Interference Alignment for Secrecy

Onur Ozan Koyluoglu, Hesham El Gamal, Lifeng Lai, and H. Vincent Poor

arXiv:0810.1187v1 [cs.IT] 7 Oct 2008

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 one with an external eavesdropper, are analyzed. The key difference between the two models is the lack of channel state information (CSI) about the external eavesdropper. Using interference alignment along with secrecy pre-coding, 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.

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 (DoF).

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 by [6]. On the other hand, the multiple access and broadcast channels with secrecy constraints were investigated in [7], [8], [9]. Finally, 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].

Here, the frequency/time selective K-user Gaussian interference channel with secrecy constraints is considered. Without the secrecy constraints, it has been recently shown that a $\frac{1}{2}$ 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 (see also [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 channels with confidential messages [16], [17], [18] and the one with an external eavesdropper [19]. The frequency selective interference channel adopted in the present paper is, however, fundamentally different from these *memoryless* models.

We consider two distinct network models, namely 1) the interference channel with confidential messages and 2) the one with an external eavesdropper. 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

Onur Ozan Koyluoglu and Hesham El Gamal are with the Department of Electrical and Computer Engineering, The Ohio State University, Columbus, OH 43210 USA. Hesham El Gamal also serves as the Director for the Wireless Intelligent Networks Center (WINC), Nile University, Cairo, Egypt. Email: {koyluogo,helgamal}@ece.osu.edu.

Lifeng Lai and H. Vincent Poor are with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA. Email: {llai,poor}@princeton.edu.

This work is submitted to IEEE Transactions on Information Theory on October 7, 2008.

The material in this paper was presented in part at the IEEE International Symposium on Information Theory, Toronto, ON in July 2008. This research was supported in part by the US NSF under Grants CCF-07-28762, CCF-03-46887, ANI-03-38807, CNS-06-25637, and CCF-07-28208.

to the same network, one can assume the availability of channel state information (CSI) while designing the secrecy coding scheme. Towards this goal, we employ an interference alignment scheme along with secrecy pre-coding 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 small dimensionality 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 mixed together*. Our secrecy pre-coding takes advantage of the phenomenon to ensure that the resulting multiple access channel (from the $K-1$ interfering users) does not reveal any useful information about each non-intended message. This way, we show that $\frac{1}{4}$ **secure** DoF per orthogonal dimension is achievable for each user in the three-user Gaussian interference channel with confidential messages. We then generalize our results to the K-user Gaussian interference channel showing that each user can achieve $\frac{K-2}{2K-2}$ secure DoF. In the second scenario, we study the external eavesdropper model where the fundamental challenge is the lack of channel state information (CSI) about the links connected to it. Despite this fact, it is shown that $1/2-1/K$ DoF per user is achievable in the ergodic setting. This result provides further evidence on 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 wireless network. The underlying idea is that the coordination between several source-destination pairs allows for *hiding* the secret messages in the background interference.

The remainder of the 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 technical results needed to develop our proofs are collected in the appendices to enhance the flow of the paper.

II. System Model

A. The Confidential Messages Scenario

We consider a frequency selective wireless network comprised of K transmitter-receiver pairs where the i^{th} receiver output at time $t \in \{1, \cdots, n\}$ and frequency slot $f \in \{1, \cdots, F\}$ is given by [1]

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

Here, $X_k(f,t)$ is the transmitted symbol of user k at frequency slot f during time t, and $Z_i(f,t) \sim \mathcal{CN}(0,1)$ is the additive white Gaussian noise at receiver i. We assume that the channel coefficients are randomly generated according to a continuous distribution and are fixed during the communication period. We also assume that the channel coefficients are known at every node in the network. The network model is provided in Fig. 1.

Using the extended channel notation of [14], the i^{th} received vector during time slot t can be written as

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

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

[1] In this paper, matrices are represented with bold capital letters ($\mathbf{X}$) and vectors are denoted as bold capital letters with bars or tildes (for example, $\bar{\mathbf{X}}$ and $\tilde{\mathbf{X}}$). We define $\mathcal{K} \triangleq \{1, \cdots, K\}$ and denote $\mathbf{X}_{\mathcal{S}} \triangleq \{\mathbf{X}_k | k \in \mathcal{S}\}$ for $\mathcal{S} \subset \mathcal{K}$. A zero-mean circularly symmetric complex Gaussian random variable with variance σ^2 is denoted by $\mathcal{CN}(0, \sigma^2)$.

We assume that each source $k \in \mathcal{K}$ has a message W_k which must be transmitted in secrecy from the remaining $K-1$ receivers. Therefore, our $(n, F, M_1, \cdots, M_K)$ secret codebook has the following components:

1) The secret message set $\mathcal{W}_k = \{1, \cdots, M_k\}$.

2) Encoding functions $f_k(.)$ which map the secret messages to the transmitted symbols, i.e., $f_k : w_k \rightarrow (\bar{\mathbf{X}}_k(1), \cdots, \bar{\mathbf{X}}_k(n))$ 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.,

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

3) Decoding functions $\phi_k(.)$ 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 $\mathbf{Y}_k = \{\bar{\mathbf{Y}}_k(1), \cdots, \bar{\mathbf{Y}}_k(n)\}$.

