Interference Alignment for Secrecy

O. Ozan Koyluoglu, *Student Member, IEEE*, Hesham El Gamal, *Fellow, IEEE*, Lifeng Lai, *Member, IEEE*, and H. Vincent Poor, *Fellow, IEEE*

***Abstract*—This paper studies the frequency/time selective K-user Gaussian interference channel with secrecy constraints. Two distinct models, namely the interference channel with confidential messages and the interference channel with an external eavesdropper, are analyzed. The key difference between the two models is the lack of channel state information (CSI) of the external eavesdropper. Using interference alignment along with secrecy precoding, it is shown that each user can achieve non-zero secure degrees of freedom (DoF) for both cases. More precisely, the proposed coding scheme achieves $\frac{K-2}{2K-2}$ secure DoF *with probability one* per user in the confidential messages model. For the external eavesdropper scenario, on the other hand, it is shown that each user can achieve $\frac{K-2}{2K}$ secure DoF *in the ergodic setting*. Remarkably, these results establish the *positive impact* of interference on the secrecy capacity region of wireless networks.**

***Index Terms*—Information theoretic security, interference alignment, interference channel, secure degrees of freedom.**

I. Introduction

THE wiretap channel was introduced by Wyner [1], in which the eavesdropper is assumed to have access to a degraded version of the intended receiver's signal. This pioneering work was later generalized to cover the non-degraded scenario [2] and the Gaussian channel [3]. However, these results show that the secrecy capacity saturates in the high signal-to-noise ratio (SNR) regime, implying a **vanishing** value for the secure degrees of freedom.

Recently, there has been a growing interest in the analysis and design of secure wireless communication networks based on information-theoretic principles. For example, the secrecy capacity of relay networks was studied in [4], [5], while the fundamental limits of the wiretap channel with feedback were analyzed in [6]. The multiple access and broadcast channels with secrecy constraints were investigated in [7]–[9], the role of multiple antennas in enhancing the secrecy capacity was established in [10], [11], and the positive impact of fading on secrecy capacity was revealed in [12], [13].

In this paper, the frequency/time selective K-user Gaussian interference channel with secrecy constraints is considered. Without the secrecy constraints, it has been recently shown that 1/2 degrees of freedom (DoF) per orthogonal dimension is achievable for each source-destination pair in this network [14]. The achievability of this result was based on the *interference alignment* technique [14], [15], by which the interfering signals are aligned to occupy a subspace orthogonal to the one spanned by the intended signal at each receiver. However, the impact of secrecy constraints on the degrees of freedom in this model has not been fully characterized. In fact, to the best of our knowledge, the only relevant prior works are the study of the two-user discrete memoryless interference channel with confidential messages [16]–[18] and the interference channel with an external eavesdropper [19], [20]. The frequency-selective interference channel adopted in this paper is fundamentally different from these *memoryless* models.

We consider two distinct network models, namely: 1) the interference channel with confidential messages; and 2) the interference channel with an external eavesdropper, each having K source-destination pairs. In the first scenario, one needs to ensure the *confidentiality* of each message from all non-intended receivers in the network. Since all users are assumed to belong to the same network, one can assume the availability of channel state information (CSI) while designing the secrecy coding scheme. (Note also that each receiver has the incentive to report its true CSI to the transmitters, as each receiver needs to decode its own message. If a receiver does not report its CSI faithfully, its rate will be reduced due to the interference. The analysis of such misbehaving users is out of the scope of this paper.) To secure such a network, we employ an interference alignment scheme along with secrecy precoding at each transmitter. Intuitively, the interference alignment scheme has two effects on each receiver i: 1) it aligns the signals from transmitters $k \neq i$ to a low-dimensional subspace; and 2) it assigns the signal from transmitter i to the orthogonal subspace. Hence, while the signal from its own transmitter is *received cleanly*, the signals from other transmitters *are superimposed on each other*. Our secrecy precoding scheme takes advantage of this phenomenon to ensure that the resulting multiple access channel from $K-1$ interfering users does not reveal any useful information about each nonintended message. For $K=3$ users, we show that $\eta = \frac{1}{4}$ secure degrees of freedom per orthogonal dimension

Manuscript received October 07, 2008; revised July 19, 2009; accepted August 26, 2010. Date of current version May 25, 2011. This work was supported in part by the National Science Foundation under Grants CCF-07-28762 and CNS-09-05398, in part by the Los Alamos National Laboratory, and in part by the Qatar National Research Fund. The material in this paper was presented at the 2008 IEEE International Symposium on Information Theory, Toronto, ON, Canada.

O. O. Koyluoglu is with the Department of Electrical and Computer Engineering, The Ohio State University, Columbus, OH 43210 USA (e-mail: koyluogo@ece.osu.edu).

H. El Gamal is with the Department of Electrical and Computer Engineering, The Ohio State University, Columbus, OH 43210 USA, and also with the Wireless Intelligent Networks Center (WINC), Nile University, Cairo, Egypt (e-mail: koyluogo; helgamal@ece.osu.edu).

L. Lai was with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA. He is now with the Department of Systems Engineering, University of Arkansas at Little Rock, Little Rock, AR 72204 USA (e-mail: lxlai@ualr.edu).

H. V. Poor is with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA (e-mail: poor@princeton.edu).

Communicated by A. J. van Wijngaarden, Associate Editor for Communications.

Digital Object Identifier 10.1109/TIT.2011.2132430

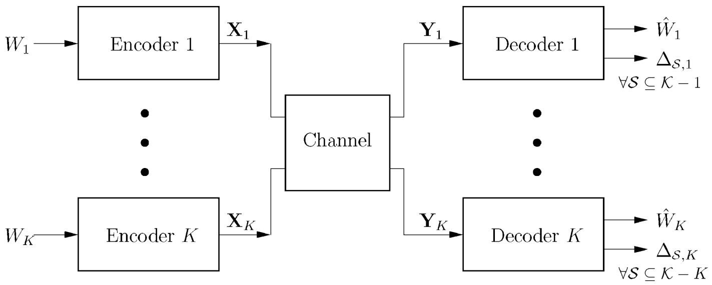

Fig. 1. K-user interference channel with confidential messages.

are achievable for each user using this scheme. We then generalize our results to the K-user Gaussian interference channel and show that each user can achieve $\eta = \frac{K-2}{2K-2}$ secure degrees of freedom, for any $K \geq 3$. In the second scenario, we study the external eavesdropper model where the fundamental challenge is the lack of eavesdropper CSI at the transmitters. Despite this fact, it is shown that $\eta = \frac{K-2}{2K}$ secure degrees of freedom per user are achievable in the ergodic setting. This result provides further evidence of the diminishing gain resulting from knowing the instantaneous CSI of the eavesdropper *a priori*. Interestingly, by comparing our results with those obtained for the point-to-point case [12], [13], one can see the positive impact of interference on the secrecy capacity region of the wireless network. The underlying idea is that the coordination between several source-destination pairs makes it possible to *hide* the secret messages in the background interference.

The remainder of this paper is organized as follows. In Section II, the system model and notation are introduced. Section III is devoted to the interference channel with confidential messages. The analysis for the external eavesdropper scenario is detailed in Section IV. Finally, we offer some concluding remarks in Section V. The lemmas are relegated to the Appendix to enhance the flow of the paper.

II. System Model

In this paper, we use the following notation. Matrices are represented by bold-faced uppercase letters ($\mathbf{X}$) and vectors are denoted as bold-faced uppercase letters with bars or tildes (for example, $\bar{\mathbf{X}}$ and $\tilde{\mathbf{X}}$). We define $\mathcal{K} \triangleq \{1, \dots, K\}$; and denote $\mathbf{X}_{\mathcal{S}} \triangleq \{\mathbf{X}_k \,|\, k \in \mathcal{S}\}$ and $W_{\mathcal{S}} \triangleq \{W_k \,|\, k \in \mathcal{S}\}$ for $\mathcal{S} \subseteq \mathcal{K}$. $\mathcal{K}-i$ denotes the set $\mathcal{K}$ after removing the element i. A zero-mean circularly symmetric complex Gaussian random variable with variance σ^2 is denoted by $\mathcal{CN}(0, \sigma^2)$. A realization of a random variable W is denoted by a corresponding lower case letter w.

We focus on the following K-user system models in this paper.

A. Confidential Messages Scenario

The confidential messages scenario is illustrated in Fig. 1 by a frequency-selective wireless network comprising F frequency bands and K transmitter-receiver pairs, where the ith receiver output at time $t \in \{1, \dots, n\}$ and frequency slot $f \in \{1, \dots, F\}$ is given by

$$Y_i(f,t) = \sum_{k=1}^{K} h_{i,k}(f) X_k(f,t) + Z_i(f,t). \qquad (1)$$

Here, $X_k(f,t)$ is the transmitted symbol of user k and $Z_i(f,t) \sim \mathcal{CN}(0,1)$ is the additive white Gaussian noise at receiver i in frequency band f at time t. We assume that the channel coefficients are independently and randomly generated according to a continuous distribution and are fixed during the communication period. (Note that the continuous distribution assumption on the channel coefficients guarantees the existence of the interference alignment matrix [14].) We assume that the channel coefficients are known at every node in the network.

