and are aligned, i.e.,  $X_{1,j} = \sqrt{p_{1,j}/p_{2,j}} X_{2,j}$ . Hence, we have

$$I(X_{1,j}, X_{2,j}; Y_j) \leq \frac{1}{2} \log \left( 1 + \frac{p_{1,j} + p_{2,j} + 2\sqrt{p_{1,j}p_{2,j}}}{\nu_j} \right) \quad \text{for } j \in \bar{\mathcal{A}}. \quad (71)$$

For the subchannel  $j \in \mathcal{A}$ , we focus on the term

$$I(Q_j, X_{2,j}; Y_j) + \gamma_1 I(X_{1,j}; Y_j | X_{2,j}, Q_j) - \gamma_1 I(X_{1,j}; Y_{2,j} | X_{2,j}, Q_j).$$

Based on the channel model defined in (11)-(12), we have

$$\begin{aligned} & I(Q_j, X_{2,j}; Y_j) + \gamma_1 I(X_{1,j}; Y_j | X_{2,j}, Q_j) - \gamma_1 I(X_{1,j}; Y_{2,j} | X_{2,j}, Q_j) \\ &= h(Y_j) + (\gamma_1 - 1)h(Y_j | X_{2,j}, Q_j) - \gamma_1 h(Y_{2,j} | X_{2,j}, Q_j) + \frac{\gamma_1}{2} \log \frac{\mu_j}{\nu_j}. \end{aligned} \quad (72)$$

Now, we consider the following two cases.

*Case 1:*  $\gamma_1 \leq 1$ . In this case, note that

$$\begin{aligned} h(Y_j | X_{2,j}, Q_j) &\geq h(Y_j | X_{1,j}, X_{2,j}, Q_j) = \frac{1}{2} \log 2\pi e \nu_j \\ h(Y_j | X_{2,j}, Q_j) &\geq h(Y_{2,j} | X_{1,j}, X_{2,j}, Q_j) = \frac{1}{2} \log 2\pi e \mu_j \\ \text{and} \quad h(Y_j) &\leq \frac{1}{2} \log (p_{1,j} + p_{2,j} + 2\sqrt{p_{1,j}p_{2,j}} + \nu_j). \end{aligned} \quad (73)$$

Hence, we have

$$\begin{aligned} & I(Q_j, X_{2,j}; Y_j) + \gamma_1 I(X_{1,j}; Y_j | X_{2,j}, Q_j) - \gamma_1 I(X_{1,j}; Y_{2,j} | X_{2,j}, Q_j) \\ &\leq \frac{1}{2} \log \left( 1 + \frac{p_{1,j} + p_{2,j} + 2\sqrt{p_{1,j}p_{2,j}}}{\nu_j} \right) \quad \text{for } j \in \mathcal{A} \text{ and } \gamma_1 \leq 1. \end{aligned} \quad (74)$$

This result implies that when the weight of the confidential-message rate is less than the weight of the common-

message rate, the optimum solution is to allocate all possible power to transmit the common message.

*Case 2:*  $\gamma_1 > 1$ . Without loss of generality, we assume that the conditional covariance of  $X_{1,j}$  given  $(X_{2,j}, Q_j)$  is given by

$$\text{cov}(X_{1,j}|X_{2,j}, Q_j) = \rho_j p_{1,j} \quad (75)$$

where  $0 \leq \rho_j \leq 1$ . By applying the extremal inequality [12, Theorem 8], we have

$$(\gamma_1 - 1)h(Y_j|X_{2,j}, Q_j) - \gamma_1 h(Y_{2,j}|X_{2,j}, Q_j) \leq \frac{\gamma_1 - 1}{2} \log 2\pi e (\rho_j p_{1,j} + \nu_j) - \frac{\gamma_1}{2} \log 2\pi e (\rho_j p_{1,j} + \mu_j). \quad (76)$$

Moreover, for a given  $\rho_j$ ,

$$h(Y_j) \leq \frac{1}{2} \log \left( p_{1,j} + p_{2,j} + 2\sqrt{(1 - \rho_j)p_{1,j}p_{2,j}} + \nu_j \right). \quad (77)$$