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

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

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 $W_{\mathcal{S}}$, $\mathcal{S} \subset \mathcal{K} - i$, is

$$\Delta_{\mathcal{S},i} \triangleq \frac{H\left(W_{\mathcal{S}}|\mathbf{Y}_i\right)}{H\left(W_{\mathcal{S}}\right)}.$$

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

$$\begin{aligned} \frac{1}{nF}\log_2 M_k &= R_k,\ \forall k \in \mathcal{K}, \\ \max\{P_{e,1}, \cdots, P_{e,K}\} &\leq \epsilon, \end{aligned} \tag{3}$$

and

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

where a symmetric secrecy notion for each user in the network is used. We also say that the symmetric degrees of freedom (per orthogonal frequency-time slot) of η is achievable with perfect secrecy, if the rate-equivocation tuple $(R_1 = R, \cdots, R_K = R, d = 1)$ is achievable and

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

B. *The External Eavesdropper Scenario*

In this model, we assume 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 denote the received signals at receiver $i \in \{1, \cdots, K, e\}$ using the extended channel notation as follows

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

where $b \in \{1, \cdots, B\}$ denotes the fading block b, $j \in \{1, \cdots, n_1\}$ denotes the j^{th} time instant of the corresponding fading block, $\mathbf{H}_{i,k}(b)$ 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 j^{th} symbol of the b^{th} fading block. We further define $\mathbf{H} \triangleq \{\mathbf{H}_{i,k}(b) : i,k \in \mathcal{K}, b \in \{1, \cdots, B\}\}$ and $\mathbf{H}_e \triangleq \{\mathbf{H}_{e,k}(b) : k \in \mathcal{K}, b \in \{1, \cdots, B\}\}$. We assume that $\mathbf{H}$ is known at all the nodes in the network, whereas $\mathbf{H}_e$ is known only at the eavesdropper (only the statistical knowledge about 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 components of the secrecy codebook remain as before with the exception that each transmitter must secure its own message *only* from the external eavesdropper. Accordingly, we modify the secrecy requirement by considering the normalized equivocation seen by the eavesdropper. We denote the observation at the eavesdropper as $\mathbf{Y}_e = \{\bar{\mathbf{Y}}_e(1), \cdots, \bar{\mathbf{Y}}_e(n)\}$, in which $\bar{\mathbf{Y}}_e(t)$ is defined similarly as $\bar{\mathbf{Y}}_i(t)$ for $t = 1, \cdots, n$. Therefore, the normalized equivocation for a subset of messages $\mathcal{S} \subset \mathcal{K}$ is given by

$$\Delta_{\mathcal{S}} \triangleq \frac{H\left(W_{\mathcal{S}} | \mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e\right)}{H\left(W_{\mathcal{S}}\right)}.$$

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

$$\begin{aligned} \frac{1}{nF} \log_2 M_k &= R_k, \ \forall k \in \mathcal{K}, \\ \max\{P_{e,1}, \cdots, P_{e,K}\} &\leq \epsilon, \end{aligned} \tag{5}$$

and

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

It then follows that the symmetric DoF with perfect secrecy is defined along the same lines as in the previous section.

III. The 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. Let $F = 2m+1$ for some $m \in \mathbb{N}$. This is the $(2m+1)$ symbol extension of the three-user channel considered in [14]. We now employ interference alignment precoding using the matrices $\bar{\mathbf{V}}_k$ of [14], so that the transmitted signals are of 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). According to the interference alignment principle, the beamforming matrices $\bar{\mathbf{V}}_k$ are constructed to satisfy the following two properties:

1) The non-intended signals seen by each receiver are aligned within some low dimensionality 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 that of $\mathbf{H}_{i,k}\bar{\mathbf{V}}_k$ for each user $k \in \mathcal{K} - i$.

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 users 2 and 3. This particular eavesdropper now sees the m streams $\tilde{\mathbf{X}}_2(t)$ and m streams $\tilde{\mathbf{X}}_3(t)$ mixed together in a multiple access channel with **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 the second potential eavesdropper. In the limit of a large $F = 2m+1$, the $m/2$ secure streams results in $1/4$ secure DoF. This intuitive discussion is formalize for the general case of a K-user Gaussian interference channel in the following.

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

Proof: We shall 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 probability that approaches to 1, for all channel coefficients, as $n, m, \rho \to \infty$.

Fix an $m \in \mathbb{N}$. Let $m_1 = (m+1)^M$, $m_k = m^M \; \forall k \neq 1$, $M = (K-1)(K-2)-1$, and $F = (m+1)^M + m^M$ frequency slots. We now generate, for each user k, $2^{nm_k\left(\frac{F}{m_k}(R_k+R_k^x)\right)}$ codewords each of length nm_k with entries that are independent and identically distributed (i.i.d.) $\sim \mathcal{CN}\left(0, \frac{\rho-\epsilon}{c_k}\right)$. 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 k^{th} 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 secrecy message and the index $w_k^x \in \{1, \cdots, M_k^x\}$ is the randomization message. It is easy to see that the secure transmission rate per orthogonal time and frequency slot is R_k.

To send a message w_k, the k^{th} transmitter looks into the bin $w_k \in \mathcal{W}_k$ and randomly selects a codeword in this bin, denoted by the index w_k^x, according to uniform distribution. 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 $\hat{\mathbf{X}}_k(w_k, w_k^x) = [\tilde{\mathbf{X}}_k(1), \cdots, \tilde{\mathbf{X}}_k(n)]$, where each element is an $m_k \times 1$ vector. Then, for each symbol time $t \in \{1, \cdots, n\}$, the transmitter employs the interference alignment scheme, and maps $\tilde{\mathbf{X}}_k(t)$ to $\bar{\mathbf{X}}_k(t)$ via $\bar{\mathbf{X}}_k(t) = \bar{\mathbf{V}}_k\tilde{\mathbf{X}}_k(t)$, where we choose the interference alignment matrices $\bar{\mathbf{V}}_k$ as in [14].

We choose the secrecy and randomization rates as follows [2].