Using the extended channel notation in [14], the ith received vector during time slot t can be written as

$$\bar{\mathbf{Y}}_i(t) = \sum_{k=1}^{K} \mathbf{H}_{i,k} \bar{\mathbf{X}}_k(t) + \bar{\mathbf{Z}}_i(t). \qquad (2)$$

Here, $\mathbf{H}_{i,k}$ is the $F \times F$ diagonal matrix of channel coefficients from transmitter k to receiver, whereas $\bar{\mathbf{Y}}_i(t) = [Y_i(1,t), \dots, Y_i(F,t)]^T$, $\bar{\mathbf{X}}_k(t) = [X_k(1,t), \dots, X_k(F,t)]^T$, and $\bar{\mathbf{Z}}_i(t) = [Z_i(1,t), \dots, Z_i(F,t)]^T$ are $F \times 1$ column vectors.

We assume that each source $k \in \mathcal{K}$ has a message W_k which must be secured from the remaining $K-1$ receivers (our definition of security will be given shortly). We assume that transmitters have the same average long-term power constraint. Therefore, our $(n, F, M_1, \dots, M_K)$ secret codebook has the following components:

1) The secret message set $\mathcal{W}_k = \{1, \dots, M_k\}$.
2) Encoding functions $f_k(\cdot)$ which map the secret messages to the transmitted symbols, i.e., $f_k : w_k \rightarrow (\bar{\mathbf{X}}_k(1), \dots, \bar{\mathbf{X}}_k(n))$ for each $w_k \in \mathcal{W}_k$. At encoder k, each codeword is designed according to the transmitter's average long-term power constraint ρ, i.e.,

$$\frac{1}{nF} \sum_{f=1}^{F} \sum_{t=1}^{n} |X_k(f,t)|^2 \leq \rho.$$

3) Decoding functions $\phi_k(\cdot)$ at receivers $k \in \mathcal{K}$ which map the received symbols to estimates of the messages: $\phi_k(\mathbf{Y}_k) = \hat{W}_k$, where $\mathbf{Y}_k = \{\bar{\mathbf{Y}}_k(1), \dots, \bar{\mathbf{Y}}_k(n)\}$.

The reliability of the transmission of user k is measured by the probability of error

$$P_{e,k} = \frac{1}{\prod_{i=1}^{K} M_i} \times \sum_{\substack{(w_1,\dots,w_K) \in \\ \mathcal{W}_1 \times \dots \times \mathcal{W}_K}} \Pr\{\phi_k(\mathbf{Y}_k) \neq w_k \,|\, (w_1, \dots, w_K) \text{ is sent}\}$$

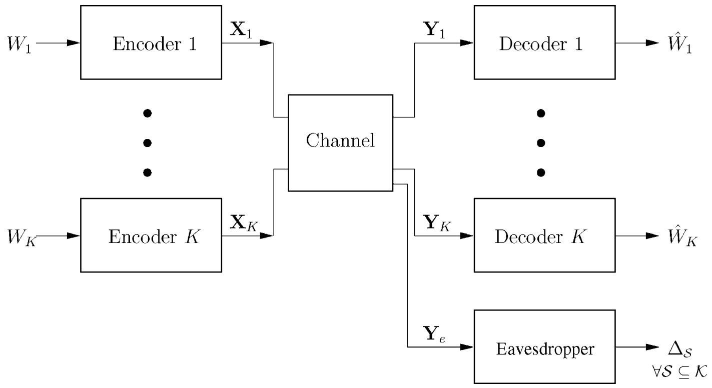

Fig. 2. K-user interference channel with an external eavesdropper.

whereas the secrecy level is measured by the normalized equivocation defined as follows [1], [3]: For receiver i, the equivocation for each subset of messages $W_{\mathcal{S}}, \mathcal{S} \subseteq \mathcal{K} - i$, is

$$\Delta_{\mathcal{S},i} \triangleq \frac{H(W_{\mathcal{S}} \mid \mathbf{Y}_i)}{H(W_{\mathcal{S}})}. \tag{3}$$

Note that this is a multiuser extension of the equivocation considered in [1] and [3].

We say that the rate-equivocation tuple $(R_1, \ldots, R_K, d)$ is achievable for the Gaussian interference channel with confidential messages, if, for any given $\epsilon > 0$, there exists an $(n, F, M_1, \ldots, M_K)$ secret codebook satisfying

$$\frac{1}{nF} \log_2 M_k = R_k, \quad \forall k \in \mathcal{K},$$
$$\max\{P_{e,1}, \ldots, P_{e,K}\} \leq \epsilon,$$

and

$$\Delta_{\mathcal{S},i} \geq d - \epsilon, \quad \forall i \in \mathcal{K}, \quad \forall \mathcal{S} \subseteq \mathcal{K} - i.$$

Note that, with this formulation, a symmetric security guarantee is satisfied for the network users. We also say that η is an achievable symmetric degrees of freedom if the rate-equivocation tuple $(R_1 = R, \ldots, R_K = R, d = 1)$ is achievable and

$$\eta = \lim_{\rho \to \infty} \frac{R}{\log(\rho)}.$$

B. External Eavesdropper Scenario

The external eavesdropper scenario assumes the existence of an external eavesdropper who observes the signals of the K sources (see Fig. 2). We consider an ergodic setting where the channel gains are fixed during a block of n_1 symbol times and then randomly change to another value for the next block. Hence, transmission time of n time slots is divided into B fading blocks with $n = n_1 B$. We use the extended channel notation, and denote the received signals at receiver $i \in \{1, \ldots, K, e\}$ during the fading block b and the time instant j as

$$\bar{\mathbf{Y}}_i(j + (b-1)n_1) = \sum_{k=1}^{K} \mathbf{H}_{i,k}(b) \bar{\mathbf{X}}_k(j + (b-1)n_1) + \bar{\mathbf{Z}}_i(j + (b-1)n_1) \tag{4}$$

where $b \in \{1, \ldots, B\}$ and $j \in \{1, \ldots, n_1\}$. Here, $\mathbf{H}_{i,k}(b)$ is the $F \times F$ diagonal matrix of channel coefficients between transmitter k and receiver i during fading block b, and $\bar{\mathbf{X}}_k(j + (b-1)n_1)$ is the transmitted vector of user k at the jth symbol of the bth fading block. We further define $\mathbf{H} \triangleq \{\mathbf{H}_{i,k}(b) : i, k \in \mathcal{K}, b \in \{1, \ldots, B\}\}$ and $\mathbf{H}_e \triangleq \{\mathbf{H}_{e,k}(b) : k \in \mathcal{K}, b \in \{1, \ldots, B\}\}$. We assume that $\mathbf{H}$ is known at all the nodes in the network, whereas $\mathbf{H}_e$ is known only at the eavesdropper, i.e., only knowledge of the statistics of the eavesdropper CSI is available to the network users. The channel coefficients are i.i.d. samples of a zero-mean unit variance complex Gaussian distribution.

The codebooks are designed such that their components remain as before with the exception that each transmitter must now secure its own message from the external eavesdropper *only*. Accordingly, we modify the secrecy requirement by considering the normalized equivocation seen by the eavesdropper. We denote the observation at the eavesdropper as $\mathbf{Y}_e = \{\bar{\mathbf{Y}}_e(1), \ldots, \bar{\mathbf{Y}}_e(n)\}$, in which $\bar{\mathbf{Y}}_e(t)$ is defined similarly as $\bar{\mathbf{Y}}_i(t)$ for $t = 1, \ldots, n$. Therefore, the normalized equivocation for a subset of messages $\mathcal{S} \subseteq \mathcal{K}$ is given by

$$\Delta_{\mathcal{S}} \triangleq \frac{H(W_{\mathcal{S}} \mid \mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e)}{H(W_{\mathcal{S}})}. \tag{5}$$

We say that the rate-equivocation tuple $(R_1, \ldots, R_K, d)$ is achievable for the Gaussian interference channel with an external eavesdropper, if, for any given $\epsilon > 0$, there exists an $(n, F, M_1, \ldots, M_K)$ secret codebook such that

$$\frac{1}{nF} \log_2 M_k = R_k, \quad \forall k \in \mathcal{K},$$
$$\max\{P_{e,1}, \ldots, P_{e,K}\} \leq \epsilon$$

and

$$\Delta_{\mathcal{S}} \geq d - \epsilon, \quad \forall \mathcal{S} \subseteq \mathcal{K}.$$

It then follows that the symmetric degrees of freedom with perfect secrecy is defined along the same lines as for the confidential messages scenario presented in the beginning of this section.

III. K-User Gaussian Interference Channel With Confidential Messages

To illustrate the main idea, we start with the intuitive argument for the three-user Gaussian interference channel. Here, the signalling scheme will be designed for an odd-valued number of frequency slots represented by $F = 2m + 1$ for some $m \in \mathbb{N}$. (This is the $(2m+1)$ symbol extension of the three-user channel

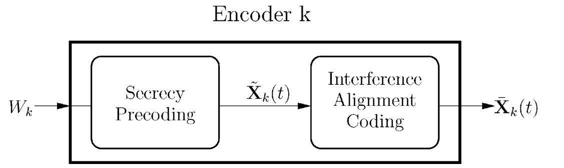

Fig. 3. Proposed encoder architecture for user k in the K-user interference channel with confidential messages.

considered in [14].) The transmitted signals are constructed in the form $\bar{\mathbf{X}}_k(t) = \bar{\mathbf{V}}_k \tilde{\mathbf{X}}_k(t)$, where $\tilde{\mathbf{X}}_k(t)$ represents the vector of m_k streams transmitted from user k (see Fig. 3), and the matrices $\bar{\mathbf{V}}_k$ represent the interference alignment precoding as described in [14]. According to the interference alignment principle [14], the beamforming matrices $\bar{\mathbf{V}}_k$ are constructed to satisfy the following two properties:

1) The nonintended signals seen by each receiver are aligned within some low-dimensional subspace. More precisely, the column space of the matrices $\mathbf{H}_{i,k}\bar{\mathbf{V}}_k$ for $k \in \mathcal{K} - i$ lie in a subspace of dimension $F - m_i$ at receiver i.
2) The intended streams span the orthogonal subspace, i.e., the columns of $\mathbf{H}_{i,i}\bar{\mathbf{V}}_i$ are independent and are orthogonal to the columns of $\mathbf{H}_{i,k}\bar{\mathbf{V}}_k$ for each user $k \in \mathcal{K} - i$.