Substituting (76) and (77) into (72), we obtain

$$\begin{aligned} & I(Q_j, X_{2,j}; Y_j) + \gamma_1 I(X_{1,j}; Y_j|X_{2,j}, Q_j) - \gamma_1 I(X_{1,j}; Y_{2,j}|X_{2,j}, Q_j) \\ & \leq \max_{0 \leq \rho_j \leq 1} \left[ \frac{1}{2} \log \left( 1 + \frac{p_{1,j} + p_{2,j} + 2\sqrt{(1 - \rho_j)p_{1,j}p_{2,j}}}{\nu_j} \right) \right. \\ & \quad \left. + \frac{\gamma_1 - 1}{2} \log 2\pi e \left( 1 + \frac{\rho_j p_{1,j}}{\nu_j} \right) - \frac{\gamma_1}{2} \log 2\pi e \left( 1 + \frac{\rho_j p_{1,j}}{\mu_j} \right) \right] \\ & = \max_{0 \leq \alpha_j \leq 1} \left[ \frac{\gamma_1}{2} \log \left( 1 + \frac{(1 - \alpha_j)p_{1,j}}{\nu_j} \right) - \frac{\gamma_1}{2} \log \left( 1 + \frac{(1 - \alpha_j)p_{1,j}}{\mu_j} \right) \right. \\ & \quad \left. + \frac{1}{2} \log \left( 1 + \frac{\alpha_j p_{1,j} + p_{2,j} + 2\sqrt{\alpha_j p_{1,j} p_{2,j}}}{(1 - \alpha_j)p_{1,j} + \nu_j} \right) \right] \quad \text{for } j \in \mathcal{A} \text{ and } \gamma_1 > 1. \end{aligned} \quad (78)$$

Finally, combining (71), (74) and (78), we complete the converse proof.

#### D. Proof of Theorem 4

We need find the optimal  $\underline{p}^* \in \mathcal{P}$  that maximizes

$$R_0 + \gamma_1 R_1 \quad (79)$$

where  $\gamma_1 \geq 0$ . The Lagrangian is given by

$$\begin{aligned} \mathcal{L} = & \sum_{j \in \mathcal{A}} \left[ \frac{1}{2} \log \left( 1 + \frac{a_j + p_{2,j} + 2\sqrt{a_j p_{2,j}}}{b_j + \nu_j} \right) + \frac{\gamma_1}{2} \log \left( 1 + \frac{b_j}{\nu_j} \right) - \frac{\gamma_1}{2} \log \left( 1 + \frac{b_j}{\mu_j} \right) \right] \\ & + \sum_{j \in \bar{\mathcal{A}}} \frac{1}{2} \log \left( 1 + \frac{a_j + p_{2,j} + 2\sqrt{a_j p_{2,j}}}{\nu_j} \right) - \lambda_1 \left[ \sum_{j \in \mathcal{A}} (a_j + b_j) + \sum_{j \in \bar{\mathcal{A}}} a_j \right] - \lambda_2 \sum_{j=1}^L p_{2,j} \end{aligned} \quad (80)$$

where  $\lambda_1$  and  $\lambda_2$  are Lagrange multiplier.

For  $j \in \bar{\mathcal{A}}$ ,  $(a_j^*, p_{2,j}^*)$  needs to maximize the following  $\mathcal{L}_j$ ,

$$\mathcal{L}_j = \frac{1}{2} \log \left( 1 + \frac{a_j + p_{2,j} + 2\sqrt{a_j p_{2,j}}}{\nu_j} \right) - \lambda_1 a_j - \lambda_2 p_{2,j}. \quad (81)$$

Taking derivative of the Lagrangian in (81) over  $a_j$  and  $p_{2,j}$ , the KKT conditions can be written as follows:

$$\begin{aligned} \frac{1}{2 \ln 2} \frac{\theta_{1,j}(a_j, p_{2,j})}{\sqrt{a_j}} &= \lambda_1 \\ \text{and} \quad \frac{1}{2 \ln 2} \frac{\theta_{1,j}(a_j, p_{2,j})}{\sqrt{p_{2,j}}} &= \lambda_2 \end{aligned} \quad (82)$$

where

$$\theta_{1,j}(a_j, p_{2,j}) = \frac{\sqrt{a_j} + \sqrt{p_{2,j}}}{\nu_j + a_j + p_{2,j} + 2\sqrt{a_j p_{2,j}}}. \quad (83)$$