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

The above rates are inside the decodability region for each user, i.e., $R_k + R_k^x \leq \frac{1}{F}I(\tilde{\mathbf{X}}_k;\bar{\mathbf{Y}}_k)$, $\forall k \in \mathcal{K}$, implying that each user can reliably decode its own streams as $n \to \infty$. Hence, using the union bound argument, we can show that for a given ϵ there exists $n_0(\epsilon)$ such that for any $n > n_0(\epsilon)$ $\max\{P_{e,1}, \cdots, P_{e,K}\} \leq \epsilon$ 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 $\mathcal{S} \subset \mathcal{K}-i$ 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 since Lemma 4 shows that perfect secrecy of the full message set implies secrecy for all subsets (Here, the full message set at the receiver i refers to $W_{\mathcal{K}-i}$.). Denoting the observation of the eavesdropper as $\mathbf{Y}_i$, we write

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

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

$$
I(W_{\mathcal{K}-i},W_{\mathcal{K}-i}^x;\mathbf{Y}_i) \leq I(\tilde{\mathbf{X}}_{\mathcal{K}-i}(1),\cdots,\tilde{\mathbf{X}}_{\mathcal{K}-i}(n);\mathbf{Y}_i) \tag{8}
$$

[2] Since the channel coefficients are fixed and known everywhere, we omit the conditioning on them here.

due to the Markov chain relationship

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

Combining this with the fact that

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

we obtain

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

Second

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

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 $\sum_{k \in \mathcal{S}} R^x_k \leq \frac{1}{F} I(\tilde{\mathbf{X}}_{\mathcal{S}}; \bar{\mathbf{Y}}_i | \tilde{\mathbf{X}}_{\mathcal{K}-\mathcal{S}-i})$, $\forall \mathcal{S} \subset \mathcal{K} - i$ [20, Chapter 14]. Then, by Fano's inequality, we have $H(W^x_{\mathcal{K}-i} | W_{\mathcal{K}-i} = w_{\mathcal{K}-i}, \mathbf{Y}_i) \leq n\delta(n, w_{\mathcal{K}-i})$, where $\delta(n, w_{\mathcal{K}-i}) \rightarrow 0$ as $n \rightarrow \infty$. Then, defining $\delta(n) \triangleq \max_{w_{\mathcal{K}-i} \in \mathcal{W}_{\mathcal{K}-i}} \delta(n, w_{\mathcal{K}-i})$, we have

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

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

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

$$\begin{aligned} \hat{\delta} &\triangleq \frac{\delta(n) + \max_{p(\tilde{\mathbf{X}}_{\mathcal{K}-i})} I(\tilde{\mathbf{X}}_{\mathcal{K}-i}; \bar{\mathbf{Y}}_i) - F \sum_{k \in \mathcal{K}-i} R^x_k}{F \sum_{k \in \mathcal{K}-i} R_k}, \\ &= \frac{\delta(n) + \max_{p(\tilde{\mathbf{X}}_{\mathcal{K}-i})} I(\tilde{\mathbf{X}}_{\mathcal{K}-i}; \bar{\mathbf{Y}}_i) - (K-1) \min_{i \in \mathcal{K}, \mathcal{S} \subseteq \mathcal{K}-i} \left\{\frac{1}{|\mathcal{S}|} I(\tilde{\mathbf{X}}_{\mathcal{S}}; \bar{\mathbf{Y}}_i | \tilde{\mathbf{X}}_{\mathcal{K}-\mathcal{S}-i})\right\}}{(K-1) \min_{i \in \mathcal{K}} \left\{I(\tilde{\mathbf{X}}_i; \bar{\mathbf{Y}}_i)\right\} - \max_{i \in \mathcal{K}} \left\{I(\tilde{\mathbf{X}}_{\mathcal{K}-i}; \bar{\mathbf{Y}}_i)\right\}}, \end{aligned} \tag{14}$$

where we used the fact that $H(W_{\mathcal{K}-i}) = nF \sum_{k \in \mathcal{K}-i} R_k$ and the rate assignment given by (6).

It is already observed that $\delta(n) \rightarrow 0$ as $n \rightarrow \infty$ 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) imply the followings.

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

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

where $r = m^M$ or $r = (m+1)^M$ depending on i,

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

and

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

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

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

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

$$\eta = \lim_{m,\rho\to\infty} \frac{R_k}{\log(\rho)} = \frac{K-2}{2K-2}. \tag{20}$$

which proves our result. ■

IV. The K-User Gaussian Interference Channel with an External Eavesdropper

First, it is easy to see 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 another one with $K+1$-users. 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 of 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, a secure DoF of $\eta = \frac{K-1}{2K}$ per frequency-time slot is almost surely achievable for each user (assuming the availability of the eavesdropper CSI).

More interestingly, it is still possible to achieve positive secure DoF per user in the **absence** of the eavesdropper CSI by exploiting the channel **ergodicity**. In the ergodic model, the channel gains are assumed to be fixed during a block of n_1 symbol times 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 use the $K = 3$ case. Here, the users of the network have $\frac{3m+1}{2m+1}$ total DoF while the multiple access channel (MAC) 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, a secure DoF of $\eta = \frac{1}{2} - \frac{1}{K}$ per frequency-time slot is achievable for each user in the ergodic setting (in the absence of the eavesdropper CSI).