Note that, to achieve these desired properties, each transmitter utilizes the CSI of the users in the network. This way, the F-dimensional received signal space at each receiver is used to create m_i interference-free dimensions, spanned by the desired streams. Now, let us consider Receiver 1 as the eavesdropper for the messages of User 2 and User 3. This particular eavesdropper now sees m streams of User 2, $\tilde{\mathbf{X}}_2(t)$, and m streams of User 3, $\tilde{\mathbf{X}}_3(t)$, mixed together in a multiple access channel, in which the receiver has **only** m dimensions. This key observation allows for the secrecy precoding $\tilde{\mathbf{X}}_2(t)$ and $\tilde{\mathbf{X}}_3(t)$ to *completely secure* $m/2$ streams in each transmitted vector. It is easy to see that a similar argument follows for securing each vector against a second potential eavesdropper. In the limit of a large values of $F = 2m + 1$, the $m/2$ secure streams results in $1/4$ secure DoF. This intuitive discussion is formalized for the general case of a K-user Gaussian interference channel as follows.

Theorem 1: For the K-user Gaussian interference channel with confidential messages, $\eta = \frac{K-2}{2K-2}$ secure degrees of freedom per frequency-time slot per user are almost surely achievable.

Proof: We will show that almost all codebooks in an appropriately constructed ensemble satisfy the achievability conditions for symmetric secure DoF of $\eta = \frac{K-2}{2K-2}$ with a probability that approaches 1 for all channel coefficients, as $n, m, \rho \to \infty$.

For a given $m \in \mathbb{N}$, the number of streams at users are set as $m_1 = (m+1)^M$ and $m_k = m^M$ for all $k \neq 1$, where $M = (K-1)(K-2) - 1$. Here, the total number of frequency slots is given by $F = (m+1)^M + m^M$. We now generate, for each user k, $2^{nm_k\left(\frac{F}{m_k}(R_k + R_k^x)\right)}$ codewords of length nm_k each with entries that are independent and identically distributed (i.i.d.) according to $\mathcal{CN}(0, \frac{\rho-\epsilon}{c_k})$. We choose c_k to satisfy the power constraint for each user: $c_k = \frac{tr(\bar{\mathbf{V}}_k \bar{\mathbf{V}}_k^H)}{F}$. These codewords are then randomly partitioned into $M_k = 2^{nFR_k}$ message bins, each consisting of $M_k^x = 2^{nFR_k^x}$ codewords. Hence, an entry of the kth user codebook will be represented by $\hat{\mathbf{X}}_k(w_k, w_k^x)$ where the bin index $w_k \in \mathcal{W}_k$ is the secret message and the index $w_k^x \in \{1, \ldots, M_k^x\}$ is the randomization message. It is easy to see that the secure transmission rate per orthogonal time and frequency slot is equal to R_k.

To send a message w_k, the kth transmitter inspects bin $w_k \in \mathcal{W}_k$ and randomly selects a codeword from this bin according to uniform distribution. The codeword index within the bin is denoted by w_k^x. It thus obtains $\hat{\mathbf{X}}_k(w_k, w_k^x)$ of length nm_k. We further partition the elements of this vector as $\hat{\mathbf{X}}_k(w_k, w_k^x) = [\tilde{\mathbf{X}}_k(1), \ldots, \tilde{\mathbf{X}}_k(n)]$, where each element is an $m_k \times 1$ vector. Then, for each symbol time $t \in \{1, \ldots, n\}$, each transmitter performs the mapping from the streams $\tilde{\mathbf{X}}_k(t)$ to channel inputs $\bar{\mathbf{X}}_k(t)$ by $\bar{\mathbf{X}}_k(t) = \bar{\mathbf{V}}_k \tilde{\mathbf{X}}_k(t)$, where the precoding matrices $\bar{\mathbf{V}}_k$ are constructed according to the interference alignment scheme [14].

We choose the secrecy and randomization rates as follows:

$$\begin{aligned} R_k = \frac{1}{F} \min_{i \in \mathcal{K}} \{ I(\tilde{\mathbf{X}}_i; \bar{\mathbf{Y}}_i) \} \\ - \frac{1}{(K-1)F} \max_{i \in \mathcal{K}} \{ I(\tilde{\mathbf{X}}_{\mathcal{K}-i}; \bar{\mathbf{Y}}_i) \}, \quad \text{and} \\ R_k^x = \frac{1}{F} \min_{i \in \mathcal{K}, \mathcal{S} \subseteq \mathcal{K}-i} \left\{ \frac{1}{|\mathcal{S}|} I(\tilde{\mathbf{X}}_{\mathcal{S}}; \bar{\mathbf{Y}}_i \,|\, \tilde{\mathbf{X}}_{\mathcal{K}-\mathcal{S}-i}) \right\}. \end{aligned} \tag{6}$$

Note that, we omit conditioning on the channel coefficients, as they are fixed and known at each user, in the above mutual information expressions.

The above rates are inside the decodability region for each user, i.e., $R_k + R_k^x \leq \frac{1}{F} I(\tilde{\mathbf{X}}_k; \bar{\mathbf{Y}}_k)$, for all $k \in \mathcal{K}$, implying that each user can reliably decode its own streams as $n \to \infty$. This argument is similar to that used to prove the standard channel coding theorem, see, e.g., [21, Theorem 8.7.1]. Hence, using the union bound argument, we can show that for a given ϵ there exists a value $n_0(\epsilon)$ such that, for any $n \geq n_0(\epsilon)$, $\max\{P_{e,1}, \ldots, P_{e,K}\} \leq \epsilon$ holds for almost all codebooks in the ensemble. Our second step is to show that $\Delta_{\mathcal{S},i}$ can be made arbitrarily close to 1 for any $i \in \mathcal{K}$ and $\mathcal{S} \subseteq \mathcal{K} - i$ for almost all codebooks in the ensemble. Towards this end, it is sufficient to focus on the equivocation at an arbitrary receiver $i \in \mathcal{K}$. Furthermore, it is sufficient to establish perfect secrecy for the full message set, i.e., the set of all nonintended messages at receiver i denoted by $W_{\mathcal{K}-i}$, as Lemma 4, given in the Appendix, shows that perfect secrecy of the full message set implies secrecy for all subsets. Denoting the observation of the eavesdropper as $\mathbf{Y}_i$, we write

$$\begin{aligned} & H(W_{\mathcal{K}-i} \,|\, \mathbf{Y}_i) \\ & = H(W_{\mathcal{K}-i}, \mathbf{Y}_i) - H(\mathbf{Y}_i) \\ & = H\left(W_{\mathcal{K}-i}, W_{\mathcal{K}-i}^x, \mathbf{Y}_i\right) \\ & \quad - H\left(W_{\mathcal{K}-i}^x \,|\, W_{\mathcal{K}-i}, \mathbf{Y}_i\right) - H(\mathbf{Y}_i) \\ & = H(W_{\mathcal{K}-i}) + H\left(W_{\mathcal{K}-i}^x \,|\, W_{\mathcal{K}-i}\right) \\ & \quad + H\left(\mathbf{Y}_i \,|\, W_{\mathcal{K}-i}, W_{\mathcal{K}-i}^x\right) \\ & \quad - H\left(W_{\mathcal{K}-i}^x \,|\, W_{\mathcal{K}-i}, \mathbf{Y}_i\right) - H(\mathbf{Y}_i) \\ & = H(W_{\mathcal{K}-i}) + H\left(W_{\mathcal{K}-i}^x\right) - I\left(W_{\mathcal{K}-i}, W_{\mathcal{K}-i}^x; \mathbf{Y}_i\right) \\ & \quad - H\left(W_{\mathcal{K}-i}^x \,|\, W_{\mathcal{K}-i}, \mathbf{Y}_i\right) \end{aligned} \tag{7}$$

where the last equality follows from the fact that $H(W^x_{\mathcal{K}-i} \mid W_{\mathcal{K}-i}) = H(W^x_{\mathcal{K}-i})$ as the randomization (i.e., codeword) indices are independent of the message (i.e., bin) indices. We now bound each term of (7). First, we have

$$I\left(W_{\mathcal{K}-i}, W^x_{\mathcal{K}-i}; \mathbf{Y}_i\right) \leq I(\tilde{\mathbf{X}}_{\mathcal{K}-i}(1), \ldots, \tilde{\mathbf{X}}_{\mathcal{K}-i}(n); \mathbf{Y}_i) \tag{8}$$

due to the Markov chain relationship

$$\left\{W_{\mathcal{K}-i}, W^x_{\mathcal{K}-i}\right\} \rightarrow \{\tilde{\mathbf{X}}_{\mathcal{K}-i}(1), \ldots, \tilde{\mathbf{X}}_{\mathcal{K}-i}(n)\} \rightarrow \mathbf{Y}_i. \tag{9}$$