This implies that the pair  $(a_j^*, p_{2,j}^*)$  that optimizes  $\mathcal{L}_j$  must satisfy

$$p_{2,j}^* = \left( \frac{\lambda_1}{\lambda_2} \right)^2 a_j^*. \quad (84)$$

Let us define

$$\beta = \lambda_1 / \lambda_2. \quad (85)$$

On substituting (84) into (81), we obtain that

$$\begin{aligned} \mathcal{L}_j &= \frac{1}{2} \log \left[ 1 + \frac{a_j(1+\beta)^2}{\nu_j} \right] - \lambda_1 a_j(1+\beta) \\ &= \int_0^{a_j(1+\beta)^2} t_{1,j}(s) ds \end{aligned} \quad (86)$$

where

$$t_{1,j}(s) = \frac{1}{(2 \ln 2)} \frac{1}{(\nu_j + s)} - \frac{\lambda_1}{1 + \beta}. \quad (87)$$

We define  $s_{1,j}$  to be the root of the equation  $t_{1,j}(s) = 0$ , i.e.,

$$\begin{aligned} s_{1,j} &= \frac{1 + \beta}{2\lambda_1 \ln 2} - \nu_j \\ &= \frac{\lambda_1 + \lambda_2}{2\lambda_1 \lambda_2 \ln 2} - \nu_j. \end{aligned} \quad (88)$$

Hence, we obtain, for  $j \in \bar{\mathcal{A}}$ ,

$$\begin{aligned} a_j^* &= \frac{1}{(1+\beta)^2} (s_{1,j})^+ \\ &= \frac{\lambda_2^2}{(\lambda_1 + \lambda_2)^2} \left( \frac{\lambda_1 + \lambda_2}{2\lambda_1\lambda_2 \ln 2} - \nu_j \right)^+ \end{aligned} \quad (89)$$

and

$$\begin{aligned} p_{2,j}^* &= \beta^2 a_j^* \\ &= \frac{\lambda_1^2}{(\lambda_1 + \lambda_2)^2} \left( \frac{\lambda_1 + \lambda_2}{2\lambda_1\lambda_2 \ln 2} - \nu_j \right)^+. \end{aligned} \quad (90)$$

For  $j \in \mathcal{A}$ ,  $(a_j^*, b_j^*, p_{2,j}^*)$  needs to maximize the following  $\mathcal{L}_j$ :

$$\mathcal{L}_j = \frac{1}{2} \log \left( 1 + \frac{a_j + p_{2,j} + 2\sqrt{a_j p_{2,j}}}{b_j + \nu_j} \right) + \frac{\gamma_1}{2} \log \left( 1 + \frac{b_j}{\nu_j} \right) - \frac{\gamma_1}{2} \log \left( 1 + \frac{b_j}{\mu_j} \right) - \lambda_1(a_j + b_j) - \lambda_2 p_{2,j}. \quad (91)$$

Taking derivative of the Lagrangian in (91) over  $a_j$  and  $p_{2,j}$ , the KKT conditions can be written as follows:

$$\begin{aligned} \frac{1}{2 \ln 2} \frac{\theta_{2,j}(a_j, b_j, p_{2,j})}{\sqrt{a_j}} &= \lambda_1 \\ \text{and} \quad \frac{1}{2 \ln 2} \frac{\theta_{2,j}(a_j, b_j, p_{2,j})}{\sqrt{p_{2,j}}} &= \lambda_2 \end{aligned} \quad (92)$$

where

$$\theta_{2,j}(a_j, b_j, p_{2,j}) = \frac{\sqrt{a_j} + \sqrt{p_{2,j}}}{\nu_j + a_j + b_j + p_{2,j} + 2\sqrt{a_j p_{2,j}}}. \quad (93)$$

This implies that the pair  $(a_j^*, p_{2,j}^*)$  that optimizes  $\mathcal{L}_j$  must satisfy

$$p_{2,j}^* = \left( \frac{\lambda_1}{\lambda_2} \right)^2 a_j^* = \beta^2 a_j^*. \quad (94)$$