Proof: Let $m \in \mathbb{N}$ and $F = (m+1)^M + m^M$, where $M = (K-1)(K-2)-1$. 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 $b \in \{1, \cdots, B\}$, we randomly pick, according to uniform distribution, a permutation from Π and denote it by π_b. 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 the 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 each of length $n_1\sum_{b=1}^{B} m_{k(b)}$, where entries are chosen i.i.d. $\sim \mathcal{CN}\left(0, \frac{P-\epsilon}{c}\right)$ for some $\epsilon > 0$ and 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. Given w_k, transmitter k chooses the corresponding bin and independently (according to uniform distribution) chooses a codeword in that bin denoted by $\hat{\mathbf{X}}_k(w_k, w_k^x)$, where w_k^x is the randomization index. This codeword is then divided into B blocks, each with a length $n_1 m_{k(b)}$ symbols. Each block is then arranged in the following $m_{k(b)} \times n_1$ matrix $[\tilde{\mathbf{X}}_k(1+(b-1)n_1), \cdots, \tilde{\mathbf{X}}_k(n_1+(b-1)n_1)]$, where $\tilde{\mathbf{X}}_k(j+(b-1)n_1)$, for $1 \leq j \leq n_1$, is an $m_{k(b)} \times 1$ vector. At time slot $t = j+(b-1)n_1$, the k^{th} transmitter maps $\tilde{\mathbf{X}}_k(t)$ to $\bar{\mathbf{X}}_k(t)$ via $\bar{\mathbf{X}}_k(t) = \bar{\mathbf{V}}_{k(b)}\tilde{\mathbf{X}}_k(t)$. Finally, we would like to emphasize the fact that in the sequel expectations will be taken with respect to the random distribution of the channel matrices and the uniform distribution underlying the permutation operators used in different fading blocks.

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 $\forall i, k \in \mathcal{K}$ and $b \in \{1, \cdots, B\}$. This property will allow us to drop the subscript i and write $\mathbb{E}[I(\tilde{\mathbf{X}}_i; \bar{\mathbf{Y}}_i|\mathbf{H})] = \mathbb{E}[I(\tilde{\mathbf{X}}; \bar{\mathbf{Y}}|\mathbf{H})], \forall i \in \mathcal{K}$ in the following. To satisfy the achievability conditions and the secrecy requirements of the network, we choose R_k and R_k^x as follows

$$\begin{aligned} R_k &= \frac{1}{KF}\left(K\mathbb{E}[I(\tilde{\mathbf{X}}; \bar{\mathbf{Y}}|\mathbf{H})] - \max_{p(\bar{\mathbf{X}}_{\mathcal{K}})} \mathbb{E}[I(\bar{\mathbf{X}}_{\mathcal{K}}; \bar{\mathbf{Y}}_e|\mathbf{H}, \mathbf{H}_e)]\right) \quad \text{and} \\ R_k^x &= \frac{1}{KF}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{K}}; \bar{\mathbf{Y}}_e|\mathbf{H}, \mathbf{H}_e)], \end{aligned} \tag{21}$$

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

$$\begin{aligned} R_k + R_k^x &= \frac{1}{F}\mathbb{E}[I(\tilde{\mathbf{X}}; \bar{\mathbf{Y}}|\mathbf{H})] - \frac{1}{KF}\max_{p(\bar{\mathbf{X}}_{\mathcal{K}})} \mathbb{E}[I(\bar{\mathbf{X}}_{\mathcal{K}}; \bar{\mathbf{Y}}_e|\mathbf{H}, \mathbf{H}_e)] + \frac{1}{KF}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{K}}; \bar{\mathbf{Y}}_e|\mathbf{H}, \mathbf{H}_e)] \\ &\leq \frac{1}{F}\mathbb{E}[I(\tilde{\mathbf{X}}; \bar{\mathbf{Y}}|\mathbf{H})], \end{aligned} \tag{22}$$

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). The next step is to study the equivocation at the eavesdropper, i.e.,

$$\begin{aligned} \frac{1}{n}H(W_{\mathcal{K}}|\mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e) &= \frac{1}{n}\big(H(W_{\mathcal{K}}, \mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e) - H(\mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e)\big) \\ &= \frac{1}{n}\big(H(W_{\mathcal{K}}, W_{\mathcal{K}}^x, \mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e) - H(W_{\mathcal{K}}^x|W_{\mathcal{K}}, \mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e) \\ &\quad - H(\mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e)\big) \\ &= \frac{1}{n}\big(H(W_{\mathcal{K}}) + H(W_{\mathcal{K}}^x|W_{\mathcal{K}}) + H(\mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e|W_{\mathcal{K}}, W_{\mathcal{K}}^x) \\ &\quad - H(W_{\mathcal{K}}^x|W_{\mathcal{K}}, \mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e) - H(\mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e)\big) \\ &= \frac{1}{n}\big(H(W_{\mathcal{K}}) + H(W_{\mathcal{K}}^x) - I(W_{\mathcal{K}}, W_{\mathcal{K}}^x; \mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e) \\ &\quad - H(W_{\mathcal{K}}^x|W_{\mathcal{K}}, \mathbf{Y}_e, \mathbf{H}, \mathbf{H}_e)\big), \end{aligned} \tag{23}$$

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

$$H(W_{\mathcal{K}}^x) = \log\left(\prod_{k=1}^{K} M_k^x\right) = \sum_{k=1}^{K} nFR_k^x = n\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{K}}; \bar{\mathbf{Y}}_e|\mathbf{H}, \mathbf{H}_e)] \tag{24}$$