Due to the fact that

$$I(\tilde{\mathbf{X}}_{\mathcal{K}-i}(1), \ldots, \tilde{\mathbf{X}}_{\mathcal{K}-i}(n); \mathbf{Y}_i) \leq n \max_{p(\tilde{\mathbf{X}}_{\mathcal{K}-i})} I(\tilde{\mathbf{X}}_{\mathcal{K}-i}; \bar{\mathbf{Y}}_i)$$

we obtain

$$I\left(W_{\mathcal{K}-i}, W^x_{\mathcal{K}-i}; \mathbf{Y}_i\right) \leq n \max_{p(\tilde{\mathbf{X}}_{\mathcal{K}-i})} I(\tilde{\mathbf{X}}_{\mathcal{K}-i}; \bar{\mathbf{Y}}_i). \tag{10}$$

Second, we have

$$H\left(W^x_{\mathcal{K}-i}\right) = \log\left(\prod_{k \neq i} M^x_k\right) = nF \sum_{k \in \mathcal{K}-i} R^x_k. \tag{11}$$

To upper bound the last term, we use the following argument. Assume that $w_{\mathcal{K}-i} \in \mathcal{W}_{\mathcal{K}-i}$ is transmitted. Given these bin indices, the remaining randomness in $W^x_{\mathcal{K}-i}$ at the eavesdropper can be resolved for almost all codebooks as the above choice of R^x_k satisfies the multiple access channel achievability conditions $\sum_{k\in\mathcal{S}} R^x_k \leq \frac{1}{F} I(\tilde{\mathbf{X}}_{\mathcal{S}}; \bar{\mathbf{Y}}_i \mid \tilde{\mathbf{X}}_{\mathcal{K}-\mathcal{S}-i}), \forall \mathcal{S} \subseteq \mathcal{K}-i$ [21, Ch. 14]. This argument follows due to the binning codebook construction, see, e.g., [1]. Then, by Fano's inequality, we have $H(W^x_{\mathcal{K}-i} \mid W_{\mathcal{K}-i} = w_{\mathcal{K}-i}, \mathbf{Y}_i) \leq n\delta(n, w_{\mathcal{K}-i})$, where $\delta(n, w_{\mathcal{K}-i}) \rightarrow 0$ as $n \rightarrow \infty$. Then, by defining $\delta(n) \triangleq \max\limits_{w_{\mathcal{K}-i}\in\mathcal{W}_{\mathcal{K}-i}} \delta(n, w_{\mathcal{K}-i})$, we have

$$\begin{aligned} H\left(W^x_{\mathcal{K}-i} \,|\, W_{\mathcal{K}-i}, \mathbf{Y}_i\right) &= \sum_{w_{\mathcal{K}-i}\in\mathcal{W}_{\mathcal{K}-i}} H\left(W^x_{\mathcal{K}-i} \,|\, W_{\mathcal{K}-i} = w_{\mathcal{K}-i}, \mathbf{Y}_i\right) \\ &\quad \times p(W_{\mathcal{K}-i} = w_{\mathcal{K}-i}) \leq n\delta(n) \end{aligned} \tag{12}$$

where $\delta(n) \rightarrow 0$ as $n \rightarrow \infty$. By substituting (10), (11), and (12) in (7) and dividing both sides by $H(W_{\mathcal{K}-i})$, we obtain

$$\Delta_{\mathcal{K}-i,i} \geq 1 - \hat{\delta} \tag{13}$$

where $\hat{\delta}$ is given by

$$\begin{aligned} \hat{\delta} &\triangleq \frac{\delta(n) + \max\limits_{p(\tilde{\mathbf{X}}_{\mathcal{K}-i})} I(\tilde{\mathbf{X}}_{\mathcal{K}-i}; \bar{\mathbf{Y}}_i) - F \sum\limits_{k\in\mathcal{K}-i} R^x_k}{F \sum\limits_{k\in\mathcal{K}-i} R_k}, \\ &= \frac{\delta(n) + \max\limits_{p(\tilde{\mathbf{X}}_{\mathcal{K}-i})} I(\tilde{\mathbf{X}}_{\mathcal{K}-i}; \bar{\mathbf{Y}}_i) - \alpha}{\beta} \end{aligned} \tag{14}$$

where

$$\alpha = (K-1) \min_{i\in\mathcal{K}, \mathcal{S}\subseteq\mathcal{K}-i} \left\{ \frac{1}{|\mathcal{S}|} I(\tilde{\mathbf{X}}_{\mathcal{S}}; \bar{\mathbf{Y}}_i \,|\, \tilde{\mathbf{X}}_{\mathcal{K}-\mathcal{S}-i}) \right\}$$

and

$$\beta = (K-1) \min_{i\in\mathcal{K}} \{I(\tilde{\mathbf{X}}_i; \bar{\mathbf{Y}}_i)\} - \max_{i\in\mathcal{K}} \{I(\tilde{\mathbf{X}}_{\mathcal{K}-i}; \bar{\mathbf{Y}}_i)\}.$$

Note that, we have used the rate assignment given by (6) and the fact that $H(W_{\mathcal{K}-i}) = nF\sum_{k\in\mathcal{K}-i} R_k$ to obtain the above expression.

We already observed as $n \rightarrow \infty$ that $\delta(n) \rightarrow 0$ for almost all codebooks in the ensemble. The orthogonality of the intended message and interference at each respective receiver along with the full rank property of the gain matrices (see Lemma 5) implies the following:

$$\lim_{\rho\rightarrow\infty} \frac{\max\limits_{p(\tilde{\mathbf{X}}_{\mathcal{K}-i})} I(\tilde{\mathbf{X}}_{\mathcal{K}-i}; \bar{\mathbf{Y}}_i)}{\log(\rho)} = F - m_i, \quad \forall i \in \mathcal{K}, \tag{15}$$

and

$$\lim_{\rho\rightarrow\infty} \frac{I(\tilde{\mathbf{X}}_{\mathcal{S}}; \bar{\mathbf{Y}}_i \,|\, \tilde{\mathbf{X}}_{\mathcal{K}-\mathcal{S}-i})}{\log(\rho)} = r \tag{16}$$

where, depending on the interfering signal dimension of receiver i, $r = m^M$ or $r = (m+1)^M$

$$\lim_{\rho\rightarrow\infty} \frac{I(\tilde{\mathbf{X}}_i; \bar{\mathbf{Y}}_i)}{\log(\rho)} = m_i, \quad \forall i \in \mathcal{K}, \tag{17}$$

and

$$\lim_{\rho\rightarrow\infty} \frac{I(\tilde{\mathbf{X}}_{\mathcal{K}-i}; \bar{\mathbf{Y}}_i)}{\log(\rho)} = F - m_i, \quad \forall i \in \mathcal{K}. \tag{18}$$

Using the observations (15), (16), (17), and (18) in (14) we see that

$$\lim_{n,m,\rho\rightarrow\infty} \hat{\delta} = 0 \tag{19}$$

for almost all codebooks in the ensemble. Hence, for any given $\epsilon > 0$, we can make $\Delta_{\mathcal{K}-i,i} \geq 1 - \epsilon$ in the limit of large n, m, and ρ. Finally, due to (6), (17), and (18), we obtain

$$\begin{aligned} \eta &= \lim_{m\rightarrow\infty} \lim_{\rho\rightarrow\infty} \frac{R_k}{\log(\rho)} \\ &= \lim_{m\rightarrow\infty} \frac{(K-1)m^M - (m+1)^M}{(K-1)(m^M + (m+1)^M)} \\ &= \frac{K-2}{2K-2} \end{aligned} \tag{20}$$

which proves our result. ∎

IV. K-User Gaussian Interference Channel With an External Eavesdropper

First, we note that, our previous results extend naturally when the eavesdropper CSI is available *a priori* at the different transmitters and receivers. Intuitively, one can imagine the existence of a virtual transmitter associated with the external eavesdropper transforming our K-user network into a $(K+1)$-user network. This way, one can achieve a secure DoF of $\eta = \frac{(K+1)-2}{2(K+1)-2} = \frac{K-1}{2K}$ per frequency-time slot for each user using the scheme presented in the previous section. For example, for a two-user network with an external eavesdropper, it is possible to achieve $\frac{1}{4}$ secure DoFs if the eavesdropper CSI is available at the transmitters. More formally, we have the following result.

Corollary 2: For the K-user Gaussian interference channel with an external eavesdropper, $\eta = \frac{K-1}{2K}$ secure degrees of freedom per frequency-time slot per user are almost surely achievable when the eavesdropper CSI is available.

More interestingly, it is still possible to achieve positive secure DoF per user in the **absence** of the eavesdropper CSI by exploiting the **ergodicity** of the channel. In the ergodic model, the channel gains are assumed to be fixed during a block of n_1 symbols and then randomly change to another value in the next block for a total of B blocks, where $n_1 \to \infty$ and $B \to \infty$.

Again, for illustration purposes, we consider the situation in which $K = 3$. Here, the users of the network have $\frac{3m+1}{2m+1}$ total DoF while the multiple access channel seen by the eavesdropper can have only one DoF from its observations. Hence, via an appropriate choice of secrecy codebooks, the $\frac{m}{2m+1}$ additional DoF can be *evenly* distributed among the network users *on the average*, allowing for a $\frac{1}{6}$ secure DoF per user without any requirement on the eavesdropper CSI. In the general case, we have the following result.