On substituting (94) into (91), we obtain that

$$\begin{aligned} \mathcal{L}_j &= \frac{1}{2} \log \left[ 1 + \frac{a_j(1+\beta)^2}{b_j + \nu_j} \right] + \frac{\gamma_1}{2} \log \left( 1 + \frac{b_j}{\nu_j} \right) - \frac{\gamma_1}{2} \log \left( 1 + \frac{b_j}{\mu_j} \right) - \lambda_1[a_j(1+\beta) + b_j] \\ &= \int_{b_j}^{b_j + a_j(1+\beta)^2} t_{1,j}(s) ds + \int_0^{b_j} t_{2,j}(s) ds \\ &\leq \int_0^\infty (\max\{t_{1,j}(s), t_{2,j}(s)\})^+ ds \end{aligned} \quad (95)$$

where  $t_{1,j}(s)$  is defined in (87) and

$$t_{2,j}(s) = \frac{\gamma_1}{2 \ln 2} \left( \frac{1}{\nu_j + s} - \frac{1}{\mu_j + s} \right) - \lambda_1. \quad (96)$$

Next, we will derive  $(a_j^*, b_j^*, p_{2,j}^*)$  that achieves the upper bound on  $\mathcal{L}_j$  in (95). We consider the point of intersection between  $t_{1,j}(s)$  and  $t_{2,j}(s)$ . By using the definitions of  $t_{1,j}(s)$  in (87) and  $t_{2,j}(s)$  in (96), the point of intersection must satisfy

$$\frac{1}{2 \ln 2} \frac{1}{\nu_j + s} - \frac{\lambda_1}{1 + \beta} = \frac{\gamma_1}{2 \ln 2} \left( \frac{1}{\nu_j + s} - \frac{1}{\mu_j + s} \right) - \lambda_1, \quad (97)$$

i.e.,

$$s^2 + \left( \mu_j + \nu_j + \frac{1}{\omega} \right) s + \left[ \mu_j \nu_j - \frac{\gamma_1(\mu_j - \nu_j) - \mu_j}{\omega} \right] = 0 \quad (98)$$

where

$$\begin{aligned} \omega &= (2\lambda_1 \ln 2) \frac{\beta}{1 + \beta} \\ &= (2 \ln 2) \frac{\lambda_1^2}{\lambda_1 + \lambda_2}. \end{aligned} \quad (99)$$

In the following, we consider two cases based on the relationship between  $\omega$  and  $(\gamma_1(\mu_j - \nu_j) - \mu_j)/(\mu_j \nu_j)$ .

1)  $\omega \geq \frac{\gamma_1(\mu_j - \nu_j) - \mu_j}{\mu_j \nu_j}$ : In this case, (98) implies that the point of intersection between  $t_{1,j}(s)$  and  $t_{2,j}(s)$  is either zero or negative. Moreover, it is easy to see, for  $s \geq 0$ ,

$$t_{1,j}(s) - t_{2,j}(s) = \frac{(\nu_j + s)(\mu_j + s)\omega - [\gamma_1(\mu_j - \nu_j) - (\mu_j + s)]}{(2 \ln 2)(\nu_j + s)(\mu_j + s)} \geq 0. \quad (100)$$

Hence, the upper bound on  $\mathcal{L}_j$  in (95) is achieved by  $b_j^* = 0$ ,

$$\begin{aligned} a_j^* &= \frac{1}{(1 + \beta)^2} (s_{1,j})^+ \\ &= \frac{\lambda_2^2}{(\lambda_1 + \lambda_2)^2} \left( \frac{\lambda_1 + \lambda_2}{2\lambda_1\lambda_2 \ln 2} - \nu_j \right)^+ \end{aligned} \quad (101)$$

and

$$\begin{aligned} p_{2,j}^* &= \beta^2 a_j^* \\ &= \frac{\lambda_1^2}{(\lambda_1 + \lambda_2)^2} \left( \frac{\lambda_1 + \lambda_2}{2\lambda_1\lambda_2 \ln 2} - \nu_j \right)^+ \end{aligned} \quad (102)$$

where  $s_{1,j}$  is defined in (88).

2)  $\omega < \frac{\gamma_1(\mu_j - \nu_j) - \mu_j}{\mu_j \nu_j}$ : In this case, (98) implies that, for  $s > 0$ ,  $t_{1,j}(s)$  and  $t_{2,j}(s)$  intersect only once at

$$\phi_j = -\frac{1}{2} \left( \mu_j + \nu_j + \frac{1}{\omega} \right) + \frac{1}{2} \sqrt{\left( \mu_j + \nu_j + \frac{1}{\omega} \right)^2 - 4 \left[ \mu_j \nu_j - \frac{\gamma_1(\mu_j - \nu_j) - \mu_j}{\omega} \right]}. \quad (103)$$