and

$$
\begin{aligned}
\lim_{n\to\infty}\frac{1}{n}I(W_{\mathcal{K}},W_{\mathcal{K}}^{x};\mathbf{Y}_e,\mathbf{H},\mathbf{H}_e) &\leq \lim_{n\to\infty}\frac{1}{n}I(\tilde{\mathbf{X}}_{\mathcal{K}}(1),\cdots,\tilde{\mathbf{X}}_{\mathcal{K}}(n);\mathbf{Y}_e,\mathbf{H},\mathbf{H}_e)\\
&= \lim_{n\to\infty}\frac{1}{n}\big(I(\tilde{\mathbf{X}}_{\mathcal{K}}(1),\cdots,\tilde{\mathbf{X}}_{\mathcal{K}}(n);\mathbf{H},\mathbf{H}_e)\\
&\quad +I(\tilde{\mathbf{X}}_{\mathcal{K}}(1),\cdots,\tilde{\mathbf{X}}_{\mathcal{K}}(n);\mathbf{Y}_e|\mathbf{H},\mathbf{H}_e)\big)\\
&= \lim_{n\to\infty}\frac{1}{n}I(\tilde{\mathbf{X}}_{\mathcal{K}}(1),\cdots,\tilde{\mathbf{X}}_{\mathcal{K}}(n);\mathbf{Y}_e|\mathbf{H},\mathbf{H}_e)\\
&= \mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{K}};\bar{\mathbf{Y}}_e|\mathbf{H},\mathbf{H}_e)], \qquad (25)
\end{aligned}
$$

where the first inequality is due to the Markov chain relationship

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

and the last one is due to ergodicity. For the last term of (23), we observe that the channel seen by the eavesdropper reduces to a fading MAC channel for the randomization messages due to the 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). Then, by Fano's inequality, we have

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

for almost all codebooks in the ensemble. Therefore, by dividing both sides of (23) by $\frac{1}{n}H(W_{\mathcal{K}})$, we can ensure

$$\Delta_{\mathcal{K}}=\frac{H(W_{\mathcal{K}}|\mathbf{Y}_e,\mathbf{H},\mathbf{H}_e)}{H(W_{\mathcal{K}})}\geq 1-\epsilon, \qquad (26)$$

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

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

and hence

$$
\begin{aligned}
\lim_{\rho\to\infty}\frac{R_k}{\log(\rho)} &= \frac{1}{KF}\left(K\left(\frac{1}{K}m_1+\frac{K-1}{K}m_2\right)-F\right)\\
&= \frac{(K-2)m^M}{KF} \qquad (27)
\end{aligned}
$$

implying that $\eta=\frac{m^M}{F}-\frac{2m^M}{KF}$ DoF is achievable for each user for any m. Consequently, we conclude that $\lim\limits_{m\to\infty}\eta=\frac{1}{2}-\frac{1}{K}$ 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 when the eavesdropper CSI is assumed to be available our results hold almost surely for all channel realizations. 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 non-zero DoF for $K\geq 2$. This seemingly surprising result is due to 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. Conclusions

In this work, we have considered the K-user Gaussian interference channel with secrecy constraints. By using the interference alignment scheme along with secrecy pre-coding at each transmitter, we have shown that each user in the network can achieve a non-zero secure DoF. Our results differentiate between the confidential messages scenario and the case where an external eavesdropper, with unknown CSI, is present in the network. The most interesting aspect of our results is, perhaps, the discovery of the role of interference in increasing the secrecy capacity of multi-user wireless networks.

Appendix I
Lemma 4

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 $\Delta_{\mathcal{K}-i,i} \geq 1 - \epsilon^*(i,\epsilon,d)$ then $\Delta_{\mathcal{S},i} \geq d - \epsilon$, $\forall \mathcal{S} \subseteq \mathcal{K} - i$.

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

$$\begin{aligned} &H(\mathcal{W}_\mathcal{S}|\mathbf{Y}_i) + H(\mathcal{W}_{\mathcal{K}-i}|\mathcal{W}_\mathcal{S},\mathbf{Y}_i) = H(\mathcal{W}_{\mathcal{K}-i}|\mathbf{Y}_i) \\ &\geq H(\mathcal{W}_{\mathcal{K}-i}) - \epsilon^*(i,\epsilon,d)H(\mathcal{W}_{\mathcal{K}-i}) \\ &\geq H(\mathcal{W}_\mathcal{S}) + H(\mathcal{W}_{\mathcal{K}-i}|\mathcal{W}_\mathcal{S}) - (1+\epsilon-d)H(\mathcal{W}_\mathcal{S}), \end{aligned} \tag{28}$$

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,

$$\Delta_{\mathcal{S},i} = \frac{H(\mathcal{W}_\mathcal{S}|\mathbf{Y}_i)}{H(\mathcal{W}_\mathcal{S})} \geq (d-\epsilon) + \frac{H(\mathcal{W}_{\mathcal{K}-i}|\mathcal{W}_\mathcal{S}) - H(\mathcal{W}_{\mathcal{K}-i}|\mathcal{W}_\mathcal{S},\mathbf{Y}_i)}{H(\mathcal{W}_\mathcal{S})} \geq (d-\epsilon),$$

as conditioning does not increase entropy. ■

Appendix II
Lemma 5

Lemma 5: The gain matrix, resulting from the interference alignment scheme, 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: We have rank$(\mathbf{H}_{k,k}\bar{\mathbf{V}}_k) = m_k$ by the construction given in [14]. Now, the second observation follows by the design of interference alignment vectors, which have linearly independent 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.). Here, rank$(\mathbf{H}_{i,k}\bar{\mathbf{V}}_k) \leq \min\{m_k, F\} = m_k$ for $i \neq k$. We need only 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 $\{h_{i,k}(1), h_{i,k}(2), \cdots, h_{i,k}(F)\}$ and denoting the rows of the interference alignment matrix by $\mathbf{v}_f$, i.e., $\bar{\mathbf{V}}_k = [\mathbf{v}_1^T; \mathbf{v}_2^T; \cdots; \mathbf{v}_F^T]^T$, we have $\mathbf{H}_{i,k}\bar{\mathbf{V}}_k = [h_{i,k}(1)\mathbf{v}_1^T; h_{i,k}(2)\mathbf{v}_2^T; \cdots; h_{i,k}(F)\mathbf{v}_F^T]^T$. At this point, as the channel gains are chosen according to a continuous distribution, the $h_{ik}(f)$'s are non-zero with probability one for $f \in \{1, 2, \cdots, F\}$. Hence, these row operations will not change the rank of a matrix, i.e., rank$(\mathbf{H}_{i,k}\bar{\mathbf{V}}_k) =$ rank$(\bar{\mathbf{V}}_k) = m_k$. Therefore, the gain matrices seen by the receivers have full rank with probability one. ■