Theorem 3: For the K-user Gaussian interference channel with an external eavesdropper, $\eta = \frac{1}{2} - \frac{1}{K}$ secure degrees of freedom per frequency-time slot per user are achievable in the ergodic setting in the absence of the eavesdropper CSI.

Proof: Let $F = (m+1)^M + m^M$ for some $m \in \mathbb{N}$ and $M = (K-1)(K-2) - 1$. We set $m_1 = (m+1)^M$ and $m_k = m^M$ for $k \neq 1$. We generate all the permutations of length K and denote this set by Π, where $|\Pi| = K!$. Then, for each fading block $b \in \{1, \ldots, B\}$, we randomly pick, according to uniform distribution, a permutation π_b from Π. In order to ensure statistical symmetry, the interference alignment matrices in each fading block will be obtained according to a different user ordering induced by π_b. More specifically, let $k(b) = \pi_b(k)$ and $\mathbf{H}^{(b)}_{i(b),k(b)} = \mathbf{H}_{i,k}(b)$. Using the newly ordered channel matrices $\mathbf{H}^{(b)}_{i(b),k(b)}$, the interference alignment matrix for user $k(b)$, i.e., $\bar{\mathbf{V}}_{k(b)}$, is generated.

For each secrecy codebook in the ensemble, we generate $2^{nF(R_k+R_k^x)}$ sequences of length $n_1 \sum_{b=1}^{B} m_{k(b)}$ each with entries are chosen i.i.d. $\sim \mathcal{CN}(0, \frac{P-\epsilon}{c})$ for some $\epsilon > 0$ and a value of c that satisfies the long term average power constraint. The existence of ϵ and c follows from the argument of Theorem 1. We independently assign each codeword to one of $M_k = 2^{nFR_k}$ bins, each having $M_k^x = 2^{nFR_k^x}$ codewords. For a given w_k, transmitter k chooses the codeword $\hat{\mathbf{X}}_k(w_k, w_k^x)$ in the bin w_k, where the randomization index w_k^x is chosen independently according to the uniform distribution. This codeword is then divided into B blocks, each with a length of $n_1 m_{k(b)}$ symbols. Each block is then arranged in the following $m_{k(b)} \times n_1$ matrix $[\tilde{\mathbf{X}}_k(1 + (b-1)n_1), \ldots, \tilde{\mathbf{X}}_k(n_1 + (b-1)n_1)]$, where $\tilde{\mathbf{X}}_k(j + (b-1)n_1)$ is an $m_{k(b)} \times 1$ vector and $1 \leq j \leq n_1$. At time slot $t = j + (b-1)n_1$, the kth transmitter maps $\tilde{\mathbf{X}}_k(t)$ to $\bar{\mathbf{X}}_k(t)$ using $\bar{\mathbf{X}}_k(t) = \bar{\mathbf{V}}_{k(b)}\tilde{\mathbf{X}}_k(t)$. Note that, the expectations in the sequel will be taken with respect to the two distributions: a) the random distribution of the channel matrices, and b) the uniform distribution for the underlying permutation operators that are used in different fading blocks. This allows us to average out the fluctuations of the eavesdropper CSI.

Our first key observation is that the equivalent channel matrices $\mathbf{H}_{i,k}(b)\bar{\mathbf{V}}_{k(b)}$ connecting $\tilde{\mathbf{X}}_k(t)$ and $\bar{\mathbf{Y}}_i(t)$ are identically distributed for all $i, k \in \mathcal{K}$ and $b \in \{1, \ldots, B\}$. This property will allow us to drop the subscript i and write $\mathbb{E}[I(\tilde{\mathbf{X}}_i; \bar{\mathbf{Y}}_i \mid \mathbf{H})] = \mathbb{E}[I(\tilde{\mathbf{X}}; \bar{\mathbf{Y}} \mid \mathbf{H})]$, for all $i \in \mathcal{K}$. To satisfy the achievability conditions and the secrecy requirements of the network, we choose R_k and R_k^x as follows:

$$R_k = \frac{1}{KF}\Bigg(K\mathbb{E}[I(\tilde{\mathbf{X}}; \bar{\mathbf{Y}} \mid \mathbf{H})] - \max_{p(\bar{\mathbf{X}}_{\mathcal{K}})} \mathbb{E}[I(\bar{\mathbf{X}}_{\mathcal{K}}; \bar{\mathbf{Y}}_e \mid \mathbf{H}, \mathbf{H}_e)]\Bigg), \tag{21}$$

and

$$R_k^x = \frac{1}{KF}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{K}}; \bar{\mathbf{Y}}_e \mid \mathbf{H}, \mathbf{H}_e)]$$

where the maximization in the first equation is among all possible input distributions. With this choice of rates, we have the following:

$$\begin{aligned} R_k + R_k^x = {} & \frac{1}{F}\mathbb{E}[I(\tilde{\mathbf{X}}; \bar{\mathbf{Y}} \mid \mathbf{H})] \\ & - \frac{1}{KF}\max_{p(\bar{\mathbf{X}}_{\mathcal{K}})} \mathbb{E}[I(\bar{\mathbf{X}}_{\mathcal{K}}; \bar{\mathbf{Y}}_e \,|\, \mathbf{H}, \mathbf{H}_e)] \\ & + \frac{1}{KF}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{K}}; \bar{\mathbf{Y}}_e \mid \mathbf{H}, \mathbf{H}_e)] \\ \leq {} & \frac{1}{F}\mathbb{E}[I(\tilde{\mathbf{X}}; \bar{\mathbf{Y}} \mid \mathbf{H})] \end{aligned}$$

where the inequality is due to the maximization among *all* possible input distributions in the second term of the equation. Hence, we have $R_k + R_k^x \leq \frac{1}{F}\mathbb{E}[I(\tilde{\mathbf{X}}; \bar{\mathbf{Y}} \,|\, \mathbf{H})]$, from which we conclude that each user in the interference network can decode its own secrecy and randomization indices as $n_1 \to \infty$ and as $B \to \infty$ using almost all codebooks in the ensemble. This argument is the fading version of the channel coding theorem. The next step is to study the equivocation at the eavesdropper, i.e.,

$$\begin{aligned} & \frac{1}{n}H(W_{\mathcal{K}} \mid \mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e) \\ & = \frac{1}{n}(H(W_{\mathcal{K}}, \mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e) - H(\mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e)) \\ & = \frac{1}{n}(H(W_{\mathcal{K}}, W_{\mathcal{K}}^x, \mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e) \\ & \quad - H(W_{\mathcal{K}}^x \,|\, W_{\mathcal{K}}, \mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e) - H(\mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e)) \\ & = \frac{1}{n}(H(W_{\mathcal{K}}) + H(W_{\mathcal{K}}^x \,|\, W_{\mathcal{K}}) \\ & \quad + H(\mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e \,|\, W_{\mathcal{K}}, W_{\mathcal{K}}^x) \\ & \quad - H(W_{\mathcal{K}}^x \,|\, W_{\mathcal{K}}, \mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e) - H(\mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e)) \\ & = \frac{1}{n}(H(W_{\mathcal{K}}) + H(W_{\mathcal{K}}^x) - I(W_{\mathcal{K}}, W_{\mathcal{K}}^x; \mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e) \\ & \quad - H(W_{\mathcal{K}}^x \,|\, W_{\mathcal{K}}, \mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e)) \end{aligned} \tag{22}$$

where the last equality follows from the fact that $H(W_{\mathcal{K}}^x \mid W_{\mathcal{K}}) = H(W_{\mathcal{K}}^x)$ as the codeword indices are independent of the bin indices. Here

$$\begin{aligned} H(W_{\mathcal{K}}^x) &= \log\left(\prod_{k=1}^{K} M_k^x\right) = \sum_{k=1}^{K} nFR_k^x \\ &= n\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{K}};\bar{\mathbf{Y}}_e \mid \mathbf{H},\mathbf{H}_e)] \end{aligned} \tag{23}$$

and

$$\begin{aligned} &\lim_{n\to\infty}\frac{1}{n}I(W_{\mathcal{K}}, W_{\mathcal{K}}^x; \mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e) \\ &\quad\le \lim_{n\to\infty}\frac{1}{n}I(\tilde{\mathbf{X}}_{\mathcal{K}}(1),\ldots,\tilde{\mathbf{X}}_{\mathcal{K}}(n); \mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e) \\ &\quad= \lim_{n\to\infty}\frac{1}{n}\Big(I(\tilde{\mathbf{X}}_{\mathcal{K}}(1),\ldots,\tilde{\mathbf{X}}_{\mathcal{K}}(n); \mathbf{H}, \mathbf{H}_e) \\ &\qquad + I(\tilde{\mathbf{X}}_{\mathcal{K}}(1),\ldots,\tilde{\mathbf{X}}_{\mathcal{K}}(n); \mathbf{Y}_e \mid \mathbf{H}, \mathbf{H}_e)\Big) \\ &\quad= \lim_{n\to\infty}\frac{1}{n}I(\tilde{\mathbf{X}}_{\mathcal{K}}(1),\ldots,\tilde{\mathbf{X}}_{\mathcal{K}}(n); \mathbf{Y}_e \mid \mathbf{H}, \mathbf{H}_e) \\ &\quad= \mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{K}};\bar{\mathbf{Y}}_e \mid \mathbf{H},\mathbf{H}_e)], \end{aligned} \tag{24}$$