Moreover, it is easy to see that  $t_{1,j}(0) < t_{2,j}(0)$ . Hence, we have

$$\begin{aligned} t_{1,j}(s) &< t_{2,j}(s) && \text{for } 0 \leq s < \phi_j \\ \text{and } t_{1,j}(s) &\geq t_{2,j}(s) && \text{for } s \geq \phi_j. \end{aligned} \quad (104)$$

Let  $s_{2,j}$  denote the largest root of  $t_{2,j}(s) = 0$ , i.e.,

$$s_{2,j} = \frac{1}{2} \left[ \sqrt{(\mu_j - \nu_j) \left( \mu_j - \nu_j + \frac{2\gamma_1}{\lambda_1 \ln 2} \right)} - (\mu_j + \nu_j) \right]. \quad (105)$$

The optimal  $(a_j^*, b_j^*, p_{2,j}^*)$  depends on the values  $t_{2,j}(0)$ ,  $s_{1,j}$  and  $\phi_j$ , and falls into the following three possibilities.

**(2.a)** If  $t_{2,j}(0) < 0$ , then both  $t_{1,j}(s)$  and  $t_{2,j}(s)$  are negative for  $s \geq 0$  (since both  $t_{1,j}(s)$  and  $t_{2,j}(s)$  are decreasing functions for  $s \geq 0$ ). Then, the upper bound on  $\mathcal{L}_j$  in (95) is achieved by  $b_j^* = 0$ ,  $a_j^* = 0$  and  $p_{2,j}^* = 0$ .

**(2.b)** If  $t_{2,j}(0) \geq 0$  and  $s_{1,j} < \phi_j$ , then the upper bound on  $\mathcal{L}_j$  in (95) is achieved by  $b_j^* = s_{2,j}$ ,  $a_j^* = 0$  and  $p_{2,j}^* = 0$ .

**(2.c)** If  $t_{2,j}(0) \geq 0$  and  $s_{1,j} \geq \phi_j$ , then the upper bound on  $\mathcal{L}_j$  in (95) is achieved by  $b_j^* = \phi_j$ ,

$$a_j^* = \frac{1}{(1 + \beta)^2} (s_{1,j} - \phi_j) \quad \text{and} \quad p_{2,j}^* = \frac{\beta^2}{(1 + \beta)^2} (s_{1,j} - \phi_j). \quad (106)$$

Combing the cases (2.a), (2.b) and (2.c), we obtain

$$\begin{aligned} a_j^* &= \frac{\lambda_2^2}{(\lambda_1 + \lambda_2)^2} (s_{1,j} - \phi_j)^+ \\ b_j^* &= (\min[\phi_j, s_{2,j}])^+ \\ \text{and } p_{2,j}^* &= \frac{\lambda_1^2}{(\lambda_1 + \lambda_2)^2} (s_{1,j} - \phi_j)^+. \end{aligned} \quad (107)$$

Finally, the Lagrange parameters  $\lambda_1 \geq 0$  and  $\lambda_2 \geq 0$  are chosen to satisfy the power constraint (22).

## REFERENCES

- [1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
- [2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
- [3] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Foundations and Trends in Communications and Information Theory*, vol. 5, pp. 355–580, 2008.
- [4] Y. Liang and H. V. Poor, "Multiple access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.
- [5] R. Liu, I. Maric, R. D. Yates, and P. Spasojevic, "The discrete memoryless multiple access channel with confidential messages," in *Proc. IEEE Int. Symp. Information Theory*, Seattle, WA, Jul. 2006, pp. 957 – 961.
- [6] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel with collective secrecy constraints," in *Proc. IEEE Int. Symp. Information Theory*, Seattle, WA, Jul. 2006.

- [7] O. Simeone and A. Yener, "The cognitive multiple access wire-tap channel," in *Proc. Conference on Information Sciences and Systems*, Baltimore, MA, Mar. 2009.
- [8] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.
- [9] P. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Nice, France, June 24–29, 2007.
- [10] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "On the throughput of secure Hybrid-ARQ protocols for Gaussian block-fading channels," *IEEE Trans. Inf. Theory*, vol. 55, pp. 1575–1591, Apr. 2009.
- [11] T. Cover and J. Thomas, *Elements of Information Theory*. New York: John Wiley Sons, Inc., 1991.
- [12] T. Liu and P. Viswanath, "An extremal inequality motivated by multiterminal information-theoretic problems," *IEEE Trans. Inf. Theory*, vol. 53, pp. 1839–1851, May 2007.