Appendix III
Lemma 6

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

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

Proof:

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

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

Appendix IV
Lemma 7

Lemma 7:

$$\frac{1}{|\mathcal{S}^c|}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{S}^c}; \bar{\mathbf{Y}}_e|\mathbf{H}, \mathbf{H}_e)] \leq \frac{1}{|\mathcal{S}|}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{S}}; \bar{\mathbf{Y}}_e|\tilde{\mathbf{X}}_{\mathcal{S}^c}, \mathbf{H}, \mathbf{H}_e)] \tag{30}$$

Proof: Let us denote $|\mathcal{S}| = S$; and define $\mathcal{S} = \{s_1, \cdots, s_S\}$ and $\mathcal{S}^c = \{s_{S+1}, \cdots, s_K\}$. Then we have

$$\begin{aligned} &\frac{1}{|\mathcal{S}^c|}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{S}^c}; \bar{\mathbf{Y}}_e|\mathbf{H}, \mathbf{H}_e)] \\ &= \frac{1}{K-S}\Big(\mathbb{E}[I(\tilde{\mathbf{X}}_{s_{S+1}}; \bar{\mathbf{Y}}_e|\mathbf{H}, \mathbf{H}_e)] + \mathbb{E}[I(\tilde{\mathbf{X}}_{s_{S+2}}; \bar{\mathbf{Y}}_e|\tilde{\mathbf{X}}_{s_{S+1}}, \mathbf{H}, \mathbf{H}_e)] + \cdots \\ &\quad + \mathbb{E}[I(\tilde{\mathbf{X}}_{s_K}; \bar{\mathbf{Y}}_e|\tilde{\mathbf{X}}_{s_{S+1}}, \cdots, \tilde{\mathbf{X}}_{s_{K-1}}, \mathbf{H}, \mathbf{H}_e)]\Big) \\ &\leq \frac{1}{K-S}\Big(\mathbb{E}[I(\tilde{\mathbf{X}}_{s_1}; \bar{\mathbf{Y}}_e|\tilde{\mathbf{X}}_{\mathcal{S}^c}, \mathbf{H}, \mathbf{H}_e)] + \mathbb{E}[I(\tilde{\mathbf{X}}_{s_1}; \bar{\mathbf{Y}}_e|\tilde{\mathbf{X}}_{\mathcal{S}^c}, \mathbf{H}, \mathbf{H}_e)] + \cdots \\ &\quad + \mathbb{E}[I(\tilde{\mathbf{X}}_{s_1}; \bar{\mathbf{Y}}_e|\tilde{\mathbf{X}}_{\mathcal{S}^c}, \mathbf{H}, \mathbf{H}_e)]\Big) \\ &= \frac{1}{K-S}\Big((K-S)\mathbb{E}[I(\tilde{\mathbf{X}}_{s_1}; \bar{\mathbf{Y}}_e|\tilde{\mathbf{X}}_{\mathcal{S}^c}, \mathbf{H}, \mathbf{H}_e)]\Big) \\ &= \frac{1}{S}\Big(S\mathbb{E}[I(\tilde{\mathbf{X}}_{s_1}; \bar{\mathbf{Y}}_e|\tilde{\mathbf{X}}_{\mathcal{S}^c}, \mathbf{H}, \mathbf{H}_e)]\Big) \\ &= \frac{1}{S}\Big(\mathbb{E}[I(\tilde{\mathbf{X}}_{s_1}; \bar{\mathbf{Y}}_e|\tilde{\mathbf{X}}_{\mathcal{S}^c}, \mathbf{H}, \mathbf{H}_e)] + \mathbb{E}[I(\tilde{\mathbf{X}}_{s_2}; \bar{\mathbf{Y}}_e|\tilde{\mathbf{X}}_{\mathcal{S}^c}, \mathbf{H}, \mathbf{H}_e)] + \cdots \\ &\quad + \mathbb{E}[I(\tilde{\mathbf{X}}_{s_S}; \bar{\mathbf{Y}}_e|\tilde{\mathbf{X}}_{\mathcal{S}^c}, \mathbf{H}, \mathbf{H}_e)]\Big) \\ &\leq \frac{1}{S}\Big(\mathbb{E}[I(\tilde{\mathbf{X}}_{s_1}; \bar{\mathbf{Y}}_e|\tilde{\mathbf{X}}_{\mathcal{S}^c}, \mathbf{H}, \mathbf{H}_e)] + \mathbb{E}[I(\tilde{\mathbf{X}}_{s_2}; \bar{\mathbf{Y}}_e|\tilde{\mathbf{X}}_{\mathcal{S}^c}, \tilde{\mathbf{X}}_{s_1}, \mathbf{H}, \mathbf{H}_e)] + \cdots \\ &\quad + \mathbb{E}[I(\tilde{\mathbf{X}}_{s_S}; \bar{\mathbf{Y}}_e|\tilde{\mathbf{X}}_{\mathcal{S}^c}, \tilde{\mathbf{X}}_{s_1}, \cdots, \tilde{\mathbf{X}}_{s_{S-1}}, \mathbf{H}, \mathbf{H}_e)]\Big) \\ &= \frac{1}{|\mathcal{S}|}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{S}}; \bar{\mathbf{Y}}_e|\tilde{\mathbf{X}}_{\mathcal{S}^c}, \mathbf{H}, \mathbf{H}_e)], \end{aligned} \tag{31}$$