where the first inequality is due to the Markov chain relationship

$$\{W_{\mathcal{K}}, W_{\mathcal{K}}^x\} \to \{\tilde{\mathbf{X}}_{\mathcal{K}}(1),\ldots,\tilde{\mathbf{X}}_{\mathcal{K}}(n)\} \to \{\mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e\}$$

and the last one is due to ergodicity. For the last term of (22), we observe that, once the bin indices are given, the channel seen by the eavesdropper reduces to a multiple access fading channel for the randomization messages due to the binning code construction. For this fading MAC, each user is able to set its randomization message rate as a fraction, $\frac{1}{K}$, of the total DoF seen by the eavesdropper as chosen in (21), and assure the decodability of the randomization messages at the eavesdropper given the secrecy message indices. (The technical details are reported in Lemma 6, Lemma 7, and Lemma 8 in the Appendix.) Due to this fact, by Fano's inequality, we have

$$\lim_{n_1, B\to\infty}\frac{H(W_{\mathcal{K}}^x \mid W_{\mathcal{K}}, \mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e)}{n_1 B} = 0$$

for almost all codebooks in the ensemble. Therefore, by dividing both sides of (22) by $\frac{1}{n}H(W_{\mathcal{K}})$, we can ensure

$$\Delta_{\mathcal{K}} = \frac{H(W_{\mathcal{K}} \mid \mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e)}{H(W_{\mathcal{K}})} \ge 1 - \epsilon \tag{25}$$

for any $\epsilon > 0$ as $n_1, B \to \infty$, which is sufficient for our purposes (please refer to Lemma 4 in the Appendix). Finally, from (21), we have

$$\lim_{\rho\to\infty}\frac{\mathbb{E}[I(\tilde{\mathbf{X}};\bar{\mathbf{Y}} \mid \mathbf{H})]}{\log(\rho)} = \left(\frac{1}{K}m_1 + \frac{K-1}{K}m_2\right),$$

and hence

$$\begin{aligned} \lim_{\rho\to\infty}\frac{R_k}{\log(\rho)} &= \frac{1}{KF}\left(K\left(\frac{1}{K}m_1 + \frac{K-1}{K}m_2\right) - F\right) \\ &= \frac{(K-2)m^M}{KF} \end{aligned} \tag{26}$$

implying that $\eta = \frac{m^M}{F} - \frac{2m^M}{KF}$ DoF is achievable for each user for any m. Consequently, we conclude that $\lim_{m\to\infty}\eta = \frac{1}{2} - \frac{1}{K}$ symmetric DoF is achievable with perfect secrecy in the ergodic setting. ■

It is important to observe that the achievability of a positive DoF for the no eavesdropper CSI scenario hinges largely on the ergodicity assumption, whereas our results hold almost surely for all channel realizations when the eavesdropper CSI is assumed to be available. This is the price entailed by the lack of eavesdropper CSI. Finally, the positive impact of interference on the secrecy capacity region is best illustrated by comparing our results to the point-to-point scenario. In [13], a point-to-point channel with an external eavesdropper was shown to have zero DoF. On the other hand, our results show that as more source-destination pairs are added to the network, each pair is able to achieve nonzero DoF for $K \ge 2$. This seemingly surprising result is due to the interference alignment technique which **not only** allows for a clean separation between the intended message and interference at each receiver, but also packs the interfering signals into a low dimensionality subspace, and hence, impairs the ability of each eavesdropper to distinguish any of the secure messages efficiently.

V. Conclusion

In this paper, we have considered the K-user Gaussian interference channel with secrecy constraints. Two scenarios have been analyzed, namely the confidential messages scenario and the case in which an external eavesdropper, with unknown CSI, is present in the network. By using an interference alignment scheme along with secrecy precoding at each transmitter, we have shown that each user in the network can achieve a nonzero secure degrees of freedom. The most interesting aspect of our results is, perhaps, the discovery of the role of interference in increasing the secrecy capacity of multiuser wireless networks.

Appendix

This Appendix contains the lemmas used in the sequel.

Lemma 4: Consider receiver $i \in \mathcal{K}$. For a given $\epsilon > 0$ and $d \in [0,1]$, $\exists\epsilon^*(i,\epsilon,d) > 0$ such that, if $\Delta_{\mathcal{K}-i,i} \ge 1 - \epsilon^*(i,\epsilon,d)$ then $\Delta_{\mathcal{S},i} \ge d - \epsilon$, $\forall\mathcal{S} \subseteq \mathcal{K} - i$.

Proof: For a given $i \in \mathcal{K}$, $\epsilon > 0$, and level of secrecy $d \in [0,1]$, let $\epsilon^*(i,\epsilon,d) = \min_{\mathcal{S}\subseteq\mathcal{K}-i}(1+\epsilon-d)\frac{H(\mathcal{W}_{\mathcal{S}})}{H(\mathcal{W}_{\mathcal{K}-i})}$. Let $\mathbf{Y}_i$ denote the received observation of the eavesdropper and assume $\Delta_{\mathcal{K}-i,i} \ge 1 - \epsilon^*(i,\epsilon,d)$. Then, for any $\mathcal{S} \subseteq \mathcal{K} - i$, we have $H(\mathcal{W}_{\mathcal{K}-i} \mid \mathbf{Y}_i) = H(\mathcal{W}_{\mathcal{S}} \mid \mathbf{Y}_i) + H(\mathcal{W}_{\mathcal{K}-i} \mid \mathcal{W}_{\mathcal{S}}, \mathbf{Y}_i)$ and

$$\begin{aligned} H(\mathcal{W}_{\mathcal{K}-i} \mid \mathbf{Y}_i) &\ge H(\mathcal{W}_{\mathcal{K}-i}) - \epsilon^*(i,\epsilon,d)H(\mathcal{W}_{\mathcal{K}-i}) \\ &\ge H(\mathcal{W}_{\mathcal{S}}) + H(\mathcal{W}_{\mathcal{K}-i} \mid \mathcal{W}_{\mathcal{S}}) \\ &\quad - (1+\epsilon-d)H(\mathcal{W}_{\mathcal{S}}), \end{aligned} \tag{27}$$

where the first inequality follows from the assumption of $\Delta_{\mathcal{K}-i,i} \geq 1 - \epsilon^*(i,\epsilon,d)$ and the second inequality follows from the choice of $\epsilon^*(i,\epsilon,d)$ above. Continuing from above

$$\begin{aligned}\Delta_{\mathcal{S},i} = \frac{H(\mathcal{W}_{\mathcal{S}} \mid \mathbf{Y}_i)}{H(\mathcal{W}_{\mathcal{S}})} &\geq (d-\epsilon)\\ +\frac{H(\mathcal{W}_{\mathcal{K}-i} \mid \mathcal{W}_{\mathcal{S}}) - H(\mathcal{W}_{\mathcal{K}-i} \mid \mathcal{W}_{\mathcal{S}}, \mathbf{Y}_i)}{H(\mathcal{W}_{\mathcal{S}})} &\geq (d-\epsilon) \end{aligned} \tag{28}$$

as conditioning does not increase entropy. ■

We remark that a similar observation is used in [7]. The above proof is more complete than the argument given in [7].

Lemma 5: Due to the interference alignment precoding, the effective channel gain matrix between transmitter k and the receiver i, i.e., $\mathbf{H}_{i,k}\bar{\mathbf{V}}_k$, has rank m_k with probability one. As the dimension of $\mathbf{H}_{i,k}\bar{\mathbf{V}}_k$ is $F \times m_k$, these matrices have full rank with probability one.

Proof: First, due to the construction given in [14], we have $\operatorname{rank}(\mathbf{H}_{k,k}\bar{\mathbf{V}}_k) = m_k$. Second, we observe that the design of interference alignment vectors ensures the linear independence of the columns. (If they had linearly dependent columns, then $\mathbf{H}_{k,k}\bar{\mathbf{V}}_k$ would not have m_k linearly independent columns, contrary to the construction of the interference alignment matrices.) It follows that $\operatorname{rank}(\mathbf{H}_{i,k}\bar{\mathbf{V}}_k) \leq \min\{m_k, F\} = m_k$ for $i \neq k$. We only need to show that the matrix $\mathbf{H}_{i,k}\bar{\mathbf{V}}_k$ has m_k linearly independent columns. Considering any $i \neq k$, representing diagonal elements of $\mathbf{H}_{i,k}$ as $\{h_{i,k}(1), h_{i,k}(2), \ldots, h_{i,k}(F)\}$ and denoting the rows of the interference alignment matrix by $\mathbf{v}_f$, i.e., $\bar{\mathbf{V}}_k = [\mathbf{v}_1^T; \mathbf{v}_2^T; \ldots; \mathbf{v}_F^T]^T$, we have $\mathbf{H}_{i,k}\bar{\mathbf{V}}_k = [h_{i,k}(1)\mathbf{v}_1^T; h_{i,k}(2)\mathbf{v}_2^T; \ldots; h_{i,k}(F)\mathbf{v}_F^T]^T$. At this point, as the channel gains are chosen according to a continuous distribution, it follows that each $h_{ik}(f)$ is non-zero with probability one for $f \in \{1, 2, \ldots, F\}$. Hence, these row operations will not change the rank of a matrix, i.e., $\operatorname{rank}(\mathbf{H}_{i,k}\bar{\mathbf{V}}_k) = \operatorname{rank}(\bar{\mathbf{V}}_k) = m_k$. Therefore, the gain matrices seen by the receivers have full rank with probability one. ■