where we repeatedly use Lemma 6 for inequalities and use the fact that $\mathbb{E}[I(\tilde{\mathbf{X}}_k;\bar{\mathbf{Y}}_e|\tilde{\mathbf{X}}_{\mathcal{L}},\mathbf{H},\mathbf{H}_e)] = \mathbb{E}[I(\tilde{\mathbf{X}}_i;\bar{\mathbf{Y}}_e|\tilde{\mathbf{X}}_{\mathcal{L}},\mathbf{H},\mathbf{H}_e)]$ for any $k \neq i$ and for any $\mathcal{L} \subset \mathcal{K} - \{k,i\}$. 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.

■

APPENDIX V
LEMMA 8

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

$$R_k^x = \frac{1}{KF}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{K}};\bar{\mathbf{Y}}_e|\mathbf{H},\mathbf{H}_e)], \tag{32}$$

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

Proof: Let $\mathcal{S} \subset \mathcal{K}$. From Lemma 7, we have

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

We continue as below.

$$\begin{aligned}
\frac{1}{|\mathcal{S}^c|}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{S}^c};\bar{\mathbf{Y}}_e|\mathbf{H},\mathbf{H}_e)] &\leq \frac{1}{|\mathcal{S}|}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{S}};\bar{\mathbf{Y}}_e|\tilde{\mathbf{X}}_{\mathcal{S}^c},\mathbf{H},\mathbf{H}_e)] &(33)\\
\Leftrightarrow |\mathcal{S}|\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{S}^c};\bar{\mathbf{Y}}_e|\mathbf{H},\mathbf{H}_e)] &\leq (K-|\mathcal{S}|)\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{S}};\bar{\mathbf{Y}}_e|\tilde{\mathbf{X}}_{\mathcal{S}^c},\mathbf{H},\mathbf{H}_e)] &(34)\\
\Leftrightarrow \frac{|\mathcal{S}|}{K}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{S}^c};\bar{\mathbf{Y}}_e|\mathbf{H},\mathbf{H}_e)] &\leq \frac{K-|\mathcal{S}|}{K}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{S}};\bar{\mathbf{Y}}_e|\tilde{\mathbf{X}}_{\mathcal{S}^c},\mathbf{H},\mathbf{H}_e)] &(35)\\
\Leftrightarrow \frac{|\mathcal{S}|}{K}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{K}};\bar{\mathbf{Y}}_e|\mathbf{H},\mathbf{H}_e)] &\leq \mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{S}};\bar{\mathbf{Y}}_e|\tilde{\mathbf{X}}_{\mathcal{S}^c},\mathbf{H},\mathbf{H}_e)], &(36)
\end{aligned}$$

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

$$\sum_{k\in\mathcal{S}} R_k^x = \frac{|\mathcal{S}|}{KF}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{K}};\bar{\mathbf{Y}}_e|\mathbf{H},\mathbf{H}_e)] \leq \frac{1}{F}\mathbb{E}[I(\tilde{\mathbf{X}}_{\mathcal{S}};\bar{\mathbf{Y}}_e|\tilde{\mathbf{X}}_{\mathcal{S}^c},\mathbf{H},\mathbf{H}_e)], \forall \mathcal{S} \subset \mathcal{K}, \tag{37}$$

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

References

[1] A. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, 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, July 1978.

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

[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, Sept. 2008.

[6] L. Lai, H. El Gamal, and H. V. Poor, "The wiretap channel with feedback: Encryption over the channel," *IEEE Trans. Inf. Theory*, to appear.

[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, June 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," *IEEE Trans. Inf. Theory*, 2007, submitted for publication.

[10] A. Khisti and G. Wornell, "The MIMOME channel," in *Proceedings of the 45th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, Sept. 2007.

[11] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, 2007, submitted for publication.

[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, June 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 Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, Sept. 2006.

[17] ——, "Discrete memoryless interference and broadcast channels with confidential messages:secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493-2507, June 2008.

[18] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai, and S. Verdu, "Capacity of cognitive interference channels with and without confidential messages," *IEEE Trans. Inf. Theory*, to appear.

[19] O. O. Koyluoglu and H. El Gamal "On the Secrecy Rate Region for the Interference Channel," in *Proc. 2008 IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'08)*, Cannes, France, Sept. 2008.

[20] T. Cover and J. Thomas, *Elements of Information Theory*, John Wiley and Sons, Inc., New York, 1991.

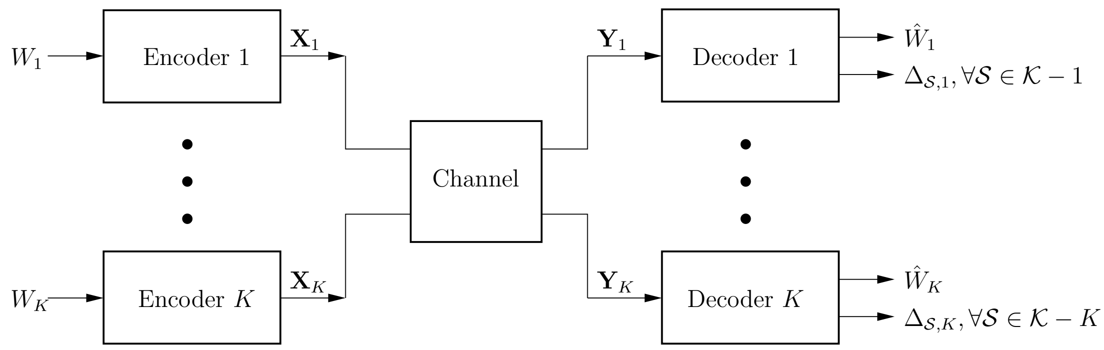

Fig. 1. K-user interference channel with confidential messages.

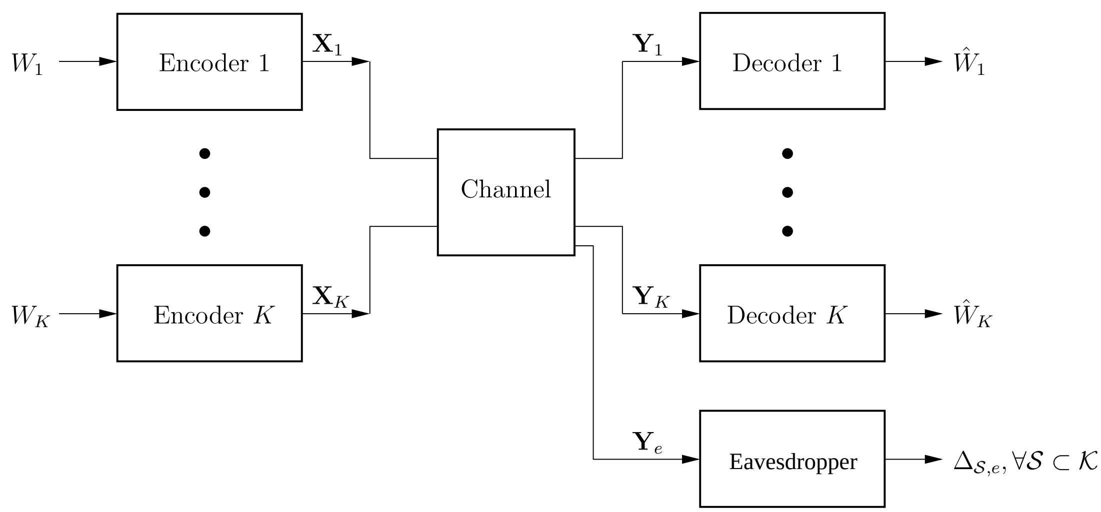

Fig. 2. K-user interference channel with an external eavesdropper.

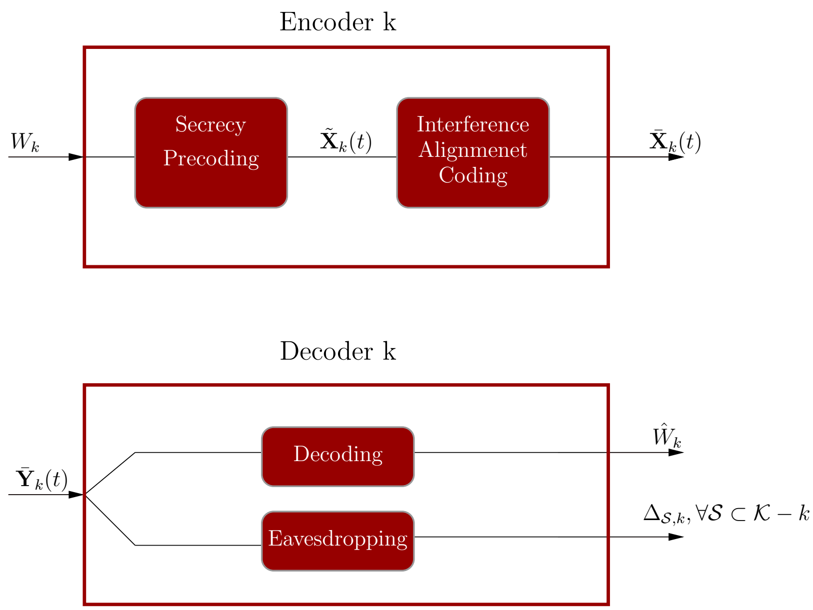

Fig. 3. Proposed encoder and decoder architecture for user k in the K-user interference channel with confidential messages.

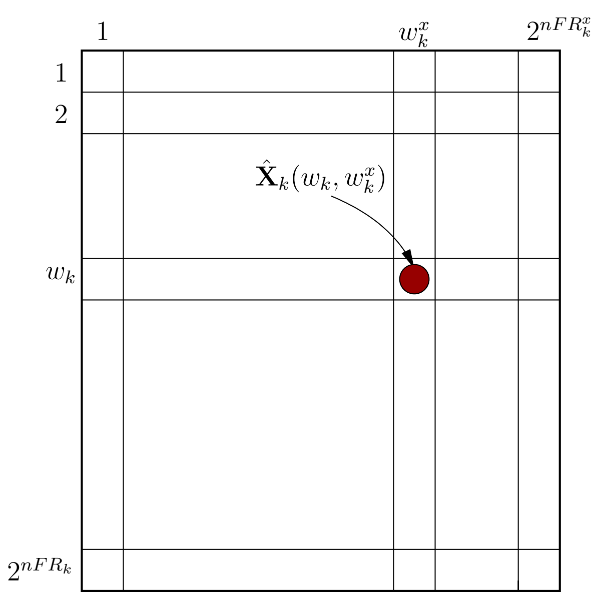

Fig. 4. Proposed codebook structure for user k. The secret message of user k results in the bin index w_k and the randomization index for the corresponding user is w_k^x. Considering these two indices, each entry of the codebook is denoted as $\hat{\mathbf{X}}_k(w_k, w_k^x)$.