Lemma 6: For any $\mathcal{M}, \mathcal{L} \subseteq \mathcal{K}$ satisfying $\mathcal{M} \cap \mathcal{L} = \emptyset$

$$I(\tilde{\mathbf{X}}_{\mathcal{M}}; \bar{\mathbf{Y}}_e \mid \mathbf{H}, \mathbf{H}_e) \leq I(\tilde{\mathbf{X}}_{\mathcal{M}}; \bar{\mathbf{Y}}_e \mid \tilde{\mathbf{X}}_{\mathcal{L}}, \mathbf{H}, \mathbf{H}_e).$$

Proof: We have

$$\begin{aligned} I(\tilde{\mathbf{X}}_{\mathcal{M}}; \bar{\mathbf{Y}}_e \mid \mathbf{H}, \mathbf{H}_e) &= H(\tilde{\mathbf{X}}_{\mathcal{M}} \mid \mathbf{H}, \mathbf{H}_e)\\ &\quad - H(\tilde{\mathbf{X}}_{\mathcal{M}} \mid \bar{\mathbf{Y}}_e, \mathbf{H}, \mathbf{H}_e)\\ &\leq H(\tilde{\mathbf{X}}_{\mathcal{M}} \mid \tilde{\mathbf{X}}_{\mathcal{L}}, \mathbf{H}, \mathbf{H}_e)\\ &\quad - H(\tilde{\mathbf{X}}_{\mathcal{M}} \mid \bar{\mathbf{Y}}_e, \tilde{\mathbf{X}}_{\mathcal{L}}, \mathbf{H}, \mathbf{H}_e)\\ &= I(\tilde{\mathbf{X}}_{\mathcal{M}}; \bar{\mathbf{Y}}_e \mid \tilde{\mathbf{X}}_{\mathcal{L}}, \mathbf{H}, \mathbf{H}_e) \end{aligned} \tag{29}$$

where the inequality is due to the fact that conditioning does not increase entropy, and the last equality follows by $H(\tilde{\mathbf{X}}_{\mathcal{M}} \mid \tilde{\mathbf{X}}_{\mathcal{L}}, \mathbf{H}, \mathbf{H}_e) = H(\tilde{\mathbf{X}}_{\mathcal{M}} \mid \mathbf{H}, \mathbf{H}_e)$ as $\mathcal{M} \cap \mathcal{L} = \emptyset$ and messages of the users are independent. ■

Lemma 7:

$$\begin{aligned} &\frac{1}{|\mathcal{S}^c|}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{S}^c}; \bar{\mathbf{Y}}_e \mid \mathbf{H}, \mathbf{H}_e)]\\ &\qquad\qquad \leq \frac{1}{|\mathcal{S}|}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{S}}; \bar{\mathbf{Y}}_e \mid \tilde{\mathbf{X}}_{\mathcal{S}^c}, \mathbf{H}, \mathbf{H}_e)] \end{aligned}$$

Proof:

Let $\mathcal{S} = \{s_1, \ldots, s_S\}$ denote a set of size $|\mathcal{S}| = S$, and denote $\mathcal{S}^c = \{s_{S+1}, \ldots, s_K\}$ of size $|\mathcal{S}^c| = K - S$. Then, we have

$$\begin{aligned} &\frac{1}{|\mathcal{S}^c|}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{S}^c}; \bar{\mathbf{Y}}_e \mid \mathbf{H}, \mathbf{H}_e)]\\ &\quad = \frac{1}{K-S}\Big(\mathbb{E}[I(\tilde{\mathbf{X}}_{s_{S+1}}; \bar{\mathbf{Y}}_e \mid \mathbf{H}, \mathbf{H}_e)]\\ &\qquad +\mathbb{E}[I(\tilde{\mathbf{X}}_{s_{S+2}}; \bar{\mathbf{Y}}_e \mid \tilde{\mathbf{X}}_{s_{S+1}}, \mathbf{H}, \mathbf{H}_e)] + \cdots\\ &\qquad +\mathbb{E}[I(\tilde{\mathbf{X}}_{s_K}; \bar{\mathbf{Y}}_e \mid \tilde{\mathbf{X}}_{s_{S+1}}, \ldots, \tilde{\mathbf{X}}_{s_{K-1}}, \mathbf{H}, \mathbf{H}_e)]\Big)\\ &\quad \leq \frac{1}{K-S}\Big(\mathbb{E}[I(\tilde{\mathbf{X}}_{s_1}; \bar{\mathbf{Y}}_e \mid \tilde{\mathbf{X}}_{\mathcal{S}^c}, \mathbf{H}, \mathbf{H}_e)]\\ &\qquad +\mathbb{E}[I(\tilde{\mathbf{X}}_{s_1}; \bar{\mathbf{Y}}_e \mid \tilde{\mathbf{X}}_{\mathcal{S}^c}, \mathbf{H}, \mathbf{H}_e)] + \cdots\\ &\qquad +\mathbb{E}[I(\tilde{\mathbf{X}}_{s_1}; \bar{\mathbf{Y}}_e \mid \tilde{\mathbf{X}}_{\mathcal{S}^c}, \mathbf{H}, \mathbf{H}_e)]\Big)\\ &\quad = \frac{1}{K-S}\Big((K-S)\mathbb{E}[I(\tilde{\mathbf{X}}_{s_1}; \bar{\mathbf{Y}}_e \mid \tilde{\mathbf{X}}_{\mathcal{S}^c}, \mathbf{H}, \mathbf{H}_e)]\Big)\\ &\quad = \frac{1}{S}\Big(S\mathbb{E}[I(\tilde{\mathbf{X}}_{s_1}; \bar{\mathbf{Y}}_e \mid \tilde{\mathbf{X}}_{\mathcal{S}^c}, \mathbf{H}, \mathbf{H}_e)]\Big)\\ &\quad = \frac{1}{S}\Big(\mathbb{E}[I(\tilde{\mathbf{X}}_{s_1}; \bar{\mathbf{Y}}_e \mid \tilde{\mathbf{X}}_{\mathcal{S}^c}, \mathbf{H}, \mathbf{H}_e)]\\ &\qquad +\mathbb{E}[I(\tilde{\mathbf{X}}_{s_2}; \bar{\mathbf{Y}}_e \mid \tilde{\mathbf{X}}_{\mathcal{S}^c}, \mathbf{H}, \mathbf{H}_e)] + \cdots\\ &\qquad +\mathbb{E}[I(\tilde{\mathbf{X}}_{s_S}; \bar{\mathbf{Y}}_e \mid \tilde{\mathbf{X}}_{\mathcal{S}^c}, \mathbf{H}, \mathbf{H}_e)]\Big)\\ &\quad \leq \frac{1}{S}\Big(\mathbb{E}[I(\tilde{\mathbf{X}}_{s_1}; \bar{\mathbf{Y}}_e \mid \tilde{\mathbf{X}}_{\mathcal{S}^c}, \mathbf{H}, \mathbf{H}_e)]\\ &\qquad +\mathbb{E}[I(\tilde{\mathbf{X}}_{s_2}; \bar{\mathbf{Y}}_e \mid \tilde{\mathbf{X}}_{\mathcal{S}^c}, \tilde{\mathbf{X}}_{s_1}, \mathbf{H}, \mathbf{H}_e)] + \cdots\\ &\qquad +\mathbb{E}[I(\tilde{\mathbf{X}}_{s_S}; \bar{\mathbf{Y}}_e \mid \tilde{\mathbf{X}}_{\mathcal{S}^c}, \tilde{\mathbf{X}}_{s_1}, \ldots, \tilde{\mathbf{X}}_{s_{S-1}}, \mathbf{H}, \mathbf{H}_e)]\Big)\\ &\quad = \frac{1}{|\mathcal{S}|}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{S}}; \bar{\mathbf{Y}}_e \mid \tilde{\mathbf{X}}_{\mathcal{S}^c}, \mathbf{H}, \mathbf{H}_e)] \end{aligned} \tag{30}$$

where we repeatedly use Lemma 6 for inequalities and use the fact that $\mathbb{E}[I(\tilde{\mathbf{X}}_k; \bar{\mathbf{Y}}_e \mid \tilde{\mathbf{X}}_{\mathcal{L}}, \mathbf{H}, \mathbf{H}_e)] = \mathbb{E}[I(\tilde{\mathbf{X}}_i; \bar{\mathbf{Y}}_e \mid \tilde{\mathbf{X}}_{\mathcal{L}}, \mathbf{H}, \mathbf{H}_e)]$ for any $k \neq i$ and for any $\mathcal{L} \subseteq \mathcal{K} - \{k, i\}$. We note that the last property stated above is due to the symmetry between network users provided by the random choice of user ordering at each fading block. ■

Lemma 8: Each user can set the randomization rates to be $\frac{1}{K}$th of the total DoF per orthogonal time-frequency slot seen by the eavesdropper, i.e., with a rate choice of

$$R_k^x = \frac{1}{KF}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{K}}; \bar{\mathbf{Y}}_e \mid \mathbf{H}, \mathbf{H}_e)] \tag{31}$$

each randomization message (codeword index), given the secrecy message (bin index) of each user, is decodable at the eavesdropper.

Proof:

Let $\mathcal{S} \subseteq \mathcal{K}$. From Lemma 7, we have

$$\frac{1}{|\mathcal{S}^c|}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{S}^c};\bar{\mathbf{Y}}_e \mid \mathbf{H},\mathbf{H}_e)] \leq \frac{1}{|\mathcal{S}|}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{S}};\bar{\mathbf{Y}}_e \mid \tilde{\mathbf{X}}_{\mathcal{S}^c},\mathbf{H},\mathbf{H}_e)].$$

We continue as shown

$$\begin{aligned}
&\frac{1}{|\mathcal{S}^c|}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{S}^c};\bar{\mathbf{Y}}_e \mid \mathbf{H},\mathbf{H}_e)]\\
&\quad\leq \frac{1}{|\mathcal{S}|}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{S}};\bar{\mathbf{Y}}_e \mid \tilde{\mathbf{X}}_{\mathcal{S}^c},\mathbf{H},\mathbf{H}_e)]\\
&\quad\Rightarrow |\mathcal{S}|\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{S}^c};\bar{\mathbf{Y}}_e \mid \mathbf{H},\mathbf{H}_e)]\\
&\quad\leq (K-|\mathcal{S}|)\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{S}};\bar{\mathbf{Y}}_e \mid \tilde{\mathbf{X}}_{\mathcal{S}^c},\mathbf{H},\mathbf{H}_e)]\\
&\quad\Rightarrow \frac{|\mathcal{S}|}{K}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{S}^c};\bar{\mathbf{Y}}_e \mid \mathbf{H},\mathbf{H}_e)]\\
&\quad\leq \frac{K-|\mathcal{S}|}{K}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{S}};\bar{\mathbf{Y}}_e \mid \tilde{\mathbf{X}}_{\mathcal{S}^c},\mathbf{H},\mathbf{H}_e)]\\
&\quad\Rightarrow \frac{|\mathcal{S}|}{K}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{K}};\bar{\mathbf{Y}}_e \mid \mathbf{H},\mathbf{H}_e)]\\
&\quad\leq \mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{S}};\bar{\mathbf{Y}}_e \mid \tilde{\mathbf{X}}_{\mathcal{S}^c},\mathbf{H},\mathbf{H}_e)],
\end{aligned}$$

from which we readily conclude that the rate assignment given by $R_k^x = \frac{1}{KF}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{K}};\bar{\mathbf{Y}}_e \mid \mathbf{H},\mathbf{H}_e)]$ satisfies

$$\sum_{k\in\mathcal{S}} R_k^x = \frac{|\mathcal{S}|}{KF}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{K}};\bar{\mathbf{Y}}_e \mid \mathbf{H},\mathbf{H}_e)] \leq \frac{1}{F}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{S}};\bar{\mathbf{Y}}_e \mid \tilde{\mathbf{X}}_{\mathcal{S}^c},\mathbf{H},\mathbf{H}_e)], \forall \mathcal{S} \subseteq \mathcal{K},$$

and hence randomization messages are decodable at the eavesdropper with this rate assignment. ■

REFERENCES

[1] A. 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] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[4] Y. Oohama, "Coding for relay channels with confidential messages," in *Proc. IEEE Inf. Theory Workshop (ITW'01)*, Cairns, Australia, Sep. 2001, pp. 87–89.

[5] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[6] L. Lai, H. El Gamal, and H. V. Poor, "The wiretap channel with feedback: Encryption over the channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 11, pp. 5059–5067, Nov. 2008.

[7] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[8] 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.

[9] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453–2496, Jun. 2008.

[10] A. Khisti and G. Wornell, "The MIMOME channel," in *Proc. 45th Annual Allerton Conf. Commun., Contr., Comput.*, Monticello, IL, Sep. 2007.

[11] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. 2008 IEEE Int. Symp. Inf. Theory (ISIT 2008)*, Toronto, Canada, Jul. 2008.

[12] 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.

[13] P. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[14] V. R. Cadambe and S. A. Jafar, "Interference alignment and degrees of freedom of the K-user interference channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3425–3441, Aug. 2008.

[15] M. A. Maddah-Ali, A. S. Motahari, and A. K. Khandani, "Communication over MIMO X channels: Interference alignment, decomposition, and performance analysis," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3457–3470, Aug. 2008.

[16] R. Liu, I. Maric, P. Spasojevic, and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages," in *Proc. 44th Ann. Allerton Conf. Commun., Contr., Comput.*, Monticello, IL, Sep. 2006.

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

[18] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai, and S. Verdu, "Capacity of cognitive interference channels with and without secrecy," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 604–619, Feb. 2009.

[19] O. O. Koyluoglu and H. El Gamal, "On the secrecy rate region for the interference channel," in *Proc. 2008 IEEE Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC'08)*, Cannes, France, Sep. 2008.

[20] O. O. Koyluoglu and H. El Gamal, "Cooperative encoding for secrecy in interference channels," *IEEE Trans. Inf. Theory*, to be published.

[21] T. Cover and J. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.

O. Ozan Koyluoglu (S'02) received the B.S. degree in electrical and electronics engineering from Bilkent University, Ankara, Turkey, in 2005, and the M.S. degree in electrical and computer engineering from Ohio State University, Columbus, in 2007.

He is currently a Ph.D. candidate at Ohio State University.

Mr. Koyluoglu is a recipient of the Ohio State University Fellowship Award (2005) and the Ohio State University Presidential Fellowship Award (2010).

Hesham El Gamal (M'99–SM'03–F'10) received the B.S. and M.S. degrees in electrical engineering from Cairo University, Cairo, Egypt, in 1993 and 1996, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Maryland at College Park, in 1999.

From 1993 to 1996, he served as a Project Manager with the Middle East Regional Office of Alcatel Telecom. From 1996 to 1999, he was a Research Assistant with the Department of Electrical and Computer Engineering, University of Maryland at College Park. From February 1999 to December 2000, he was with the Advanced Development Group, Hughes Network Systems (HNS), Germantown, MD, as a Senior Member of Technical Staff. Since January 2001, he has been with the Electrical and Computer Engineering Department, Ohio State University, where he is now a Professor. He held visiting appointments at UCLA, Institut Eurecom, and served as a Founding Director for the Wireless Intelligent Networks Center (WINC) at Nile University (2007–2009). He holds 12 patents.

Dr. El Gamal is a recipient of the HNS Annual Achievement Award (2000), the OSU College of Engineering Lumley Research Award (2003, 2008), the OSU Electrical Engineering Department FARMER Young Faculty Development Fund (2003–2008), the OSU Stanley E. Harrison Award (2008), and the National Science Foundation CAREER Award (2004). He has served as an Associate Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS (2001–2005), an Associate Editor for the IEEE TRANSACTIONS ON MOBILE COMPUTING (2003–2007), a Guest Associate Editor for the IEEE TRANSACTIONS ON INFORMATION THEORY Special Issue on Cooperative Communications (2007), a member of the SP4COM Technical Committee (2002–2005), a Co-Chair of the Globecom'08 Communication Theory Symposium, and a Co-Chair of the 2010 IEEE Information Theory Workshop. He currently serves as an Associate Editor for the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY and a Guest Associate Editor for the IEEE TRANSACTIONS ON INFORMATION THEORY.

Lifeng Lai (M'07) received the B.E. and M.E. degrees from Zhejiang University, Hangzhou, China, in 2001 and 2004, respectively, and the Ph.D. degree from The Ohio State University, Columbus, in 2007.

He was a Distinguished University Fellow of The Ohio State University from 2004 to 2007 and a Postdoctoral Research Associate at Princeton University, Princeton, NJ, from 2007 to 2009. Since August 2009, he has been an Assistant Professor with the University of Arkansas, Little Rock.

Dr. Lai is a corecipient of 2008 IEEE Global Communications Conference Best Paper Award.

H. Vincent Poor (S'72-M'77–SM'82–F'87) received the Ph.D. degree in electrical engineering and computer science from Princeton University, Princeton, NJ, in 1977.

From 1977 until 1990, he was on the faculty of the University of Illinois at Urbana-Champaign. Since 1990, he has been on the faculty at Princeton University, where he is the Dean of Engineering and Applied Science, and the Michael Henry Strater University Professor of Electrical Engineering. His research interests are in the areas of stochastic analysis, statistical signal processing and information theory, and their applications in wireless networks and related fields. Among his publications in these areas are *Quickest Detection* (Cambridge University Press, 2009), coauthored with O. Hadjiliadis, and *Information Theoretic Security* (Now Publishers, 2009), coauthored with Y. Liang and S. Shamai.

Dr. Poor is a member of the National Academy of Engineering, a Fellow of the American Academy of Arts and Sciences, and an International Fellow of the Royal Academy of Engineering (U.K.). He is also a Fellow of the Institute of Mathematical Statistics, the Optical Society of America, and other organizations. In 1990, he served as President of the IEEE Information Theory Society, in 2004–2007 as the Editor-in-Chief of these TRANSACTIONS, and in 2009 as General Co-Chair of the IEEE International Symposium on Information Theory, held in Seoul, South Korea. He received a Guggenheim Fellowship in 2002 and the IEEE Education Medal in 2005. Recent recognition of his work includes the 2008 Aaron D. Wyner Distinguished Service Award of the IEEE Information Theory Society, the 2009 Edwin Howard Armstrong Achievement Award of the IEEE Communications Society, the 2010 IET Ambrose Fleming Medal for Achievement in Communications, the 2010 IET Ambrose Fleming Medal for Achievement in Communications, and the 2011 IEEE Eric E. Sumner Award.